Việt Nam

Khuôn khổ Cung cấp Dịch vụ Nhận dạng Điện tử

Tháng 04/2015

GITDR

ĐÔNG Á VÀ THÁI BÌNH DƯƠNG

Mục lục

HÌNH ẢNH VÀ BẢNG BIỂU

Từ và thuật ngữ viết tắt

Từ viết tắt	Từ đầy đủ
AEBA	Tài khoản ngân hàng truy cập bằng Aadhaar (Mã căn cước của Ấn Độ)
AES	Chuẩn mã hoá tiên tiến
AITA	Cục ứng dụng CNTT
ANSI	Viện Tiêu chuẩn Quốc gia Hoa Kỳ
APB	Cầu Thanh toán bằng Aadhaar (mã căn cước của Ấn Độ)
API	Giao diện lập trình ứng dụng
ASA	Cơ quan quản lý dịch vụ xác thực
ATM	Máy rút tiền tự động
AUA	Cơ quan quản lý người sử dụng dịch vụ xác thực
BC	Đại diện ngân hàng
BFD	Phát hiện ngón tay tốt nhất
BIN	Mã số nhận dạng của ngân hàng
BoV	Ngân hàng Việt Nam (Bank of Vietnam)
CA	Cơ quan có thẩm quyền chứng nhận
CBS	Khách hàng/người thụ hưởng/người đăng ký thuê bao
CBS	Hệ thống ngân hàng lõi
CIC	Trung tâm Thông tin Tín dụng
CIDR	Trung tâm Lưu trữ Dữ liệu Nhận dạng Tập trung
CMB	Uỷ ban Di trú của Công dân
CRIDS	Trung tâm Lưu trữ dữ liệu định danh điện tử Công dân Tập trung
CRL	Danh mục huỷ chứng nhận
CSP	Nhà cung cấp dịch vụ chứng nhận
DDoS	Tấn công bằng từ chối dịch vụ phân tán
DDSVP	Thủ tục Thẩm định và Chuẩn mực Dữ liệu Dân số
DIT	Cục Công nghệ và Thông tin
DMZ	Khu phi quân sự
DoB	Ngày sinh
DoS	Từ chối dịch vụ
DSA	Luật chữ ký số
DSS	Hệ thống hỗ trợ quyết định
DSS	Dịch vụ chữ ký số
ECB	Sổ mã điện tử
EIDAV	Cơ quan Quản lý định danh điện tử Việt Nam
eDocument	Tài liệu điện tử
eEBA	Tài khoản điện tử truy cập bằng định danh điện tử (eID)

Từ viết tắt	Từ đầy đủ
EHR	Hồ sơ y tế điện tử/ Y bạ điện tử
eID	Định danh điện tử
EISDF	Khuôn khổ cung cấp dịch vụ theo định danh điện tử
EISDP	Hệ thống cung cấp dịch vụ nhận dạng điện tử
eKYC	Nhận dạng và xác thực khách hàng điện tử
EMS	Phần mềm giám sát doanh nghiệp
ePayment	Thanh toán điện tử
ePB	Cầu thanh toán bằng định danh điện tử (eID)
eSP	Hệ thống tạo nguồn thông tin định danh điện tử (eID)
FIR	Độ phân giải hình ảnh vân tay
FIPS	Tiêu chuẩn xử lý thông tin liên bang
FMR	Độ phân giải chi tiết vân tay
GB	Gigabyte
GbE	Gigabit Ethernet
GoV	Chính phủ Việt Nam
GPRS	Dịch vụ dữ liệu di động theo gói
GSM	Hệ thống thông tin di động toàn cầu
HMAC	Mã nhận thực bản tin dựa trên hàm Hash
HTTP	Giao thức truyền siêu văn bản
HTTPS	Giao thức truyền siêu văn bản an toàn
HVAC	Điều hoà không khí, thông gió và sưởi ấm
ICT	Công nghệ thông tin và truyền thông
IDA	Luật tài liệu chứng minh nhận dạng
IIR	Độ phận giải hình ảnh võng mạc
IP	Giao thức internet
ISCA	Tổ chức sử dung dịch vụ nhận dạng
ISMS	Hệ thống quản lý an ninh thông tin
ISO	Tổ chức Tiêu chuẩn Quốc tế
ISPA	Tổ chức cung cấp dịch vụ nhận dạng
IT	Công nghệ thông tin
ITU	Liên đoàn Viễn thông Quốc tế
IVR	Trả lời bằng giọng nói tương tác
KYC	Nhận dạng và xác thực khách hàng
KYR	Nhận dạng và xác thực cư dân
LDAP	Giao thức truy cập nhanh các dịch vụ thư mục
LoB	Lĩnh vực nghiệp vụ
LPG	Khí hoá lỏng
MB	Megabyte

Từ viết tắt	Từ đầy đủ
MBPS	Megabit trên giây
MIC	Bộ Thông tin và Truyền thông
MIS	Hệ thống thông tin quản lý
MISP	Nhà cung cấp dịch vụ nhận dạng được quản lý
MIT	Bộ Công nghệ Thông tin
MoE	Bộ Môi trường
MoET	Bộ Giáo dục và Đào tạo
MoF	Bộ Tài chính
MoH	Bộ Y tế
MoLISA	Bộ Lao động Thương binh và Xã hội
MNO	Nhà điều hành mạng di động
MPS	Bộ Công An
NAF	Khuôn khổ xác thực điện tử quốc gia
NEPS	Dịch vụ thanh toán điện tử quốc gia
NESP	Hệ thống tạo nguồn thông tin định danh điện tử quốc gia
NFC	Công nghệ giao tiếp tầm ngắn
NID	Hệ thống định danh điện tử quốc gia
NIDAV	Cơ quan Quản lý Nhận dạng Quốc gia Việt Nam
NIN	Mã số chứng minh nhận dạng quốc gia
NIPS	Hệ thống bảo vệ xâm nhập mạng
NISDF	Khuôn khổ cung cấp dịch vụ nhận dạng quốc gia
NISDP	Hệ thống cung cấp dịch vụ nhận dạng quốc gia
NREGS	Chương trình bảo lãnh việc làm nông thôn quốc gia
NSP	Nhà cung cấp dịch vụ mạng
OCSP	Giao thức kiểm tra chứng thực trực tuyến
OTA	Cập nhật phần mềm từ xa
OTP	Mật khẩu dùng một lần
PAN	Số tài khoản vĩnh viễn
PC	Máy tính cá nhân
PDCA	Lập kế hoạch – thực hiện – kiểm tra – hành động
PDPA	Luật bảo vệ dữ liệu cá nhân
PID	Dữ liệu nhận dạng cá nhân
PIN	Mã số nhận dạng cá nhân
PKCS	Tiêu chuẩn mã hoá công khai
PKI	Cơ sở hạ tầng mã khoá công khai
PoA	Chứng minh địa chỉ
PoI	Chứng minh nhận dạng
PoP	Điểm đăng nhập mạng

Từ viết tắt	Từ đầy đủ
PoS	Máy thanh toán tiền bằng thẻ (máy PoS)
PPP	Quan hệ hợp tác công-tư
PSU	Thực thi dịch vụ công
PUB	Ấn bản
PUE	Hiệu quả sử dụng điện
PUK	Mã mở khoá cá nhân
QA	Đảm bảo chất lượng
RA	Tổ chức quản lý đăng ký
RAM	Bộ nhớ truy xuất ngẫn nhiên (Bộ nhớ RAM)
RDBMS	Hệ thống quản lý cơ sở dữ liệu quan hệ
RPM	Vòng quay trên một phút
SAN	Mạng vùng lưu trữ
SAS	Chuẩn giao tiếp SCSI theo se-ri
SBV	Ngân hàng Nhà nước Việt Nam
SDK	Bộ công cụ phát triển phần mềm
SHA	Thuật toán Hash bảo mật
SI	Nhà tích hợp giải pháp
SIM	Mô-đun nhận dạng người đăng ký thuê bao (thẻ SIM vật lý, phần mềm hoặc các hình thức khác)
SLA	Thoả thuận về mức độ dịch vụ
SMS	Dịch vụ tin nhắn ngắn
SMSC	Trung tâm dịch vụ tin nhắn ngắn
SOAP	Giao thức truy suất đối tượng đơn giản (giao thức SOAP)
SQL	Ngôn ngữ truy vấn theo cấu trúc (SQL)
SSCD	Thiết bị tạo chữ ký bảo mật
SSL	Giao thức truyền nhận bảo mật (Giao thức SLL)
SSO	Đăng nhập một lần (SSO)
STQC	Chứng nhận chất lượng và kiểm thử về chuẩn hoá
TA	Hỗ trợ kỹ thuật
TB	Terabyte
ToR	Top of Rack
TPS	Số giao dịch trên một giây
TSP	Nhà cung cấp dịch vụ tin cậy
TSP	Nhà cung cấp dịch vụ theo dấu thời gian
UID	Mã số nhận dạng duy nhất
UIDAI	Tổng cục Nhận dạng duy nhất Ấn Độ
UPS	Bộ lưu điện
URL	Bộ định vị tài nguyên đồng nhất (URL)

Từ viết tắt	Từ đầy đủ
USSD	Dữ liệu dich vụ bổ sung phi cấu trúc (USSD)
VGCA	Cơ quan quản lý chứng nhận của Chính phủ Việt Nam
VM	Máy ảo
VNPT	Tập đoàn Bưu điễn và Viễn thông Việt Nam
VSS	Bảo hiểm Xã hội Việt Nam
W3C	Hiệp hội lập ra các chuẩn cho internet
WPKI	Cơ sở hạ tầng mã khoá công cộng không dây
XAdES	Chữ ký điện tử tiên tiến theo ngôn ngữ đánh dấu khả mở XML
XML	Ngôn ngữ đánh dấu khả mở (XML)

Tóm lược Tổng quan

Các bộ ngành thuộc chính phủ và các tổ chức tư nhân tại Việt Nam ngày nay đang phải đối mặt với thách thức nhằm có được mã số nhận dạng duy nhất để nhận dạng và xác thực công dân trong quá trình cung cấp dịch vụ. Chính phủ Việt Nam (CPVN) đã ghi nhận thách thức này, và Bộ Công An hiện đang thí điểm một Hệ thống định danh (NID) mới.

Chính phủ Việt Nam cũng đã bày tỏ quan tâm nhằm tìm hiểu khả năng triển khai một khuôn khổ cung cấp dịch vụ trên cơ sở định danh điện tử đầy đủ. Hệ thống điện tử đó có thể được xây dựng dựa trên hệ thống định danh Quốc gia (NID) đang thí điểm. Để đáp ứng yêu cầu của Chính phủ Việt Nam, Ngân hàng Thế giới (WB) đang tiến hành một hoạt động hỗ trợ kỹ thuật nhằm xác định tầm nhìn và chiến lược, đồng thời đưa ra khuyến nghị nhằm triển khai chiến lược đó. Nghiên cứu này tập trung đề cập tới các hệ thống định danh điện tử (eID) tiên tiến nhằm tăng cường trách nhiệm giải trình và hiệu suất cung cấp dịch vụ.

Đề xuất về tầm nhìn và chiến lược triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) tại Việt Nam được lập trên cơ sở kinh nghiệm của các quốc gia như Ấn Độ, Ét-xtô-nia và Bỉ. Hiện trạng cơ sở hạ tầng công nghệ thông tin và khuôn khổ thể chế của Việt Nam cũng được đưa vào cân nhắc.

Các bài học rút ra qua kinh nghiệm quốc tế được sắp xếp theo các vấn đề chính như: (i) mở rộng năng lực Hệ thống định danh điện tử quốc gia để triển khai định danh điện tử (eID); (ii) hồ sơ định danh điện tử (eID) của công dân bao gồm một Mã số định danh công dân duy nhất toàn quốc gia (NIN), kết nối với các dữ liệu về nhân chủng và sinh trắc có thể được truy cập trực tuyến; (iii) quá trình hình thành hồ sơ định danh điện tử (eID) và Mã số định danh công dân (NIN) là được thực hiện qua một quy trình sinh trắc và loại bỏ trùng lặp tập trung ở cấp quốc gia để đảm bảo tính duy nhất; và (iv) hồ sơ định danh điện tử (eID) có thể xác định nhận dạng của công dân một cách rõ ràng cho các đơn vị ở cả khu vực công và tư nhân trên toàn quốc, mặc dù không nhất thiết phải sử dụng để chứng minh tư cách công dân.

Dịch vụ xác thực định danh điện tử (eID) là một trong những lợi ích chính mà cơ quan quản lý chứng minh ở trung ương có thể đem lại dựa trên cơ sở hạ tầng quốc gia. Mục đích của việc xác thực định danh điện tử là nhằm tạo điều kiện cho những người có định danh điện tử (eID) có thể chứng minh nhận dạng của mình trên phương tiện số và mạng trực tuyến, đồng thời các nhà cung cấp dịch vụ có thể khẳng định nhận dạng do công dân khai báo để cung cấp dịch vụ và quyền lợi một cách chính xác. Các dịch vụ quan trọng khác được đêm lại là khả năng tạo nguồn thông tin định danh điện tử (eID), bằng cách nhúng mã số định danh công dân (NIN) vào các cơ sở dữ liệu của nhà cung cấp dịch vụ; thực hiện quy trình nhận dạng và xác nhận khách

hàng điện tử (eKYC), thanh toán điện tử (ePayment); tài liệu điện tử bảo mật (eDocument); và nhận dạng di động (mobile ID).

Bài học rút ra về mặt kỹ thuật bao gồm phải thiết lập một Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) để thu thập dữ liệu sinh trắc và nhân chủng học được thu thập trong quá trình tuyển chọn với một thủ tục loại bỏ trùng lặp. Mã số định danh công dân (NIN) sau đó được tạo lập ngẫu nhiên để tránh gian lận và mất trộm. Dữ liệu sinh trắc nhằm đảm bảo tính duy nhất và cần sử dụng phối hợp với dữ liệu nhân chủng học.

Các quy trình định danh điện tử (eID), như xác thực nhận dạng điện tử, nhận dạng và xác nhận khách hàng điện tử (eKYC), nhận dạng di động, v.v. có thể được coi là một dịch vụ mạng không lưu lại trạng thái do cơ sở hạ tầng tập trung về định danh điện tử và thông tin được trích xuất từ Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Việc xác thực định danh điện tử có thể dựa trên một hoặc nhiều yếu tố và các yếu tố đó có thể là yếu tố nhân chủng học, sinh trắc học, mật khẩu sử dụng một lần (OTP), chứng nhận số, hoặc các yếu tố kết hợp. Khả năng tương tác liên thông trong xác thực sinh trắc được hỗ trợ qua việc xác định các đặc tả kỹ thuật về thiết bị sinh trắc học, các chuẩn mực dữ liệu và các bộ công cụ phát triển phần mềm chung (SDK), cũng như hàm API của các nhà cung cấp thiết bị khác nhau. Cơ sở hạ tầng CNTT để chạy các quy trình định danh điện tử (eID) có thể được hỗ trợ bằng năng lực kỹ thuật trong nước, công nghệ đảm bảo của các nhà cung cấp trong nước. Thiết kế của hệ thống định danh điện tử theo đề xuất có thể tạo thuận lợi cho việc tích hợp các dịch vụ hiện hành/dự kiến của Chính phủ Việt Nam và của khu vực tư nhân.

Việc sử dụng chức năng nhận dạng di động có thể đơn giản hoá vấn đề chữ ký số và xác thực định danh điện tử (eID) bằng cách thay thế các thẻ thông minh và bộ đọc bằng điện thoại di động và SIM chuyên dụng (có thể là thẻ vật lý, phần mềm hoặc các cơ chế định danh người thuê bao phù hợp khác) cấp cho công dân. Chức năng nhận dạng di động có thể sử dụng sinh trắc hoặc chứng nhận số qua triển khai cơ sở hạ tầng mã khoá công khai không dây (wPKI) và cổng di động của một nhà điều hành mạng di động quốc doanh (MNO). Phương thức xác thực bằng sinh trắc hoặc chứng nhận số và chữ ký có thể sử dụng các dịch vụ trên cơ sở mô hình giao tiếp dựa trên các luồng công việc chuẩn hoá chung, định dạng tài liệu chung và các công nghệ chuẩn mở. Chính phủ Việt Nam có thể thiết lập cổng thông tin Chính phủ điện tử một cửa để chung cấp các dịch vụ điện tử của nhiều cơ quan khác nhau của chính phủ, với vai trò là cổng thông tin cho toàn bộ các cơ quan công quyền.

Bài học rút ra về mặt thể chế cũng đòi hỏi phải thiết lập một cơ cấu tổ chức gồm hai cơ quan riêng biệt của chính phủ: cơ quan quản lý nhà nước tổng thể và cơ quan điều hành các dịch vụ định danh điện tử (eID). Nhận dạng cá nhân phải đảm bảo được tính duy nhất và độc lập với

dịch vụ được cung cấp. Trên đó, ta có thể lập ra một uỷ ban liên bộ ở cấp cao nhất của chính phủ để ban hành các quyết định về định danh điện tử (eID) và các vấn đề liên quan. Cơ cấu tổ chức theo hình thức quan hệ hợp tác công – tư (PPP) có thể mở rộng cũng nên áp dụng để cấp định danh điện tử (eID) có tính bảo mật và chất lượng cao. An ninh ở mức độ cao được đảm bảo bằng cách giới hạn chỉ cho phép một vài tổ chức có thẩm quyền được truy cập trực tiếp vào quy trình định danh điện tử (eID) trực tuyến với tư cách là Tổ chức cung cấp dịch vụ định danh điện tử (ISPA); và chỉ có một Tổ chức sử dung dịch vụ định danh điện tử (ISCA) đăng ký với tổ chức trên mới được yêu cầu thông tin về nhận dạng để cung cấp ra ngoài.

Cơ cấu tổ chức theo hình thức quan hệ hợp tác công – tư (PPP) có thể cần áp dụng cho dịch vụ nhận dạng di động, sinh trắc hoặc chứng nhận số và chữ ký số nhằm phát hành SIM nhận dạng di động và kích hoạt các SIM đó. Những trách nhiệm đó có thể được giao cho một – hoặc một số – nhà điều hành mạng di động (MNO) quốc doanh, trong đó có cả trách nhiệm tạo lập nhận dạng bằng sinh trắc, chứng nhận số và dấu thời gian cho Nhà cung cấp dịch vụ chứng nhận (CSP) và nhà cung cấp dịch vụ dấu thời gian (TSP). Luật chữ ký số (DSA) có thể quy định về vai trò và trách nhiệm liên quan đến cấp chữ ký số. Chính phủ Việt Nam cần lập ra các uỷ ban về chuẩn mực – với thành viên ở cả khu vực công và tư nhân – để xác định ra các chuẩn mực như chuẩn mực về dữ liệu nhân chủng và sinh trắc, công nghệ và quy trình nghiệp vụ.

Bài học rút ra về mô hình hoạt động đòi hỏi phải đăng nhập mới thông tin công dân để cấp định danh điện tử (eID). Đây là khuyến nghị – thay vì sử dụng lại dữ liệu trước đó được nhập bằng các ứng dụng tại các cơ quan khác nhau cảu chính phủ – nhằm đảm bảo có được dữ liệu chất lượng cao. Định danh điện tử eID) dựa trên mô hình hoạt động theo hình thức quan hệ hợp tác công – tư (PPP) bảo mật và có thể mở rộng trong đó chỉ có một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) duy nhất được truy cập trực tiếp. Tổ chức sử dụng dịch vụ định danh điện tử (ISCA), về phần mình, phải yêu cầu Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) liên quan hỗ trợ để lấy thông tin về định danh điện tử (eID) nhằm thực hiện chức năng cung cấp dịch vụ của mình. Cơ quan của chính quyền trung ương chịu trách nhiệm về định danh điện tử (eID) có thể quản lý một cổng thông tin công cộng để nâng cao nhận thức kỹ thuật đồng thời hỗ trợ kỹ thuật cho các cơ quan và tổ chức sử dụng. Một nhu cầu nữa có thể là cần thiết lập một quy trình xác nhận các thiết bị sinh trắc để đảm bảo các thiết bị đó tuân thủ các yêu cầu kỹ thuật của Chính phủ Việt Nam.

Mô hình vận hành dịch vụ nhận dạng di động cũng có thể theo hình thức quan hệ hợp tác công – tư (PPP), trong đó nhận dạng di động do một hoặc một số nhà điều hành cung cấp tại các cơ sở bán lẻ ở địa phương. Công dân có thể kích hoạt dịch vụ trên thiết bị cầm tay của họ bằng SIM chuyên dụng mới. Nhà cung cấp dịch vụ có thể yêu cầu định danh điện tử (eID) từ phía công dân qua dịch vụ tin nhắn ngắn (SMS) sử dụng TSP, theo mã số đăng ký thuê bao hệ thống thông tin

di động toàn cầu (GSM) và/hoặc yêu cầu nhập liệu mã số nhận dạng cá nhân (PIN) để xác thực. Chính phủ Việt Nam có thể thiết lập các trung tâm cuộc gọi là các dịch vụ trực tuyến toàn thời gian, như "DocStop" và "CheckDoc", để tránh gian lận.

Bài học rút ra về can thiệp chính sách cho thấy cần xây dựng hoặc cập nhật Luật tài liệu chứng minh nhận dạng (IDA) để quy định ở cấp độ quốc gia về tạo lập mã số chứng minh nhận dạng quốc gia (NIN), Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID) và định danh điện tử (eID). Luật có thể cho phép định danh điện tử (eID) có giá trị tương đương với các tài liệu chứng minh nhận dạng trên giấy tờ. Luật chữ ký số (DSA) cũng có thể quy định chữ ký viết tay trên giấy và chữ ký số có giá trị pháp lý như nhau. Luật bảo vệ dữ liệu cá nhân (PDPA) cũng có thể được cập nhật để quy định về việc sử dụng cơ sở dữ liệu và dữ liệu cá nhân của các cơ quan công quyền cũng như các tổ chức tư nhân. Các nhà cung cấp dịch vụ ở cả khu vực công và khu vực tư nhân cũng có thể cập nhật các chuẩn mực về nhận dạng và xác thực khách hàng điện tử (KYC) của mình để bổ sung thêm các chức năng về định danh điện tử (eID) và nhận dạng và xác thực khách hàng (eKYC).

Hiện nay, hình thức Chứng minh Nhận dạng (PoI) phổ biến nhất của các nhà cung cấp dịch vụ ở cả khu vực công và khu vực tư nhân là sử dụng Chứng minh thư Nhân dân do Bộ Công an cấp cho công dân. Sự phụ thuộc vào thẻ chứng minh thư cho thấy đây là một thách thức do thẻ là thẻ giấy do cấp tỉnh cấp ra, trong khi chưa có cơ chế để đảm bảo tính duy nhất của nó ở cấp quốc gia. Kết quả là các nhà cung cấp dịch vụ rốt cuộc sẽ thấy đây là cách làm tốn kém do nhận dạng thiếu nhất quán và bị trùng lặp. Chứng minh thư trên giấy cũng đem lại kết quả là rủi ro cao hơn về mất trộm nhận dạng.

Hiện đang có nhu cầu cần xây dựng một Hệ thống định danh điện tử quốc gia hiệu quả hơn và có căn cứ hơn. Việc này có thể bao hàm cả quy trình tạo lập nhận dạng duy nhất cấp quốc gia trên cơ sở Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Hệ thống đó hiện đang được Bộ Công an triển khai.

Bên cạnh đó là nhu cầu định danh điện tử (eID) quốc gia cho công dân Việt Nam để sử dụng cho các mục đích trên internet. Nhu cầu này sẽ khuyến khích sử dụng chính phủ điện tử, hỗ trợ đổi mới về dịch vụ điện tử ở cả khu vực công và tư nhân, đồng thời tăng cường bảo mật an ninh mạng. Định danh điện tử (eID) sẽ tạo điều kiện để công dân có thể yêu cầu và tiếp nhận dịch vụ và quyền lợi từ phía các đơn vị thuộc khu vực công và tư nhân ở bất kỳ nơi đâu, bất kỳ lúc nào, và sử dụng bất kỳ thiết bị nào mà không cần phải có mặt tại một nơi nào đó để xác thực nhận dạng.

Đề xuất về tầm nhìn cho Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể bao gồm các dịch vụ như xác thực, tạo nguồn thông tin, nhận dạng và xác thực khách hàng (eKYC), chữ ký số, thanh toán điện tử (ePayment), và nhận dạng di động (mobile ID). Định danh điện tử (eID) có thể hỗ trợ các loại hình mã thông báo (token) chuẩn khác nhau trên cơ sở: (i) "những gì người sử dụng đang có" như di động/mật khẩu dùng một lần (OTP)/sinh trắc/chứng nhận số; (ii) "những gì người sử dụng biết" như mã số nhận dạng cá nhân (mã PIN); và (iii) "người sử dụng là ai" như vân tay và hình ảnh võng mạc.

Chiến lược triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) bao hàm phải thiết lập cơ sở hạ tầng CNTT tập trung, dùng chung và một hệ thống dịch vụ chung gọi là Hệ thống cung cấp dịch vụ định danh điện tử (EISDP). Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) được sử dụng để cung cấp các dịch vụ định danh điện tử (eID và các ứng dụng chung cho các nhà cung cấp dịch vụ để nhận dạng công dân đảm bảo tính duy nhất. Thành phần chính của hệ thống quản lý tập trung này là một cổng thông tin công cộng dùng chung dưới hình thức một điểm dịch vụ một cửa trực tuyến cho toàn bộ các dịch vụ về định danh điện tử (eID) và các ứng dụng dùng chung như Trung tâm lưu trữ dữ liệu nhận dạng tập trung (CRIDS), Hệ thống thông tin quản lý (MIS), Hệ thống hỗ trợ quyết định (DSS), Phân tích gian lận, và đăng ký Tổ chức cung cấp dịch vụ định danh điện tử (ISPA)/ Tổ chức sử dung dịch vụ định danh điện tử (ISCA).

Cơ sở hạ tầng CNTT bao gồm phần cứng và phần mềm có thể được triển khai tại các trung tâm dữ liệu để chạy các ứng dụng và các dịch vụ định danh điện tử (eID). Cơ sở hạ tầng vật chất này bao gồm trung tâm dữ liệu, trung tâm dữ liệu phục hồi thảm hoạ của của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và trung tâm dữ liệu của Bộ Công An. Các hệ thống an ninh và bảo mật bao gồm các hệ thống bảo mật cho phần cứng và phần mềm, mạng CNTT "end-to-end" và cơ sở vật chất với nhiều lớp bảo vệ được thiết kế để hạn chế chỉ cho phép nhận sự có thẩm quyền mới được thâm nhập và sử dụng dữ liệu sinh trắc.

Mỗi Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể thiết lập một trung tâm dữ liệu với cơ sở hạ tầng CNTT, ứng dụng phần mềm và kết nối mạng bảo mật theo yêu cầu với trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để truy cập các dịch vụ định danh điện tử (eID). Mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) cũng có thể thiết lập một trung tâm dữ liệu để quản lý các ứng dụng cung cấp dịch vụ trực tuyến và các thiết bị đầu máy thanh toán tiền bằng thẻ (máy PoS), nơi công dân có thể đến sử dụng dịch vụ. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) thiết lập mạng CNTT theo yêu cầu để kết nối các cơ sở bán hàng của họ với trung tâm dữ liệu và sau đó kết nối với trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) để chuyển các yêu cầu về dịch vụ định danh điện tử (eID) của mình lên Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) và nhận phản hồi về theo cùng kênh đó.

Khuyến nghị về khuôn khổ thể chế bao gồm các khuyến nghị về vận hành mô hình như hình thành một cơ quan riêng, Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), trực thuộc bộ phụ trách về nhận dạng điện tử, vừa là cơ quan chủ quản vừa theo dõi giám sát Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) và các dịch vụ định danh điện tử (eID). Bộ phụ trách có thể phân cấp trách nhiệm thiết kế, triển khai và quản lý hoạt động cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) đóng vai trò là nhà cung cấp dịch vụ nhận dạng được quản lý (MISP). Các đơn vị khu vực công hoặc khu vực tư nhân muốn sử dụng các dịch vụ định danh điện tử (eID) trong quá trình cung cấp dịch vụ của mình có thể được Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) cho phép truy cập dịch vụ qua hệ thống mạng của cơ quan đó. Chỉ có Tổ chức cung cấp dịch vụ định danh điện tử (ISPA), cho dù thuộc khu vực công hay tư nhân, mới được đăng ký với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để truy xuất trực tiếp thông tin định danh điện tử (eID) nhằm đảm bảo an ninh ở mức độ cao cho cơ sở dữ liệu tập trung này. Nhà cung cấp dịch vụ đó phải chịu trách nhiệm tạo nguồn thông tin về Mã số định danh công dân (NIN) vào cơ sở dữ liệu của mình; nhà cung cấp này cũng chịu trách nhiệm về việc số hoá và tập trung hoá cơ sở dữ liệu của mình. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể cung cấp các công cụ và hướng dẫn về định danh điện tử (eID) cho nhà cung cấp dịch vụ đó trong quá trình tạo nguồn thông tin của họ. Bốn chức năng tác nghiệp chính trong dịch vụ nhận dạng di động (mobile ID) có thể là cung cấp SIM, kích hoạt chứng nhận/ người sử dụng, sử dụng và kết thúc dịch vụ.

Khuyến nghị về mặt thế chế còn bao gồm phải xác định và phân công các vai trò chính cho các thành phần thuộc cơ cấu tổ chức. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), trực thuộc bộ phụ trách về nhận dạng điện tử, có vai trò chính là cơ quan chủ quản vừa theo dõi giám sát việc triển khai và quản lý vận hành Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) và các dịch vụ định danh điện tử (eID). Một Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) có thể đứng ra thay mặt cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) chịu trách nhiệm triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) ó thể là một đơn vị thuộc khu vực công hoặc tư nhân có nhiệm vụ thiết lập kết nối bảo mật với trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để truyền các yêu cầu xác thực định danh điện tử (eID) thay mặt cho Tổ chức sử dung dịch vụ định danh điện tử (ISCA), sau đó nhận phản hồi lại từ các máy chủ xác thực định danh điện tử (eID) đảm bảo an ninh ở mức độ cao. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể là một cơ quan cung cấp dịch vụ thuộc khu vực công hoặc tư nhân, tìm cách sử dụng các dịch vụ định danh điện tử (eID), và người có định danh điện tử (eID) có thể là công dân được Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) cấp định danh điện tử (eID). Các bên liên quan chính trong việc cung cấp dịch vụ nhận dạng di động, ngoài các tổ chức và đơn vị nêu trên, còn có thể bao gồm Tổ chức quản lý đăng ký (RA), chẳng hạn một Nhà điều hành mạng di động

(MNO) chịu trách nhiệm cung cấp SIM chuyên dụng cho công dân; nhà cung cấp dịch vụ tin cậy (TSP) cũng là nhà điều hành di động, nhưng chịu trách nhiệm chuyển tiếp trả lời yêu cầu dịch vụ nhận dạng di động từ Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) vào điện thoại di động của công dân; và Cơ quan có thẩm quyền chứng nhận (CA) chịu trách nhiệm cấp và thẩm định chứng nhận và dữ liệu ký kết theo yêu cầu dịch vụ của nhà cung cấp dịch vụ tin cậy (TSP).

Khuyến nghị về mặt chính sách bao gồm cập nhật và soạn thảo Luật tài liệu chứng minh nhận dạng (IDA) để hướng dẫn cấp quốc gia về ban hành Mã số chứng minh nhận dạng quốc gia (NIN), nhằm đảm bảo định danh điện tử có giá trị pháp lý tương đương như Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID), và cập nhật Luật chữ ký số (DSA) để sử dụng Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) và các dịch vụ định danh điện tử (eID) nhằm cho phép ký chữ ký số và xác định chữ ký số có giá trị pháp lý tương đương chữ ký viết tay.

Để các phản hồi nhận dạng và xác nhận khách hàng điện tử (eKYC) có giá trị pháp lý tương đương như tài liệu giấy, các chính sách liên quan của chính phủ có thể cũng cần được cập nhật. Các nhà cung cấp dịch vụ ở cả khu vực công và khu vực tư nhân có thể cập nhật các thông lệ nhận dạng và xác nhận khách hàng (KYC) của họ nhằm bổ sung tính năng về mã số chứng minh nhận dạng quốc gia (NIN)/ định danh điện tử (eID), và chấp nhận phải hồi nhận dạng và xác nhận khách hàng điện tử (eKYC) là nhận dạng và xác nhận khách hàng (KYC) hợp lệ. Chính sách quốc gia về các chuẩn mực mở như hiện nay nhằm thúc đẩy khả năng tương tác liên thông có thể được cập nhật để bổ sung các thuộc tính sinh trắc và nhân chủng học vào hồ sơ định danh điện tử của công dân trong các chuẩn dữ liệu và siêu dữ liệu, đồng thời các chuẩn mực mở về dữ liệu sinh trắc như hình ảnh vân tay, chi tiết vân tay và hình ảnh võng mạc. Luật bảo vệ dữ liệu cá nhân (PDPA) cũng nên được ban hành để quy định về việc các cơ quan công quyền và các tổ chức thuộc khu vực tư nhân sử dụng thông tin cá nhân.

Đề xuất về chiến lược truyền thông nhằm nâng cao nhận thức và vận động các bên liên quan áp dụng khuôn khổ bao gồm thiết lập một cổng thông tin công cộng, các khoá đào tạo trực tuyến và trên lớp học, các chương trình tăng cường năng lực nhằm vào đối tượng công dân và các quan chức/nhà điều hành, các chương trình xúc tiến và khuyến trương, các tài liệu kỹ thuật dành cho các chuyên gia phần mềm và những người có thẩm quyền quyết định về mặt kỹ thuật có quan tâm đến việc sử dụng các dịch vụ định danh điện tử (eID).

Việc triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể được thực hiện theo hai giai đoạn: giai đoạn thí điểm và triển khai rộng đầy đủ. Giai đoạn thí điểm nhằm thiết lập Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF); và trách nhiệm thành lập Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể giao cho bộ phụ trách. Việc này bao gồm

phải thiết lập trung tâm dữ liệu cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) di chuyển dữ liệu của công dân từ dự án thí điểm hiện tại của Bộ Công an sang Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Ngoài ra là nhiệm vụ triển khai các chức năng sau: xác thực định danh điện tử (eID), nhận dạng và xác thực khách hàng điện tử (eKYC), tạo nguồn thông tin định danh điện tử (eID), và nhận dạng di động. Có thể bố trí hai Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và một Cơ quan cung cấp dịch vụ định danh điện tử (ISPA). Về nhận dạng di động, Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể phân cấp việc thiết kế và triển khai cho Tập đoàn Bưu chính Viễn thông Việt Nam (VNPT) hoặc Viettel, để họ đảm nhận vai trò Tổ chức quản lý đăng ký (RA) và Nhà cung cấp dịch vụ tin cậy (TSP).

Dự toán ngân sách cao cho thiết kế và triển khai dự án thí điểm và triển khai rộng chỉ mang tính hướng dẫn. Dự toán này nhằm chỉ ra quy mô đầu tư có thể phải tính dến để thiết kế và triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Tổng mức đầu tư cho việc thiết kế, triển khai và quản lý vận hành giai đoạn thí điểm trong một năm (không triển khai nhận dạng di động) được dự toán ở mức 54 triệu USD. Kinh phí này bao gồm thiết lập và triển khai các cơ sở hạ tầng thể chế và CNTT cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và hai Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể có một điểm cung cấp dịch vụ tại một quận tại Hà Nội. Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) được lựa chọn trong giai đoạn thí điểm có thể là VNPT hoặc Viettel; còn Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể là Bảo hiểm Xã hội Việt Nam (VSS) hoặc Ngân hàng Việt Nam (BoV). Tổ chức quản lý đăng ký (RA) và Nhà cung cấp dịch vụ tin cậy (TSP) có thể là Viettel hoặc VNPT. Dữ liệu sinh trắc và nhân chủng học được lưu trữ tại Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) thuộc Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể được tải nhập từ cơ sở dữ liệu của Bộ Công An (MPS) với dữ liệu về công dân được thu thập trong dự án thí điểm hệ thống cơ sở dữ liệu dân cư hiện nay. Dự kiến dữ liệu do Bộ Công an thu thập đã bao phủ ít nhất một triệu công dân. Dự toán kinh phí thí điểm dựa trên việc cung cấp 100.000 nhận dạng di động. Tổng mức đầu tư để triển khai rộng trong năm năm vận hành dự kiến lên đến 192 triệu USD. Dự toán này đã bao gồm tăng cường năng lực cơ sở hạ tầng thể chế và CNTT đã thiết lập trong giai đoạn thí điểm. Ngoài ra là kinh phí bổ sung thêm một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và thêm khoảng 20 Tổ chức sử dung dịch vụ định danh điện tử (ISCA) với các điểm cung cấp dịch vụ của mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) dự kiến lên đến 124 điểm (mỗi tỉnh một điểm và cứ 10 quận/huyện lại có một điểm). Mười Tổ chức quản lý đăng ký (RA) bổ sung sẽ thành lập thêm 100 điểm phục vụ cho mỗi Tổ chức quản lý đăng ký (RA) và hai Nhà cung cấp dịch vụ tin cậy (TSP) bổ sung. Dự toán kinh phí đó còn bao gồm cung cấp các SIM mới để nhận dạng di động cho 90 triệu công dân. Ngoài ra là chi phí cho các nỗ lực xây dựng năng lực, thiết lập các chuẩn mực khung và xây dựng các chính

sách cần thiết của chính phủ để triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) và dịch vụ định danh điện tử (eID). Tổng kinh phí để thiết kế và triển khai hai giai đoạn trên nếu không triển khai phương án nhận dạng di động tuỳ chọn được dự toán ở mức 246 triệu USD.

Dự toán kinh phí tăng thêm để triển khai phương án nhận dạng di động tuỳ chọn trong giai đoạn thí điểm là 4 triệu USD. Số này bao gồm cung cấp 100.000 nhận dạng di động, một Tổ chức quản lý đăng ký (RA) và một Nhà cung cấp dịch vụ tin cậy (TSP) trong giai đoạn thí điểm. Dự toán kinh phí để triển khai phương án nhận dạng di động tuỳ chọn trong giai đoạn triển khai rộng là 61 triệu USD. Số này bao gồm cung cấp 90 triệu nhận dạng di động, hai Tổ chức quản lý đăng ký (RA), một Nhà cung cấp dịch vụ tin cậy (TSP) và 123 điểm cung cấp dịch vụ đăng ký cho mỗi tổ chức.

Tài liệu này có thể là cơ sở để xây dựng tầm nhìn và kế hoạch chi tiết để triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Để triển khai hiệu quả Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF), ta cần bóc tách chi tiết kiến trúc kỹ thuật tổng thể của khuôn khổ thành các hợp phần kỹ thuật, đồng thời phải đánh giá chi tiết tình trạng cơ sở hạ tầng CNTT hiện nay. Kế hoạch triển khai chi tiết cũng phải đề cập đến các vấn đề chính sách, cơ cấu tổ chức, mô hình vận hành, nguồn lực cơ sở hạ tầng, và các giai đoạn triển khai từng hợp phần.

1.0 Giới thiệu

1.1 Mục đích

Tài liệu nghiên cứu này nhằm đề xuất tầm nhìn và các khuyến nghị triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) tại Việt Nam. Ngoài ra tài liệu cũng chỉ ra các vai trò của rất nhiều các bên liên quan (khu vực công, khu vực tư nhân, cộng đồng phát triển, v.v.) trong lĩnh vực này. Tài liệu nghiên cứu đưa ra khuyến nghị về các loại dịch vụ định danh điện tử (eID) phù hợp và tiên tiến có thể được triển khai để chuyển đổi và nâng cao trách nhiệm giải trình cũng như hiệu suất cung cấp dịch vụ tại nhiều lĩnh vực. Những khuyến nghị đó dựa trên nghiên cứu kinh nghiệm quốc tế và xác định các khả năng trên cơ sở đánh giá hiện trạng trong nước. Nội dung tài liệu đặc biệt quan tâm đến các hệ thống định danh điện tử (eID) vận hành trên điện thoại di động, cũng như các hệ thống có tiềm năng phát triển rộng ở cả khu vực công và khu vực tư nhân ở Việt Nam.

1.2 Bối cảnh và sự cần thiết

Nhiều bằng chứng cho thấy các hệ thống cung cấp dịch vụ định danh điện tử (eID) đem lại rất nhiều lợi ích cho các cá nhân, doanh nghiệp và chính quyền. Việc mở rộng các hệ thống định dạng quốc gia sang định danh điện tử (eID) sử dụng các công nghệ sinh trắc và công nghệ số có thể dẫn đến mở rộng phạm vi của các hệ thống nhận dạng chính thức. Đây là tiền đề để phát triển. Rõ ràng, tình trạng thiếu khả năng xác thực bản thân gây cản trở đến việc một cá nhân được tiếp cận các quyền và dịch vụ cơ bản của khu vực công và khu vực tư nhân.

Định danh điện tử (eID) được coi là phương tiện quan trọng để đổi mới trong khu vực công và tư nhân vì nó hỗ trợ nhiều về xác thực điện tử; ngoài ra nó còn hỗ trợ cải thiện giá trị của các dịch vụ đòi hỏi phải đảm bảo và bảo mật ở mức cao. Việc sử dụng định danh điện tử (eID) đem lại lợi ích kinh tế về mặt giảm chi phí và tăng năng suất trong khu vực công, đồng thời hỗ trợ khả năng sử dụng các dịch vụ trực tuyến. Sự đảm bảo và tin cậy liên quan đến nhận dạng trực tuyến – kể cả sự tin cậy hai chiều giữa các bên tham gia giao dịch hoặc trao đổi trực tuyến – đem lại sự thuận tiện cho tất cả các bên tham gia.

Các hệ thống định danh điện tử (eID) có thể giúp giảm gian lận trong nhận dạng và cho phép các cá nhân sử dụng dịch vụ một cách an toàn hơn trong rất nhiều hoàn cảnh như giao dịch ngân hàng qua điện thoại, các ứng dụng chăm sóc sức khoẻ qua di động. Vì trộm danh tính là một thách thức lớn, chính phủ ở nhiều quốc gia trên thế giới đang phải thiết lập các hệ thống cung cấp dịch vụ dựa trên định danh điện tử (eID). Các hệ thống này hỗ trợ cung cấp lợi ích cho

những đối tượng được hưởng, ví dụ những người nghèo nhất trong diện nghèo (những người đủ tiêu chuẩn hưởng phúc lợi xã hội, cứu trợ thiên tai, v.v. như tại Ken-nya và Pa-kít-stan) và người cao tuổi (ví dụ, những người hưởng hưu trí tại Ni-giê-ria). Các hệ thống này cũng tạo điều kiện cung cấp các dịch vụ như trợ cấp có điều kiện bằng tiền mặt (cho các mục đích hỗ trợ giáo dục như tại Ấn Độ và Tan-za-nia).

Vai trò của khu vực tư nhân trong việc triển khai cơ sở hạ tầng cung cấp dịch vụ trên cơ sở định danh điện tử (eID) cũng hết sức quan trọng vì tiềm năng đảm bảo tính khả thi và bền vững của dự án. Rất nhiều quốc gia như Bỉ, Ét-xtô-nia và Ấn Độ đã triển khai thành công các hệ thống định danh điện tử (eID) theo mô hình quan hệ hợp tác công – tư (PPP).

Hầu hết các bộ ngành của chính phủ và các tổ chức tại khu vực tư nhân ở Việt Nam ngày nay đang gặp phải thách thức là không có được nhận dạng duy nhất cho mỗi công dân. Điều này có thể do không có một hệ thống tập trung của quốc gia để cấp mã định danh duy nhất cho công dân. Thẻ chứng minh thư nhân dân hiện nay được cấp ở cấp Quận/ Huyện do đó mã số chứng minh được cấp cho công dân không có tính duy nhất trên toàn quốc.

Trong bối cảnh đó, Chính phủ Việt Nam đã bày tỏ quan tâm nhằm xem xét khả năng triển khai một Khuôn khổ đầy đủ về cung cấp dịch vụ trên cơ sở định danh điện tử (EISDF). Bộ Công an (MPS) hiện đang thí điểm một Hệ thống định danh điện tử quốc gia mới. Ngoài ra, Chính phủ Việt Nam cũng đang chuẩn bị các điều kiện cần thiết để triển khai Cơ sở hạ tầng mã khoá công khai (PKI) và cấp thẻ công dân bắt buộc. Chính phủ Việt Nam cũng đang có kế hoạch xây dựng một Khuôn khổ xác thực điện tử quốc gia (NAF) nhằm tạo môi trường thuận lợi hết sức cần thiết để người sử dụng có thể tiếp cận các dịch vụ của chính phủ và tiếp cận phúc lợi xã hội bằng định danh điện tử (eID). Trong thời gian tới, Chính phủ Việt Nam mong muốn tận dụng các hạ tầng đó để tối ưu hoá đầu tư công, đẩy mạnh cung cấp dịch vụ công và chính phủ điện tử cho công dân Việt Nam, đặc biệt là những người nghèo nhất.

Trên cơ sở đó, tài liệu nghiên cứu này có mục tiêu nhằm xác định tầm nhìn và chiến lược triển khai nhằm cung cấp dịch vụ trên cơ sở định danh điện tử tại Việt Nam. Tài liệu nghiên cứu này cũng đặc biệt qua tâm đến các dịch vụ nhận dạng mới nhằm tăng cường trách nhiệm giải trình và hiệu suất cung cấp dịch vụ. Tài liệu cũng giới thiệu về các hệ thống và đưa ra các phương án về chia sẻ rủi ro, đầu tư và lợi ích qua hình thức quan hệ hợp tác công – tư (PPP).

2.0 Phương pháp luận

Phương pháp luận của nghiên cứu này dựa trên cách tiếp cận ba bước, bao gồm các hoạt động dưới đây.

1. Nghiên cứu kinh nghiệm quốc tế về cung cấp dịch vụ trên cơ sở định danh điện tử (eID). Đây là việc cần thiết nhằm xác định các yếu tố chính có ảnh hưởng đến việc triển khai và áp dụng định danh điện tử (eID), đồng thời xác định những thông lệ tốt nhất cho thể áp dụng cho Việt Nam trên cơ sở các khái niệm chung về nhận dạng điện tử, các khía cạnh kỹ thuật và thể chế, và chính sách.

2. Xác định tầm nhìn về định danh điện tử (eID) cho Việt nam trên cơ sở những bài học rút ra qua kinh nghiệm quốc tế.

3. Đề xuất khuyến nghị xây dựng tầm nhìn về định danh điện tử (eID) và chiến lược triển khai trên cơ sở phân tích hiện trạng cơ sở hạ tầng công nghệ thông tin (CNTT) và khuôn khổ thể chế tại Việt Nam.

Phương thức nghiên cứu của tài liệu nghiên cứu này được mô tả dưới đây.

1. Thu thập dữ liệu thứ cấp qua nghiên cứu tài liệu kết hợp với nghiên cứu tại thực địa qua phối hợp với các biên liên quan.

2. Thu thập thông tin về các thông lệ quốc tế tốt nhất qua nghiên cứu tài liệu, đặc biệt là thông tin liên quan đến kinh nghiệm quốc tế về cung cấp dịch vụ trên cơ sở định danh điện tử (eID).

3. Thực hiện tham vấn rộng trong nước với các bên liên quan để tìm hiểu về quan điểm và kiến thức của họ cũng như khuyến nghị triển khai. Việc này bao gồm thu thập thông tin về Hệ thống định danh điện tử quốc gia hiện hành, các đề án công nghệ thông tin và truyền thông liên quan, môi trường thuận lợi và cơ sở hạ tầng.

4. Thu thập thông tin đầu vào từ các bên liên quan, phối hợp với các bên liên quan trong các hoạt động liên quan và chia sẻ kết quả nghiên cứu với các tổ chức liên quan như các bộ khác nhau – đặc biệt là Bộ Công an, Bộ Thông tin và Truyền thông, Bộ Lao động, Thương binh và Xã hội, Bộ giáo dục và Đào tạo, Bộ Tư pháp, Bộ Nội vụ, Bộ Y tế, Bộ Nông nghiệp và Phát triển Nông thôn). Các bên liên quan khác bao gồm Cục Ứng dụng CNTT (AITA), Ngân hàng Nhà nước Việt Nam, các ngân hàng tư nhân, các doanh nghiệp viễn thông lớn và Cơ quan quản lý chứng nhận của Chính phủ Việt Nam (VGCA).

3.0 Bài học rút ra qua kinh nghiệm quốc tế

Chính phủ Việt Nam có nhiều phương án khác nhau để triển khai các dịch vụ định danh điện tử (eID). Một vài trong số các kết luận chính về các khái nhiệm chung, cũng như các khía cạnh về thể chế và kỹ thuật có thể ảnh hưởng đến công tác triển khai như mô tả dưới đây được đúc rút qua kinh nghiệm của các quốc gia được nghiên cứu; bao gồm Ấn Độ, Ét-xtô-nia và Bỉ. Phụ lục 5 cung cấp mô tả chi tiết kinh nghiệm cụ thể của mỗi quốc gia trong đó.

Các ý tưởng chung. Một số ý tưởng chung về các dịch vụ định danh điện tử (eID) đúc rút qua kinh nghiệm của Ấn Độ, Ét-xtô-nia và Bỉ được trình bày dưới đây.

1. **Mở rộng hệ thống nhận dạng của quốc gia để bao gồm cả nhận dạng điện tử.** Hệ thống nhận dạng của quốc gia (NID) có thể được mở rộng dể hỗ trợ định danh điện tử (eID) có thể được xác nhận trực tuyến. Lợi ích chính là khả năng sử dụng nhận dạng di động nhằm tạo điều kiện cho các đơn vị cung cấp dịch vụ có thể xác thực cá nhân là một người duy nhất, ở bất kỳ đâu, vào bất kỳ lúc nào. Ngoài ra, nó còn hỗ trợ loại bỏ nhận dạng trùng lặp và giả mạo qua đó tạo điều kiện mở rộng dịch vụ, cho phép các đơn vị cung cấp dịch vụ có thể sử dụng nhiều kênh khác nhau để cung cấp dịch vụ, giảm tình trạng lợi dụng chức quyền và gây phiền nhiễu cho đối tượng thụ hưởng qua giảm phụ thuộc vào các quy trình thủ công, hỗ trợ nâng cao hiệu suất cung cấp dịch vụ, cung cấp bút tích kiểm tra điện tử, giảm chi phí và rủi ro mất trộm nhận dạng.
    a. Nhận dạng quốc gia (NID) của một công dân có thể được mở rộng để bổ sung hồ sơ định danh điện tử (eID) duy nhất, bao gồm một Mã số định danh công dân (NIN) duy nhất, gắn với các dữ liệu sinh trắc và nhân chủng học của công dân có thể được truy xuất trực tuyến.
    b. Việc hình thành hồ sơ định danh điện tử (eID) quốc gia với Mã số định danh công dân (NIN) là một quy trình tập trung nhằm loại bỏ trùng lặp thông tin sinh trắc ở cấp quốc gia để tạo điều kiện cung cấp nhận dạng duy nhất để Chứng minh Nhận dạng (PoI) mang tính pháp lý có thể chấp nhận với tất cả các nhà cung cấp dịch vụ ở cả khu vực công và tư nhân. Cần thiết lập cơ sở hạ tầng để hình thành Hệ thống định danh điện tử quốc gia (NID) và cung cấp các dịch vụ định danh điện tử (eID).
    c. Mã số định danh công dân (NIN) và định danh điện tử (eID) có thể chứng minh về nhận dạng của một cá nhân, nhưng không chứng minh được tư cách công dân của công dân đó (ví dụ trường hợp Ấn Độ).
    d. Mã số định danh công dân (NIN) nhận dạng công dân và cung cấp phương tiện để xác định nhận dạng đó cho các đơn vị ở khu vực công và tư nhân trên cả nước.

Ba đặc điểm chính của Mã số định danh công dân (NIN) là tính không đổi (không thay đổi trong suốt cuộc đời của công dân), tính duy nhất (không bao giờ có chuyện hai công dân có cùng Mã số định danh công dân (NIN)) và tính sử dụng phổ quát (mã nhận dạng đó có thể được sử dụng tại các ứng dụng và môi trường khác nhau).

2. **Xác thực định danh điện tử.** Mục đích của xác thực định danh điện tử (eID) là tạo điều kiện để người có định danh điện tử (eID) chứng minh được nhận dạng của mình trực tuyến và bằng kỹ thuật số; đồng thời các nhà cung cấp dịch vụ có thể khẳng định thông tin khai báo về nhận dạng của công dân để cung cấp dịch vụ và cho phép tiếp cận lợi ích.
    a. Quy trình xác thực định danh điện tử (eID) và Mã số định danh công dân (NIN) được các nhà cung cấp dịch vụ sử dụng để xác định sự hiện diện và chứng minh về việc cung cấp dịch vụ, xác nhận về nhận dạng và xác thực khác hàng (KYC). Đồng thời đó là cách để thống nhất thông tin xoanh quanh công dân.
    b. Xác thực định danh điện tử (eID) cho phép khẳng định về đối tượng thụ hưởng nhằm đảm bảo cung cấp dịch vụ cho đúng người. Đồng thời nó còn hỗ trợ theo dõi sự thời gian làm việc trong trường hợp trả lương theo báo cáo về số ngày làm việc thực tế của đối tượng thụ hưởng cho chương trình.
    c. Xác thực định danh điện tử (eID) hỗ trợ nhận dạng và xử lý quá trình thẩm nhận để thiết lập thông tin nhận dạng và xác nhận khách hàng (KYC), là yêu cầu chính để tuyển chọn hoặc mở tài khoản cho khách hàng mới. Việc sử dụng xác thực định danh điện tử (eID) làm giảm đáng kể chi phí của quy trình nhận dạng và xác nhận khách hàng (KYC). Đó cũng là cách để chứng minh nhận dạng chung cho các yêu cầu chuẩn liên quan đến an ninh như tại sân bay, khách sạn và các cơ sở khác, hay chứng minh nhận dạng trong thi cử ở trường học. Đó cũng là cách để thẩm định và xử lý dữ liệu nhân chủng học trong các cơ sở dữ liệu về cung cấp dịch vụ nhằm hỗ trợ quản lý và làm sạch cơ sở dữ liệu.

3. **Tạo nguồn thông tin về Mã số chứng minh nhận dạng quốc gia (NIN).** Để các nhà cung cấp dịch vụ tận dụng được sự hỗ trợ về định danh điện tử (eID) trong việc cung cấp các sản phẩm dịch vụ của họ, trước hết họ cần phải thu thập thông tin về Mã số định danh công dân (NIN) duy nhất đối với khách hàng, đối tượng thụ hưởng và người đăng ký thuê bao của họ. Sau khi đã có được thông tin đó, nhà cung cấp dịch vụ phải sắp xếp đối chiếu và lưu trữ thông tin đó cùng với mã số nhận dạng duy nhất của riêng họ (ví dụ mã số khách hàng hoặc đối tượng thụ hưởng) trong các cơ sở dữ liệu riêng của họ. Quy

trình đưa thông tin về Mã số định danh công dân (NIN) của khách hàng, đối tượng thụ hưởng và người đăng ký thuê bao và cơ sở dữ liệu của dịch vụ cung cấp được gọi là tạo nguồn thông tin về định danh điện tử (eID). Quy trình tạo nguồn thông tin nhất thiết phải thực hiện trước khi số hoá và tập trung hoá thông tin trong cơ sở dữ liệu của nhà cung cấp dịch vụ, và sẽ hỗ trợ cả phương pháp áp từ trên xuống và phương pháp hữu cơ.

a. Phương pháp áp từ trên xuống sử dụng dữ liệu cá nhân hiện tại của công dân qua quy trình đăng ký trước đó và không đòi hỏi phải liên hệ trực tiếp với công dân đó. Còn phương pháp hữu cơ đòi hỏi nhà cung cấp dịch vụ phải liên hệ với công dân đó, hoặc ngược lại, để thực hiện tạo nguồn thông tin. Sau khi hoàn thành quá trình tạo nguồn thông tin là quá trình xác thực sinh trắc học hoặc nhân chủng học, đặc biệt khi không cập nhật được trữ tiếp cơ sở dữ liệu về cung cấp dịch vụ.
b. Quy trình tạo nguồn dữ liệu được thiết kế để xử lý những thách thức chung trong các cơ sở dữ liệu cung cấp dịch vụ. Đó là dữ liệu không đầy đủ hoặc thông tin lặp giữa các nguồn dữ liệu khác nhau hoặc ngôn ngữ khác nhau.
c. Cơ quan chủ quản của chính phủ cần cung cấp hệ thống tạo nguồn thông tin tập trung và các tiện ích tạo nguồn thông tin để các nhà cung cấp dịch vụ sử dụng nhằm thực hiện quy trình một cách chính xác, nhanh hơn và liền mạch. Đây là yêu cầu quan trọng để áp dụng nhanh chóng hơn việc cung cấp dịch vụ trên cơ sở định danh điện tử (eID).

4. **Cung cấp các nhóm và phương tiện vật chất hỗ trợ.** Cơ quan chủ quản của chính phủ cần xây dựng các nhóm hỗ trợ và phương tiện vật chất để hỗ trợ cho các nhà cung cấp dịch vụ áp dụng và triển khai quy trình cung cấp dịch vụ theo định danh điện tử (eID). Các nhóm hỗ trợ bao gồm nhóm hỗ trợ ứng dụng, các tư vấn được mời tham gia, các nhà cung cấp phần mềm để hỗ trợ các nhà cung cấp dịch vụ xây dựng các ứng dụng và quy trình cần thiết. Tài liệu hỗ trợ để hướng dẫn việc tận dụng và tích hợp chức năng định danh điện tử (eID) trong các giải pháp cho nhà cung cấp dịch vụ bao gồm cả khuôn khổ xác thực, sẵn sàng và làm quen với ứng dụng, hướng dẫn và mô hình vận hành, các tiêu chí, danh mục kiểm tra và các biểu mẫu hoạt động để trở thành Tổ chức sử dung dịch vụ định danh điện tử (ISCA) hoặc Tổ chức cung cấp dịch vụ định danh điện tử (ISPA), và tạo nguồn thông tin định danh điện tử (eID) để nhúng các Mã số chứng minh nhận dạng quốc gia (NIN).

5. **Các thiết bị đầu cuối.** Các thiết bị đầu cuối có thể do các Tổ chức sử dung dịch vụ định danh điện tử (ISCA) (thuộc khu vực công và tư nhân) sử dụng để cung cấp dịch vụ cho công dân. Ví dụ bao gồm các thiết bị rút tiền vi tiểu (micro ATM), các thiết bị và thiết bị đầu cuối máy thanh toán tiền bằng thẻ (Máy PoS), các máy rút tiền tự động (ATM), các thiết bị đảm bảo an ninh truy cập. Các thiết bị này được cài ứng dụng của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) để hỗ trợ cơ chế thu thập số liệu sinh trắc của công dân cho các mục đích xác thực định danh điện tử (eID). Các tính năng bổ sung của các thiết bị đầu cuối đó phụ thuộc vào nhu cầu dịch vụ cụ thể do các Tổ chức sử dung dịch vụ định danh điện tử (ISCA) cung cấp. Các thiết bị đó cần tuân thủ các yêu cầu kỹ thuật do chính phủ ban hành để bảo vệ các thông tin sinh trắc học và nhân chủng học do công dân cung cấp.

6. **Quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC).** Quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC) nhằm xác nhận nhận dạng của khách hàng. Các nhà cung cấp dịch vụ cần thực hiện quy trình này qua phương tiện điện tử với sự đồng ý rõ ràng từ phía khách hàng. Quy trình này cho phép cung cấp dịch vụ tức thời không cần giấy tờ cho công dân. Chính phủ có thể triển khai quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC) bằng cách sử dụng cùng một cơ sở hạ tầng và mô hình hoạt động được thiết lập cho việc xác thực nhận dạng điện tử.
    a. Trong quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC), công dân cần cho phép chính phủ xác thực định danh điện tử (eID) bằng cách sử dụng dữ liệu sinh trắc hoặc mật khẩu dùng một lần (OTP) để cung cấp dữ liệu nhân chủng học cùng với hình ảnh được ký chữ ký số và được mã hoá của họ cho các nhà cung cấp dịch vụ. Qua đó các nhà cung cấp dịch vụ có thể thực hiện quy trình nhận dạng và xác nhận khách hàng (KYC) theo thời gian thực và không cần giấy tờ.
    b. Quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC) cho phép các nhà cung cấp dịch vụ có thể cung cấp dịch vụ tức thời cho công dân, bằng không sẽ phải mất vài ngày để thẩm định các hồ sơ giấy tờ liên quan để kích hoạt dịch vụ.
    c. Việc sử dụng quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC) giúp tránh được chi phí xử lý lặp đi lặp lại quy trình nhận dạng và xác nhận khách hàng (KYC), chi phí lưu trữ và xử lý trên giấy, rủi ro giả mạo trong các giấy tờ chứng minh nhận dạng và chứng minh địa chỉ.

7. **Dịch vụ thanh toán điện tử.** Chính phủ có thể triển khai cơ chế thanh toán điện tử (ePayment) trên cơ sở định danh điện tử (eID), để tăng cường minh bạch, trách nhiệm giải trình, hiệu suất và đảm bảo thanh toán đúng đối tượng trong các chương trình phúc

lợi của chính phủ như chương trình hưu trí qua bảo hiểm xã hội, phúc lợi y tế, v.v. đối với các đối tượng hưởng lợi dự kiến.

a. Thanh toán điện tử (ePayment) cũng có thể hỗ trợ chuyển khoản liền mạch toàn bộ các khoản thanh toán chi trả trong chương trình phúc lợi vào Tài khoản ngân hàng mở theo định danh điện tử (eBA) của đối tượng thụ hưởng. Tài khoản ngân hàng mở theo định danh điện tử (eBA) có thể được coi là tài khoản ngân hàng thông thường được định danh qua nhận dạng điện tử của đối tượng thụ hưởng.
b. Trong thời gian đăng ký nhận dạng điện tử, công dân cần cung cấp chi tiết về tài khoản ngân hàng hiện có của họ hoặc yêu cầu mở tài khoản ngân hàng mới gắn với Mã số định danh công dân (NIN) của mình để nhận các khoản thanh toán theo các chương trình phúc lợi.
c. Cầu thanh toán điện tử (ePB) gồm một cơ sở dữ liệu nhằm lưu trữ thông tin Mã số định danh công dân (NIN) và Tài khoản ngân hàng mở theo định danh điện tử (eBA) tương ứng của họ để tiếp nhận các khoản phúc lợi và an sinh xã hội từ các cơ quan khác nhau của chính phủ.
d. Giải pháp đảm bảo công bằng tiếp cận tài chính bao gồm kết hợp sử dụng Mã số định danh công dân (NIN) như một địa chỉ thanh toán cùng với chức năng nhận dạng và xác nhận khách hàng điện tử (eKYC) để tạo lập tài khoản tức thời trên cơ sở hạ tầng thanh toán dựa trên định danh điện tử (eID). Giai đoạn thí điểm cần giải quyết các vấn đề chính liên quan đến quy trình và thủ tục mở tài khoản, và \đánh giá về tác động của việc sử dụng Mã số định danh công dân (NIN) để định danh tàikhoarn trong hệ thống thanh toán của quốc gia.
e. Khi sử dụng Mã số định danh công dân (NIN) như một địa chỉ thanh toán, tiền được chuyển cho bất kỳ công dân nào cho dù người đó có tài khoản ngân hàng hay không. Nếu người nhận tiền có Tài khoản ngân hàng mở theo định danh điện tử (eBA), tiền sẽ được chuyển thẳng vào đó, nếu người nhận chưa có Tài khoản ngân hàng mở theo định danh điện tử (eBA), một tài khoản tức thời sẽ được tạo lập trên cơ sở Mã số định danh công dân (NIN), với bên ghi có được đóng băng. Tiền chuyển về sẽ được ghi nợ vào tài khoản tức thời đó. Tài khoản tức thời đó sẽ được kích hoạt trong lần rút tiền đầu tiên trên cơ sở chức năng nhận dạng và xác nhận khách hàng điện tử (eKYC).

8. **Địa chỉ thư điện tử chính thức của công dân.** Chính phủ có thể cung cấp một địa chỉ thư điện tử (email) chính thức cho mỗi công dân. Địa chỉ thư điện tử (email) này được sử dụng để giao tiếp chính thức với chính phủ, nhưng cũng có thể sử dụng cho cả các giao tiếp với khu vực tư nhân. Địa chỉ thư điện tử (email) do chính phủ cung cấp đóng vai trò

là tiếp nhận, và công dân có thể xác định chi tiết tài khoản thư điện tử vào thời điểm đăng ký để tiếp nhận các thông điệp điện tử. Toàn bộ các địa chỉ thư điện tử (email) có thể được liệt kê công khai trong danh mục đăng ký quốc gia của các nhà cung cấp dịch vụ chứng nhận của chính phủ.

9. **Dịch vụ tài liệu điện tử bảo mật**. Chính phủ có thể cung cấp dịch vụ tài liệu điện tử (eDocument) bảo mật để tạo điều kiện chuyển tải an toàn các tệp điện tử trong một môi trường không an toàn, như internet. Dịch vụ này có thể cung cấp các tính năng mã hoá và giải mã tài liệu điện tử (eDocument) bằng sinh trắc hoặc chứng nhận số gắn với hồ sơ định danh điện tử của cá nhân. Để có thêm chi tiết, đề nghị tham khảo kinh nghiệm của Ét-xtô-nia tại Phụ lục 5.

10. **Các dịch vụ nhận dạng di động.** Chính phủ có thể cung cấp dịch vụ nhận dạng di động cho những người có định danh điện tử có đăng ký để sử dụng nhằm xác thực điện tử và ký điện tử bằng điện thoại di động. Trong kịch bản này, điện thoại di động có các chức năng SIM (nghĩa là thẻ vật lý, phần mềm hoặc các cơ chế định danh người thuê bao khác) tương đương với thẻ chứng minh thư và máy đọc thẻ.
    a. Khi muốn sử dụng dịch vụ nhận dạng di động, công dân cần phải có một SIM chuyên dụng để có thể sử dụng dịch vụ. Thẻ này có thể có bằng cách ký hợp đồng dịch vụ với một nhà điều hành di động quốc gia được giao chức năng này.
    b. Nhận dạng di động có thể được sử dụng ở bất kỳ đâu trên thế giới nếu được phủ sóng di động. Không cần phải cài đặt phần mềm máy tính để chức này này có thể hoạt động. Phần mềm này được cài trên SIM của điện thoại di động. Nó có thể được sử dụng trên các thiết bị điện thoại đời mới. Khi công nghệ điện thoại thông minh trở nên phổ biến hơn, việc sử dụng phương án nhận dạng di động càng trở nên thuận tiện, cho phép người sử dụng thậm chí có thể bỏ phiếu qua internet từ điện thoại di động chẳng hạn.

Khía cạnh kỹ thuật. Một số bài học rút ra qua nghiên cứu kinh nghiệm quốc tế trên khía cạnh kỹ thuật về triển khai cung cấp dịch vụ trên cơ sở định danh điện tử (eID) được mô tả chi tiết tại Phụ lục 5 và được liệt kê dưới đây.

1. **Xác định định danh điện tử quốc gia duy nhất và bảo mật.**
    a. **Tính duy nhất là thuộc tính thiết yếu.** Hồ sơ định danh điện tử quốc gia của công dân bao gồm Mã số định danh công dân (NIN) duy nhất gắn với các dữ liệu sinh trắc và nhân chủng học được lưu trữ tại Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS).

b. **Sử dụng tính năng truy vấn và khai thác báo cáo (intelligence) là không khôn ngoan.** Tải nhập tính năng khai thác tình báo vào các mã số nhận dạng khiến cho các mã số đó dễ bị gian lận và mất trộm. Chính vì thế, Mã số định danh công dân (NIN) phải là mã số ngẫu nhiên và duy nhất gán cho công dân, không gắn với bất kỳ tính năng khai thác tình báo nào.

c. **Thu thập dữ liệu qua đăng ký trên toàn quốc**. Bước đầu tiên để ban hành định danh điện tử (eID) quốc gia là phải thực hiện một quy trình đăng ký để thu thập thông tin sinh trắc và nhân chủng học của công dân. Tính duy nhất của dữ liệu cung cấp được xác lập qua một quy trình loại bỏ trùng lặp. Sau quy trình loại bỏ trùng lặp, Mã số định danh công dân (NIN) sẽ được cấp phát và thông tin chi tiết sẽ được gửi cho công dân theo đường thư tín.

d. **Loại bỏ trùng lặp thông tin sinh trắc để đảm bảo tính duy nhất.** Đảm bảo tính duy nhất có nghĩa là chỉ gán một Mã số định danh công dân (NIN) duy nhất cho một người, và một người chỉ có một mã số nhận dạng duy nhất. Hồ sơ công dân cần được qua một quy trình chặt chẽ nhằm loại bỏ trùng lặp về thông tin sinh trắc và nhân chủng học với độ chính xác lên đến 99,00% trước khi được giao mã số nhận dạng duy nhất. Chỉ riêng dữ liệu nhân chủng học cũng chưa đủ để đảm bảo tính duy nhất. Tuy nhiên, nhận dạng duy nhất có thể được đảm bảo bằng cách gắn các thuộc tính nhân chủng học với các thuộc tính sinh trắc học như dấu vân tay và hình ảnh võng mạc của cá nhân đó.

2. **Tận dụng Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) để xác thực nhận dạng điện tử.**

a. Quy trình xác thực định danh điện tử có thể coi là một dịch vụ mạng không lưu lại trạng thái qua giao thức truyền siêu văn bản an toàn (HTTPS). Việc sử dụng định dạng dữ liệu mở với ngôn ngữ đánh dấu mở (XML) và giao thức được sử dụng phổ biến như giao thức truyền siêu văn bản (HTTP) cho phép dễ dàng áp dụng và triển khai các dịch vụ định danh điện tử (eID).

b. Quy trình xác thực định danh điện tử (eID) hoạt động bằng cách sử dụng Mã số định danh công dân (NIN) cùng với dữ liệu nhận dạng cá nhân của người có định danh điện tử (eID) làm đầu vào, và sau đó chuyển các đầu vào đó sang Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) để đối chiếu. Tiếp theo Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) sẽ thẩm định độ chính xác trên cơ sở khớp nối 1: 1 với thông tin nhận dạng của người có định danh điện tử (eID). Dịch vụ này hoặc khẳng định thông tin chứng minh nhận dạng hoặc thẩm định thông tin do công dân cung cấp. Để bảo vệ sự

riêng tư của công dân, dịch vụ chỉ cung cấp câu trả lời dưới dạng "có/không", và không đưa ra thông tin về nhận dạng cá nhân trong câu trả lời.

c. Quy trình xác thực định danh điện tử (eID) có thể được cung cấp cho công dân để chứng minh nhận dạng trực tuyến tại bất kỳ nơi đâu, vào bất kỳ lúc nào, bằng nhiều phương thức khác nhau. Nó có thể hỗ trợ xác thực đơn yếu tố và đa yếu tố. Mã số định danh công dân (NIN) – bên cạnh các thuộc tính như nhân chủng học, mật khẩu sử dụng một lần (OTP), chứng nhận số, hoặc thông tin sinh trắc đơn/đa chiều (vân tay và/hoặc hình ảnh võng mạc) – có thể được sử dụng để xác thực đơn yếu tố. Ngược lại, những thuộc tính này có thể được sử dụng kết hợp (đa yếu tố) để đảm bảo nhu cầu xác thực theo yêu cầu. Mã số chứng minh nhận dạng quốc gia (NIN), bản thân nó, không thể được coi là một yếu tố để xác thực.
d. Quy trình xác thực định danh điện tử (eID) có thể hỗ trợ nhiều loại hình xác thực tuỳ theo loại đầu vào (thông tin nhân chủng học, mật khẩu dùng một lần (OTP), chứng nhận số, thông tin sinh trắc học, hoặc đa yếu tố). Toàn bộ các loại yêu cầu xác thực định danh điện tử (eID) cần sử dụng Mã số định danh công dân (NIN) làm một trong các đầu vào để xác thực khớp nối 1:1 trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS).
e. Quy trình xác thực định danh điện tử (eID) có thể hỗ trợ mô hình xác thực mở rộng và có thể được thiết kế trên quan điểm tăng cường các hệ thống xác thực hiện hành của các nhà cung cấp dịch vụ, chứ không phải chỉ thay thế hệ thống hiện hành. Mặc dù mô hình mở rộng không yêu cầu phải có sự tồn tại – hoặc sử dụng – xác thực riêng của nhà ucng cấp dịch vụ (nếu nhà cung cấp dịch vụ mong muốn, họ có thể sử dụng dịch vụ xác thực định danh điện tử (eID) riêng đó), nhưng họ được khuyến khích sử dụng dịch vụ xác thực định danh điện tử (eID) phối hợp với dịch vụ xác thực cục bộ của riêng họ để hệ thống tổng thể trở nên mạnh hơn và đáng tin cậy hơn. Cách này có thể được gọi là mô hình mở rộng về xác thực định danh điện tử (eID).
f. Quy trình xác thực định danh điện tử (eID) bao gồm các tính năng bảo mật và riêng tư như trả lời bằng "có/không", yêu cầu/trả lời được ký chữ ký số, mã số trả lời, dấu thời gian trả lời, và khả năng tự thẩm định câu trả lời, mã hoá và chống mất trộm. Để tìm hiểu thêm chi tiết về các tính năng bảo mật và riêng tư trong quy trình xác thực định danh điện tử (eID), đề nghị tham khảo kinh nghiệm của Ấn Độ tại Phụ lục 5.
g. Quy trình xác thực định danh điện tử (eID) cũng hỗ trợ tạo dữ liệu nhớ đệm tại nhiều điểm cuối để cho phép cung cấp dịch vụ trong trường hợp kết nối mạng chập chờn.

3. **Các thiết bị và chuẩn mực về dữ liệu sinh trắc**

   a. **Yêu cầu kỹ thuật đối với thiết bị sinh trắc.** Thiết bị đầu cuối sử dụng trong quy trình xác thực sinh trắc học phải quét/đọc được dấu vân tay và võng mạc của công dân. Chính phủ có thể xác định các yêu cầu kỹ thuật về thiết bị sinh trắc[1] trên cơ sở các chuẩn mực mở để thông tin liên quan được quét/đọc qua thiết bị đảm bảo về chất lượng dữ liệu và độ chính xác ở mức cao.

   b. **Tiêu chuẩn dữ liệu sinh trắc.** Để đáp ứng nhu cầu to lớn về các thiết bị quét/đọc thông tin sinh trắc cần thiết trong xác thực định danh điện tử (eID), điều cần thiết là phải mua thiết bị từ các nhà cung cấp chuyên về xác thực sinh trắc học. Tuy nhiên, điều đó chỉ có thể thực hiện nếu có sự tương tác liên thông giữa các thiết bị được sản xuất và bán bởi các nhà cung cấp khác nhau để thu thập và đối chiếu dữ liệu. Một cơ quan chuyên trách của chính phủ có thể đứng ra xác định các chuẩn mực về dữ liệu sinh trắc trên cơ sở các chuẩn mực mở về hình ảnh vân tay, chi tiết dấu vân tay, hình ảnh võng mạc và ảnh khuôn mặt để đảm bảo có sự tương tác liên thông. Bộ tiêu chuẩn ISO 19794 về các chuẩn mực sinh trắc học để công nhận vân tay, khuôn mặt và võng mạc do Tổ chức Tiêu chuẩn Quốc tế (ISO) xây dựng là một tiêu chuẩn được chấp nhận chung và phản ánh tốt nhất các kinh nghiệm trước đó của Mỹ và châu Âu về sinh trắc học.

   c. **Yêu cầu kỹ thuật về thông tin sinh trắc.** Yêu cầu kỹ thuật về Giao diện lập trình ứng dụng (hàm API) cho Bộ công cụ phát triển phần mềm sinh trắc (SDK) là một giao diện thống nhất duy nhất cho các phương thức khác nhau (khuôn mặt, vân tay, võng mạc) được sử dụng cho các nhà lập trình Bộ công cụ phát triển phần mềm sinh trắc (SDK) của các nhà cung cấp thiết bị sinh trắc nhằm cung cấp tính năng cho các mô-đun khác nhau cho Hệ thống cung cấp dịch vụ định danh điện tử (EISDP). Qua đó các nhà cung cấp có được sự trung lập vì việc sử dụng chuẩn Giao diện lập trình ứng dụng (hàm API) và các tiêu chuẩn mở sẽ giúp loại bỏ các tính năng riêng và đặc thù theo nhà cung cấp. Điều đó cũng khuyến khích tạo khả năng tương tác liên thông bằng cách sử dụng các giao diện chuẩn, các giao thức và định nghĩa định dạng dữ liệu chung trong tất cả các hợp phần có cùng tính năng như nhau. Giao diện lập trình ứng dụng (hàm API) mở cũng cho phép sử dụng các thuật toán tốt nhất cho các mục đích đặc biệt. Giao diện lập trình ứng dụng (hàm API) cho phép kiểm tra chất lượng, phân đoạn, phân chia thời

[1] Yêu cầu kỹ thuật về thiết bị sinh trắc để xác thực nhận dạng tại Ấn độ – http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Authentication_.pdf

gian, trích xuất và khớp nối các tính năng với nhau. Các yêu cầu kỹ thuật này cần được công bố trên cổng thông tin công cộng của chính phủ.

d. **Công nghệ "phát hiện ngón tay tốt nhất".** Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) coi "phát hiện ngón tay tốt nhất" là một dịch vụ mạng không lưu lại trạng thái. Dịch vụ này có thể yêu cầu bằng ứng dụng của các nhà cung cấp dịch vụ để phát hiện ngón tay của công dân đem lại kết quả tốt nhất trong số các kết quả đối chiếu thành công. Sau đó công dân này sẽ sử dụng ngón tay tốt nhất đó để đảm bảo tỷ lệ thành công cao hơn trong những lần xác thực định danh điện tử (eID) sinh trắc học. Cơ hội đối chiếu khớp có thể khác nhau do có sự khác biệt về chất lượng của các ngón tay. Sự khác biệt này cũng có thể tồn tại do cách thức công dân tương tác bình thường với máy quét vân tay tiêu biểu, và các ngón tay khác nhau hiển nhiên có số lượng thông tin nhận dạng khác nhau tuỳ thuộc vào kích cỡ ngón tay và mức độ phổ biến của vân tay. Do đó, phát hiện được ngón tay tốt nhất để xác thực định danh điện tử (eID) sinh trắc học có thể cải thiện độ chính xác của kết quả.

4. **Cơ sở hạ tầng CNTT định danh điện tử tin cậy và khả tín với công nghệ đảm bảo và được hỗ trợ kỹ thuật trong nước**. Chính phủ có thể xây dựng một cơ sở hạ tầng định danh điện tử (eID) đáng tin cậy và khả tín với đội ngũ hỗ trợ kỹ thuật toàn thời gian. Giải pháp kỹ thuật này dựa trên công nghệ đã được minh chứng do các nhà cung cấp công nghệ hoặc phần mềm trong nước cung cấp. Giải pháp này có thể mở rộng, linh hoạt, dựa trên chuẩn mực để có thể mở rộng ra các dịch vụ khác, và trong tương lai có thể sử dụng ngoài biên giới.

5. **Năng lực kỹ thuật nội bộ trong nước về dịch vụ và cơ sở hạ tầng CNTT về định danh điện tử (eID).** Chính phủ có thể xây dựng năng lực kỹ thuật trong nước mang tính tự đảm bảo để thiết kế và triển khai cơ sở hạ tầng và các dịch vụ CNTT về định danh điện tử (eID). Đây là phương án nên thực hiện hơn là dựa vào nhà cung cấp công nghệ hoặc phần mềm nước ngoài để cung cấp và hỗ trợ bảo hành cho một cơ sở hạ tầng vô cùng quan trọng của quốc gia. Sự phụ thuộc vào nhà thầu nước ngoài sẽ dẫn đến những tác động nguy hại về khả năng vận hành hàng ngày của quốc gia trong tương lai. Chính vì những cân nhắc đó, khuyến nghị đưa ra là cần phát triển theo mô hình phần mềm may đo. Trong trường hợp chính phủ quyết định sử dụng giải pháp đã được đóng gói gọn gàng của các nhà thầu nước ngoài, chính phủ có thể xây dựng năng lực nội bộ để triển khai và quản lý giải pháp đó.

6. **Thiết kế định danh điện tử để tích hợp dễ dàng với dịch vụ của các nhà cung cấp.** Chính phủ có thể thiết kế hoạt động triển khai các dịch vụ định danh điện tử (eID) để tạo điều kiện cho việc tích hợp với các hệ thống cung cấp dịch vụ chính hiện nay và trong tương lai của các nhà cung cấp. Điều này cho phép bổ sung các tính năng như chữ ký số, xác thực điện tử và mã hoá tài liệu. Chính phủ có thể triển khai các biện pháp sau để đáp ứng các yêu cầu về tích hợp.
    a. **Áp dụng các luồng công việc chuẩn trong quy trình cung cấp dịch vụ**. Chẳng hạn, luồng công việc chuẩn về chữ ký số sử dụng định dạng tài liệu phổ biến cần được áp dụng. Để có thêm chi tiết, đề nghị tham khảo về triển khai chữ ký số tại Ét-xtô-nia qua mô tả tại Phụ lục 5.
    b. **Mã số định danh công dân duy nhất được cấp tập trung**. Nên triển khai một cơ sở dữ liệu tập trung về Mã số định danh công dân (NIN) đã cấp cho công dân. Cần phải có một cơ sở hạ tầng về định danh điện tử (eID) đáng tin cậy và khả tín để tạo điều kiện cung cấp dịch vụ nhận dạng. Để có thêm chi tiết về cơ sở hạ tầng CNTT và cơ sở dữ liệu về định danh điện tử (eID) tập trung, đề nghị tham khảo kinh nghiệm của Ấn Độ được mô tả tại Phụ lục 5.
    c. **Điểm truy cập tập trung duy nhất đối với các các dịch vụ công**. Xác thực điện tử nên được sử dụng dưới dạng một mã thông báo bảo mật (token) cho các dịch vụ khác nhau mà chỉ cần truy cập qua một điểm tập trung duy nhất: cổng thông tin công dân điện tử.

7. **Thiết kế các dịch vụ nhận dạng di động để tăng cường áp dụng các dịch vụ định danh điện tử (eID)**. Tại Ét-xtô-nia, quá trình triển khai định danh điện tử (eID) được cải thiện qua triển khai các dịch vụ nhận dạng di động (mobile ID) vì sự gia nhập của thị trường điện thoại di động tại quốc gia đó đã lên đến trên 100%. Sự cải thiện được đem lại qua khả năng dễ dàng sử dụng điện thoại di động làm thiết bị xác thực, so với việc dùng một thẻ đọc thông minh gắn với máy tính cá nhân. Để có thêm chi tiết về kinh nghiệm triển khai nhận dạng di động tại Ét-xtô-nia, đề nghị tham khảo Phụ lục 5. Một số bài học về thiết kế kỹ thuật thu được qua kinh ghiệm triển khai các dịch vụ nhận dạng di động của Ét-xtô-nia được trình bày dưới đây.
    a. Các phương pháp chữ ký di động và xác thực qua di động chấp nhận sử dụng Mã số định danh công dân (NIN) và mã số nhận dạng cá nhân (PIN) và số điện thoại là các tham số đầu vào. Việc sử dụng số điện thoại làm tham số đầu vào duy nhất có thể dẫn đến các vấn đề về bảo mật vì đây là thông tin công khai. Do đó, bổ sung thêm mã số nhận dạng cá nhân (PIN) và Mã số định danh công dân (NIN) đem lại những cải thiện về bảo mật.

b. Thiết kế kỹ thuật về nhận dạng di động cần dựa trên cơ sở hạ tầng mã khoá công cộng không dây (wPKI), ví dụ yêu cầu kỹ thuật về wPKI[2] trong đó, điện thoại di động đóng vai trò là máy đọc thẻ thông minh có màn hình hiển thị. Giao tiếp giữa máy tính cá nhân (PC) và điện thoại di động được thực hiện qua chức năng xác thực/ ký chữ ký bằng thiết bị di động và cổng thông tin của nhà điều hành Hệ thống thông tin di động toàn cầu (GSM).

c. Cổng thông tin di động sử dụng một công nghệ chuẩn gọi là cập nhật phần mềm/dữ liệu từ xa (Over-The-Air[3] (OTA)) để trao đổi và chạy ứng dụng trên SIM của điện thoại di động mà không cần kết nối vật lý với thẻ.

d. Chức năng xác thực/chữ ký sẽ gửi yêu cầu xác thực/chữ ký (yêu cầu wPKI[4]) cho một hệ thống xử lý hậu trường của Nhà điều hành mạng di động (MNO) bằng mạng giao thức internet (IP) và qua đó gửi yêu cầu vào cổng thông tin di động. Cổng này sẽ chuyển tiếp yêu cầu vào điện thoại di động của công dân bằng dịch vụ tin nhắn ngắn (SMS).

e. Điện thoại di động sẽ hỗ trợ các tính năng kỹ thuật cần thiết để sử dụng cho các chức năng nhận dạng di động. Chẳng hạn Ét-xtô-nia đã công bố các đặc tả kỹ thuật về điện thoại di động để có thể sử dụng các dịch vụ nhận dạng di động. Các đặc tả kỹ thuật này bao gồm hỗ trợ cho các tiêu chuẩn GSM Giai đoạn 2+[5], bộ công cụ ứng dụng SIM[6] cho phép cập nhật từ xa (OTA), và tuân thủ các chuẩn GSM[7].

8. **Chữ ký số và xác thực chứng nhận số.**

a. Kiến trúc chữ ký số dựa trên các chuẩn mở phổ biến về cấp, xử lý và xác nhận chữ ký số. Nó có thể kết nối với bất kỳ phần mềm mới hoặc hiện hành nào. Các hợp phần của hệ thống này bao gồm một chương trình máy trạm riêng rẽ, một cổng mạng và một dich vụ mạng dựa trên Giao thực truy suất đối tượng đơn giản (SOAP) cho phép tích hợp dễ dàng với tính năng chữ ký số, xác thực và nhận chữ ký với các hệ thống thông tin khác.

---

[2] Yêu cầu kỹ thuật về wPKI - http://www.signature.lt/KK/wPKI-specification.pdf

[3] Công nghệ Over-The-Air - http://www.gemalto.com/techno/ota/

[4] các giao dịch di động wPKI - http://wpki.eu/doku/lib/exe/fetch.php/wiki:baltic_wpki_standard_draft-0.3.pdf

[5] GSM 11.11 Hệ thống viễn thông di động số (Giai đoạn 2+); Đặc tả kỹ thuật về giao diện thiết bị di động - thẻ SIM (mô-đun nhận dạng người đăng ký thuê bao) (SIM-ME) - http://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf

[6] Bộ công cụ ứng dụng SIM - http://www.gemalto.com/techno/stk/

[7] GSM 11.14 Hệ thống viễn thông di động số (Giai đoạn 2+); Đặc tả kỹ thuật về bộ công cụ ứng dụng SIM cho giao diện giao diện thiết bị di động - thẻ SIM (mô-đun nhận dạng người đăng ký thuê bao) (SIM-ME) - http://www.etsi.org/deliver/etsi_g3ts/11/1114/05.04.00_60/gsmts_1114v050400p.pdf

b. Tương tự như Ét-xtô-nia, chính phủ có thể chọn mô hình giao tiếp sử dụng các luồng công việc chuẩn và định dạng tài liệu phổ biến như Chuẩn chữ ký điện tử tiên tiến theo ngôn ngữ đánh dấu mở XML (XadES) tạo ra một định dạng mà cấu trúc của nó cho phép lưu trữ dữ liệu chữ ký, các thuộc tính của chữ ký và các thuộc tính bảo mật liên quan đến chữ ký số; do đó nó sẽ hỗ trợ để các hệ thống để hiểu theo cùng một cách.
c. Chính phủ Việt Nam có thể xác định ra các chuẩn mực về thẻ thông minh và xác thực số trên cơ sở các chuẩn mở nhằm tăng cường khả năng tác nghiệp liên thông. Để tìm hiểu thêm chi tiết về kinh nghiệm quốc tế nhằm tận dụng các chuẩn mở và được sử dụng phổ biến về thẻ thông minh và chứng nhận số, đề nghị tham khảo Phụ lục 5.
d. Chính phủ có thể cung cấp phần mềm để cài đặt trên thiết bị kết nối internet của công dân (máy tính xách tay, máy tính để bàn, v.v.) để tạo điều kiện cho họ sử dụng thẻ nhận dạng cá nhân điện tử nhằm truy cập vào các dịch vụ điện tử của khu vực công và khu vực tư nhân, ký chữ ký số trên tài liệu, và mã hoá tài liệu để truyền an toàn. Phần mềm này có thể được gọi chung là phần mềm nhận dạng. Chính phủ có thể hướng dẫn cho công dân vào trang web công cộng của chính phủ để cài đặt phần mềm nhận dạng trên các thiết bị của họ. Để tìm hiểu thêm chi tiết về phần mềm nhận dạng, đề nghị tham khảo kinh nghiệm của Ét-xtô-nia tại Phụ lục 5.
e. Một số phần mềm thường được cung cấp trong khuôn khổ này bao gồm:
    i. Thư viện phần mềm cho các chuyên gia phát triển quan tâm đến tích hợp các năng lực về chữ ký và xác thực chứng nhận số trong phần mềm của họ.
    ii. Dịch vụ như máy chủ giao thức kiểm tra chứng thực trực tuyến (OCSP) để kiểm tra tính hợp lệ của các chứng nhận theo thời gian thực và lâu dài. Để có thêm chi tiết, đề nghị tham khảo kinh nghiệm của Ét-xtô-nia tại Phụ lục 5.

9. **Cổng thông tin dịch vụ chính phủ điện tử chung theo cơ chế một cửa.** Chính phủ có thể thiết kế một cổng thông tin dịch vụ chính phủ điện tử chung để cung cấp toàn bộ các dịch vụ điện tử của các bộ ngành khác nhau với năng lực đăng nhập một lần (SSO) bằng xác thực định danh điện tử (eID).

<u>Khía cạnh thể chế.</u> Một số bài học về mặt thể chế, bao gồm cả cơ cấu tổ chức và mô hình vận hành rút ra qua nghiên cứu kinh nhiệm quốc tế được mô tả chi tiết tại Phụ lục 5 và được liệt kê dưới đây.

Cơ cấu tổ chức

1. **Tách bạch về mặt tổ chức trong chính phủ cơ quan quản lý nhà nước và cơ quan điều hành tổng thể các dịch vụ định danh điện tử (eID).** Bất kỳ đơn vị cung cấp dịch vụ nào cũng cần xác định nhận dạng và quyền hưởng dịch vụ của đối tượng thụ hưởng. Mặc dù nhận dạng cá nhân là duy nhất và độc lập với loại hình dịch vụ mong muốn, quyền hưởng lại có tính đặc thù đối với dịch vụ được cung cấp và nó phải được xác lập riêng bởi từng đơn vị cung cấp dịch vụ. Do đó, tại ba quốc gia nghiên cứu (Ấn Độ, Ét-xtô-nia và Bỉ), thay vì giao vai trò và trách nhiệm về các dịch vụ định danh điện tử (eID) cho một bộ hiện có, họ có thể thành lập ra một cơ quan chính phủ mới để làm nhiệm vụ quản lý nhà nước và cơ quan điều hành tổng thể các dịch vụ định danh điện tử (eID). Để có thêm chi tiết, đề nghị tham khảo Phụ lục 5.

2. **Thành lập một uỷ ban liên bộ có thẩm quyền quyết định về các dịch vụ định danh điện tử (eID) và các vấn đề liên quan**. Uỷ ban ở cấp cao nhất trong chính phủ có thể được thành lập, do tổng thống hoặc thủ tướng đứng đầu. Các thành viên có thể là bộ trưởng các bộ liên quan như tài chính, tư pháp, thông tin và truyền thông, lao động, v.v. là các đơn vị có chức năng quản lý toàn bộ các vấn đề liên quan đến hệ thống định danh điện tử (eID), bao gồm tổ chức, kế hoạch, chính sách, chương trình, vốn, phương pháp luận cần áp dụng để hoàn thành mục tiêu. Ủy ban cấp cao đó cũng nên có sự tham gia của các nhóm người sử dụng phát triển phần mềm, các tổ chức phát triển quốc tế để đảm bảo chuẩn mực mở, đồng thời áp dụng được các thông lệ tốt nhất về bảo mật và bảo vệ dữ liệu của công dân.

3. **Cơ cấu tổ chức theo hình thức quan hệ hợp tác công – tư (PPP) có thể mở rộng để cung cấp các dịch vụ định danh điện tử (eID) với chất lượng và độ bảo mật cao.** Nhu cầu về các yêu cầu về khả năng mở rộng để đáp ứng tốc độ tăng trưởng theo cấp số nhân về nhu cầu các dịch vụ định danh điện tử (eID) có thể được đáp ứng qua việc thiết kế một cơ cấu tổ chức có thể mở rộng theo mô hình quan hệ hợp tác công – tư (PPP). Theo mô hình đó, chính phủ có thể xác định các vai trò trong hệ môi trường có thể thuê ngoài khu vực tư nhân thực hiện. Đơn vị cung cấp dịch vụ ban đầu có thể nhỏ, nhưng có thể mở rộng quy mô nếu nhu cầu dịch vụ tăng lên.
    a. Nhu cầu bảo mật cao trong quản lý Dữ liệu nhận dạng cá nhân (PID) trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) có thể được đảm bảo bằng cách hạn chế chỉ cho phép một số tổ chức có thẩm quyền được truy cập với vai trò là Tổ chức cung cấp dịch vụ nhận dạng trực tuyến (ISPA).

b. Chức năng nhận dạng di động có thể được triển khai theo hình thức quan hệ hợp tác công – tư (PPP) giữa cơ quan chính phủ chịu trách nhiệm về định danh điện tử (eID) và các Nhà điều hành mạng di động (MNO). Cơ quan chính phủ đó có thể phân cấp trách nhiệm về cung cấp SIM có tính năng nhận dạng di động cho Nhà điều hành mạng di động (MNO). Việc đăng ký sử dụng và kích hoạt chức năng nhận dạng di động có thể được thực hiện bởi Tổ chức quản lý đăng ký (RA) là nơi nhận yêu cầu đăng ký sử dụng và kích hoạt dịch vụ từ phía công dân. Vai trò của Tổ chức quản lý đăng ký (RA) được thực hiện bởi các Nhà điều hành mạng di động (MNO) hoạt động bên cạnh cơ quan phụ trách an ninh công cộng của chính phủ. Yêu cầu tạo chứng nhận mới được phân quyền cho Cơ quan có thẩm quyền chứng nhận (CA) của Nhà cung cấp dịch vụ chứng nhận (CSP).
c. Các dịch vụ định danh điện tử (eID) trên cơ sở sinh trắc hoặc chứng nhận số như xác thực định danh điện tử (eID) có thể áp dụng cơ cấu tổ chức theo hình thức quan hệ hợp tác công – tư (PPP) nhằm đảm bảo dịch vụ có khả năng mở rộng và đáp ứng các thoả thuận về mức độ dịch vụ (SLA) do chính phủ xác định. Chính phủ có thể phân cấp vai trò của trung tâm chứng nhận cho một cơ quan chính phủ được xác định tại Luật chữ ký số (DSA), để thuê các nhà cung cấp dịch vụ thuộc khu vực tư nhân thay mặt cho mình triển khai và cung cấp dịch vụ đó. Trung tâm chứng nhận đó chịu trách nhiệm quản lý việc điều hành dịch vụ như quản lý các quy trình giao thức truy cập nhanh các dịch vụ thư mục (LDAP), giao thức kiểm tra chứng thực trực tuyến (OCSP), và các quy trình liên quan đến chứng nhận khác, kênh phân phối cho người sử dụng cuối cùng qua các điểm bán lẻ tập trung của họ, phát triển và bảo trì phần mềm nhận dạng và các gói cài đặt, sổ tay hướng dẫn và hướng dẫn bằng hình ảnh công bố trên cổng thông tin công cộng của chính phủ và các trung tâm quản lý cuộc gọi.
d. Để cung cấp các dịch vụ định danh điện tử (eID) trên cơ sở thẻ thông minh chứng thực số/sinh trắc, chính phủ cần thuê ngoài các nhà cung cấp thuộc khu vực tư nhân được huy động và chứng nhận để cung cấp tính năng cá nhân hoá thẻ. Nhà cung cấp đó phải chịu trách nhiệm cá nhân hoá thẻ cả về phương diện vật lý và điện tử. Nhà cungc ấp sẽ nhận được ứng dụng thẻ từ cơ quan chính phủ để sản xuất, in ấn và khắc dữ liệu cá nhân trên thẻ, tạo ra mã khoá trên vi mạch và nhúng thông tin chứng nhận trên thẻ.
e. Luật chữ ký số (DSA) xác định vai trò và trách nhiệm của các bên liên quan đến xử lý chữ ký số. Một số vai trò có thể được giao cho các Nhà cung cấp dịch vụ chứng nhận (CSP) để chứng nhận rằng công dân có nhận dạng đúng theo tên gọi và mã số nhận dạng cá nhân (PIN). Nhà cung cấp dịch vụ chứng nhận (CSP) phải

là pháp nhân đáp ứng các yêu cầu pháp lý cụ thể, còn nhà cung cấp dịch vụ dấu thời gian (TSP) sẽ cung cấp dấu thời gian, đơn giản là một đơn vị dữ liệu chứng minh rằng có dữ liệu cụ thể nào đó tồn tại ở một thời điểm cụ thể.

4. **Uỷ ban về Chuẩn về Dữ liệu Sinh trắc.** Chính phủ có thể thành lập một uỷ ban quốc gia để xác định các chuẩn mực về dữ liệu sinh trắc có thể áp dụng cho các thiết bị quét/đọc, khai thác và đối chiếu dữ liệu sinh trắc học. Các chuẩn này cần được ban hành trên cơ sở các chuẩn mực hiện hành đang được sử dụng phổ biến trong ngành của quốc gia và quốc tế. Uỷ ban bao gồm các thành viên từ phía chính phủ, giới nghiên cứu, các chuyên gia trong ngành; chuẩn mực này được xác định qua tham vấn với các cơ quan khác của chính phủ và các nhà cung cấp dịch vụ tại khu vực tư nhân.

5. **Các dịch vụ định danh điện tử (eID), cơ sở hạ tầng thông tin và các dịch vụ thuộc sở hữu và quản lý bởi Bộ phụ trách về công nghệ thông tin.** Chính phủ có thể có một bộ/cơ quan chịu trách nhiệm về các chính sách liên quan đến CNTT và cung cấp các dịch vụ CNTT cho các cơ quan chính phủ đang triển khai điều hành điện tử. Cơ quan này chịu trách nhiệm hỗ trợ kỹ thuật, các dịch vụ và cơ sở hạ tầng CNTT dùng chung trên toàn quốc mà cơ quan chính phủ chịu trách nhiệm có thể được sử dụng để cung cấp dịch vụ định danh điện tử (eID).

6. **Uỷ ban về bảo mật thông tin riêng tư.** Uỷ ban về bảo mật thông tin riêng tư có thể được thành lập để báo cáo cho cơ quan có thẩm quyền cao nhất (Nghị viện hoặc văn phòng Tổng thống) nhằm đảm bảo các quy định về bảo mật thông tin riêng liên quan đến dữ liệu nhận dạng và sử dụng dữ liệu luôn được tôn trọng.

Mô hình hoạt động

1. **Đăng ký mới công dân cho các dịch vụ định danh điện tử (eID) để đảm bảo dữ liệu định danh điện tử (eID) chất lượng cao.** Chất lượng dữ liệu cá nhân trong cơ sở dữ liệu của các nhà cung cấp đang bị thiếu và có rất nhiều vấn đề về gian lận, trùng lặp/ đối tượng ma. Để tránh các vấn đề đó được đưa vào cơ sở dữ liệu nhận dạng điện tử, dữ liệu cá nhân – cả dữ liệu sinh trắc và nhân chủng học – cần được thu thập và xác nhận qua một quy trình đăng ký. Điều này nhằm đảm bảo dữ liệu được thu thập là dữ liệu sạch ngay từ đầu quy trình.

2. **Hệ thống người giới thiệu trong các dịch vụ định danh điện tử dành cho tất cả mọi người.** Hệ thống Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) là hệ thống dành

cho tất cả mọi người và được sử dụng cho mọi công dân, bao gồm cả những người chưa có giấy tờ chứng minh nhận dạng dưới bất kỳ hình thức nào. Có thể cần phải có một "hệ thống người giới thiệu" cho các công dân không có chứng minh nhận dạng dưới bất kỳ hình thức nào và định danh điện tử (eID) sẽ là hình thức chứng minh nhận dạng đầu tiên của họ. Người giới thiệu là người đứng ra bảo lãnh về dữ liệu nhân chủng học cá nhân của cá nhân đó được nhập liệu vào hệ thống định danh điện tử (eID). Cần lưu ý rằng hệ thống đó có thể có vấn đề, cần được giám sát chặt chẽ bởi xã hội dân sự và có cơ chế khiếu nại phản hồi rõ ràng từ phía các bên liên quan ở địa phương.

3. **Mô hình hoạt động cung cấp dịch vụ định danh điện tử bảo mật theo hình thức quan hệ hợp tác công – tư (PPP)**. Mô hình hoạt động nhằm cung cấp các dịch vụ định danh điện tử (eID) sử dụng Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) có thể được mở rộng và thực hiện theo mô hình quan hệ hợp tác công – tư (PPP).
    a. Mô hình hoạt động này nhằm đảm bảo an ninh bảo mật của Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) qua việc chỉ cho phép một số lượng hạn chế các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có đăng ký được kết nối trực tiếp với các dịch vụ định danh điện tử (eID) qua web.
    b. Một đơn vị bất kỳ muốn sử dụng các dịch vụ định danh điện tử (eID) được cung cấp bởi Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) cần phải đăng nhập với tư cách là Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và phải ký kết thoả thuận với cơ quan chủ quản của chính phủ. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) phải thực hiện điều đó qua Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).
    c. Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể thiết lập kết nối bảo mật tới các dịch vụ định danh điện tử (eID) trên Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) để truyền yêu cầu thay mặt cho các Tổ chức sử dung dịch vụ định danh điện tử (ISCA), sau đó nhận phản hồi lại từ các dịch vụ đó.
    d. Các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể tạo lập và duy trì kết nối bảo mật của họ với Hệ thống cung cấp dịch vụ định danh điện tử (EISDP), tuân thủ theo các chuẩn mực và yêu cầu kỹ thuật do cơ quan chủ quản của chính phủ đặt ra.
    e. Có thể cần phải có một quy trình đăng ký tham gia cho các bên liên quan (ISPA, ISCA, v.v.) để cung cấp các dịch vụ định danh điện tử (eID) cho các tổ chức thuộc chính phủ và khu vực tư nhân. Quy trình này chỉ cần đơn giản, nhưng đồng thời phải bao gồm các yếu tố đối trọng và cân đối cần thiết để đảm bảo các cơ quan được lựa chọn có khả năng cung cấp dịch vụ. Cần phải có một quy trình được

xác định rõ ràng theo từng bước để đăng ký làm Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) hoặc Tổ chức sử dung dịch vụ định danh điện tử (ISCA), trong đó bao gồm một danh mục các tài liệu theo hồ sơ cho từng loại tổ chức như công bố trên cổng thông tin công cộng.

4. **Nhận thức và chấp nhận về mặt kỹ thuật.** Có thể cần có một cổng thông tin công cộng để nâng cao nhận thức kỹ thuật và cung cấp hỗ trợ kỹ thuật cho các cơ quan đơn vị sử dụng ở cả khu vực công và khu vực tư nhân. Cổng thông tin này nhằm công bố các tài liệu kỹ thuật như các chuẩn mực, các yêu cầu kỹ thuật về giao diện lập trình ứng dụng (hàm API) trên cổng thông tin để các chuyên gia phần mềm quan tâm có thể lồng ghép các dịch vụ định danh điện tử (eID) vào các ứng dụng của họ.

5. **Chứng nhận thiết bị sinh trắc hoặc mã số nhận dạng duy nhất (UID) cho các ứng dụng sử dụng định danh điện tử (eID).** Có thể cần áp dụng một quy trình chứng nhận đối với các thiết bị sinh trắc để đảm bảo các thiết bị đó tuân thủ theo các đặc tả kỹ thuật do cơ quan chủ quản của chính phủ ban hành. Trách nhiệm triển khai quy trình chứng nhận được giao cho một vụ/cục tại Bộ Thông tin và Truyền thông (MIC) chịu trách nhiệm về cung cấp các dịch vụ đảm bảo chất lượng trong lĩnh vực CNTT và điện tử trong mạng lưới các trung tâm và phòng thí nghiệm của quốc gia. Đơn vị này có thể duy trình một danh mục các thiết bị sinh trắc của các nhà cung cấp được chứng nhận. Các nhà cung cấp nếu muốn thiết bị sinh trắc của họ được chứng nhận cần tuân thủ theo quy trình chứng nhận do vụ/cục đó đặt ra. Quy trình này được công bố trên cổng thông tin công cộng của cơ quan chủ quản của chính phủ. Phương án khác là thiết bị có thể sử dụng chuẩn mã nhận dạng duy nhất (UID) của Ấn Độ, để giảm chi phí, cải thiện chung về hiệu suất và bảo mật.

6. **Mô hình vận hành dịch vụ định danh di động an toàn và có thể mở rộng theo hình thức quan hệ hợp tác công – tư (PPP).**
    a. **Đăng nhập bảo mật.** Giống như tại Ét-xtô-nia, kịch bản tiêu biểu về xác thực định danh điện tử trên cơ sở định danh di động được sử dụng để đăng nhập vào các trang thong tin bảo mật, ví dụ tài khoản ngân hàng của công dân, có thể là:
        i. Công dân bấm vào nút chọn "kích hoạt bằng định danh di động trên trang web được hỗ trợ.
        ii. Công dân được nhắc đăng nhập bằng số điện thoại di động và mã số nhận dạng cá nhân (PIN) của mình.
        iii. Trang web đó sẽ thể hiện một mã xác nhận duy nhất.

iv. Điện thoại sẽ phát tiếng kêu bíp và biểu diễn trên màn hình chỉ báo cho thấy kết nối đang được thiết lập.
v. Màn hình điện thoại hiện lên mã số xác nhận và tên dịch vụ xác thực nhận dạng điện tử.
vi. Nếu tên dịch vụ là đúng và mã số xác nhận khớp với con số được hiển thị trên trang của máy tính, thì đó là điều kiện an toàn để ấn nút "Chấp nhận".
vii. Người sử dụng được nhắc nhập mã số nhận dạng cá nhân di động trên điện thoại di động.
viii. Màn hình điện thoại biến mất và trang web tự động được tải lại bằng màn hình đã đăng nhập.

b. **Cung cấp định danh di động.** Các nhà điều hành di dộng quốc gia trong nước có thể phát hành định danh di động qua các cửa hàng tại địa phương của họ. Công dân có thể tìm đến nhà điều hành di động gần nhất để có được SIM có chức năng nhận dạng di động. Nhà cung cấp dịch vụ đó có thể chuyển tiếp ứng dụng cho Nhà điều hành mạng di động (MNO) và thông báo cho công dân địa điểm để nhận SIM. Công dân đó có thể được yêu cầu phải mang thẻ chứng minh nhận dạng của mình với những chứng nhận hợp lệ để được nhận định danh di động và phải ký kết hợp đồng (thoả thuận đăng ký thuê bao nhận dạng di động) để hoàn tất giao dịch. Chính phủ có thể phân giao trách nhiệm phát hành định danh di động cho các nhà điều hành di động quốc gia. Nhà điều hành mạng di động (MNO) xác định nhận dạng của người sử dụng bằng thẻ chứng minh nhận dạng và sau khi xác thực thành công, sẽ chuyển SIM mới cho công dân đó. Trong quá trình cung cấp, SIM được gắn với một Thiết bị tạo chữ ký bảo mật (SSCD) duy nhất của công dân đó, và Thiết bị tạo chữ ký bảo mật (SSCD) này sau đó có thể được sử dụng để cấp ra chứng nhận đủ điều kiện. Chứng nhận Thiết bị tạo chữ ký bảo mật (SSCD) nhằm tuyến bố kích hoạt cho SIM cụ thể và được sử dụng bởi toàn bộ các Nhà cung cấp dịch vụ tin cậy (TSP). Nhà điều hành mạng di động (MNO) có thể cung cấp mã số duy nhất cho công dân để kích hoạt chứng nhận đủ điều kiện.

c. **Kích hoạt chứng nhận/đăng ký sử dụng.** Công dân được kích hoạt dịch vụ trên thiết bị cầm tay của mình với SIM chuyên dụng mới. Để kích hoạt dịch vụ nhận dạng di động hoặc áp dụng cho các chứng nhận, công dân đó cần vào trang web của cơ quan an ninh công cộng, Tổ chức quản lý đăng ký (RA). Công dân đó cần điền vào mẫu đơn trực tuyến và nhập thẻ chứng minh nhận dạng của mình vào máy đọc thẻ, sau đó tuân thủ theo hướng dẫn. Mục đích của quy trình kích hoạt

chứng nhận là để tạo và kích hoạt chứng nhận đủ điều kiện. Công dân đó cần gửi yêu cầu kích hoạt chứng nhận đủ điều kiện bằng điện thoại di động với SIM mới. Tổ chức quản lý đăng ký (RA) sẽ khởi tạo chữ ký bằng cách trả lời cho thiết bị di động của công dân đó để ký dữ liệu cá nhân. Công dân đó cần thẩm định dữ liệu và sau đó ký kết bằng cách nhập mã kích hoạt chứng nhận trên thiết bị. Tổ chức quản lý đăng ký (RA) lúc này nhận được dữ liệu cá nhân đã ký kết. Tổ chức quản lý đăng ký (RA) sau đó gắn dữ liệu bổ sung, bao gồm chứng nhận thiết bị, trước khi chuyển yêu cầu kích hoạt chứng nhận cho Cơ quan có thẩm quyền chứng nhận (CA). Cơ quan có thẩm quyền chứng nhận (CA) sẽ tạo lập và kích hoạt chứng nhận đủ điều kiện và công bố chứng nhận đó.

d. **Sử dụng.** Nhà cung cấp dịch vụ có thể yêu cầu dịch vụ, như xác thực định danh điện tử từ một Nhà cung cấp dịch vụ tin cậy (TSP) và sử dụng mã số nhận dạng cá nhân và/hoặc số thuê bao GSM để xác nhận công dân. Nhà cung cấp dịch vụ tin cậy (TSP) có thể tạo yêu cầu chữ ký và gửi yêu cầu đó vào điện thoại di động của công dân. Công dân đó sẽ ký kết yêu cầu bằng cách nhập mã số nhận dạng cá nhân (PIN) được giao. Nhà cung cấp dịch vụ tin cậy (TSP) tiếp theo nhận được dữ liệu chữ ký. Nhà cung cấp dịch vụ tin cậy (TSP) sau đó kiểm tra tính xác thực của dữ liệu chữ ký cũng như tính xác thực của chứng nhận đó. Nhà cung cấp dịch vụ sau đó được tiếp nhận các dịch vụ liên quan đến định danh điện tử (eID) của Nhà cung cấp dịch vụ tin cậy (TSP).

e. **Kết thúc.** Công dân có thể ngừng sử dụng nhận dạng di động vì một số lý do, chẳng hạn như: công dân có thể không còn sử dụng dịch vụ nữa, bị mất hoặc có vấn đề về thiết bị tạo chữ ký bảo mật (SSDC), chứng nhận đủ điều kiện đã hết hạn, hoặc công dân đó có thể vi phạm thoả thuận giữa Cơ quan có thẩm quyền chứng nhận (CA) và người sử dụng. Trong trường hợp chứng nhận bị thu hồi, Tổ chức quản lý đăng ký (RA) sẽ thông báo cho Cơ quan có thẩm quyền chứng nhận (CA) về tình trạng đó và Cơ quan có thẩm quyền chứng nhận (CA) ngay lập tức huỷ bỏ chứng nhận. Lúc này, Danh mục huỷ bỏ chứng nhận (CRL) có thể được cập nhật. Trong trường hợp bị khoá SIM do mất hoặc hư hỏng SIM, chứng nhận thiết bị sẽ bị rút khỏi danh mục các thiết bị tạo chữ ký bảo mật (SSDC) được sử dụng bởi toàn bộ các Nhà cung cấp dịch vụ tin cậy (TSP).

f. **Phí định danh di động.** Nhà điều hành di động có thể thu phí công dân để cho phép sử dụng dịch vụ định danh di động. Phí đó có thể bao gồm phí thuê bao một lần cũng như phí hàng tháng. Nếu định danh di động được sử dụng ở nước ngoài, mỗi giao dịch định danh di động sẽ được tính phí bằng chi phí gửi tin nhắn văn bản dựa trên danh mục giá của gói đó.

7. **Thiết bị và phần mềm nhận dạng sẵn có để đẩy mạnh áp dụng.** Để đẩy mạnh việc áp dụng chữ ký số trong khu vực, công nghệ và phần mềm tương thích có thể có sẵn cho các bên sử dụng mong muốn lồng ghép chữ ký số vào các ứng dụng của họ.

8. **Dịch vụ trực tuyến và trung tâm giải đáp thắc mắc 24/7 để ngăn ngừa gian lận định danh điện tử (eID).** Để ngăn ngừa gian lận định danh điện tử (eID), chính phủ có thể thiết lập trung tâm giải đáp thắc mắc 24/7 suốt năm hoặc cung cấp các dịch vụ "DocStop" và "CheckDoc". DocStop giúp tránh rủi ro gian lận trong sử dụng các tài liệu định danh điện tử và cả hệ quả tài chính của điều đó. DocStop cho phép công dân nhanh chóng khoá hồ sơ định danh điện tử (eID) và thẻ nhận dạng trong trường hợp thông tin liên quan bị mất, bị mất trộm hoặc có vấn đề. Công dân đó cần phải gọi số miễn phí về DocStop để báo cáo về trường hợp của mình. Dịch vụ này được cung cấp 24/7 trong suốt năm. Dịch vụ CheckDoc cho phép công dân xác nhận theo thời gian thực về tính hợp lệ của các tài liệu định danh điện tử (eID); nó cũng xác định ra các tài liệu định danh điện tử (eID) bị mất trộm, thất thoát, hết hạn, mất hiệu lực hoặc chưa bao giờ sử dụng. Để sử dụng dịch vụ này, công dân hoặc tổ chức sử dụng cần phải đăng ký bằng cách điền vào mẫu đăng ký. Trang web đó có thể được truy cập bằng tên người sử dụng và mật khẩu sau khi đăng ký thành công.

<u>Chính sách</u>

1. **Nhận dạng và xác nhận khách hàng (KYC).** Các nhà cung cấp dịch vụ ở cả khu vực công và tư nhân tại các lĩnh vực như ngân hàng, bảo hiểm, thị trường vốn, viễn thông, kinh doanh khí hoá lỏng (LPG), đường sắt, v.v. có thể cập nhật các thông lệ nhằm nhận dạng và xác nhận khách hàng (KYC) của mình để định danh điện tử cũng được coi là hình thức nhận dạng và xác nhận khách hàng (KYC) hợp lệ.

2. **Chính sách về chuẩn dữ liệu sinh trắc.** Chính phủ có thể ban hành chính sách ở cấp quốc gia nhằm chuẩn hoá về sử dụng dữ liệu sinh trắc cho các mục đích nhận dạng và xác thực của công dân.

3. **Luật chữ ký số (DSA).** Chính phủ có thể thông qua Luật chữ ký số (DSA) nhằm đảm bảo chữ ký số của công dân được phát hành bởi một cơ quan chính phủ có thẩm quyền là chứng nhận hợp lệ và có giá trị ràng buộc pháp lý, tương đương với chữ ký viết tay trên giấy. Chữ ký số và chữ ký viết tay có thể được coi là tương đương ở cả khu vực công và tư nhân theo Luật này. Luật chữ ký số (DSA) cũng có thể quy định các đơn vị hành chính

và sự nghiệp của chính phủ phải chấp nhận các tài liệu có chữ ký số. Luật chữ ký số (DSA) cũng đảm bảo mỗi chữ ký số là chữ ký nhận dạng duy nhất, ràng buộc cá nhân đó với dữ liệu được ký kết, và đảm bảo rằng dữ liệu được ký kết không bị làm sai lệch mà không làm cho chữ ký đó mất hiệu lực.

4. **Các quy tắc và quy định về nhà cung cấp dịch vụ chứng nhận.** Một trong những nội dung chính của Luật chữ ký số (DSA) là nhằm xác định ra các quy tắc và quy định liên quan đến các Nhà cung cấp dịch vụ chứng nhận (CSP) nơi ban hành chứng nhận số cho người sử dụng và quản lý các dịch vụ bảo mật liên quan. Luật chữ ký số (DSA) cần đặt ra các yêu cầu chặt chẽ về thủ tục và tài chính để đảm bảo các Nhà cung cấp dịch vụ chứng nhận (CSP) được thành lập và quản lý một cách phù hợp để thực hiện các chức năng của họ với chuẩn mực cao nhất có thể.

5. **Các quy tắc và quy định về nhà cung cấp dịch vụ dấu thời gian.** Luật chữ ký số (DSA) cũng quy định về đánh dấu thời gian bởi các Nhà cung cấp dịch vụ tin cậy (TSP). Các nhà cung cấp dịch vụ này cần tuân thủ các luật và quy định tương tự như áp dụng cho các Nhà cung cấp dịch vụ chứng nhận (CSP). Dấu thời gian đơn giản là một mẩu dữ liệu để chứng thực về việc đã diễn ra một sự kiện vào một thời điểm cụ thể. Luật chữ ký số (DSA) cần đảm bảo dữ liệu được đánh dấu thời gian không bị thay đổi hoặc sửa chữa mà không làm mất hiệu lực của dấu thời gian đó.

6. **Luật bảo vệ dữ liệu cá nhân (PDPA).** Luật bảo vệ dữ liệu cá nhân (PDPA) quy định về việc sử dụng các cơ sở dữ liệu và dữ liệu cá nhân bởi các cơ quan công quyền và các đơn vị thuộc khu vực tư nhân. Luật quy định về nhiệm vụ của một đơn vị thanh tra về bảo vệ dữ liệu trong chính phủ để giám sát việc tuân thủ các yêu cầu của Luật; đồng thời để thực thi hiệu lực nếu cần thiết. Chiến lược bảo vệ thẻ nhận dạng là lưu trữ dữ liệu cá nhân trên thẻ ở mức tối thiểu. Còn dữ liệu được lưu giữ tại các cơ sở dữ liệu có độ bảo mật cao tại các trung tâm có thẩm quyền. Cá nhân có thể sử dụng thẻ này để làm chìa khoá (phương pháp cấp quyền) nhằm truy cập thông tin cá nhân của mình trên cơ sở dữ liệu đó. Các yêu cầu từ bên thứ ba (ví dụ đại diện của chính quyền) về dữ liệu cá nhân sẽ được ghi lại vào bản ghi, và các bản ghi đó được công bố trực tuyến cho cá nhân đó theo yêu cầu (qua cổng thông tin của công dân).

7. **Luật tài liệu chứng minh nhận dạng (IDA).** Chính phủ có thể thông qua hoặc cập nhật nếu đã có Luật tài liệu chứng minh nhận dạng (IDA), quy định về các tài liệu liên quan

nhằm hướng dẫn ở cấp quốc gia về tạo lập Mã số định danh công dân (NIN) và cấp thẻ nhận dạng và định danh điện tử (eID) cho các công dân của quốc gia.

a. Luật tài liệu chứng minh nhận dạng (IDA) có thể coi định danh điện tử (eID) có giá trị tương đương như tài liệu chứng minh nhận dạng trên giấy hiện nay cho tất cả các mục đích pháp lý.
b. Luật tài liệu chứng minh nhận dạng (IDA) có thể xác định mục đích của thẻ và Mã số định danh công dân (NIN) để nhằm chứng minh tư cách công dân. Tại Ấn Độ, số chứng minh nhận dạng duy nhất (UID) chỉ được sử dụng để chứng minh nhận dạng, chứ không chứng minh được tư cách công dân. Để có thêm chi tiết, đề nghị tham khảo kinh nghiệm của Ấn Độ tại Phụ lục 5.
c. Luật tài liệu chứng minh nhận dạng (IDA) có thể quy định dữ liệu sinh trắc và nhân chủng học của công dân đã được loại bỏ trùng lặp và xử lý để phục vụ mục đích cá nhân hoá trên thẻ cũng có thể được nhập vào hệ thống đăng ký dân số quốc gia theo Luật về đăng ký dân số.

4.0 Hiện trạng sử dụng nhận dạng và các vấn đề về cung cấp dịch vụ mà Việt Nam đang phải đối mặt

Phần tìm hiểu hiện trạng các hệ thống nhận dạng và các vấn đề về cung cấp dịch vụ liên quan đến nhận dạng mà các công dân cũng như nhà cung cấp dịch vụ ở cả khu vực công và tư nhân phải đối mặt được trình bày dưới đây. Nội dung tìm hiểu này được soạn thảo qua thảo luận với các bên liên quan tại Việt Nam cũng như nghiên cứu tài liệu thứ cấp trên mạng.

4.1 Tìm hiểu về hiện trạng các hệ thống nhận dạng tại Việt Nam

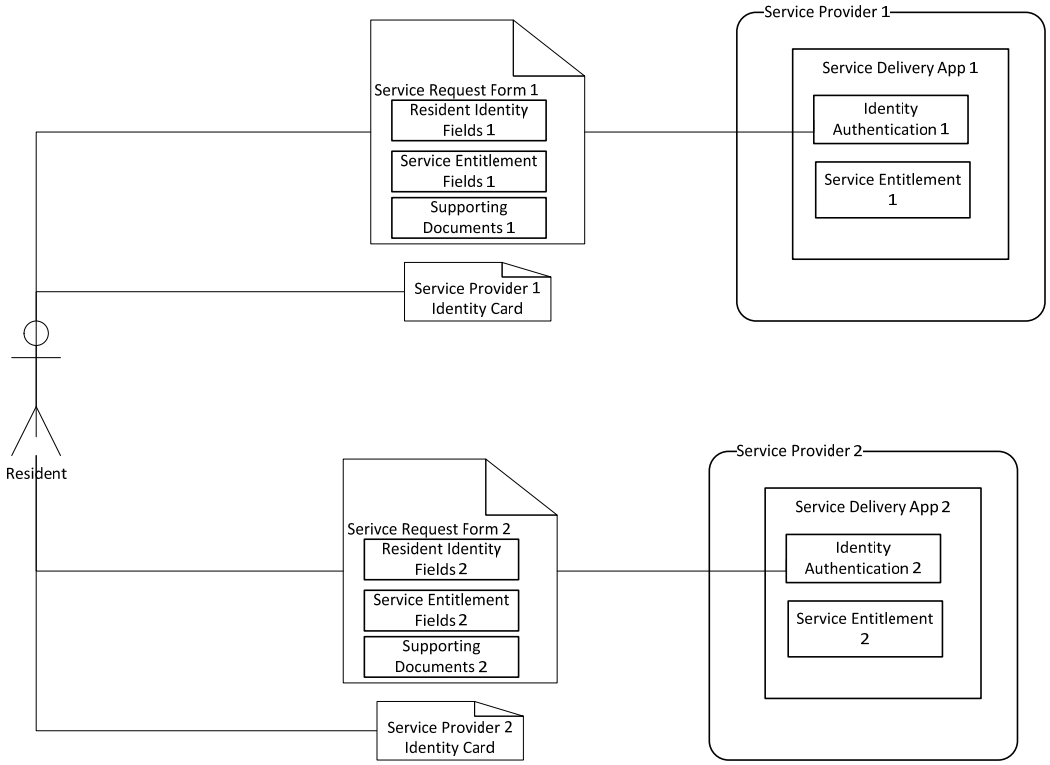
Thẻ chứng minh thư nhân dân: Tài liệu chứng minh nhận dạng chung tại Việt Nam

Hình 4.1: Thẻ chứng minh thư nhân dân

Bộ Công an (MPS) cấp thẻ chứng minh thư nhân dân (thẻ chứng minh nhận dạng) và mã số chứng minh nhận dạng cho toàn bộ công dân tại Việt Nam. Các nhà cung cấp dịch vụ sử dụng thẻ đó làm tài liệu chứng minh nhận dạng để xác định nhận dạng của một công dân. Thẻ chứng minh nhận dạng là tấm thẻ giấy Sở Công an cấp tỉnh cấp cho tất cả các công dân có độ tuổi trên

14. Thẻ này mang tên gọi, địa chỉ, độ tuổi, chiều cao, cân nặng, ngày phát hành, và một vết vân tay; thẻ có giá trị trong vòng mười năm. Khoảng 98% người dân Việt Nam có thẻ này.

Hiện trạng quy trình tạo lập và xác thực nhận dạng trong quá trình cung cấp dịch vụ tại Việt Nam



Hình 4.2: Quy trình xác thực nhận dạng hiện hành để cung cấp dịch vụ

Tại Việt Nam cũng như các quốc gia khác, các đơn vị ở cả khu vực công và khu vực tư nhân trên toàn quốc thường yêu cầu chứng minh nhận dạng trước khi cung cấp dịch vụ cho các cá nhân công dân. Đối với một tổ chức bất kỳ, xác định nhận dạng và quyền hưởng của đối tượng thụ hưởng là yêu cầu cần thiết trước khi cung cấp dịch vụ cho một công dân, cho dù đó là mở tài khoản ngân hàng, rút hoặc gửi tiền, hay cấp mã số thuế, nhận hưu bổng, hoặc đi du lịch. Nhận dạng cá nhân có thể mang tính duy nhất và độc lập với dịch vụ sử dụng, nhưng quyền hưởng lại được xác lập rất cụ thể cho dịch vụ mong muốn; do đó, hai vấn đề này phải được xác định riêng. Chẳng hạn, thẻ bảo hiểm y tế thường được cấp dựa trên thẩm định nhận dạng của cá nhân (tên gọi, địa chỉ) và xác định quyền hưởng bảo hiểm y tế.

Việc xác lập nhận dạng thường bao gồm hai bước: tạo lập nhận dạng và xác thực nhận dạng. Việc tạo lập nhận dạng là cơ chế xác định nhận dạng của một cá nhân bằng cách cung cấp (các) mã thông báo nhận dạng (token) cho người đó theo cùng một hình thức (vật chất và/hoặc điện

tử). Đây là hoạt động diễn ra một lần. Việc xác thực nhận dạng là quy trình thẩm định "cá nhân người đòi hỏi đó là ai" bằng cách kiểm tra mã thông báo nhận dạng gán cho cá nhân đó. Việc này có thể thực hiện bằng hình thức thủ công, điện tử hoặc kết hợp cả hai.

Các nhà cung cấp dịch vụ ở cả khu vực công và tư nhân thường thực hiện các quy trình riêng của họ trong việc tạo lập nhận dạng, bên cạnh việc xác định quyền hưởng dịch vụ. Để minh hoạ cho điều đó, Bảo hiểm Xã hội Việt Nam (VSS) duy trì một cơ sở dữ liệu riêng về các đối tượng thụ hưởng và xác định quyền hưởng dịch vụ của những người đó theo từng chương trình phúc lợi như bảo hiểm y tế và bảo hiểm xã hội. Mỗi công dân được giao một mã thông báo nhận dạng riêng cho từng chương trình để xác thực nhận dạng và thẩm định quyền hưởng.

Mỗi nhà cung cấp dịch vụ tại Việt Nam thường phải sử dụng thẻ chứng minh nhận dạng và các tài liệu chứng minh nhận dạng khác như hộ chiếu để xác định nhận dạng nhằm tạo ra thẻ nhận dạng mới liên quan cụ thể đến nhà cung cấp dịch vụ mới đó. Thẻ nhận dạng đó cũng được sử dụng để xác lập quyền hưởng dịch vụ. Công dân phải trình thẻ nhận dạng cụ thể liên quan đến nhà cung cấp đó để xác thực và hưởng quyền của mình vào thời điểm dịch vụ được cung cấp.

Bảo hiểm Xã hội Việt Nam (VSS). Bảo hiểm Xã hội Việt Nam (VSS) đang trong quá trình tập trung và hợp nhất các cơ sở dữ liệu về đối tượng hưởng lợi tại các chương trình khác nhau, bao gồm bảo hiểm y tế và bảo hiểm xã hội hiện đang tồn tại ở cấp địa phương. Hiện nay, khó ai có thể xác định được một công dân duy nhất từ các cơ sở dữ liệu khác nhau theo chương trình vì các hệ thống CNTT và cơ sở dữ liệu đều có cấu trúc phân tán và không có chuẩn dữ liệu chung để lưu trữ thông tin cơ bản về công dân đó. Hơn nữa, mỗi cơ sở dữ liệu lại lưu trữ một hệ thống nhận dạng riêng để xác định ra đối tượng thụ hưởng. Mã số chứng minh nhận dạng trong sổ sách của bảo hiểm y tế và bảo hiểm xã hội không nhất quán với nhau. Trong tổng dân số gồm 90 triệu công dân Việt Nam, 10 triệu hiện thuộc lực lượng lao động và khoảng 60 triệu được cấp thẻ bảo hiểm y tế. Hiện đang có nhu cầu về một mã số nhận dạng duy nhất gán cho các công dân để họ có thể sử dụng suốt đời. Bảo hiểm Xã hội Việt Nam (VSS) hiện đang đợi Chính phủ Việt Nam cấp Mã số định danh công dân (NIN) cho công dân để họ có thể quản lý tốt hơn các chương trình bảo hiểm y tế và bảo hiểm xã hội của mình.

Bộ Lao động, Thương binh và Xã hội. Phòng Lao động thuộc Bộ Lao động, Thương binh và Xã hội (MoLISA) hiện đang duy trì hai cơ sở dữ liệu tách biệt không liên quan với nhau về cung và cầu trên thị trường lao động do sử dụng các trường dữ liệu khác nhau để nhận dạng đối tượng thụ hưởng trên các cơ sở dữ liệu. Dữ liệu về cầu trên cơ sở dữ liệu chủ yếu thu thập từ các cơ quan của chính phủ, doanh nghiệp nhà nước và doanh nghiệp tư nhân. Các trường dữ liệu để nhận dạng công dân trên cơ sở dữ liệu đó là thẻ chứng minh nhận dạng hoặc hộ chiếu. Dữ liệu về cung trên các cơ sở dữ liệu đó sử dụng sổ hộ khẩu để nhận dạng đối tượng thụ hưởng.

Người thụ hưởng được cấp một mã số duy nhất dựa vào mã địa bàn do chính quyền cấp theo địa chỉ thường trú của công dân đó, bao gồm mã vùng, mã tỉnh, mã huyện, mã xã, số hộ khẩu và mã số thành viên gia đình. Bộ hiện đang thực hiện thí điểm tại hai huyện về thu thập thông tin cung cho cơ sở dữ liệu theo thẻ chứng minh, coi đó là tài liệu chứng minh nhận dạng chính để có thể kết nối với thông tin cầu trên các cơ sở dữ liệu. Bộ cũng đang cập nhật các cơ sở dữ liệu hàng năm để đảm bảo độ chính xác của thông tin – một quy trình tốn nhiều công sức và thời gian. Bộ có khả năng tránh nhu cầu phải cập nhật hàng năm và củng cố các cơ sở dữ liệu tự động nếu có một hệ thống chứng minh nhận dạng duy nhất cho các công dân. Các tổ chức và đơn vị của chinh phủ và của khu vực công dân cũng có thể sử dụng hệ thống này để nhận dạng người lao động của mình và công dân nói chung. Bộ đang thu thập dữ liệu về đối tượng thụ hưởng có độ tuổi từ mười trở lên trên cơ sở dữ liệu về thị trường lao động. Chính vì vậy Bộ mong muốn kiến nghị chính phủ giảm độ tuổi tối thiểu cần cấp mã số chứng minh nhận dạng quốc gia xuống mười tuổi. Hiện nay đề xuất độ tuổi bắt đầu được cấp thẻ chứng minh nhận dạng là 14 tuổi.

Bộ Giáo dục và Đào tạo. Bộ Giáo dục và Đào tạo (MoET) đang thiết kế một Hệ thống thông tin quản lý giáo dục tập trung (EMIS) cho toàn bộ các trường học tại Việt Nam để thống nhất quản lý hoạt động. Bộ đang cung cấp kết nối internet miễn phí cho toàn bộ các trường học trên cả nước và đang trong quá trình xây dựng các cơ sở dữ liệu điện tử về học sinh và giáo viên trên toàn quốc. Cơ sở dữ liệu điện tử gồm 20 triệu học sinh trên toàn quốc sẽ được hình thành trong ba năm. Bộ Giáo dục và Đào tạo (MoET) bày tỏ nhu cầu có mã số chứng minh nhận dạng duy nhất công dân để giúp xác định chính xác học sinh và giáo viên giữa các trường. Hiện nay, Bộ đang gặp khó khăn trong việc xác định nhận dạng những học sinh chuyển trường trong các năm qua. Bên cạnh đó là những thách thức tương tự trong việc xác định giáo viên và nhu cầu đào tạo giáo viên.

Bộ Y tế. Bộ Y tế (MoH) đang triển khai nhiều chương trình của chính phủ nhằm cung cấp phúc lợi cho công dân như bảo hiểm y tế, miễn phí thuốc HIV, v.v. trên cơ sở nhận dạng công dân. Bộ đã không thành công trong nỗ lực xây dựng một hệ thống nhận dạng bệnh nhân duy nhất trong mười năm qua sao cho mỗi bệnh nhân chỉ có một mã số chứng minh nhận dạng có thể sử dụng tại các bệnh viện khác nhau và các dịch vụ chăm sóc y tế khác. Nhận dạng bệnh nhân duy nhất này có thể được bệnh nhân sử dụng suốt đời với mục định để nhận dạng và duy trì Hồ sơ y tế điện tử/ Y bạ điện tử (EHR). Bộ mong muốn tận dụng được hệ thống chứng minh nhận dạng quốc gia và mã số nhân jdangj duy nhất trong hệ thống của mình để xác nhận bệnh nhân. Bộ Y tế (MoH) bày tỏ quan ngại về tình trạng thiếu nhận thức về lợi ích của các Hệ thống định danh điện tử quốc gia (NID) và định danh điện tử (eID) cho công dân. Trên 70% dân số hiện không có kiến thức về công nghệ và có thể chưa quen sử dụng máy tính cũng như các thiết bị máy thanh

toán tiền bằng thẻ (máy PoS). Do đó, cần có phải có các chương trình nâng cao nhận thức về lợi ích của Hệ thống định danh điện tử quốc gia (NID) cho công dân, về sử dụng máy tính và các thiết bị khác để nâng cao hiệu quả chăm sóc y tế.

Ngân hàng Nhà nước Việt Nam. Các cán bộ Ngân hàng Nhà nước Việt Nam (SBV) bày tỏ quan ngại về vấn đề không có khả năng xác nhận nhận dạng duy nhất của cá nhân khi cấp chữ ký số. Mặt khác, họ đã cấp chữ ký số cho 7.000 cán bộ nhân viên của Ngân hàng Nhà nước Việt Nam (SBV) và các ngân hàng thương mại. Về cơ bản, chữ ký số được sử dụng trong thanh toán ngân hàng qua internet, ký kết các kết quả tài chính và báo cáo chính phủ. Hiện người ta đang sử dụng nhiều loại tài liệu chứng minh nhận dạng (PoI) khác nhau để xác nhận nhận dạng của công dân, đó là thẻ chứng minh nhận dạng, hộ chiếu, bằng lái xe, v.v. Việc triển khai một Hệ thống định danh điện tử quốc gia (NID) duy nhất với mã số duy nhất sẽ giải quyết được các vấn đề hiện nay là trùng lặp và mất trộm nhận dạng.

Tập đoàn Bưu chính Viễn thông Việt Nam (VNTP) và Tập đoàn Viettel. Hai nhà cung cấp dịch vụ viễn thông lớn nhất tại Việt Nam là Tập đoàn Bưu chính Viễn thông Việt Nam (VNPT) và Tập đoàn Viettel, mỗi tập đoàn có một mạng lưới khoảng 50 triệu khách hàng. Cả hai tập đoàn đều bày tỏ nhu cầu phải có một hệ thống nhận dạng duy nhất để thẩm định nhận dạng của công dân vào thời điểm đăng ký khách hàng mới. Hiện nay, các tập đoàn này đang cung cấp nhiều dịch vụ giá trị gia tăng trực tuyến trên máy tính và điện thoại di động như eBanking, mBanking, thanh toán các hoá đơn tiện ích, v.v. Các tập đoàn này cũng đang có kế hoạch triển khai SIM mới sử dụng chữ ký số để nộp tờ khai thuế điện tử, thanh toán điện tử và sử dụng dịch vụ ngân hàng di động. Các tập đoàn này đồng ý rằng đinh danh di động là dịch vụ khả thi về mặt năng lực kỹ thuật; tuy nhiên, cần phải có các biện pháp pháp lý nhằm thực thi hiệu lực của việc cấp và sử dụng hình thức định danh điện tử (eID) mới.

Vietcombank. Cũng như với các tổ chức khác được nêu tên ở chương này, Vietcombank cũng gặp phải những khó khăn trong việc xác nhận nhận dạng của công dân vào thời điểm đăng ký khách hàng mới trong hệ thống của mình. Vấn đề này là do có nhiều tài liệu chứng minh nhận dạng để xác nhận. Ngân hàng đã gặp phải các trường hợp, trong đó một cá nhân mở hai tài khoản ngân hàng khác nhau với hai nhận dạng khác nhau sử dụng hai tài liệu chứng minh nhận dạng (PoI) khác nhau. Vì lý do đó, ngân hàng không thể có được lịch sử tín dụng chính xác của công dân từ Trung tâm thông tin tín dụng (CIC). Các cán bộ của ngân hàng bày tỏ nhu cầu phải có một Hệ thống định danh điện tử quốc gia để họ có thể có được nhận dạng duy nhất cho công dân vào thời điểm đăng ký. Họ cũng mong muốn chính phủ cung cấp những hướng dẫn và hỗ trợ kỹ thuật cần thiết để hệ thống của họ được tích hợp với hệ thống định danh điện tử (eID) mới, và đảm bảo cả thẻ chứng minh nhận dạng cũ và hình thức định danh điện tử (eID) mới đều có hiệu lực trong giai đoạn quá độ.

4.2 Các vấn đề thường gặp về nhận dạng khi cung cấp dịch vụ tại Việt Nam

Cách tiếp cận hiện nay trong cơ chế tạo lập và xác thực nhận dạng đã dẫn đến những khó khăn như sau.

Chưa có nhận dạng duy nhất cho công dân

Thẻ chứng minh nhận dạng hiện nay đang sử dụng được chính quyền cấp tỉnh cấp cho công dân qua một chương trình tạo và cấp mã số cục bộ ở địa phương mà không có sự phối hợp chung ở cấp quốc gia. Do đó, có trường hợp bị trùng mã số ở các tỉnh khác nhau. Kết quả là, khó có thể nhận dạng duy nhất một công dân nếu chỉ dùng thẻ chứng minh nhận dạng.

Quy trình tạo lập và xác thực nhận dạng riêng của các nhà cung cấp dịch vụ bị trùng lặp, thiếu thống nhất và tốn kém

Do hệ thống nhận dạng hiện nay thiếu hiếu hiệu quả trong việc cung cấp nhận dạng duy nhất cho công dân, các nhà cung cấp dịch vụ ở cả khu vực công và tư nhân thường phải thực hiện quy trình riêng của họ để tạo lập nhận dạng khách hàng/ đối tượng thụ hưởng. Đây là yếu tố bổ sung bên cạnh việc xác định quyền hưởng dịch vụ, với khả năng tác nghiệp liên thông hạn chế hoặc thậm chí không có vì hầu hết các bằng chứng thông báo nhận dạng (token) chỉ được chấp nhận cho mục đích cụ thể và tại địa điểm cụ thể mà thôi. Hệ thống nhận dạng hiện nay chỉ hoạt động ở chế độ được hỗ trợ vì hầu hét các thẻ nhận dạng do các tổ chức cung cấp dịch vụ cung cấp đều là thẻ vật lý dựa trên "những gì bạn có". Điều này dẫn đến việc mỗi nhà cung cấp dịch vụ phải tốn phí nhiều hơn để thiết lập cơ chế xác thực. Hơn nữa, quy trình này có khả năng mở rộng hạn chế và gây ra vô cùng nhiều bất tiện cho công dân.

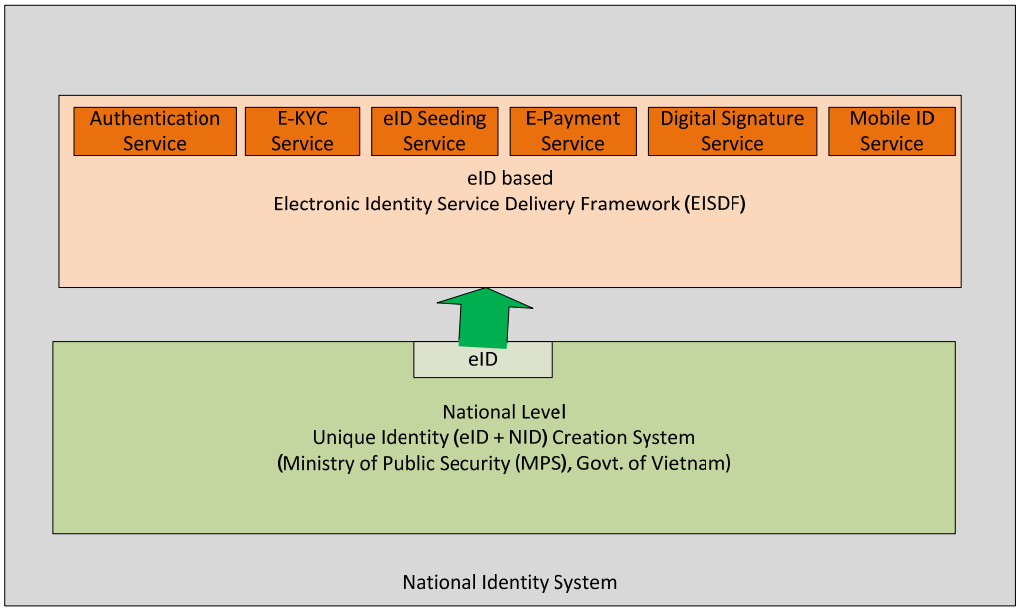
Quy trình tạo lập nhận dạng của nhà cung cấp dịch vụ có sự khác biệt về thông tin cá nhân được thu thập. Lý do là nhu cầu thẩm định và xác nhận thông tin đó dẫn đến việc tạo ra các nhận dạng khác nhau cho cùng một công dân. Ví dụ, Bảo hiểm Xã hội Việt Nam (VSS) duy trì một cơ sở dữ liệu riêng về các đối tượng thụ hưởng và xác định quyền hưởng dịch vụ của các đối tượng đó theo mỗi chương trình phúc lợi (bảo hiểm xã hội, bảo hiểm y tế, v.v.). Mỗi chương trình lại cấp ra một loại bằng chứng thông báo nhận dạng riêng (token) chẳng hạn dưới hình thức phiếu giấy. Điều này dẫn đến rò rỉ lợi ích phúc lợi do rất nhiều nhận dạng trùng lặp và giả mạo được tạo ra trong cùng một chương trình hưởng lợi. Các đơn vị cung cấp dịch vụ không có khả năng đối chiếu liên kết các lợi ích khác nhau cho cùng một công dân từ các chương trình khác nhau, vì thậm chí còn không có khả năng thẩm định chính xác được quyền hưởng. Thách thức đó có khả năng làm giảm tác động của các chương trình phúc lợi.

Thẻ chứng minh nhận dạng bằng giấy dẫn đến rủi ro mất trộm nhận dạng cao hơn

Với thẻ chứng minh nhận dạng bằng giấy, có một rủi ro lớn về chuyện mất trộm nhận dạng và lạm dụng bản sao khi trình chứng minh nhận dạng (PoI). Tài liệu vật lý có thể dễ dàng bị giả mạo và khó có thể xác định được các bản giả hoặc bản nhái. Đồng thời, những tài liệu đó không thể sử dụng để xác nhận người mang bằng chứng thông báo nhận dạng (token) đó chính là người được chứng minh nhận dạng trên thẻ, trừ khi thẻ đó có chứa ảnh.

Ngoài ra, thẻ chứng minh nhận dạng hiện tại dễ bị lạm dụng do thiếu hình thức bút tích kiểm tra xác thực mà chỉ dựa vào cơ chế kiểm tra thủ công khó thực hiện.

5.0 Tầm nhìn cho Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF)



Hình 5.1: Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF)

Để giải quyết những thách thức hiện các nhà cung cấp dịch vụ đang phải đối mặt liên quan đến nhận dạng duy nhất và xác nhận nhận dạng cho khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao, cần phải thiết lập một Hệ thống định danh điện tử quốc gia (NID) hiệu quả và có căn cứ hơn, bao gồm phải tạo lập định danh điện tử (eID) duy nhất ở cấp quốc gia và các dịch vụ định danh điện tử (eID), còn được gọi chung là Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) (Hình 5.1). Hệ thống định danh điện tử quốc gia (NID) đang được Bộ Công an (MPS) triển khai. Một hệ thống như thế nếu được triển khai sẽ giúp thực hiện được tầm nhìn về chính phủ điện tử (eGovernment) và hỗ trợ đổi mới về dịch vụ điện tử (eService) ở cả khu vực công và tư nhân, đồng thời tăng cường an ninh mạng. Định danh điện tử (eID) có thể tạo điều kiện cho công dân yêu cầu và tiếp nhận dịch vụ của các nhà cung cấp dịch vụ ở cả khu vực công và tư nhân ở bất kỳ nơi đâu, bất kỳ thời điểm nào, và bằng sử dụng bất kỳ thiết bị nào. Trọng tâm của chương này là nhằm xây dựng tầm nhìn cho Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF).

5.1 Mô tả tổng quát về Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF)

Các dịch vụ được cung cấp. Dưới đây là dẫn chứng về một số dịch vụ chính có thể được cung cấp sau khi triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF).

1. **Dịch vụ xác thực nhận dạng điện tử**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) hỗ trợ cung cấp các dịch vụ nhận dạng duy nhất và xác thực định danh điện tử trên toàn quốc cho công dân theo hình thức vật lý hoặc trực tuyến. Các nhà cung cấp dịch vụ ở cả khu vực công và khu vực tư nhân sẽ sử dụng khuôn khổ đó để cung cấp dịch vụ trên cơ sở định danh điện tử (eID) bằng cách sử dụng các ứng dụng dựa trên định danh điện tử (eID) cho các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao của họ.

2. **Dịch vụ tạo nguồn thông tin nhận dạng điện tử.** Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) cung cấp dịch vụ tạo nguồn thông tin định danh điện tử (eID), cho phép sử dụng tính năng xác thực định danh điện tử bằng cách đối chiếu hồ sơ các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao với Mã số định danh công dân (NIN) duy nhất được tạo ra ở cấp quốc gia qua đăng ký.

3. **Dịch vụ chữ ký số**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) giúp hiện thực hoá việc công dân ký chữ ký số trên các tài liệu điện tử (eDocument) trong các giao dịch với các đơn vị và tổ chức thuộc khu vực công và tư nhân. Điều này cho phép thực hiện các luồng công việc dịch vụ điện tử phi giấy tờ và bỏ qua nhu cầu phải sử dụng chữ ký viết tay.

4. **Dịch vụ nhận dạng và xác nhận khách hàng điện tử.** The Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể cung cấp quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC) qua đó, nhà cung cấp dịch vụ có khả năng định danh điện tử các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao của mình sau khi được cấp quyền khai thác. Quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC) dựa trên định danh điện tử (eID) sẽ cung cấp chứng minh nhận dạng (PoI) cũng như chứng minh địa chỉ (PoA) tức thời và không thể từ chối, cùng với ngày sinh và giới tính. Bên cạnh đó, nó còn tạo ra số điện thoại và địa chỉ thư điện tử của công dân cho nhà cung cấp dịch vụ, qua đó uy trình cung cấp dịch vụ ngày càng hợp lý hoá hơn.

5. **Dịch vụ thanh toán điện tử (ePayment)**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) cung cấp dịch vụ thanh toán điện tử tập trung trên cơ sở định danh điện tử (eID) qua Hệ thống cung cung cấp dịch vụ định danh điện tử (EISDP). Với chức năng thanh toán điện tử (ePayment), các cơ quan đơn vị của chính phủ có thể chuyển tiền phúc lợi của các chương trình công như phúc lợi hưu trí xã hội, phúc lợi y tế, học bổng, v.v. cho các đối tượng thụ hưởng dự kiến. Mặc dù trọng tâm của báo cáo này là thanh toán giữa Chính phủ với Người dân, nếu dịch vụ thanh toán điện tử cũng được sử dụng cho cộng đồng doanh nghiệp và người dân, nó có thể sử dụng để hỗ trợ thanh toán Doanh nghiệp với Người dân, Người dân với Doanh nghiệp, và Người dân với Người dân.

Các khái niệm chính về Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Sau đây là một số khái niệm chính nhằm cung cấp liền mạch các dịch vụ định danh điện tử (eID).

1. **Cơ quan cung cấp dịch vụ nhận dạng tập trung của quốc gia**. Dự kiến, Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) do một cơ quan cung cấp dịch vụ nhận dạng quốc gia tập trung của chính phủ sở hữu, thiết kế và triển khai.

2. **Ứng dụng và cung cấp dịch vụ dựa trên định danh điện tử (eID).** Các ứng dụng cung cấp dịch vụ có thể sử dụng các chức năng định danh điện tử (eID) để nhận dạng và xác thực công dân được gọi chung là các "ứng dụng dựa trên nhận dạng điện tử". Việc sử dụng các ứng dụng dựa trên định danh điện tử có thể được gọi chung là "cung cấp dịch vụ dựa trên đinh danh điện tử".

3. **Quy trình tạo nhận dạng tập trung quốc gia tập**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) dựa trên một hệ thống tạo nhận dạng tập trung do một cơ quan cấp quốc gia của chính phủ vận hành. Quy trình tập trung để tạo nhận dạng nhằm đảm bảo tính duy nhất của định danh điện tử (eID). Do đó, các nhà cung cấp dịch vụ sử dụng Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) không cần phải tạo lập thêm một quy trình riêng để xác thực nhận dạng cho các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao. Điều này giúp tránh tình trạng các nhà cung cấp dịch vụ khác nhau tạo ra nhiều nhận dạng khác nhau cho cùng một công dân.

   Cơ chế này loại bỏ nhu cầu phải thực hiện các nỗ lực trùng lặp của các nhà cung cấp dịch vụ nhằm tạo lập nhận dạng, và về tổng thể dẫn đến giảm chi phí nhận dạng chung.

   Khuôn khổ này còn tận dụng được lợi thế của tiến bộ công nghệ nhằm tạo điều kiện cho các nhà cung cấp dịch vụ nâng cao chất lượng dịch vụ cho công dân và trao quyền để công dân có thể chứng minh nhận dạng của mình ở bất kỳ nơi đâu, vào bất kỳ thời điểm

nào, theo các phương thức khác nhau bằng định danh điện tử (eID) áp dụng chung và không thể bãi bỏ.

4. **Nhận dạng trở thành nhận dạng số hoá, có thể thẩm định trực tuyến và tương tác liên thông**. Quá trình số hoá và thông tin trực tuyến luôn được minh chứng về giá trị nâng cao khả năng tiếp cận, thuận tiện và minh bạch cho tất cả mọi người. Trong điều kiện Việt Nam có tỷ lệ tham gia internet cao[8] với cáp quang được lắp đặt tới tận cấp xã và kết nối không dây băng thông rộng ở cấp thôn với tỷ lệ thâm nhập thị trường di động trên 100%[9], hiện nay các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao đang ngày càng có nhu cầu về dịch vụ điện tử cả từ phía các cơ quan của chính phủ và của các tổ chức tư nhân. Dịch vụ điện tử đòi hỏi phải có định danh điện tử (eID) có thể xác nhận qua hình thức số và trực tuyến để có thể cung cấp dịch vụ. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) nhằm tận dụng tiến bộ về công nghệ bằng cách sử dụng định danh điện tử có thể xác nhận bằng hình thức số và trực tuyến đồng thời đảm bảo khả năng tương tác liên thông để chứng minh nhận dạng duy nhất cho công dân.

5. **Nhận dạng trên cơ sở Mã số định danh công dân của quốc gia (NIN), các thuộc tính nhân chủng học và sinh trắc học**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) sẽ tận dụng định danh điện tử (eID) được sử dụng qua quy trình tạo lập nhận dạng của Bộ Công An. Mã định danh điện tử (eID) duy nhất được xác định dựa trên các thuộc tính nhân chủng học (tên gọi, giới tính, độ tuổi, địa chỉ, v.v.) và sinh trắc học (vân tay, võng mạc) và cả Mã số định danh công dân (NIN) của một cá nhân do chính quyền trung ương cấp cho người đó. Nếu chỉ dữ liệu nhân chúng học thì chưa đủ để đảm bảo tính duy nhất; tuy nhiên, thông tin này sẽ được gắn kết với các thuộc tính sinh trắc học của cá nhân đó để tạo ra nhận dạng duy nhất nhằm tạo lập Mã số định danh công dân quốc gia (NIN).

6. **Mã số định danh công dân (NIN) toàn cục và không thể bác bỏ.** Mã số định danh công dân (NIN) nhằm nhận dạng công dân và trao cho họ phương tiện để xác lập nhận dạng của mình cho các đơn vị và tổ chức ở khu vực công và tư nhân tại quốc gia. Mã số định danh công dân (NIN) có ba đặc điểm chính:
   a. Tính không đổi: Là mã duy nhất trong suốt vòng đời của công dân.

---

[8] Báo cáo thống kê về internet tại Vietnam – http://www.thongkeinternet.vn/jsp/trangchu/index.jsp
[9] Thuê bao điện thoại di động – http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2012/Mobile_cellular_2000-2011.xls

b. Tính duy nhất: Mỗi công dân chỉ có một mã số nhận dạng, không có chuyện hai công dân trên cả nước sử dụng cùng một mã số nhận dạng.
c. Tính sử dụng phổ quát: Mã số nhân dạng có thể được đồng thời sử dụng cho các ứng dụng và môi trường khác nhau của các nhà cung cấp dịch vụ khác nhau trên cả nước.

7. **Tính duy nhất Mã số định danh công dân (NIN) được đảm bảo qua loại bỏ trùng lặp dữ liệu sinh trắc học**. Mã số định danh công dân (NIN) được Bộ Công An (MPS) cấp ra trong một quá trình tạo lập gọi là đăng ký, trong đó thông tin nhân chủng học và sinh trắc học của công dân được thu thập và tính duy nhất của dữ liệu cung cấp được xác lập qua một quy trình gọi là quy trình loại bỏ trùng lặp. Quy trình loại bỏ trùng lặp bao gồm chạy chương trình đối chiếu thông tin về nhân chủng học và sinh trắc học thu được qua đăng ký để so sánh 1:1 hai bộ dữ liệu nhằm đảm bảo độ chính xác lên đến 99,99% trước khi gán mã số nhận dạng duy nhất cho công dân. Sau khi loại bỏ trùng lặp, Mã số định danh công dân (NIN) có thể được cấp ra và chi tiết được gửi cho công dân qua đường thư tín.

   Định danh điện tử có thể xác nhận theo hình thức số và trực tuyến sẽ làm giảm nguy cơ mất trộm nhận dạng và loại bỏ các vấn đề về tài liệu giả mạo hoặc bị sao chép. Việc giả mạo tài liệu chứng minh nhận dạng trên giấy dễ hơn nhiều so với giả mạo nhận dạng số có thể được xác nhận trực tuyến.

   Định danh điện tử (eID) được cấp bằng Dữ liệu nhận dạng cá nhân (PID) dựa trên thông tin nhận chủng học và sinh trắc học đã được so sánh của một cá nhân tuân thủ theo chính sách quốc gia của chính phủ nhằm đảm bảo khả năng tương tác liên thông.

8. **Bằng chứng thông báo nhận dạng chuẩn hoá (token)**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) hỗ trợ các bằng chứng thông báo nhận dạng (token) chuẩn các loại khác nhau, tuỳ theo yêu cầu về chữ ký điện tử và xác thực nhận dạng của các nhà cung cấp dịch vụ hoặc các chương trình cụ thể của họ. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) hỗ trợ ba loại bằng chứng thông báo nhận dạng (token): Mã số nhận dạng cá nhân (PIN) hoặc "cái người sử dụng biết", mật khẩu dùng một lần (OTP)/ di động/ chứng nhận số, hoặc "cái người sử dụng có"; vân tay hoặc võng mạc, hoặc "người sử dụng là ai". Khái niệm bằng chứng thông báo nhận dạng (token) được mô tả chi tiết tại Phụ lục 1. Định danh điện tử (eID) của công dân được gán nhiều bằng chứng thông báo nhận dạng (token) khác nhau được sử dụng, cho phù hợp với các mục đích xác thực và chữ ký điện tử dựa trên nhu cầu nghiệp vụ của dịch vụ được cung cấp.

Những cân nhắc chung về an ninh và bảo mật. Các chức năng định danh điện tử (eID), theo dự kiến, sẽ được cung cấp trực tuyến hàng ngày tại các ứng dụng và các miền khác nhau. Một dịch vụ trực tuyến có thể phải chịu nhiều hình thức tấn công, bao gồm cả các cuộc tấn công quy mô lớn và có tổ chức. Điều đó có nghĩa là đảm bảo an ninh và bảo mật trong cung cấp dịch vụ điện tử là vấn đề quan trọng nhất. Thiết kế của định danh điện tử bao gồm cả biện pháp an ninh bảo mật ở các cập độ khác nhau nhằm đảm bảo khả năng bảo vệ ở mức độ cao nhất. Các vấn đề này được mô tả dưới đây.

Những cân nhắc về đảm bảo an ninh

1. **Đảm bảo an ninh về dữ liệu công dân thu được trong quá trình yêu cầu dịch vụ**. Hệ thống định danh điện tử (eID) phải đảm bảo an ninh cho gói dữ liệu nhận dạng cá nhân (PID block) thu được trong các ứng dụng và các thiết bị giao tiếp bằng các phương thức khác nhau.
    a. **Mã hoá và chống can thiệp.** Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) cần mã hoá dữ liệu tại thiết bị thu thập thông tin trước khi truyền dữ liệu đó trên mạng. Dữ liệu mã hoá không được lưu nếu không được xác thực thông tin trong bộ nhớ đệm trong một giai đoạn ngắn rồi được xoá đi sau khi truyền. Dữ liệu sinh trắc và mật khẩu dùng một lần (OTP) thu được cho mục đích xác thực không được lưu lại lâu dài trên cơ sở dữ liệu. Dịch vụ này cũng hỗ trợ Mã nhận thực bản tin dựa trên hàm Hash (HMAC) để đảm bảo gói dữ liệu nhận dạng cá nhân (PID block) không bị can thiệp trong quá trình di chuyển.
    b. **Hệ môi trường cung ứng dịch vụ tin cậy.** Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) sẽ có một cơ chế đăng ký và xác thực thiết bị đầu cuối, nhà điều hành và các bên tham gia khác để đảm bảo tạo ra một hệ môi trường cung ứng dịch vụ tin cậy. Ứng dụng cung cấp dịch vụ được ký chữ ký số trên thiết bị đầu cuối có thể được sử dụng để xác định ra các ứng dụng và thiết bị đáng tin cậy. Nhà điều hành cần được xác thực trong trường hợp các thiết bị được nhà điều hành hỗ trợ.
    c. **Yêu cầu và phản hồi cho các dịch vụ dựa trên ký nhận số**. Bên cạnh chuyện mã hoá dữ liệu, nhà cung cấp đã đăng ký phải ký nhận đối với yêu cầu dịch vụ và phản hồi về dịch vụ phải được ký nhận bởi cơ quan chủ quản của chính phủ để thiết lập ra cơ chế đảm bảo tin cậy và không thể chối bỏ giữa nhà cung cấp đó và cơ quan đó. Nguồn yêu cầu giao diện lập trình ứng dụng (hàm API) phải được xác thực tốt để đảm bảo các yêu cầu độc hại không được xử lý. Việc cơ quan chính phủ ký nhận số trên phản hồi nhằm đảm bảo tính trung thực của phản hồi và độ tin cậy và nhà cung cấp có thể tin tưởng thực tế là phản hồi đó thực chất là

phản hồi đúng thẩm quyền. Tính năng này cho phép các ứng dụng có thể xác nhận định danh điện tử (eID) trực tuyến hoàn toàn, qua đó tránh phải xử lý giấy từ và giảm chi phí về tổng thể.

d. **Dấu thời gian phản hồi.** Phản hồi dịch vụ định danh điện tử (eID) theo yêu cầu cần có dấu thời gian để cho phép các ứng dụng có thể xác nhận "khi nào" dịch vụ được cung cấp hoặc khi nào việc xác thực công dân được thực hiện. Các ứng dụng có thể sử dụng tính năng này cho các mục đích kiểm tra. Tính năng này có thể giúp ích trong việc sàng lọc theo khoảng thời gian khi một Mã số định danh công dân (NIN) cụ thể được cấp ra trong quá trình xác thực.

e. **Cơ chế chứng nhận và kiểm tra**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) sẽ tạo cơ chế để chứng nhận và kiểm tra các giao dịch và dữ liệu. Các phản hồi và siêu dữ liệu sẽ được lưu trữ phục vụ các mục đích kiểm tra trong một khoảng thời gian tối thiểu là sáu tháng. Các quy trình chứng nhận và kiểm tra chuẩn sẽ được thiết lập cho các thiết bị ứng dụng và các mạng tổng thể trong hệ môi trường. Mỗi yêu cầu dịch vụ sẽ tạo ra một mã phản hồi duy nhất để sử dụng cho các mục đích kiểm tra và giải quyết vấn đề. Mã này cũng nhằm phân biệt từng giao dịch trong hệ thống, tương tự như mã cấp quyền duy nhất cho từng giao dịch thẻ tín dụng.

f. **Phân tích gian lận.** Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) sẽ sử dụng phần mềm phân tích gian lận, là bộ công cụ phát hiện nhằm xác định những đòi hỏi đáng nghi ngờ ngay từ đầu.

g. **Phần mềm chống vi-rút.** Phần mềm chống vi-rút/phần mềm độc hại sẽ được cài đặt cùng với các biện pháp kiểm soát an ninh mạng và các chương trình xác thực điểm cuối khác.

2. **Đảm bảo an ninh cho mạng từ nguồn tới đích (End-to-end Network).** Việc cung cấp dịch vụ định danh điện tử (eID) sử dụng mạng được bảo vệ để truyền dữ liệu qua một kênh an toàn như giao thức lớp cổng bảo mật (SSL), đường truyền thuê bao bảo mật hoặc đường truyền riêng tương tự để bảo vệ chống tấn công qua mạng dẫn đến từ chối dịch vụ (DoS). Thiết kế dịch vụ cũng đảm bảo khả năng dự phòng và sẵn sàng ở mức cao trong trường hợp một số bộ phận của mạng bị tác động hoặc mất khả năng sử dụng. Các nhà cung cấp dịch vụ và đối tác của họ (các đại lý, các nhà cung cấp ứng dụng, v.v.) cần đảm bảo an ninh mạng ở mức phù hợp sao cho các hệ thống của họ được bảo vệ không bị tấn công.

3. **Đảm bảo an ninh cho các điểm cuối dịch vụ/ Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS).** Nếu Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) tập trung phải sử dụng mạng công cộng như mạng internet để giao tiếp với các đối tác, có khả năng nó sẽ bị tấn công bằng từ chối dịch vụ hoặc từ chối dịch vụ phân tán (DoS/DDoS). Vì nhiều ứng dụng trong nước sẽ phụ thuộc nhiều vào các tính năng như tính năng xác thực định danh điện tử (eID), điều quan trọng có tầm chiến lược là khuôn khổ này không bị tấn công qua các mạng công cộng bất kỳ như internet, và không được tạo ra "điểm duy nhất" bị tấn công có thể gây ảnh hưởng cho nhiều dịch vụ. Hiện có các biện pháp để bảo vệ dữ liệu định danh điện tử (eID) hoàn toàn không phải chịu các cuộc tấn công mạng trái phép trực tiếp từ hệ thống bên ngoài dẫn đến từ chối dịch vụ (DoS) và mất trộm dữ liệu. Các biện pháp này được giải thích dưới đây.
    a. **Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).** Dịch vụ của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) được duy trì trong vùng an toàn và chỉ bộc lộ ra ngoài qua các điểm cuối mạng. Thiết kế này bao gồm tạo ra các tổ chức được cấp quyền như Tổ chức cung cấp dịch vụ định danh điện tử (ISPA), và dịch vụ xác thực chỉ bị bộc lộ qua kết nối cá nhân bảo mật của họ qua các đường thuê bao. Đây là yêu cầu chiến lược nhằm đảm bảo luôn tồn tại nhiều điểm cuối để cungc ấp dịch vụ xác thực một cách an toàn, nhưng luôn luôn sẵn sàng.
    b. **Sử dụng mã giấy phép**. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) hỗ trợ thực hiện ý tưởng mã giấy phép tương tự như cấp phép sử dụng phần mềm: người sử dụng giấy phép được cấp một dãy các chữ số và/hoặc chữ cái. Điều này đảm bảo nhà cung cấp dịch vụ có thẩm quyền có thể truy cập vào dịch vụ xác thực. Nó cũng tạo cơ chế để thực thi hiệu lực sử dụng, hạn sử dụng tính năng cụ thể. Đồng thời nó cho phép các nhà cung cấp dịch vụ mở rộng dịch vụ giao diện lập trình ứng dụng (hàm API) cho các tổ chức đối tác và để đảm bảo tin cậy các yêu cầu của họ.

4. **Quản lý an ninh theo tiêu chuẩn.** Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) cũng triển khai quản lý an ninh theo các tiêu chuẩn, bao gồm các biện pháp như các cơ chế kiểm soát, các biện pháp kiểm soát an ninh tiềm năng, quản lý an ninh thông tin, quy trình Lập kế hoạch – Thực hiện – Kiểm tra – Hành động (PDCA), hệ thống quản lý an ninh thông tin (ISMS), đánh giá rủi ro và triển khai. Chức năng xác thực định danh điện tử (eID) sẽ hỗ trợ các tiêu chuẩn như ISO 27001[i] về quản lý an ninh thông tin, ISO 27002[ii] về các cơ chế kiểm soát và kiểm soát tiềm năng, ISO 27003[iii] về hướng dẫn sử dụng quy trình Lập kế hoạch – Thực hiện – Kiểm tra – Hành động (PDCA), ISO 27004[iv] về

hiệu quả triển khai Hệ thống quản lý an ninh thông tin (ISMS), và ISO 27005[v] về đánh giá rủi ro, ...

Những cân nhắc về bảo mật riêng tư

1. **Trả lời bằng "có/không".** Tính năng này chỉ được áp dụng trong xác thực. Việc xác thực định danh điện tử cho phép các ứng dụng "xác nhận" nhận dạng do công dân khai báo khi yêu cầu dịch vụ, đồng thời bảo mật riêng tư dữ liệu của người đó. Chức năng xác thực định danh điện tử (eID) chỉ trả lời bằng "có/không", chứ không phản hồi bằng thông tin về nhận dạng cá nhân. Đây là một trong những phương án chiến lược quan trọng để đảm bảo bảo mật riêng tư về dữ liệu công dân – nghĩa là không có cơ chế nào để "lấy" dữ liệu về một công dân qua Giao diện lập trình ứng dụng (hàm API) nhằm xác thực.

   Để minh hoạ, giả sử Giao diện lập trình ứng dụng (hàm API) xác thực bao gồm xử lý các câu hỏi và câu trả lời theo cách như sau: "công dân khai báo tên của mình là vân vân và hỏi có đúng không?" Quy trình xác thực định danh điện tử (eID) có thể trả lời bằng câu trả lời "có/không", nhưng nó không cho phép đặt các câu hỏi như "Địa chỉ của công dân có số chứng minh nhận dạng quốc gia như thế này là gì?"

2. **Tự xác nhận câu trả lời.** Câu trả lời yêu cầu xác thực định danh điện tử (eID) và nhận dạng và xác nhận khách hàng điện tử (eKYC) là phiên bản điện tử của hình thức xác nhận nhận dạng và chứng minh xác nhận. Nó cho phép tách bạch giữa việc sử dụng câu trả lời với yêu cầu dịch vụ thực tế tạo ra câu trả lời đó. Câu trả lời sẽ được sử dụng lâu dài sau khi được tạo ra và được sử dụng nhiều lần nếu cần. Thông lệ hiện nay trong xác nhận nhận dạng được thực hiện bằng cách thu thập các bản sao tài liệu "được chứng thực". Việc chứng thực cho phép hệ thống "tin tưởng" thực tế là bản sao đó thực chất được xác nhận theo bản gốc. Ở cấp độ cao hơn, câu trả lời xác thực định danh điện tử còn cho phép các đơn vị cung cấp dịch vụ được tự xác nhận như sau:
   - Việc xác thực này thực chất có được xác nhận bởi cơ quan chính phủ cấp ra định danh điện tử (eID) đó hay không? Chữ ký số sẽ cho phép thực hiện phép kiểm tra này. Điều này cũng giống như kiểm tra xem một cán bộ có thẩm quyền đã ký hay chưa.
   - Việc xác thực này có phải là xác thực cho một Mã số chứng minh nhận dạng quốc gia (NIN)?
   - Việc xác thực này có phải đã được thực hiện trong tháng "n" vừa qua? Câu trả lời có dấu thời gian cho phép biết điều này. Nếu biết được việc chứng minh bằng xác thực mới diễn ra gần đây cũng có ích.

- Cái gì đã được xác thực? “dấu vết sử dụng” trong “thông tin” cho phép kiểm tra điều này.
- Có phải tên gọi, ngày sinh, v.v. đã được xác nhận hay không?
- Thông tin sinh trắc học có được sử dụng hay không?
- Địa chỉ được xác nhận toàn bộ hay một phần?
- Địa chỉ được xác nhận khi xác thực có giống như địa chỉ hiện nay công dân đang cung cấp hay không? Giá trị hash của dữ liệu nhân chủng học sẽ được sử dụng để xác định riêng thông tin bí mật.
- Trong trường hợp hệ thống hưu trí, công dân hàng năm cần xác định thực tế là họ đang còn sống. Việc này hiện đang được thực hiện bằng cách công dân phải đến gặp cán bộ có thẩm quyền để ký vào một tờ tuyên bố. Qua sử dụng xác thực định danh điện tử (eID), một cơ quan có thể xác thực công dân một cách độc lập và cung cấp câu trả lời cho hệ thống hưu trí. Ứng dụng hưu trí có thể trả lời câu hỏi “Liệu một người có Mã số định danh công dân (NIN) như thế đã được xác thực bằng sinh trắc trong sáu tháng qua hay chưa?” bằng cách xác nhận trả lời bằng ngôn ngữ đánh dấu mở (XML). Qua đó ta biết được người đó còn sống hay không.
- Câu trả lời xác thực định danh điện tử (eID) cũng tương tự như tài liệu giấy hiện nay được sử dụng với câu “gửi các bên có liên quan” do một cán bộ có thẩm quyền ký vào một ngày cụ thể với nội dung là “xác nhận người có Mã số định danh công dân (NIN) như thế có tên gọi và địa chỉ như sau”.
- Câu trả lời định danh điện tử (eID) có thể được đơn giản coi là một phiên bản điện tử của hồ sơ giấy và có thể được tin cậy và tự xác nhận bởi một ứng dụng của bên thứ ba.

3. **Yêu cầu dịch vụ không đồng bộ qua mã giao dịch.** Định danh điện tử (eID) có thể do các ứng dụng của nhà cung cấp dịch vụ yêu cầu dưới trạng thái không đồng bộ, nghĩa là việc truyền dữ liệu bị chập chờn chứ không theo luồng ổn định. Các nhà cung cấp dịch vụ sẽ sử dụng mã giao dịch để gán mã nhận dạng giao dịch nghiệp vụ lô-gic, trong khi tích hợp các dịch vụ định danh điện tử (eID). Tính năng này cho phép chương trình yêu cầu/trả lời được đồng bộ hoặc không đồng bộ mà không phải lo lắng về cách gắn yêu cầu với phản hồi cụ thể cho yêu cầu đó. Bất kỳ khi nào có sự tích hợp giữa hai hệ thống độc lập, điều quan trọng là mỗi giao dịch phải có một “mã số nhận dạng” chung để thể hiện mối quan hệ giữa yêu cầu và phản hồi; đồng thời để tạo bút tích kiểm tra về sau. Ví dụ, khi thực hiện một giao dịch thanh toán, ngân hàng sẽ phải theo dõi giao dịch đó

theo suốt luồng giao dịch. Phản hồi dịch vụ cũng chứa cùng mã giao dịch trong yêu cầu dịch vụ nhằm cho phép các ứng dụng gắn kết được phản hồi với một yêu cầu cụ thể.

4. **Dịch vụ nhớ đệm.** Hệ thống định danh điện tử (eID) còn hỗ trợ "dịch vụ nhớ đệm", trong đó dữ liệu nhận dạng cá nhân (PID) của nhiều người có định danh điện tử (eID) được thu thập và được chứa tại vùng đệm trong thiết bị yêu cầu dịch vụ để truyền đi sau đó. Quy trình dịch vụ nhớ đệm do vậy hơi khác một chút so với trường hợp thông thường cho đến khi yêu cầu dịch vụ được truyền đi từ thiết bị yêu cầu dịch vụ. Từ lúc này, mô hình và quy trình lại tương tự như kịch bản thông thường: tập hợp yêu cầu dịch vụ nhớ đệm được kiểm tra, việc thẩm định cấu trúc dữ liệu được thực hiện và được chuyển sang máy chủ xử lý yêu cầu dịch vụ. Sau khi nhận được kết quả dịch vụ cho mỗi yêu cầu, ứng dụng cung cấp dịch vụ sẽ chuyển lại kết quả vào cùng thiết bị yêu cầu dịch vụ đã gửi đi yêu cầu đó. Mặc dù thiết bị yêu cầu dịch vụ có thể truyền nhiều yêu cầu cùng lúc, nhưng mỗi yêu cầu sẽ được xử lý như một giao dịch riêng trong máy chủ và mỗi yêu cầu sẽ có một mã xác thực riêng. Trách nhiệm của nhà cung cấp dịch vụ là phải đảm bảo các thiết bị yêu cầu dịch vụ được sử dụng có khả năng quản lý dịch vụ nhớ đệm (bao gồm cả khả năng lưu trữ nhiều yêu cầu, chuyển các yêu cầu đó vào cùng thời điểm, nhận và lưu trữ kết quả của nhiều yêu cầu). Cần có một hạn mức trần về khoảng thời gian các yêu cầu được nhớ đệm. Khoảng thời gian này có thể được xác định qua các yêu cầu kỹ thuật mà cơ quan chủ quản của chính phủ đề ra. Vì dịch vụ nhớ đệm chỉ được cung cấp để hỗ trợ các vấn đề thường gặp về khả năng kết nối tại cơ sở, việc nhớ đệm các yêu cầu chỉ được thực hiện đối với các thiết bị yêu cầu dịch vụ, chứ không thực hiện trên máy chủ của các nhà cung cấp dịch vụ.

Phương thức sử dụng dịch vụ nhận dạng phổ biến. Các nhà cung cấp dịch vụ có thể sử dụng hệ thống định danh điện tử (eID) của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) theo ba cách chính như sau:

1. **Xác định thông tin nhận dạng và xác nhận khách hàng (KYC)**
    a. **Nhận dạng và xác nhận khách hàng (KYC) cho các dịch vụ khác nhau.** Việc xác nhận nhận dạng và địa chỉ khách hàng là yêu cầu quan trọng đối với các nhà cung cấp dịch vụ để đăng ký một khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao mới hoặc mở tài khoản mới cho một cá nhân. Ví dụ bao gồm cấp mã số thuế mới, kết nối điện thoại, mở tài khoản ngân hàng hoặc tài khoản dịch vụ internet cho doanh nghiệp trực tuyến. Nhà cung cấp dịch vụ trong trường hợp đó cần có khả năng xác nhận nhận dạng và địa chỉ của người đăng ký bằng cách sử dụng xác thực định danh điện tử (eID). Phương thức này dự kiến sẽ làm giảm

đáng kể chi phí cho quy trình nhận dạng và xác nhận khách hàng (KYC) cho các nhà cung cấp dịch vụ.

b. **Chứng minh chung về nhận dạng.** Chứng minh nhận dạng (PoI) là một yêu cầu chuẩn liên quan đến an ninh, ví dụ để vào sân bay, để đủ tư cách dự thi hoặc kiểm tra sức khoẻ tại trường học hoặc bệnh viện, vì có rất nhiều trường hợp giả mạo được báo cáo hàng năm. Các trang web thương mại điện tử, mạng xã hội, internet cũng đòi hỏi phải xác thực định danh điện tử nhằm xác nhận khách hàng và người đăng ký thuê bao mỗi khi cần xác nhận nhận dạng thực của người tham gia giao dịch.

c. **Xác nhận địa chỉ và dữ liệu nhận chủng học.** Dữ liệu nhân chủng học của khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao tại cơ sở dữ liệu của các nhà cung cấp dịch vụ cũng được xác nhận; quy trình này giúp quản lý và làm sạch cơ sở dữ liệu để loại bỏ nhận dạng trùng lặp và nhận dạng ảo.

2. **Xác định sự tồn tại và bằng chứng cung cấp**

   a. **Xác nhận nhận dạng của đối tượng thụ hưởng**. Rất nhiều chương trình trong các lĩnh vực xã hội yêu cầu phải xác nhận nhận dạng của đối tượng thụ hưởng trước khi cung cấp dịch vụ, dự kiến đó sẽ là các tổ chức sử dụng nhiều dịch vụ xác thực định danh điện tử (eID). Ví dụ về sử dụng bao gồm, cung cấp thức ăn và dầu hoả để trợ cấp cho các đối tượng dưới ngưỡng nghèo, cung cấp dịch vụ y tế cho các đối tượng hưởng bảo hiểm y tế, đăng ký đơn xin việc của các đối tượng, ... Việc xác nhận nhận dạng nhằm đảm bảo dịch vụ được cung cáp cho đúng đối tượng.

   b. **Điểm danh.** Một mục đích nữa của việc xác thực định danh điện tử (eID) là xác định sự hiện diện của đối tượng của chương trình tại một địa điểm để điểm danh đối tượng đó. Ví dụ, điểm danh học sinh và giáo viên trong các hoạt động giáo dục, điểm danh người lao động cho các chương trình liên quan đến việc làm, trong đó các khoản chi được thực hiện theo số ngày làm việc thực tế mà đối tượng báo cáo cho chương trình.

   c. **Giao dịch tài chính.** Các ngân hàng cần xác thực khách hàng của mình bằng định danh điện tử (eID) và các thông tin nhận dạng liên quan đến ngân hàng khác (số tài khoản, chứng minh thư, mật khẩu/mật khẩu sử dụng một lần (OPT)) trước khi cho phép giao dịch tài chính như chuyển tiền và rút tiền diễn ra.

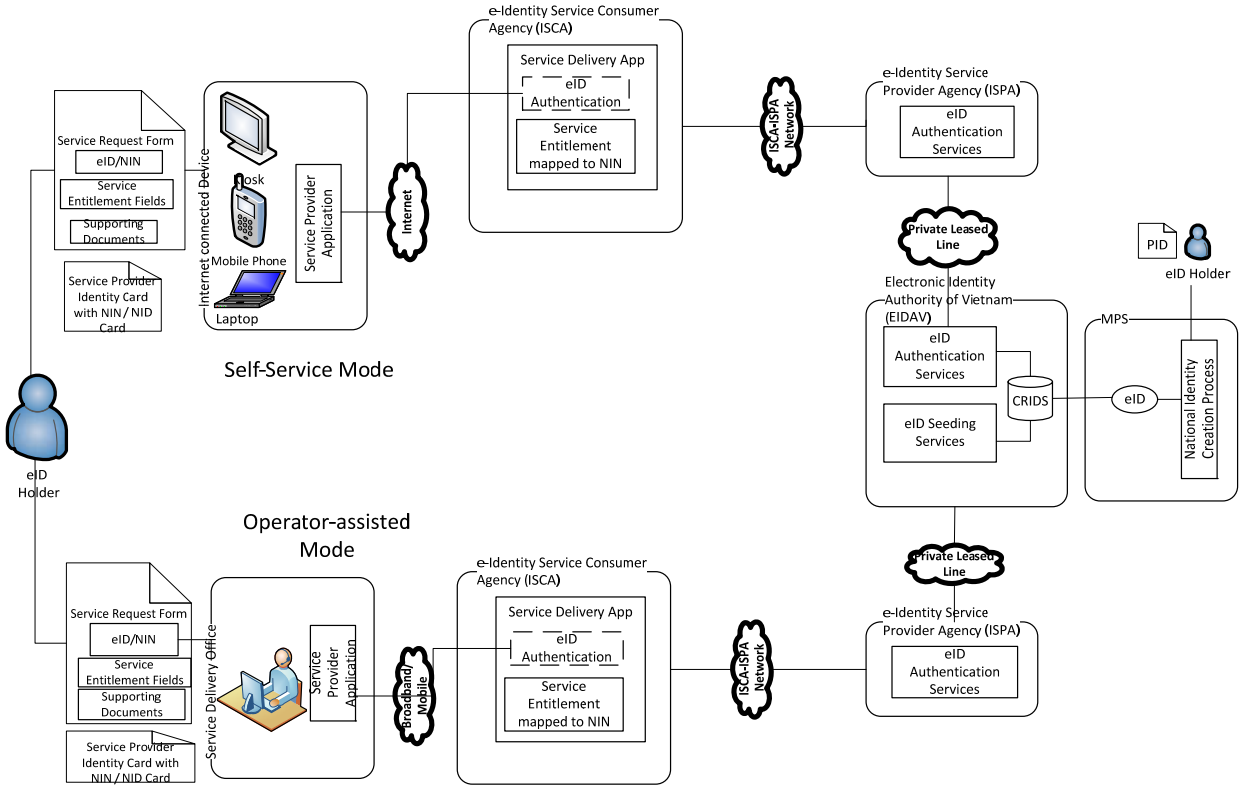
3. **Thống nhất thông tin xoay quanh công dân.** Mã số định danh công dân (NIN) được sử dụng là mã số nhận dạng chung để liên kết các cơ sở dữ liệu liên quan. Ứng dụng liên kết các cơ sở dữ liệu đó nhằm:

a. Tạo thông tin theo góc nhìn 360 độ về công dân đó qua các chương trình phúc lợi xã hội, như các chương trình hỗ trợ cho vay để học tập, các chương trình y tế trợ cấp cho trẻ sơ sinh, phụ nữ có thai, hưu bổng của người cao tuổi, v.v. Góc nhìn như thế cần có để cải thiện hiệu quả các chương trình của chính phủ và đảm bảo lợi ích đến được đúng đối tượng.
b. Cơ sở dữ liệu về hồ sơ bệnh nhân và chăm sóc y tế/ y bạ ở cấp cơ sở, khu vực và quốc gia.
c. Phòng thông tin đánh giá uy tín tín dụng của khách hàng.
d. Cơ sở dữ liệu quốc gia về kỹ năng và việc làm, để theo dõi các cá nhân trong suốt vòng đời.
e. Các tổ chức lớn như ngân hàng, công ty bảo hiểm cần triển khai thông tin duy nhất về khách hàng cho tất cả các dịch vụ.

5.2 Mô tả chi tiết về các dịch vụ nhận dạng điện tử

Phần dưới đây mô tả về các dịch vụ định danh điện tử (eID) các tính năng cụ thể của các dịch vụ đó.

5.2.1 Dịch vụ xác thực nhận dạng điện tử



Hình 5.2: Hình ảnh chức năng của khuôn khổ cung cấp dịch vụ nhận dạng điện tử

Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) nhằm xác thực định danh điện tử trên một nền tảng trực tuyến sẵn có, an toàn và có thể mở rộng trên toàn quốc để xác nhận nhận dạng của công dân. Mã số định danh công dân (NIN) và hồ sơ định danh điện tử của công dân có thể được xác nhận trực tuyến qua các thuộc tính nhân chủng học, sinh trắc học qua các mạng băng thông rộng, mạng cáp, mạng di động.

Dịch vụ xác thực định danh điện tử (eID) được người có định danh điện tử (eID) sử dụng để chứng minh nhận dạng của mình bằng hình thức số và trực tuyến, đồng thời các nhà cung cấp dịch vụ ở cả khu vực công và tư nhân có thể khẳng định những khai báo nhận dạng của công dân nhằm cung cấp dịch vụ và cho phép khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao được tiếp cận lợi ích. Các nhà cung cấp dịch vụ có khả năng xác thực định danh điện tử (eID) cho các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao theo các hình thức khác nhau theo cả phương thức tự phục vụ qua các thiết bị di động, hoặc ki-ốt hoặc các thiết bị kết nối internet hoặc theo phương thức được nhà điều hành hỗ trợ qua các thiết bị đầu cuối máy thanh toán tiền bằng thẻ (máy PoS) tại địa chỉ lựa chọn như được mô tả tại Hình 5.2. Các kịch bản hỗ trợ được mô tả chi tiết tại Phụ lục 1.

Việc xác thực định danh điện tử (eID) dựa trên nhu cầu tiên quyết là công dân phải đảm bảo có nhận dạng duy nhất qua Mã số định danh công dân (NIN) cấp cho người đó. Dịch vụ này sẽ sử dụng Mã số định danh công dân (NIN) và Mã số nhận dạng cá nhân (PIN) của người có mã số định danh điện tử (eID) làm đầu vào để qua đó thẩm định sự chính xác của dữ liệu trên cơ sở đối chiếu so sánh. Dịch vụ này sẽ gửi câu trả lời "có/không" để khẳng định về chứng minh nhận dạng hoặc xác nhận thông tin do công dân cung cấp.

Các loại dịch vụ xác thực nhận dạng điện tử. Vì nhận đạng diện tử (eID) nhằm trao quyền cho công dân để có thể chứng minh nhận dạng của họ vào bất kỳ lúc nào, ở bất kỳ nơi đâu và theo nhiều phương thức khác nhau, dịch vụ xác thực đề xuất cần hỗ trợ nhiều cách thức xác thực.

Hỗ trợ xác thực đơn yếu tố và đa yếu tố. Hệ thống định danh điện tử (eID) cần hỗ trợ xác thực đơn yếu tố và đa yếu tố. Bản thân Mã số định danh công dân (NIN) không phải là yếu tố để xác thực. Mọi loại hình xác thực đòi hỏi phải có Mã số định danh công dân (NIN) đối với mọi yêu cầu để có thể đối chiếu 1:1 cho mỗi giao dịch. Mã số định danh công dân (NIN) được sử dụng cùng với các thuộc tính nhân chủng học hoặc đơn/đa thông tin sinh trắc học nhằm xác thực một yếu tố, và những thuộc tính đó có thể được sử dụng kết hợp với nhau nhằm xác thực đa yếu tố để đảm bảo nhu cầu xác thực theo yêu cầu.

Phân loại dịch vụ xác thực định danh điện tử (eID) trên cơ sở loại thuộc tính xác thực. Các loại thuộc tính xác thực được phân loại trên cơ sở các thuộc tính được sử dụng để hỗ trợ cho các dịch vụ xác thực sau của nhà cung cấp dịch vụ tuỳ thuộc vào nhu cầu nghiệp vụ của họ:

Loại 1: Xác thực nhân chủng học nghĩa là sử dụng một/kết hợp nhiều thuộc tính nhân chủng học như tên gọi, địa chỉ, ngày sinh, giới tính, số điện thoại di động và địa chỉ email. Thông tin này được sử dụng định kỳ để kiểm tra tính hợp lệ của các chứng nhận hoặc để làm sạch cơ sở dữ liệu của nhà cung cấp dịch vụ bằng cách loại bỏ trùng lặp. Các nhà cung cấp dịch vụ cũng có thể sử dụng loại hình xác thực nhân chủng học này để xác định khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao trước khi thực hiện mỗi giao dịch.

Loại 2: Xác thực bằng mật khẩu dùng một lần (OTP) nghĩa là sử dụng mất khẩu dùng một lần. Mật khẩu này sẽ được gửi vào điện thoại di động hoặc thư điện tử (email) theo yêu cầu của công dân hoặc của một ứng dụng. Mật khẩu đó được sử dụng để xác thực công dân cho các giao dịch trên internet hoặc di động cũng như trong các trường hợp việc triển khai công nghệ sinh trắc gặp khó khăn hoặc không thực tiễn. Tính năng xác thực bằng mật khẩu dùng một lần (OTP) cho phép tăng cường xác thực bằng cách chứng nhận việc sở hữu điện thoại di động đó của công dân. Xác thực định danh điện tử (eID) được hỗ trợ bởi thông tin sinh trắc và/hoặc mật khẩu dùng một lần (OTP). Thông tin sinh trắc cung cấp ra một yếu tố (bạn là ai), còn mật khẩu dùng một lần (OTP) cung cấp thêm một yếu tố bổ sung (bạn có cái gì). Ứng dụng của các nhà cung cấp dịch vụ thường sử dụng mật khẩu dùng một lần (OTP) làm yếu tố (bạn có cái gì) để xác thực đơn yếu tố, hoặc kết hợp với thông tin sinh trắc là yếu tố (bạn là ai) để xác thực hai yếu tố. Tóm lại, yêu cầu xác thực bằng mật khẩu dùng một lần (OTP) cần được khởi xướng qua các cổng dịch vụ tin nhắn ngắn (SMS)/ dữ liệu dịch vụ bổ sung phi cấu trúc (USSD); hoặc khởi xướng bởi ứng dụng của nhà cung cấp dịch vụ thay mặt cho công dân qua giao diện lập trình ứng dụng (hàm API) bằng mật khẩu sử dụng một lần. Cần lưu ý rằng thông tin xác thực mật khẩu dùng một lần (OTP) luôn được gửi vào điện thoại di động hoặc thư điện tử của công dân, và ứng dụng này dự kiến sẽ thu thập thông tin đó trong quá trình xác thực sao cho mật khẩu dùng một lần sẽ được xác nhận trong quá trình xác thực.

Loại 3: xác thực chứng nhận số hoặc sinh trắc là sử dụng chữ ký số do cơ quan có thẩm quyền tại Việt Nam cấp cho người có định danh điện tử (eID). Nhà cung cấp dịch vụ sẽ cấp ra một thẻ thông minh, trên có có chứng nhận số/sinh trắc hoặc sử dụng nhận dạng di động để xác thực công dân. Thẻ này được sử dụng để xác thực công dân trên các giao dịch di động hoặc trên internet và trong các trường hợp khắp khó khăn trong việc

sử dụng công nghệ sinh trắc và kịch bản nghiệp vụ đòi hỏi phải đảm bảo an ninh bảo mật ở mức cao.

Loại 4: Xác thực sinh trắc là sử dụng vân tay và/hoặc hình ảnh võng mạc. Nó đòi hỏi công dân phải có mặt để lấy dấu vân tay/ hình ảnh võng mạc vào thiết bị. Xác thực sinh trắc cần sử dụng trong các kịch bản như nhận dạng và xác nhận khách hàng (KYC), các giao dịch tài chính, điểm danh. Tính năng đối chiếu dữ liệu sinh trắc hỗ trợ đối chiếu vân tay đơn lẻ hoặc kết hợp nhiều yếu tố như sử dụng phân giải chi tiết vân tay (FMR) hoặc phân giải hình ảnh vân tay (FIR) và đối chiếu võng mạc bằng phân giản hình ảnh võng mạc (IIR).

Loại 5: Xác thực đa yếu tố là sử dụng vân tay và/hoặc võng mạc và/hoặc chứng nhận số/sinh trắc và/hoặc mật khẩu dùng một lần/ di động. Xác thực theo cách này cần áp dụng trong các trường hợp cần có sự đảm bảo lớn hơn.

Phân loại xác thực định danh điện tử dựa trên nhu cầu về mức độ đảm bảo. Các nhà cung cấp dịch vụ cần lựa chọn loại hình xác thực như xác thực đơn yếu tố hoặc đa yếu tố dựa trên mức độ đảm bảo về khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao theo yêu cầu của nhà cung cấp dịch vụ. Các tiêu chí lựa chọn phụ thuộc vào các yếu tố rủi ro, tác động, chi phí triển khai và khối lượng công việc xác thực. Các nội dung này được mô tả chi tiết tại Phụ lục 1.

Khả năng đảm bảo xác thực tăng lên với các thuộc tính sinh trắc học. Xác thực nhân chủng học (Loại 1) dựa trên các thuộc tính nhân chủng học và không đảm bảo "chứng minh sự hiện diện"; do đó phương thức này có mức độ đảm bảo thấp so với xác thực dựa trên các thuộc tính sinh trắc học, chứng nhận số và mật khẩu dùng một lần (OTP). Xác thực bằng mật khẩu dùng một lần (OTP) (loại hai) hoặc xác thực bằng chứng nhận số (loại ba) dựa trên thuộc tính mật khẩu dùng một lần (OTP) hoặc chứng nhận số, còn Mã số nhận dạng cá nhân (PIN) đảm bảo "chứng minh sự hiện diện" của điện thoại di động/ thư điện tử (email) do công dân đăng lý hoặc sự tồn tại của chứng nhận số và Mã số nhận dạng cá nhân (PIN). Quy trình này có mức độ đảm bảo cao hơn so với xác thực bằng thông tin nhân chủng học. Tuy nhiên, vì di động/ thư điện tử (email) hoặc chứng nhận và Mã số nhận dạng cá nhân (PIN) trên thẻ thông minh hoặc điện thoại di động có thể được dùng chung với người nhà hoặc bạn bè, nó không đảm bảo khả năng "chứng minh sự hiện diện" và do đó có mức độ đảm bảo thấp hơn so với xác thực dựa trên các thuộc tính sinh trắc học. Xác thực nhận trắc học cho thấy có sự hiện diện của cá nhân đó; do vậy, đây là mức độ đảm bảo cao nhất. Mức độ đảm bảo có thể còn cao hơn nếu sử dụng cả các phương thức sinh trắc khác nhau như vân tay và mồng mặt trong quy trình này.

Hỗ trợ mô hình xác thực mở rộng. Hầu hết các hệ thống xác thực hiện nay của các nhà cung cấp dịch vụ ở Việt Nam có lẽ đều được coi là "cục bộ" (nghĩa là chỉ được tạo lập, quản lý và/hoặc có giá trị cho một số dịch vụ, một số tình huống hoặc một số đơn vị) và "có thể bãi bỏ" (trong đó một yếu tố nhận dạng hiện tại có thể bị bãi bỏ và cấp phát lại do hết hạn, bị mất tác dụng hoặc các lý do hợp lệ khác). Các hệ thống xác thực cục bộ và có thể bãi bỏ như vậy có những điểm mạnh và hạn chế riêng. Mặt khác, Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể được coi là hệ thống "toàn cục" (vì nó được hình thành và quản lý bởi một cơ quan duy nhất của quốc gia và được áp dụng cho mọi tình huống, dịch vụ và nhà cung cấp dịch vụ) và không thể bãi bỏ (vì các yếu tố định danh điện tử (eID) như vân tay và võng mạc thường không bị bãi bỏ hoặc thay thế. Các hệ thống xác thực vĩnh viễn/không thể huỷ bỏ và toàn cục cũng có những điểm mạnh và hạn chế riêng.

Trong mô hình xác thực mở rộng, dịch vụ xác thực định danh điện tử (eID) toàn cục/không thể bãi bỏ cùng tồn tại và tăng cường cho dịch vụ xác thực cục bộ/ có thể bãi bỏ. Dự kiến, phương thức mở rộng sẽ hình thành nên các hệ thống xác thực mạnh hơn và đáng tin cậy hơn là chỉ dựa vào mô hình toàn cục/ không thể bãi bỏ hoặc mô hình cục bộ/ có thể bãi bỏ.

Do vậy, Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) được thiết kế trên quan điểm nhằm tăng cường các hệ thống xác thực hiện hành của các nhà cung cấp dịch vụ chứ không phải thay thế chúng. Mặc dù mô hình mở rộng không buộc các nhà cung cấp dịch vụ phải có sẵn hoặc đang sử dụng dịch vụ xác thực riêng của họ (nếu nhà cung cấp dịch vụ muốn, họ có thể chỉ cần sử dụng riêng Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF)), tuy nhiên, các nhà cung cấp dịch vụ được khuyến khích sử dụng Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) phối hợp với các hệ thống cục bộ của họ để tạo ra một hệ thống mạnh hơn và đáng tin cậy hơn.

Dịch vụ xác thực đề xuất trong trường hợp xác thực đa yếu tố sẽ hỗ trợ cho mô hình xác thực mở rộng, trong đó các nhà cung cấp dịch vụ có thể sử dụng cả hai yếu tố của hệ thống định danh điện tử (eID) đề xuất hoặc một yếu tố của hệ thống định danh điện tử (eID) đề xuất cộng với yếu tố thứ hai từ một nguồn khác kể cả là nguồn của nhà cung cấp dịch vụ đó. Chẳng hạn, một ngân hàng có thể lựa chọn kết hợp thông tin sinh trắc học và mật khẩu dùng một lần (OTP) làm các yếu tố xác thực của hệ thống định danh điện tử (eID) đề xuất, còn một ngân hàng khác lại chọn cách xác thực sinh trắc học từ hệ thống đề xuất phối hợp với thẻ rút tiền tự động (ATM)/ mật khẩu sử dụng một lần (OTP) do ngân hàng đó phát hành.

5.2.2 Dịch vụ nhận dạng và xác nhận khách hàng điện tử

Một trong những nền tảng căn bản để cung cấp dịch vụ là quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC); nhằm xác định nhận dạng của công dân cùng với địa chỉ và các

thông tin cơ bản khác như ngày sinh, giới tính. Thông thường, thông tin nhận dạng và xác nhận khách hàng (KYC) này được sử dụng kết hợp với các thông tin khác để xác định điều kiện thụ hưởng – học bổng, vốn vay, lương hưu an sinh xã hội, kết nối di động, v.v.

Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) cung cấp dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) tập trung qua Hệ thống cung cấp dịch vụ định danh điện tử (EISDP); qua đó quy trình nhận dạng và xác nhận khách hàng (KYC) có thể được thực hiện điện tử với sự đồng ý rõ ràng từ phía công dân. Dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) trên cơ sở định danh điện tử (eID) sẽ cung cấp bằng chứng nhận dạng (PoI) và bằng chứng địa chỉ (PoA) điện tử, tức thời, và không thể bác bỏ cùng với ngày sinh và giới tính. Ngoài ra, dịch vụ đó còn cung cấp số điện thoại và địa chỉ thư điện tử của công dân, nhằm hợp lý hoá quy trình hơn nữa.

Các nhà cung cấp dịch vụ sử dụng chức năng nhận dạng và xác nhận khách hàng điện tử (eKYC) chủ yếu để thực hiện quy trình nhận dạng và xác nhận khách hàng (KYC) khi đăng ký khách hàng mới hoặc đối tượng thụ hưởng mới, hoặc kết nối hồ sơ về công dân lưu trữ trên cơ sở dữ liệu của mình với cơ sở dữ liệu Mã số chứng minh nhận dạng quốc gia (NIN)/ định danh điện tử (eID). Dịch vụ chỉ được truy suất qua các nhà cung cấp dịch vụ được cấp quyền sử dụng mạng an toàn của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA). Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) sẽ tạo cơ chế để đăng ký các nhà sử dụng dịch vụ để họ có thể sử dụng chức năng nhận dạng và xác nhận khách hàng điện tử (eKYC).

Quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC) được thực hiện tại địa điểm của một đại lý qua xác thực sinh trắc hoặc từ xa bằng mật khẩu dùng một lần (OTP) hoặc kết nối qua điện thoại di động hoặc trang web. Trong quy trình nhận dạng và xác nhận khách hàng điện tử (eKYC), công cần cần cho phép cơ quan chủ quản của chính phủ – được sử dụng thông tin sinh trắc học/chứng nhận số/ mật khẩu dùng một lần (OTP) qua xác thực định danh điện tử – để gửi dữ liệu nhân chủng học của họ cùng với ảnh của họ, được ký chữ ký số và mã hoá, cho các nhà cung cấp dịch vụ.

Cơ quan chủ quản của chính phủ sẽ công khai các yêu cầu kỹ thuật về giao diện lập trình ứng dụng (hàm API) nhằm nhận dạng và xác nhận khách hàng điện tử (eKYC) trên cổng thông tin công cộng của họ. Nhà cung cấp dịch vụ được uỷ quyền sẽ sử dụng chức năng nhận dạng và xác nhận khách hàng điện tử (eKYC) bằng ứng dụng ngoài vi về nhận dạng và xác nhận khách hàng điện tử (eKYC). Ứng dụng này sẽ thu thập Mã số định danh công dân (NIN) cùng với thông tin sinh trắc học/ chứng nhận số/ mật khẩu dùng một lần (OTP) của công dân để hình thành nên ngôn ngữ đánh dấu mở (XML) về nhận dạng và xác nhận khách hàng điện tử (eKYC) bằng cách gói các gói Dữ liệu nhận dạng cá nhân (PID) mã hoá ngôn ngữ đánh dấu mở (XLM), dán chữ ký

số và gửi vào hệ thống nhận dạng và xác nhận khách hàng điện tử (eKYC) qua một mạng tư nhân bảo mật của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA). Hệ thống nhận dạng và xác nhận khách hàng điện tử (eKYC) qua đó sẽ xác thực công dân. Nếu việc xác thực thành công, hệ thống sẽ phản hồi bằng hình ảnh và dữ liệu nhân chủng học đã được mã hoá, có chữ ký số theo định dạng ngôn ngữ đánh dấu khả mở (SML). Ảnh và dữ liệu trong phản hồi được mã hoá bằng mã mở khoá công khai của nhà cung cấp dịch vụ.

Dưới đây là một số đặc điểm của dịch vụ:

1. **Không sử dụng giấy.** Dịch vụ này hoàn toàn là dịch vụ điện tử, loại bỏ nhu cầu quản lý tài liệu.

2. **Dựa trên nội dung**. Dữ liệu nhận dạng và xác nhận khách hàng (KYC) chỉ được cung cấp với sự cho phép của công dân đó qua xác thực định danh điện tử (eID), qua đó bảo vệ được thông tin riêng tư của công dân.

3. **Loại bỏ được tình trạng giả mạo tài liệu**. Việc loại bỏ bản sao các tài liệu khác nhau hiện đang lưu trữ tại cơ sở của các nhà cung cấp dịch vụ khác nhau loại bỏ được rủi ro gian lận nhận dạng và bảo vệ được nhận dạng của công dân. Ngoài ra, vì dữ liệu nhận dạng và xác nhận khách hàng điện tử (eKYC) do cơ quan chủ quản của chính phủ cung cấp trực tiếp nên không có rủi ro về giấy tờ giả mạo.

4. **Tính chất không thể chối bỏ.** Việc sử dụng xác thực công dân để cho phép, việc nhà cung cấp dịch vụ gán chữ ký số theo yêu cầu nhận dạng và xác nhận khách hàng điện tử (eKYC), và việc gán chữ ký số của cơ quan chủ sở hữu của chính phủ khi cung cấp nhận dạng và xác nhận khách hàng điện tử (eKYC) khiến cho toàn bộ giao dịch không thể bị các bên liên quan chối bỏ.

5. **Chi phí thấp.** Việc loại bỏ xác nhận trên giấy, di chuyển và lưu trữ giấy tờ có thể làm giải chi phí của quy trình nhận dạng và xác nhận khách hàng (KYC) chỉ bằng một phần so với chi phí ngày nay.

6. **Tính chất tức thời.** Dịch vụ sẽ được tự động hoá hoàn toàn, và dữ liệu nhận dạng và xác nhận khách hàng (KYC) sẽ được cung cấp theo thời gian thực mà không có bất kỳ can thiệp thủ công nào.

7. **Tính chất có thể đọc trên máy**. Dữ liệu nhận dạng và xác nhận khách hàng (KYC) điện tử có chữ ký số do cơ quan chủ sở hữu của chính phủ cung cấp có thể đọc được trên máy, để nhà cung cấp dịch vụ có thể lưu trữ trực tiếp dữ liệu đó dưới dạng hồ sơ khách hàng trên cơ sở dữ liệu của mình, phục vụ mục đích cung cấp dịch vụ, kiểm tra, ... mà không có sự can thiệp của con người, qua đó giảm chi phí và sai sót trong quy trình.

8. **Tính chất an toàn và tuân thủ với chính sách CNTT.** Cả hai điểm cuối chuyển giao dữ liệu đều được bảo mật qua sử dụng chữ ký số và mã hoá tuân theo chính sách bảo mật CNTT quốc gia, qua đó tài liệu nhận dạng và xác nhận khách hàng điện tử (eKYC) có tính chất pháp lý tương đương với tài liệu giấy. Ngoài ra, việc sử dụng chữ ký số và mã hoá nhằm đảm bảo trong quá trình đó, các bên không có thẩm quyền không thể can thiệp hoặc lấy trộm dữ liệu.

5.2.3 Dịch vụ tạo nguồn thông tin nhận dạng điện tử

Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) nhằm cung cấp dịch vụ tạo nguồn thông tin nhận dạng điện tử, là một quy trình nhằm đưa Mã số định danh công dân (NIN) của một công dân vào cơ sở dữ liệu của các nhà cung cấp dịch vụ để có thể xác thực nhận dạng điện tử. Quy trình này cho phép nhà cung cấp dịch vụ được đối chiếu hồ sơ về khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao với Mã số chứng minh nhận dạng quốc gia (NIN). Mục tiêu không phải để thay thế mã số nhận dạng duy nhất mà hiện nay các nhà cung cấp dịch vụ đang sử dụng mà để cho phép xác thực định danh điện tử liền mạch bằng Mã số định danh công dân (NIN) mà không gây ảnh hưởng gì đến bất kỳ giao diện nào khác mà nhà cung cấp dịch vụ đang duy trì cho khách hàng của họ.

Điều này giúp loại bỏ nhận dạng trùng lặp và nhận dạng giả mạo trong cơ ở dữ liệu của các nhà cung cấp dịch vụ, và qua đó giảm thất thoát lợi ích phúc lợi. Điều này cũng cho phép các nhà cung cấp dịch vụ được lệ hệ và đối chiếu lợi ích của các chương trình khác nhau bằng cách đối chiếu Mã số định danh công dân (NIN) duy nhất với hồ sơ về khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao. Cách làm này dẫn đến việc cung cấp quyền lợi một cách hợp lý với kết quả đem lại tác động lớn hơn cho các chương trình phúc lợi. Nhu cầu lặp đi lặp lại về kiểm tra nhận dạng và xác nhận khách hàng (KYC) trong quá trình cung cấp dịch vụ cũng có thể tránh được qua việc tạo nguồn thông tin Mã số định danh công dân (NIN) trong cơ sở dữ liệu của các nhà cung cấp dịch vụ.

Các nhà cung cấp dịch vụ chịu trách nhiệm về tạo nguồn thông tin cho các cơ sở dữ liệu của họ bằng thông tin về Mã số chứng minh nhận dạng quốc gia (NIN)/ định danh điện tử (eID). Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) sẽ cung cấp cho họ những công cụ cần thiết, hỗ

trợ về chuyên môn, thông lệ tốt nhất, và tư vấn theo yêu cầu để giúp triển khai quy trình tạo nguồn thông tin. Một số công cụ sẽ được cung cấp bao gồm các tiện ích tạo nguồn thông tin và Hệ thống tạo nguồn thông tin định danh điện tử quốc gia (NESP); như được mô tả chi tiết tại Phụ lục 1. Quy trình tạo nguồn thông tin định danh điện tử (eID) là sự kết hợp của một số quy trình con và không có một giải pháp duy nhất nào có thể áp dụng cho tất cả các trường hợp. Do đó, điều quan trọng là mỗi quy trình tạo nguồn thông tin phải được phân tích kỹ lưỡng và phải lên kế hoạc trước khi bắt tay vào tạo nguồn thông tin trong thực tế.

Quy trình tạo nguồn thông tin định danh điện tử (eID) cần được thực hiện sau khi số hoá và tập trung hoá dữ liệu trên cơ sở dữ liệu của nhà cung cấp dịch vụ. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) hỗ trợ phương pháp áp từ trên xuống và phương pháp hữu cơ khi tạo nguồn thông tin. Trong trường hợp phương pháp áp từ trên xuống, nhà cung cấp dịch vụ cần sử dụng một cơ sở dữ liệu sẵn có về công dân để so sánh với hồ sơ về công dân trong cơ sở dữ liệu cung cấp dịch vụ; nhà cung cấp dịch vụ không cần phải liên hệ với công dân để thực hiện quy trình tạo nguồn thông tin. Tuy nhiên, trong trường hợp áp dụng phương pháp tương tác, nhà cung cấp dịch vụ phải liên hệ với công dân, hoặc ngược lại để cập nhật Mã số định danh công dân (NIN) trên cơ sở dữ liệu của mình. Sau khi hoàn tất việc tạo nguồn thông tin áp từ trên xuống và tạo nguồn thông tin hữu cơ trong đó cơ sở dữ liệu không được phép cập nhật trực tiếp, bước tiếp theo là thực hiện xác thực nhân chủng học đối với dữ liệu tại cơ sở dữ liệu cung cấp dịch vụ. Điều này nhằm đảm bảo quy trình tạo nguồn thông tin được thực hiện một cách chính xác.

5.2.4 Dịch vụ thanh toán điện tử

Để tăng cường minh bạch, trách nhiệm giải trình, hiệu quả và nhằm đúng đối tượng hưởng lợi trong các chương trình của chính phủ như hưu trí, chăm sóc y tế, học bổng, v.v. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể cung cấp một cơ chế thanh toán gọi là Dịch vụ thanh toán điện tử trên cơ sở định danh điện tử của quốc gia (NEPS). Dịch vụ thanh toán điện tử quốc gia (NEPS) tận dụng tính năng xác thực điện tử (eID) và Tài khoản ngân hàng điện tử truy cập bằng định danh điện tử (eBA) để định tuyến khoản thanh toán cho một công dân bất kỳ trên cơ sở định danh điện tử (eID). Dịch vụ thanh toán điện tử quốc gia (NEPS) cung cấp Cầu thanh toán điện tử dựa trên định danh điện tử quốc gia tập trung (ePB) trong đó duy trì kho lưu trữ Mã số định danh công dân / định danh điện tử (eID) và đối chiếu Tài khoản ngân hàng điện tử truy cập bằng định danh điện tử (eBA) cho tất cả những người có định danh điện tử (eID) tại Việt Nam. Công dân cần cung cấp những chi tiết chính về thông tin ngân hàng để nhận phúc lợi của chính phủ vào thời điểm Hệ thống định danh điện tử quốc gia được đăng ký sử dụng cho Tài khoản ngân hàng điện tử truy cập bằng định danh điện tử (eBA). Trong trường hợp công dân không cung cấp thông tin về tài khoản ngân hàng tại thời điểm đăng ký, hệ thống sẽ ngay lập

tức tạo ra một tài khoản trên cơ sở Mã số chứng minh nhận dạng quốc gia (NIN)/ định danh điện tử (eID) và coi đó là Tài khoản ngân hàng điện tử truy cập bằng định danh điện tử (eBA) cho công dân với bên nợ đóng băng. Tiền chuyển vào sẽ được ghi có vào tài khoản mở tức thì được kích hoạt trong lần rút tiền đầu tiên trên cơ sở nhận dạng và xác nhận khách hàng điện tử (eKYC).

Cơ quan chủ quản của chính phủ về định danh điện tử (eID), cùng với các đơn vị và tổ chức liên quan khác thuộc chính phủ và khu vực tư nhân sẽ chỉ định một cơ quan của chính phủ chịu trách nhiệm triển khai và quản lý Dịch vụ thanh toán điện tử quốc gia (NEPS).

Các bộ ngành của chính phủ phải đăng ký để sử dụng Dịch vụ thanh toán điện tử quốc gia (NEPS) khi giải ngân các khoản thanh toán phúc lợi của chính phủ qua các ngân hàng bảo trợ được đăng ký. Ngân hàng bảo trở là các ngân hàng (thương mại và thương mại quốc doanh) ở Việt Nam có thể cung cấp dịch vụ của họ giúp các bộ ngành của chính phủ chi trả phúc lợi của chính phủ cho người dân Việt Nam. Ngân hàng phải đăng ký làm ngân hàng bảo trợ với Dịch vụ thanh toán điện tử quốc gia (NEPS) mới có thể cung cấp dịch vụ đó cho các bộ ngành của chính phủ. Các ngân hàng thuộc khu vực công và tư nhân cần phải đăng ký với Dịch vụ thanh toán điện tử quốc gia (NEPS) để làm ngân hàng bảo trợ nhằm cung cấp Dịch vụ thanh toán điện tử quốc gia (NEPS) cho các đơn vị sử dụng. Đơn vị sử dụng cần nộp hồ sơ Cầu thanh toán điện tử (ePB) cùng với Mã số định danh công dân (NIN)/ định danh điện tử (eID) của đối tượng hưởng lợi, mã số nhận dạng của đơn vị sử dụng, mã số tham chiếu của chương trình phúc lợi và số tiền phải thanh toán vào ngân hàng của đối tượng thụ hưởng theo một định dạng được xác định trước cho ngân hàng bảo trợ. Hồ sơ Cầu thanh toán điện tử là một tệp theo một định dạng được xác định trước do cơ quan chính phủ đó tạo ra, trong đó có các chi tiết về thanh toán cho toàn bộ các đối tượng hưởng lợi của chương trình phúc lợi. Hồ sơ này được gửi theo phương thức điện tử vào hệ thống CNTT của ngân hàng bảo trợ. Ngân hàng bảo trợ xác nhận dữ liệu và gắn mã số nhận dạng của ngân hàng (BIN) vào hồ sơ Cầu thanht oán điệnt ử (ePB) để gửi vào hệ thống Dịch vụ thanh toán điện tử quốc gia (NEPS).

Ngân hàng bảo trợ sẽ bổ sung mã số nhận dạng ngân hàng được phát hành qua Dịch vụ thanh toán điện tử quốc gia (NEPS) vào hồ sơ Cầu thanh toán điện tử (ePB) và tải lên máy chủ của Dịch vụ thanh toán điện tử quốc gia (NEPS). Dịch vụ thanh toán điện tử quốc gia (NEPS) sẽ xử lý hồ sơ được tải lên, lập hồ sơ cho ngân hàng thụ hưởng và tạo lập hồ sơ thanh toán. Ngân hàng đích sau đó sẽ tải hồ sơ đến để xử lý ghi có sau khi hồ sơ thanh toán đã được xử lý. Sử dụng hồ sơ ghi có, ngân hàng đích cần sử dụng Hệ thống ngân hàng lõi (CBS) để ghi có vốn cho tài khoản ngân hàng của đối tượng thụ hưởng.

Ngân hàng thụ hưởng sẽ cung cấp ứng dụng trên nền web hoặc di động cho các đối tượng thụ hưởng sử dụng để rút tiền, kiểm tra số dư tài khoản của họ và cho phép kích hoạt thanh toán điện tử. Vấn đề vè cách thức ứng dụng đề xuất cho phép rút tiền cũng có thể được xem xét trong

giai đoạn thí điểm. Ứng dụng này sẽ xác thực đối tượng thụ hưởng bằng cách sử dụng định danh điện tử (eID) trước khi cho phép đối tượng đó được tiếp cận tài khoản để thực hiện một giao dịch bất kỳ. Đối với công dân không được tiếp cận ứng dụng trên nền web hoặc di động, người đó có thể ra một chi nhánh ngân hàng để thực hiện giao dịch. Công dân đó cũng có thể sử dụng máy rút tiền vi mô (micro-ATM) tại đại diện ngân hàng (BC) gần đó để thực hiện giao dịch nhằm tránh mất thời gian và công sức đi lại khi phải ra chi nhánh ngân hàng đóng tại nơi không thuận tiện đi lại.

Qua đó ta có thể khuyến khích công dân tại Việt Nam sử dụng hệ thống ngân hàng chính thống và thanh toán điện tử cho các giao dịch tài chính. Ngoài ra đó còn là một kênh chi trả các khoản phúc lợi nhanh hơn mà không phải qua trung gian. Ngoài ra việc tiếp cận tài khoản ngân hàng sẽ thuận lợi hơn và bất kỳ thời điểm nào và ở bất kỳ nơi đâu.

Đối với các bộ ngành của chính phủ, việc sử dụng định danh điện tử làm mã khoá chính sẽ loại bỏ được đối tượng thụ hưởng ma và giả mạo, qua đó đảm bảo đúng đối tượng hơn. Định danh điện tử cũng giúp giảm thời gian và chi phí xử lý thanh toán và tạo ra bút tích kiểm tra điện tử và khả năng theo dõi từ đầu đến cuối toàn bộ giao dịch nhằm nâng cao tính minh bạch và trách nhiệm giải trình trong các bộ ngành.

Đối với các ngân hàng, việc sử dụng hệ thống định danh điện tử (eID) giúp tạo ra nhận dạng duy nhất cho khách hàng, khuyến khích thanh toán điện tử và qua đó giảm chi phí quản lý ngân quỹ. Hệ thống còn tăng cường khả năng tiếp cận khách hàng tại các vùng sâu và vùng xa theo mô hình đại diện ngân hàng và máy rút tiền vi mô (micro-ATM), qua đó thu hút khách hàng tốt hơn.

Có một số vấn đề cần cân nhắc trong ý tưởng đề xuất ở trên:

- Giả định đặt ra là một người chỉ có một tài khoản ngân hàng;
- Người đó phải đến cơ quan quản lý định danh trong trường hợp có thay đổi về số tài khoản ngân hàng;
- Có trường hợp ngân hàng không tham gia vào phía gửi, thì cơ quan quản lý định danh phải xử lý vốn đó; và
- Có trường hợp mã số định danh của người đó không gắn với số tài khoản

Mặc dù phương thức này có thể hoạt động trong bối cảnh Việt Nam, nhưng vẫn còn có các phương án cân nhắc khác. Ví dụ, cơ quan chịu trách nhiệm về chi trả phúc lợi có thể chỉ cần quản lý mã số định danh và số tài khoản ngân hàng. Nếu có quan ngại về sở hữu số tài khoản ngân hàng, cơ quan đó có thể xác thực tên, v.v. với cơ quan quản lý định danh và với ngân hàng. Bằng cách này, người thụ hưởng quan hệ trực tiếp với cơ quan đó.

5.2.5 Dịch vụ chữ ký số

Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) cung cấp dịch vụ chữ ký số tập trung trong Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) qua đó, công dân có thể ký kết số các tài liệu điện tử, và cho phép cung cấp dịch vụ điện tử từ đầu đến cuối tại Việt Nam. Dịch vụ này cung cấp một hệ thống chung để ký, xử lý và xác nhận chữ ký số. Hệ thống này có thể được kết nối với một ứng dụng cung cấp dịch vụ bất kỳ hiện có hoặc mới sử dụng các luồng công việc chuẩn hoá chung dưới hình thức định dạng tài liệu chung áp dụng cho một dịch vụ độc lập với nhà cung cấp dịch vụ. Dịch vụ này sử dụng chứng nhận số do một cơ quan có thẩm quyền của Chính phủ Việt Nam cấp cho công dân. Chứng nhận số được cấp cho công dân vào thời điểm đăng ký tham gia hệ thống định danh điện tử (eID), hoặc công dân có thể yêu cầu cấp chứng nhận số riêng sau khi được cấp định danh điện tử (eID). Việc cấp chứng nhận số đòi hỏi phải có Mã số chứng minh nhận dạng quốc gia (NIN).

Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) sẽ cung cấp phần mềm để công dân sử dụng khi cần ký vào tài liệu điện tử (eDocuments). Phần mềm này bao gồm các thứ viện nền và trung gian, tiện ích khách hàng, các dịch vụ web và các ứng dụng cho người sử dụng cuối cùng. Tiện ích khách hàng có thể được cài đặt trên máy tính bàn/ máy tính xách tay/ điện thoại thông minh được kết nối internet của công dân dùng để ký vào tài liệu điện tử (eDocument) bằng thẻ định danh điện tử (eID) hoặc nhận dạng di động, để kiểm tra tính hợp lệ của các chữ ký số, để mở và lưu tài liệu trong hộp chứa chữ ký. Tiện ích khách hàng này cũng được cungc ấp để bất kỳ ai cũng có thể tải về miễn phí từ cổng thông tin công cộng của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Cổng điện tử này sẽ cung cấp hướng dẫn để công dân cài đặt phần mềm trên thiết bị của họ. Hoạt động của tiện ích khác hàng trên trình duyệt internet hoặc màn hình máy tính được mô tả chi tiết tại Phụ lục 1.

5.2.6 Dịch vụ nhận dạng di động

Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể cung cấp dịch vụ nhận dạng di động để ký chữ ký số trên các tài liệu điện tử (eDocument) và xác thực người có định danh điện tử (eID). Dịch vụ định danh điện tử còn cho phép công dân sử dụng điện thoại di động của mình như một hình thức định danh điện tử an toàn để xác thực và ký chữ ký số. Giống như thẻ chứng minh nhận dạng, điện thoại sẽ được sử dụng để truy cập vào các dịch vụ điện tử an toàn và ký chữ ký số trên tài liệu, nhưng ưu điểm của nó là không cần phải có máy đọc thẻ. Chữ ký số và chứng nhận số liên quan có thể được phát hành cho người dân cần dịch vụ đó, vì việc triển khai đồng bộ cho mọi người dân khó có thể khả thi trên góc độ quy trình và quản lý.

Chữ ký số có chất lượng là các chữ ký số tiên tiên dựa trên chứ nhận đủ điều kiện do Thiết bị tạo chữ ký bảo mật (SSCD) tạo ra. Thông thường, thiết bị này có hàm ý là phải sử dụng một loại

thẻ thông minh cụ thể. Vì máy tính cá nhân hoặc máy xách tay trên thị trường không có máy đọc thẻ để sử dụng thẻ thông minh – thủ tục cần thực hiện trước khi có thể dùng thẻ – việc cài đặt máy đọc thẻ rất tốn kém và mất thời gian. Trong trường hợp nhận dạng di động, ta không cần phải cài đặt máy đọc thẻ và cài đặt một cách phức tạp mà vẫn có thể sử dụng tính năng này. Chức năng này có thể được sử dụng ở bất kỳ đâu trên thế giới miễn là được phủ sóng di động.

Liên đoàn Viễn thông Quốc tế (ITU) xếp hạng Việt Nam đứng thứ tám trên thế giới về mật độ đăng ký thuê bao di động. Do đó nhận dạng di động là một phương án tốt để định danh điện tử (eID) được áp dụng sớm. Công nghệ điện thoại thông minh đang trở nên ngày càng phổ biến, nên phương án nhận dạng di động đang ngày càng trở nên thuận tiện, cho phép sử dụng nhiều hơn định danh điện tử trong các ứng dụng di động. Điều này sẽ giúp các nhà điều hành mạng di động (MNO) hàng đầu tại Việt Nam tăng doanh số trên mỗi người đăng ký thuê bao mà không cần phải bổ sung thêm người đăng ký thuê bao trên thực tế.

Hệ thống này dựa trên một SIM điện thoại di động chuyên dụng chỉ được cấp khi công dân yêu cầu dịch vụ từ nhà điều hành điện thoại di động. SIM di động này lưu hai chứng nhận cùng với các mã khoá riêng cho các chứng nhận đó và một ứng dụng nhỏ để xác thực và ký chữ ký số.

Chính phủ có thể giao trách nhiệm cấp phát nhận dạng di động cho các nhà điều hành di động trên quốc gia, gồm Viettel, Mobiphone, Vinaphone, v.v. qua các cửa hàng tại địa phương cua rhoj. Công dân chỉ cần ký hợp đồng (thoả thuận đăng ký thuê bao nhận dạng di động) với nhà điều hành đi động đó để được cấp nhận dạng di động. Sau đó công dân đó kích hoạt dịch vụ của SIM chuyên dụng mới có trên thiết bị cầm tay. Để kích hoạt dịch vụ nhận dạng di động hoặc sử dụng chứng nhận, công dân phải lên trang web của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) để khai báo hồ sơ trực tuyến.

Nhà điều hành di động sẽ tính phí công dân để cung cấp dịch vụ nhận dạng di động. Mức phí bao gồm phí đăng ký thuê bao một lần và phí hàng tháng. Nếu nhận dạng di động được sử dụng ở ngoài Việt Nam, mỗi giao dịch nhận dạng di động sẽ được tính thêm phí gửi tin nhắn theo quy định tại danh mục giá các gói dịch vụ.

Nhận dạng di động được công dân sử dụng để đăng nhập vào các trang bảo mật; ví dụ tài khoản ngân hàng:

1. Công dân cần kích vào lựa chọn “đăng nhập bằng nhận dạng di động” trên trang web được hỗ trợ.

2. Sau đó công dân được nhắc phải nhập số di động của mình và mã số nhận dạng cá nhân của mình.

3. Trang web sẽ đưa ra một mã xác nhận trực tuyến duy nhất.

4. Điện thoại sẽ phát tiếng bíp và màn hình hiện ra thông báo kết nối đã được thực hiện.

5. Màn hình điện thoại sẽ thể hiện tên dịch vụ xác thực và mã số xác nhận.

6. Nếu tên dịch vụ là đúng và mã xác nhận tương ứng với số được thể hiện trên trang màn hình máy tính, lúc đó người sử dụng có thể ấn nút “chấp nhận”.

7. Người sử dụng sẽ được nhắc nhập Mã số nhận dạng cá nhân bằng nhận dạng di động trên điện thoại.

8. Màn hình điện thoại sẽ tắt đi và trang web được tự động tải lại và màn hình đã đăng nhập.

6.0 Các khuyến nghị về chiến lược triển khai

Chiến lược triển khai để thực hiện tầm nhìn về Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) bao gồm các phương án kiến trúc kỹ thuật tổng thể để xây dựng nền tảng và cơ sở hạ tầng công nghệ thông tin tiên tiến, có khả năng mở rộng và bảo mật để cung cấp dịch vụ định danh điện tử (eID). Phương án này sẽ hỗ trợ một khuôn khổ pháp lý và thể chế, bao gồm cả mô hình tổ chức, mô hình vận hành xác định ra các chính sách cần thiết của quốc gia để điều hành và quản lý nhà nước khuôn khổ đó. Phương án cũng có thể bao gồm một chiến lược truyền thông để nâng cao nhận thức và tạo công cụ để một số bên liên quan chính thúc đẩy việc áp dụng khuôn khổ này tại Việt Nam. Phần dưới đây trình bày một số khuyến nghị về chiến lược triển khai liên quan đến khuôn khổ nhận dạng điện tử, các phương án kỹ thuật, chiến lược truyền thông, cơ chế chính sách và thể chế cho Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF).

6.1 Khuyến nghị về kỹ thuật

1. **Hệ thống cung cấp dịch vụ định danh điện tử (EISDP).** Nền tảng dịch vụ chung và cơ sở hạ tầng CNTT tập trung dùng chung có thể được thiết kế và triển khai theo các cơ chế chuẩn phổ biến và các công nghệ dựa trên chuẩn mở để hỗ trợ các quy trình liên quan đến định danh điện tử (eID) do các nhà cung cấp dịch vụ ở cả khu vực chính phủ và khu vực tư nhân thực hiện. Các nhà cung cấp dịch vụ có thể phân cấp các quy trình phổ biến về định danh điện tử như nhận dạng duy nhất và xác thực nhận dạng cho khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao của họ một cách trực tuyến tại Hệ thống cung cấp dịch vụ định danh điện tử (EISDP), thay vì tạo ra cơ chế riêng về nhận dạng và xác thức của họ. Điều này nhằm loại bỏ các nỗ lực trùng lặp trong việc tạo nhận dạng và qua đó giảm chi phí tổng thể của quy trình cung cấp dịch vụ. Điều này cũng cho phép thực hiện quy trình nhận dạng xác thực nhận dạng chuẩn hoá với khả năng tương tác liên thông cho công dân giữa tất cả các nhà cung cấp dịch vụ tại Việt Nam.

2. **Các hợp phần kỹ thuật chính của Hệ thống cung cấp dịch vụ định danh điện tử (EISDP).**
    a. **Cổng thông tin công cộng.** Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) có thể là một cổng công cộng chung để chia sẻ thông tin công khai liên quan đến các dịch vụ nhận dạng cho công dân, các nội dung kỹ thuật, môi trường phát triển và kiểm thử cho các nhà phát triển phần mềm để giúp họ xây dựng các ứng dụng phần mềm dựa trên nhận dạng điện tử, và quản lý dịch vụ, giám sát các ứng dụng để các bên liên quan có thể truy cập qua internet và intranet. Cổng

thông tin này có thể hỗ trợ năng lực đăng ký sử dụng và xác thực để tiếp cận nội dung được bảo mật trong cổng. Về chi tiết kỹ thuật và mô tả sâu về cổng thông tin này, đề nghị tham khảo Phụ lục 4.

b. **Dịch vụ định danh điện tử và các ứng dụng chung.** Một một số ứng dụng và chức năng định danh điện tử của nhà cung cấp dịch vụ để cung cấp nhận dạng duy nhất và xác thực nhận dạng cho công dân có thể được quản lý trên Hệ thống cung cấp dịch vụ định danh điện tử (EISDP), thay vì để từng nhà cung cấp dịch vụ tự lưu trữ và quản lý. Một số ứng dụng và chức năng định danh điện tử (eID) phổ biến có thể được lưu trữ và quản lý trên Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) bao gồm:
    i. Hệ thống định danh điện tử (eID và ứng dụng nhận dạng và xác nhận khách hàng điện tử (eKYC), tạo nguồn thông tin định danh điện tử (eID), các dịch vụ nhận dạng di động và chữ ký số.
    ii. Các ứng dụng phổ biến: Hệ thống thông tin quản lý (MIS), hệ thống hỗ trợ ra quyết định (DSS), phân tích gian lận, các ứng dụng quản lý và đăng ký của các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và các Tổ chức sử dung dịch vụ định danh điện tử (ISCA), các hệ thống quản lý cơ sở hạ tầng CNTT và ứng dụng.
    iii. Trung tâm lưu trữ dữ liệu nhận dạng công dân tập trung (CRIDS)/Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) có thể lưu và quản lý phiên bản cập nhật nhất của cơ sở dữ liệu định danh điện tử (eID) có độ bảo mật cao (Mã số chứng minh nhận dạng quốc gia (NIN)+ dữ liệu sinh trắc và nhân chủng học) của công dân.

c. **Cơ sở hạ tầng CNTT (phần cứng và phần mềm)**. Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) có thể hỗ trợ các khuyến nghị về cơ sở hạ tầng CNTT như được mô tả dưới đây. Về mô tả chi tiết, đề nghị tham khảo Phụ lục 5.
    i. Các dịch vụ định danh điện tử (eID) có thể được coi là các dịch vụ web không lưu lại trạng thái.
    ii. Các dịch vụ định danh điện tử (eID) và các ứng dụng chung có thể được lưu và quản lý tại hai tổ hợp cung cấp trang tin điện tử (web farm) riêng, có khả năng mở rộng, có độ sẵn sàng cao và được ảo hoá với tổ hợp các máy chủ web ảo tại trong tâm dữ liệu tập trung.
    iii. Cơ sở hạ tầng CNTT có thể hỗ trợ năng lực và ảo hoá máy chủ để quản lý môi trường hạ tầng CNTT thực tế vào ảo hoá.
    iv. Các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) không được truy cập trực tiếp từ mạng công cộng mà chỉ được

truy cập qua Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có đăng ký bằng đường kết nối thuê bao riêng với độ dư thừa gấp đôi vào các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

v. Các biện pháp an ninh phù hợp có thể được thiết kế để ngăn ngừa truy cập trái phép từ bên ngoài vào mạng riêng được lưu giữ bởi các tổ hợp cung cấp trang tin điện tử (web farm) trong vùng bảo mật của cơ sở hạ tầng mạng được bảo vệ bằng tường lửa, và mạng riêng biệt tách riêng với các cổng chuyển đổi dư thừa.

vi. Dữ liệu có thể được lưu trữ trong các máy chủ và thiết bị lưu trữ tại vùng dữ liệu tách bạch khỏi vùng an toàn bằng tường lửa. Hệ thống lưu trữ dữ liệu được thiết kế để đảm bảo khả năng mở rộng và độ sẵn sàng cao.

vii. Trung tâm phục hồi thảm hoạ cũng có năng lực và cấu hình tương tự như trung tâm dữ liệu sản xuất và sẽ vận hành theo chế độ chủ động – chủ động.

viii. Các máy chủ môi trường phát triển và cổng thông tin có thể được truy cập qua internet và được tách riêng hoàn toàn với các máy chủ và mạng của các khu vực dữ liệu và bảo mật tại Khu phi quân sự (DMZ). Các máy chủ của cổng thông tin công cộng và các môi trường phát triển có thể được tách hoàn toàn ra khỏi các máy chủ tại khu vực dữ liệu và bảo mật.

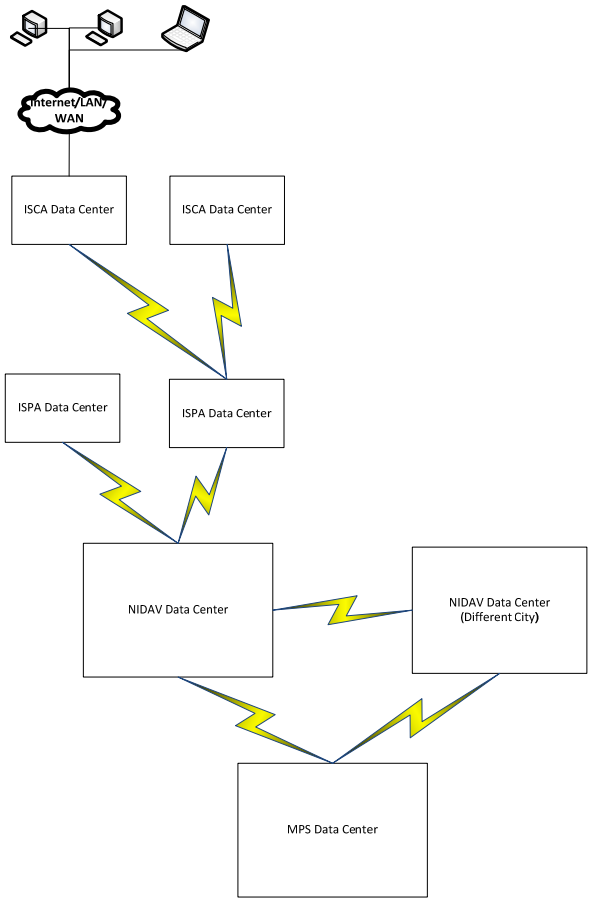
ix. Dữ liệu định danh điện tử (eID) của công dân tại Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) có thể được nhập liệu và cập nhật trên cơ sở thường xuyên bằng quy trình tạo nhận dạng tập trung cấp quốc gia. Thay vì tái tạo lại quy trình tạo nhận dạng, Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) có thể được nhập liệu bằng cách sử dụng lại cơ sở dữ liệu công dân của Bộ Công An (PMS) cấp thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID) và Mã số định danh công dân (NIN) cho công dân của Việt Nam.

x. Vì Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID) và Mã số định danh công dân (NIN) sẽ do Bộ Công an cấp ở cấp quốc gia, điều đó có nghĩa là sẽ có một quy trình duy nhất để tạo lập nhận dạng và xác nhận định dạng đó; do vậy, vấn đề một công dân có nhiều nhận dạng có thể được giải quyết Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID) có thể được sử dụng như một dạng mã thông báo nhận dạng quốc gia để chứng minh nhận dạng riêng của công dân, còn Mã số định danh công dân (NIN) có thể được dùng làm mã số nhận dạng duy nhất

đối với định danh điện tử của công dân đó trong Khuôn khổ dự kiến về định danh điện tử (EISDF).

xi. Dữ liệu về công dân mới có thể được chuyển giao định kỳ từ phía Bộ Công An (MPS) sang Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) nếu và khi có công dân mới được đăng ký tại Bộ Công an (MPS) cho đến khi toàn bộ công dân đã được cấp Mã số định danh công dân (NIN) và Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID). Một mô hình hoạt động bảo mật cần được thiết kế để chuyển giao thông tin cập nhật, như thay đổi địa chỉ giữa Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) và cơ sở dữ liệu về công dân của Bộ Công An (MPS) trên cơ sở thường xuyên.

d. **Cơ sở hạ tầng vật chất.** Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể đòi hỏi phải triển khai cơ sở hạ tầng vật chất như các trung tâm dữ liệu tại các địa bàn khác nhau dựa trên các yêu cầu triển khai và tổ chức của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Cơ sở hạ tầng vật chất của Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) có thể là một bộ phận cơ sở hạ tầng vật chất tổng thể của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Hình dưới đây mô tả về khả năng tổ chức cơ sở hạ tầng vật lý cần xây dựng để triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) tổng thể.



Hình 6.6 – Cách thức tổ chức cơ sở hạ tầng vật lý cho Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF)

Cơ sở hạ tầng vật lý của Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) có thể bao gồm các thành phần như sau, và thông tin chi tiết về từng thành phần được mô tả tại Phụ lục 4.

i. **Trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).** Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) được lưu và quản lý tại một trung tâm dữ liệu tập trung của quốc gia, gọi là trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Vì toàn bộ các dịch vụ định danh điện tử (eID) của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) đều được lưu và quản lý tại trung tâm dữ liệu này và các dịch vụ định danh điện tử (eID) sẽ được sử dụng bởi các ứng dụng quan trọng của các đơn vị và tổ chức của chính phủ và khu vực tư nhân, cho nên trung tâm dữ liệu này được coi là một cơ sở hạ tầng quan trọng của quốc gia.

ii. **Trung tâm phục hồi thảm hoạ của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).** Trung tâm phục hồi thảm hoạ có thể được xây dựng tại một địa bàn khác, chẳng hạn tại một thành khố khác có tính chất địa chấn khác biệt với địa bàn của trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Trung tâm phục hồi thảm hoạ nhằm hỗ trợ chuyển đổi dự phòng cho các dịch vụ định danh điện tử (eID), các ứng dụng và cơ sở hạ tầng CNTT của trung tâm dữ liệu thuộc Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Trung tâm này có thể vận hành theo chế độ chủ động – chủ động và có thể lưu và quản lý các dịch vụ định danh điện tử (eID) và các ứng dụng để cân bằng tải và làm giải pháp khắc phục lỗi cho trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV); trong trường hợp có sự cố, nó sẽ được chuyển đổi cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) sử dụng.

iii. **Trung tâm dữ liệu của Bộ Công an.** Trung tâm dữ liệu của Bộ Công An (MPS) có thể lưu và quản lý cơ sở dữ liệu thông tin nhận dạng quốc gia, và cơ sở dữ liệu đó được dùng để nhập liệu cho cơ sở dữ liệu công dân tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) nhằm cung cấp các dịch vụ nhận dạng.

e. **Các hệ thống an ninh và bảo mật.** Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) có thể cung cấp các chức năng bảo mật chung được lưu và quản lý tại hệ thống đó. Một số chức năng có thể bao gồm bảo mật mạng từ đầu đến cuối bằng các thông lệ bảo mật mạng tiêu chuẩn ở nhiều cấp độ như sử dụng các kênh mã hoá, lọc IP, xác thực hệ thống và thiết bị, tạo các vùng bảo mật, bảo vệ mạnh qua tường lửa và Hệ thống bảo vệ xâm nhập mạng (NIPS), kiểm tra, ... Cơ sở hạ tầng an ninh vật lý có thể là một hệ thống an ninh nhiều cấp chỉ cho phép nhân sự có thẩm quyền được thâm nhập và tiếp cận dựa trên thông tin sinh trắc, v.v.

f. **Quản lý vận hành.** Hệ thống quản lý và giám sát vận hành bao gồm các giải pháp ở cấp độ chính sách, thể chế và kỹ thuật đối với toàn bộ các cơ sở hạ tầng công nghệ và vật chất, các ứng dụng và dịch vụ nhận dạng, các giao diện cung cấp thông tin của Hệ thống cung cấp dịch vụ định danh điện tử (EISDP).

3. **Trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).** Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể là tổ chức của chính phủ hoặc tư nhân được phép thiết lập kết nối mạng riêng và bảo mật giữa trung tâm dữ liệu của họ với trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), tuân thủ theo các chuẩn mực và yêu cầu kỹ thuật của Khuôn khổ cung cấp dịch vụ định danh điện tử

(EISDF). Tổ chức cung cấp dịch vụ định danh điện tử (ISPA), với khả năng kết nối mạng tuân thủ theo Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF), cung cấp dịch vụ qua trung tâm dữ liệu của họ cho các Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và chuyển tiếp yêu cầu dịch vụ nhận dạng của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) đến Hệ thống cung cấp dịch vụ định danh điện tử (EISDP). Một số khuyến nghị về kỹ thuật cho trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) được trình bày dưới đây, thông tin chi tiết có thể được tham khảo tại Phụ lục 4.

a. Chỉ có trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) mới được gửi các yêu cầu dịch vụ nhận dạng vào trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) là cơ sở hạ tầng quan trọng để cung cấp các dịch vụ định danh điện tử (eID); do đó, thiết kế của trung tâm dữ liệu cần phải có giải pháp phục hồi thảm hoạ với tính năng hỗ trợ sao lưu dữ liệu từ xa.
b. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể công khai trên cổng thông tin điện tử công cộng của họ quy trình đăng ký làm Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) đối vơi các tổ chức của chính phủ hoặc của tư nhân bất kỳ. Cổng thong tin này cũng được dùng để công bố các tài liệu hướng dẫn kỹ thuật chi tiết về thành lập và vận hành trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).
c. Các ứng dụng và cơ sở dữ liệu của mỗi Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể được lưu và quản lý trên các máy chủ ảo hoá có khả năng mở rộng và có khả năng khắc phục lỗi cao. Trung tâm dữ liệu cũng có thể phải có các phần cứng và phần mềm theo yêu cầu để bảo mật, sao lưu dữ liệu, giám sát và quản trị trung tâm dữ liệu.

4. **Trung tâm dữ liệu của Tổ chức sử dung dịch vụ định danh điện tử (ISCA).** Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể lưu và quản lý các ứng dụng cung cấp dịch vụ của họ tại trung tâm dữ liệu tại Tổ chức sử dung dịch vụ định danh điện tử (ISCA) đó và tích hợp chúng với các dịch vụ định danh điện tử (eID) để tạo nhận dạng duy nhất và xác thực nhận dạng cho các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao của mình. Trung tâm dữ liệu của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể được kết nối với các thiết bị đầu cuối máy thanh toán tiền bằng thẻ (máy PoS) và trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) chuyên trách. Một số khuyến nghị về kỹ thuật cho trung tâm dữ liệu của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) được trình bày dưới đây, thông tin chi tiết có thể được tham khảo tại Phụ lục 4.

a. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể lưu và quản lý các ứng dụng cung cấp dịch vụ trên nền web tại trung tâm dữ liệu của họ, và các ứng dụng dựa trên khách hàng tại thiết bị đầu cuối máy thanh toán bằng thẻ (máy PoS) của họ để gửi các yêu cầu dịch vụ định danh điện tử (eID) lên trung tâm dữ liệu của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) để chuyển tiếp lên trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) qua mạng được bảo mật.
b. Các ứng dụng và cơ sở hạ tầng của mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể được lưu và quản lý tại các máy chủ ảo hoá có khả năng khắc phục lỗi và mở rộng cao. Trung tâm dữ liệu cũng có thể phải có các phần cứng và phần mềm theo yêu cầu để bảo mật, sao lưu dữ liệu, giám sát và quản trị trung tâm dữ liệu.
c. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể công khai quy trình đăng ký Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và hướng dẫn kỹ thuật chi tiết về thành lập trung tâm dữ liệu của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) lên cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).
d. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) phải cập nhật các ứng dụng máy thanh toán tiền bằng thẻ (máy PoS) và các ứng dụng cung cấp dịch vụ của mình để tích hợp với các yêu cầu Giao diện lập trùng ứng dụng (hàm API) về dịch vụ định danh điện tử của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) theo các hướng dẫn kỹ thuật do Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) đảm bảo dịch vụ được cung cấp an toàn và không gặp sự cố.
e. Các ứng dụng máy thanh toán tiền bằng thẻ (máy PoS) có thể là các ứng dụng tập trung trên nền web hoặc các ứng dụng dựa trên khách hàng phong phú được kết nối với các thiết bị sinh trắc tuân thủ theo yêu cầu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) như các thiết bị máy ảnh, thu thập thông tin vân tay, quét võng mạc, được sử dụng để thu thập dữ liệu sinh trắc của công dân.

5. **Các dịch vụ xác thực nhận dạng điện tử**. Một số khuyến nghị kỹ thuật về triển khai các dịch vụ xác thực định danh điện tử (eID) được trình bày dưới đây, để có thêm chi tiết, đề nghị tham khảo Phụ lục 4.
    a. Dịch vụ xác thực định danh điện tử (eID) có thể bao gồm nhiều phương án để công dân có thể xác thực bản thân qua hệ thống và có thể hỗ trợ "xác thực thông tin nhân chủng học" và/hoặc "xác thực thông tin sinh trắc học" và/hoặc chứng nhận số/ mật khẩu dùng một lần (OTP).

b. Dịch vụ xác thực định danh điện tử (eID) có thể được coi là dịch vụ web không lưu lại trạng thái sử dụng định dạng dữ liệu mở theo ngôn ngữ đánh dấu mở rộng (XML), giao thức được sử dụng phổ biến như giao thức truyền siêu văn bản (HTTP) và các công nghệ dựa trên chuẩn mở. Điều này nhằm hỗ tạo điều kiện thuận lợi cho việc áp dụng và triển khai các dịch vụ xác thực nhận dạng điện tử. Để tìm hiểu thêm khuyến nghị về các chuẩn mở, đề nghị tham khảo Phụ lục 4.
c. Để hỗ trợ bảo mật mạnh từ đầu đến cuối, chỉ có các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và các Tổ chức sử dung dịch vụ định danh điện tử (ISCA) mới được phép sử dụng dịch vụ qua sử dụng mã đăng ký duy nhất và các mã khoá theo giấy phép để đảm bảo tính chất không thể bác bỏ và trung thực của thông điệp. Để tránh can thiệp yêu cầu và tấn công từ trong ra, dữ liệu sẽ không được lưu giữ tại thiết bị hoặc các tệp theo dõi.
d. Hệ thống cung cấp dịch vụ định danh điện tử (EISDP), Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể duy trì các hồ sơ kiểm tra cho toàn bộ siêu dữ liệu của yêu cầu xác thực cùng phản hồi để phục vụ giải quyết vấn đề, kiểm tra, và phân tích nghiệp vụ.
e. Máy chủ của Hệ thống cung cấp dịch vụ định danh điện tử (EISDP), các Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể hỗ trợ tạo vùng nhớ đêm cho các yêu cầu xác thực và phản hồi để hỗ trợ một số trường hợp kết nối chập chờn tại trung tâm dữ liệu của các Tổ chức sử dung dịch vụ định danh điện tử (ISCA), các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và Hệ thống cung cấp dịch vụ định danh điện tử (EISDP).
f. Dịch vụ xác thực định danh điện tử (eID) có thể sử dụng Mã số định danh công dân (NIN) cùng với dữ liệu nhận dạng cá nhân (PID) của người có định danh điện tử (eID) làm thông tin đầu vào để gửi dữ liệu lên Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) để đối chiếu, sau đó Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) xác nhận độ chính xác của dữ liệu cung cấp bằng cách so sánh đối chiếu 1:1 với thông tin nhận dạng của người có định danh điện tử (eID) mà nó có được. Dịch vụ được phản hồi bằng câu trả lời (có/không) để một là khẳng định chứng minh nhận dạng (PoI) hoặc thẩm định thông tin do công dân cung cấp.
g. Trong tất cả các loại hình dịch vụ xác thực định danh điện tử (eID), Mã số định danh công dân (NIN) có thể được gửi kèm các yếu tố xác thực đơn/đa yếu tố để xác thực đảm bảo đối chiếu khớp 1:1.
h. Việc triển khai xác thực thông tin nhân chủng học có thể bao gồm đối chiếu các thuộc tính nhân chủng học cơ bản của công dân, như tên gọi, địa chỉ, giới tính,

v.v. được thu thập trong dữ liệu đầu vào yêu cầu dịch vụ cùng với dữ liệu về nhận dạng cá nhân (PID) lưu trữ tại tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Phụ lục 4 mô tả cụ thể hơn về các trường dữ liệu nhân chủng học và thiết kế cách so sánh đối chiếu.

i. Dịch vụ xác thực sinh trắc học cho phép ứng dụng của các nhà cung cấp dịch vụ xác nhận xem công dân đó có "là người được khai báo hay không". Một số ứng dụng có thể đòi hỏi phải xác nhận vật lý bằng người thực để đảm bảo phục vụ được đúng công dân và xác thực được đúng đối tượng thụ hưởng để cung cấp dịch vụ. Việc triển khai dịch vụ xác thực sinh trắc học có thể bao gồm cả triển khai đối chiếu vân tay và/hoặc võng mạc. Dữ liệu sinh trắc học do thiết bị đầu vào thu thập cần tuân thủ với các chuẩn mở để tăng cường khả năng tác nghiệp liên thông và tránh tình trạng phụ thuộc vào nhà cung cấp. Chi tiết cụ thể hơn được mô tả tại Phụ lục 4.

j. Dịch vụ xác thực bằng mật khẩu dùng một lần (OTP) cho phép công dân khởi xướng yêu cầu xác thực bằng mật khẩu dùng một lần (OTP) qua sử dụng các cổng thông tin dữ liệu dịch vụ bổ sung phi cấu trúc (USSD)/ Dịch vụ tin nhắn ngắn (SMS) hoặc khởi xướng bằng ứng dụng của nhà cung cấp dịch vụ thay mặt cho công dân bằng giao diện lập trình ứng dụng (hàm API) bằng mật khẩu dùng một lần (OTP). Xác thực bằng mật khẩu dùng một lần luôn được gửi về điện thoại di động/ địa chỉ email của công dân và ứng dụng này sẽ thu thập thông tin đó trong quá trình xác thực sao cho mật khẩu dùng một lần cũng có thể được xác nhận trong quá trình xác thực.

k. Dịch vụ xác thực bằng chứng nhận số/sinh trắc cho phép công dân đút Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID) vào máy đọc thẻ được kết nối với máy tính có kết nối internet để xác thực trên ứng dung của nhà cung cấp dịch vụ. Ứng dụng của nhà cung cấp dịch vụ sẽ đọc chứng nhận số/sinh trắc trên thẻ và gửi yêu cầu vào dịch vụ web để xác thực qua sử dụng chứng nhận số/sinh trắc dưới dạng giao diện lập trình ứng dụng (hàm API) cho dịch vụ xác thực định danh điện tử (eID).

l. Dịch vụ xác thực chứng nhận số/sinh trắc cũng có thể được khởi xướng bằng nhận dạng di động. Công dân có khả năng lựa chọn phương án nhận dạng di động để xác thực trên trang web của nhà cung cấp dịch vụ. Công cân cần nhập số điện thoại và Mã số định danh công dân (NIN) lên trang web. Ứng dụng này sẽ gửi yêu cầu giao diện lập trình ứng dụng (hàm API) dịch vụ xác thực định danh điện tử cho nhận dạng di động với phải hồi là một mã duy nhất trên trang web. Ứng dụng này cũng có thể kết nối với điện thoại di động và kích hoạt ứng dụng

xác thực định danh điện tử (eID) trên điện thoại di động và trình bày cùng mã duy nhất đó.

m. Thiết kế dịch vụ xác thực có thể được mở rộng và hỗ trợ các mã thông báo khác nhau như qua điện thoại di động, mã công nghệ giao tiếp tầm ngắn (NFC), thẻ thông minh v.v. ngày nay và trong tương lai. Ta cũng nên bổ sung thêm yếu tố thứ hai ("công dân đó có gì") cho giao dịch tự phục vụ từ phía công dân.
n. Phản hồi xác thực có thể được sử dụng như một bằng chứng nhận dạng (PoI) và bằng chứng địa chỉ (PoA) số vào một thời điểm sau đó bằng cách bổ sung siêu thông tin tại các chi tiết dữ liệu nhận dạng cá nhân (PID) tại yêu cầu xác thực vào phản hồi xác thực.

6. **Dịch vụ nhận dạng và xác nhận khách hàng điện tử**. Dưới đây là một số khuyến nghị kỹ thuật về triển khai dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC):
    a. Dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) cho phép quy trình nhận dạng và xác nhận khách hàng (KYC) được thực hiện bằng phương thức điện tử với sự cho phép rõ ràng từ phía công dân. Dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) dựa trên định danh điện tử (eID) có thể cung cấp chứng minh nhận dạng (PoI) và chứng minh địa chỉ (PoA) điện tử, tức thời, và không thể bác bỏ cùng với ngày sinh và giới tính.
    b. Kiến trúc kỹ thuật và thiết kế về an ninh cũng có thể tương tự như đối với dịch vụ xác thực nhận dạng điện tử.
    c. Dịch vụ này có thể chỉ dành cho các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có đăng ký và được thực hiện tại các địa điểm đại lý bằng xác thực sinh trắc, hoặc từ xa bằng mật khẩu dùng một lần (OTP) qua kết nối di động hoặc trang web.
    d. Công dân có thể cho phép Tổ chức sử dung dịch vụ định danh điện tử (ISCA), qua xác thực định danh điện tử (eID) bằng dữ liệu sinh trắc/ chứng nhận số/ mật khẩu dùng một lần (OTP), gửi dữ liệu nhân chủng học và ảnh của mình được ký chữ ký số và được mã hoá cho các nhà cung cấp dịch vụ.
    e. Phản hồi của dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) có thể được thực hiện bằng ngôn ngữ đánh dấu mở rộng (XML) được ký chữ ký số và được mã hoá, chứa dữ liệu nhân chủng học và ảnh của công dân. Phản hồi này có thể được nhà cung cấp dịch vụ sử dụng làm chứng từ nhận dạng và xác nhận khách hàng điện tử (eKYC) để cung cấp dịch vụ cho công dân.

7. **Dịch vụ chứng nhận số.** Kiến trúc kỹ thuật của các dịch vụ chứng nhận số cũng tương tự như những gì hiện được cung cấp bởi Cơ quan quản lý chứng nhận số của Chính phủ Việt Nam (VGCA).

8. **Dịch vụ nhận dạng di động.** Dưới đây là một số khuyến nghị kỹ thuật về triển khai dịch vụ nhận dạng di động, chi tiết đầy đủ được trình bày tại Phụ lục 4.
    a. Dịch vụ nhận dạng di động có thể được thực hiện trên SIM được cấp quyền bởi Cơ sở hạ tầng mã khoá công cộng không dây (wPKI) với sự hỗ trợ của hồ sơ bảo vệ chuẩn. SIM này có thể được mua qua qua môi trường bảo mật và được sử dụng cho điện thoại di động hỗ trợ sử dụng thẻ.
    b. SIM này có thể có mô-đun Thiết bị tạo chữ ký bảo mật (SSCD), với hai cặp mã khoá; một để xác thực và một cho các mục đích tính năng chữ ký/không thể bác bỏ.
    c. Dịch vụ nhận dạng di động có thể được lưu và quản lý trên Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) dưới dạng dịch vụ web không lưu lại trạng thái. Ứng dụng cung cấp dịch vụ có thể được lưu và quản lý trên trung tâm dữ liệu của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và qua đó có thể yêu cầu dịch vụ nhận dạng di động được lưu và quản lý tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) với Mã số chứng minh nhận dạng quốc gia (NIN), số điện thoại và Mã số nhận dạng cá nhân (PIN).
    d. Về phần mình, dịch vụ này xác nhận số điện thoại được cung cấp làm thông tin đầu vào với số điện thoại được lưu trữ tại Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) cho công dân đó. Sau khi xác nhận thành công, nó sẽ yêu cầu dịchv ụ web của Nhà cung cấp dịch vụ tin cậy (TSP) được lưu trữ tại trung tâm dữ liệu của Nhà cung cấp dịch vụ tin cậy (TSP) đó qua kết nối internet an toàn bằng số điện thoại, mã số xác nhận và Mã số nhận dạng cá nhân (PIN).
    e. Để phản hồi, dịch vụ của Nhà cung cấp dịch vụ tin cậy sẽ tạo ra mã xác nhận và gửi mã đó lên trang web của Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Dịch vụ này cũng tạo ra yêu cầu chữ ký với mã số xác nhận, số điện thoại và Mã số nhận dạng cá nhân (PIN) để gửi vào điện thoại di động qua cổng dịch vụ tin nhắn ngắn (SMS) và dịch vụ cập nhật từ xa (OTA) của Nhà cung cấp dịch vụ tin cậy (TSP) qua mạng không dây dưới hình thức dịch vụ tin nhắn ngắn (SMS).
    f. Dịch vụ tin nhắn ngắn cập nhật từ xa (OTA SMS) kích hoạt ứng dụng xác nhận nhận dạng trên SIM. Dịch vụ này hiển thị mã số xác nhận cũng là mã số được hiển thị trên máy tính của công dân. Công dân xác nhận mã số xác nhận được

hiển thị trên thiết bị di động với mã số hiển thị trên máy tính và sau đó ký yêu cầu bằng cách nhập Mã số nhận dạng cá nhân (PIN).

g. Sau khi xác thực thành công, công dân đăng nhập vào trang web bảo mật.
h. Dịch vụ nhận dạng di động có thể đòi hỏi phải cung cấp SIM, đăng ký người sử dụng, kích hoạt chứng nhận và kết thúc dịch vụ. Chi tiết kỹ thuật đầy đủ liên quan đến các hoạt động đó được trình bày tại Phụ lục 4.

9. **Dịch vụ tạo nguồn thông tin nhận dạng điện tử.** Dưới đây là một số khuyến nghị kỹ thuật về triển khai dịch vụ tạo nguồn thông tin nhận dạng đầy đủ.
    a. **Tiện ích tạo nguồn thông tin** có thể là một tiện ích khách hàng trên màn hinh máy tính để tạo nguồn thông tin Mã số định danh công dân (NIN) trong hồ sơ công dân được lưu trữ trên cơ sở dữ liệu của nhà cung cấp dịch vụ. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể tải tiện ích này về từ cổng thông tin điện tử của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và cài đặt trên máy chủ của mình để thực hiện. Tiện ích này cung cấp năng lực trích xuất, tổng hợp, tiêu chuẩn hoá và so sánh đối chiếu dữ liệu. Tiện ích này có thể kết nối với các các nguồn dữ liệu khác để lấy dữ liệu nhận dạng cá nhân liên quan về từ các cơ sở dữ liệu tham chiếu. Nó cũng có thể lấy dữ liệu về từ các bảng dữ liệu liên quan trong cơ sở dữ liệu của nhà cung cấp dịch vụ. Để tìm hiểu chi tiết về tính năng của tiện ích này, đề nghị tham khảo Phụ lục 4.
    b. **Hệ thống tạo nguồn thông tin định danh điện tử quốc gia (NESP)** có thể là một ứng dụng web được lưu và quản lý trên cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Công dân và người sử dụng được cấp quyền ("người tạo nguồn thông tin") của nhà cung cấp dịch vụ có thể đăng nhập để gửi yêu cầu tạo nguồn thông tin và xác nhận yêu cầu ("người xác nhận"). Hệ thống tạo nguồn thông tin định danh điện tử quốc gia (NESP) có thể truy cập dữ liệu về công dân được lưu trữ tại Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) bằng các dịch vụ web, và dữ liệu về công dân tại cơ sở dữ liệu cho phép sử dụng dịch vụ bằng các dịch vụ web hoặc thiết lập cơ sở dữ liệu cho phép sử dụng dịch vụ tại Hệ thống tạo nguồn thông tin định danh điện tử quốc gia (NESP). Dịch vụ web để truy xuất dữ liệu về công dân tại cơ sở dữ liệu cho phép sử dụng dịch vụ có thể được lưu và quản lý tại máy chủ của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) trong trung tâm dữ liệu của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) đó. Một phương án nữa là tạo bản sao cơ sở dữ liệu cho phép sử dụng dịch vụ đó vào máy chủ cơ sở dữ liệu tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam

(EIDAV) trong Hệ thống tạo nguồn thông tin định danh điện tử quốc gia (NESP). Hệ thống tạo nguồn thông tin định danh điện tử quốc gia (NESP) cũng có thể tạo cơ chế để yêu cầu dịch vụ xác thực định danh điện tử (eID) được lưu và quản lý trên Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) để thực hiện xác thực thông tin sinh trắc và nhân chủng học để xác nhận tạo nguồn thông tin.

6.2 Khuyến nghị về thể chế

Một số khuyến nghị về mặt thể chế liên quan đến mô hình hoạt động và cơ cấu tổ chức cần có để triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) trên góc độ kỹ thuật và vận hành được trình bày dưới đây.

6.2.1 Mô hình hoạt động

Dịch vụ xác thực nhận dạng điện tử

Dịch vụ xác thực định danh điện tử có thể được các nhà cung cấp dịch vụ sử dụng trên toàn quốc ở Việt Nam. Dịch vụ này có thể được điều hành bằng một mô hình hoạt động có khả năng mở rộng cao trên cơ sở hình thức quan hệ hợp tác công – tư (PPP) để đáp ứng nhu cầu của các nhà cung cấp dịch vụ hiện nay và trong tương lai. Một số khuyến nghị về mô hình hoạt động cho dịch vụ xác thực định danh điện tử (eID) được trình bày dưới đây:

1. Dịch vụ xác thực định danh điện tử (eID) có thể được cung cấp trong phạm vi Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) cho toàn bộ các nhà cung cấp dịch vụ tại Việt Nam. Do đó, nó có thể được quản lý và chủ quản bởi một bộ ở cấp trung ương chịu trách nhiệm cung cấp các dịch vụ định danh điện tử (eID) như xác thực định danh điện tử (eID) cho các nhà cung cấp dịch vụ, nhưng không chịu trách nhiệm về quyền hưởng dịch vụ. Bộ chịu trách nhiệm đó có thể thành lập một cơ quan, gọi là Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) cho mục đích đó.

2. Bộ chịu trách nhiệm sẽ giao cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) làm Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) để thiết kế và triển khai dịch vụ xác thực định danh điện tử (eID), lưu và quản lý dịch vụ đó tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) thuộc Hệ thống cung cấp dịch vụ định danh điện tử (EISDP). Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể thuê nhà thầu tích hợp giải pháp (SI) để triển khai dịch vụ qua đấu thầu. Họ cũng có thể triển

khai quy trình đăng ký cung cấp dịch vụ xác thực định danh điện tử (eID) trên cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

3. Các nhà cung cấp dịch vụ thuộc khu vực công hoặc tư nhân mong muốn sử dụng các dịch vụ định danh điện tử (eID) như xác thực định danh điện tử (eID) có thể đăng ký làm Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và ký thoả thuận với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

4. Tổ chức sử dung dịch vụ định danh điện tử (ISCA), về phần mình, có thể thỏa thuận với một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) thuộc khu vực công hoặc tư nhân. Để đảm bảo an ninh ở mức độ cao đối với cơ sở dữ liệu về công dân được lưu trữ tập trung tại Hệ thống cung cấp dịch vụ định danh điện tử (EISDP), chỉ có một số lượng hạn chế các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) đủ tiêu chuẩn mới được phép kết nối trực tiếp với các máy chủ tại các trung tâm dữ liệu tập trung của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

5. Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể thiết lập kết nối bảo mật với các máy chủ dịch vụ định danh điện tử (eID) tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để truyền các yêu cầu dịch vụ như dịch vụ xác thực định danh điện tử (eID) thay mặt cho các Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và tiếp nhận phản hồi lại.

6. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể quy định về các tiêu chuẩn và yêu cầu kỹ thuật để Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) tuân thủ trong việc thiết lập và duy trì kết nối bảo mật với các dịch vụ tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

7. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể áp dụng phương án tự kết nối với máy chủ của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) hoặc qua một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) hiện có.

8. Hơn nữa, nhà cung cấp dịch vụ nếu muốn sử dụng các dịch vụ định danh điện tử (eID) như dịch vụ xác thực có thể có phương án trở thành một Tổ chức sử dung dịch vụ định danh điện tử (ISCA), hoặc truy cập các dịch vụ định danh điện tử (eID) qua một Tổ chức sử dung dịch vụ định danh điện tử (ISCA) hiện có. Trong trường hợp thứ hai, nó có thể

trở thành một tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) hiện hành mà nó tham gia cùng.

Dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC)

Sau đây là một số khuyến nghị về mô hình hoạt động đối với dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC).

1. Tương tự như dịch vụ xác thực nhận dạng điện tử, dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) có thể do Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) quản lý và làm chủ quản.

2. Nhà cung cáp dịch vụ muốn sử dụng dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) cho các dịch vụ của minh có thể đăng ký làm Tổ chức sử dung dịch vụ định danh điện tử (ISCA) được phép truy cập vào dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) và được ký hợp đồng với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

3. Tổ chức sử dung dịch vụ định danh điện tử (ISCA), về phần mình, sẽ tham gia với Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) để huyển tuyến yêu cầu dịch vụ và nhận phản hồi lại từ dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) được lưu và quản lý tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) qua mạng an toàn của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).

4. Dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) có thể được thực hiện tại địa điểm đại lý khi sử dụng xác thực bằng thông tin sinh trắc học hay từ xa khi sử dụng mật khẩu dùng một lần (OTP) qua kết nối di động hoặc trang web. Trong quá trình nhận dạng và xác nhận khách hàng điện tử (eKYC), công dân có thể cho phép cơ quan chủ quản của chính phủ, qua việc xác thực định danh điện tử bằng thông tin sinh trắc/ chứng nhận số/ mật khẩu dùng một lần (OTP), được cung cấp dữ liệu nhân chủng học và ảnh của công dân được ký chữ ký số và được mã hoá cho nhà cung cấp dịch vụ.

5. Công dân đó có thể đến Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và, qua sự hỗ trợ của một nhà điều hành hoặc bằng cách sử dụng một thiết bị có kết nối internet, truy cập ứng dụng để nhập liệu dữ liệu yêu cầu dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC). Phản hồi nhận được bằng ngôn ngữ đánh dấu mở rộng (XML) mã hoá có thể được nhà cung cấp dịch vụ coi là chứng từ nhận dạng và xác nhận khách hàng điện tử (eKYC) khi cung cấp dịch vụ cho công dân đó.

6. Công dân đó có thể lưu giữ chứng từ nhận dạng và xác nhận khách hàng điện tử (eKYC) để sử dụng về sau khi yêu cầu dịch vụ từ các nhà cungc ấp dịch vụ có đăng ký tại Việt Nam.

Dịch vụ tạo nguồn thông tin nhận dạng điện tử

Sau đây là một số khuyến nghị về mô hình hoạt động cho dịch vụ tạo nguồn thông tin định danh điện tử (eID).

1. Các nhà cung cấp dịch vụ đang sử dụng các dịch vụ định danh điện tử (eID) trong quá trình cungc ấp dịch vụ của ho có thể chịu trách nhiệm tạo nguồn thông tin định danh điện tử (eID)/ Mã số định danh công dân (NIN) trên cơ sở dữ liệu cho phép sử dụng dịch vụ để tạo nhận dạng duy nhất cho các khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao của mình.

2. Chiến lược triển khai tạo nguồn thông tin Mã số chứng minh nhận dạng quốc gia (NIN)/ định danh điện tử (eID) tại cơ sở dữ liệu cho phép sử dụng dịch vụ của các nhà cung cấp dịch vụ có thể kết hợp nhiều tiểu chiến lược và không có một giải pháp duy nhất nào áp dụng được cho tất cả các trường hợp. Do đó, điều quan trọng là quy trình tạo nguồn thông tin phải được phân tích thấu đáo và lập kế hoạch trước khi thực hiện tạo nguồn thông tin trên thực tế.

3. Điều kiện tiên quyết để tạo nguồn thông tin định danh điện tử (eID) là các nhà cung cấp dịch vụ phải chuẩn bị cơ sở dữ liệu cho phép sử dụng dịch vụ bằng cách thực hiện số hoá dữ liệu và tập trung hoá dữ liệu. Nếu nhà cung cấp dịch vụ đã có cơ sở dữ liệu cho phép sử dụng dịch vụ được số hoá và tập trung hoá, thì không cần phải làm gì thêm trên góc độ tạo nguồn thông tin dữ liệu định danh điện tử (eID). Để tìm hiểu mô tả chi tiết về số hoá và tập trung hoá dữ liệu, tham khảo Phụ lục 4.

4. Trên cơ sở dữ liệu sẵn có và các yêu cầu khác, nhà cung cấp dịch vụ có thể chọn giữa phương thức áp từ trên xuống và phương thức hữu cơ để tạo nguồn thông tin Mã số định danh công dân (NIN) trên cơ sở dữ liệu cho phép sử dụng dịch vụ của họ. Để tìm hiểu mô tả chi tiết về các chiến lược tạo nguồn thông tin dữ liệu định danh điện tử (eID), tham khảo Phụ lục 4.

5. Khi sử dụng phương thức áp từ trên xuống, nhà cung cấp dịch vụ có thể sử dụng tiện ích tạo nguồn thông tin ngoại tuyến hoặc Hệ thống tạo nguồn dữ liệu định danh điện tử (eSP) để tạo nguồn thông tin Mã số định danh công dân (NIN) một lần. Trong trường hợp tạo nguồn thông tin hữu cơ, nhà cung cấp dịch vụ đó sử dụng Hệ thống tạo nguồn dữ liệu định danh điện tử (eSP) để chức năng tạo nguồn thông tin gửi yêu cầu tạo nguồn thông tin cho các công dân để họ phản hồi; công dân cũng có thể chủ động tự nguyện tạo nguồn cho mình.

6. Các nhà cung cấp dịch vụ phải đăng ký với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để sử dụng tiện ích tạo nguồn thông tin ngoại tuyến và đăng ký trực tuyến tại cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) với tư cách là đơn vị tạo nguồn thông tin và đơn vị xác nhận thông tin để sử dụng Hệ thống tạo nguồn dữ liệu định danh điện tử (eSP).

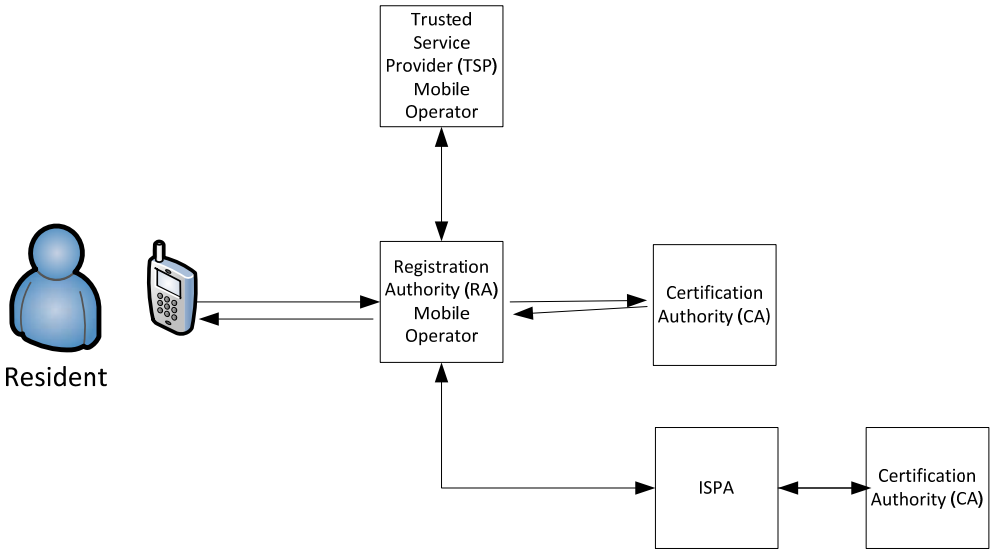
7. Nhà cung cấp dịch vụ có thể đăng ký làm Tổ chức sử dung dịch vụ định danh điện tử (ISCA) trên cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để thực hiện xác thực thông tin nhân chủng học cho hồ sơ khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao của mình tại cơ sở dữ liệu của mình bằng dịch vụ xác thực định danh điện tử (eID) để xác nhận quy trình tạo nguồn thông tin. Trong trường hợp không xác thực thông tin nhân chủng học được, nhà cung cấp dịch vụ đó có thể tìm hiểu lý do thất bại. Dưới đây là một số lý do:
    a. Mã số định danh công dân (NIN) được tạo nguồn thông tin vào bản ghi không đúng. Điều này có thể xảy ra trong trường hợp đối chiếu chưa khớp nối được đầy đủ hoặc còn mơ hồ.
    b. Công dân cập nhật dữ liệu nhận dạng cá nhân (PID) của mình trên Trung tâm lưu trữ dữ liệu nhận dạng tập trung (CIDR) do hôn nhân, thay đổi địa chỉ, cập nhật lại thông tin chưa chính xác, v.v.
    c. Dữ liệu chưa chính xác hoặc mẫu KYR+ chưa đầy đủ được thu thập trong quá trình đăng ký (ví dụ mã số thẻ bảo hiểm y tế chưa chính xác).

8. Xác thực thông tin sinh trắc có thể được thực hiện tại các thiết bị điểm chạm được nhà điều hành hỗ trợ để cập nhật trực tiếp cho cơ sở dữ liệu cung cấp dịch vụ.

9. Dịch vụ tạo nguồn thông tin định danh điện tử (eID) có thể được thiết kế để giải quyết một số thách thức chung trong quá trình tạo nguồn thông tin. Về những thách thức chung trong tạo nguồn thông tin và giải pháp xử lý, đề nghị tham khảo Phụ lục 4.

Dịch vụ nhận dạng di động

Dịch vụ nhận dạng di động có thể được quản lý qua mô hình hoạt động theo hình thức quan hệ đối tác công – tư (PPP) có khả năng mở rộng cao với bốn thủ tục hoạt động chính: đó là cung cấp SIM, kích hoạt chứng nhận, sử dụng và kết thúc dịch vụ. Các thủ tục hoạt động được thực hiện bởi các đơn vị được xác định trong cơ cấu tổ chức cung cấp dịch vụ nhận dạng di động ở phần sau trong tài liệu này. Dưới đây là khuyến nghị về các thủ tục hoạt động,



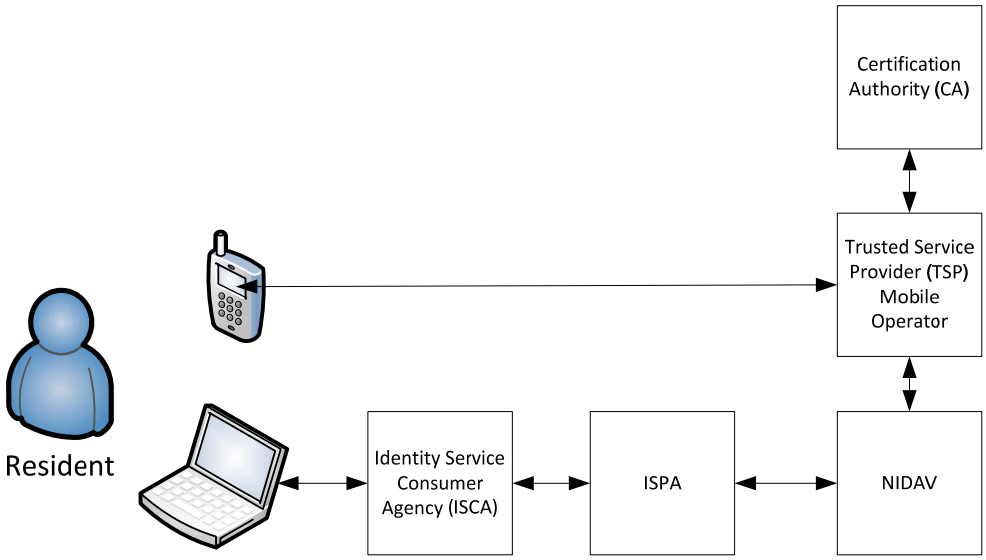
Hình 6.1: Mô hình hoạt động dịch vụ nhận dạng di động – Cung cấp SIM/ kích hoạt chứng nhận

1. **Cung cấp SIM**
    a. Công dân muốn sử dụng dịch vụ nhận dạng di động có thể đến đại lý gần nhất của nhà điều hành di động có đăng ký với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để làm Cơ quan quản lý đăng ký (RA) được phê duyệt,
    b. Cơ quan quản lý đăng ký (RA) có thể cung cấp các SIM chuyên dụng có tính năng thiết bị tạo chữ ký bảo mật (SSCD) có khả năng cấp ra chứng nhận số/sinh trắc đủ điều kiện cho mục đích xác thực và ký chữ ký.
    c. Cơ quan quản lý đăng ký (RA) có thể xác nhận nhận dạng của công dân bằng Mã số định danh công dân (NIN) và thông tin sinh trắc học của người đó bằng dịch vụ xác thực nhận dạng điện tử. Cơ quan quản lý đăng ký (RA) có thể đăng ký làm Tổ chức sử dung dịch vụ định danh điện tử (ISCA) với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để gửi yêu cầu dịch vụ xác thực định danh điện tử với Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có đăng ký.

d. Sau khi xác nhận thành công nhận dạng điện tử, Cơ quan quản lý đăng ký (RA) có thể cấp cho công dân SIM chuyên dụng cùng với mã kích hoạt bí mật trong một thủ tục gặp mặt trực tiếp.
e. Cơ quan quản lý đăng ký (RA) có thể tuyên bố chứng nhận thiết bị tạo chữ ký bảo mật (SSCD) đã được kích hoạt cho SIM cụ thể đó và thông tin đó được gửi cho toàn bộ các Nhà cung cấp dịch vụ tin cậy (TSP).

2. **Đăng ký sử dụng/ kích hoạt chứng nhận**
    a. Công dân sử dụng điện thoại di động của mình để khởi động ứng dụng kích hoạt SIM lưu trữ trên SIM đó. Công dân đó có thể gửi yêu cầu để kích hoạt chứng nhận đủ điều kiện.
    b. Cơ quan quản lý đăng ký (RA) có thể phản hồi yêu ầu bằng cách khởi động hoạt động trên thiết bị di động của công dân để ký vào dữ liệu nhận dạng cá nhân (PID). Dữ liệu nhận dạng cá nhân (PID) bao gồm Mã số định danh công dân (NIN) cùng với các chi tiết nhân chủng học đó.
    c. Công dân có thể thẩm định dữ liệu và ký bằng cách nhập liệu mã kích hoạt chứng nhận thiết bị của họ.
    d. Cơ quan quản lý đăng ký (RA) có thể tiếp nhận dữ liệu nhận dạng cá nhân (PID) và bổ sung thêm dữ liệu bổ sung bao gồm chứng nhận thiết bị, sau đó gửi yêu cầu kích hoạt chứng nhận cho Cơ quan có thẩm quyền chứng nhận (CA). Cơ quan quản lý đăng ký (RA) cung gửi yêu cầu dịch vụ cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) qua một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có đăng ký để cập nhật số điện thoại vào hồ sơ nhận dạng của công dân đó.
    e. Cơ quan có thẩm quyền chứng nhận (CA) co thể tạo và kích hoạt chứng nhận và cung cấp thông tin đó cho các Nhà cung cấp dịch vụ tin cậy (TSP) và Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).
    f. Công dân có thể được thông báo về tình trạng hoạt động và có cơ hội thay đổi mã pin.

3. **Sử dụng**



Hình 6.2: Mô hình hoạt động sử dụng dịch vụ nhận dạng điện tử

a. Công dân có thể sử dụng dịch vụ định danh điện tử để xác thực định danh điện tử (eID) trên một trang web bảo mật, ví dụ ngân hàng trực tuyến.
b. Công dânc ó thể truy cập trang web bảo mật của Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Trang web được hỗ trợ sẽ có lựa chọn ấn nút "đăng nhập bằng nhận dạng di động".
c. Công dân có thể được nhắc nhập số di động được đăng ký, Mã số định danh công dân (NIN) và mã số nhận dạng cá nhân (PIN) của mình.
d. Hệ thống của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể yêu cầu dịch vụ nhận dạng vào dịch vụ web nhận dạng di động của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF), bằng cách gửi số di động, Mã số định danh công dân (NIN) và mã số nhận dạng cá nhân (PIN) tới Nhà cung cấp dịch vụ tin cậy (TSP) qua Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).
e. Dịch vụ nhận dạng di động của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể xác nhận số di động được cung cấp bằng số di động được lưu trữ bằng Mã số định danh công dân (NIN) nhận được và chuyển yêu cầu dịch vụ cho Nhà cung cấp dịch vụ tin cậy (TSP) cùng với số di động, mã xác nhận và Mã số nhận dạng cá nhân (PIN). Dịch vụ này có thể tạo ra mã xác nhận và gửi đến trang web của Tổ chức sử dung dịch vụ định danh điện tử (ISCA).
f. Nhà cung cấp dịch vụ tin cậy (TSP) có thể tạo yêu cầu chữ ký bằng mã xác nhận, số điện thoại di động, Mã số nhận dạng cá nhân (PIN) và gửi yêu cầu đó vào máy điện thoại di động của công dân.

g. Công dân có thể kiểm tra mã xác nhận trên điện thoại di động của mình với mã số trên trang web và ký yê cầu bằng cách nhập Mã số nhận dạng cá nhân (PIN).
h. Nhà cung cấp dịch vụ tin cậy (TSP) có thể nhận dữ liệu chữ ký để gửi cho Cơ quan có thẩm quyền chứng nhận (CA) để xác nhận dữ liệu chữ ký và chứng nhận.
i. Nhà cung cấp dịch vụ tin cậy (TSP) có thể chuyển tiếp phản hồi nhận được từ phía Cơ quan có thẩm quyền chứng nhận (CA) cho Tổ chức sử dung dịch vụ định danh điện tử (ISCA) thông qua Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).
j. Sau khi xác thực thành công, công dân đăng nhập vào trang web bảo mật đó.

4. **Kết thúc**
    a. Công dân có thể ngừng sử dụng dịch vụ nhận dạng di động bằng một số cách:
        i. Công dân thông báo cho Cơ quan quản lý đăng ký (RA) về mong muốn ngừng sử dụng dịch vụ của mình.
        ii. Công dân thông báo cho Cơ quan quản lý đăng ký (RA) về việc mất hoặc mất tác dụng thiết bị tạo chữ ký bảo mật (SSCD).
        iii. Chứng nhận được cấp đã hết hạn.
        iv. Cơ quan quản lý đăng ký (RA) phát hiện người sử dụng đã vi phạm thoả thuận giữa Cơ quan có thẩm quyền chứng nhận và người sử dụng, hoặc các văn bản pháp luật quy định về dịch vụ nhận dạng di động.
    b. Trong trường hợp thu hồi chứng nhận, Cơ quan quản lý đăng ký (RA) phải thông báo cho Cơ quan có thẩm quyền chứng nhận (CA) về việc thu hồi chứng nhận. Sau đó Cơ quan có thẩm quyền chứng nhận (CA) ngay lập tức thu hồi chứng nhận và hưu hành danh mục thu hồi chứng nhận mới được cập nhật (CRL) cho toàn bộ các Nhà cung cấp dịch vụ tin cậy (TSP).
    c. Trong trường hợp khoá SIM do mất hoặc hư hỏng SIM, chứng nhận thiết bị sẽ được đưa ra khỏi danh sách các thiết bị tạo chữ ký số bảo mật (SSCD) hợp lệ áp dụng cho tất cả các Nhà cung cấp dịch vụ tin cậy (TSP).

6.2.2 Cơ cấu tổ chức

Phần dưới đây đưa ra khuyến nghị về các vai trò chính trong cơ cấu tổ chức để vận hành và quản lý các dịch vụ định danh điện tử (eID) trong phạm vi Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Tham khảo Phụ lục 4 để tìm hiểu mô tả chi tiết hơn về các vai trò và trách nhiệm.

1. **Dịch vụ xác thực nhận dạng điện tử: Các vai trò chính**

a. **Cơ quan quản lý định danh điện tử Việt Nam.** Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể được thành lập với nhiệm vụ tạo định danh điện tử và cung cấp các dịch vụ định danh điện tử (eID) trong phạm vi Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) như xác thực định danh điện tử (eID) cho các nhà cung cấp dịch vụ đủ điều kiện tại khu vực công và tư nhân. Điều này cho phép thực hiện các chức năng nghiệp vụ yêu cầu phải xác lập nhận dạng của khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao cũng như người lao động. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể là cơ quan quản lý nhà nước và giám sát theo dõi hệ môi trường các dịch vụ định danh điện tử (eID) thuộc Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Cơ quan này cũng có thể tự thực hiện hoặc hoặc thông qua một cơ quan khác thực hiện chức năng chủ quản và quản lý Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) để lưu trữ Mã số định danh công dân (NIN) và Dữ liệu nhận dạng cá nhân (PID) liên quan. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể quản lý Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) và máy chủ xác thực định danh điện tử (eID) qua một Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP).
b. **Nhà cung cấp dịch vụ nhận dạng được quản lý.** Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) có thể là đơn vị thay mặt cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để cung cấp các dịch vụ định danh điện tử (eID) như dịch vụ xác thực. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể thuê một hoặc một số Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) tuỳ theo số lượng yêu cầu dịch vụ. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có trách nhiệm triển khai và vận hành kiến trúc kỹ thuật của Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) với tư cách là Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) trong giai đoạn thí điểm.
c. **Tổ chức cung cấp dịch vụ nhận dạng.** Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể là cơ quan của chính phủ hoặc tư nhân được thiết lập kết nối bảo mật với trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), tuân thủ theo các chuẩn mực và yêu cầu kỹ thuật do Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) đặt ra để thay mặt cho Tổ chức sử dung dịch vụ định danh điện tử (ISCA) chuyển yêu cầu xác thực định danh điện tử (eID) và nhận phản hồi lại từ các máy chủ xác thực định danh điện tử (eID). Chỉ các đơn vị được ký hợp đồng với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) làm Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) mới có thể gửi yêu cầu dịch vụ về xác thực nhận dạng điện tử; không một đơn vị nào khác có thể giao tiếp trực

tiếp với các dịch vụ nhận dạng. Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể có quan hệ với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) qua một hợp đồng pháp lý chính thức. Các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể sử dụng kết nối mạng tuân thủ theo yêu cầu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để cung cấp dịch vụ cho một hoặc một số Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và có thể chuyển yêu cầu xác thực của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) vào máy chủ xác thực của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể là:

i. Một bộ ngành của chính phủ như Vụ viễn thông của Bộ Thông tin và Truyền thông (MIC) có thể trở thành Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và được thiết lập kết nối đường thuê bao tuân thủ theo yêu cầu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) với các máy chủ xác thực định danh điện tử (eID) để một số bộ ngành trong nước có thể chuyển yêu cầu xác thực của họ qua đó.
ii. Một công ty viễn thông như Tập đoàn Viettel hoặc VNPT có thể xin phép Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) đồng ý cho thiết lập kết nối bảo mật với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để cung cấp dịch vụ với tư cách là Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) cho các Tổ chức sử dung dịch vụ định danh điện tử (ISPA).
iii. Một ngân hàng quốc doanh như Ngân hàng Việt Nam (BoV) có thể thiết lập kết nối tuân thủ theo yêu cầu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) với các máy chủ xác thực định danh điện tử (eID) để cung cấp dịch vụ xác thực và có thể cả các dịch vụ đem lại giá trị gia tăng cho bản thân họ và các ngân hàng nhỏ hơn khác.

d. **Tổ chức sử dung dịch vụ nhận dạng điện tử.** Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể là một đơn vị thuộc chính phủ hoặc khu vực tư nhân mong muốn sử dụng các dịch vụ định danh điện tử (eID) như dịch vụ xác thực để thực hiện một hoặc một số dịch vụ của mình. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể theo phương án tự mình kết nối vào máy chủ xác thực (trong trường hợp này họ cần được sự đồng ý của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) cho phép trở thành Tổ chức sử dung dịch vụ định danh điện tử (ISPA)) hoặc qua một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) hiện hành thực hiện chuyển yêu cầu dịch vụ của mình. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) cũng có thể gửi yêu cầu dịch vụ của các đơn vị khác gọi là "tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA)". Tổ chức sử dung

dịch vụ định danh điện tử (ISCA) có thể đóng vai trò đơn vị tổng hợp để cung cấp dịch vụ xác thực cho các tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) và cũng có thể cung cấp các dịch vụ tạo giá trị gia tăng như xác thực đa bên, báo cáo Hệ thống thông tin quản lý (MIS) và cấp quyền cho các tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA). Tổ chức sử dung dịch vụ định danh điện tử (ISCA) phải ký kết hợp đồng chính thức với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để tiếp cận các dịch vụ định danh điện tử (eID) thuộc phạm vi Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể là:

i. Bảo hiểm Xã hội Việt Nam (VSS) mong muốn xác thực công dân là đối tượng trước khi cung cấp phúc lợi.
ii. Một ngân hàng muốn xác thực khách hàng của mình trước khi cho phép họ thực hiện giao dịch tài chính như rút hoặc chuyển tiền.
iii. Cơ quan quản lý một khu vực bảo mật cao muốn xác thực các cá nhân muốn vào địa điểm đó.
iv. Một trang web thương mại điện tử hoặc mạng xã hội muốn xác thực khách hàng hoặc người đăng ký thuê bao trong quá trình đăng ký.

e. **Tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA).** Một pháp nhân bất kỳ có đăng ký tại Việt Nam mong muốn sử dụng các dịch vụ định danh điện tử (eID) thuộc phạm vi Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể trở thành một Tổ chức sử dung dịch vụ định danh điện tử (ISCA), hoặc có thể truy cập dịch vụ nhận dạng qua một Tổ chức sử dung dịch vụ định danh điện tử (ISCA) hiện hành. Trong trường hợp thứ hai, pháp nhân đó có thể trở thành tổ chức con (sub-ISCA) của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) họ lựa chọn. Tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) không có quan hệ hợp đồng trực tiếp với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Chỉ có Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có quan hệ hợp đồng với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và chịu trách nhiệm về mọi yêu cầu dịch vụ qua tổ chức đó, bao gồm cả các yêu cầu phát sinh từ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA). Tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) có thể là:

i. Bộ ngành của chính phủ đóng tại cấp tỉnh có thể trở thành Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và các đơn vị trực thuộc, cục/vụ của bộ ngành đó có thể tiếp cận các dịch vụ định danh điện tử (eID) với tư

cách là tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA).

ii. Một doanh nghiệp nhỏ như ngân hàng địa phương không muốn tham gia quan hệ hợp đồng chính thức với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), nhưng vẫn cần sử dụng các dịch vụ nhận dạng, có thể lựa chọn trở thành tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA).

iii. Một số đơn vị có thể liên kết với nhau qua một Tổ chức sử dung dịch vụ định danh điện tử (ISCA) duy nhất vì lý do nghiệp vụ, ví dụ, một số khách sạn có thể tiếp cận dịch vụ xác thực định danh điện tử (eID) với tư cách là tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) của một hiệp hội khách sạn đã trở thành Tổ chức sử dung dịch vụ định danh điện tử (ISCA).

f. **Các thiết bị xác thực**. Đó có thể là các thiết bị điện tử đóng vai trò quan trọng trong dịch vụ xác thực định danh điện tử (eID). Các thiết bị này có thể thu thập dữ liệu nhận dạng cá nhân (PID) từ những người có định danh điện tử (eID), chuẩn bị thông tin để truyền di, chuyển gói thông tin xác thực và nhận kết quả về. Đó có thể là những thiết bị tự hoạt động hoặc hoạt động với sự hỗ trợ của nhà điều hành. Các ví dụ về thiết bị xác thực định danh điện tử (eID) có thể là máy tính bàn, máy tính xách tay, ki-ốt, các thiết bị di động cầm tay, v.v. nếu cần, được kết nối với thiết bị sinh trắc để thu thập vân tay và hình ảnh võng mạc. Thiết bị này có thể được vạn hành bởi Tổ chức sử dung dịch vụ định danh điện tử (ISCA)/ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) hoặc đại lý của nó.

g. **Người có nhận dạng điện tử**. Người có định danh điện tử là cá nhân đủ điều kiện bất kỳ đã đăng ký với Bộ Công An (MPS) để được cấp một Mã số định danh công dân (NIN) duy nhất và Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID). Trong bối cảnh xác thực nhận dạng điện tử, người có định danh điện tử thường có quan hệ với Tổ chức sử dung dịch vụ định danh điện tử (ISCA)/ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) với tư cách là khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao hoặc người lao động của tổ chức đó, và với tư cách đó họ được tiếp cận các dịch vụ do Tổ chức sử dung dịch vụ định danh điện tử (ISCA)/ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) cung cấp. Để cho phép họ tiếp cận dịch vụ, định danh điện tử của họ được xác thực qua sử dụng Dữ liệu nhận dạng cá nhân của họ trên cơ sở dữ liệu. Tuỳ theo loại hình xác thực do Tổ chức sử dung dịch vụ

định danh điện tử (ISCA)/ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) sử dụng, người có định danh điện tử có thể phải cung cấp thông tin nhân chủng học và/hoặc nhân trắc học của họ.

2. **Dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC): Các vai trò chính**
    a. **Cơ quan quản lý định danh điện tử Việt Nam.** Trong dịch vụ xác thực nhận dạng điện tử, Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể là cơ quan quản lý nhà nước và cơ quan điều hành dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) và hệ môi trường hỗ trợ. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể quyết định về mô hình tham gia và hoạt động của dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) đồng thời xác định các tiêu chí về điều kiện tham gia của Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) và Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) cũng quyết định về các chuẩn mực và yêu cầu kỹ thuật để các bên tham gia hệ môi trường dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) phải tuân thủ (bao gồm Tổ chức cung cấp dịch vụ định danh điện tử (ISPA), Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA)).
    b. **Nhà cung cấp dịch vụ nhận dạng được quản lý.** Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) có thể thay mặt cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) cung cấp dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC). Các lĩnh vực trách nhiệm chính của Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) có thể bao gồm các hoạt động giao dịch nhận dạng và xác nhận khách hàng điện tử (eKYC) (như nhận yêu cầu xác thực, thực hiện đối chiếu Dữ liệu nhận dạng cá nhân PID) nhận được qua yêu cầu dịch vụ xác thực định danh điện tử và truyền lại kết quả), vận hành mạng lưới, vận hành trung tâm dữ liệu, sử dụng dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC), thoả thuận về mức độ dịch vụ (SLA) với Tổ chức sử dung dịch vụ định danh điện tử (ISCA), nếu có, và giám sát các chỉ tiêu về hoạt động và hiệu quả hoạt động.
    c. **Tổ chức cung cấp dịch vụ nhận dạng điện tử.** Dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) chỉ có thể được truy cập qua mạng an toàn của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).
    d. **Tổ chức sử dung dịch vụ nhận dạng điện tử.** Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể là đơn vị mong muốn sử dụng dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) để cung cấp dịch vụ của mình. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể ký hợp đồng chính thức với Cơ quan quản

lý định danh điện tử Việt Nam (EIDAV) để tiếp cận dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể đảm bảo yêu cầu nhận dạng và xác nhận khách hàng điện tử (eKYC) từ phát ra thiết bị yêu cầu dịch vụ tuân thủ với các chuẩn mực và yêu cầu kỹ thuật do Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và được hoàn tất trước khi chuyển yêu cầu đó cho Tổ chức cung cấp dịch vụ định danh điện tử (ISPA). Để có thêm thông tin chi tiết, đề nghị tham khảo Phụ lục 4.

e. **Tổ chức con của Tổ chức sử dung dịch vụ nhận dạng điện tử.** Một pháp nhân bất kỳ tại Việt Nam muốn sử dụng dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) để cung cấp dịch vụ của mình có thể trở thành một Tổ chức sử dung dịch vụ định danh điện tử (ISCA) hoặc có thể tiếp cận dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) qua một Tổ chức sử dung dịch vụ định danh điện tử (ISCA) hiện hành. Trong trường hợp thứ hai, tổ chức đó đã trở thành một tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) mà nó có quan hệ đối tác cùng.

f. **Các thiết bị dịch vụ nhận dạng điện tử**. Thiết bị định danh điện tử dùng cho dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) cũng có thể là thiết bị dùng cho xác thực nhận dạng điện tử, và cũng có năng lực thu thập thông tin đầu vào cần thiết cho dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC). Thiết bị này có thể tự vận hành và vận hành với sự hỗ trợ của nhà điều hành. Ví dụ về thiết bị dịch vụ định danh điện tử (eID) bao gồm máy tính bàn, máy tích xách tay, ki-ốt, thiết bị di động cầm tay, v.v. được kết nối với thiết bị sinh trắc, nếu cần, để thu thập hình ảnh vân tay và/hoặc võng mạc. Các thiết bị này có thể được vận hành bởi Tổ chức sử dung dịch vụ định danh điện tử (ISCA)/ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) hoặc đại lý của nó.

g. **Người có nhận dạng điện tử.** Trong bối cảnh dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC), người có định danh điện tử (eID) thường là khách hàng/ đối tượng thụ hưởng/ người đăng ký thuê bao hoặc người lao động của Tổ chức sử dung dịch vụ định danh điện tử (ISCA)/ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA), và với tư cách đó muốn được tiếp cận dịch vụ của Tổ chức sử dung dịch vụ định danh điện tử (ISCA)/ tổ chức con của Tổ chức sử dung dịch vụ định danh điện tử (sub-ISCA) đó. Để họ được tiếp cận dịch vụ, họ cần cung cấp dữ liệu nhận dạng và xác nhận khách hàng (KYC) của mình để đăng ký dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC).

Người có định danh điện tử có trách nhiệm đồng ý thực hiện dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC).

3. **Dịch vụ nhận dạng di động: Các vai trò chính**
    a. **Cơ quan quản lý đăng ký**. Cơ quan quản lý đăng ký (RA) thường là nhà điều hành di động quốc doanh như as Viettel, Mobiphone, Vinaphone, v.v. chịu trách nhiệm cung cấp SIM chuyên dụng có tính năng thiết bị tạo chữ ký bảo mật (SSCD) cho công dân tại các điểm cung cấp dịch vụ của họ trên toàn quốc. Nhà điều hành di động phải đăng ký với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để trở thành Cơ quan quản lý đăng ký (RA). Nhà điều hành mạng di đông (MNO) đó có thể làm việc với Bộ Công An (MPS) nhằm cung cấp SIM chuyên dụng.
    b. **Nhà cung cấp dịch vụ tin cậy.** Nhà cung cấp dịch vụ tin cậy (TSP) cũng có thể là Nhà điều hành mạng di động (MNO) chịu trách nhiệm chuyển yêu cầu dịch vụ nhận dạng di động từ Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) vào điện thoại di động của công dân quan mạng di động. Cơ quan này cũng chịu trách nhiệm gửi dữ liệu được ký từ điện thoại di động cho Cơ quan quản lý đăng ký (RA) và phản hồi lại Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) bằng phản hồi xác thực. Nhà điều hành di động đó phải đăng ký với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để trở thành Nhà cung cấp dịch vụ tin cậy (TSP).
    c. **Cơ quan có thẩm quyền chứng nhận**. Cơ quan có thẩm quyền chứng nhận (CA) chịu trách nhiệm cấp chứng nhận; cơ quan này cũng chịu trách nhiệm xác nhận chứng nhận và dữ liệu được ký để phản hồi yêu cầu dịch vụ của Nhà cung cấp dịch vụ tin cậy (TSP). Cơ quan có thẩm quyền chứng nhận (CA) có thể là một cơ quan có thẩm quyền của chính phủ như Cơ quan quản lý xác nhận của Chính phủ Việt Nam (VGCA).
    d. **Cơ quan quản lý định danh điện tử Việt Nam.** Trong trường hợp nhận dạng di động, Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể lưu và quản lý dịch vụ này trên trung tâm dữ liệu của mình và sẽ đăng ký và thuê toàn bộ các đơn vị trong hệ môi trường có các vai trò khác nhau trong việc cung cấp dịch vụ có thể mở rộng.
    e. **Tổ chức sử dung dịch vụ nhận dạng điện tử.** Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể là một đơn vị bất kỳ muốn sử dụng dịch vụ nhận dạng di động để cung cấp dịch vụ của mình Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể sử dụng nhận dạng di động để thực hiện một hoặc nhiều dịch vụ của mình.

f. **Tổ chức cung cấp dịch vụ nhận dạng điện tử.** Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) có thể là đơn vị thiết lập kết nối bảo mật với dịch vụ nhận dạng di động được lưu và quản lý tại các máy chủ tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để thay mặt cho Tổ chức sử dụng dịch vụ định danh điện tử (ISCA) truyền yêu cầu xác thực và nhận phản hồi.

g. **Thiết bị điện thoại di động có SIM chuyên dụng**. Thiết bị điện thoại di động có SIM chuyên dụng do Cơ quan quản lý đăng ký (RA) cấp ra có thể gửi yêu cầu dịch vụ nhận dạng di động từ thiết bị bằng ứng dụng và các mã khoá bảo mật được lưu trên SIM.

h. **Người sử dụng – công dân.** Người sử dụng – công dân có thể là cá nhân đăng ký với Cơ quan quản lý đăng ký (RA) để được nhận SIM chuyên dụng có tính năng thiết bị tạo chữ ký bảo mật (SSCD) và chứng nhận số/sinh trắc được kích hoạt cùng với mã khoá bảo mật trên SIM đó.

6.3 Khuyến nghị về chính sách

Để đảm bảo triển khai thành công Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) tại Việt Nam, cần phải có những chính sách hỗ trợ của quốc gia nhằm tạo điều kiện hình thành một cơ cấu điều hành để có được môi trường thuận lợi. Dưới đây là một số khuyến nghị về can thiệp chính sách.

1. Chính phủ Việt Nam cần cập nhật các chính sách liên quan nhằm cho phép phản hồi nhận dạng và xác nhận khách hàng điện tử (eKYC) cũng có giá trị pháp lý tương tự như tài liệu nhận dạng và xác nhận khách hàng (KYC), tương đương tài liệu nhận dạng và xác nhận khách hàng (KYC) trên giấy để hưởng dịch vụ do các nhà cung cấp dịch vụ cung cấp.

2. Các nhà cung cấp dịch vụ ở cả khu vực chính phủ và khu vực tư nhân như ngân hàng, bảo hiểm, thị trường vốn, viễn thông, khí hoá lỏng, đường sắt, v.v. có thể cập nhật các thông lệ nhận dạng và xác nhận khách hàng (KYC) để chấp nhận cả Mã số định danh công dân (NIN) và định danh điện tử (eID) cũng như phản hồi nhận dạng và xác nhận khách hàng điện tử (eKYC) có giá trị tương đương phản hồi nhận dạng và xác nhận khách hàng (KYC).

3. Chính phủ Việt Nam cần xây dựng chính sách quốc gia hoặc cập nhật chính sách hiện hành về các chuẩn mực dữ liệu và siêu dữ liệu để áp dụng các dạng dữ liệu và siêu dữ

liệu trong các trường dữ liệu nhân chủng học và sinh trắc học của công dân lưu trữ tại cơ sở dữ liệu tập trung về định danh điện tử quốc gia. Cần phải có một chính sách quốc gia về đặc tả kỹ thuật nhận dạng và xác thực cư dân (KYR) tuân thủ với các chuẩn mực về dữ liệu và siêu dữ liệu đó.

4. Các chính sách hiện hành của quốc gia về áp dụng các chuẩn mở nhằm đẩy mạnh khả năng tác nghiệp liên thông có thể được cập nhật để áp dụng cho định dạng dữ liệu định danh điện tử (eID). Chính sách này có thể bao gồm các chuẩn mực về dữ liệu sinh trắc như hình ảnh vân tay, dấu vân tay và hình ảnh võng mạc.

5. Chính sách quốc gia hiện hành về Luật chữ ký số (DSA) cần được rà soát và cập nhật, nếu cần để quy định về sử dụng chứng nhận số hoặc sinh trắc trong Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) trên cơ sở những khuyến nghị kỹ thuật được bàn ở phần trên trong chương này. Thông thường, chữ ký số và chữ ký viết cần có giá trị tương đương ở cả khu vực công và khu vực tư. Luật chữ ký số (DSA) cần đảm bảo mỗi chữ ký số phải nhận dạng được người ký duy nhất, ràng buộc được cá nhân đó với dữ liệu đã ký, và đảm bảo dữ liệu đã ký không bị can thiệp ngược nếu không làm cho chữ ký đó bị mất hiệu lực.

6. Luật chữ ký số có thể quy định các yêu cầu chặt chẽ về thủ tục và tài chính để đảm bảo Nhà cung cấp dịch vụ xác nhận (CSP) và Nhà cung cấp dịch vụ dấu thời gian (TSP) được thành lập và quản lý đầy đủ để thực thi các chức năng của họ với các chuẩn mực cao nhất có thể.

7. Chính sách hiện hành của quốc gia về bảo mật CNTT có thẻ được cập nhật để đề ra những yêu cầu vè an ninh bảo mật cho định danh điện tử (eID) và Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) như đã nêu tại các khuyến nghị về kỹ thuật và thể chế được thảo luận ở phần trên trong chương này.

8. Luật bảo vệ dữ liệu cá nhân (PDPA) có thể quy định về việc các tổ chức và đơn vị thuộc khu vực công và tư nhân sử dụng dữ liệu cá nhân và các cơ sở dữ liệu có chứa các thông tin cá nhân. Cần phải có một cơ quan thanh tra độc lập về bảo vệ dữ liệu ngoài chính phủ, nhằm đảm bảo đáp ứng các yêu cầu và thực thi hiệu lực tuân thủ Luật nếu cần. Cơ quan này sẽ báo cáo cho cơ quan cao nhất thuộc Văn phòng Thủ tướng. Yêu cầu của các bên thứ ba (v.d. đại diện của chính quyền) về dữ liệu cá nhân cần được ghi lại và bản ghi

phải được công khai trực tuyến cho cá nhân đó theo yêu cầu qua cổng thông tin dành cho công dân.

9. Công nghệ dựa trên chuẩn mở khi triển khai chính phủ điện tử cần được khuyến khích sử dụng qua chính sách của quốc gia về chuẩn mở. Đó có thể là các đặc tả kỹ thuật về tiêu chuẩn áp dụng cho các thiết bị sinh trắc, danh mục các nhà cung cấp thiết bị sinh trắc được phê duyệt và đặc tả kỹ thuật chuẩn cho đường truyền thuê bao chuyên dụng áp dụng cho Tổ chức cung cấp dịch vụ định danh điện tử (ISPA), v.v.

10. Chính phủ Việt Nam có thể thông qua Luật về tài liệu chứng minh nhận dạng (IDA) quy định về những hướng dẫn của quốc gia trong việc hình thành Mã số định danh công dân (NIN) bắt buộc, Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID) và định danh điện tử (eID) cho các công dân trong nước. Luật cũng có thể quy định rằng định danh điện tử (eID) có thể có giá trị pháp lý tương tự như Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID). Luật có thể quy định về mục đích sử dụng thẻ và mã số về mặt chứng minh tư cách công dân. Luật có thể quy định rằng dữ liệu sinh trắc và nhân chủng học đã được xử lý và loại bỏ trùng lặp được sử dụng để cá nhân hoá thẻ đó cũng có thể được nhập vào đăng ký dân số của quốc gia theo Luật về đăng ký dân số. Có thể cần có quy định pháp lý dưới dạng nghị định về chuyển dữ liệu công dân từ Bộ Công An (MPS) sang Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) và các dịch vụ định danh điện tử (eID) trên cơ sở định kỳ.

11. Chính phủ Việt Nam có thể tiến hành đăng ký công dân cho chương trình nhận dạng quốc gia mới và cung cấp mã số nhận dạng quốc gia cho tất cả các công dân. Điều này có thể giúp sớm thí điểm sử dụng định danh điện tử (eID) dưới hình thức định danh điện tử (eID) dựa trên dữ liệu công dân thu thập từ chương trình nhận dạng quốc gia.

6.4 Khuyến nghị về chiến lược truyền thông

Chiến lược truyền thông có thể bao gồm các bước được thực hiện để nâng cao nhận thức và thúc đẩy việc áp dụng khuôn khổ giữa các bên liên quan chính; như các nhà cung cấp dịch vụ ở khu vực công và tư nhân cũng như công dân Việt Nam. Sau đây là một số khuyến nghị về chiến lược truyền thông.

1. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể thiết lập một cổng thông tin công cộng để nâng cao nhận thức cho các bên liên quan trong hệ môi trường định danh điện tử (eID) và hỗ trợ cho người sử dụng các dịch vụ xác thực định danh điện tử (eID) bằng cách công bố các tài liệu liên quan đến các giải pháp kỹ thuật và các bản cập nhật.

2. Cần phải có các chương trình nâng cao năng lực dưới hình thức đào tạo trực tuyến và trên lớp dành cho công dân và các cán bộ/ đơn vị điều hành ở cả chính phủ và khu vực tư nhân.

3. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể công bố hệ thống các tài liệu kỹ thuật dành cho các bên liên quan có chuyên môn kỹ thuật trong hệ môi trường xác thực nhận dạng điện tử, có thể gồm những người có thẩm quyền quyết định về mặt kỹ thuật, các kỹ sư kỹ thuật và cán bộ phát triển tại Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), và các nhà cung cấp dịch vụ khác chịu trách nhiệm về thiết kế, phát triển và duy trì hệ thống xác thực định danh điện tử (eID).

4. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) cũng có thể công bố một bộ tài liệu dành cho các chuyên gia phần mềm làm việc trong lĩnh vực công nghệ như những người có thẩm quyền quyết định về mặt kỹ thuật, các kỹ sư kỹ thuật, các nhà phát triển tại các cơ quan của chính phủ và nhà cung cấp dịch vụ khu vực tư nhân quan tâm đến việc lồng ghép các dịch vụ xác thực định danh điện tử (eID) trong các ứng dụng của họ. Một ví dụ về tài liệu kỹ thuật có thể là đặc tả kỹ thuật giao diện lập trình ứng dụng (hàm API) cho các dịch vụ xác thực hiện dạng điện tử (eID).

5. Để cải thiện việc các nhà cung cấp áp dụng các dịch vụ định danh điện tử (eID) thuộc Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) trong chính phủ và trong khu vực tư nhân, Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể thiết lập môi trường phát triển và kiểm thử dưới hình thức URL công khai (ví dụ, https://auth.eidav.gov.vn) mà các chuyên gia phát triển phần mềm của các tổ chức cung cấp dịch vụ có thể truy cập qua internet và và sử dụng khi xây dựng các ứng dụng liên quan.

6. Để cải thiện việc các nhà cung cấp áp dụng các dịch vụ định danh điện tử (eID) thuộc Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) như xác thực định danh điện tử (eID), Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể triển khai tham khảo một thư viện khách hàng xác thực định danh điện tử nhằm đóng góp và mã hoá các gói

dữ liệu xác thực theo các ngôn ngữ lập trình khác nhau. Ta có thể tạo cơ chế để khuyến khích xây dựng những ràng buộc về nguôn ngữ lập trình khác trong số các thành viên của cộng đồng lập trình phần mềm để trình lên Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Các chuyên gia phát triển có thể tải những thư viên đó cùng với các mã khoá công khai của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), tất cả đều có chữ ký số của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để sử dụng cho ứng dụng của họ.

7. Chính phủ Việt Nam có thể triển khai các chiến dịch nâng cao nhận thức trong số các nhà cung cấp dịch vụ của chính phủ và khu vực tư nhân nhằm tận dụng lợi ích của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) trong các quy trình nghiệp vụ của họ.

8. Các chiến dịch nâng cao nhận thức, xúc tiến và khuyến khích và người sử dụng sớm, cá nhân các công dân và các tổ chức thuộc khu vực tư nhân có thể được hoạch định hoặc tổ chức nhằm cải thiện áp dụng nhận dạng quốc gia. Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) có thể cung cấp miễn phí các dịch vụ định danh điện tử (eID) cho các nhà cung cấp dịch vụ trong giai đoạn thí điểm để khuyến khích họ sử dụng dịch vụ.

6.5 Khuyến nghị về triển khai thí điểm

Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) tại Việt Nam có thể được triển khai theo hai giai đoạn: giai đoạn thí điểm và triển khai rộng đầy đủ. Dưới đây là một số khuyến nghị về giai đoạn triển khai thí điểm.

1. **Hệ thống cung cấp dịch vụ định danh điện tử**
    a. Thành lập Cơ quan quản lý định danh điện tử Việt Nam (EIDAV): Thành lập một cơ quan độc lập trong chính phủ để tạo định danh điện tử (eID), cung cấp và duy trì các dịch vụ định danh điện tử (eID) thuộc Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF).
    b. Khởi tạo quy trình lưu trữ tập trung dữ liệu nhận dạng công dân và cập nhật định kỳ.
        i. Thay vì thu thập lại Dữ liệu nhận dang cá nhân (PID) của công dân cho Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS), khuyến nghị đưa ra là sử dụng lại Dữ liệu nhận dang cá nhân (PID) đã được thu thập và xử lý để tạo Mã số định danh công dân (NIN) duy nhất

và Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID) của Bộ Công An (MPS).

ii. Có thể có cần phải có yêu cầu pháp lý dưới hình thức một nghị định về chuyển dữ liệu công dân từ Bộ Công An (MPS) sang Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) tại Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để triển khai các dịch vụ định danh điện tử (eID) thuộc Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF).

iii. Dữ liệu nhận dạng cá nhân (PID) lưu trữ tại Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) có thể là dữ liệu sinh trắc và nhân chủng học của công dân.

iv. Dữ liệu mới về công dân có thể được chuyển tải định kỳ từ Bộ Công An (MPS) sang Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) mỗi khi Bộ đó đăng ký cho công dân mới cho đến khi toàn bộ công dân đã được cấp Mã số định danh công dân (NIN) và Thẻ chứng minh của Hệ thống định danh điện tử quốc gia (NID).

v. Một khuyến nghị nữa có thể là áp dụng mô hình vận hành bảo mật để chuyển tải thông tin cập nhật trong cơ sở dữ liệu về công cân của Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) và Bộ Công An (MPS), chẳng hạn khi có thay đổi về địa chỉ, v.v. trên cơ sở thường xuyên.

c. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) sẽ thành lập trung dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) dựa trên các khuyến nghị kỹ thuật về Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) như đã bàn ở chương này.

d. Bộ Thông tin và Truyền thông (MIC) về phần mình sẽ thiết lập trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) theo các khuyến nghị kỹ thuật về Hệ thống cung cấp dịch vụ định danh điện tử (EISDP) như đã thảo luận tại phần trên trong chương này.

e. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể thiết lập quy trình đăng ký cho các Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và Tổ chức sử dung dịch vụ định danh điện tử (ISCA) trên cổng thông tin công khai của họ. Các nhà điều hành viễn thông quốc gia tại Việt Nam có đủ năng lực thiết lập kết nối bảo mật chuyên dụng vào trung tâm của Cơ quan Quản lý Nhận dạng Quốc gia Việt Nam (NIDAV). Cơ quan Quản lý Nhận dạng Quốc gia Việt Nam (NIDAV) có thể lựa chọn Tập đoàn Viettel và/hoặc VNPT để đảm nhiệm vai trò Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) trong giai đoạn thí điểm.

2. **Dịch vụ xác thực định danh điện tử**

   a. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) với tư cách là Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP), chịu trách nhiệm thiết kế và triển khai dịch vụ xác thực định danh điện tử (eID) sau đó lưu và quản lý dịch vụ đó tại trung tâm dữ liệu của mình trên Hệ thống cung cấp dịch vụ định danh điện tử (EISDP). Cơ quan này cũng có thể triển khai quy trình đăng ký dịch vụ xác thực định danh điện tử (eID) trên cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

   b. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể thuê nhà thầu tích hợp giải pháp (SI) triển khai dịch vụ qua đấu thầu.

   c. Các nhà cung cấp dịch vụ thuộc các tổ chức của chính phủ và khu vực tư nhân có thể đăng ký với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) trên cổng thông tin công cộng để sử dụng dịch vụ xác thực định danh điện tử (eID). Sau khi được Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) phê duyệt, các nhà cung cấp dịch vụ đó có thể cài đặt giao diện lập trình ứng dụng (API) dịch vụ xác thực định danh điện tử (eID) trên ứng dụng cung cấp dịch vụ của họ bằng thiết bị tại điểm cung cấp của họ theo những hướng dẫn do Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) cung cấp. Sau đó việc thiết lập phần cứng, phần mềm, quy trình và mạng sẽ được thực hiện.

   d. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) sẽ cập nhật các chính sách CNTT tại Việt Nam để cho phép thực hiện dịch vụ xác thực định danh điện tử để các nhà cung cấp dịch vụ có thể sử dụng như một công cụ được chấp nhận về xác nhận nhận dạng.

   e. Để khuyến khích sử dụng dịch vụ, cơ quan này có thể cung cấp dịch vụ miễn phí cho các nhà cung cấp dịch vụ.

   f. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể xây dựng những chiến dịch nâng cao nhận thức cho công dân và các nhà cung cấp dịch vụ. Có thể sẽ có những chương trình nâng cao năng lực qua các khoá tập huấn trực tuyến và trên lớp học nhằm vào công dân và các cán bộ nhà nước/ đơn vị điều hành trong chính phủ và khu vực tư nhân. Có thể cần phải có các chương trình đào tạo phát triển phần mềm nhằm vào cộng đồng các chuyên gia phát triển tại các tổ chức cung cấp dịch vụ.

3. **Dịch vụ tạo nguồn thông tin nhận dạng điện tử**

a. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể cung cấp tiện ích tạo nguồn thông tin ngoại tuyến, Hệ thống tạo nguồn dữ liệu định danh điện tử (eSP) và quy trình đăng ký trên cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), bằng cách phân công cho một nhà thầu tích hợp hệ thống qua quy trình đấu thầu.
b. Chính phủ, cùng với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), có thể lựa chọn một nhà cung cấp dịch vụ từ chính phủ và khu vực tư nhân để triển khai thí điểm dịch vụ tạo nguồn thông tin định danh điện tử (eID). Các tổ chức khu vực công và tư nhân được lựa chọn thí điểm có thể là Bảo hiểm Xã hội Việt Nam và VNTP hoặc Viettel.
c. Các nhà cung cấp dịch vụ được lựa chọn có thể chuẩn bị cơ sở dữ liệu cho phép sử dụng dịch vụ bằng cách thực hiện số hoá và tập trung hoá dữ liệu.
d. Các nhà cung cấp dịch vụ lựa chọn có thể đăng ký là Tổ chức sử dung dịch vụ định danh điện tử (ISCA) bằng cách tuân thủ theo quy trình đăng ký do Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) công bố trên cổng thông tin công cộng của họ
e. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) cũng có thể đăng ký tải tiện ích tạo nguòn thông tin về và yêu cầu truy cập vào Hệ thống tạo nguồn dữ liệu định danh điện tử (eSP). Họ cũng có thể đưa ra phương án tải nhập cơ sở dữ liệu cho phép sử dụng dịch vụ hoặc cung cấp các chi tiết dịch vụ web vào thời điểm đăng ký.
f. Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thê rtrieern khai chiến lược lựa chọn để tạo nguồn thông tin bằng cách xây dựng các chương trình thu thập dữ liệu. Sau khi hoàn thành tạo nguồn thông tin, Tổ chức sử dung dịch vụ định danh điện tử (ISCA) có thể thực hiện việc xác nhận tạo nguồn thông tin bằng Hệ thống tạo nguồn dữ liệu định danh điện tử (eSP), tiện ích tạo nguồn thông tin và đẩy cơ sở dữ liệu cho phép sử dụng dịch vụ lên máy chủ của họ tại trung tâm dữ liệu của họ.

4. **Dịch vụ nhận dạng và xác nhận khách hàng điện tử**
   a. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có trách nhiệm thiết kế và triển khai dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) cho Bộ Thông tin và Truyền thông (MIC) đồng thời lưu và quản lý dịch vụ tại trung tâm dữ liệu của mình thuộc Hệ thống cung cấp dịch vụ định danh điện tử (EISDP). Cơ quan này cũng có thể cung cấp quy trình đăng ký dịch vụ nhận dạng và xác nhận

khách hàng điện tử (eKYC) trên cổng thông tin công cộng của Cơ quan Quản lý Nhận dạng Quốc gia Việt Nam (NIDAV).

b. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể thuê nhà thầu tích hợp hệ thống, được lựa chọn qua quy trình đấu thầu, để triển khai dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC).

c. Nhà cung cấp dịch vụ được lựa chọn có thể đăng ký dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) trên cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Sau khi được Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) phê duyệt, các nhà cung cấp dịch vụ đó có thể cài đặt dịch vụ nhận dạng và xác nhận khách hàng điện tử (eKYC) trên ứng dụng của họ theo hướng dẫn của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Lúc này, việc thiết lập phần cứng, phần mềm, quy trình và mạng có thể được thực hiện.

d. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) sẽ cập nhật về chính sách CNTT tại Việt Nam nhằm cho phép phản hồi nhận dạng và xác nhận khách hàng điện tử (eKYC) được coi là tài liệu nhận dạng và xác nhận khách hàng (KYC) hợp pháp và hợp lệ, tương đương với phiên bản trên giấy.

e. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể phối hợp với các cơ quan khác của chính phủ như Bảo hiểm Xã hội Việt Nam (VSS), Bộ Lao động Thương binh và Xã hội (MoLISA), Bộ Môi trường (MoE), Bộ Tài chính (MoF) và các tổ chức thuộc khu vực tư nhân như Ngân hàng Việt Nam (BoV), Viettel, v.v. để cập nhật các thông lệ nhận dạng và xác nhận khách hàng (KYC) của họ sao cho Mã số định danh công dân (NIN) và phản hồi nhận dạng và xác nhận khách hàng điện tử (eKYC) được coi là tài liệu nhận dạng và xác nhận khách hàng (KYC) hợp lệ.

f. Để khuyến khích sử dụng dịchv ụ, cơ quan này có thể cung cấp dịch vụ miễn phí cho các nhà cung cấp dịch vụ.

5. **Dịch vụ nhận dạng di động**

a. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có trách nhiệm thiết kế và triển khai dịch vụ nhận dạng di động, và lưu và quản lý dịch vụ đó trên trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) thuộc Hệ thống cung cấp dịch vụ định danh điện tử (EISDP).

b. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể phân công việc triển khai và vận hành các dịch vụ nhận dạng di động cho các nhà điều hành viễn thông trong nước như Viettel và VNPT.

c. Nhà điều hành viễn thông được lựa chọn có thể tận dụng các nhà sản xuất SIM hiện hành của họ để hình thành các SIM nhận dạng di động mới theo các yêu cầu kỹ thuật được cung cấp.
d. Nhà điều hành viễn thông có thể thiết lập các cơ sở hạ tầng cần thiết tại các điểm bán lẻ của họ để cung cấp SIM nhằm thực hiện vai trò của Tổ chức quản lý đăng ký (RA) dịch vụ nhận dạng di động.
e. Nhà điều hành viễn thông có thể đào tạo cho công dân về đăng ký sử dụng và kích hoạt nhận dạng di động của mình đồng thời sử dụng điện thoại di động để xác thực định danh điện tử (eID).
f. Nhà điều hành viễn thông có thể triển khai quy trình cung cấp chứng nhận số của Cơ quan quản lý xác nhận của Chính phủ Việt Nam (VGCA). Cơ quan quản lý xác nhận của Chính phủ Việt Nam (VGCA) cũng có thể cung cấp dịch vụ giao thức kiểm tra chứng thực trực tuyến (OCSP) để xác nhận chứng nhận số là hợp lệ vào thời điểm xác thực nhận dạng bằng dịch vụ nhận dạng di động.
g. Nhà cung cấp dịch vụ muốn sử dụng nhận dạng di động theo cơ chế xác thực định danh điện tử (eID) cần cập nhật ứng dụng cung cấp dịch vụ của mình để sử dụng dịch vụ nhận dạng di động. Nhà điều hành viễn thông có thể hỗ trợ cho nhà cung cấp dịch vụ đó cài đặt dịch vụ nhận dạng di động trong ứng dụng cung cấp dịch vụ của họ.
h. Nhà cung cấp dịch vụ đó có thể đào tạo trực tuyến và ngoại tuyến cho khách hàng cuối cùng nhằm sử dụng nhận dạng di động để xác nhận nhận dạng hợp lệ của khách hàng.
i. Nhà điều hành di động có thể thiết lập các cơ sở hạ tầng kỹ thuật cần thiết trong các trung tâm dữ liệu của mình như được trình bày tại các khuyến nghị kỹ thuật về dịch vụ nhận dạng di động.

7.0 Dự trù kinh phí

7.1 Cơ sở lập dự trù kinh phí

Dự trù kinh phí nhằm thiết kế và triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) bao gồm kinh phí cho dự án thí điểm ban đầu và giai đoạn triển khai đầy đủ khuôn khổ đó trên toàn quốc. Dự trù kinh phí tổng thể nhằm triển khai tầm nhìn của khuôn khổ được lập dựa trên thông tin của Chính phủ Việt Nam và đề xuất về cơ cấu khu vực tư nhân. Bản dự trù này được lập dựa trên phương pháp ước tính chỉ số đầu tư trung bình. Phương pháp này tận dụng dự trù kinh phí của các dự án đại diện tiêu biểu của rất nhiều các dự án tương tự để ước tính ra quy mô đầu tư tiêu biểu cho dự án để trên cơ sở đó dự toán kinh phí và tổng mức đầu tư cho dự án. Dự trù kinh phí được cung cấp ở đây chỉ mang tính hướng dẫn và không nhất thiết được dùng cho mục đích lập dự toán. Tuy nhiên, thông tin này có thể giúp Chính phủ Việt Nam và các cơ quan triển khai nắm được khả năng về quy mô đầu tư cần thiết cho việc thiết kế và triển khai khuôn khổ đó. Cần phải đánh giá nghiên cứu thêm để có thể đưa ra ước tính chính xác trên cơ sở các chi tiết về triển khai cùng với hiểu biết về cơ cấu hiện tại và nhu cầu nâng cao năng lực để triển khai khuôn khổ đó.

7.2 Chi tiết kinh phí

Bản dự trù kinh phí này bao gồm thiết kế, triển khai, vận hành cơ sở hạ tầng tập trung của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Dự trù kinh phí về nhận dạng di động, Tổ chức quản lý đăng ký (RA), và các Nhà cung cấp dịch vụ tin cậy (TSP) cũng được đưa ra để triển khai lựa chọn về dịch vụ nhận dạng di động. Bản dự trù này bao gồm chi phí cơ sở hạ tầng vật chất (xây dựng các toà nhà mới, điện, nước, đồ đạc) và cơ sở hạ tầng CNTT (phần cứng, phần mềm, thiết bị mạng). Nội dung thứ hai còn ban gồm thiết kế và phát triển các ứng dụng phần mềm, xây dựng các chuẩn mực và quy trình hoạt động. Bên cạnh phần cơ sở hạ tầng, kinh phí còn phải bao gồm cả lương cho cá bộ và chương trình xây dựng năng lực cho tất cả các bên liên quan trong hệ môi trường đó. Chi phí vận hành còn bao gồm kinh phí vận hành và duy trì cơ sở hạ tầng đó và cơ cấu thể chế trong giai đoạn một năm thí điểm và năm năm triển khai rộng trên toàn quốc.

Dự án sẽ được triển khai theo hai giai đoạn. Giai đoạn thứ nhất là giai đoạn thí điểm, tiếp theo là giai đoạn triển khai rộng đầy đủ.

7.2.1 Dự trù kinh phí cho giai đoạn thí điểm không bao gồm triển khai nhận dạng di động

Dự trù kinh phí cho giai đoạn thí điểm bao gồm thiết lập và triển khai các cơ sở hạ tầng thể chế và CNTT cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) và hai Tổ chức sử dung dịch vụ định danh điện tử (ISPA). Mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) sẽ tổ chức một điểm cung cấp dịch vụ tại một quận tại Hà Nội. Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) được lựa chọn thí điểm có thể là Viettel hoặc Tập đoàn Bưu chính Viễn thông Việt Nam (VNPT), và Tổ chức sử dung dịch vụ định danh điện tử (ISCA) là Viettel hoặc VNPT và Bảo hiểm Xã hội Việt Nam (VSS). Tổ chức quản lý đăng ký (RA) và Nhà cung cấp dịch vụ tin cậy có thể là Viettel hoặc VNPT. Dữ liệu sinh trắc và nhân chủng học của công dân được lưu giữ tại Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) sẽ được tải nhập từ cơ sở dữ liệu về công dân do Bộ Công An (MPS) thu thập trong hoạt động nhận dạng quốc gia thí điểm của họ. Giả định ở đây là dữ liệu công dân do Bộ Công An (MPS) thu thập trong hoạt động nhận dạng quốc gia thí điểm của họ hiện có tối thiểu một triệu công dân. Chi tiết dự trù kinh phí giai đoạn thí điểm được trình bày trong bảng dưới đây.

Particulars	Capital Budget (K USD)	Operating Budget (K USD)
EIDAV Data Center (A1)	$20,966.00	$3,144.90
EIDAV Disaster Recovery Center (A2)	$16,263.00	$2,439.45
Geographical Data Backup Center (A3)	$610.00	$91.50
MPS Data Migration (A4)	$1,100.00	$165.00
EIDAV IT and Institutional Infrastructure (A=A1+A2+A3+A4)	**$38,939.00**	**$5,840.85**
ISPA Data Center (B1)	$5,554.50	$833.18
ISPA IT and Institutional Infrastructure (B=B1)	**$5,554.50**	**$833.18**
ISCA Data Center (C1)	$2,437.40	$365.61
ISCA Service Delivery Outlets (C2)	$29.18	$4.38
ISCA IT and Institutional Infrastructure (C=C1+C2)	**$2,466.58**	**$369.99**
Awareness, Trainings and Capacity Building (D)	**$100.00**	**$0.00**
National IT Standards and Policies (E)	**$100.00**	**$0.00**
Total Budget = (J = A+B+C+D+E)	**$47,160.08**	**$7,044.02**
Total (Capital + Operating Budget)	**$54,204.10**	

Bảng 1: Chi tiết dự trù kinh phí giai đoạn thí điểm

Như được trình bày ở bảng trên, tổng mức đầu tư cho giai đoạn thí điểm được dự trù ở mức **54,2 triệu USD**. Số này bao gồm chi phí đầu tư là **47,16 triệu USD** và chi phí vận hành là **7,04 triệu USD** trong năm đầu tiên.

Dưới đây là mô tả chi tiết dự trù kinh phí đầu tư trong giai đoạn thí điểm.

1. **Cơ sở hạ tầng thể chế và CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).** Dự trù kinh phí để thiết kế và triển khai cơ sở hạ tầng thể chế, CNTT, vật chất tập trung là **38,94 triệu USD**. Số này bao gồm thiết kế và triển khai trung tâm dữ liệu tập trung, trung tâm phục hồi thảm hoạ và trung tâm sao lưu dữ liệu địa lý của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Dự trù kinh phí cho mỗi trung tâm dữ liệu bao gồm toà nhà vật lý, nội thất, điện, nước, đồ đạc; thiết lập hạ tầng CNTT như phần cứng, phần mềm và thiết bị mạnh. Số này cũng bao gồm chi phí thiết lập cơ sở hạ tầng CNTT giữa trung tâm dữ liệu của Bộ Công An (MPS) và của Cơ quan quản lý định danh

điện tử Việt Nam (EIDAV) để chuyển dữ liệu về công dân từ Bộ Công An (MPS) sang trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

2. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).** Dự trù kinh phí để thiết kế và triển khai trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) tại Viettel/VNPT là **5,56 triệu USD**. Số này bao gồm thiết kế và triển khai trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA). Dự trù kinh phí để thiết lập trung tâm dữ liệu cho Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) bao gồm thiết kế và triển khai cơ sở hạ tầng CNTT (phần cứng, phần mềm, mạng), mua sắm hạ tầng CNTT tuân thủ theo yêu cầu thiết kế và đặc tả kỹ thuật CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

   Cơ sở hạ tầng thể chế và CNTT của Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Dự trù kinh phí nhằm thiết kế và triển khai trung tâm dữ liệu của hai Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và một điểm cung cấp dịch vụ cho mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) tại Viettel/VNPT và Bảo hiểm Xã hội Việt Nam (VSS) là **2,47 triệu USD**. Số này bao gồm thiết kế và triển khai các trung tâm dữ liệu và điểm cung cấp dịch vụ tại mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Dự trù kinh phí để thiết lập trung tâm dữ liệu và điểm cung cấp dịch vụ bao gồm thiết kế, kiến trúc và triển khai cơ sở hạ tầng CNTT theo thiết kế và đặc tả kỹ thuật CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Số này cũng bao gồm thiết kế, phát triển và triển khai các ứng dụng máy thanh toán tiền bằng thẻ (máy PoS), tuỳ chỉnh ứng dụng máy thanh toán tiền bằng thẻ hiện hành để tích hợp với các dịch vụ nhận dạng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), tạo nguồn thông tin Mã số định danh công dân (NIN) trên cơ sở dữ liệu của các ứng dụng máy thanh toán tiền bằng thẻ (PoS) và lĩnh vực nghiệp vụ (LoB) hiện hành.

3. **Nâng cao nhận thức, đào tạo và nâng cao năng lực.** Dự trù kinh phí bao gồm đào tạo nâng cao năng lực cho toàn bộ các bên liên quan trong hệ môi trường, đào tạo kỹ thuật và quy trình cho các bên liên quan, các chương trình nâng cao nhận thức, đào tạo trực tiếp và trực tuyến cho công dân và người sử dụng nhận dạng di động và các dịch vụ nhận dạng khác của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Dự trù kinh phí về nâng cao nhận thức, đào tạo và nâng cao năng lực là **100.000 USD.**

4. **Chuẩn mực và chính sách CNTT quốc gia**. Dự trù kinh phí để thiết lập các uỷ ban của chính phủ và khu vực tư nhân để xây dựng và thông qua các chính sách của chính phủ và chuẩn mực CNTT là **100.000 USD**.

Dưới đây là chi tiết dự trù kinh phí hoạt động trong giai đoạn thí điểm.

1. **Cơ sở hạ tầng thể chế và CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).** Dự trù kinh phí để vận hành cơ sở hạ tầng vật chất, CNTT và thể chế tập trung trong một năm là **5,84 triệu USD**. Số này bao gồm vận hành và duy trì cơ sở hạ tầng vật chất nhu tiền điện, nước hàng tháng, sửa chữa và lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm, thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu, trung tâm phục hồi thảm hoạ và trung tâm sao lưu dữ liệu. Ngoài ra, số này còn bao gồm chi phí liên tục chuyển và quản lý dữ liệu từ Bộ Công An (MPS) sang trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

2. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).** Dự trù kinh phí để vận hành cơ sở hạ tầng vật chất, CNTT và thể chế của trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) trong một năm là **833.180 USD**. Số này bao gồm vận hành và duy tu bảo dưỡng cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa và lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm, thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu.

   Cơ sở hạ tầng thể chế và CNTT của Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Dự trù kinh phí để vận hành cơ sở hạ tầng vật chất, CNTT và thể chế của trung tâm dữ liệu trong một năm là **369.990 USD**. Số này bao gồm vận hành và duy tu bảo dưỡng cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa và lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm, thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu và cán bộ cung cấp dịch vụ tại điểm cung cấp.

7.2.2 Dự trù kinh phí triển khai phương án lựa chọn về nhận dạng di động trong giai đoạn thí điểm

Dự trù kinh phí để triển khai phương án lựa chọn về nhận dạng di động trong giai đoạn thí điểm được trình bày dưới đây. Dự trù kinh phí này được lập dựa trên triển khai rộng 10.000 nhận dạng di động, một Tổ chức quản lý đăng ký (RA) và một Nhà cung cấp dịch vụ tin cậy (TSP) trong giai đoạn thí điểm.

Chi tiết dự trù kinh phí đầu tư và vận hành để triển khai phương án tuỳ chọn là nhận dạng di động trong giai đoạn thí điểm được trình bày trong bảng dưới đây.

Particulars	Capital Budget (K USD)	Operating Budget (K USD)
RA Data Center (D1)	$2,218.70	$332.81
RA Service Delivery Outlets (D2)	$14.59	$2.19
SIM Provision (D3)	$50.00	$0.00
RA IT and Institutional Infrastructure (D=D1+D2+D3)	**$2,283.29**	**$335.00**
TSP Data Center (E1)	$1,903.70	$285.56
TSP IT and Institutional Infrastructure (E=E1)	**$1,903.70**	**$285.56**
Total Budget = (K = D+E)	**$4,186.99**	**$620.56**
Total (Capital + Operating Budget)	**$4,807.55**	

Bảng 2: Chi tiết dự trù kinh phí triển khai nhận dạng di động trong giai đoạn thí điểm

Như trình bày ở bảng trên, tổng mức đầu tư để triển khai phương án tuỳ chọn là nhận dạng di động trong giai đoạn thí điểm được dự trù ở mức **4,81 triệu USD**. Số này gồm kinh phí đầu tư là **4,19 triệu USD** và kinh phí vận hành là **620.000** trong năm đầu tiên.

Dưới đây là chi tiết dự trù kinh phí đầu tư để triển khai phương án tuỳ chọn là nhận dạng di động trong giai đoạn thí điểm.

1. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức quản lý đăng ký (RA).** Dự trù kinh phí để thiết kế và triển khai trung tâm dữ liệu của Tổ chức quản lý đăng ký (RA) và một điểm cung cấp dịch vụ của Viettel/VNPT là **2,28 triệu USD**. Số này bao gồm thiết kế và triển khai trung tâm dữ liệu và điểm cung cấp dịch vụ của Tổ chức quản lý đăng ký (RA). Dự trù kinh phí này để thiết lập trung tâm dữ liệu và điểm cung cấp dịch vụ bao gồm thiết kế, kiến trúc và triển khai cơ sở hạ tầng CNTT tuân thủ theo thiết kế và đặc tả kỹ thuật CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Số này còn bao gồm thiết kế, phát triển và triển khai các ứng dụng máy thanh toán tiền bằng thẻ (Máy PoS), tuỳ chỉnh các ứng dụng máy thanh toán tiền bằng thẻ hiện hành để cung cấp SIM nhận

dạng di động (giả sử là sử dụng thẻ SIM), kích hoạt chứng nhận số hoặc sinh trắc và tạo nguồn thông tin Mã số định danh công dân (NIN) trên cơ sở dữ liệu công dân của nhà cung cấp dịch vụ.

2. **Cơ sở hạ tầng thể chế và CNTT của Nhà cung cấp dịch vụ tin cậy (TSP).** Dự trù kinh phí để thiết kế và triển khai trung tâm dữ liệu của Nhà cung cấp dịch vụ tin cậy (TSP) tại Viettel/VNPT là **1,90 triệu USD**. Dự trù kinh phí để thiết lập trung tâm dữ liệu và điểm cung cấp dịch vụ bao gồm thiết kế, kiến trúc và triển khai cơ sở hạ tầng CNTT tuân thủ theo thiết kế và đặc tả kỹ thuật CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

Dưới đây là chi tiết dự trù kinh phí hoạt động để triển khai phương án tuỳ chọn là nhận dạng di động trong giai đoạn thí điểm

1. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức quản lý đăng ký (RA).** Dự trù kinh phí để vận hành cơ sở hạ tầng vật lý, CNTT, thể chế của trung tâm dữ liệu và điểm cung cấp dịch vụ trong một năm là **334.990 USD**. Số này bao gồm vận hành và duy tu bảo dưỡng cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa và lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm, thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu và cán bộ cung cấp dịch vụ tại các điểm cung cấp.

2. **Cơ sở hạ tầng thể chế và CNTT của Nhà cung cấp dịch vụ tin cậy (TSP).** Dự trù kinh phí để vận hành cơ sở hạ tầng vật lý, CNTT, thể chế của trung tâm dữ liệu trong một năm là **285.560 USD**. Số này bao gồm vận hành và duy tu bảo dưỡng cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa và lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm, thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu.

7.2.3 Dự trù ngân sách cho giai đoạn triển khai rộng đầy đủ không bao gồm triển khai nhận dạng di động

Particulars	Capital Budget (K USD)	Operating Budget (K USD)	Units	Total Capital Budget (M USD)	Total Operating Budget (M USD)
EIDAV Data Center (A1)	$9,160.00	$22,594.50	1	$9.16	$22.59
EIDAV Disaster Recovery Center (A2)	$9,160.00	$22,594.50	1	$9.16	$22.59
Geographical Data Backup Center (A3)	$830.00	$457.50	1	$0.83	$0.46
MPS Data Migration (A4)	$500.00	$375.00	1	$0.50	$0.38
EIDAV IT and Institutional Infrastructure (A = A1+A2+A3+A4)				**$19.65**	**$46.02**
ISPA Data Center (B1)	$5,554.50	$4,167.08	2	$11.11	$8.33
ISPA IT and Institutional Infrastructure (B = B1)				**$11.11**	**$8.33**
ISCA Data Center (C1)	$1,218.70	$914.03	20	$24.37	$18.28
ISCA Service Delivery Outlets (C2)	$14.59	$10.94	2,480	$36.18	$27.14
ISCA IT and Institutional Infrastructure (C = C1+C2)				**$60.56**	**$45.42**
Awareness, Trainings and Capacity Building (D)	**$1,000.00**		**1**	**$1.00**	**$0.00**
National IT Standards and Policies (E)	**$200.00**		**1**	**$0.20**	**$0.00**
Total Budget = (J = A+B+C+D+E)				**$92.52**	**$99.77**
Total (Capital + Operating Budget)	**$192.29**				

Bảng 3: Chi tiết dự trù kinh phí giai đoạn triển khai rộng

Như trình bày ở bảng trên, tổng mức đầu tư cho giai đoạn triển khai rộng đầy đủ được dự trù ở mức **192,29 triệu USD**. Số này gồm tổng kinh phí đầu tư là **92,52 triệu USD** và tổng chi phí vận hành là **99,77 triệu** trong năm năm.

Dự trù ngân sách để triển khai rộng đầy đủ bao gồm bổ sung năng lực cho các cơ sở hạ tầng CNTT và thể chế được thiết lập trong giai đoạn thí điểm tại Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Số này còn bao gồm thiết lập và triển khai các cơ sở hạ tầng thể chế và CNTT cho thêm một Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) ngoài tổ chức đã thiết lập trong giai đoạn thí điểm. Có thêm khoảng 20 Tổ chức sử dung dịch vụ định danh điện tử (ISCA) sẽ được thiết lập với 124 điểm cung cấp (mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) sẽ thiết lập một điểm cho mỗi tỉnh và một điểm cho mười quận huyện) để cung cấp dịch vụ cho công dân. Có thêm mười Tổ chức quản lý đăng ký nữa sẽ được thiết lập, trong đó mỗi tổ chức có 100 điểm cung cấp dịch vụ, và có thêm hai Nhà cung cấp dịch vụ tin cậy (TSP). Ngoài ra, số bày còn bao gồm dự trù ngân sách cho các hoạt động nâng cao năng lực và xây dựng các chuẩn mực và chính sách cần thiết của chính phủ về Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) để triển khai khuôn khổ và hệ thống định danh điện tử (eID).

Dưới đây là chi tiết dự trù ngân sách đầu tư cho giai đoạn triển khai rộng đầy đủ:

1. **Cơ sở hạ tầng thể chế và CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).** Dự trù ngân sách để mở rộng năng lực cơ sở hạ tầng vật chất, CNTT và thể chế tập trung để triển khai rộng đầy đủ khuôn khổ này là **19.65 triệu USD**. Số này bao gồm tăng cường năng lực cho trung tâm dữ liệu tập trung, trung tâm phục hồi thảm hoạ và trung tâm sao lưu dữ liệu địa lý của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Dự trù ngân sách cho mỗi trung tâm dữ liệu bao gồm năng lực điện, nước và đồ đạc bổ sung; cơ sở hạ tầng CNTT bổ sung như phần cứng, phần mềm, thiết bị mạng để đáp ứng các yêu cầu triển khai rộng đầy đủ. Phần này còn bao gồm chi phí thiết kê, phát triển và triển khai các ứng dụng theo yêu cầu và ứng dụng đóng gói, nâng cấp và cập nhật các ứng dụng hiện hành. Ngoài ra, số này bao gồm cả chi phí nâng cấp cơ sở hạ tầng CNTT giữa Bộ Công An (MPS) và trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để chuyển dữ liệu công dân từ Bộ Công An (MPS) sang trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

2. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).** Dự trù kinh phí để thiết kế và triển khai hai trung tâm dữ liệu Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) bổ sung tại Vittel/VNPT hoặc tại nhà cung cấp khác để đáp ứng nhu cầu cho toàn bộ các Tổ chức sử dung dịch vụ định danh điện tử (ISCA) là **11,11 triệu USD**. Số này bao gồm thiết kế và triển khai trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA). Dự trù kinh phí để thiết lập trung tâm dữ liệu của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) bao gồm thiết kế, kiến trúc và triển khai cơ sở hạ tầng CNTT (phần cứng, phần mềm và mạng), mua sắm cơ sở hạ tầng CNTT theo thiết kế và đặc tả yêu cầu CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

   Cơ sở hạ tầng thể chế và CNTT của Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Dự trù kinh phí để thiết kế và triển khai hai trung tâm dữ liệu của 20 Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và 124 điểm cung cấp dịch vụ (một cho mỗi tỉnh và một cho 10 quận huyện) của mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA) là **60,56 triệu USD**. Số này bao gồm thiết kế và triển khai các trung tâm dữ liệu và điểm cung cấp dịch vụ của Tổ chức sử dung dịch vụ định danh điện tử (ISCA) cho mỗi Tổ chức sử dung dịch vụ định danh điện tử (ISCA). Dự trù ngân sách để thiết lập các trung tâm dữ liệu và điểm cung cấp dịch vụ đó bao gồm thiết kế, kiến trúc và triển khai cơ sở hạ tầng CNTT (phần cứng, phần mềm và mạng), mua sắm cơ sở hạ tầng CNTT theo thiết kế và đặc tả yêu cầu CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Số này còn bao gồm thiết kế, phát triển và triển khai các ứng dụng máy thanh toán bằng thẻ (máy PoS)

theo yêu cầu, tuỳ chỉnh các ứng dụng máy thanh toán bằng thẻ (máy PoS) hiện hành để tích hợp với các dịch vụ định danh điện tử (eID) của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), tạo nguồn thông tin Mã số định danh công dân (NIN) tại cơ sở dữ liệu của ứng dụng lĩnh vực nghiệp vụ (LoB) và máy thanh toán bằng thẻ (máy PoS) hiện hành.

3. **Nâng cao nhận thức, đào tạo và nâng cao năng lực**. Dự trù kinh phí bao gồm đào tạo nâng cao năng lực cho toàn bộ các bên liên quan trong hệmooi trường, các khoá đào tạo về kỹ thuật và quy trình cho các bên liên quan, các chương trình nâng cao nhận thức cho công dân và người sử dụng nhận dạng di động và các dịch vụ định danh điện tử (eID) khác của Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF). Dự trù kinh phí nhằm nâng cao nhận thức, đào tạo và nâng cao năng lực là **1 triệu USD**, ngoài ngân sách về nâng cao năng lực trong giai đoạn thí điểm.

4. **Các chuẩn mực và chính sách quốc gia về CNTT.** Dự trù ngân sách để thiết lập các uỷ ban của chính phủ và khu vực công nhằm phát triển và thông qua các chuẩn mực CNTT và chính sách của chính phủ là **0,2 triệu USD**.

Bảng dưới đây trình bày chi tiết dự trù kinh phí hoạt động cho giai đoạn triển khai rộng đầy đủ trong năm năm hoạt động.

1. **Cơ sở hạ tầng thể chế và CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).** Dự trù kinh phí hoạt động cho các cơ sở hạ tầng vật chất, CNTT và thể chế tập trung ở cấp quốc gia trong năm năm là **46,02 triệu USD**. Số này bao gồm kinh phí vận hành và duy trì cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa, lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm và thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu, trung tâm phục hồi thảm hoạ và trung tâm sao lưu dữ liệu. Số này còn bao gồm quản lý và chuyển dữ liệu liên tục từ Bộ Công An (MPS) sang trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

2. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức cung cấp dịch vụ định danh điện tử (ISPA).** Dự trù kinh phí hoạt động cho các cơ sở hạ tầng vật chất, CNTT và thể chế tập trung của các trung tâm dữ liệu tập trung cho hai Tổ chức cung cấp dịch vụ định danh điện tử (ISPA) là **8,33 triệu USD**. Số này bao gồm kinh phí vận hành và duy trì cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa, lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm và thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu.

3. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức sử dung dịch vụ định danh điện tử (ISCA).** Dự trù kinh phí hoạt động cho các cơ sở hạ tầng vật chất, CNTT và thể chế tập trung của các trung tâm dữ liệu và điểm cung cấp dịch vụ trong năm năm cho 20 Tổ chức sử dung dịch vụ định danh điện tử (ISCA) và 124 điểm cung cấp dịch vụ của họ là **45,42 triệu USD**. Số này bao gồm kinh phí vận hành và duy trì cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa, lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm và thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu và cán bộ tại các điểm cung cấp dịch vụ.

7.2.4 Dự trù kinh phí cho phương án tuỳ chọn về nhận dạng di động trong giai đoạn triển khai rộng đầy đủ

Dưới đây là mô tả dự trù kinh phí để triển khai phương án lựa chọn là nhận dạng di động trong giai đoạn triển khai rộng đầy đủ. Dự trù kinh phí này dựa trên việc triển khai rộng 90 triệu nhận dạng di động, hai Tổ chức quản lý đăng ký (RA), 200 điểm cung cấp dịch vụ của Tổ chức quản lý đăng ký (RA) và một Nhà cung cấp dịch vụ tin cậy (TSP) trong giai đoạn triển khai rộng.

Bảng dưới đây trình bày chi tiết dự trù kinh phí đầu tư và hoạt động để triển khai phương án tuỳ chọn về nhận dạng di động trong giai đoạn triển khai rộng.

Particulars	Capital Budget (K USD)	Operating Budget (K USD)	Units	Total Capital Budget (M USD)	Total Operating Budget (M USD)
RA Data Center (D1)	$2,218.70	$1,664.03	2	$4.44	$3.33
RA Service Delivery Outlets (D2)	$14.59	$10.94	200	$2.92	$2.19
SIM Provision (D3)	$44,950.00	$0.00	1	$44.95	$0.00
RA IT and Institutional Infrastructure (D = D1+D2+D3)				**$52.31**	**$5.52**
TSP Data Center (E1)	$1,903.70	$1,427.78	1	$1.90	$1.43
TSP IT and Institutional Infrastructure (E=E1)				**$1.90**	**$1.43**
Total Budget = (K = D+E)				**$54.21**	**$6.94**

Total (Capital + Operating Budget)	**$61.15**

Bảng 4: Chi tiết dự trù kinh phí để triển khai rộng phương án nhận dạng di động

Như trình bày tại bảng trên, tổng mức đầu tư để triển khai phương án tuỳ chỉnh về nhận dạng di động trong giai đoạn triển khai rộng đầy đủ được dự trù ở mức 61,15 triệu USD. Số này bao gồm kinh phí đầu tư là 54,21 triệu và kinh phí hoạt động là 6,94 triệu USD trong năm năm đầu.

Dưới đây là chi tiết dự trù kinh phí đầu tư giai đoạn mở rộng cho phương án triển khai nhận dạng di động.

1. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức quản lý đăng ký (RA).** Dự trù kinh phí để thiết kế và triển khai hai trung tâm dữ liệu mới của Tổ chức quản lý đăng ký (RA) mới và 100 điểm cung cấp dịch vụ của mỗi Tổ chức quản lý đăng ký (RA) tại Viettel/VNPT, hoặc trung tâm dữ liệu và điểm cung cấp dịch vụ hiện hành của một nhà điều hành di động khác là **52,31 triệu USD**. Số này bao gồm thiết kế và triển khai trung tâm dữ liệu và các điểm cung cấp dịch vụ của Tổ chức quản lý đăng ký (RA). Dự trù kinh phí để thiết lập trung tâm dữ liệu và điểm cung cấp dịch vụ bao gòm thiết kế, phát triển và triển khai các ứng dụng máy thanh toán bằng thẻ (máy PoS) theo yêu cầu, tuỳ chỉnh các ứng dụng máy thanh toán bằng thẻ (máy PoS) hiện hành để cung cấp SIM nhận dạng di động, kích hoạt chứng nhận số, và tạo nguồn thông tin Mã số định danh công dân (NIN) trên cơ sở dữ liệu của nhà cung cấp dịch vụ. Số này còn bao gồm kinh phí cung cấp 90 triệu SIM có nhận dạng di động bên cạnh 100.000 đơn vị dự kiến tại giai đoạn thí điểm.

2. **Cơ sở hạ tầng thể chế và CNTT của Nhà cung cấp dịch vụ tin cậy (TSP).** Dự trù kinh phí để thiết kế và triển khai thêm trung tâm dữ liệu của Nhà cung cấp dịch vụ tin cậy (TSP) tại Viettel/VNPT, hoặc một nhà điều hành di động khác là **1,90 triệu USD.** Dự trù ngân sách để thiết lập trung tâm dữ liệu này bao gồm thiết kế, kiến trúc và triển khai cơ sở hạ tầng CNTT theo thiết kế và đặc tả yêu cầu CNTT của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

Dưới đây là chi tiết dự trù kinh phí hoạt động trong giai đoạn mở rộng khi triển khai phương án tuỳ chọn là nhận dạng di động

1. **Cơ sở hạ tầng thể chế và CNTT của Tổ chức quản lý đăng ký (RA).** Dự trù ngân sách để vận hành các cơ sở hạ tầng vật lý, CNTT và thể chế cho các trung tâm dữ liệu và điểm cung cấp dịch vụ của hai Tổ chức quản lý đăng ký (RA) và 200 điểm cung cấp dịch vụ của các tổ chức đó là **5,52 triệu USD.** Số này bao gồm vận hành và duy trì cơ sở hạ tầng vật lý như điện, nước hàng tháng, sửa chữa, lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm và thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu và cán bộ tại các điểm cung cấp dịch vụ.

2. **Cơ sở hạ tầng thể chế và CNTT của Nhà cung cấp dịch vụ tin cậy (TSP).** Dự trù ngân sách để vận hành các cơ sở hạ tầng vật lý, CNTT và thể chế cho một Nhà cung cấp dịch vụ tin cậy (TSP) trong năm năm là **1,43 triệu USD**. Số này bao gồm vận hành và duy trì cơ sở hạ

tầng vật lý như điện, nước hàng tháng, sửa chữa, lau dọn toà nhà, lương cán bộ. Số này còn bao gồm duy tu bảo dưỡng và nâng cấp phần cứng, phần mềm và thiết bị mạng, lương cán bộ CNTT tại trung tâm dữ liệu.

7.2.5 Tổng dự trù kinh phí nếu không triển khai nhận dạng di động

	Capital Budget (M USD)	Operting Budget (M USD)	Total Budget (M USD)
Pilot Phase with 1 year of Operation (A)	$ 47.16	$ 7.04	**$ 54.20**
Complete Rollout Phase with 5 years of Operation (B)	$ 92.52	$ 99.77	**$192.29**
Total Budget (C=A+B)	**$139.68**	**$ 106.81**	**$246.49**

Bảng 5: Tổng kinh phí để triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF)

Như trình bày ở bảng trên, tổng dự trù kinh phí cho giai đoạn thí điểm gồm một năm vận hành là **54,20 triệu USD**, còn tổng dự trù kinh phí cho giai đoạn triển khai rộng đầy đủ gồm năm năm vận hành là **192,29 triệu USD**. Dự trù ngân sách tổng thể để triển khai Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF) tại Việt Nam theo hai giai đoạn (thí điểm và triển khai rộng) là **246,49 triệu USD**.

8.0 Các Phụ lục

Phụ lục 1

1. Các loại bằng chứng thông báo nhận dạng (token)

Danh tính của một cá nhân có thể được tạo ra và được chứng thực bằng cách cung cấp ba loại bằng chứng thông báo nhận dạng sau:

Những gì người dùng biết. Ví dụ như tên người dùng, mật khẩu, mã PIN, và các câu hỏi bí mật và các câu trả lời. Chúng có thể chỉ sử dụng được qua xác nhận điện tử. Và thường không được sử dụng cho những xác nhận mang tính vật lý, vì nếu được biết bởi một người khác thì ngay lập tức sẽ bị mất đi giá trị để xác minh danh tính.

Những gì người dùng có. Ví dụ như thẻ giấy căn cước, thẻ bảo hiểm y tế, thẻ truy cập, thẻ ATM và điện thoại di động. Đối với loại này, có thể được xác nhận bằng điện tử và / hoặc bằng tay về hình thức của thẻ. Ví dụ, giấy chứng minh nhân dân và thẻ bảo hiểm y tế chỉ có thể được xác thực bằng tay, trong khi thẻ ATM và thẻ truy cập có thể được chứng thực bằng điện tử. Đây là hình thức phổ biến nhất của thẻ nhận dạng tại Việt Nam.

Ai là người sử dụng. Ví dụ như dấu vân tay, mẫu võng mạc, hình ảnh khuôn mặt, dấu hiệu cơ thể và giọng nói. Đối với loại này, có thể được xác định bằng điện tử và/hoặc bằng tay về hình thức của thẻ. Ví dụ, giấy chứng minh nhân dân và thẻ bảo hiểm y tế chỉ có thể được chứng thực bằng điện tử. Đây là hình thức phổ biến nhất của thẻ nhận dạng tại Việt Nam.

II. Tiêu chí lựa chọn hình thức chứng thực của nhà cung cấp dịch vụ

Các nhà cung cấp dịch vụ có thể lựa chọn hình thức chứng thực dựa trên một số tiêu chí sau đây:

1. Mức độ, loại rủi ro và tác động đến người dùng trong trường hợp nhận dạng không chính xác tại thời điểm cung cấp dịch vụ. Loại rủi ro và tác động đến người dùng bao gồm sự bất tiện và tai nạn, mất mát về tài chính, và vi phạm an ninh và sự riêng tư.

2. Mức độ, loại rủi ro và tác động đến các nhà cung cấp dịch vụ trong trường hợp xác thực không chính xác trong giao dịch kinh doanh. Loại rủi ro và tác động đến các nhà cung cấp dịch vụ bao gồm tổn thất về tài chính, thắt chặt kinh doanh, mức độ bảo mật và sự riêng tư, và mối đe dọa cho an ninh quốc gia.

3. Chi phí và hậu cần để thực hiện một loại xác nhận. Ví dụ, sinh trắc học sẽ đòi hỏi đầu tư vào thiết bị và sự hiện diện của người dùng, trong khi mật khẩu dùng một lần (OTP) đòi hỏi người dùng phải có điện thoại di động.

4. Số lượng chứng thực cần dựa trên số lượng đối tượng và tần số chứng thực cần thiết. Ví dụ, an ninh được đảm bảo ở mức độ cao có thể thích hợp cho mục đích nhận dạng và xác thực khách hàng (KYC) của một lần mở tài khoản, phát hành dịch vụ trong khi yêu cầu đảm bảo sẽ thấp hơn cho các giao dịch thường xuyên như cung cấp dịch vụ.

Trong trường hợp có nguy cơ cao hơn về danh tính bị lạm dụng, chứng thực kết hợp nhiều yếu tố cùng lúc cần được xem xét để loại bỏ sự xuất hiện của các trường hợp như vậy.

III. Các kịch bản hỗ trợ tự phục vụ và tổng đài cung cấp dịch vụ

Kịch bản 1: Tổng đài hỗ trợ giao dịch bằng cách sử dụng thiết bị đầu cuối của máy thanh toán bằng thẻ (PoS) tại các địa điểm cung cấp dịch vụ được chỉ định

1. Trong kịch bản này, người dùng có thể đến địa điểm cung cấp dịch vụ được chỉ định (ví dụ như công cộng hay tư nhân) để yêu cầu dịch vụ. Người dùng trình bày Mã số định danh công dân (NIN) và dữ liệu nhận dạng cá nhân về nhân khẩu, sinh trắc học và kỹ thuật cần thiết được đọc bởi các thiết bị của nhà cung cấp dịch vụ. Trong trường hợp chứng nhận bằng kỹ thuật số hoặc sinh trắc, các thiết bị này sẽ có khả năng đọc từ thẻ thông minh bằng cách sử dụng một đầu đọc thẻ hoặc từ điện thoại di động.
2. Nhà điều hành dịch vụ cung cấp dữ liệu nhận dạng của công dân cho các phần mềm ứng dụng cho phép chứng thực định danh điện tử (eID) được cài đặt trên thiết bị đầu cuối có thẩm quyền. Trong trường hợp của nhận dạng di động, công dân sẽ tự chứng thực bằng cách cung cấp mã PIN trên điện thoại di động của họ.
3. Phần mềm ứng dụng đóng gói các thông số đầu vào, mã hóa, và chuyển tới các dịch vụ xác thực định danh điện tử (eID) trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) tập trung trên một mạng di động băng thông rộng.
4. Dịch vụ định danh điện tử (eID) trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) sẽ gửi câu trả lời "có / không" dựa trên các các thông số đầu vào phù hợp.
5. Dựa trên những phản hồi từ các dịch vụ định danh điện tử (eID), nhà cung cấp dịch vụ sẽ thực hiện giao dịch phù hợp.

Kịch bản 2: Giao dịch tự phục vụ sử dụng điện thoại di động, các ki ốt và thiết bị kết nối mạng internet

1. Trong kịch bản này người dùng có thể tiến hành giao dịch tự phục vụ sử dụng dịch vụ chứng thực định danh điện tử (eID) trên điện thoại di động hoặc trên một thiết bị có kết nối mạng internet như là máy tính bảng, máy tính cá nhân (PC), ki ốt, máy tính xách tay...

2. Người dùng nhập những dữ liệu giao dịch trên điện thoại di động/thiết bị kết nối mạng để truy cập vào điện thoại di động/ thiết bị kết nối mạng cho phép ứng dụng cung cấp dịch vụ của nhà cung cấp.
3. Người dùng cung cấp Mã số chứng minh nhận dạng quốc gia (NIN), dữ liệu nhân chủng học cần thiết hoặc chứng chỉ số/sinh trắc cùng với mật khẩu dùng một lần (OTP) cho nhà cung cấp dịch vụ, các thuộc tính cụ thể (có thể là tên miền số tài khoản, mật khẩu, mã PIN, vv). Trong trường hợp chứng chỉ số, người dùng cũng có thể sử dụng nhận dạng di động được hỗ trợ trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Dữ liệu sinh trắc học như dấu vân tay cũng có thể được sử dụng mặc dù chưa phổ biến trên điện thoại di động hoặc máy tính. Tuy nhiên, Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể cung cấp đặc tả kỹ thuật chuẩn cho các thiết bị sinh trắc học (mã số nhận dạng duy nhất (UID) hoặc khác) và lưu vào danh sách các nhà cung cấp đã được phê duyệt của các thiết bị này.
4. Bước 3, 4, và 5 giống như trong kịch bản 1 trên.

Kịch bản 3: Môi trường thử nghiệm cho các nhà cung cấp dịch vụ và nhà phát triển phần mềm

1. Nhà cung cấp dịch vụ có thể sử dụng môi trường đã được thử nghiệm và phát triển được cung cấp trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) để xây dựng ứng dụng phần mềm của họ để có thể sử dụng dịch vụ xác thực định danh điện tử (eID).

2. Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể cung cấp một bộ định vị tài nguyên đồng nhất (URL) công cộng (ví dụ, https://auth.EIDAV.gov.vn) nơi các nhà phát triển phần mềm có thể truy cập vào các giao diện lập trình ứng dụng (hàm API) cho dịch vụ xác thực định danh điện tử (eID).

3. Điều này sẽ giúp cho việc kiểm tra các cài đặt của phần mềm định danh điện tử (eID) trên các thiết bị và máy chủ của nhà cung cấp dịch vụ.

IV. Tiện ích và Nền tảng tạo nguồn thông tin nhận dạng điện tử

Tiện ích tạo nguồn thông tin

Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể tạo nguồn thông tin tiện ích đối với nhà cung cấp dịch vụ để thực hiện các hoạt động phổ biến bao gồm cả khai thác dữ liệu, hợp nhất, chuẩn hóa và đối chiếu. Các nhà cung cấp dịch vụ sẽ cần phải đăng ký trong hệ thống

và ký hợp đồng sử dụng tiện ích chỉ cho những mục đích đã có dự định trước. Một số các tính năng của công cụ này là:

1. **Trích xuất dữ liệu nguồn**. Tiện ích sẽ có thể kết nối với các nguồn dữ liệu khác nhau để kéo dữ liệu nhận dạng cá nhân (PID) liên quan từ cơ sở dữ liệu tham chiếu. Nó cũng sẽ lấy dữ liệu từ các bảng dữ liệu có liên quan trong cơ sở dữ liệu cung cấp dịch vụ của nhà cung cấp dịch vụ.

2. **Đối chiếu và tạo nguồn thông tin**. Tiện ích sẽ cung cấp khả năng trong đó một hoặc nhiều trường dữ liệu nhận dạng cá nhân (PID) tương ứng (tên, ngày sinh, tuổi, giới tính) trong hồ sơ công dân tại các cơ sở dữ liệu cung cấp dịch vụ có thể được kết hợp với các trường tương ứng trong các hồ sơ nhận dạng từ cơ sở dữ liệu tham chiếu. Do đó các ánh xạ được tạo ra có thể chiết xuất sang dạng Excel để xem xét và phê duyệt của cơ quan có thẩm quyền do nhà cung cấp dịch vụ chỉ định. Chức năng tiện ích của sự đối chiếu và tạo nguồn thông tin sẽ được giới hạn chỉ trong việc tạo ra các bản đồ và xuất sang Excel. Dự kiến là dựa trên những dữ liệu của bản đồ này, các nhà cung cấp dịch vụ sẽ tạo ra các ngôn ngữ truy vấn theo cấu trúc (SQL) tuỳ chỉnh để cập nhật cơ sở dữ liệu cung cấp dịch vụ.

3. **Xác thực nhân chủng học**. Để xác minh xem việc tạo nguồn thông tin đã được thực hiện một cách chính xác hay chưa, điều quan trọng là các hồ sơ ghi chép của công dân tại các cơ sở dữ liệu cung cấp dịch vụ chứng thực được dân số học. Mục tiêu của xác thực nhân chủng học là để kiểm tra xem các trường Mã số định danh công dân (NIN) và dữ liệu nhận dạng cá nhân (PID) được phản ánh một cách chính xác và phù hợp với các dữ liệu trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Bài viết xác thực nhân khẩu học, tình trạng xác thực có thể được đánh dấu là "đạt/ không đạt". Trong trường hợp "không đạt", mã lỗi có thể chỉ ra và giải thích lý do cho việc chứng thực thất bại có thể được sử dụng cho các mục đích điều tra. Các điều kiện tiên quyết để xác thực nhân khẩu học là nhà cung cấp dịch vụ đăng ký trong hệ thống gọi cho dịch vụ chứng thực định danh điện tử (eID) để xác thực nhân khẩu học.

Nền tảng tạo nguồn thông tin định danh điện tử (eID) tập trung

Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể cung cấp nền tảng tạo nguồn thông tin định danh điện tử (ESP) tập trung như một phần của nền tảng cung cấp dịch vụ định danh điện tử (EISDP) mà sẽ cho phép hội tụ các kênh tạo nguồn khác nhau vào một khu vực trung tâm. Nền tảng tạo nguồn thông tin định danh điện tử (ESP) sẽ được tiếp cận với các nhà khai thác trong các tổ chức cung cấp dịch vụ khác nhau cho việc xác minh các nguồn và đưa vào cơ sở dữ liệu cung cấp dịch vụ của họ. Nó sẽ hỗ trợ một cách hiệu quả và liền mạch các nguồn của Mã số

định danh công dân (NIN) vào cơ sở dữ liệu của nhà cung cấp dịch vụ, qua đó cho phép áp dụng nhanh việc cung cấp dịch vụ định danh điện tử (eID) được kích hoạt tại Việt Nam.

Các yêu cầu tạo nguồn sẽ đi đến nền tảng tạo nguồn thông tin định danh điện tử (ESP) từ các kênh đầu vào khác nhau. Mỗi yêu cầu tạo nguồn là một đệ trình của Mã số định danh công dân (NIN) và đối tượng thụ hưởng / người đăng ký thuê bao / danh tính khách hàng (ID) có liên quan đến hệ thống cung cấp dịch vụ.

Nền tảng tạo nguồn thông tin định danh điện tử (ESP) có thể được công bố trên cổng thông tin công cộng của Cơ quan Quản lý Định danh điện tử Việt Nam (EIDAV) và các công dân có thể truy cập trực tiếp để gửi yêu cầu tạo nguồn. Người sử dụng có thẩm quyền từ các tổ chức cung cấp dịch vụ có thể truy cập đăng nhập dựa trên yêu cầu tạo nguồn ("người tạo nguồn thông tin") thay mặt cho công dân. Người sử dụng có thẩm quyền của các tổ chức cung cấp dịch vụ có thể truy cập đăng nhập để xác nhận yêu cầu ("người xác nhận"). Người xác nhận có thể xử lý các yêu cầu tạo nguồn bằng cách so sánh dữ liệu nhận dạng cá nhân (PID) của công dân từ Trung tâm Lưu trữ dữ liệu Định danh điện tử Công dân Tập trung (CRIDS) (được cung cấp cho ESP thông qua các dịch vụ web) với dữ liệu nhận dạng cá nhân (PID) của công dân từ cơ sở dữ liệu của chương trình thụ hưởng (sẵn có trên ESP hoặc thông qua một dịch vụ web hoặc thiết lập trên cơ sở dữ liệu ESP riêng bởi người quản trị hệ thống).

V. Tiện ích khách hàng với chữ ký số

Công dân bắt đầu các tiện ích khách hàng trên máy tính của họ và lựa chọn tài liệu sẽ được ký kết trong ứng dụng. Sử dụng thẻ của Hệ thống định danh điện tử quốc gia (NID) do Bộ Công An (MPS) cấp vào đầu đọc thẻ gắn vào máy tính, các công dân ký vào văn bản đã được lựa chọn. Ứng dụng đọc chứng nhận chữ ký số từ thẻ ID và tạo ra một chữ ký số sử dụng khóa riêng bằng cách cung cấp mã PIN. Sau khi chữ ký số được tạo ra, hiệu lực của Giấy chứng nhận của người ký thu được trong định dạng của Giao thức kiểm tra chứng thực trực tuyến (OCSP) phản hồi và được lưu trữ trong văn bản ký kết. Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể cung cấp dịch vụ Giao thức kiểm tra chứng thực trực tuyến (OCSP) để xác nhận chữ ký số. Các ứng dụng khách hàng gọi các dịch vụ web Giao thức kiểm tra chứng thực trực tuyến (OCSP) lưu trữ trong Nền tảng cung cấp dịch vụ định danh điện tử (EISDP) bằng cách cung cấp các chứng chỉ xác thực của người dân, và hàng loạt các chữ ký số lộn xộn. Những chữ ký số này được nhận lại trong phản ứng Giao thức kiểm tra chứng thực trực tuyến (OCSP). Các dịch vụ Giao thức kiểm tra chứng thực trực tuyến (OCSP) hoạt động như một công chứng viên điện tử kỹ thuật số xác nhận chữ ký được tạo ra tại địa điểm đó với một thẻ thông minh.

Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) cũng có thể cung cấp các tùy chọn để ký tên vào tài liệu bằng cách sử dụng trình duyệt Internet trên chính máy tính đó bằng cách kết nối với cổng thông tin công cộng của Các Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Chức năng của nó tương tự như các chương trình khách hàng và có thể được sử dụng để tạo ra và xác minh chữ ký số. Ngoài ra, nó có thể được sử dụng để ký các tài liệu của một số người. Nó cho phép chỉ định những người có chữ ký là cần thiết trên các tài liệu và tất cả đều có thể ký tên trên cổng thông tin tương tự. Mỗi người sử dụng có một thư mục / tài liệu riêng của mình mà không ai nhìn thấy, nhưng bất cứ ai cũng có thể gửi các tài liệu có chữ ký của người sử dụng.

Các văn bản ký kết bao gồm trong từng ngăn chứa: các tài liệu gốc, giấy chứng nhận được sử dụng để ký kết, thời gian ký kết, nơi ký, vai trò của người ký, và các thông tin xác nhận hợp lệ, cụ thể là, Giao thức kiểm tra chứng thực trực tuyến (OCSP) phản hồi và chứng chỉ của người phản hồi trong Giao thức kiểm tra chứng thực trực tuyến (OCSP). Không cần bổ sung bất kỳ thông tin nào để xác minh tính hợp lệ của chữ ký.

Các nhà cung cấp dịch vụ có thể đưa các tính năng chữ ký số vào các ứng dụng cung cấp dịch vụ của họ bằng cách sử dụng cơ sở và thư viện trung gian cung cấp bởi khuôn khổ.

Khuôn khổ cho phép giá trị của chữ ký số được kéo dài bằng cách duy trì các bản ghi của các phản ứng của Giao thức kiểm tra chứng thực trực tuyến (OCSP) và thay đổi trong tính hợp lệ được chứng nhận.

Phụ lục 2: Phương thức và các quy định đối chiếu dữ liệu nhân chủng học

I. Những quy định về đối chiếu tên

Đối chiếu tên. Đối với tên của công dân, có thể có những phương thức hỗ trợ như so sánh "chính xác" và so sánh "từng phần". Khi sử dụng phương thức so sánh "chính xác" thì tên được so sánh phải trùng khớp hoàn toàn với tên được lưu trong Trung tâm Lưu trữ dữ liệu Định danh điện tử Công dân Tập trung (CRIDS). Mặc dù được so sánh trong trường hợp nhạy cảm, tất cả những từ của tên phải được sắp xếp theo cùng một thứ tự chính xác như đã được cung cấp bởi các công dân. Khi sử dụng phương thức so sánh "từng phần" thì tên được so sánh với trong Trung tâm Lưu trữ dữ liệu Định danh điện tử Công dân Tập trung (CRIDS) dựa trên các nguyên tắc sau:

1. Những từ của tên có thể hiển thị theo bất kỳ thứ tự nào trong thuộc tính "tên". Ví dụ, nếu tên được lưu giữ là "Pham Dang Nguyen", thì bất kỳ dữ liệu đầu vào nào như – "Nguyen Pham Dang", "Pham Nguyen Dang", "Dang Pham Nguyen" hoặc bất kỳ kết hợp khác – cũng có thể đưa ra kết quả trùng khớp.
2. Sử dụng tiêu đề cụ thể có thể được phép vào thuộc tính "tên". Đây là những tiêu chí có thể bỏ qua tuỳ theo mục đích sử dụng. Các chức danh được hỗ trợ là "Ông", "Bà" ,"Cô", và "Tiến sĩ". Không có danh hiệu nào khác hiện đang được hỗ trợ. Ví dụ, nếu tên được lưu giữ là "Pham Nguyen", thì sau đó bất kỳ dữ liệu đầu vào nào như– "Tiến sĩ Pham Nguyen "," Bà Pham Nguyen "hoặc" Cô Pham Nguyen "– đều có thể đưa ra kết quả trùng khớp.
3. Ký tự đặc biệt sau đây, nếu có trong thuộc tính "tên", được bỏ qua trong khi so khớp:
    a. Dấu chấm (.)
    b. Dấu phẩy (,)
    c. Dấu gạch ngang (–)
    d. Dấu hoa thị (*)
    e. Mở và đóng ngoặc tròn [( )]
    f. Mở và đóng ngoặc vuông ([ ])
    g. Dấu nháy đơn (`)
    h. Nháy đơn (')
    i. Nháy kép (")
    j. Dấu gạch chéo (/)
    k. Dấu gạch chéo ngược (\)
    l. Dấu thăng (#)
    m. Hàng đầu, đuôi, và hai hoặc nhiều khoảng trống tiếp giáp được loại bỏ trước khi so khớp. Ví dụ, nếu tên của công dân được lưu trữ là "Pham Nguyen", thì "Nguyen, Pham" có thể đưa ra kết quả trùng khớp.

n. Đầu vào có thể không chứa bất kỳ từ bổ sung hoặc viết tắt nào mà không có trong cơ sở dữ liệu. Điều này có thể dẫn đến việc so khớp không thành công và xác thực lỗi. Ví dụ, nếu tên được lưu trữ là "Pham Nguyen", thì ", ông Pham Dang Nguyen" hoặc "Pham Dang" hoặc "D Pham Nguyen" có thể đưa ra kết quả so sánh không khớp vì những từ "Dang" và "D" không có trong cơ sở dữ liệu trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS).

o. Khi trị số ngưỡng của so khớp từng phần với một phần khác là hơn 100%, thì dữ liệu đầu vào có thể bỏ qua một số từ, hoặc từ viết tắt có thể được sử dụng thay cho các từ đầy đủ. Việc so khớp này được coi là thành công khi đầu vào có chứa một số lượng tối thiểu phù hợp với những từ đầy đủ được xác định bởi trị số ngưỡng của so khớp từng phần. Ví dụ, nếu tên được lưu trữ là "Pham Dang Nguyen", và trị số ngưỡng được quy định là 60%. Điều đó có nghĩa là 60% của tổng số từ phải trùng khớp. Trong trường hợp của "Pham Dang Nguyen", 60% của ba chữ là 1,8 được làm tròn lên hai chữ.

   Vì vậy, bất kỳ các dữ liệu đầu vào nào dưới đây cũng có thể đưa ra kết quả trùng khớp:

   i. "Pham Nguyen" phù hợp vì có ít nhất hai từ đầy đủ
   ii. "Nguyen, Pham Dang" phù hợp bởi vì có ít nhất hai từ đầy đủ theo thứ tự bất kỳ, và dấu phẩy (,) được bỏ qua.
   iii. "Pham D Nguyen" phù hợp bởi vì nó có ít nhất hai từ đầy đủ theo thứ tự bất kỳ, và "D" là chữ cái đầu của "Dang".

   Các dữ liệu đầu vào dưới đây có thể đưa ra kết quả không trùng khớp:

   i. "Pham" không phù hợp vì số lượng từ ít hơn mức tối thiểu quy định.
   ii. "Pham DN" không phù hợp từ các chữ cái đầu không được tính là những từ đầy đủ; do đó, số lượng phù hợp với những từ đầy đủ là ít hơn mức tối thiểu quy định.
   iii. "S Pham Nguyen" không phù hợp bởi vì trong khi "Pham" và "Nguyen" là những từ đầy đủ, thì "S" không phải là chữ cái đầu của "Dang".

4. Phương thức so sánh có thể hỗ trợ cả hai ngôn ngữ, tức là cả tiếng Anh và tiếng Việt. Tên bằng tiếng Việt có thể là một chuỗi mã thống nhất và có thể sử dụng việc so sánh ngữ âm với các dữ liệu được lưu trữ trong trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS).

II. Những quy định về đối chiếu địa chỉ

1. **Đối chiếu địa chỉ.** Đối với địa chỉ của công dân, có thể hỗ trợ cho cả hai phương thức là so sánh "chính xác" và "từng phần". Có một "trị số ngưỡng" định nghĩa cho chiến lược so khớp "từng phần" với định nghĩa tỷ lệ phần trăm của những từ đầy đủ từ các địa chỉ được lưu trữ trong cơ sở dữ liệu của trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) phải được quy định trong các dữ liệu đầu vào của các yêu cầu dịch vụ để việc so sánh được thành công.
2. **Chuẩn hóa.** Giá trị địa chỉ trong các dữ liệu đầu vào cho các yêu cầu dịch vụ và địa chỉ của công dân lưu trữ trong trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) đều được chuẩn hoá sử dụng các quy tắc sau đây trước khi so sánh. Các ký tự / cụm từ sau được bỏ qua:
    a. Dấu chấm (.)
    b. Dấu phẩy (,)
    c. Dấu gạch ngang (-)
    d. Dấu hoa thị (*)
    e. Mở và đóng ngoặc tròn [( )]
    f. Mở và đóng ngoặc vuông ([ ])
    g. Dấu nháy đơn (`)
    h. Nháy đơn (‘)
    i. Nháy kép (“)
    j. Dấu gạch chéo (/)
    k. Dấu gạch chéo ngược (\)
    l. Dấu thăng (#)
    m. Những dấu hiệu chú ý, chẳng hạn như "C / O", "S / O", "D / O", "W / O", "H / O"
    n. “Số” (“No.”)
    o. Khoảng trống ở đầu và đuôi được cắt bớt và nhiều khoảng trống liên tiếp sẽ được thay thế bằng một khoảng trống duy nhất.
3. Khi sử dụng phương thức so sánh "chính xác", thuộc tính địa chỉ được chuẩn hoá của các dữ liệu đầu vào được so khớp chính xác với địa chỉ được chuẩn hoá của công dân.
4. Khi sử dụng phương thức so khớp "từng phần", thuộc tính địa chỉ được chuẩn hoá sẽ so khớp với một phần của địa chỉ được chuẩn hoá của công dân. Sau đây là các quy tắc của so khớp từng phần:
    a. Những từ có thể xuất hiện theo bất kỳ thứ tự nào.

b. Những chuẩn hoá bổ sung dưới đây được áp dụng cho cả giá trị địa chỉ dữ liệu đầu vào và địa chỉ lưu trữ trong cơ sở dữ liệu trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS)
c. Những từ sử dụng thông thường được thay thế bằng từ viết tắt:
    i. “apartment” => “apt”
    ii. “street” => “st”
    iii. “road” => “rd”
    iv. “main” => “mn”
    v. “cross” => “crs”
    vi. “sector” => “sec”
    vii. “opposite” => “opp”
    viii. “market” => “mkt”
    ix. Hậu tố thường được sử dụng với các con số như "st", "nd", "th", và "th" sẽ được loại bỏ. Ví dụ, 21st được chuyển thành 21, 44th được chuyển thành 44, vv.

5. Khi sử dụng với trị số ngưỡng khác hơn 100, một số từ có thể được bỏ qua trong các đầu vào. So sánh được coi là thành công nếu số lượng từ tối thiểu của cả từ phải trùng khớp, được xác định bởi trị số ngưỡng hiển thị ở đầu vào. Đây là một kịch bản mà chiến lược so sánh từng phần với trị số ngưỡng 60% được áp dụng cho các giá trị sau đây của địa chỉ công dân: c/o Pham Dung Nguyen, Căn hộ số 12, tòa nhà Trong, phố Chùa Bộc, Quận Đống Đa, Hà Nội, Việt Nam, 560055
    a. Đây có thể là địa chỉ bình thường: Pham dung nguyen apt 12 trong building chua boc st quan dong da Hanoi vietnam 560055
    b. Đây là những ví dụ về sự so khớp và kết quả của chúng:
        i. “s/o Pham Dung Nguyen, Trong Building, apt #12, chua boc st, hanoi – 560055” có thể được chuẩn hoá thành “pham dung nguyen trong building apt 12 chua boc st hanoi 560055” – cho kết quả thành công khi so khớp vì có 12 từ trùng khớp (lớn hơn 11 từ làm tròn lên là 60% của 17 từ).
        ii. “s/o Pham Dung Nguyen, Trong Building Hanoi 560055” có thể được chuẩn hoá thành “pham dung nguyen trong building hanoi 560055” – cho kết quả không thành công khi so sánh vì chỉ có 8 từ trùng khớp (trong khi yêu cầu tối thiểu là 11 từ tương đương với 60%).
6. Chiến lược so khớp địa chỉ có thể hỗ trợ các địa chỉ bằng cả tiếng Anh và tiếng Việt, sử dụng so khớp ngữ âm.

Phụ lục 3

I. Đề xuất cơ cấu địa chỉ tiêu chuẩn

Các thuộc tính cố định của cơ cấu địa chỉ tiêu chuẩn được quy định dưới đây:

CO - "gửi đến" tên người

House - nhận dạng nhà

Street - tên đường phố

Landmark - địa danh, nếu có

LOC - địa phương nơi cư trú của cư dân

VTC - tên của làng, thị xã, thành phố

Commune - Tên xã

District - huyện tên

Province - tên tỉnh

PC - mã bưu điện

II. Dữ liệu sử dụng được mã hoá

Chữ số thập lục phân trong "dữ liệu sử dụng được mã hoá" cho hệ thống Aadhaar của Ấn Độ được diễn giải dựa trên quy tắc dưới đây.

Số thập lục phân thứ nhất:

Bit 3-0: phiên bản mã hóa số. Nó có thể là hệ thập lục phân "1" (nhị phân: 0001) để mã hóa quy định tại văn bản này.

Số thập lục phân thứ hai:

Bit 3: Thuộc tính "Pi> name" có được sử dụng không?
Bit 2: Thuộc tính "Pi> lname"có được sử dụng không?
Bit 1: Thuộc tính "Pi> gender" có được sử dụng không?
Bit 0: Thuộc tính "Pi> dob" có được sử dụng không?

Số thập lục phân thứ ba:

Bit 3: Thuộc tính "Pi> phone" có được sử dụng không?
Bit 2: Thuộc tính "Pi> email" có được sử dụng không?
Bit 1: Thuộc tính "Pi> age" có được sử dụng không?
Bit 0: Thuộc tính "Pa> co" có được sử dụng không?

Số thập lục phân thứ tư:

Bit 3: Thuộc tính "Pa> house" có được sử dụng không?
Bit 2: Thuộc tính "Pa> street" có được sử dụng không?
Bit 1: Thuộc tính "Pa> lm" có được sử dụng không?
Bit 0: Thuộc tính "Pa> loc" có được sử dụng không?

Số thập lục phân thứ năm:

Bit 3: Thuộc tính "Pa> vtc" có được sử dụng không?
Bit 2: Thuộc tính "Pa> dist" có được sử dụng không?
Bit 1: Thuộc tính "Pa> state" có được sử dụng không?
Bit 0: Thuộc tính "Pa> pc" có được sử dụng không?

Số thập lục phân thứ sáu:

Bit 3: Thuộc tính "Pfa> av" có được sử dụng không?
Bit 2: Thuộc tính "Pfa> lav" có được sử dụng không?
Bit 1: "FMR" có được sử dụng để xác thực sinh trắc học không?
Bit 0: "FIR" có được sử dụng để xác thực sinh trắc học không?

Số thập lục phân thứ bảy:

Bit 3: "IIR" có được sử dụng để xác thực sinh trắc học không?
Bit 2: Thuộc tính "Pv-> pin" có được sử dụng không?
Bit 1: Thuộc tính "Pv-> Otp" có được sử dụng không?
Bit 0: "Tkn” có được sử dụng không?

Số thập lục phân thứ tám:

Bit 3: Thuộc tính "Pa> po" có được sử dụng không?
Bit 2: Thuộc tính "Pa> subdist" có được sử dụng không ?
Bit 1: Thuộc tính "Pa> dobt" có được sử dụng không?
Bit 0: Không sử dụng.

Những số thập lục phân từ thứ tám đến mười hai:

Hiện không sử dụng. Có thể có giá trị bằng 0.

Ví dụ, nếu một xác thực được thực hiện cho số Aadhaar "123412341234" và sử dụng các thuộc tính nhân khẩu học "name", "gender", "dob", "phone", cùng với sinh trắc học độ phân giải chi tiết vân tay (FMR) và mật khẩu dùng một lần (OTP);

<Pid ts="public" ver="1.0"><Demo><Pi ms="E" name="Anand John" gender="M" dob="19690126" phone="9999912345"/></Demo><Bios> <Bio type="FMR">
YjRmYmJkMTZkZGQ4OGQxYTY5YjI0M2ZiYjU4YTFlNmQwMmQ1YTgyYjNmODU4YT
MzYzQyZmNhOWUxN2QwNGVhNGMyMzExZjUyYmY4NjA5ZDVkZDY4YWU2NWE4OTNjNTMwNTJi
M2U1YzQ5YTZkMGM2NzkyYTJlOGNhMTMxNDg0YWQ2MWM1ZGYzZGU0MTAzNExZWVlN2E0MjU
4ZjQ3ODg3NTU3ZWNmYzcwY2NkM2QwZmIzZjg5OTg3NjEzNzA3ZDliZjkyMWU3NTc3OGU2NGJk
MmM3MDhiNGQ4NDgyZGJmMGM3YjY3ZGZkZGZkNjIyNgwMTllNjhhMmI4MjQxZWY0MA==

</Bio></Bios><Pv otp="111111"/></Pid>

thì giá trị của thuộc tính "thông tin" có thể là:

"0166c782e8f95ba958f28adaae576c42a263c2449af416fb844499bef7fd41b2d00212be474bf2
a6bfd4f361389ae66809babc144829129ae2315d6bab02045aa1B8002200000"

trong đó:

"01" – là phiên bản của cấu trúc thông tin

"66c782e8f95ba958f28adaae576c42a263c2449af416fb844499bef7fd41b2d0" – là thuật toán Hash bảo mật 256 (SHA-256) của số Aadhaar

"0212be474bf2a6bfd4f361389ae66809babc144829129ae2315d6bab020455aa" – là thuật toán Hash bảo mật 256 (SHA-256) của yếu tố "Demo" (như một chuỗi)

“1B8002200000” (bit nhị phân “00011011100000000000001000100000000000000000000”) – đại diện cho dữ liệu đã được mã hoá của tên (name), giới tính (gender), ngày sinh (date of birth), số điện thoại (phone), độ phân giải chi tiết vân tay (FMR), và mật khẩu sử dụng một lần (OTP) trong yêu cầu chứng thực.

Phụ lục 4

I. Mô tả chi tiết các thành phần kỹ thuật của Nền tảng cung cấp dịch vụ định danh điện tử (EISDP)

Các tính năng của cổng thông tin công cộng

1. **Thông tin công cộng và các dịch vụ di động.** Nền tảng cung cấp dịch vụ định danh điện tử (EISDP) có thể cung cấp cổng thông tin công cộng phổ biến để chia sẻ tất cả thông tin có liên quan đến các dịch vụ định danh điện tử (eID) có thể truy cập qua Internet. Các cổng thông tin có thể hỗ trợ trình duyệt Internet trên máy tính xách tay, máy tính để bàn và các thiết bị di động. Các cổng thông tin có thể có tất cả thông tin được công khai có sẵn cho người sử dụng, và một số nội dung có thể yêu cầu phải đăng ký và xác thực. Cổng thông tin công cộng còn có thể cung cấp khả năng đăng ký để truy cập vào nội dung được bảo vệ trên cổng thông tin. Cổng thông tin cũng có thể cung cấp thông tin liên quan đến Tổ chức cung cấp dịch vụ nhận dạng (ISPAs) và Tổ chức sử dụng dịch vụ nhận dạng (ISCAs).

2. **Thông tin nhà phát triển và các dịch vụ**. Cổng thông tin cũng có thể cung cấp nội dung cho các nhà phát triển phần mềm để giúp họ phát triển ứng dụng phần mềm hiển thị dịch vụ định danh điện tử (eID) trên Nền tảng cung cấp dịch vụ định danh điện tử (EISDP). Nội dung của các nhà phát triển có thể bao gồm hướng dẫn kỹ thuật sử dụng, mẫu mã, blog, các nhóm thảo luận và môi trường thử nghiệm cho các ứng dụng.

3. Cổng thông tin có thể được lưu trữ trên một tổ hợp cung cấp trang tin điện tử (web farm) cân bằng tải thuê trên các máy chủ web ảo tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Các phần mềm cổng thông tin có thể có nội dung và có những khả năng quản lý người dùng và hỗ trợ đa ngôn ngữ.

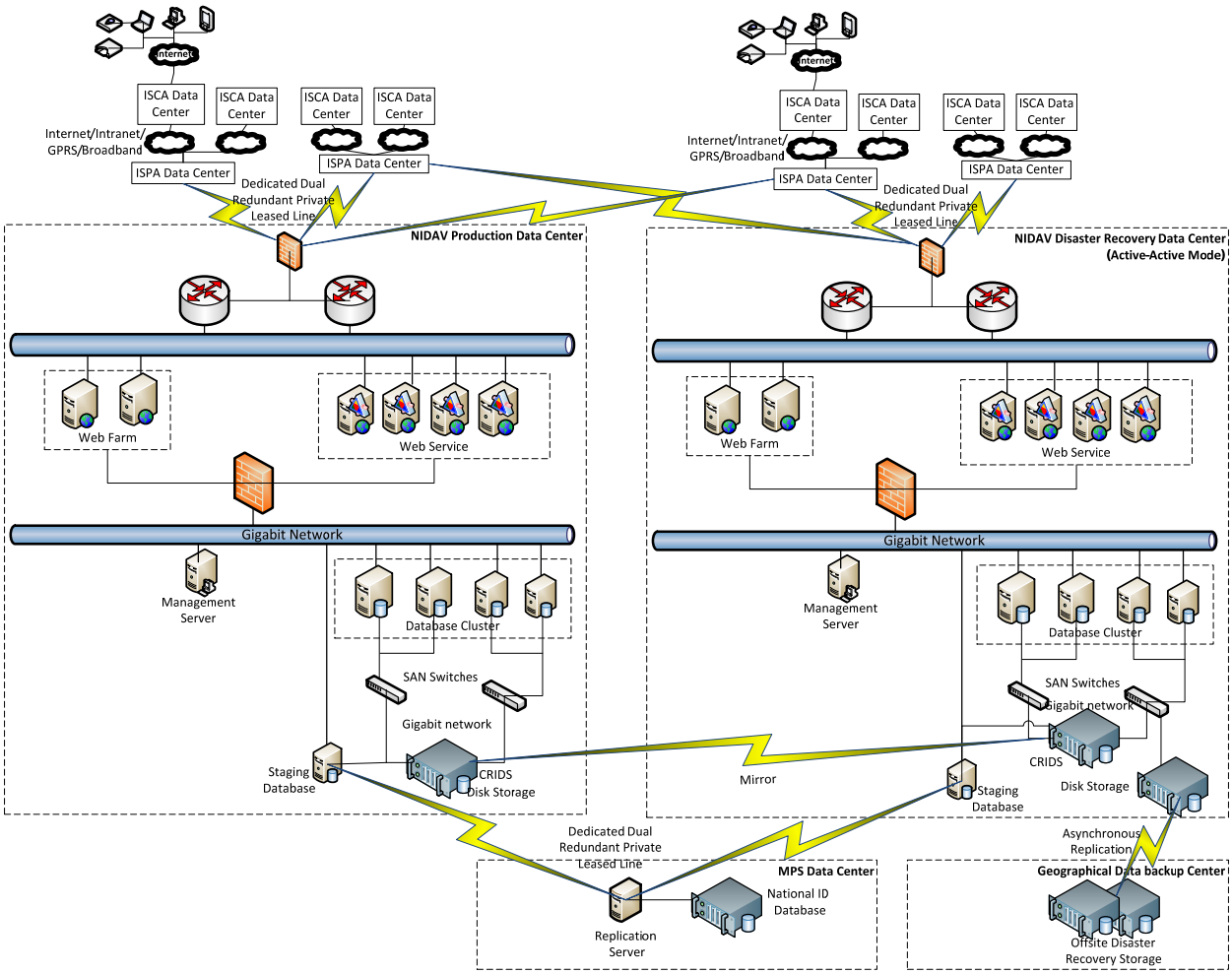
4. Môi trường phát triển có thể bao gồm việc lắp đặt các dịch vụ định danh điện tử (eID) như xác thực, nhận dạng và xác thực khách hàng điện tử (eKYC) và các dịch vụ nhận dạng di động như các dịch vụ web không quốc tịch. Các dữ liệu có thể được lưu trữ trên máy chủ cơ sở dữ liệu ở chế độ chủ động- chủ động (active-active) trợ giúp với Mạng vùng lưu trữ (SAN).

5. Cổng thông tin công cộng và môi trường phát triển có thể hỗ trợ chuyển đổi dự phòng từ một hệ thống khắc phục sự cố tại một vị trí địa lý khác với trung tâm dữ liệu. Hệ thống này

có thể chuyển sang sử dụng trang web phục hồi sự cố trong trường hợp có hư hỏng. Các dữ liệu từ cổng thông tin công cộng và cơ sở dữ liệu của môi trường phát triển có thể được nhân rộng trong một chế độ không đồng bộ với trang web sao lưu.

Cơ sở hạ tầng CNTT (phần cứng và phần mềm)

Nền tảng cung cấp dịch vụ định danh điện tử (EISDP) có thể là cơ sở hạ tầng CNTT chung và được chia sẻ dịch vụ để cung cấp dịch vụ định danh điện tử (eID) trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Nó có thể được lưu trữ tại tầng hai của mô hình 3 tầng (tier 3) trên trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) ở chế độ chủ động- chủ động (active-active). Các kiến trúc triển khai chi tiết được mô tả dưới đây.



Hình 8.1: Kiến trúc triển khai Nền tảng cung cấp dịch vụ định danh điện tử (EISDP)

1. Trung tâm dữ liệu của Cơ quan Quản lý Định danh điện tử Việt Nam (EIDAV)- nơi sản xuất và khắc phục sự cố - có thể được lưu trữ ở chế độ chủ động-chủ động với sự hỗ trợ chuyển đổi dự phòng cho nhau.

2. Các trung tâm dữ liệu có thể được kết nối với nhau bằng cách sử dụng cáp quang dựa trên đường kết nối thuê bao riêng với khả năng liên kết gấp đôi. Các trung tâm dữ liệu không thể truy cập trực tiếp từ các mạng công cộng mà chỉ được truy cập qua Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có đăng bằng đường kết nối thuê bao riêng với khả năng liên kết gấp đôi vào các trung tâm dữ liệu thuộc Tổ chức cung cấp dịch vụ nhận dạng (ISPA) và Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

3. Những yêu cầu băng thông có thể được tính toán dựa trên khối lượng giao dịch dự kiến từ các Tổ chức sử dung dịch vụ nhận dạng (ISCAs).
    a. Ước tính khoảng 5K băng thông trung bình là cần thiết cho mỗi giao diện lập trình ứng dụng (API).
    b. Xử lý khoảng một triệu giao dịch mỗi giờ đòi hỏi trung bình khoảng 280 giao dịch mỗi giây (tps). Khi tăng đột biến lên 30-40%, băng thông cho khoảng 400 tps cần phải được lên kế hoạch. Và sẽ rơi vào khoảng 16 Mbps (400 * 5K * 8 bit / giây)
    c. Các Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể bắt đầu với một liên kết 8 Mbps và mở rộng khi dung lượng tăng lên.

4. Dịch vụ định danh điện tử (eID) nói chung có thể được thể hiện như các dịch vụ web không quốc tịch. Nó có thể được lưu trữ trên các trang web ảo hoá với cụm máy chủ web ảo. Và có thể chạy các phần mềm của lớp nền tảng ảo hoá (hypervisor) để quản lý máy ảo trên một máy chủ riêng biệt. Nó còn có thể giúp quản lý dữ liệu và lấy dữ liệu lập dự phòng của các máy ảo trên các máy chủ. Hypervisor và bộ phần mềm quản lý máy ảo có thể được cài đặt để quản lý chung các cơ sở hạ tầng CNTT ảo và thật cho hai trung tâm dữ liệu trên. Nó cũng có thể thực hiện hỗ trợ chuyển đổi dự phòng bằng cách sử dụng sự di chuyển của các máy ảo trên các máy chủ thật và giữa các trung tâm dữ liệu.

5. Những ứng dụng kinh doanh dịch vụ định danh điện tử (eID) như Tổ chức cung cấp dịch vụ nhận dạng (ISPA) và Tổ chức sử dung dịch vụ nhận dạng (ISCA) đăng ký, quản lý và giám sát, báo cáo và các ứng dụng hệ thống thông tin quản lý (MIS), các ứng dụng phân tích, cổng thông tin mạng nội bộ, và giải pháp gửi thư có thể được lưu trữ trên một tổ hợp cung cấp trang tin điện tử (web farm) ảo hóa với các tổ hợp máy chủ web ảo.

6. Cả hai hệ thống web có thể được lưu trữ trong một khu vực an toàn của cơ sở hạ tầng mạng được tường lửa bảo vệ, và mạng cô lập riêng biệt với thiết bị chuyển mạch dự phòng để ngăn chặn bất kỳ truy cập gây hại nào từ bên ngoài của mạng riêng.

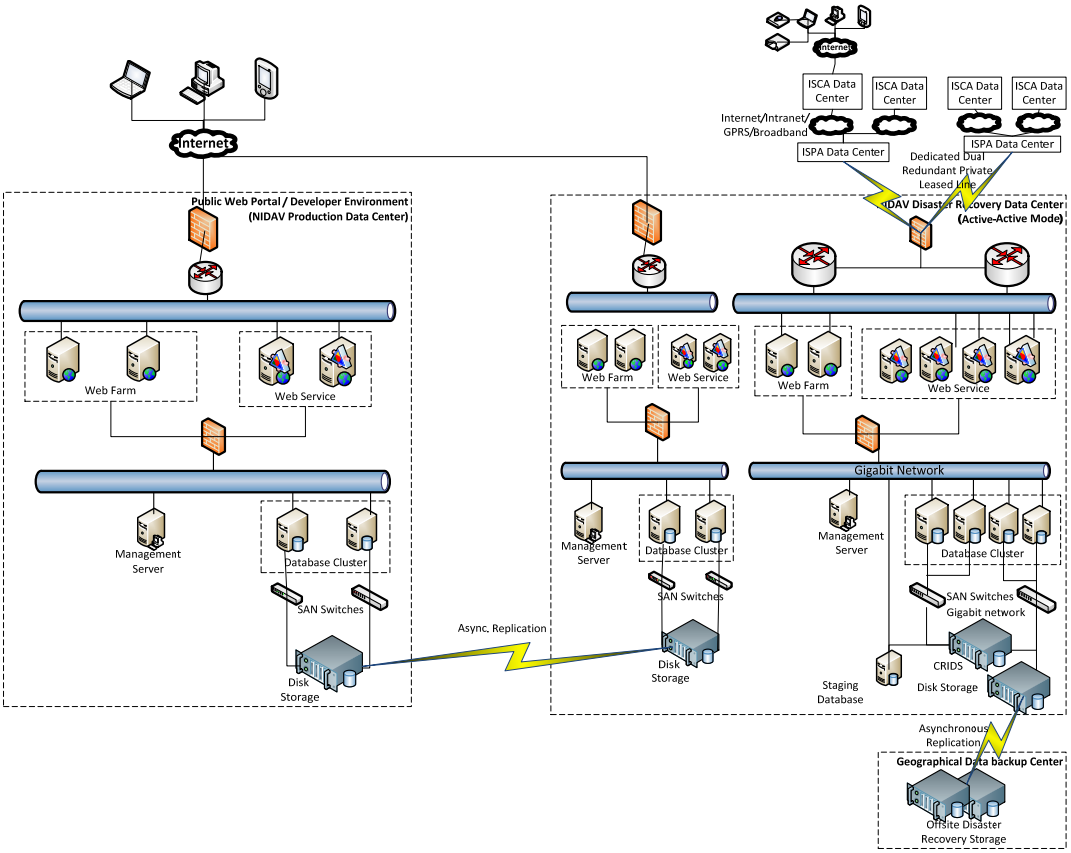
7. Dữ liệu có thể được lưu trữ trên các máy chủ và thiết bị lưu trữ trong vùng dữ liệu có thể được tách ra khỏi vùng an toàn bằng cách sử dụng tường lửa. Hệ thống lưu trữ dữ liệu có thể bao gồm các máy chủ cơ sở dữ liệu theo cụm với mạng vùng lưu trữ (SAN) kết nối với các máy chủ cơ sở dữ liệu ở chế độ hoạt động tích cực. Mạng vùng lưu trữ (SAN) có thể được kết nối với máy chủ cơ sở dữ liệu bằng cách sử dụng thiết bị chuyển mạch dự phòng lưu trữ trên một sợi cáp quang gigabit. Dung lượng lưu trữ của các phương tiện truyền thông trên mạng vùng lưu trữ (SAN) có thể dựa trên khối lượng giao dịch dự kiến từ các Tổ chức sử dung dịch vụ nhận dạng (ISCAs).
    a. Ước tính khoảng 5KB dữ liệu được sử dụng để lưu trữ một giao dịch.
    b. Đối với 10 triệu giao dịch mỗi ngày, lưu trữ mạng vùng lưu trữ (SAN) có thể yêu cầu 50 GB dung lượng.
    c. Nếu lưu trữ dữ liệu trực tuyến của một tháng là cần thiết, thì 1,5 TB dung lượng lưu trữ trực tuyến được yêu cầu về lưu trữ SAN vượt lên có thể được chuyển vào băng.
    d. Ước tính, kích thước của dữ liệu chứng minh nhân dân cho một người dân là 5 MB. Điều này bao gồm các dữ liệu nhân chủng học và sinh trắc học. Các dữ liệu sinh trắc học có thể bao gồm 10 dấu vân tay, ảnh chụp, và 2 lần quét võng mạc. Tổng kích thước cần thiết để lưu trữ dữ liệu của 91 triệu dân của Việt Nam tăng với tỷ lệ 10% sẽ có khoảng 500 TB (100 triệu x 5 MB) vào năm 2015.
    e. Tổng dung lượng lưu trữ mạng vùng lưu trữ (SAN) cho các dữ liệu ID của tất cả người dân Việt Nam và dữ liệu giao dịch của một tháng có thể xấp xỉ 500 TB.
    f. Tổng chi phí của đĩa 15K RPM SAS sẽ là 800.000 đô la Mỹ - dựa trên chi phí 1.600 đô la Mỹ cho mỗi một TB.

8. Lưu lượng truy cập trên mạng vùng lưu trữ (SAN) sẽ sử dụng một Gigabit Ethernet (GbE) trong vùng dữ liệu để truyền dữ liệu giữa các trang web chủ trong vùng an toàn và các cụm cơ sở dữ liệu trong vùng dữ liệu. Nó cũng sẽ được sử dụng cho mạng vùng lưu trữ (SAN) giữa các phương tiện lưu trữ và các cụm máy chủ cơ sở dữ liệu. Kiến trúc mạng có thể bao gồm cáp, card mạng, chuyển mạch lớp tập hợp, và Top-of-Rack (ToR) chuyển mạch. Chi phí đầu tư có thể bao gồm chuyển mạch lõi mạng, cáp, card mạng, chuyển mạch lớp tập hợp và chi phí chuyển đổi ToR. Kinh phí hoạt động sẽ bao gồm việc sử dụng

nguồn điện và làm mát, điện tử và cập nhật cơ sở hạ tầng cơ bản, tăng trưởng dự kiến, quản lý và các chi phí rủi ro.

9. Trung tâm phục hồi sự cố có thể có cấu hình và tính năng tương tự như của các trung tâm dữ liệu sản xuất và sẽ vận hành ở chế độ chủ động-chủ động.

10. Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) cũng có thể cung cấp một cổng thông tin công cộng có thể truy cập qua Internet. Cổng thông tin công cộng, ngoài việc cung cấp dịch vụ nhận dạng thông tin liên quan đến người dân và các tổ chức cá nhân, cũng có thể cung cấp thông tin nhằm vào các nhà phát triển phần mềm – những người có thể muốn thiết kế các ứng dụng dựa trên định danh điện tử (eID). Cổng thông tin công cộng cũng sẽ mở ra môi trường phát triển cho các ứng dụng thử nghiệm. Kiến trúc triển khai kỹ thuật cho các cổng thông tin công cộng và môi trường phát triển được mô tả như dưới đây.



Hình 8.2: Kiến trúc triển khai kỹ thuật cho môi trường phát triển và Cổng thông tin công cộng

11. Cổng thông tin công cộng và môi trường phát triển có thể được lưu trữ trong trung tâm dữ liệu sản xuất của Cơ quan Quản lý Định danh điện tử Việt Nam (EIDAV) với sự hỗ trợ chuyển đổi dự phòng từ trung tâm của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) phục hồi dữ liệu sau thảm hoạ. Chúng có khả năng chịu lỗi và giải pháp cân bằng tải trên cả hai trung tâm.

12. Cổng thông tin công cộng và các máy chủ môi trường phát triển có thể được truy cập qua Internet và có thể bị cô lập hoàn toàn từ các máy chủ và mạng lưới an toàn và các vùng dữ liệu trong khu phi quân sự (DMZ). Các máy chủ của họ có thể được lưu trữ trên một phân đoạn khác của mạng tách biệt hoàn toàn với các máy chủ trong tuyến bảo mật và các vùng dữ liệu.

13. Cổng thông tin công cộng có thể được lưu trữ trên các hệ thống web ảo trên các máy ảo được lưu trữ trên hai cụm máy chủ web thật.

14. Môi trường phát triển có thể mở ra các chức năng nhận dạng như các dịch vụ web trên hệ thống web ảo trên các máy ảo được lưu trữ trên các cụm máy chủ web thật.

15. Các máy chủ quản lý có thể chạy các phần mềm quản lý máy ảo. Nó có thể giúp quản lý việc cấp và lấy dữ liệu của hypervisor và máy ảo trên các máy chủ. Hypervisor và phần mềm quản lý máy ảo phù hợp có thể được cài đặt bộ phần mềm quản lý cơ sở hạ tầng chung cả thật và ảo cho hai trung tâm dữ liệu. Nó cũng có thể thực hiện hỗ trợ chuyển đổi dự phòng bằng cách sử dụng sự di chuyển của các máy ảo trên máy chủ thật và trên các trung tâm dữ liệu.

16. Cả hai hệ thống web có thể được lưu trữ trong khu phi quân sự (DMZ) và có thể được truy cập được trên Internet.

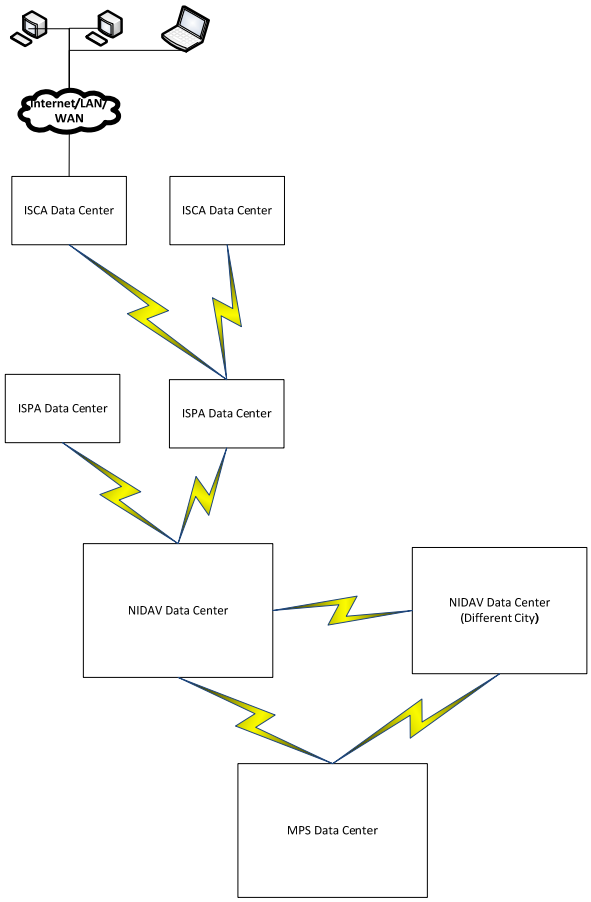
17. Cơ sở dữ liệu môi trường phát triển và các tài liệu trong máy chủ quản lý nội dung có thể được lưu trữ trong khu vực dữ liệu an toàn tách ra từ khu phi quân sự (DMZ) bởi tường lửa.

18. Cơ sở dữ liệu nhận dạng mẫu cho các môi trường phát triển có thể được lưu trữ trên cụm máy chủ kết nối với SAN sử dụng thiết bị chuyển mạch kép qua sợi cáp quang dựa vào mạng Ethernet.

19. Dung lượng lưu trữ trên mạng vùng lưu trữ (SAN) sẽ vào khoảng 15 TB.

Cơ sở hạ tầng vật chất

Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể đòi hỏi phải triển khai các cơ sở hạ tầng như các trung tâm dữ liệu tại các địa bàn khác nhau dựa trên các yêu cầu triển khai và tổ chức trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Hình dưới đây mô tả về khả năng tổ chức cơ sở hạ tầng vật chất cần xây dựng để triển khai Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF).



Hình 8.3: Cách thức tổ chức cơ sở hạ tầng vật chất cho Khuôn khổ cung cấp dịch vụ định danh điện tử (EISDF)

Những tính năng của trung tâm dữ liệu Cơ quan Quản lý Định danh điện tử Việt Nam (EIDAV)

1. Nền tảng cung cấp dịch vụ định danh điện tử (EISDP) có thể được lưu trữ tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Tất cả các chức năng nhận dạng trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể được lưu trữ tại trung tâm dữ liệu này và các dịch vụ có thể được sử dụng bởi các ứng dụng quan trọng của chính phủ và các tổ chức thuộc khối tư nhân; Vì vậy, trung tâm dữ liệu này có thể được chỉ định cơ sở hạ tầng quan trọng.

2. Trung tâm dữ liệu có thể được thiết kế như một trung tâm dữ liệu tier 3 với 99,982% thời gian. Thiết kế có thể bao gồm kiến trúc xây dựng, cơ sở cấu trúc liên kết, cơ sở hạ tầng kỹ thuật và cơ sở hạ tầng công nghệ. Cơ sở cấu trúc liên kết có thể bao gồm quy hoạch không gian. Cơ sở hạ tầng kỹ thuật có thể giải quyết hệ thống cơ khí liên quan đến việc duy trì môi trường bên trong của một trung tâm dữ liệu như sưởi, thông gió và điều hòa nhiệt độ (HVAC). Đồng thời cũng có thể bao gồm cơ sở hạ tầng điện như dịch vụ tiện ích, phân phối, chuyển đổi, và bỏ qua từ các nguồn điện, bộ lưu điện (UPS), vv. Thiết kế hệ thống điện có thể tuân thủ theo các yêu cầu hiệu quả sử dụng điện (PUE) và tiêu chuẩn năng lượng.

3. Tòa nhà trung tâm dữ liệu có thể được xây dựng trên diện tích 1.000 mét vuông. Tòa nhà sẽ có phòng máy chủ, phòng điều khiển trung tâm, trung tâm quản lý mạng, phòng phân phối UPS, phân phối điện và phòng quản lý, phòng kiểm soát cháy, phòng hội nghị và các phòng trưng bày, ...

Các tính năng trung tâm phục hồi sự cố của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV)

1. Trung tâm khôi phục dữ liệu sau thảm họa sẽ được xây dựng ở một vị trí địa lý khác như là một thành phố khác trong một vùng địa chấn khác với các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Nó sẽ cung cấp các hỗ trợ chuyển đổi dự phòng cho các dịch vụ nhận dạng, các ứng dụng và cơ sở hạ tầng CNTT của các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Nó sẽ làm việc ở chế độ chủ động- chủ động (active-active) và sẽ tổ chức các dịch vụ nhận dạng và các ứng dụng để cung cấp giải pháp cân bằng tải và khả năng chịu lỗi cho các trung tâm dữ liệu của Cơ quan Quản lý Định danh điện tử Việt Nam (EIDAV) trong trường hợp thất bại.

2. Kích thước xây dựng có thể cũng giống như các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) là 1.000 mét vuông. Thông số kỹ thuật tòa nhà cũng sẽ giống nhau đối với cơ sở hạ tầng thiết kế cơ khí, điện và viễn thông.

3. Mạng giữa hai trung tâm dữ liệu sẽ là kết nối dự phòng kép được thuê riêng.

Những tính năng trung tâm dữ liệu của Bộ Công An

1. Trung tâm dữ liệu của Bộ Công An (MPS) tương tự như nơi lưu trữ các cơ sở dữ liệu nhận dạng quốc gia.

2. Hệ thống định danh điện tử quốc gia (NID) trong cơ sở dữ liệu của Bộ Công An được sử dụng để lưu trữ trong cơ sở dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Dữ liệu có thể được chuyển bằng cách sử dụng một cơ chế sao chép cơ sở dữ liệu bảo mật cao.

3. Có một đường dây dự phòng kép chuyên dụng thiết lập đường truyền cho thuê riêng cài đặt giữa các trung tâm dữ liệu của Bộ Công An và hai trung tâm dữ liệu của Cơ quan Quản lý Định danh điện tử Việt Nam (EIDAV).

Hệ thống an toàn và an ninh

Nền tảng cung cấp dịch vụ định danh điện tử (EISDP) cung cấp các dịch vụ an ninh chung có thể được sử dụng bởi các dịch vụ lưu trữ trên nền tảng này. Vấn đề được thảo luận như dưới đây.

1. An ninh mạng từ nguồn tới đích (end-to-end) có thể được thực hiện bằng cách sử dụng thực hành mạng tiêu chuẩn như sử dụng các kênh mã hóa, sử dụng giấy chứng nhận kỹ thuật số, lọc địa chỉ IP, xác thực của các hệ thống và các thiết bị, bảo vệ mạng thông qua các bức tường lửa và hệ thống bảo vệ xâm nhập mạng (NIPS), kiểm toán, vv.

2. Nhiều mức độ an ninh mạng thông qua sự sáng tạo của khu phi quân sự (DMZ), ứng dụng và dữ liệu khu vực, và bảo vệ tất cả các vùng dữ liệu sử dụng nhiều tường lửa, hệ thống bảo vệ xâm nhập mạng (NIPS), và kiểm soát chặt chẽ truy cập và kế hoạch kiểm toán.

3. Các máy chủ lưu trữ các dịch vụ sẽ chỉ được tiếp xúc với các nhà cung cấp dịch vụ ủy quyền thông qua các kết nối bảo mật riêng sử dụng đường truyền để đảm bảo nhiều điểm kết cuối tồn tại để cung cấp dịch vụ trong một chế độ luôn luôn có sẵn.

4. Cơ sở vật chất hạ tầng bảo mật sẽ có nhiều cấp độ của hệ thống bảo mật cho phép cá nhân đã được xác nhận truy nhập dựa trên các yếu tố như sinh trắc học, so với những cơ sở hạ tầng khác.

Dịch vụ xác thực nhận dạng điện tử

Việc xác thực định danh điện tử (eID) có thể được thực hiện bằng cách sử dụng dữ liệu nhân khẩu học và/hoặc dữ liệu sinh trắc học và/hoặc mật khẩu sử dụng một lần (OTP)/Giấy chứng nhận kỹ thuật số. Có nhiều cách để người dân có thể xác thực được và chi tiết sẽ được thảo luận dưới đây.

1. Các hàm xác thực định danh điện tử có thể được thực hiện trên dịch vụ web không quốc tịch trên Giao thức truyền siêu văn bản an toàn (HTTPS). Việc sử dụng các định dạng dữ liệu mở trong Ngôn ngữ đánh dấu khả mở (XML) và giao thức được sử dụng rộng rãi như Giao thức truyền siêu văn bản (HTTP) có thể cho phép áp dụng dễ dàng và triển khai xác thực định danh điện tử (eID). Việc xác thực định danh điện tử (ID) có thể được thực hiện dưới định dạng Bộ định vị tài nguyên đồng nhất (URL) với các dữ liệu đầu vào gửi đến URL này như một tài liệu Ngôn ngữ đánh dấu khả mở (XML) bằng cách sử dụng loại nội dung ứng dụng/XML hoặc văn bản/XML. Câu trả lời tương ứng từ dịch vụ này cũng có thể dưới định dạng XML.

2. Các hàm xác thực định danh điện tử có thể được thể hiện dưới các hình thức của các Giao diện lập trình ứng dụng (API) có thể được sử dụng bởi các nhà cung cấp dịch vụ để kết hợp các loại hình dịch vụ xác thực định danh điện tử và các tính năng trong ứng dụng cung cấp dịch vụ của chúng.

3. Nền tảng cung cấp dịch vụ định danh điện tử (EISDP) có thể duy trì một phiên bản cập nhật thông tin định danh điện tử của công dân, như: Mã số định danh công dân (NIN) + dữ liệu nhân khẩu học và sinh trắc học, Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Dịch vụ chứng thực định danh điện tử có thể được lưu trữ trên máy chủ xác thực nhận dạng điện tử; và Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS), trên một máy chủ cơ sở dữ liệu riêng biệt. Hai máy chủ này đều được lưu trữ trong trung tâm dữ liệu có độ bảo mật cao của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

4. Để đảm bảo cho một giải pháp có khả năng mở rộng và chịu lỗi, đáp ứng được thời gian phản ứng của các thoả thuận về mức độ dịch vụ (SLAs), các dịch vụ xác thực định danh điện tử (eID) và Trung tâm Lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) được lưu trữ trên cân bằng tải và cụm thiết lập dựa trên bộ máy chủ. Các dịch vụ xác thực định danh điện tử (eID), cùng với Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS), có thể được lưu trữ trên một khu vực an toàn và chỉ tiếp xúc với các nhà cung cấp dịch vụ đã được ủy quyền thông qua các kết nối cá nhân sử dụng đường

truyền để đảm bảo nhiều điểm kết cuối tồn tại để cung cấp dịch vụ trong một chế độ luôn luôn sẵn có.

5. Để đảm bảo an ninh từ nguồn tới đích (end-to-end) và tránh yêu cầu giả mạo và các cuộc tấn công của người trung gian (man-in-the-middle attack), điều quan trọng là mã hóa dữ liệu diễn ra tại thời điểm thu thập dữ liệu từ thiết bị. Vì lý do bảo mật nên những dữ liệu thu thập được của công dân để xác thực định danh điện tử (eID) có thể không được lưu trữ trong các thiết bị hoặc các file bản ghi. Nó cũng rất cần thiết cho các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) và các Tổ chức cung cấp dịch vụ nhận dạng (ISPAs) để duy trì hồ sơ kiểm toán cho tất cả các siêu dữ liệu yêu cầu xác thực đi kèm các phản ứng.

6. Cơ sở dữ liệu của định danh điện tử (eID) trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) có thể được gắn linh kiện vào và cập nhật một cách thường xuyên sử dụng một quá trình tạo danh tính tập trung cấp quốc gia. Thay vì tái tạo quá trình này, Nền tảng cung cấp dịch vụ định danh điện tử (EISDP) có thể tái sử dụng các dữ liệu công dân của Bộ Công An (MSP) thu thập được trong việc ban hành các dữ liệu trong Hệ thống định danh điện tử quốc gia (NID) và mã số chứng minh nhận dạng quốc gia (NIN).

7. Được biết Hệ thống định danh điện tử quốc gia (NID) và Mã số định danh công dân (NIN) hiện đang được thử nghiệm bởi Bộ Công An (MPS) ở cấp quốc gia, có thể đây là một quá trình duy nhất để tạo ra nhận dạng và xác minh. Do đó vấn đề với việc có nhiều danh tính cho cùng một công dân có thể được giải quyết. Thẻ của Hệ thống định danh điện tử quốc gia (NID) có thể được sử dụng như bằng chứng thông báo nhận dạng được phát hành chung ở cấp quốc gia để xác nhận tính duy nhất của công dân, trong khi Mã số định danh công dân (NIN) có thể được sử dụng như là định danh duy nhất cho định danh điện tử (eID) của người công dân trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF).

8. Chức năng xác thực định danh điện tử (eID) có thể lấy Mã số định danh công dân (NIN) cùng với Dữ liệu nhận dạng cá nhân (PID) của người sở hữu định danh điện tử (eID) như là đầu vào có thể gửi dữ liệu vào Trung tâm Lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) để so khớp, sau đó Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) sẽ xác minh tính chính xác của dữ liệu được cung cấp trên cơ sở khớp với thông tin nhận dạng sẵn có của người sở hữu định danh điện tử (eID). Dịch vụ này có

thể phản hồi lại với câu trả lời "có / không" hoặc xác nhận các giấy tờ chứng minh hoặc xác minh các thông tin do công dân cung cấp.

9. Trong tất cả các hình thức xác thực định danh điện tử (eID), Mã số định danh công dân (NIN) có thể được gửi cùng với các xác thực đơn/đa yếu tố như vậy mà kết quả được giảm xuống để đối chiếu 1: 1.

10. Chức năng xác thực có thể tìm kiếm và chọn lọc bản ghi thông tin của công dân trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) sử dụng Mã số chứng minh nhận dạng quốc gia (NIN); sau đó các đầu vào nhân khẩu học/sinh trắc học được so sánh với dữ liệu lưu trữ do công dân cung cấp trong quá trình đăng ký/cập nhật.

11. Việc thực hiện các kiểu xác thực nhân khẩu học có thể bao gồm sự so sánh của các thuộc tính nhân khẩu học cơ bản sau đây:
    - Tên tiếng Anh và tiếng Việt
    - Địa chỉ
    - Giới tính
    - Ngày sinh (ngày đầy đủ hoặc chỉ năm)
    - Tuổi (xác minh nếu một công dân là trên/dưới một độ tuổi được đưa ra)
    - Điện thoại (số điện thoại di động được xác nhận của công dân)
    - Email (địa chỉ thư điện tử được xác nhận của công dân)

12. Các dữ liệu nhân khẩu học khớp với tính năng có thể được thực hiện dựa trên thiết kế sau.
    - **Đối chiếu tên**. Điều này có thể cho phép xác minh tên của công dân đối với hồ sơ của họ được lưu trữ trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Tính năng tên phù hợp có thể thực hiện những phương thức khác nhau có thể là khớp chính xác hoàn toàn hoặc chỉ khớp một phần với mức độ chấp nhận được và dựa trên những nhu cầu để áp dụng (ví dụ, một sự so sánh chặt chẽ với một sự so sánh linh hoạt hơi lỏng lẻo), các phương thức khác nhau có thể được sử dụng tuỳ theo. Ví dụ, khi một ứng dụng ngân hàng có thể lựa chọn phương thức so sánh từng phần, ứng dụng hộ chiếu/thị thực có thể được chọn để so sánh khi nó đòi hỏi tên thật đầy đủ của một công dân (như được tìm thấy trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS)). Một ví dụ khác: một người dân với Mã số định danh công dân (NIN) 123443211234 và có tên trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) là "Kim Pham Nguyen" muốn mở một tài khoản ngân hàng. Các ứng dụng ngân hàng xác thực nhân khẩu học bằng cách sử dụng quá trình

Nhận dạng và xác thực khách hàng điện tử (eKYC) vì những ứng dụng này không đòi hỏi cung cấp tên đầy đủ chính xác, và thay vào đó sẽ cho phép một tên khớp với từng phần. Nếu ứng dụng sử dụng phương thức so sánh từng phần và quy định giá trị khớp (hoặc các mức) là 50 - có nghĩa là các từ phải trùng khớp tới 50% hoặc hơn trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS)- và sau khi thu nhập được tài khoản của khách hàng mới có thể được tạo lập. Các quy tắc để phù hợp với tên được mô tả chi tiết trong Phụ lục 2.

- **Đối chiếu ngày sinh**. Điều này có thể cho phép cập nhật đầy đủ ngày sinh hoặc chỉ yêu cầu năm sinh.
- **Đối chiếu tuổi**. Một số lợi ích mà công dân được hưởng từ chính phủ có thể có những yêu cầu về tuổi. Tính năng này có thể so sánh độ tuổi của cá nhân được lưu giữ trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) với độ tuổi quy định tại thời điểm cung cấp dịch vụ.
- **Đối chiếu điện thoại di động và email**. Tính năng này có thể so sánh các số điện thoại di động và địa chỉ email được lưu trữ trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) với những cá nhân được cung cấp tại thời điểm cung cấp dịch vụ.
- **Đối chiếu địa chỉ**. Một số dịch vụ như ngân hàng, truyền thông, và phúc lợi của chính phủ tại Việt Nam phụ thuộc vào xác minh địa chỉ để hoàn tất giao dịch ban đầu và bắt đầu quá trình Nhận dạng và xác thực khách hàng (KYC). Hiện nay, việc xác minh được thực hiện thông qua các tài liệu trên giấy đó cũng là cơ sở để đảm bảo giao dịch trong việc thực hiện các yêu cầu quy định. Địa chỉ cần so sánh có thể được thực hiện trực tuyến bằng cách kiểm tra địa chỉ này với các dữ liệu trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Cấu trúc địa chỉ phổ biến quy định của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) với sự giúp đỡ của các Bộ, ban ngành và các cơ quan khác có thể được sử dụng để lưu trữ và so sánh với địa chỉ thị xã và nông thôn dưới định dạng điện tử. Địa chỉ được so sánh ở cấp độ này có thể hỗ trợ sau đây.
    i. **Đối chiếu địa chỉ có cấu trúc** cho phép các trường như thôn / thành phố, xã, huyện, tỉnh, mã vùng, vv, được so sánh riêng lẻ hoặc kết hợp. Tính năng này có thể cho phép xác minh địa chỉ của các ứng dụng của nhà cung cấp dịch vụ và có thể cung cấp tùy chọn để xác nhận địa chỉ sử dụng cấu trúc địa chỉ chuẩn định danh điện tử (eID) toàn bộ hoặc một phần. Cấu trúc địa chỉ chuẩn đề xuất được quy định tại Phụ lục 3. Ví dụ, khi phát hành SIM, ứng dụng điều hành viễn thông có thể nắm bắt địa chỉ và chỉ đơn giản là kiểm tra các tỉnh, huyện hoặc mã vùng để đảm bảo rằng các công dân

thuộc về một phạm vi viễn thông nói riêng. Để nhập dữ liệu trong các ứng dụng nhanh hơn, thẻ Hệ thống định danh điện tử quốc gia (NID) có thể chứa một mã vạch 2-D hoặc mã phản hồi nhanh (mã QR) được viết ở định dạng XML có thể được đọc với một trang web / máy ảnh điện thoại di động tiêu chuẩn. Ứng dụng cung cấp dịch vụ được khuyến khích để quét mã vạch 2-D trên thẻ Hệ thống định danh điện tử quốc gia (NID) để các trường địa chỉ được gán vào theo một cách có cấu trúc. Nếu một ứng dụng không quét mã vạch, nhưng cần phải có các dữ liệu địa chỉ tự nhập vào từ thẻ của Hệ thống định danh điện tử quốc gia (NID) dưới dạng một chuỗi đơn, thì phương thức so sánh địa chỉ phi cấu trúc có thể được sử dụng. Phương thức so sánh chi tiết với địa chỉ phi cấu trúc được quy định tại Phụ lục 2. Địa chỉ có cấu trúc có thể bao gồm các lĩnh vực sau đây có thể được xác nhận độc lập hoặc kết hợp:

- Các trường có lưu lượng miễn phí (do công dân cung cấp)
  - ✓ Tên người
  - ✓ Ký hiệu nhận dạng nhà (chuỗi đơn có chứa nhà, chung cư, hoặc số nhà, tên, vv)
  - ✓ Ký hiệu nhận dạng đường (chuỗi đơn có chứa số, tên đường)
  - ✓ Chi tiết điểm mốc
  - ✓ Tên Địa phương và các chi tiết
- Các trường được dựa trên dữ liệu tổng thể được mã hóa
  - ✓ Tên thôn/thị xã/thành phố
  - ✓ Tên khu vực
  - ✓ Tên tỉnh
  - ✓ Tên huyện
  - ✓ Tên xã
  - ✓ Mã vùng
  - ✓ Tên Bưu điện

ii. **Đối chiếu địa chỉ phi cấu trúc** được sử dụng khi nhà cung cấp dịch vụ áp dụng việc ghi chép địa chỉ thủ công từ thẻ của Hệ thống định danh điện tử quốc gia (NID) hoặc từ những thông tin do công dân cung cấp. Điều này cho phép một địa chỉ được lưu giữ dưới dạng một chuỗi đơn và được kết hợp với địa chỉ trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS). Mặc dù lựa chọn này là dễ dàng cho việc xác minh dữ liệu hiện có hoặc tự nhập vào, nó yêu cầu việc so sánh không theo một

trật tự nghiêm ngặt và không đòi hỏi phải có tất cả các phần của địa chỉ đầy đủ. Vì lý do này, xác thực định danh điện tử (eID) có thể cho phép phương thức so sánh từng phần với địa chỉ cần so sánh và các ứng dụng này có thể được phép lựa chọn mức độ trùng khớp với khả năng cho phép dựa trên nhu cầu của họ. Nhìn chung, trong khi so sánh có cấu trúc cung cấp kết quả chính xác hơn, thì so sánh phi cấu trúc lại cho phép sự linh hoạt hơn.

13. Dịch vụ xác thực sinh trắc học sẽ cho phép các ứng dụng của các nhà cung cấp dịch vụ xác nhận xem công dân đó có "là người được khai báo hay không". Một số ứng dụng có thể đòi hỏi phải xác nhận vật lý bằng người thực. Việc triển khai xác thực sinh trắc học sẽ có các tính năng sau:
    - **Đối chiếu dấu vân tay**. Điều này có thể cho phép một trong nhiều ngón tay sẽ được sử dụng để so sánh tùy theo nhu cầu của ứng dụng. Sử dụng nhiều ngón tay cho phép phương thức kết hợp tốt hơn trên máy chủ xác thực cho chính xác hơn. Xác thực bằng cách sử dụng dấu vân tay hoặc vân tay có thể là độ phân giải chi tiết vân tay (FMR) hoặc độ phân giải hình ảnh vân tay (FIR). Trong khi các ứng dụng cho độ phân giải chi tiết vân tay (FMR) có thể hoạt động trên mạng băng thông thấp, thì những ứng dụng cho độ phân giải hình ảnh vân tay (FIR) sẽ yêu cầu băng thông cao hơn.
    - **Đối chiếu võng mạc**. Nói chung, so sánh võng mạc chính xác hơn so sánh dấu vân tay. So sánh võng mạc dựa trên độ phân giải hình ảnh võng mạc (IIR).

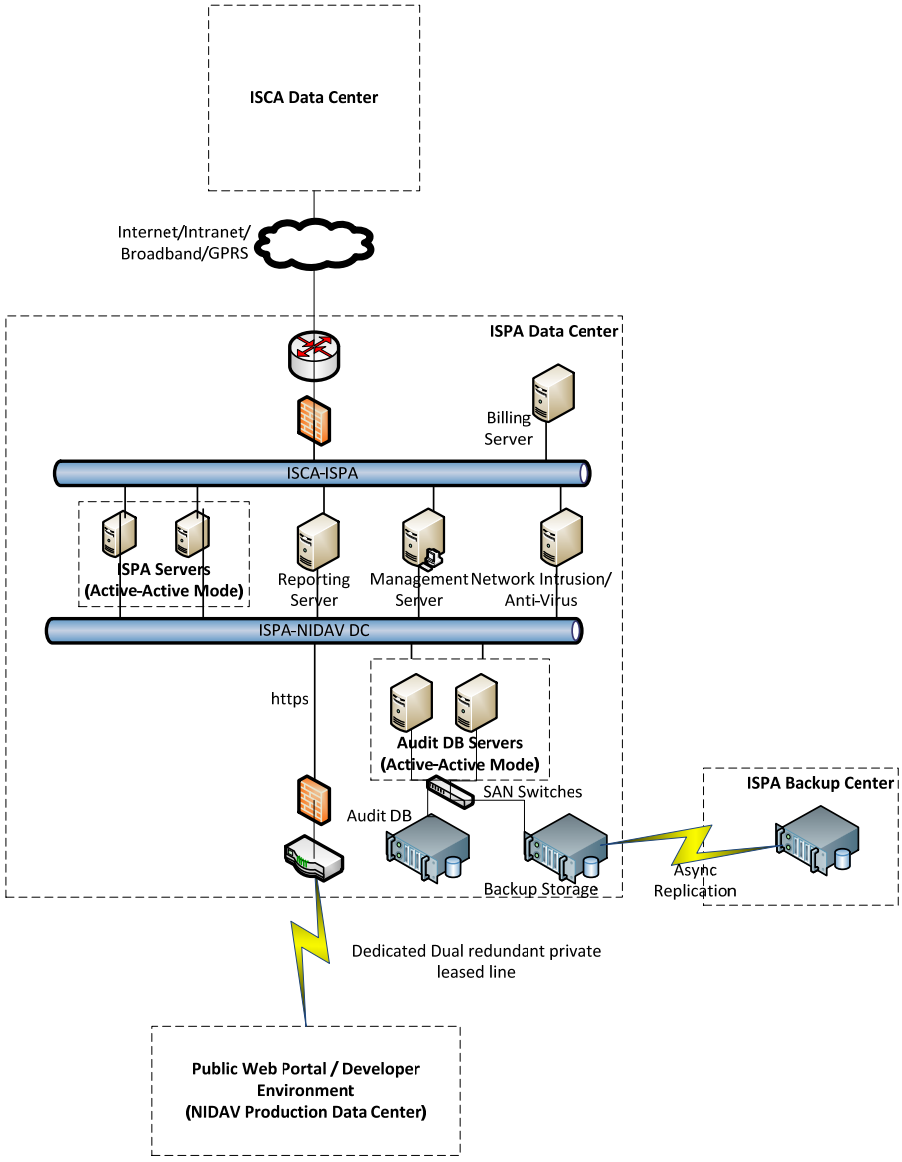
14. Dữ liệu sinh trắc học do thiết bị đầu vào thu thập cần tuân thủ với các chuẩn mở . Độ phân giải chi tiết vân tay (FMR) có thể tuân thủ tiêu chuẩn ISO 19794-2 định dạng tiểu tiết ngón tay không có tiện ích mở rộng độc quyền. Độ phân giải hình ảnh vân tay (FIR) có thể thực hiện theo tiêu chuẩn ISO 19794-4 định dạng hình ảnh đó sẽ có một hình ảnh nén hay không nén, dạng PNG, WSQ, hoặc jpeg2000. Độ phân giải hình ảnh vân tay (FIR) có thể tuân thủ các tiêu chuẩn ISO 19794-6 định dạng hình ảnh đó sẽ là loại png, hoặc jpeg2000.

15. Để cải thiện độ chính xác và giảm số lượng các trận đấu, yêu cầu xác thực sinh trắc học có thể chứa các "gợi ý vị trí" cho mỗi mẫu sinh trắc học. Gợi ý vị trí được sử dụng trên máy chủ để tối ưu hóa của việc so sánh. Các giá trị gợi ý vị trí hợp lệ là LEFT_IRIS, RIGHT_IRIS, LEFT_INDEX, LEFT_LITTLE, LEFT_MIDDLE, LEFT_RING, LEFT_THUMB, RIGHT_INDEX, RIGHT_LITTLE, RIGHT_MIDDLE, RIGHT_RING, và RIGHT_THUMB.

Những tính năng trung tâm dữ liệu của Tổ chức cung cấp dịch vụ nhận dạng (ISPA)

1. Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể là một doanh nghiệp tư nhân hoặc nhà nước. Các Tổ chức cung cấp dịch vụ nhận dạng (ISPA) cung cấp kết nối mạng riêng cho các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) và chuyển tiếp yêu cầu dịch vụ nhận dạng đến Nền tảng cung cấp dịch vụ định danh điện tử (EISDP). Chỉ có cơ quan ký hợp đồng với Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) như các Tổ chức cung cấp dịch vụ nhận dạng (ISPAs) có thể gửi yêu cầu dịch vụ nhận dạng để các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Quá trình đăng ký Tổ chức cung cấp dịch vụ nhận dạng (ISPA), cũng như hướng dẫn kỹ thuật chi tiết để thành lập và hoạt động của trung tâm Tổ chức cung cấp dịch vụ nhận dạng (ISPA), có thể được công bố trên cổng thông tin công cộng trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF).

2. Các Tổ chức cung cấp dịch vụ nhận dạng (ISPAs) có thể thiết lập dự phòng kép và kết nối đường thuê bao riêng chuyên dụng giữa các trung tâm dữ liệu và các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Một trung tâm dữ liệu của Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể là một cơ sở hạ tầng quan trọng trong việc cung cấp các dịch vụ nhận dạng; do đó, thiết kế của nó sẽ bao gồm một giải pháp khắc phục thảm họa với sự hỗ trợ sao lưu dữ liệu từ xa. Các Tổ chức cung cấp dịch vụ nhận dạng (ISPAs) sẽ thiết lập trung tâm dữ liệu của họ với khả năng mở rộng hỗ trợ cho các Tổ chức sử dung dịch vụ nhận dạng (ISCAs). Kiến trúc triển khai kỹ thuật cho các trung tâm dữ liệu được mô tả trong Hình 8.4.



Hình 8.4: Kiến trúc triển khai kỹ thuật cho các trung tâm dữ liệu ISPA

3. Những yêu cầu băng thông cho các trung tâm dữ liệu của Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể được tính dựa trên khối lượng giao dịch dự kiến từ các Tổ chức sử dụng dịch vụ nhận dạng (ISCAs). Khoảng băng thông 5K là cần thiết cho mỗi giao diện lập trình ứng dụng (hàm API). Hơn nữa, xử lý khoảng một triệu giao dịch mỗi giờ sẽ yêu cầu 280 giao dịch mỗi giây (TPS) trung bình. So với tăng vọt 30-40 phần trăm, băng thông cho khoảng 400 TPS sẽ phải được lên kế hoạch. Điều này hóa ra là khoảng 16 Mbps (400x5Kx8 bit/giây). Căn cứ theo tính toán trên, Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể bắt đầu với một liên kết tám Mbps và mở rộng khi khối lượng tăng lên.

4. Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể cung cấp một cặp bộ định tuyến đến trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) chấm dứt đường thuê bao. Các thiết bị mạng như thiết bị định tuyến (router) và thiết bị chuyển mạch (switch) được cài đặt để hiển thị kết nối giữa các trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA) và Tổ chức cung cấp dịch vụ nhận dạng (ISPA). Một Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể triển khai ít nhất hai máy chủ ở chế độ chủ động-chủ động (active-active) để phục vụ cho việc lưu trữ trong trung tâm dữ liệu. Các máy chủ có thể được nhóm lại và ảo hóa với các máy chủ blade/rack dual quad-core với 64 Gigabyte (GB) Bộ nhớ truy xuất ngẫu nhiên (RAM).

5. Máy chủ tường lửa có thể được triển khai để đảm bảo an ninh cho mạng giữa Tổ chức sử dung dịch vụ nhận dạng (ISCA) và Tổ chức cung cấp dịch vụ nhận dạng (ISPA), giữa Tổ chức cung cấp dịch vụ nhận dạng (ISPA) và Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Ngoài các bức tường lửa, một Tổ chức cung cấp dịch vụ nhận dạng (ISPA) cũng có thể triển khai mạng phát hiện xâm nhập và hệ thống ngăn chặn, chống virus và hệ thống chống phần mềm độc hại nhằm đảm bảo bảo vệ khỏi các cuộc tấn công.

6. Để ngăn chặn điểm chịu lỗi duy nhất của cơ sở dữ liệu kiểm toán, hai máy chủ cơ sở dữ liệu được đặt ở chế độ chủ động-chủ động sẵn sàng cao. Các lưu trữ trên mạng vùng dữ liệu (SAN) có thể được kết nối với các máy chủ cơ sở dữ liệu bằng cách sử dụng thiết bị chuyển mạch và mạng cáp quang.

7. Dữ liệu của 6 tháng kiểm toán có thể được duy trì bởi Tổ chức cung cấp dịch vụ nhận dạng (ISPA). Với dung lượng dữ liệu kiểm toán là 5K cho mỗi giao dịch, mười triệu giao dịch mỗi ngày sẽ yêu cầu Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có 50 GB một ngày, tương đương 1,5 TB một tháng. Nếu qua một tháng, dữ liệu có thể được chuyển đến nơi khác để lưu trữ sao lưu. Để đảm bảo tính sẵn sàng cao của dữ liệu, dữ liệu giao dịch kiểm toán cũng có thể được sao lưu tại một địa từ xa bằng cách sử dụng sao chép không đồng bộ.

8. Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể thiết lập máy chủ riêng biệt: một cho báo cáo Hệ thống thông tin quản lý (MIS) và thanh toán, và một cho quản lý và giám sát của ảo hóa, mạng, các máy chủ, cơ sở dữ liệu, sao lưu, sao chép và các ứng dụng. Các hệ điều hành lớp máy chủ và hypervisor có thể được triển khai trên tất cả các máy chủ thật trong trung tâm dữ liệu.

9. Các máy ảo (VM) chủ và khách có thể được cài đặt bằng cách khai thác trình quản lý máy ảo trên máy chủ quản lý. Các phần mềm máy chủ của Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể được triển khai trên các máy ảo. Các phần mềm cơ sở dữ liệu có thể được cài đặt trên các máy chủ cơ sở dữ liệu, trong khi bất kỳ phần mềm giám sát doanh nghiệp (EMS) nào cũng có thể được triển khai để giám sát hệ thống sản xuất một cách hiệu quả.

Những tính năng trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA)

1. Tổ chức sử dung dịch vụ nhận dạng có thể là một doanh nghiệp của chính phủ hoặc của tư nhân có đăng ký trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) để tận dụng các dịch vụ trong việc xác định và chứng thực của khách hàng. Các yêu cầu dịch vụ nhận dạng trên Tổ chức sử dung dịch vụ nhận dạng (ISCA) sẽ được giải quyết thông qua một Tổ chức cung cấp dịch vụ nhận dạng (ISPA), kênh trực tiếp duy nhất đến Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

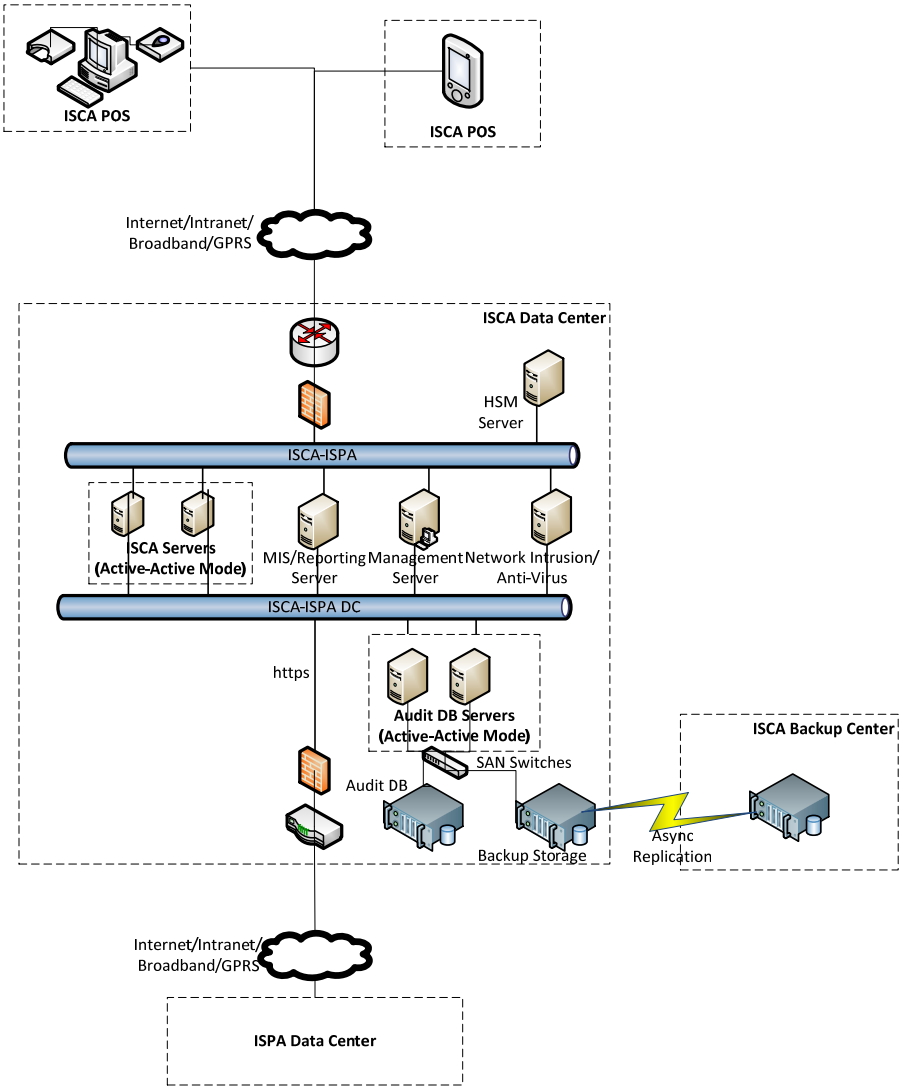
2. Quá trình đăng ký trên Tổ chức sử dung dịch vụ nhận dạng (ISCA) cũng như hướng dẫn kỹ thuật chi tiết để cài đặt và vận hành một trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA), có thể được công bố trên cổng thông tin công cộng trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Tổ chức sử dung dịch vụ nhận dạng (ISCA) sẽ tự cung cấp một giải pháp khắc phục thảm họa với hỗ trợ khôi phục dữ liệu từ xa theo quy định của hướng dẫn trong Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) cho trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA).

3. Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể thiết lập kết nối mạng để có thể gửi yêu cầu và nhận phản hồi từ Tổ chức cung cấp dịch vụ nhận dạng (ISPA) được chỉ định. Và cũng được khuyến nghị rằng Tổ chức sử dung dịch vụ nhận dạng (ISCA) phải có đường dây thuê bao riêng. Tuy nhiên, nó có thể được phép sử dụng băng thông rộng hiện có hoặc kết nối Internet GPRS.

4. Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể phát triển ứng dụng cung cấp dịch vụ riêng của mình và được tích hợp các giao diện lập trình ứng dụng (hàm API). Các hướng dẫn kỹ thuật được cung cấp bởi Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể được tuân thủ để thiết lập một dịch vụ cung cấp kiểm chứng an toàn.

5. Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể lưu trữ các ứng dụng cung cấp dịch vụ dựa trên web riêng của mình trong trung tâm dữ liệu và các ứng dụng dựa trên khách hàng của mình trên thiết bị đầu cuối của máy thanh toán tiền bằng thẻ (PoS) được tích hợp

vào Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Yêu cầu sẽ được gửi từ các thiết bị đầu cuối của máy thanh toán tiền bằng thẻ (PoS) tới các trung tâm dữ liệu Tổ chức sử dung dịch vụ nhận dạng (ISCA) thì đó sẽ chuyển đến các Tổ chức cung cấp dịch vụ nhận dạng (ISPA) thông qua một mạng lưới an toàn.



Hình 8.5: Kiến trúc triển khai kỹ thuật cho Trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA) và máy thanh toán tiền bằng thẻ (PoS

6. Tùy theo yêu cầu kinh doanh mà các dịch vụ nhận dạng khác nhau như nhận dạng và xác nhận khách hàng điện tử (eKYC), nhận dạng điện thoại di động… có thể được sử dụng. Các

cơ sở kinh doanh có thể sử dụng nhân khẩu học, sinh trắc học, hoặc sự kết hợp của hai loại chứng thực trên.

7. Phần mềm trên máy thanh toán tiền bằng thẻ (PoS) có thể là một ứng dụng dựa trên web tập trung hoặc ứng dụng khách hàng phong phú. Các thiết bị đầu cuối của máy thanh toán tiền bằng thẻ (PoS) có thể được trang bị với các thiết bị sinh trắc học Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) tương thích với dấu vân tay, quét võng mạc, khuôn mặt và ảnh chụp. Các dữ liệu được thu thập sau đó sẽ phù hợp với các tiêu chuẩn dữ liệu theo quy định của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

8. Các ứng dụng trên máy thanh toán tiền bằng thẻ (PoS) có thể đóng gói các dữ liệu nhân khẩu học và sinh trắc học theo các hướng dẫn kỹ thuật cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để xác thực định danh điện tử (eID). Các gói phần mềm có thể bao gồm mã hóa dữ liệu bằng cách sử dụng khóa đối xứng và thêm khóa riêng của Tổ chức sử dung dịch vụ nhận dạng (ISCA) được chỉ định bởi Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Các dữ liệu đóng gói có thể được truyền qua mạng giữa các thiết bị đầu cuối trên máy thanh toán tiền bằng thẻ (PoS) và các trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA).

9. Các trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể bảo đảm lưu lượng truy cập đến từ thiết bị đầu cuối trên máy thanh toán tiền bằng thẻ (PoS) sử dụng tường lửa, phát hiện xâm nhập, chống virus, và các hệ thống chống phần mềm độc hại và có thể được lưu trữ trên một máy chủ riêng biệt. Nó cũng có thể lưu trữ các mô-đun bảo mật phần cứng để quản lý khóa riêng.

10. Ứng dụng máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA) nhận được dữ liệu mã hóa đầu vào, xử lý nó và chuyển tiếp các gói dữ liệu xác nhận đến Tổ chức cung cấp dịch vụ nhận dạng (ISPA). Các ứng dụng máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể được lưu trữ trên các máy chủ của tổ chức này và có hai máy chủ ảo hóa và nhóm các máy chủ riêng biệt ở chế độ chủ động-chủ động (active-active). Quá trình ảo hóa có thể được xử lý bởi các máy chủ quản lý được lưu trữ riêng biệt.

11. Các tính năng của Hệ thống thông tin quản lý (MIS) có thể được lưu tại trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA) phục vụ cho việc phân tích dữ liệu và báo cáo trong nội bộ và bên ngoài.

12. Hai máy chủ cơ sở dữ liệu sẵn sàng cài đặt ở chế độ chủ động-chủ động (active-active) thành các nhóm riêng biệt được triển khai cho các cơ sở dữ liệu kiểm toán để ngăn ngừa điểm chịu lỗi duy nhất.

13. Lưu trữ trên Mạng vùng lưu trữ (SAN) được kết nối với các máy chủ cơ sở dữ liệu bằng cách sử dụng thiết bị chuyển mạch trên Mạng vùng lưu trữ (SAN) và mạng cáp quang. Giá trị của dữ liệu kiểm toán sáu tháng có thể được duy trì bởi Tổ chức sử dung dịch vụ nhận dạng (ISCA). Nếu kích thước cho mỗi giao dịch kiểm toán là 5K và có một triệu giao dịch mỗi ngày, Tổ chức cung cấp dịch vụ nhận dạng (ISPA) sẽ yêu cầu 5GB dung lượng để lưu trữ hàng ngày. Trong một tháng sẽ cần tới dung lượng lưu trữ là 150 GB; hơn một tháng, dữ liệu có thể được chuyển sang lưu trữ sao lưu.

14. Dữ liệu lưu trữ trên Mạng vùng lưu trữ (SAN) có thể được sao lưu trong trang web và ngoài trang sử dụng nhân rộng không đồng bộ.

15. Phần mềm giám sát để giám sát có hiệu quả hệ thống sản xuất có thể được triển khai. Bất kỳ phần mềm giám sát doanh nghiệp (EMS) nào cũng có thể được sử dụng.

16. Các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) có thể được chỉ định một mã số và chữ duy nhất của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) tại thời điểm đăng ký để nhận diện Tổ chức sử dung dịch vụ nhận dạng (ISCA). Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể gửi mã duy nhất của nó như một phần của dịch vụ yêu cầu thông số đầu vào để nhận dạng tới Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) như là người dùng được đăng ký của dịch vụ xác thực định danh điện tử (eID).

17. Các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) có thể tự động xác nhận chứng nhận của Giao thức truyền nhận bảo mật (Giao thức SSL) và đảm bảo nó được xác nhận so với danh sách thu hồi trực tuyến.

18. Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có một máy chủ trong trung tâm dữ liệu và có thể gửi các yêu cầu dịch vụ tới các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) đến máy chủ xác thực trong các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Các máy chủ của Tổ chức cung cấp dịch vụ nhận dạng (ISPA) có thể thêm một trong những khoá bản quyền hợp lệ (valid license key) của mình cho các gói yêu cầu dịch vụ từ các Tổ chức sử dung dịch vụ nhận dạng (ISCAs). Các máy chủ xác thực có thể chỉ

chấp nhận yêu cầu từ các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) hợp lệ và từ địa chỉ IP tĩnh được đăng ký thông qua một mạng riêng an toàn.

19. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể xác định một định dạng dữ liệu của ngôn ngữ đánh dấu khả mở (XML) tiêu chuẩn để nhập yêu cầu dịch vụ xác thực. Các định dạng có thể cho phép lưu trữ cả dữ liệu nhân khẩu học và sinh trắc học. Các dữ liệu nhân khẩu học trong những trường dữ liệu có thể tuân theo thông số kỹ thuật nhận dạng và xác thực cư dân (KYR) và hỗ trợ thu thập dữ liệu bằng cả tiếng Anh và tiếng Việt. Các định dạng có thể hỗ trợ việc cung cấp để xác định ngôn ngữ cho các dữ liệu nhân khẩu học cho yêu cầu dịch vụ.

20. Thử nghiệm kiểm toán có thể được lưu trữ và duy trì bởi Tổ chức sử dung dịch vụ nhận dạng (ISCAs), các Tổ chức cung cấp dịch vụ nhận dạng (ISPAs) và Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) trên các máy chủ của họ; mỗi yêu cầu dịch vụ và phản ứng trong các tài liệu ngôn ngữ đánh dấu khả mở (XML) có thể được lưu giữ trong một khoảng thời gian thời gian cho phép để giải quyết vấn đề, kiểm toán và trí tuệ doanh nghiệp.

21. Do kiến trúc kỹ thuật dựa trên giao thức phi trạng thái, có thể có một mã giao dịch duy nhất (Transaction ID) gắn liền với mọi yêu cầu dịch vụ và phản hồi để theo dõi các bản báo cáo trong cả quá trình trên các hệ thống khác nhau. Tổ chức sử dung dịch vụ nhận dạng (ISCAs) cũng được khuyến nghị sử dụng thuộc tính này cho yêu cầu tương ứng với những phản hồi cho kiểm toán và xác minh.

22. **Khoá bản quyền**. Mỗi Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể được giao một khoá bản quyền hợp lệ của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể được sử dụng trong quá trình xác thực. Khoá bản quyền có thể là một chuỗi chữ số duy nhất của chiều dài lên đến 64 ký tự, và có thể có thời hạn sử dụng được tích hợp vào. Cổng thông tin điều hành của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể cung cấp một cơ chế tự phục vụ cho người quản trị Tổ chức sử dung dịch vụ nhận dạng (ISCA) để tạo ra một khoá bản quyền mới và gia hạn trước khi hết hạn.

23. **Khoá tạm thời**. Khoá tạm thời là các khoá đối xứng được sử dụng để mã hoá tất cả các yêu cầu và phản hồi trong một phiên giao dịch . Các khoá tạm thời có thể là 256-bit chuẩn mã hoá tiên tiến (AES), có thể được tạo ra bởi các Tổ chức sử dung dịch vụ nhận dạng (ISCA) sử dụng mã hóa được hỗ trợ bởi khoá công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Nó được mã hóa bằng cách sử dụng thêm mã hóa cơ sở-64 để cho

phép truyền qua giao thức truyền siêu văn bản an toàn (HTTPS). Các khoá tạm thời được mã hóa và giải mã có thể được thêm vào các tài liệu của ngôn ngữ đánh dấu khả mở (XML) gửi như các dữ liệu đầu vào trong các yêu cầu dịch vụ. Các mã hóa của khóa sẽ đảm bảo rằng nó chỉ được biết trong Tổ chức sử dung dịch vụ nhận dạng (ISCA) có liên quan và Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) - và không bị lấy đi bởi các cuộc tấn công của người trung gian (man-in-the-middle attack) trên dây dẫn.

24. Dữ liệu nhận dạng cá nhân (PID) thu trên một thiết bị được mã hóa trên chính thiết bị thu vì những lý do an ninh. Dữ liệu nhận dạng cá nhân (PID) có thể bao gồm cả dữ liệu văn bản nhị phân sinh trắc học và nhân khẩu học, sẽ được tiếp tục mã hóa để truyền qua giao thức giao thức truyền siêu văn bản an toàn (HTTPS) được thiết kế để xử lý các dữ liệu văn bản. Các dịch vụ chứng thực có thể cung cấp cả hai lựa chọn mã hóa các dữ liệu nhị phân và văn bản sang base 64 encoding[10] để chuyển dữ liệu nhị phân trên phương tiện thông tin được lập ra để xử lý dữ liệu văn bản, hoặc ở dạng nhị phân dựa trên tiêu chuẩn Protocol Buffer[11]. Base 64 encoding của Dữ liệu nhận dạng cá nhân (PID) và đóng gói tiếp các dữ liệu đầu vào trong vỏ bọc ngôn ngữ đánh dấu khả mở (XML) có thể được thực hiện trên thiết bị hoặc máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA) tùy theo nhu cầu Dung lượng thiết bị, giao thức giữa các thiết bị và máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA), và định dạng dữ liệu được sử dụng giữa các thiết bị và máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA), vv, có thể được xem xét khi lựa chọn.

25. Kết cấu dịch vụ xác thực có thể được mở rộng và những bằng chứng thông báo nhận dạng (token) khác nhau như điện thoại di động, công nghệ giao tiếp tầm ngắn (NFC) , thẻ thông minh, vv, ngày hôm nay và trong tương lai. Điều này có thể hữu ích trong việc thêm yếu tố xác thực thứ hai ("cái người sử dụng có") cho một giao dịch tự phục vụ của công dân. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể hỗ trợ thẻ nhận dạng quốc gia mới, nhận dạng di động, đăng ký điện thoại di động, và nhận dạng email công dân như các loại bằng chứng thông báo nhận dạng.

26. Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể làm việc với các nhà điều hành công ty viễn thông để lấy được số điện thoại di động của thiết bị di động trong khi một yêu cầu dịch vụ đang được thực hiện để đảm bảo rằng các yêu cầu có xuất xứ từ số điện thoại di động đã đăng ký của công dân.

---

[10] Base-64 encoding - https://en.wikipedia.org/wiki/Base64

[11] Protocol Buffers standard - http://code.google.com/p/protobuf/

27. Mỗi yêu cầu xác thực có thể lấy các loại bằng chứng thông báo nhận dạng và giá trị của các bằng chứng này để sử dụng cho việc bắt đầu một yêu cầu dịch vụ.

28. **Giả mạo dữ liệu nhận dạng cá nhân**. Để đảm bảo rằng các Dữ liệu nhận dạng cá nhân (PID) không được can thiệp vào quá trình truyền tải từ thiết bị sang máy chủ xác thực, có thể chuyển thành hàm hash SHA-256 trong chuỗi ngôn ngữ đánh dấu khả mở (XML) của Dữ liệu nhận dạng cá nhân (PID) trước khi gửi đi. Giá trị hash được tính toán được bổ sung vào tài liệu ngôn ngữ đánh dấu khả mở (XML) và được gửi như các dữ liệu đầu vào đến các yêu cầu dịch vụ. Ngoài ra, khi các máy chủ xác thực nhận được văn bản yêu cầu của ngôn ngữ đánh dấu khả mở (XML), nó có thể tính toán lại giá trị hash của Dữ liệu nhận dạng cá nhân (PID) và so sánh nó với giá trị hash nhận được trong các yêu cầu dịch vụ. Nếu các giá trị không trùng khớp sẽ bị từ chối yêu cầu chứng thực với một mã báo lỗi là Dữ liệu nhận dạng cá nhân (PID) đã bị giả mạo.

29. **Đảm bảo toàn vẹn dữ liệu và ngăn chặn sự chống chối từ**. Chữ ký điện tử có thể được sử dụng để đảm bảo tính toàn vẹn của thông điệp trong quá trình truyền tải và ngăn chặn sự chống chối từ nguồn gốc của các yêu cầu dịch vụ. Các văn bản ngôn ngữ đánh dấu khả mở (XML) yêu cầu dịch vụ có thể sử dụng chữ ký điện tử bằng ngôn ngữ đánh dấu khả mở (XML) của Tổ chức sử dung dịch vụ nhận dạng (ISCA) hoặc Tổ chức cung cấp dịch vụ nhận dạng (ISPA), tùy thuộc vào cơ quan tạo ra các văn bản yêu cầu ngôn ngữ đánh dấu khả mở (XML) cuối cùng. Bằng cách ký vào văn bản ngôn ngữ đánh dấu khả mở (XML), sự an ninh và toàn vẹn thông điệp giữa các máy chủ được chứng nhận còn nguyên vẹn và yêu cầu thực sự đã được gửi bởi người ký.

30. Chữ ký điện tử có thể được mua bởi các Tổ chức sử dung dịch vụ nhận dạng (ISCA) và Tổ chức cung cấp dịch vụ nhận dạng (ISPA) từ các cấp có thẩm quyền cấp giấy chứng nhận hợp lệ theo Luật chữ ký điện tử[12]. Chữ ký điện tử có thể là một giấy chứng nhận cấp II hoặc cấp III. Giấy chứng nhận điện tử có thể bao gồm hai phần: chứng chỉ X.509 đại diện cho các khóa chung và khóa riêng được sử dụng cho chữ ký điện tử. Khóa riêng có thể được lưu trữ an toàn và chủ sở hữu giấy chứng nhận sẽ có trách nhiệm đảm bảo rằng nó không bị tổn hại. Các máy chủ xác thực của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có

[12] Digital Signature Act - http://www.moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=4172

thể kiểm tra để đảm bảo rằng giấy chứng nhận thuộc về Tổ chức sử dung dịch vụ nhận dạng (ISCA) hoặc Tổ chức cung cấp dịch vụ nhận dạng (ISPA) và đã được cơ quan cấp giấy chứng nhận có thẩm quyền ban hành. Do đó, điều bắt buộc là thuộc tính "O" của "Subject" trong chứng chỉ X.509 phải khớp với tên của cơ quan đó.

31. Có thể đánh dấu thời gian bằng cách chụp xác thực đầu vào trên một thiết bị. Định dạng của các dấu thời gian có thể là "YYYY-MM-DDThh: mm: ss" và tuân theo tiêu chuẩn ISO 8601. Múi giờ có thể không được xác định và được tự động mặc định cho Công nghệ thông tin và truyền thông (ICT) (UTC 7,00). Các dấu thời gian đóng một vai trò quan trọng; do đó các thiết bị được khuyến cáo nên đồng bộ thời gian với một máy chủ thời gian.

32. Các máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA) và Tổ chức cung cấp dịch vụ nhận dạng (ISPA) và có thể hỗ trợ bộ đệm của yêu cầu xác thực và gửi yêu cầu đến máy chủ xác thực để hỗ trợ trong trường hợp thiếu kết nối mạng không thường xuyên trên trường. Thời gian tối đa mà các yêu cầu có thể được đệm (xếp hàng đợi) được xác định bởi chính sách hoạt động CNTT trong khuôn khổ bảo mật CNTT Quốc gia và khuôn khổ cung cấp dịch vụ nhận dạng quốc gia (NISDF). Mọi yêu cầu với giá trị được đánh dấu thời gian cũ hơn mức quy định sẽ bị từ chối.

33. Theo chính sách bảo mật của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV), nếu số lần thất bại vượt qua ngưỡng cho phép, hồ sơ lưu trú tại các Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) có thể bị tạm hoãn lại. Ngưỡng trên có thể được tự động tính toán dựa trên những suy nghiệm khác nhau và có thể không phải là một số tĩnh.

34. Phản hồi từ dịch vụ xác thực là một văn bản ngôn ngữ đánh dấu khả mở (XML). Vì lý do riêng tư, sẽ không trả lại bất kỳ dữ liệu cá nhân của công dân và chỉ phản hồi với câu trả lời "có/không".

35. Dịch vụ xác thực có thể cung cấp một cơ chế để xác nhận tính xác thực của câu trả lời cho các mục đích không thoái thác. Để kích hoạt tính năng kiểm tra, kiểm toán, phản ứng có thể được xác thực bằng chữ ký số của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và chữ ký sẽ là một phần của phản ứng. Chữ ký có thể được xác nhận bằng cách sử dụng khóa công khai Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và chữ ký sẽ thực hiện theo các tiêu chuẩn chữ ký ngôn ngữ đánh dấu khả mở (XML) Hiệp hội lập ra các

chuẩn cho internet (W3C) (W3C XML signature standard[13]). Các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) có thể bảo vệ phản hồi xác thực cho mỗi yêu cầu phát sinh từ máy chủ của họ cho các mục đích không thoái thác.

36. Phản hồi xác thực có thể cung cấp một cơ chế hợp tác, kết hợp phản ứng với các yêu cầu bằng cách gửi đi cùng một danh tính giao dịch đi kèm với yêu cầu phải có phản hồi trở lại. Và cũng có thể bao gồm các dấu thời gian khi tạo ra các phản hồi.

37. Để kích hoạt một cơ chế trong đó các phản ứng chứng thực được sử dụng vào lần sau như Chứng minh nhận dạng (PoI) và Chứng minh Địa chỉ (PoA) số, phản hồi có thể thêm các siêu thông tin cho các chi tiết Dữ liệu nhận dạng cá nhân (PID) trong các yêu cầu chứng thực. Điều này có thể bao gồm giá trị băm SHA-256 của Mã số chứng minh nhận dạng quốc gia (NIN), giá trị băm SHA-256 của phần nhân khẩu học của khu Dữ liệu nhận dạng cá nhân (PID) và mã hóa dữ liệu sử dụng trong định dạng HEX các thuộc tính nhân khẩu học sử dụng khác nhau của yêu cầu chứng thực này. Thiết kế của các dữ liệu được mã hóa sử dụng cho hệ thống Aadhaar của Ấn Độ được mô tả trong Phụ lục 5.

38. Dịch vụ chứng thực định danh điện tử (eID) có thể được bắt nguồn hoặc là từ "nơi đăng ký" hoặc là từ một thiết bị đầu cuối "công cộng". Các thiết bị công cộng là những trường hợp không có nơi lưu trữ an toàn cho các khoá. Các kết nối giữa các thiết bị công cộng và bộ chứng thực có thể sử dụng một giao thức an toàn như HTTPS.

39. Đối với các thiết bị công cộng, dữ liệu có thể được mã hóa với một mã tạm thời năng động bằng cách sử dụng thuật toán đối xứng AES-256 (AES/ECB/PKCS7Padding). Các mã tạm thời, lần lượt, có thể được mã hóa với mã công cộng 2048-bit của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) sử dụng thuật toán bất đối xứng (RSA/ECB/PKCS1Padding). Các khoá tạm thời có thể không được lưu trữ bất cứ nơi nào, ngoại trừ trong bộ nhớ, và nó có thể không được tái sử dụng qua giao dịch. Khi sử dụng các thiết bị công cộng, được khuyến nghị cao là nên sử dụng mật khẩu sử dụng một lần (OTP).

40. Các bước để đóng gói và mã hóa các yêu cầu dịch vụ trên thiết bị "công cộng" là:
    a. Các Mã số chứng minh nhận dạng quốc gia (NIN), chi tiết nhân khẩu học và sinh trắc học được yêu cầu bởi ứng dụng được nhập vào các thiết bị cùng với các yếu tố khác như mật khẩu sử dụng một lần (OTP), nếu được sử dụng. Nếu mật khẩu sử

[13] W3C XML Signature standard - http://www.w3.org/TR/xmldsig-core/

dụng một lần (OTP) được sử dụng, yêu cầu phải gửi đến máy chủ chứng thực định danh điện tử (eID) cùng với Mã số chứng minh nhận dạng quốc gia (NIN). Máy chủ chứng thực định danh điện tử (eID) gửi lại mật khẩu sử dụng một lần (OTP) cho điện thoại di động được đăng ký của công dân qua dịch vụ nhắn tin ngắn (SMS) và địa chỉ email đã đăng ký.

b. Các ứng dụng của Tổ chức sử dung dịch vụ nhận dạng (ISCA)/ Tổ chức sử dung dịch vụ nhận dạng (ISCA) phụ tạo ra mã tạm thời một lần.
c. Việc chứng thực "dữ liệu" khối Ngôn ngữ đánh dấu khả mở (XML) có thể được mã hóa bằng cách sử dụng khoá tạm thời một lần và sau đó được mã hóa lại (base 64).
d. Các khoá tạm thời sau đó có thể được mã hóa với khoá công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).
e. Việc áp dụng Tổ chức sử dung dịch vụ nhận dạng (ISCA) trên thiết bị có thể gửi các khối mã hóa cùng với dữ liệu Mã nhận thực bản tin dựa trên hàm Hash (HMAC) đến máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA).
f. Các máy chủ của Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể tạo ra đầu vào bằng Ngôn ngữ đánh dấu khả mở (XML) cho chứng thực cuối để yêu cầu dịch vụ, bao gồm cả mã bản quyền và tham chiếu giao dịch (thuộc tính txn), và gửi dữ liệu đến máy chủ chứng thực định danh điện tử (eID) thông qua mạng lưới Tổ chức cung cấp dịch vụ nhận dạng (ISPA).
g. Các máy chủ chứng thực định danh điện tử (eID) giải mã mã tạm thời bằng mã riêng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV). Các khối dữ liệu sau đó được giải mã bằng cách sử dụng khoá tạm thời.
h. Giải mã sinh trắc học và nhân khẩu học thông tin của công dân - và mật khẩu sử dụng một lần (OTP) tuỳ chọn - được xem xét trong quá trình so khớp dựa trên đầu vào.
i. Các máy chủ chứng thực định danh điện tử (eID) phản hồi bằng câu trả lời "có/không" trong Ngôn ngữ đánh dấu khả mở (XML) có chữ ký số.

41. **Kiểm tra nhận dạng**. Việc chứng thực định danh điện tử (eID) có thể ghi lại tất cả các yêu cầu chứng thực và phản hồi của họ cho mục đích kiểm toán. Bằng cách cung cấp các Mã số định danh công dân (NIN) và mã phản hồi xác thực, Tổ chức sử dung dịch vụ nhận dạng (ISCA) có thể yêu cầu Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) xác nhận kết quả của chứng thực cùng với các yếu tố xác thực đã được trình bày trong yêu cầu đó. Chính sách an ninh CNTT quốc gia và hoạt động CNTT trong Khuôn khổ cung cấp dịch vụ

theo định danh điện tử (EISDF) có thể quyết định việc kiểm tra này nên được duy trì trong bao lâu.

42. Tất cả các phản hồi chứng thực được ký số hoá bởi các Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và các Tổ chức sử dung dịch vụ nhận dạng (ISCAs) có thể được khuyến cáo để xác nhận tính toàn vẹn các phản hồi và có thể theo dõi các mục đích kiểm tra. Ngoài ra, các thuộc tính như dấu thời gian và sử dụng dữ liệu nhân khẩu học trong các phản hồi xác thực cũng được sử dụng để kiểm tra xem các yêu cầu có thực sự là cho một Mã số định danh công dân (NIN) cụ thể hay không, nếu yêu cầu thực sự đã có một yếu tố sinh trắc học, hoặc khi xác thực đã được thực hiện, vv . Với những phản hồi chứng thực có thể tự xác minh cho phép tin tưởng các ứng dụng bên thứ ba và xác minh phản hồi bằng chữ ký điện tử khá giống với sự tin tưởng ngoại tuyến như một một tài liệu công chứng.

43. Để đảm bảo cho các giải pháp được áp dụng rộng rãi và tương thích với các hệ thống hiện có, những công nghệ phù hợp với các tiêu chuẩn mở cũng được khuyến khích sử dụng. Một số tiêu chuẩn mở có thể được xem xét là:
    a. **Những tiêu chuẩn dữ liệu nhân khẩu học**. Có một tiêu chuẩn cho việc thu thập dữ liệu nhân khẩu học cần thiết của công dân để thông tin nhận dạng này hoạt động trên những hệ thống khác nhau và đảm bảo khả năng tương tác qua nhiều cơ quan chính phủ và tư nhân sử dụng Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Điều quan trọng là việc thu thập và xác minh dữ liệu nhân khẩu học cơ bản cho mỗi công dân được chuẩn hóa trên tất cả các đối tác của Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF). Ví dụ, Tổng cục nhận dạng duy nhất Ấn Độ (UIDAI) thành lập Thủ tục thẩm định và chuẩn mực dữ liệu dân số (DDSVP) (Demographic Data Standards and Verification Procedure (DDSVP) committee[14]) cho mục đích này.
    b. **Những tiêu chuẩn sinh trắc học**. Các Cơ quan Quản lý Định danh điện tử Việt Nam (EIDAV) có thể thiết lập một ủy ban để xác định các tiêu chuẩn sinh trắc học dựa trên các tiêu chuẩn quốc gia và quốc tế; nó cũng có thể xác định thực tế tốt nhất, độ chính xác kỳ vọng, khả năng tương tác, sự phù hợp và hiệu quả trong các tiêu chuẩn sinh trắc học. Ví dụ, Tổng cục nhận dạng duy nhất Ấn Độ (UIDAI) thành lập một ủy ban tiêu chuẩn sinh trắc học[15].

---

[14] Demographic Data Standards and Verification procedure (DDSVP) committee - http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf

[15] Biometric standards - http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf

c. Giao diện lập trình ứng dụng (hàm API) định danh điện tử (eID) sinh trắc học (eID Biometric APIs (eID Biometric APIs[16])
d. Thuật toán mã hoá dữ liệu – ANXI X3.92
e. Dịch vụ tài chính ngân hàng – phân phối Quản lý mã đối xứng – ANSI X9.24
f. Khoá công cộng mã hoá cho ngành công nghiệp dịch vụ tài chính: Thoả thuận các khoá đối xứng sử dụng mã hoá rời rạc – ANSI X9.42
g. Thuật toán mã hóa dữ liệu bộ ba: Phương thức hoạt động – ANSI X9.52
h. Yêu cầu bảo mật cho Mo đun mã hoá – FIPS PUB 140-2
i. Quản lý và bảo mật mã số nhận dạng cá nhân (PIN) – tiêu chuẩn ISO 9564
j. Công nghệ thông tin – Kỹ thuật an toàn – Chức năng Hash – ISO 10118
k. Công nghệ thông tin – Kỹ thuật an ninh – Quản lý mã – ISO 11770
l. Công nghệ thông tin – Kỹ thuật an ninh – Các thuật toán mã hóa – ISO 18033
m. Tiêu chuẩn sinh trắc học – ISO 19794-4, ISO 19794-6
n. Tiêu chuẩn định dạng thời gian và ngày tháng – tiêu chuẩn ISO 8601
o. Chữ ký trong ngôn ngữ đánh dấu khả mở (XML)- http://www.w3.org/TR/xmldsig-core/
p. Siêu dữ liệu và dữ liệu tiêu chuẩn cho mã hoá cá nhân và khu vực – ví dụ, tiêu chuẩn chính quyền điện tử (eGovernance standards[17]) theo quy định của Chính phủ Ấn Độ.
q. Bộ đệm giao thức – http://code.google.com/p/protobuf/
r. Tiêu chuẩn định vị – tiêu chuẩn ISO 6709

Những tính năng của dịch vụ nhận dạng di động (Mobile ID)

1. SIM được sử dụng cho dịch vụ nhận dạng di động được sản xuất trong một môi trường an toàn và phải phù hợp với cấu hình bảo hộ theo quy định của Ủy ban châu Âu Hiệp định Hội thảo Tiêu chuẩn (CWA) 14.169 với hệ thống đánh giá khả năng an toàn cấp độ 4+ (EAL4+) theo các tiêu chí chung (CC) về tiêu chuẩn an toàn (ISO/IEC15048). Các nhà cung cấp SIM phải cung cấp giấy chứng nhận theo yêu cầu của cơ quan có thẩm quyền chứng nhận (CA) cho một sản phẩm SIM cụ thể.

---

[16] eID Biometric APIs – http://uidai.gov.in/UID_PDF/Working_Papers/Aadhaar_ABIS_API.pdf

[17]Metadata and data standards – http://egovstandards.gov.in/standardsandFramework/metadata-and-data-standards/MDDS_Standard_release_version_1.0__Dec_24_2k9.pdf

2. SIM có thể có thiết bị tạo chữ ký bảo mật (SSCD) với hai cặp khoá: một để xác thực, một cho mục đích tính năng chữ ký/không thể bác bỏ. Chìa khóa đăng ký có thể được bảo vệ bởi mã PIN.

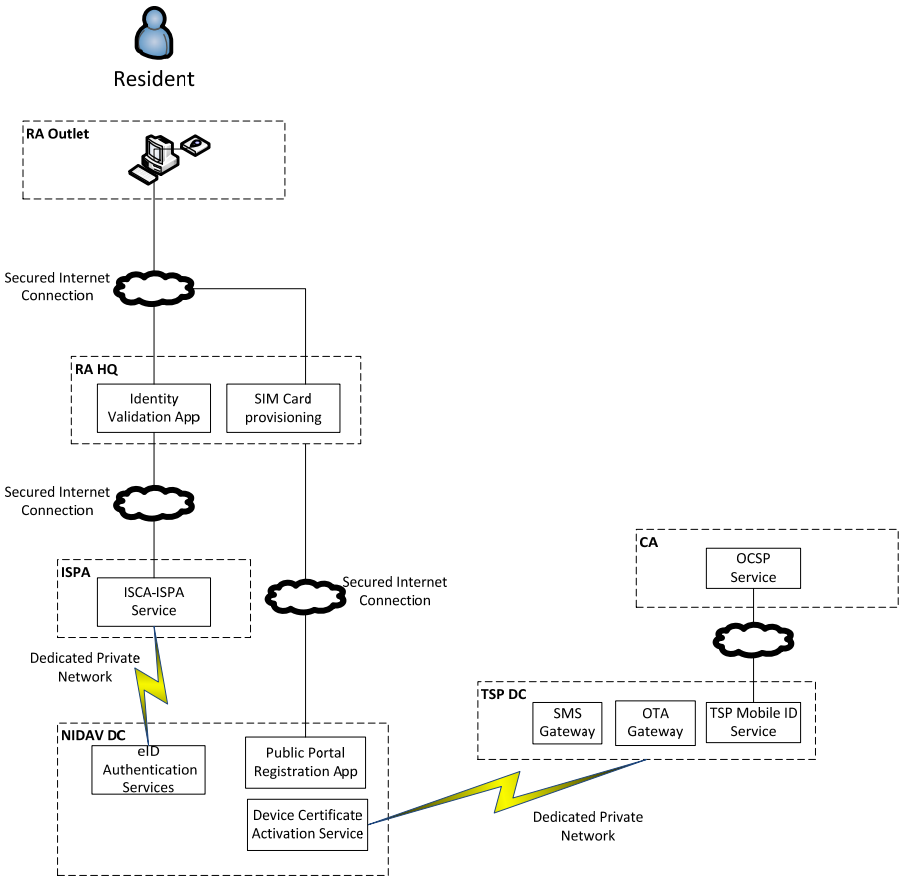
3. Ứng dụng có thể được lưu trữ trên SIM là giao diện cập nhật tin nhắn từ xa SMS Over-The-Air (OTA) để giao dịch chứng thực, giao dịch chữ ký số, thay đổi mã PIN, bỏ chặn phím riêng với mã mở khoá PIN (PUK), giải mã dữ liệu mã hóa và giải mã, hiển thị các tin nhắn văn bản.

4. Điện thoại di động có thể hỗ trợ ít nhất Phase 2 + SIM Toolkit.

5. Chi phí ước tính cho việc sản xuất SIM với cơ sở hạ tầng mã khóa công cộng không dây (wPKI) có thể là 1-2 đô la với chứng nhận số hoá và ứng dụng được tải về trên khu vực thiết bị tạo chữ ký bảo mật (SSCD).

6. Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể phải cung cấp các thông số kỹ thuật tiêu chuẩn cho các SIM đã kích hoạt cơ sở hạ tầng mã khóa công cộng không dây (wPKI) cho dịch vụ nhận dạng di động và được hỗ trợ điện thoại di động.

7. Thiết kế cung cấp SIM

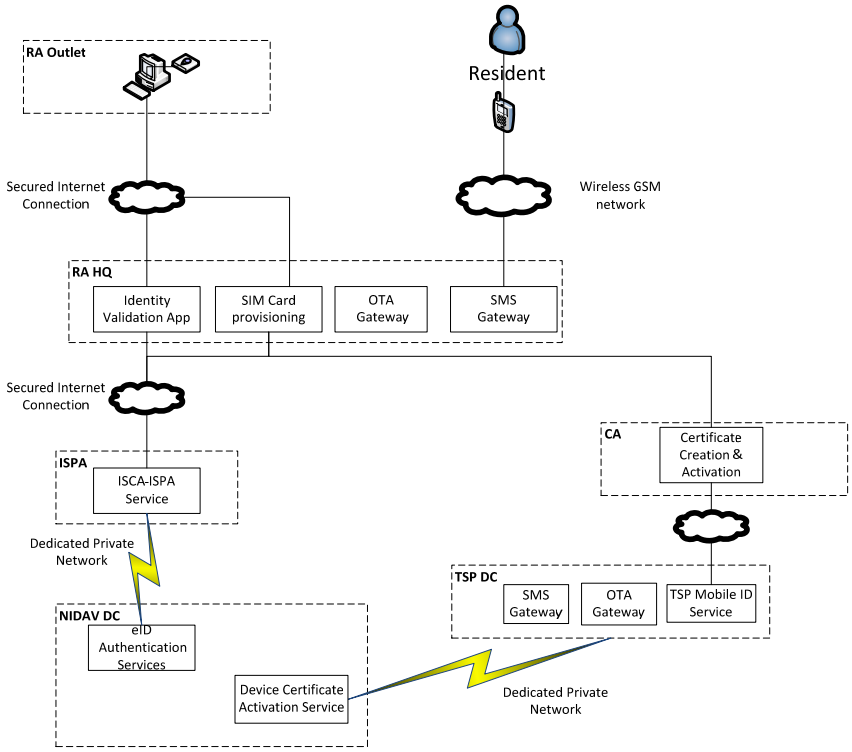


Hình 8.6: Kiến trúc kỹ thuật cung cấp SIM

a. Cổng thông tin của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể cung cấp các ứng dụng đăng ký cho các đơn vị có liên quan tới các dịch vụ nhận dạng di động như Tổ chức quản lý đăng ký (RA), nhà cung cấp dịch vụ tin cậy (TSP), Tổ chức sử dung dịch vụ nhận dạng (ISCA), Tổ chức cung cấp dịch vụ nhận dạng (ISPA) và cơ quan có thẩm quyền chứng nhận (CA).
b. Tổ chức quản lý đăng ký (RA) có thể thiết lập các đại cung cấp dự phòng SIM, đăng ký sử dụng và kích hoạt chứng chỉ.
c. Tổ chức quản lý đăng ký (RA) có thể lưu trữ các ứng dụng để xác nhận danh tính người dân trên các máy chủ trong trung tâm dữ liệu và cung cấp truy cập Internet tại các đại lý để thực hiện xác nhận danh tính của công dân tại thời điểm cung cấp dự phòng SIM. Các ứng dụng xác nhận danh tính có thể có cấu trúc kỹ thuật tương tự như các ứng dụng của Tổ chức sử dung dịch vụ nhận dạng (ISCA) mà có thể gọi cho dịch vụ xác thực danh tính được cung cấp bởi Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) để xác thực sinh trắc học. Các đại lý có thể cài đặt chế độ đọc sinh trắc học với các ứng dụng để xác minh danh tính của công dân.

d. Tổ chức quản lý đăng ký (RA) cũng có thể lưu trữ các ứng dụng web để kích hoạt giấy chứng nhận thiết bị của một SIM và lưu nó tại các Nhà cung cấp dịch vụ tin cậy (TSPs). Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) có thể lưu trữ một dịch vụ web trong trung tâm dữ liệu sản xuất với mục đích phổ biến các chi tiết kích hoạt chứng nhận thiết bị cho các Nhà cung cấp dịch vụ tin cậy (TSPs). Các đại lý của Tổ chức quản lý đăng ký (RA) có thể điểm lại ứng dụng này trên Internet.

8. Thiết kế kích hoạt chứng nhận/đăng ký người dùng



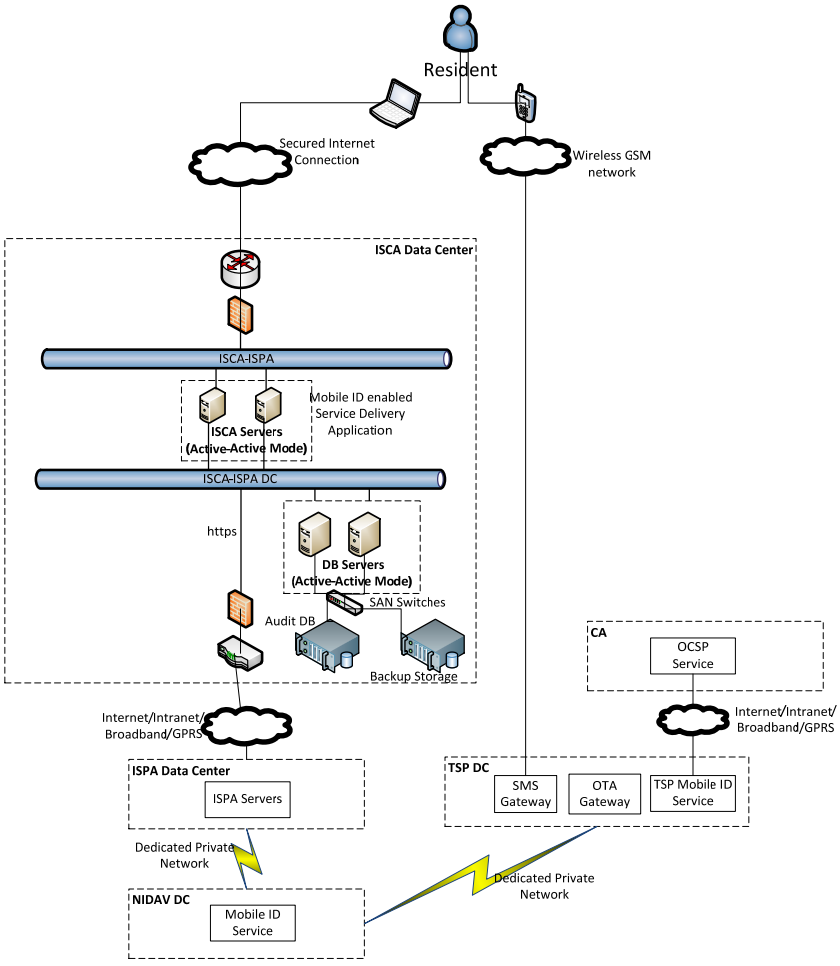
Hình 8.7: Kiến trúc kỹ thuật kích hoạt chứng nhận/đăng ký người dùng

a. Người dùng khởi chạy ứng dụng kích hoạt SIM trên điện thoại di động. Ứng dụng này sẽ gửi yêu cầu kích hoạt qua Hệ thống thông tin di động toàn cầu (GSM) đến cổng lưu trữ Trung tâm dịch vụ tin nhắn ngắn (SMSC) / SMS trong trung tâm dữ liệu của Tổ chức quản lý đăng ký (RA). Trung tâm dịch vụ tin nhắn ngắn (SMSC) chuyển các yêu cầu cho các ứng dụng kích hoạt SIM được lưu trữ trong các máy chủ back-end trong trung tâm dữ liệu.
b. Đáp lại, các ứng dụng gửi yêu cầu cho chữ ký trên các dữ liệu nhận dạng cá nhân thông qua cập nhật phần mềm từ xa (OTA) và cổng tin nhắn SMS. Công dân xác minh dữ liệu và đăng ký bằng cách nhập mã kích hoạt thiết bị.

c. Tổ chức quản lý đăng ký (RA) nhận được dữ liệu cá nhân đã đăng ký và bao gồm cả các thông tin khác như giấy chứng nhận thiết bị; sau đó chuyển tiếp yêu cầu để kích hoạt chứng nhận cho cơ quan có thẩm quyền chứng nhận (CA) được chỉ định qua kết nối Internet an toàn. Tổ chức quản lý đăng ký (RA) cũng gửi yêu cầu dịch vụ cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) qua một Tổ chức cung cấp dịch vụ nhận dạng (ISPA) đã đăng ký để cập nhật hồ sơ nhận dạng của công dân với số điện thoại di động.

d. Cơ quan có thẩm quyền chứng nhận (CA) tạo ra và kích hoạt chứng nhận đủ điều kiện và phát hành để thông báo cho các nhà cung cấp dịch vụ tin cậy (TSPs) và Cơ quan quản lý định danh điện tử Việt Nam (EIDAV).

9. Thiết kế sử dụng



Hình 8.8: Kiến trúc kỹ thuật sử dụng nhận dạng di động (Mobile ID)

a. Các nhà cung cấp dịch vụ tích hợp các ứng dụng cung cấp dịch vụ vào các dịch vụ nhận dạng điện thoại di động và lưu trữ nó trên trung tâm dữ liệu của Tổ chức sử dung dịch vụ nhận dạng (ISCA). Các ứng dụng cung cấp dịch vụ có các tùy chọn để nhấp vào "Đăng nhập với ID điện thoại di động".
b. Hệ thống Tổ chức sử dung dịch vụ nhận dạng (ISCA) lấy dịch vụ nhận dạng di động trên web của Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) lưu trữ trên các trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) với Mã số chứng minh nhận dạng quốc gia (NIN), số điện thoại di động và số PIN của người dân thông qua Tổ chức cung cấp dịch vụ nhận dạng (ISPA).
c. Dịch vụ nhận dạng di động trên web của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) xác nhận số điện thoại di động được cung cấp bằng cách sử dụng số điện thoại di động lưu trữ cho Mã số định danh công dân (NIN) được đưa ra trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS).
d. Sau khi xác nhận thành công, các dịch vụ web của nhà cung cấp dịch vụ tin cậy (TSP) được lưu trữ trong trung tâm dữ liệu của nhà cung cấp dịch vụ tin cậy (TSP) qua kết nối Internet an toàn với số điện thoại di động, mã xác minh và mã PIN.
e. Đáp lại, các dịch vụ của nhà cung cấp dịch vụ tin cậy (TSP) tạo ra các mã xác minh và gửi đến các trang web Tổ chức sử dung dịch vụ nhận dạng (ISCA). Và cũng tạo ra yêu cầu chữ ký với mã xác minh, số điện thoại và mã PIN; sau đó sẽ gửi tới điện thoại di động của công dân bằng cách sử dụng dịch vụ cập nhật từ xa (OTA) và tin nhắn cổng thông SMS của nhà cung cấp dịch vụ tin cậy (TSP) qua mạng không dây ở định dạng tin nhắn SMS.
f. Các tin nhắn SMS đặc biệt thông qua dịch vụ cập nhật từ xa (OTA) kích hoạt các ứng dụng xác minh danh tính trên SIM. Nó sẽ hiển thị các mã xác nhận giống hệt như hiển thị trên máy tính của công dân. Công dân sẽ xác nhận các mã này trên thiết bị di động với một trong những hiển thị trên máy tính và đăng ký yêu cầu bằng cách nhập mã PIN.
g. Nhà cung cấp dịch vụ tin cậy (TSP) nhận được dữ liệu chữ ký và các cuộc gọi từ dịch vụ Giao thức kiểm tra chứng thực trực tuyến (OCSP) của Cơ quan có thẩm quyền chứng nhận (CA) để xác nhận các dữ liệu chữ ký và giấy chứng nhận.
h. Nhà cung cấp dịch vụ tin cậy (TSP) chuyển các phản hồi nhận được từ Cơ quan có thẩm quyền chứng nhận (CA) đến Tổ chức sử dung dịch vụ nhận dạng (ISCA) thông qua Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) và Tổ chức cung cấp dịch vụ nhận dạng (ISPA).
i. Dựa trên xác thực thành công, công dân có thể đăng nhập vào các trang web an toàn.

10. Thủ tục huỷ dịch vụ
    a. Trong trường hợp huỷ chứng nhận, Tổ chức quản lý đăng ký (RA) sẽ thông báo cho cơ quan có thẩm quyền chứng nhận (CA) để huỷ chứng nhận và ngay lập tức cơ quan có này sẽ tiến hành huỷ bỏ và công bố bản cập nhật của Danh mục huỷ chứng nhận (CRL) vì lợi ích của các Nhà cung cấp dịch vụ tin cậy (TSPs). Nó cũng cảnh báo cho Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) thông qua Tổ chức cung cấp dịch vụ nhận dạng (ISPA) để cập nhật các hồ sơ nhận dạng trong các Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) và tắt dịch vụ nhận dạng di động cho người dân với cùng các lý do trên.
    b. Trong trường hợp chặn SIM do bị mất hoặc hỏng SIM, chứng nhận thiết bị được đưa ra khỏi danh sách các khu vực thiết bị tạo chữ ký bảo mật (SSCDs) hợp lệ có sẵn đến các Nhà cung cấp dịch vụ tin cậy (TSPs). Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) được cảnh báo thông qua Tổ chức cung cấp dịch vụ nhận dạng (ISPA) để cập nhật các hồ sơ nhận dạng trong các Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS) và tắt dịch vụ nhận dạng di động cho công dân với cùng các lý do trên.

Dịch vụ tạo nguồn nhận dạng điện tử

Tiện ích tạo nguồn có thể là một chương trình cho máy tính để bàn sẵn sàng để tải về từ cổng thông tin công cộng của Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) sau khi đăng ký thành công.

1. Tổ chức sử dung dịch vụ nhận dạng (ISCA) tải các tiện ích từ cổng thông tin và cài đặt trên máy chủ khi thực thi.

2. Tiện ích cung cấp các khả năng khai thác, hợp nhất, chuẩn hóa và so sánh dữ liệu. Các tiện ích kết nối với các nguồn dữ liệu khác nhau để kéo Dữ liệu nhận dạng cá nhân (PID) có liên quan từ cơ sở dữ liệu tham khảo. Nó cũng kéo dữ liệu từ các bảng dữ liệu có liên quan trong cơ sở dữ liệu cung cấp dịch vụ của nhà cung cấp dịch vụ.

3. Tiện ích cung cấp khả năng trong đó một hoặc nhiều trường tương ứng của Dữ liệu nhận dạng cá nhân (PID) (tên, số phận sinh, tuổi, giới tính) từ hồ sơ công dân tại các cơ sở dữ liệu cung cấp dịch vụ có thể trùng khớp với các trường tương đương trong các hồ sơ nhận dạng từ cơ sở dữ liệu tham khảo. Do đó việc tạo lập bảng có thể xuất sang Excel để xem xét và phê duyệt của cơ quan có thẩm quyền đã được nhà cung cấp dịch vụ chỉ định. Chức

năng so sánh - tạo nguồn tiện ích được giới hạn trong việc chỉ tạo lập ra các bảng và xuất sang Excel. Dựa trên dữ liệu ánh xạ, các nhà cung cấp dịch vụ có thể tạo ra các lệnh tùy chỉnh của Ngôn ngữ truy vấn theo cấu trúc (SQL) để cập nhật cơ sở dữ liệu cung cấp dịch vụ.

4. Tiện ích cũng cho phép xác thực của tạo nguồn bằng cách thực hiện chứng thực nhân khẩu học / sinh trắc học sử dụng dịch vụ chứng thực định danh điện tử (eID). Tổ chức sử dung dịch vụ nhận dạng (ISCA) đăng ký với Cơ quan quản lý định danh điện tử Việt Nam (EIDAV) để yêu cầu dịch vụ chứng thực định danh điện tử (eID).

Điều kiện tiên quyết để tạo nguồn định danh điện tử (eID)

Quá trình tạo nguồn định danh điện tử (eID) nhất thiết phải bắt đầu bằng số hóa dữ liệu và tập trung.

Số hóa dữ liệu về cơ bản có nghĩa là đối chiếu của dữ liệu cung cấp dịch vụ trong một định dạng điện tử (cơ sở dữ liệu / Excel hoặc tương tự) từ nơi mà dữ liệu có thể được lấy ra bằng cách sử dụng các truy vấn SQL tiêu chuẩn từ một Hệ thống quản lý cơ sở dữ liệu quan hệ (RDBMS) - sau này có thể MySQL, SQL Server, Oracle , Sybase, DB2 hoặc tương tự. Điều quan trọng là các dữ liệu nhận dạng cá nhân từ từ trở nên nhất quán trên nhiều hệ thống. Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) cũng là một sáng kiến để chuẩn hóa thông tin nhận dạng cá nhân, và các dữ liệu định danh điện tử (eID) có thể được sử dụng để làm sạch các dữ liệu hiện có.

Dữ liệu tập trung chủ yếu là quản lý dữ liệu sẵn có và khả năng tiếp cận các dữ liệu cung cấp dịch vụ được phân phối. Mục tiêu ở đây là cho phép tạo nguồn tiện ích để truy cập dữ liệu cung cấp dịch vụ và tất cả các thông tin có liên quan trong ít nhất là chế độ chỉ đọc (read-only). Ví dụ, trong dữ liệu về hưu trí của Việt Nam có thể đã có sẵn trong nơi chứa dữ liệu giữa từng địa phương. Một cái nhìn hợp nhất về toàn bộ dữ liệu có thể cho phép Bảo hiểm xã hội Việt Nam (VSS) cải thiện cung cấp dịch vụ trong khi đồng thời loại bỏ các vấn đề của việc có một người được hưởng cùng một lợi ích tương tự từ hai địa phương khác nhau.

Phương thức tạo nguồn nhận dạng điện tử

Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể hỗ trợ hai cách tạo nguồn cơ sở dữ liệu cung cấp dịch vụ với định danh điện tử (eID)/ Mã số chứng minh nhận dạng quốc gia (NIN): phương pháp áp từ trên xuống (top-down) và phương pháp hữu cơ (organic).

Phương pháp áp từ trên xuống có thể sử dụng khi thu thập dữ liệu nhận dạng cá nhân (PID) của công dân tại thời điểm đăng nhập để tạo ra Hệ thống định danh điện tử quốc gia (NID) và thẻ Hệ

thống định danh điện tử quốc gia (NID), và cơ sở dữ liệu dân số cả nước có sẵn tại Bộ Công An (MPS). Trong phương pháp này, các trường dữ liệu nhận dạng cá nhân (PID) trong cơ sở dữ liệu tham chiếu được tạo ra bằng cách sử dụng cơ sở dữ liệu trong Hệ thống định danh điện tử quốc gia (NID) để so sánh với các trường tương đương trong các cơ sở dữ liệu cung cấp dịch vụ nhằm tìm ra một kết quả trùng khớp phù hợp. Ngay sau đó, Mã số định danh công dân (NIN) từ cơ sở dữ liệu tham khảo được nhúng vào cơ sở dữ liệu cung cấp dịch vụ của nhà cung cấp dịch vụ. Tùy thuộc vào các trường dữ liệu nhận dạng cá nhân (PID) của công dân được thu thập tại thời điểm đăng nhập trong Hệ thống định danh điện tử quốc gia (NID), Khuôn khổ cung cấp dịch vụ theo định danh điện tử (EISDF) có thể hỗ trợ hai kịch bản cho sự trùng khớp duy nhất của hồ sơ công dân. Xét ví dụ trong đó số thẻ bảo hiểm y tế đã được thu thập trong các trường dữ liệu công dân tại thời điểm đăng ký trong Hệ thống định danh điện tử quốc gia (NID). Trường số thẻ bảo hiểm y tế cùng với tên của công dân, có thể được sử dụng để tìm thấy một hồ sơ trùng khớp duy nhất trong cơ sở dữ liệu bảo hiểm y tế được duy trì bởi cơ quan BHXH.

Cơ sở dữ liệu cung cấp dịch vụ

Health Insurance Card Number	NIN	Name	DoB	Province Code	Applicant No	Bank Code	Bank Name
1234523		Viet Huong Thảo	16-Aug-78	234	...	...	...
4453898		Hau Hung Vuong	12-Sep-76	234			
2545322		Trang Nguyen	2-Jan-65	234	...	...	...
4352893		Nam Luong	4-Feb-68	234	...	...	...
5423492		Hieu Duong	23-Apr-75	234			...
7354858		Hoang Trần	13-May-56	234	...	...	..

NIN	Name	Age	DoB	Address	Health Insurance Card Number
345674565234	Viet Huong Thảo	22	16-Aug-78	63 Ly Thai To, Hanoi, Vietnam	1234523
345676565678	Hau Hung Vuong	24	12-Sep-76	63 Ly Thai To, Hanoi, Vietnam	4453898
245678565123	Trang Nguyen	45	2-Jan-65	63 Ly Thai To, Hanoi, Vietnam	2545322
123674565234	Nam Luong	35	4-Feb-68	63 Ly Thai To, Hanoi, Vietnam	4352893
439667365834	Hieu Duong	38	23-Apr-75	63 Ly Thai To, Hanoi, Vietnam	5423492
534457456503	Hoang Trần	32	13-May-56	63 Ly Thai To, Hanoi, Vietnam	7354858

Cơ sở dữ liệu đăng ký thẻ Hệ thống định danh điện tử quốc gia (NID)

Một kịch bản khác có thể là một trường hợp không có thêm các trường lấy được khi đăng ký cho thẻ Hệ thống định danh điện tử quốc gia (NID). Trong trường hợp này, một hoặc nhiều trường dữ liệu nhận dạng cá nhân (PID) có thể được sử dụng để so sánh. Hãy xem xét ví dụ về cơ sở dữ liệu cung cấp dịch vụ của nhà cung cấp viễn thông với nhận dạng của khách hàng.

Cơ sở dữ liệu cung cấp dịch vụ

NIN	Name	Age	DoB	Address	Mobile No
345674565234	Viet Huong Thảo	22	16-Aug-78	63 Ly Thai To, Hanoi, Vietnam	84-4 39346600
345676565678	Hau Hung Vuong	24	12-Sep-76	63 Ly Thai To, Hanoi, Vietnam	84-4 39346719
245678565123	Trang Nguyen	45	2-Jan-65	63 Ly Thai To, Hanoi, Vietnam	84-4 39312330
123674565234	Nam Lương	35	4-Feb-68	63 Ly Thai To, Hanoi, Vietnam	84-3 23446600
439667365834	Hieu Dương	38	23-Apr-75	63 Ly Thai To, Hanoi, Vietnam	84-4 39344321
534457456503	Hoang Trần	32	13-May-56	63 Ly Thai To, Hanoi, Vietnam	84-4 39231344

Customer No	NIN	Name	DoB	Address	Mobile No	Email	Plan Name
12434		Viet Huong Thảo	16-Aug-78	63 Ly Thai To, Hanoi, Vietnam	84-4 39346600	...	...
12342		Hau Hung Vuong	12-Sep-76	63 Ly Thai To, Hanoi, Vietnam	84-4 39346719	...	...
23453		Trang Nguyen	2-Jan-65	63 Ly Thai To, Hanoi, Vietnam	84-4 39312330	tra...	XYZ
22342		Nam Lương	4-Feb-68	63 Ly Thai To, Hanoi, Vietnam	84-3 23446600	....	...
34567		Hieu Dương	23-Apr-75	63 Ly Thai To, Hanoi, Vietnam	84-4 39344321	...	...
23123		Hoang Trần	13-May-56	63 Ly Thai To, Hanoi, Vietnam	84-4 39231344	...	...

Cơ sở dữ liệu danh mục khách hàng của công ty viễn thông

Như đã trình bày ở trên, các trường của dữ liệu nhận dạng cá nhân (PID) (tên, ngày sinh, địa chỉ) từ cơ sở dữ liệu đăng nhập Hệ thống định danh điện tử quốc gia (NID) được đối chiếu với các trường tương ứng của dữ liệu nhận dạng cá nhân (PID) trong bảng cung cấp dịch vụ và dựa trên với tỷ lệ phần trăm trùng khớp của các trường riêng biệt – số lượng trùng khớp sẽ được tính tổng thể. Việc tạo nguồn trùng khớp 100% là vô cùng lý tưởng, nhưng rất hiếm khi xảy ra; do đó, có thể được giả định rằng nếu tỷ lệ trùng khớp vượt quá một ngưỡng xác định trước (có thể là 80%) thì việc so khớp được tiến hành.

Việc thu thập thông tin bổ sung trong suốt quá trình đăng nhập vào Hệ thống định danh điện tử quốc gia (NID) có thể làm cho việc tao nguồn trở nên đơn giản; và có thể được sử dụng để đối chiếu với hồ sơ giữa các dữ liệu nhận dạng cá nhân (PID) và các bảng cung cấp dịch vụ có nhận dạng duy nhất đã được thu thập trước đó. Sự hiện diện của một số thẻ bảo hiểm y tế, một số thẻ làm việc, hoặc bất kỳ nhận dạng duy nhất nào khác có thể chứng minh cho lợi ích của việc tìm kiếm một sự so sánh.

Phương pháp hữu cơ có thể yêu cầu các nhà cung cấp dịch vụ liên hệ với công dân, hoặc ngược lại, để cập nhật các Mã số định danh công dân (NIN) / định danh điện tử (eID) trong cơ sở dữ liệu cung cấp dịch vụ. Nó có thể liên quan đến việc tạo ra các "điểm tiếp xúc" tại nơi công dân tự nguyện, hoặc do các nhà cung cấp dịch vụ tạo ra, khởi tạo bao gồm Mã số định danh công dân (NIN) / định danh điện tử (eID) của ông/bà trong cơ sở dữ liệu cung cấp dịch vụ. Cách tiếp cận này có thể được thực hiện trong chế độ tương tác hoặc hàng loạt.

Trong chế độ tương tác, các cư dân có thể tiếp cận các nhà cung cấp dịch vụ vì những lý do sau đây:

1. Để tận dụng các bộ phận đặc trưng mang lại lợi ích cho chương trình và/hoặc dịch vụ. Các điểm tiếp xúc có thể thuộc lĩnh vực này hoặc trong các văn phòng cung cấp dịch vụ.
2. Để hồi đáp với chiến dịch của các nhà cung cấp dịch vụ đăng ký Mã số định danh công dân (NIN) / định danh điện tử (eID) để phục vụ lợi ích và dịch vụ cụ thể.
3. Công dân tự nguyện tiếp cận các nhà cung cấp dịch để đăng ký Mã số định danh công dân (NIN) / định danh điện tử (eID) cho một dịch vụ cụ thể.

Trong chế độ hàng loạt, nhà cung cấp dịch vụ đưa ra danh sách của các cặp dữ liệu (định danh điện tử (eID)/ Mã số chứng minh nhận dạng quốc gia (NIN), nhận dạng và xác thực cư dân (KYR +)) để xử lý. Các nhà cung cấp dịch vụ có thể triển khai một chương trình mới, nơi có thể thực hiện nhập dữ liệu ngoại tuyến với dưới dạng trình ứng dụng của công dân; nó cũng có thể sử dụng các chương trình hiện tại cho người đăng ký mới.

Các ban này có thể tận dụng một hoặc nhiều kênh giao tiếp với công dân để thu thập Mã số chứng minh nhận dạng quốc gia (NIN)/định danh điện tử (eID) của họ. Một số các kênh có thể được sử dụng là:

1. **Thu thập tài liệu tại các đại lý**. Công dân có thể nộp bản sao thẻ của Hệ thống định danh điện tử quốc gia (NID) và mẫu đăng ký cho nhà cung cấp dịch vụ (ví dụ, thẻ bảo hiểm y tế). Sau đó các nhà cung cấp dịch vụ cập nhật cơ sở dữ liệu cung cấp dịch vụ dựa trên thông tin đã được cung cấp.

2. **Tin nhắn SMS**. Các nhà cung cấp dịch vụ cho phép một ứng dụng dựa trên tin nhắn SMS. Công dân sẽ gửi một tin nhắn SMS có chứa Mã số định danh công dân (NIN) và một số đăng ký cho nhà cung cấp dịch vụ. Ví dụ: UPD < Mã số chứng minh nhận dạng quốc gia (NIN)> <Số thẻ Bảo hiểm y tế > được gửi đến một số 59.999 (chỉ có tính minh họa). Ứng dụng back-end tạo nguồn Mã số định danh công dân (NIN) trong cơ sở dữ liệu bằng cách sử dụng số thẻ bảo hiểm y tế như là một khoá. Đối với việc xác minh thông tin được cung cấp, các nhà cung cấp dịch vụ cần phải thực hiện chứng thực nhân khẩu học sau khi tạo nguồn.

3. **Cập nhật điều hành hỗ trợ tại đại lý**. Các nhà cung cấp dịch vụ cho phép tạo nguồn trực tiếp của Mã số định danh công dân (NIN) / định danh điện tử (eID) tại điểm tiếp xúc với công dân nơi công dân có thể mang theo thẻ Hệ thống định danh điện tử quốc gia (NID) và một bản đăng ký dịch vụ. Một công dân được chứng thực cả nhân khẩu học và sinh trắc

học trước khi Mã số định danh công dân (NIN) được tạo nguồn vào cơ sở dữ liệu cung cấp dịch vụ.

4. **Email**. Tương tự như các phương pháp tiếp cận dựa trên tin nhắn SMS, email được gửi đi trong một định dạng được xác định trước cùng với bản sao quét hỗ trợ tài liệu đính kèm. Khi nhận được email, ứng dụng back-end trích xuất các thông tin cần thiết từ email và tạo nguồn cơ sở dữ liệu một cách thích hợp. Trong trường hợp thất bại, công dân sẽ được thông báo bằng một email trả lời.

5. **Bưu điện/ Chuyển phát nhanh**. Tương tự như phương pháp thu thập tài liệu đề cập trước đó; Tuy nhiên, trong trường hợp này việc thu thập tài liệu diễn ra dưới hình thức bưu điện/ chuyển phát nhanh.

6. **Trả lời bằng giọng nói tương tác**. Một điện thoại dựa trên ứng dụng trả lời bằng giọng nói tương tác (IVR) có thể thu thập Mã số định danh công dân (NIN) và só đăng ký theo một cách tương tác. Sau khi có được thông tin cần thiết, ứng dụng back-end sẽ tạo nguồn cơ sở dữ liệu cung cấp dịch vụ thích hợp. Xác thực nhân khẩu học có thể được thực hiện sau khi tạo nguồn để xác minh.

7. **Cổng thông tin Web tự cập nhật**. Các nhà cung cấp dịch vụ có thể mở ra một cổng thông tin cho công dân để cập nhật số điện thoại hoặc số tài khoản thụ hưởng nhận dạng của họ, cùng với Mã số chứng minh nhận dạng quốc gia (NIN). Các nhà cung cấp dịch vụ có thể làm một chứng thực nhân khẩu học ở back-end trước khi cập nhật cơ sở dữ liệu của họ với Mã số định danh công dân (NIN) / định danh điện tử (eID).

Những thách thức tạo nguồn phổ biến và giải pháp

Các dịch vụ tạo nguồn định danh điện tử (eID) có thể được thiết kế để giải quyết một số thách thức chung trong quá trình tạo nguồn. Dưới đây là một số trong những thách thức chung cho các quy trình cần thiết hoặc cách giải quyết được thiết kế nhằm khắc phục chúng.

1. **Dữ liệu đầy đủ không được thu thập trong cơ sở dữ liệu cung cấp dịch vụ**. Dữ liệu thường được nhập thủ công bởi các nhà điều hành bán chuyên nghiệp dẫn đến các mục không đầy đủ và không chính xác trong cơ sở dữ liệu cung cấp dịch vụ. Thiếu một đảm bảo chất lượng (QA) phù hợp được xử lý bởi các nhà cung cấp dịch vụ cũng đóng góp thêm cho vấn đề này. Một chiến lược số hóa dữ liệu có thể giải quyết vấn đề tiềm tàng này.

2. **Không có sự kết hợp chính xác giữa thông tin tương tự trên các nguồn dữ liệu khác nhau**. Qua quan sát có thể thấy cùng một dữ liệu trên các bảng khác nhau không được nhập tương tự. Lấy trường hợp của tên "Hau Hung Vuong" và "HH Vuong" là đề cập đến cùng một người. Việc tạo nguồn có thể hỗ trợ chính xác / một phần kết hợp của các trường dữ liệu khác nhau; Vì vậy, vấn đề này có thể được xử lý trong quá trình làm sạch và chuẩn hoá dữ liệu.

3. **Dữ liệu trong cơ sở dữ liệu cung cấp dịch vụ bằng tiếng Việt**. Việc đối chiếu dữ liệu trong cùng một ngôn ngữ có thể được thực hiện với các thuật toán so sánh tiêu chuẩn, nhưng nếu thông tin trong cơ sở dữ liệu bằng các ngôn ngữ khác nhau (ví dụ, tiếng Anh và tiếng Việt) thì không có cách nào so sánh được. Nếu quá trình đối chiếu được thực hiện, thì cần phải có các thuật toán cực kỳ thông minh và phức tạp để thay đổi mức độ dữ liệu được thực hiện trong cơ sở dữ liệu.

4. **Tất cả các dữ liệu cần thiết không có sẵn**. Cần phải có hoạch cẩn thận và phối hợp với các nhóm hỗ trợ . Ví dụ, thông tin mã hóa để mã hóa và giải mã có thể được cung cấp trong trường hợp chỉ có mã số được lưu trữ (thường trong lĩnh vực giới tính, nam giới được lưu trữ là 1 trong khi nữ là 2).

5. **Công cụ thường có sẵn trở nên không có khả năng để xử lý khối lượng lớn dữ liệu**. Thông thường mọi người thích sử dụng Microsoft Excel để xử lý dữ liệu. Tuy nhiên, có thể quan sát thấy sau một vài nghìn hồ sơ được nhập vào một bảng tính Excel, thời gian phản hồi của công cụ này bị suy giảm đáng kể. Trong trường hợp này, các công cụ cơ sở dữ liệu thay thế có thể được xem xét; ví dụ, nhập dữ liệu vào một cơ sở dữ liệu (MySQL, MS SQL Server, Oracle, vv).

6. **Huy động công dân**. Trong trường hợp của tạo nguồn có hệ thống, huy động công dân là cần thiết để hoàn thành việc tạo nguồn. Một cách tiếp cận tạo nguồn có hệ thống đa kênh cần phải được sử dụng để huy động có hiệu quả.

II. Cơ cấu tổ chức: Vai trò và trách nhiệm

Dịch vụ nhận dạng điện tử

Trách nhiệm của Cơ quan quản lý Định danh điện tử Việt Nam (EIDAV)

1. Cơ quan quản lý Định danh điện tử Việt Nam thực hiện cơ chế cập nhật dữ liệu nhận dạng cá nhân mới nhất của công dân từ Hệ thống định danh điện tử quốc gia của Bộ Công an theo định kỳ.

2. Cơ quan quản lý Định danh điện tử Việt Nam sẽ cung cấp dịch vụ định danh điện tử (EISDF) như xác nhận với các tổ chức sử dung dịch vụ nhận dạng (ISCA) mong muốn sử dụng dịch vụ nhằm thiết lập định danh điện tử (eID)-/Hệ thống định danh điện tử quốc gia-người dùng trước khi tiến hành các công việc tiếp theo.

3. Cơ quan quản lý Định danh điện tử Việt Nam xác định mô hình hoạt động và cam kết đối với việc cung cấp dịch vụ nhận dạng điện tử.

4. Cơ quan quản lý Định danh điện tử Việt Nam xác định các nguyên tắc liên quan đến việc sử dụng nhận dạng điện tử, Mã số định danh công dân (NIN) và dịch vụ thuộc khuôn khổ cung cấp dịch vụ nhận dạng điện tử.

5. Cơ quan quản lý Định danh điện tử Việt Nam xác định tiêu chí thích hợp đối với các nhà cung cấp dịch vụ nhận dạng được quản lý (MISP), tạo thuận lợi cho thủ tục đăng ký, áp dụng và ký kết hợp đồng với các nhà cung cấp MISP.

6. Cơ quan quản lý Định danh điện tử Việt Nam xác định tiêu chí thích hợp đối với các tổ chức cung cấp dịch vụ nhận dạng (ISPA), tạo thuận lợi cho thủ tục đăng ký, áp dụng và ký kết hợp đồng với các tổ chức cung cấp ISPA.

7. Cơ quan quản lý Định danh điện tử Việt Nam xác định tiêu chí thích hợp đối với các tổ chức sử dung dịch vụ nhận dạng (ISCA), tạo thuận lợi cho thủ tục đăng ký, áp dụng và ký kết hợp đồng với các tổ chức sử dung ISCA.

8. Cơ quan quản lý Định danh điện tử Việt Nam xác định các chuẩn mực và điều khoản sẽ được tuân thủ bởi tất cả các thành viên tham gia hệ thống cung cấp dịch vụ định danh điện tử – gồm các tổ chức cung cấp dịch vụ nhận dạng ISPAs, các tổ chức sử dung dich vụ nhận dạng ISCA và các tiểu tổ chức sử dung dịch vụ nhận dạng. Những chuẩn mực và điều khoản sẽ gồm hệ thống, quy trình, và các điều khoản liên quan đến giao diện lập trình ứng dụng (API), cơ sở hạ tầng (gồm các thiết bị), quy trình, kỹ thuật, chứng nhận (nếu phù hợp), kiểm tra, bảo mật và các thỏa thuận về mức độ dịch vụ (SLA) (nếu phù hợp). Như vậy, Cơ quan quản lý Định danh điện tử Việt Nam sẽ xác định các chuẩn mực và điều khoản tối

thiểu đối với dịch vụ cung cấp nhận dạng điện tử, trong khi các đối tác hệ thống có thể mở rộng và bổ sung thêm các điều khoản và tiêu chuẩn để đáp ứng nhu cầu phạm vi ứng dụng của họ.

9. Cơ quan quản lý Định danh điện tử Việt Nam ban hành trên trang điện tử của mình các văn bản về chuẩn mực và điều khoản có hiệu lực. Cơ quan quản lý Định danh điện tử Việt Nam cũng có thể chọn cách thức chứng nhận cho tất cả những ứng dụng sẽ được sử dụng bởi các tổ chức sử dung dịch vụ nhận dạng (và các tiểu tổ chức sử dung dịch vụ nhận dạng) nhằm khởi động hoạt động nhận dạng điện tử, bao gồm:
    a. Chứng nhận (tự chứng nhận hoặc thông qua các tổ chức độc lập đã được phê duyệt) đối với ứng dụng (như các ứng dụng về quy trình nhận dạng của hệ thống các tổ chức sử dung dịch vụ nhận dạng) có thể được sử dụng bởi tổ chức sử dung dịch vụ nhận dạng và các thành viên khác trong việc chứng nhận nhận dạng điện tử.
    b. Chứng nhận bằng cảm biến vân tay hoặc võng mạc, và cặp thiết bị tách được gắn vào các thiết bị nhận dạng. Đây là trách nhiệm của người bán trang thiết bị phù hợp để nhận được chứng nhận sản phẩm bởi Cơ quan chứng nhận chất lượng và kiểm thử về chuẩn hóa (STQC) của Bộ Thông tin truyền thông.

10. Cơ quan quản lý Định danh điện tử Việt Nam được bảo lưu quyền chỉ đạo kiểm tra tất cả các thành viên chính trong hệ thống cung cấp dịch vụ nhận dạng bao gồm các tổ chức dịch vụ nhận dạng (ISPA) và tổ chức sử dung dịch vụ nhận dạng (ISCA) – dù tự thực hiện hay thông qua Cơ quan quản lý Định danh điện tử Việt Nam – các cơ quan kiểm tra độc lập được chỉ định/phê duyệt – nhằm kiểm nghiệm sự tuân thủ những chuẩn mực và điều khoản đã có hiệu lực. Trong quá trình kiểm tra, Cơ quan quản lý Định danh điện tử Việt Nam/cơ quan kiểm tra có thể thanh tra cơ sở kinh doanh, quá trình hoạt động và hệ thống, cơ sở hạ tầng, bảo mật,… của đối tượng được kiểm tra.

11. Cơ quan quản lý Định danh điện tử Việt Nam được giữ quyền đưa ra hành động phù hợp chống lại các bên không tuân thủ các điều khoản, bao gồm việc không cho bên đó sử dụng hệ thống dịch vụ nhận dạng EISDF hoặc chấm dứt hợp đồng sau một khoảng thời gian phù hợp để có hành động điều chỉnh theo quy định trong hợp đồng tương ứng.

12. Cơ quan quản lý Định danh điện tử Việt Nam cung cấp cơ chế giải quyết tranh chấp khung trong khuôn khổ cung cấp dịch vụ định danh điện tử EISDF.

13. Trong tương lai, nếu có bất kỳ chi phí nào gắn với khuôn khổ cung cấp dịch vụ nhận dạng EISDF, Cơ quan quản lý Định danh điện tử Việt Nam sẽ quyết định mức phí hoặc thiết lập khung để xác định mức phí đó.

14. Cơ quan quản lý Định danh điện tử Việt Nam có thể đảm nhiệm bất cứ vai trò nào, khi cần thiết, để đảm bảo rằng hệ thống vẫn tiếp tục cung cấp dịch vụ không bị gián đoạn và hoạt động bình thường.

Trách nhiệm của Nhà cung cấp dịch vụ nhận dạng được quản lý

Trách nhiệm chính của Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) gồm hoạt động giao dịch xác nhận trong khuôn khổ cung cấp dịch vụ nhận dạng (như tiếp nhận yêu cầu nhận dạng, thực hiện việc kết nối Dữ liệu nhận dạng cá nhân nhận được với thông tin xác nhận tại Trung tâm Lưu trữ dữ liệu nhận dạng tập trung (CRIDS), và gửi kết quả) liên quan tới kết nối mạng, trung tâm dữ liệu, dịch vụ xác nhận sẵn có, thỏa thuận về mức độ dịch vụ (SLA) với các tổ chức sử dung dịch vụ nhận dạng (nếu có) và quản lý hệ thống hoạt động và thực thi.

Trách nhiệm của Tổ chức cung cấp dịch vụ nhận dạng

1. Tổ chức cung cấp dịch vụ nhận dạng ISPA gắn với hợp đồng với Cơ quan quản lý định danh điện tử Việt Nam bằng cách tuân theo các chuẩn mực và điều khoản của Cơ quan quản lý định danh điện tử Việt Nam, gồm các thỏa thuận về mức độ dịch vụ (SLA) nếu phù hợp.

2. Tổ chức cung cấp dịch vụ nhận dạng ISPA đảm bảo rằng tất cả hoạt động và cơ sở hạ tầng – gồm hệ thống, quy trình, công nghệ thông tin và cơ sở hạ tầng sinh trắc học, bảo mật,… – đều được tuân thủ theo các tiêu chuẩn và điều khoản của Cơ quan quản lý định danh điện tử Việt Nam.

3. Khi Tổ chức cung cấp dịch vụ nhận dạng nhận được yêu cầu dịch vụ như việc chứng thực của Tổ chức cung cấp dịch vụ nhận dạng, thì Tổ chức cung cấp dịch vụ nhận dạng nên tiến hành thủ tục kiểm tra sơ bộ đối với những thông tin yêu cầu dịch vụ trước khi chuyển đến máy chủ nền tảng cung cấp dịch vụ nhận dạng điện tử. Yêu cầu này sẽ chỉ được chuyển tới máy chủ xác nhận nếu đáp ứng đủ các điều kiện và hoàn chỉnh. Nếu không, yêu cầu sẽ được gửi trả lại Tổ chức sử dung dịch vụ nhận dạng với thông báo lỗi phù hợp (thông báo này sau đó sẽ được chuyển tiếp tới thiết bị xác nhận với đầy đủ hướng dẫn cần thiết).

4. Khi tiếp nhận phản hồi từ máy chủ, Tổ chức cung cấp dịch vụ nhận dạng sẽ chuyển kết quả giao dịch tới Tổ chức sử dung dịch vụ nhận dạng đã đưa ra yêu cầu.

5. Tổ chức cung cấp dịch vụ nhận dạng được gợi ý nên duy trì nhật ký của tất cả những giao dịch đã được thực hiện. Nhật ký sẽ được duy trì trong một khoảng thời gian cụ thể xác định bởi Cơ quan quản lý định danh điện tử VIệt Nam và có thể được chia sẻ với các đối tượng khác, nhưng chỉ về mặt thông tin cơ bản. Nhật ký này có thể thu thập được chi tiết giao dịch như mã số chứng minh nhận dạng quốc gia, yêu cầu Tổ chức sử dung dịch vụ nhận dạng,... nhưng dữ liệu nhận dạng cá nhân không liên kết với bất kỳ giao dịch xác nhận nào. Việc lưu trữ nhật ký thực hiện sẽ tuân theo luật áp dụng của từng nước.

6. Trong quá trình triển khai hoạt động, Tổ chức cung cấp dịch vụ nhận dạng sẽ tuân theo tất cả luật và quy định áp dụng của quốc gia trong phạm vi quản lý và bảo mật dữ liệu.

7. Tổ chức cung cấp dịch vụ nhận dạng đảm bảo rằng hệ thống dịch vụ nhận dạng của mình được kiểm soát bởi một cơ quan kiểm soát hệ thống thông tin đã được chứng nhận bởi một cơ quan đã được công nhận trước khi tiến hành các hoạt động. Tổ chức cung cấp dịch vụ nhận dạng có thể cung cấp báo cáo kiểm tra đã chứng nhận tới Cơ quan quản lý định danh điện tử Việt Nam sau khi xác nhận là phù hợp với các tiêu chuẩn, định hướng, điều khoản... đã có hiệu lực.

8. Hàng năm, tổ chức cung cấp dịch vụ nhận dạng đảm bảo rằng các hoạt động và hệ thống liên quan đến dịch vụ nhận dạng được kiểm tra bởi các cơ quan kiểm tra hệ thống thông tin đã được chứng nhận bởi một tổ chức chính thức. Tổ chức cung cấp dịch vụ nhận dạng cung cấp báo cáo kiểm tra đã được chứng nhận tới Cơ quan quản lý định danh điện tử Việt Nam sau khi xác nhận là phù hợp với các tiêu chuẩn, định hướng, điều khoản... đã có hiệu lực. Ngoài ra, Cơ quan quản lý định danh điện tử Việt Nam được bảo lưu quyền kiểm tra Tổ chức cung cấp dịch vụ nhận dạng ISPA (tự kiểm tra hoặc thông qua Cơ quan quản ký định danh điện tử Việt Nam-cơ quan được chỉ định hoặc phê duyệt). Trong quá trình kiểm tra, Tổ chức cung cấp dịch vụ nhận dạng phối hợp chặt chẽ với Cơ quan quản lý định danh điện tử Việt Nam hoặc tổ chức kiểm tra và cung cấp truy cập cho các cơ sở kinh doanh, thủ tục, biên bản, hệ thống, biên chế và các vấn đề khác có liên quan đối với hoạt động nhận dạng. Trong trường hợp không tuân thủ quy định, Cơ quan quản lý định danh điện tử Việt Nam được tiến hành các hành động cần thiết như kết thúc hợp đồng sau một khoảng thời gian phù hợp để có hành động điều chỉnh. Chi phí kiểm tra do Tổ chức cung cấp dịch vụ nhận dạng chi trả.

9. Tổ chức cung cấp dịch vụ nhận dạng duy trì việc thông báo cho Cơ quan quản ký định danh điện tử Việt Nam về danh sách máy chủ của Tổ chức sử dung dịch vụ nhận dạng. Khi ký hợp đồng với một tổ chức sử dung dịch vụ nhận dạng mới, Tổ chức cung cấp dịch vụ nhận dạng phải thông báo cho Cơ quan quản lý định danh điện tử Việt Nam (theo chi tiết yêu cầu bởi Cơ quan quản lý định danh điện tử Việt Nam) trước khi tiến hành thực hiện dịch vụ cho Tổ chức sử dung dịch vụ nhận dạng. Tương tự, khi một tổ chức cung cấp dịch vụ nhận dạng không còn ràng buộc với Tổ chức sử dung dịch vụ nhận dạng, tổ chức đó sẽ thông báo Cơ quan quản lý định danh điện tử Việt Nam trong vòng 7 ngày kể từ ngày kết thúc ràng buộc.

10. Tổ chức cung cấp dịch vụ nhận dạng có thể ký hợp đồng với Tổ chức sử dung dịch vụ nhận dạng để cung cấp bất kỳ dịch vụ có giá trị gia tăng nào. Tuy nhiên, những dịch vụ có giá trị gia tăng này không được thể hiện dưới hình thức dịch vụ nhận dạng.

11. Tổ chức cung cấp dịch vụ nhận dạng chịu trách nhiệm với Cơ quan quản lý định danh điện tử Việt Nam về tất cả các hoạt động liên quan đến việc xác nhận được đề cập đến trong hợp đồng giữa Cơ quan quản lý định danh điện tử Việt Nam và Tổ chức cung cấp dịch vụ nhận dạng. Ngay cả trong trường hợp hoạt động đầu ra của Tổ chức cung cấp dịch vụ nhận dạng thông tin tới các đối tượng khác, trách nhiệm đối với những hoạt động này và kết quả xác nhận vẫn thuộc về Tổ chức cung cấp dịch vụ nhận dạng.

12. Trong trường hợp điều tra liên quan đến gian lận kết quả xác nhận hoặc tranh chấp, Tổ chức cung cấp dịch vụ nhận dạng tăng cường phối hợp với Cơ quan quản lý định danh điện tử Việt Nam (hoặc chi nhánh) và/hoặc bất kỳ cơ quan điều tra có thẩm quyền nào. Việc phối hợp này gồm cung cấp quyền truy cập cơ sở, biên bản, hệ thống, biên chế, cơ sở hạ tầng, bất kỳ nguồn/thông tin liên quan khác và bất kỳ lĩnh vực nào liên quan đến hoạt động xác nhận.

<u>Tiêu chí phù hợp</u>

Các tiêu chí quy định đối với một Tổ chức cung cấp dịch vụ nhận dạng ISPA được liệt kê như sau.

1. Tổ chức có thể là:
    a. Một Bộ/cơ quan cấp trung ương/địa phương của Chính phủ hoặc đơn vị thực thi nhiệm vụ công (PSU) do Bộ/cơ quan địa phương đó chủ trì và quản lý; hoặc một tổ chức hợp pháp dưới quyền cơ quan trung ương/địa phương đó; hoặc một tổ chức

phi lợi nhuận/tổ chức chuyên quản cấp quốc gia; hoặc một công ty đã được đăng ký tại Việt Nam đáp ứng các yêu cầu sau:

i. Khả năng tài chính: Mỗi năm lãi ít nhất 100 triệu đồng trong vòng 3 năm trờ lại đây.
ii. Khả năng kỹ thuật.
iii. Một nhà cung cấp dịch vụ viễn thông (TSP) đang hoạt động trong mạng lưới cáp quang tại Việt Nam và có tối thiểu 100 điểm đăng nhập mạng (PoP) tại tất cả các tỉnh thành; hoặc một nhà cung cấp dịch vụ mạng (NSP) có khả năng cung cấp kết nối mạng về truyền dữ liệu, giọng nói và có thoả thuận với một nhà cung cấp dịch vụ tin cậy (TSP) đã có 100 điểm đăng nhập mạng; hoặc một nhà tích hợp giải pháp (SI) có thoả thuận với một nhà cung cấp dịch vụ tin cậy (TSP)/nhà cung cấp dịch vụ mạng (NSP) như đề cập tới ở trên.

b. Chi nhánh chưa vào danh sách đen của cơ quan trung ương/địa phương, hoặc bất kỳ đơn vị thực thi dịch vụ công (PSU) nào trong vòng 5 năm gần đây.

2. Chi nhánh chứng minh được khả năng triển khai thiết kế, cấu hình, thực thi và duy trì được cơ sở hạ tầng và hệ thống theo yêu cầu của Tổ chức cung cấp dịch vụ nhận dạng ISPA theo điều khoản của Cơ quan quản lý định danh điện tử Việt Nam; đồng thời chứng thực được sự thiết yếu của nguồn nhân lực với những kỹ năng cần thiết để thể hiện đúng chức năng dự kiến. Quyết định của Cơ quan quản lý định danh điện tử Việt Nam liên quan đến ký kết hợp đồng hay không phụ thuộc chính vào tiềm năng của Tổ chức cung cấp dịch vụ nhận dạng.

3. Tổ chức cung cấp dịch vụ nhận dạng ISPA sẽ tham gia khuôn khổ cung cấp dịch vụ định danh điện tử EISDF thông qua thủ tục bổ nhiệm được xác định và chỉ đạo bởi Cơ quan quản lý định danh điện tử Việt Nam. Các tổ chức có nguyện vọng trở thành Tổ chức cung cấp dịch vụ nhận dạng có thể đăng ký với Cơ quan quản lý định danh điện tử Việt Nam bằng cách cung cấp những thông tin cần thiết với những giấy tờ phù hợp. Cơ quan quản lý định danh điện tử Việt Nam kiểm tra đơn đăng ký và phê duyệt các đăng ký đạt tiêu chuẩn là Tổ chức cung cấp dịch vụ định danh điện tử (ISPA). Tổ chức cung cấp dịch vụ định danh điện tử được phê duyệt sẽ ký hợp đồng với Cơ quan quản lý định danh điện tử Việt Nam và được phép thiết lập kết nối bảo mật với máy chủ chứng thực của Cơ quan quản lý dịch vụ định danh điện tử Việt Nam; kết nối này tuân thủ các chuẩn mực và điều khoản của Cơ quan quản lý định danh điện tử Việt Nam.

4. Mỗi hợp đồng của Tổ chức cung cấp dịch vụ nhận dạng (ISPA) đều quy định thời hạn hợp đồng cụ thể, kết thúc thời hạn hợp đồng, Tổ chức cung cấp dịch vụ nhận dạng được tự do đăng ký để gia hạn hợp đồng. Cơ quan quản lý định danh điện tử Việt Nam sẽ đánh giá các đăng ký gia hạn này và phê duyệt đăng ký đạt tiêu chuẩn.

Trách nhiệm của Tổ chức sử dung dịch vụ nhận dạng ISCA

1. Tổ chức sử dung dịch vụ nhận dạng thông báo tới Cơ quan quản lý định danh điện tử Việt Nam về từng giao dịch với mong muốn có được xác nhận chính xác nếu có. Lựa chọn tiêu chí xác nhận thể hiện việc xác nhận thông tin cụ thể được yêu cầu từ dịch vụ định danh điện tử tới Hệ thống định danh điện tử quốc gia và tới người nắm giữ để khởi động dịch vụ đó. Lựa chọn xác nhận thông tin là quyết định của riêng Tổ chức sử dung dịch vụ nhận dạng, không phải của bên nào khác, gồm cả Cơ quan quản lý định danh điện tử Việt Nam và các Tổ chức cung cấp dịch vụ nhận dạng, chịu trách nhiệm đối với quyết định này. Có thể Tổ chức sử dung dịch vụ nhận dạng thay đổi loại dịch vụ nhận dạng nếu có nhu cầu, và thông báo tới Cơ quan quản lý định danh điện tử Việt Nam.

2. Tổ chức sử dung dịch vụ nhận dạng tham gia vào quá trình và Tổ chức này bổ sung vào danh sách do Cơ quan quản lý định danh điện tử Việt Nam cấp để bắt đầu cung cấp dịch vụ trong khuôn khổ cung cấp dịch vụ nhận dạng điện tử. Khi có bất kỳ tiêu chí nào thay đổi, Tổ chức sử dung dịch vụ nhận dạng sẽ thông báo Cơ quan quản lý định danh điện tử Việt Nam về danh mục dịch vụ để được xác nhận. Quá trình này có thể được thực hiện bằng phương thức tự thực hiện, như cập nhật trực tuyến thông qua cổng điện tử của Cơ quan quản ký định danh điện tử Việt Nam.

3. Tổ chức sử dung dịch vụ nhận dạng thiết lập hoạt động liên quan đến dịch vụ nhận dạng (gồm hệ thống, quy trình, kỹ thuật, cơ sở vật chất, bảo mật…) phù hợp với tiêu chuẩn và quy định của Cơ quan quản lý định danh điện tử Việt Nam.

4. Tổ chức sử dung dịch vụ nhận dạng chịu trách nhiệm cung cấp mạng lưới từ các thiết bị nhận dạng tới máy chủ của Tổ chức sử dung dịch vụ nhận dạng và giữa tổ chức sử dung dịch vụ nhận dạng với máy chủ của Tổ chức cung cấp dịch vụ nhận dạng. Điều này phù hợp với các quy định bảo mật của Cơ quan quản lý định danh điện tử Việt Nam. Ngoài ra, đây cũng là trách nhiệm về việc mua và triển khai các chứng nhận/phần mềm/phần cứng… phù hợp với tiêu chuẩn nhận dạng của dịch vụ nhận dạng điện tử.

5. Tổ chức sử dung dịch vụ nhận dạng đảm bảo rằng các thiết bị được sử dụng cho dịch vụ nhận dạng sẽ được mua, triển khai và quản lý bởi tổ chức hoặc chi nhánh phù hợp với quy định và tiêu chuẩn của Cơ quan quản ký định danh điện tử Việt Nam được công bố bởi Cơ quan quản ký định danh điện tử Việt Nam.

6. Tổ chức sử dung dịch vụ nhận dạng truy cập vào tất cả các giao dịch của dịch vụ nhận dạng và duy trì chúng trong một khoảng thời gian cụ thể. Việc truy cập có thể ghi lại cụ thể từng giao dịch nhận dạng, nhưng không phải phản hồi tới dữ liệu nhận dạng cá nhân. Việc lưu trữ truy cập giao dịch phù hợp với luật và quy định áp dụng của quốc gia. Thông tin truy cập cụ thể được lưu trữ, thời hạn lưu trữ và các nội dung khác của lưu trữ dữ liệu sẽ được xác định bởi các tiêu chuẩn, quy định phù hợp với dịch vụ và lĩnh vực của Cơ quan quản lý định danh điện tử Việt Nam, yêu cầu của Tổ chức sử dung dịch vụ nhận dạng và các luật và quy định hiện hành khác.

7. Tổ chức sử dung dịch vụ nhận dạng cần triển khai chương trình phân tích gian lận có thể được dùng để phân tích các giao dịch nhận dạng liên quan để xác định những trường hợp và cách thức gian lận. Nếu Tổ chức sử dung dịch vụ nhận dạng trở thành nạn nhân của gian lận, hoặc phát hiện ra cách thức gian lận thông qua chương trình phân tích gian lận, thì tổ chức sẽ chia sẻ những thông tin cần thiết với Cơ quan quản lý định danh điện tử Việt Nam.

8. Dữ liệu nhận dạng cá nhận đã được mã hoá có thể không được lưu giữ, trừ khi chúng được xác nhận qua bước trung gian trong một thời gian ngắn, sau khi truyền dữ liệu sẽ bị xoá. Dữ liệu mật khẩu dùng một lần (OTP) và dữ liệu sinh trắc học khác được sử dụng với mục đích xác nhận nhận đạng điện tử sẽ không được lưu trữ trong bất kỳ hệ thống lưu trữ hoặc cơ sở dữ liệu nào. Tổ chức sử dung dịch vụ nhận dạng đảm bảo tất cả luật và quy định liên quan đều được tuân thủ liên quan đến lưu trữ và bảo vệ dữ liệu trong hệ thống; đồng thời đảm bảo rằng các đơn vị (nếu có) và các thiết bị xác nhận đều phù hợp.

9. Trong trường hợp các thiết bị xác nhận được hoạt động bởi Tổ chức sử dung dịch vụ nhận dạng (hoặc chi nhánh của tổ chức đó), trách nhiệm của Tổ chức sử dung dịch vụ nhận dạng là đảm bảo rằng việc tập huấn đầy đủ về các hoạt động đã được triển khai tới tất cả đại diện cung cấp dịch vụ.

10. Tổ chức sử dung dịch vụ nhận dạng đảm bảo rằng hệ thống xác nhận định danh điện tử được kiểm tra bởi một cơ quan kiểm tra hệ thống thông tin đã được chứng nhận bởi cơ

quan đã được công nhận trước khi tiến hành các hoạt động. Tổ chức sử dung dịch vụ nhận dạng sẽ cung cấp báo cáo kiểm tra tới Cơ quan quản lý định danh điện tử Việt Nam để xác nhận phù hợp với các tiêu chuẩn, định hướng và quy định hiện hành…

11. Tổ chức sử dung dịch vụ nhận dạng đảm bảo rằng hệ thống và hoạt động định danh điện tử được kiểm tra bởi một cơ quan kiểm tra hệ thống thông tin đã được chứng nhận bởi cơ quan đã được công nhận theo định kỳ hàng năm để xác nhận là phù hợp với các tiêu chuẩn và quy định của Cơ quan quản lý định danh điện tử Việt Nam; báo cáo kiểm tra sẽ được chia sẻ nếu Cơ quan quản lý định danh điện tử Việt Nam yêu cầu. Trách nhiệm của Tổ chức sử dung dịch vụ nhận dạng là đảm bảo rằng các tiểu tổ chức sử dung dịch vụ nhận dạng và các chi nhánh cũng được kiểm tra thường xuyên. Ngoài ra, Cơ quan quản lý định danh điện tử Việt Nam sẽ bảo lưu quyền kiểm tra hoạt động và hệ thống của Tổ chức sử dung dịch vụ nhận dạng (và chi nhánh của tổ chức, nếu có) bằng cách tự kiểm tra hoặc thông qua các cơ quan kiểm tra được chỉ định. Trong quá trình kiểm tra, Tổ chức sử dung dịch vụ nhận dạng cần phối hợp chặt chẽ với cơ quan kiểm tra và cung cấp truy cập cần thiết liên quan đến cơ sở, quy trình, biên bản, hệ thống, nhân viên và bất kỳ lĩnh vực nào khác phục vụ cho hoạt động xác nhận. Trường hợp không phù hợp, Cơ quan quản lý định danh điện tử Việt Nam được tiến hành những hoạt động cần thiết (như chấm dứt hợp đồng sau một thời hạn phù hợp để điều chỉnh hoạt động). Chi phí cho việc kiểm tra này được chi bởi Tổ chức sử dung dịch vụ nhận dạng.

12. Tổ chức sử dung dịch vụ nhận dạng chịu trách nhiệm xác định cơ chế giải quyết ngoại lệ và cơ chế hỗ trợ xác nhận khi xác nhận của dịch vụ định danh điện tử bị lỗi. Xác nhận lỗi xảy ra trong quá trình, cơ sở vật chất (gồm nguồn điện, công nghệ thông tin, thiết bị, mạng lưới kết nối) hoặc đọc dữ liệu sinh trắc học của người yêu cầu dịch vụ định danh điện tử không được đáp ứng hoặc sử dụng cho nhiều mục đích.

13. Khi Tổ chức sử dung dịch vụ nhận dạng thiết lập quan hệ đối tác với một tiểu Tổ chức sử dung dịch vụ nhận dạng, Tổ chức sử dung dịch vụ nhận dạng thông báo tới Cơ quan quản lý định danh điện tử Việt Nam về quan hệ đối tác trước khi bắt đầu hoạt động của tiểu Tổ chức sử dung dịch vụ nhận dạng mới. Tương tự, khi một tiểu Tổ chức sử dung dịch vụ nhận dạng kết thúc hợp tác với Tổ chức sử dung dịch vụ nhận dạng, Tổ chức sử dung dịch vụ nhận dạng cần thông bảo tới Cơ quan quản lý định danh điện tử Việt Nam trong vòng 7 ngày (hoặc một khoảng thời gian cụ thể) về việc kết thúc hợp tác. Quá trình cập nhật được dự tính theo phương thức tự cập nhật (self-service) (như cập nhật trực tuyến thông qua Cổng thông tin điện tử của Cơ quan quản lý nhận dang điện tử Việt Nam). Khi Tổ chức sử

dung dịch vụ nhận dạng hợp tác với một tiểu Tổ chức sử dung dịch vụ nhận dạng, Tổ chức sẽ tạo ra một mã cho tiểu Tổ chức sử dung dịch vụ nhận dạng để xác định tiểu Tổ chức sử dung dịch vụ nhận dạng cụ thể. Khi thông báo Cơ quan quản lý định danh điện tử Việt Nam, về quan hệ đối tác với tiểu Tổ chức sử dung dịch vụ nhận dạng, Tổ chức sử dung dịch vụ nhận dạng cũng thông báo tới Cơ quan quản lý định danh điện tử Việt Nam về mã của tiểu Tổ chức sử dung dịch vụ nhận dạng mới. Khi chuyển yêu cầu dịch vụ nhận dạng từ tiểu Tổ chức sử dung dịch vụ nhận dạng, Tổ chức sử dung dịch vụ nhận dạng luôn kèm theo mã của tiểu Tổ chức sử dung dịch vụ nhận dạng để việc truy cập giao dịch xác nhận định danh điện tử có thể theo dõi tất cả các yêu cầu nhận dạng. Mỗi tiểu Tổ chức sử dung dịch vụ nhận dạng cần có một từ khoá chứng nhận riêng đuọc sử dụng để việc liên hệ hoặc ngắt liên hệ của tiểu Tổ chức sử dung dịch vụ nhận dạng có thể thực hiện bằng cách tạo mới hoặc huỷ bỏ những từ khoá chứng nhận tương ứng.

14. Trách nhiệm của tổ chức sử dung dịch vụ nhận dạng là đảm bảo tất cả các tiểu Tổ chức sử dung dịch vụ nhận dạng được kiểm tra thường xuyên để phù hợp với quy định của Cơ quan quản lý định danh điện tử Việt Nam. Trong trường hợp không phù hợp, Tổ chức sử dung dịch vụ nhận dạng cần báo cáo lên Cơ quan quản lý định danh điện tử Việt Nam và tiến hành hoạt động sửa chữa kịp thời theo hướng dẫn của Cơ quan quản lý định danh điện tử Việt Nam.

15. Khi Tổ chức sử dung dịch vụ nhận dạng thoả thuận với tiểu Tổ chức sử dung dịch vụ nhận dạng, từ khía cạnh của Cơ quan quản lý định danh điện tử Việt Nam, Tổ chức sử dung dịch vụ nhận dạng chịu trách nhiệm kết nối giữa thiết bị nhận dạng của tiểu Tổ chức sử dung dịch vụ nhận dạng với hệ thống của Tổ chức sử dung dịch vụ nhận dạng.

16. Ngay cả khi thông tin đầu ra về hoạt động của Tổ chức sử dung dịch vụ nhận dạng được cung cấp cho bên thứ ba, trách nhiệm về hoạt động dịch vụ nhận dạng vẫn thuộc về Tổ chức sử dung dịch vụ nhận dạng. Tổ chức sử dung dịch vụ nhận dạng cũng chịu trách nhiệm nhằm đảm bảo rằng hoạt động dịch vụ nhận dạng của bên thứ ba phù hợp với tiêu chuẩn và quy định của Cơ quan quản lý định danh điện tử Việt Nam, và những quy định này thường xuyên được kiểm tra bởi cơ quan kiểm tra độc lập được chỉ định.

17. Trong trường hợp điều tra gian lận hoặc tranh chấp liên quan đến việc nhận dạng, Tổ chức sử dung dịch vụ nhận dạng sẽ mở rộng hợp tác chặt chẽ với Cơ quan quản lý định danh điện tử Việt Nam (hoặc chi nhánh của Cơ quan) và/hoặc bất kỳ cơ quan điều tra có thẩm quyền nào. Việc này bao gồm cả cung cấp quyền truy cập đối với cơ sở, bản ghi, nhân viên,

những nguồn thông tin phù hợp và bất kỳ lĩnh vực nào phù hợp khác đối với hoạt động nhận dạng.

18. Tổ chức sử dung dịch vụ nhận dạng chủ động thông báo cho Cơ quan quản lý định danh điện tử Việt Nam về bất kỳ dữ liệu nhận dạng điện tử, dịch vụ xác nhận hay bất cứ dữ liệu liên quan đến định danh điện tử hoặc hệ thống thuộc mạng lưới của Tổ chức.

Các tiêu chí phù hợp

Các tiêu chí phù hợp của một Tổ chức sử dung dịch vụ nhận dạng được liệt kê như dưới đây.

1. Tổ chức có thể là:
    a. Một Bộ/cơ quan cấp trung ương/địa phương của Chính phủ hoặc đơn vị thực thi nhiệm vụ công (PSU) do Bộ/cơ quan địa phương đó chủ trì và quản lý; hoặc một tổ chức hợp pháp dưới quyền cơ quan trung ương/địa phương đó; hoặc một tổ chức phi lợi nhuận/tổ chức chuyên quản cấp quốc gia; hoặc một tổ chức tài chính/ngân hàng/công ty viễn thông.
    b. Một đơn vị pháp lý đã được đăng ký tại Việt Nam đang tìm kiếm để sử dụng dịch vụ nhận dạng và triển khai cung cấp dịch vụ. Các ứng dụng do các tổ chức này cung cấp có thể được cân nhắc phê duyệt bởi hội đồng quản trị của Tổ chức sử dung dịch vụ nhận dạng và được thành lập bởi Cơ quan quản lý định danh điện tử Việt Nam.

2. Tổ chức chứng minh năng lực triển khai và thực thi, duy trì cơ sở vật chất và yêu cầu hệ thống để trở thành Tổ chức sử dung dịch vụ nhận dạng. Quyết định của Cơ quan quản lý định danh điện tử Việt Nam liên quan đến thiết lập quan hệ với Tổ chức sử dung dịch vụ nhận dạng sẽ được đưa ra.

3. Các tổ chức tìm kiếm sử dụng dịch vụ định danh điện tử nhằm triển khai các dịch vụ ứng dụng đối với Cơ quan quản lý định danh điện tử bằng cách cung cấp thông tin cần thiết theo yêu cầu của những tài liệu hỗ trợ, cũng như những thông tin về Tổ chức cung cấp dịch vụ nhận dạng (ISPA) thông qua việc Tổ chức sử dung dịch vụ nhận dạng sẽ kết nối với máy chủ nhận dạng.

4. Khi nhận được thông tin cần thiết (và tài liệu, nếu có), Cơ quan quản lý định danh điện tử sẽ phê duyệt Tổ chức sử dung dịch vụ nhận dạng. Sau khi được phê duyệt, Tổ chức sử dung dịch vụ nhận dạng và Cơ quan quản lý định danh điện tử Việt Nam sẽ ký hợp đồng.

Trách nhiệm của một tiểu Tổ chức sử dung dịch vụ nhận dạng

Trách nhiệm của một tiểu Tổ chức sử dung dịch vụ nhận dạng sẽ giống trách nhiệm của một Tổ chức sử dung dịch vụ nhận dạng. Những trách nhiệm của Tổ chức sử dung dịch vụ nhận dạng được nêu như trên cũng sẽ được áp dụng đối với tiểu Tổ chức sử dung dịch vụ nhận dạng.

Các tiêu chí thích hợp

1. Một tổ chức có mong muốn trở thành một tiểu Tổ chức sử dung dịch vụ nhận dạng cần xác định rõ mục tiêu thoả thuận và đăng ký với Tổ chức sử dung dịch vụ nhận dạng bằng cách cung cấp thông tin cần thiết và các tài liệu hỗ trợ, nếu cần.

2. Tiểu Tổ chức sử dung dịch vụ nhận dạng cam kết phù hợp với tiêu chuẩn và quy định của Cơ quan quản lý định danh điện tử về hoạt động xác nhận nhận dạng điện tử.

3. Tổ chức sử dung dịch vụ nhận dạng thông báo cho Cơ quan quản lý định danh điện tử Việt Nam về thoả thuận với tiểu Tổ chức sử dung dịch vụ nhận dạng và triển khai cung cấp dịch vụ tiếp sau đó.

Thiết bị nhận dạng

Tiêu chí thực hiện

1. Các thiết bị nhận dạng được triển khai theo hệ thống xác nhận định danh điện tử bởi Tổ chức sử dung dịch vụ nhận dạng, tiểu Tổ chức sử dung dịch vụ nhận dạng hoặc chi nhánh của Tổ chức sử dung dịch vụ nhận dạng/tiểu Tổ chức sử dung dịch vụ nhận dạng hoặc nơi đưa ra yêu cầu nhận dạng điện tử.

2. Tổ chức sử dung dịch vụ nhận dạng/tiểu Tổ chức sử dung dịch vụ nhận dạng chịu trách nhiệm cung cấp mạng lưới kết nối từ các thiết bị tới máy chủ của Tổ chức sử dung dịch vụ nhận dạng/tiểu Tổ chức sử dung dịch vụ nhận dạng và tới máy chủ của Tổ chức sử dung dịch vụ nhận dạng/ Tổ chức cung cấp dịch vụ nhận dạng, đây cũng là trách nhiệm tìm kiếm và triển khai bất kỳ phần cứng/phần mềm/chứng nhận nào phù hợp với tiêu chuẩn xác nhận nhận dạng điện tử.

3. Tổ chức sử dung dịch vụ nhận dạng/tiểu Tổ chức sử dung dịch vụ nhận dạng chịu trách nhiệm cài đặt phần cứng/phần mềm/chứng nhận phù hợp với tiêu chuẩn xác nhận định

danh điện tử kết nối với thiết bị kết nối mạng của khách hàng/người hưởng lợi/ người đăng ký (CBS).

Chức năng của các thiết bị nhận dạng

1. Các chức năng này phù hợp với tiêu chuẩn và quy định của Cơ quan quản lý định danh điện tử Việt Nam.

2. Các thiết bị nhận dạng sinh trắc học phù hợp với tiêu chuẩn dữ liệu sinh trắc học và được chứng nhận là phù hợp bởi cơ quan có thẩm quyền của chính phủ.

3. Các thiết bị nhận dạng sinh trắc học sử dụng biện pháp khám phá tốt nhất trong khuôn khổ cung cấp dịch vụ nhận dạng điện tử.

4. Thiết bị nhận dạng sinh trắc học cung cấp thiết bị sản phẩm của họ sử dụng bộ công cụ phát triển phầm mềm (SDK) giao điện lập trình ứng dụng (API) đã được Cơ quan quản lý định danh điện tử Việt Nam công bố nhằm đảm bảo sự tương kết.

5. Thiết bị nhận dạng có thể được hỗ trợ hoạt động hoặc tự hoạt động.

6. Những thiết bị này có khả năng thu thập thông tin phù hợp từ Hệ thống định danh điện tử quốc gia/người yêu cầu dịch vụ nhận dạng điện tử, chuẩn bị gói dữ liệu nhận dạng (gói dữ liệu nhận dạng cá nhân), thực hiện cấu trúc dữ liệu còn giá trị, truyền gói dữ liệu và nhận kết quả nhận dạng theo hướng dẫn tại các bước tiếp theo, nếu có. Việc thu thập dữ liệu định danh điện tử bằng các thiết bị nhận dạng được tiến hành phù hợp với quy định của Cơ quan quản lý định danh điện tử Việt Nam.

7. Các thiết bị nhận dạng thực hiện không theo dữ liệu sinh trắc học của người yêu cầu định danh điện tử và dữ liệu mật khẩu dùng một lần (OTP) sẽ được ghi lại với mục đích xác nhận định danh điện tử trong suốt giao dịch, trừ trường hợp nhận dạng qua bước trung gian được mô tả như dưới đây, khi mà các thiết bị này có thể được lưu trữ dưới dạng dữ liệu mã hoá trong một khoảng thời gian nhất định.

8. Xét về mặt lưu trữ dữ liệu, các thiết bị nhận dạng tuân theo luật và quy định hiện hành của quốc gia.

Trách nhiệm của bên yêu cầu dịch vụ nhận dạng điện tử/Hệ thống định danh điện tử quốc gia

1. Đối tượng nắm giữ dịch vụ nhận dạng điện tử/Hệ thống định danh điện tử quốc gia thoả thuận để được có thẩm quyền đối với dữ liệu nhận dạng cá nhân dựa trên dịch vụ định danh điện tử và thể hiện sự tự nguyện truy cập dịch vụ của Tổ chức sử dung dịch vụ nhận dạng/ tiểu Tổ chức sử dung dịch vụ nhận dạng.

2. Trách nhiệm của đối tượng nắm giữ dịch vụ nhận dạng điện tử/ Hệ thống định danh điện tử quốc gia là giữ cho dữ liệu nhận dạng cá nhân của họ luôn có hiệu lực và sẵn sàng trong Trung tâm Lưu trữ dữ liệu nhận dạng điện tủe công dân tập trung (CRIDS). Họ hoạt động tương tự theo định kỳ hoặc theo yêu cầu trong một số trường hợp. Một số ví dụ có thể được cập nhật như khi cần:
    a. Thông báo Bộ Công an về thay đổi địa chỉ.
    b. Cập nhật thu thập dấu vân tay trên cơ sở định kỳ.
    c. Sửa đổi lỗi.
3. Đối tượng nắm giữ dịch vụ nhận dạng điện tử/Hệ thống định danh điện tử quốc gia có thể tiếp cận Cơ quan quản lý định danh điện tử Việt Nam trong trường hợp họ có lý do tin rằng dữ liệu định danh điện tử cá nhân của họ được thoả hiệp bởi bất kỳ tổ chức nào thuộc hệ thống nhận dạng.

4. Đối tượng nắm giữ dịch vụ nhận dạng điện tử/Hệ thống định danh điện tử quốc gia chủ động thông báo cho Cơ quan quản lý định danh điện tử Việt Nam về việc không sử dụng được dịch vụ nhận dạng hoặc dữ liệu định danh điện tử nào.

Quyền hạn, trách nhiệm và nghĩa vụ của đối tượng nắm giữ dịch vụ nhận dạng điện tử/Hệ thống định danh điện tử quốc gia được quy định chi tiết trong điều lệ của đối tượng nắm giữ dịch vụ nhận dạng điện tử/Hệ thống định danh điện tử quốc gia.

<u>Các tiêu chí phù hợp</u>

Những cá nhân thích hợp yêu cầu dịch vụ định danh điện tử truy cập hệ thống định danh điện tử khi đăng ký với Bộ Công an bằng cách cung cấp thông tin nhận dạng nhân khẩu học và sinh trắc học. Khi hoàn thành quá trình đăng ký, mỗi cá nhân thích hợp sẽ nhận được Mã số định danh công dân (NIN) của người đó. Thông tin nhận dạng này được lưu trữ đề phòng việc trao đổi thông tin về Mã số định danh công dân (NIN) trong Trung tâm lưu trữ dữ liệu định danh điện tử công dân tập trung (CRIDS).

Dịch vụ lựa chọn nhận dạng điện tử

Mô hình hoạt động của dịch vụ lựa chọn định danh điện tử được quản lý và hoạt động bởi các tổ chức trong khuôn khổ cung cấp dịch vụ định danh điện tử có vài trò và trách nhiệm đã được định rõ. Những vai trò và trách nhiệm chính được mô tả như sau:

1. Cơ quan quản lý nhận dạng quốc gia Việt Nam (NIDAV) cung cấp công cụ, chuyên gia, kinh nghiệm thực tiễn tốt nhất và tư vấn tham vấn cần thiết về yêu cầu đối với nhà cung cấp dịch vụ để thực hiện việc lựa chọn dịch vụ nhận dạng điện tử, như:
    a. Lựa chọn mức độ khả dụng và nền tảng tạo nguồn thông tin định danh điện tử quốc gia (NESP) để các nhà cung cấp dịch vụ sử dụng.
    b. Tài liệu cần thiết trên cổng thông tin điện tử công cộng.
    c. Đăng ký trực tuyến trên cổng thông tin điện tử công cộng để Tổ chức sử dung dịch vụ nhận dạng có thể tiếp cận những công cụ phù hợp.

2. Tổ chức sử dung dịch vụ nhận dạng (ISCA) là nhà cung cấp quan tâm đến chức năng giám định nhận dạng sử dụng trong quá trình chuyển giao dịch vụ; tổ chức này sẽ chịu trách nhiệm lựa chọn mã số chứng minh nhận dạng quốc gia/định danh điện tử trong cơ sở dữ liệu hiện có. Một số trách nhiệm của tổ chức này gồm:
    a. Chuẩn bị cơ sở dữ liệu sẵn có bằng cách thực hiện số hoá và tập trung hoá dữ liệu.
    b. Chọn chiến lược lựa chọn: phương pháp chọn từ trên xuống hoặc phương pháp hữu cơ.
    c. Đăng ký với Cơ quan quản lý định danh điện tử Việt Nam để sử dụng mức độ thoả dụng ngoại tuyến và nền tảng tạo nguồn thông tin định danh điện tử quốc gia NESP.
    d. Thực hiện nhận dạng nhân khẩu học và sinh trắc học để nhận dạng điện tử.
    e. Thiết lập kênh truyền thông tin theo yêu cầu với hệ thống ngân hàng lõi (CBS), nếu dùng phương pháp lựa chọn hữu cơ.

Dịch vụ Nhận dạng và xác thực khách hàng điện tử eKYC

Mô hình hoạt động của quá trình nhận dạng và xác thực khác hàng điện tử được quản lý và hoạt động bởi cùng tổ chức kết cấu liên quan đến dịch vụ nhận dạng điện tử. Những vai trò và trách nhiệm chính của nhận dạng và xác thực khách hàng điện tử được mô tả như sau.

1. **Cơ quan quản lý nhận dạng quốc gia Việt Nam.** Giống như nhận dạng điện tử, Hệ thống định danh điện tử quốc gia được quy định và giám sát về thủ tục và hệ thống hỗ trợ nhận dạng và xác thực khách hàng điện tử. Chức năng gồm:

a. Cung cấp quyền truy cập nhận dạng và xác thực khách hàng điện tử theo mong muốn của Tổ chức sử dung dịch vụ nhận dạng để sử dụng hoạt động kinh doanh như là điều kiện tiên quyết mở rộng dịch vụ tới các đối tượng nắm giữ dịch vụ nhận dạng điện tử/Hệ thống định danh điện tử quốc gia.
b. Xác định mô hình hoạt động và thoả thuận về nhận dạng và xác thực khách hàng điện tử.
c. Xác định quy luật liên quan đến sử dung dịch vụ nhận dạng và xác thực khách hàng điện tử.
d. Đảm bảo rằng các tiêu chí phù hợp với nhà cung cấp dịch vụ nhận dạng được quản lý (MISP) gồm thiết kế và thực hiện nhận dạng và xác thực khách hàng điện tử như là một phần trách nhiệm.
e. Xác định các tiêu chí phù hợp và tiếp nhận quy trình để Tổ chức sử dung dịch vụ nhận dạng tiếp cận dịch vụ nhận dạng và xác thực khách hàng điện tử, tạo thuận lợi ứng dụng và đăng ký sử dụng, sau đó có thể ký hợp đồng với Tổ chức sử dung dịch vụ nhận dạng.
f. Xác định tiêu chuẩn và quy định có thể được gắn với tất cả các tổ chức (như Tổ chức cung cấp dịch vụ nhận dạng, Tổ chức sử dung dịch vụ nhận dạng và các tiểu tổ chức sử dung dịch vụ nhận dạng) tham gia vào hệ thống nhận dạng và xác thực khách hàng điện tử. Các tiêu chuẩn và quy định về hệ thống và thủ tục, có thể gồm các quy định đối với giao diện lập trình ứng dụng (API), cơ sở vật chất, thiết bị, thủ tục, kỹ thuật, chứng nhận (nếu có), kiểm tra, bảo mật, và thoả thuận về mức độ dịch vụ (SLA) (nếu thích hợp). Như vậy, Hệ thống định danh điện tử quốc gia sẽ xác định các tiêu chuẩn và quy định tối thiểu đối với nhận dạng và xác thực khách hàng điện tử, trong khi các đối tác trong hệ thống có thể mở rộng và bổ sung các tiêu chuẩn và quy định khác để đáp ứng nhu cầu ứng dụng và miền xác định.
g. Công bố các văn bản trên trang web về tiêu chuẩn và quy định liên quan đến nhận dạng và xác thực khách hàng điện tử. Hệ thống định danh điện tử quốc gia có thể lựa chọn tất cả các ứng dụng được sử dụng bởi Tổ chức sử dung dịch vụ nhận dạng (và tiểu Tổ chức sử dung dịch vụ nhận dạng) trong việc khởi động hoạt động nhận dạng và xác thực khách hàng điện tử – bằng cách tự khởi động hoặc thông qua các chi nhánh chứng nhận độc lập được phê duyệt.

2. **Nhà cung cấp dịch vụ nhận dạng được quản lý (MISP).** Nhà cung cấp dịch vụ nhận dạng được quản lý có thể đưa ra dịch vụ nhận dạng và xác thực khách hàng điện tử thay mặt cho Hệ thống định danh điện tử quốc gia. Trách nhiệm và lĩnh vực chính gồm hoạt động giao dịch nhận dạng và xác thực khách hàng điện tử (như tiếp nhận yêu cầu nhận dạng,

thực hiện khớp nối dữ liệu nhận dạng cá nhân nhận được bằng cách liên hệ dịch vụ nhận dạng và truyền kết quả), mạng lưới và dữ liệu hoạt động trung tâm, dịch vụ nhận dạng và xác thực khách hàng điện tử sẵn có, thoả thuận về mức độ dịch vụ với Tổ chức sử dung dịch vụ nhận dạng (nếu có) và điều hành hoạt động và thực hiện.

3. **Tổ chức cung cấp dịch vụ nhận dạng.** Kênh chính kết nối với dịch vụ nhận dạng và xác thực khách hàng điện tử là thông qua mạng lưới bảo mật của một tổ chức cung cấp dịch vụ nhận dạng.

4. **Tổ chức sử dung dịch vụ nhận dạng.** Tổ chức sử dung dịch vụ nhận dạng có thể là một tổ chức yêu cầu sử dụng dịch vụ nhận dạng và xác thực khách hàng điện tử để khởi động chuyển giao dịch vụ. Mỗi Tổ chức sử dung dịch vụ nhận dạng có thể sử dụng quá trình nhận dạng và xác thực khách hàng điện tử để khởi động một hoặc nhiều dịch vụ. Một Tổ chức sử dung dịch vụ nhận dạng ký hợp đồng chính thức với Hệ thống định danh điện tử quốc gia để được truy cập. Tổ chức sử dung dịch vụ nhận dạng đảm bảo rằng yêu cầu ban đầu về nhận dạng và xác thực khách hàng điện tử từ thiết bị của tổ chức là phù hợp với tiêu chuẩn và quy định hiện hành của Hệ thống định danh điện tử quốc gia và được hoàn thành trước khi truyền dữ liệu đến Tổ chức cung cấp dịch vụ nhận dạng.
    a. Chuyển giao dịch vụ nhận dạng và xác thực khách hàng điện tử yêu cầu liên lạc với dịch vụ xác nhận để nhận được sự đồng ý của cư dân. Theo đó, Tổ chức sử dung dịch vụ nhận dạng, ngoài trách nhiệm về dịch vụ nhận dạng và xác thực khách hàng điện tử cũng phải có trách nhiệm liên quan đến việc chuyển giao dịch vụ xác nhận.
    b. Tổ chức sử dung dịch vụ nhận dạng gắn với quá trình và danh mục đang thực hiện của Tổ chức sử dung dịch vụ nhận dạng được cung cấp bởi Hệ thống định danh điện tử quốc gia nhằm triển khai dịch vụ nhận dạng và xác thực khách hàng điện tử. Khi có bất kỳ sự thay đổi tiêu chí nào, Tổ chức sử dung dịch vụ nhận dạng sẽ thông báo cho Hệ thống định danh điện tử quốc gia về danh mục dịch vụ của mình mà đã được thực hiện bởi dịch vụ nhận dạng và xác thực khách hàng điện tử. Việc này có thể được tiến hành theo hình thức tự giác như cập nhật trực tuyến trên cổng thông tin của Hệ thống định danh điện tử quốc gia.
    c. Tổ chức sử dung dịch vụ nhận dạng có thể công bố những hoạt động liên quan đến dịch vụ nhận dạng và xác thực khách hàng điện tử (bao gồm hệ thống, quy trình, kỹ thuật, cơ sở vật chất, bảo mật…) phù hợp với tiêu chuẩn và quy định của Hệ thống định danh điện tử quốc gia.

d. Tổ chức sử dung dịch vụ nhận dạng có thể sử dụng mạng lưới được cung cấp bởi Tổ chức sử dung dịch vụ nhận dạng giữa các thiết bị cung cấp dịch vụ nhận dạng, và Tổ chức sử dung dịch vụ nhận dạng với máy chủ của tổ chức, cho dịch vụ xác nhận. Ngoài ra, tổ chức cũng có trách nhiệm triển khai các phần cứng, phần mền, chứng nhận… phù hợp với tiêu chuẩn nhận dạng và xác thực khách hàng điện tử.
e. Tổ chứ sử dung dịch vụ nhận dạng có thể truy cập vào tất cả giao dịch nhận dạng và xác thực khách hàng điện tử và duy trì chúng trong một khoảng thời gian nhất định. Những thông tin chi tiết của giao dịch nhận dạng và xác thực khách hàng điện tử, nhưng không phải thông tin về dữ liệu nhận dạng cá nhân. Việc lưu trữ truy cập phải phù hợp với luật và quy định hiện hành của quốc gia. Chi tiết truy cập được lưu trữ, thời gian lưu trữ và bất kỳ thông tin lư trữ dữ liệu nào đều tuân theo quy định áp dụng đối với dịch vụ của Tổ chức sử dung dịch vụ nhận dạng, và yêu cầu của riêng tổ chức sử dung dịch vụ nhận dạng cũng như quy định và luật hiện hành.
f. Cách thức phân tích gian lận được triển khai bởi Tổ chức sử dung dịch vụ nhận dạng sẽ có khả năng phân tích giao dịch liên quan đến nhận dạng và xác thực khách hàng điện tử để xác định các trường hợp và cách thức gian lận.
g. Trong trường hợp thiết bị dịch vụ nhận dạng được tiến hành bởi nhân viên của Tổ chức sử dung dịch vụ nhận dạng (hoặc của chi nhánh), Tổ chức sử dung dịch vụ nhậnd ạng sẽ chịu trách nhiệm nhằm đảm bảo rằng nhân viên sẽ được tập huấn phù hợp để thực hiện những nhiệm vụ liên quan đến nhận dạng và xác thực khách hàng điện tử.
h. Tổ chức sử dung dịch vụ nhận dạng đảm bảo rằng hệ thống liên quan đến nhận dạng và xác thực khách hàng điện tử được kiểm tra bởi một cơ quan kiểm tra chứng nhận bởi tổ chức được công nhận trước khi tiến hành hoạt động. Tổ chức cung cấp dịch vụ nhận dạng cung cấp báo cáo kiểm tra được chứng nhận cho Hệ thống định danh điện tử quốc gia để xác nhận tính phù hợp với các quy định, định hướng, quy định có hiệu lực.
i. Tổ chức sử dung dịch vụ nhận dạng có trách nhiệm xác định cơ chế hỗ trợ và giải quyết ngoại lệ khi chức năng nhận dạng và xác thực khách hàng điện tử bị lỗi. Lỗi xảy ra do quá trình, cơ sở vật chất (gồm nguồn điện, CNTT, thiết bị, mạng lưới kết nối) hoặc đọc dữ liệu sinh trắc học (nơi dữ liệu sinh trắc học không thể được yêu cầu hoặc sử dụng vì lý do nào đó).
j. Khi truyền yêu cầu nhận dạng và xác thực khách hàng điện tử từ một tiểu Tổ chức cung cấp dịch vụ nhận dạng, Tổ chức cung cấp dịch vụ nhận dạng luôn kèm theo

mã của tiểu Tổ chức cung cấp dịch vụ nhận dạng để việc truy cập có thể giữ nguyên trạng của tất cả các giao dịch.

k. Hoạt động Tổ chức cung cấp dịch vụ nhận dạng được mở rộng cho bên thứ ba thì trách nhiệm đối với hoạt động nhận dạng và xác thực khách hàng điện tử và kết quả nhận dạng vẫn sẽ thuộc về Tổ chức sử dung dịch vụ nhận dạng. Tổ chức sử dung dịch vụ nhận dạng cũng sẽ chịu trách nhiệm đảm bảo hoạt động liên quan đến nhận dạng và xác thực khách hàng điện tử như hoạt động được thực hiện bởi bên thứ ba phù hợp với tiêu chuẩn và quy định của Hệ thống định danh điện tử quốc gia. Tổ chức sử dung dịch vụ nhận dạng cũng sẽ đảm bảo hoạt động của bên thứ ba được kiểm tra thường xuyên bởi một cơ quan kiểm tra độc lập đã được phê duyệt.

l. Trong trươngd hợp điều tra gian lận hoặc tranh chấp liên quan đến nhận dạng và xác thực khách hàng điện tử, Tổ chức sử dung dịch vụ nhận dạng mở rộng phạm vi hợp tác với Hệ thống định danh điện tử quốc gia (hoặc cơ quan của hệ thống) và/hoặc cơ quan điều tra có thẩm quyền khác. Việc này gồm cung cấp quyền tiếp cận cơ sở, biên bản, nhân viên, hệ thống, nguồn thông tin phù hợp và bất kỳ lĩnh vực của hoạt động xác nhận nào khác – cũng như hoạt động của tổ chức thuộc hệ thống.

5. **Tiểu Tổ chức sử dung dịch vụ nhận dạng.** Bất kỳ tổ chức đăng ký hợp pháp nào tại Việt Nam muốn sử dụng dịch vụ nhận dạng và xác thực khách hàng điện tử để triển khai hoạt động và trở thành một Tổ chức sử dung dịch vụ nhận dạng hoặc có thể tiếp cận một tổ chức thông qua tổ chức đã có. Trong trường hợp này, sẽ trở thành tiểu tổ chức sử dung dịch vụ nhận dạng mà Tổ chức sử dung dịch vụ nhận dạng có thoả thuận.

6. **Thiết bị phục vụ dịch vụ nhận dạng.** Có thể giống như thiết bị được sử dụng trong xác nhận nhận dạng và xác thực khách hàng điện tử và sẽ có khả năng nắm được thông tin đầu vào được yêu cầu theo dịch vụ nhận dạng và xác thực khách hàng điện tử. Thiết bị này có thể được hỗ trợ hoạt động hoặc tự hoạt động. Thiết bị có thể là máy tính để bản, máy tính xách tay, ki-ốt, điện thoại cầm tay… được kết nối, nếu được yêu cầu, với công cụ sinh trắc học để lưu lại dấu vân tay hoặc hình ảnh. Thiết bị này sẽ được hoạt động bởi Tổ chức sử dung dịch vụ nhận dạng hoặc tiểu Tổ chức sử dung dịch vụ nhận dạng, hoặc đon vị thuộc Tổ chức sử dung dịch vụ nhận dạng/tiểu Tổ chức sử dung dịch vụ nhận dạng.

7. **Đon vị nắm giữ nhận dạng điệ tử/ Hệ thống định danh điện tử quốc gia.** Trong bối cảnh dịch vụ nhận dạng và xác thực khách hàng điện tử, những đơn vị này thường được kết hợp

với Tổ chức sử dung dịch vụ nhận dạng hoặc tiểu Tổ chức sử dung dịch vụ nhận dạng với tư cách khách hàng, nhận viên; như: các đơn vị này tìm cách tiếp cận với dịch vụ của Tổ chức sử dung dịch vụ nhận dạng hoặc tiểu Tổ chức sử dung dịch vụ nhận dạng. Với họ, những người cần cung cấp dữ liệu KYC để đăng ký dịch vụ KYC điện tử. Đơn vị nắm giữ nhận dạng điện tử/hê thống nhận dạng quốc gia phải chịu trách nhiệm về việc đồng ý quy trình cung cấp dịch vụ KYC điện tử.

Dịch vụ nhận dạng điệc tử qua điện thoại.

Điện thoại di động với SIM được chuyên biệt hoá.

Điện thoai di động với SIM được chuyên biệt hoá có khả năng tạo chữ ký bảo mật (SSCD) được kích hoạt chứng nhận điện tử và mã khoá riêng. Điện thoại này được ban hành bởi Tổ chức quản lý đăng ký RA và chủ trì ứng dụng yêu cầu dịch vụ nhận dạng qua điện thoại và lưu trữ mã riêng trên SIM.

Trách nhiệm của Tổ chức quản lý đăng ký

Tổ chức quản lý đăng ký RA là nhà mạng di động cấp quốc gia như Viettel, Mobiphone, Vinaphone… chịu trách nhiệm cung cấp SIM với chức năng là thiết bị tạo chữ ký bảo mật SSCD cho cư dân tại các điểm bán hàng trên khắp cả nước. Một nhà mạng di động muốn trở thành Tổ chức quản lý đăng ký sẽ phải đăng ký với Cơ quan quản lý định danh điện tử Việt Nam.

Tổ chức quản lý đăng ký RA sẽ có trách nhiệm đăng ký đối với người sử dụng và kích hoạt chứng nhận dịch vụ nhận dạng bằng điện thoại cho người dân. Tổ chức này cũng chịu trách nhiệm về việc ngừng cung cấp dịch vụ do một số lý do như theo yêu cầu của người dân, mất hoặc kết hợp thiết bị tạo chữ lý bảo mật SSCD, hết hạn chứng nhận, hoặc vi phạm hợp đồng giữa người sử dụng với Cơ quan có thẩm quyền chứng nhận.

Trách nhiệm của nhà cung cấp dịch vụ tin cậy

Nhà cung cấp dịch vụ tin cậy (TSP) là nhà mạng di động chịu trách nhiệm chuyển yêu cầu dịch vụ định danh điện tử bằng di động từ Cơ quan quản lý định danh điện tử Việt Nam tới điện thoại di động của người dân thông qua mạng di động. Nhà cung cấp này cũng chịu trách nhiệm gửi dữ liệu đã ký từ di động tới Cơ quan có thẩm quyền chứng nhận CA, và phản hồi xác nhận cho Cơ quan quản lý định danh điện tử Vlệt Nam.

Nhà mạng di động phải đăng ký với Cơ quan quản lý định danh điện tử Việt Nam để trở thành một nhà cung cấp dịch vụ tin cậy có thẩm quyền. Nhà cung cấp dịch vụ tin cậy cung cấp cơ sở hạ

tầng mã khoá không dây wPKI cho Cơ quan quản lý định danh điện tử Việt Nam và Tổ chức sử dung dịch vụ nhận dạng và sẽ chịu trách nhiệm về những vấn đề liên quan đến cơ sở hạ tầng mã khoá và cung cấp giải pháp.

Trách nhiệm của Cơ quan có thẩm quyền chứng nhận CA

Cơ quan có thẩm quyền chứng nhận CA chịu trách nhiệm ban hành và hợp thức hoá chứng nhận; đồng thời hợp thức hoá dữ liệu đã ký khi phản hồi yêu cầu của nhà cung cấp dịch vụ tin cậy TSP.

Trách nhiệm của Cơ quan quản lý định danh điện tử Việt Nam

Cơ quan quản lý định danh điện tử Việt Nam chủ trì dịch vụ định danh điện tử bằng di động tại dữ liệu trung tâm, và đăng ký và thuê tất cả đối tượng trong hệ thống có thể đóng vai trò chuyển giao dịch vụ theo thang bậc.

Trách nhiệm của Tổ chức sử dung dịch vụ nhận dạng

Tổ chức sử dung dịch vụ nhận dạng có thể là bất kỳ tổ chức nào có nhu cầu sử dụng chức năng định danh điện tử bằng di động để khởi động dịch vụ. Mỗi tổ chức sử dung dịch vụ nhận dạng có thể sử dụng dịch vụ định danh điện tử qua di động để khởi động một hoặc nhiều dịch vụ. Tổ chức sử dung dịch vụ nhận dạng sẽ chịu trách nhiệm kết hợp ứng dụng chuyển giao dịch vụ (website) cho dịch vụ định danh điện tử qua di động được cung cấp bởi Cơ quan quản lý định danh điện tử Việt Nam.

Trách nhiệm của Tổ chức cung cấp dịch vụ nhận dạng

Tổ chức cung cấp dịch vụ nhận dạng có thể là tổ chức thiết lập bảo mật kết nối với dịch vụ định danh điện tử qua di động tại trung tâm dữ liệu của Cơ quan quản lý định danh điện tử Việt Nam. Tổ chức này sẽ truyền yêu cầu xác nhận thay cho Tổ chức sử dung dịch vụ nhận dạng và nhận phản hồi từ máy chủ định danh điện tử qua di động..

Trách nhiệm của người sử dụng

Người sử dụng có thể mua SIM từ đại lý dịch vụ dành cho người sử dụng. Để yêu cầu, người sử dụng phải cung cấp mã số chứng minh nhận dạng quốc gia NIN và dữ liệu nhân khẩu học để cho phép xác nhận tại đại lý dịch vụ của tổ chức đăng ký. Người sử dụng sẽ hợp thức hoá dữ liệu liên quan đến nhận dạng trên di động trong suôt quá trình sau đăng ký, yêu cầu của người sử dụng về mã số nhận dạng cá nhận PIN và mã số kích hoạt. Sau đó, người sử dụng sẽ chịu trách nhiệm đối với thẻ của mình.

Phụ lục 5: Kinh nghiệm thực tiễn

Nhiều quốc gia đã kích hoạt hệ thống định danh điện tử quốc gia và đang ở nhiều giai đoạn phát triển và sử dụng khác nhau. Do nhiều quốc gia mới chỉ bắt đầu giới thiệu sản phẩm mới lần đầu, thông qua nhiều mức mở rộng để người dân có thể nhận dịch vụ định danh điện tử và các tổ chức chính phủ cũng như tổ chức kinh doanh kích hoạt dịch vụ mới để sử dụng lợi thế này. Trong khi không có quốc gia nào đạt được việc thông qua và sử dụng toàn cầu, thì một số nước đã đạt nhiều tiến bộ hơn những nước khác. Nội dung phần này đề cập đến các dịch vụ định danh điện tử khác nhau được triển khai bởi 3 nước: Ấn Độ, Ét-xtô-nia và Bỉ; và làm rõ dịch vụ định danh điện tử được cải thiện chất lượng cung cấp cho khách hàng tại 3 nước này như thế nào. Phụ lục này cũng rút ra những kinh nghiệm và làm rõ những yếu tố chính có thể ảnh hưởng đến việc triển khai thành công và tăng mức độ sử dụng của hệ thống nhận dạng điện tử.

I. Ấn Độ

1. Tại Ấn Độ, việc không có khả năng tăng khả năng nhận dạng là một trong những cản trơ lớn nhất khiến cho người nghèo không tiếp cận được lợi ích và trợ cấp. Chính phủ Ấn Độ không cung cấp văn bản cấp quốc gia nào cụ thể về số người sử dụng dịch vụ nhận dạng. Thiếu nhận dạng người dân ở cấp độ quốc gia, các tổ chức dịch vụ khó theo dõi quá trình xác nhận nhận dạng đối với khách hàng/người hưởng lợi/người đăng ký (CBS) của mình. Những dấu hiệu cung cấp bởi các tổ chức dịch vụ đối với cá nân được sử dụng cho cả mục đích nhận dạng và xác minh tính pháp lý. Là một phần của quá trình tạo dịch vụ nhận dạng, hầu hết các cơ quan dịch vụ yêu cầu các cá nhân phải cung cấp giấy tờ tùy thân hay hóa đơn sử dụng dịch vụ được cung cấp bởi cơ quan dịch vụ khác như thẻ số tài khoản vĩnh viễn (PAN), hộ chiếu, giấy phép, hóa đơn điện thoại bằng lái... Chỉ 50 triệu người Ấn Độ đã có hộ chiếu, gần 100 triệu đã có thẻ PAN, và khoảng 200 triệu đã có giấy phép lái xe, còn lại phần lớn dân số không có bất kỳ giấy tờ chứng minh danh tính. Cách tiếp cận này dẫn đến một tình huống mà một bộ phận dân cư có nhiều thẻ nhận dạng, trong khi phần lớn không có bất kỳ giấy tờ nào khi sử dụng bất kỳ dịch vụ nào. Ngoài ra, chỉ có một số thẻ nhận dạng nhất định được chấp nhận là bằng chứng cấp quốc gia, ví dụ, thẻ PAN, hộ chiếu, sổ hộ khẩu. Để đạt được mục tiêu về tài chính và giảm đói nghèo trong cả nước, cần thiết phải có một hệ thống nhận dạng để những người không có bất kỳ giấy tờ chứng minh nào cũng có thể tham gia vào các chương trình xã hội và hưởng lợi ích mà họ được hưởng.

2. Tạo ra bước tiến để có một hệ thống nhận dạng dẫn đến những thách thức sau đây:

a. Nhiều cơ sở nhận dạng cho cùng một người do thiếu một cơ chế cấp quốc gia để nhận diện một cá nhân.

b. Hạn chế hoặc không có khả năng tương tác như hầu hết các thẻ nhận dạng được chấp nhận cho một mục đích cụ thể và chỉ ở một địa điểm cụ thể.

c. Rò rỉ các phúc lợi do việc tạo ra sự trùng lặp và nhận diện giả trong chương trình lợi ích tương tự khi không thể nhận diện cá nhân.

d. Nguy cơ bị đánh cắp nhận dạng cư trú và sử dụng sai bản phô tô giấy tờ tùy thân nộp làm bằng chứng là cao, và dễ dàng để giả mạo các tài liệu trên giấy.

e. Trùng lặp các nỗ lực trong việc tạo ra nhận dạng trong phạm vi của từng cơ quan dịch vụ tăng tổng chi phí nhận dạng, và gây ra bất tiện cho các cá nhân.

f. Tạo ra cơ sở nhận dạng riêng cho mỗi chương trình đối với kết quả cùng một cá nhân trong các cơ quan dịch vụ, không tương quan lợi ích khác nhau cho một cá nhân thông qua các chương trình khác nhau dẫn đến không có khả năng để xác minh quyền lợi chính xác và tác động có tác động thấp hơn từ các chương trình phúc lợi.

3. Hầu hết các cơ quan dịch vụ ban hành thẻ nhận dạng vật lý của "những gì người dùng có" như thẻ PAN, lương hưu, Đề án đảm bảo việc làm cho người nông thôn cấp quốc gia (NREGS), … mà chỉ có thể được xác thực bằng tay. Việc nhận dạng này xác nhận cơ chế thể hiện qua những thách thức sau đây:

a. Chi phí thiết lập cao hơn với khả năng mở rộng hạn chế. Nó chỉ hoạt động trong chế độ được hỗ trợ.

b. Khó khăn trong việc xác định giấy tờ giả và bản sao.

c. Không có khả năng để xác minh rằng người mang thẻ là chủ sở hữu hợp pháp trừ khi có ảnh của người đó.

d. Khó khăn trong việc sử dụng sai công nhận - không có cơ chế xác thực dấu vết kiểm tra; thay vào đó đòi hỏi phải có kiểm tra thủ công.

4. Trong bối cảnh này, Chính phủ Ấn Độ bắt tay vào thực hiện Dự án nhận dạng duy nhất (UID) vào tháng 1 năm 2009 với mục tiêu đưa ra một số nhận dạng duy nhất được biết đến như Aadhaar. Các Aadhaar có thể được kiểm tra và chứng thực một cách hiệu quả chi phí trực tuyến và đủ chặt chẽ để loại bỏ trùng lặp và giả mạo danh tính.

5. Aadhaar xác định cư dân thường trú và cung cấp các phương tiện để xác định rõ nhạn dạng cho các tổ chức công và tư trên toàn quốc. Ba đặc điểm chính của Aadhaar là: (a) vĩnh viễn (tồn tại trong suốt cuộc đời của một cá nhân); (b) độc đáo (mỗi người dân có một ID, không có hai người dân có ID giống nhau); và (c) toàn cầu (nhận dạng tương tự có thể được sử dụng trên các ứng dụng và các lĩnh vực).

6. Aadhaar được cung cấp trong quá trình thu thập thông tin cá nhân và sinh trắc học của người cư trú và tính duy nhất của dữ liệu được thiết lập thông qua một quá trình gọi là chống trùng lắp. Sau quá trình chống trùng lắp này, một số Aadhaar được ban hành và gửi thông báo chi tiết tới cư dân.

7. **Cơ quan nhận dạng duy nhất của Ấn Độ (UIDAI)** đã thông qua việc sử dụng công nghệ sinh trắc học như là một phần của chiến lược cốt lõi trong việc đáp ứng mục tiêu ngăn chặn việc phát hành số lượng nhận dạng trùng lặp đối với đối tượng cư trú. Thông tin sinh trắc học được sử dụng là dấu vân tay và quét võng mạc. Quá trình liên quan đến việc chống trùng lắp dữ liệu phù hợp với sinh trắc học của người cư trú về thông tin của những người dân trong cơ sở dữ liệu để đảm bảo tính duy nhất. Chỉ sau khi thực hiện quá trình này, một số Aadhaar 12 chữ số sẽ được phát hành.

8. Đối với bất kỳ cơ quan dịch vụ nào, xây dựng hệ thống nhận dạng và dịch vụ cho người thụ hưởng là cần thiết. Mặc dù nhận dạng cá nhân có thể là duy nhất và độc lập về yêu cầu dịch vụ nhưng quyền lợi của các dịch vụ được thiết lập bởi từng cơ quan dịch vụ riêng biệt. Do đó, thay vì chỉ định vai trò và trách nhiệm của các dịch vụ nhận dạng của các cơ quan hiện có, UIDAI được tạo ra là cơ quan quản lý và giám sát tổng thể của hệ thống xác nhận Aadhaar.

9. UIDAI được thành lập dưới quyền Ủy ban Kế hoạch. Cơ quan này được tạo ra bởi sự bảo trợ của Ủy ban Kế hoạch để đảm bảo một hệ thống nhận dạng trung lập cho các cơ quan có thẩm quyền và, đồng thời, cho phép tiếp cận tập trung để đạt được các mục tiêu đặt ra cho các Kế hoạch năm năm lần thứ mười một giai đoạn 2007-2012. Vai trò của cơ quan này là để phát triển và thực hiện các cơ sở hạ tầng thể chế, kỹ thuật và pháp lý cần thiết để phát hành nhận dạng duy nhất cho các cư dân Ấn Độ. Các UIDAI đã được tạo ra như một cơ quan theo luật định tuân thủ một đạo luật riêng biệt để thực hiện mục tiêu của mình. Luật cũng quy định các quy tắc, quy định, quy trình và các giao thức để được theo dõi bởi các cơ quan khác nhau hợp tác với UIDAI trong việc ban hành và kiểm tra số nhận dạng duy nhất.

10. UID chỉ cung cấp danh tính. Phạm vi quản lý của các UIDAI [18] được giới hạn việc phát hành một số nhận dạng duy nhất liên quan đến thông tin nhân khẩu học và sinh trắc học của một người. Không phải là trách nhiệm phát hành thẻ. UID chỉ có thể đảm bảo nhận dạng, không quyền lợi hay lợi ích.

---

[18] http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf

11. Số UID không chứa thông tin. Việc tải thông tin vào số chứng minh khiến cho dễ bị gian lận và trộm cắp. UID là một số ngẫu nhiên.

12. Một ủy ban chỉ đạo nội các do Thủ tướng Chính phủ và một nhóm các bộ trưởng của các bộ chủ chốt như Tài chính, Nông nghiệp, Ngoại giao, Luật pháp và Tư pháp, Thông tin và Truyền thông, Lao động và việc làm, đã được thành lập với chức năng quản lý tất cả các vấn đề liên quan đến UIDAI, bao gồm cả của tổ chức, kế hoạch, chính sách, chương trình, đề án, kinh phí và phương pháp được áp dụng để đạt được các mục tiêu của uỷ ban.

13. Dự án bao gồm việc thành lập cơ sở hạ tầng nhận dạng cấp quốc gia cho việc tạo ra và sử dụng nhận dạng duy nhất của quốc gia đó trực tuyến và có thể kiểm chứng. Nó giải quyết những thách thức phải đối mặt hiện có của các cơ quan dịch vụ về cơ sở nhận dạng. Sau đây là những lợi ích quan trọng:

a. Kể từ khi hoạt động ở Ấn Độ, đây là nhận dạng có thể kiểm chứng trực tuyến.

b. Không bị trùng lặp nên tránh rò rỉ phúc lợi.

c. Xác nhận cá nhân khi mỗi cùng là một người duy nhất mọi lúc mọi nơi; do đó, đảm bảo rằng các yêu sách chính đáng sẽ được phục vụ và hưởng lợi.

d. Có khả năng mở rộng các dịch vụ xác nhận trực tuyến, cho phép các cơ quan dịch vụ sử dụng nhiều kênh cung cấp dịch vụ.

e. Làm giảm nhiễu thụ hưởng và tìm kiếm do phụ thuộc ít hơn vào quy trình thủ công.

f. Là một quá trình cung cấp dịch vụ hiệu quả hơn và giảm chi phí của cơ sở nhận dạng.

g. Giúp loại bỏ sự cần thiết phải nộp bản sao của các tài liệu nhận dạng và làm giảm nguy cơ đánh cắp nhận dạng kết hợp với các tài liệu sử dụng.

h. Có một hệ thống kiểm toán điện tử tích hợp cho phép các cơ quan dịch vụ để theo dõi quá trình cung cấp dịch vụ một cách hiệu quả hơn.

14. UID chứng minh nhận dạng, không chứng minh quốc tịch. UID là bằng chứng về nhận dạng và không trao quyền công dân.

15. Các cơ sở dữ liệu nhận dạng trước đó ở Ấn Độ liên quan đến vấn đề gian lận và trùng lặp hoặc người thụ hưởng ảo. Để ngăn chặn điều này áp dụng vào cơ sở dữ liệu mới, UIDAI quyết định không sử dụng dữ liệu đã tồn tại trước đó. Thay vào đó, thực hiện một quá trình đăng ký mới cho việc thu thập phù hợp và xác minh thông tin nhân khẩu học và sinh trắc học của người dân. Điều này đảm bảo rằng các dữ liệu thu thập sạch từ khi bắt đầu chương trình.

16. UIDAI giới thiệu hệ thống "người giới thiệu" cho những người dân không có bất kỳ hình thức nhận dạng nào và là nơi UID sẽ là hình thức đầu tiên xác định họ có quyền truy cập. Điều này đã được cho phép bao gồm tài chính để nhiều người nghèo và người dân thiệt thòi có thể nhận được một UID. Người giới thiệu có thể là một người chịu trách nhiệm bảo lãnh dữ liệu nhân khẩu học cá nhân của người cư trú trong hệ thống UID.

17. Các dịch vụ chính cung cấp cho người dân và các nhà cung cấp dịch vụ trong các tổ chức công và tư là xác nhận Aadhaar. Mục đích xác nhận là cho phép tổ chức quản lý Aadhaar chứng minh danh tính bằng kỹ thuật số và trực tuyến, và các nhà cung cấp dịch vụ xác nhận nhận dạng của người dân trước khi cung cấp dịch vụ hoặc tiếp cận lợi ích.

18. Thông thường, một nhận dạng cá nhân được xác định theo các thuộc tính nhân khẩu học, ví dụ như tên, giới tính, tuổi và địa chỉ. Tuy nhiên, dữ liệu nhân khẩu học tự nó không thể đảm bảo tính duy nhất. Tính duy nhất của nhận dạng, tuy nhiên, có thể bằng cách liên kết các thuộc tính nhân khẩu học với các thuộc tính sinh trắc học như dấu vân tay và quét mống mắt mẫu của cá nhân. Aadhaar là một số nhận dạng được tạo ra từ 12 chữ số ngẫu nhiên duy nhất được gán cho người cư trú. Nó có liên quan đến dữ liệu nhân khẩu học và sinh trắc học cá nhân duy nhất của cư dân lưu trữ trong cơ sở dữ liệu tập trung, trung tâm lưu trữ dữ liệu tập trung (CIDR). Vì mục đích duy nhất, có một số nhận dạng với một người, và một người có một số nhận dạng duy nhất. Để đạt được điều này, hồ sơ cá nhân cư trú được điều hành thông qua một quá trình chống trùng lắp về nhân khẩu học và sinh trắc học nghiêm ngặt với 99,99% độ chính xác trước khi ấn định số nhận dạng duy nhất cho hồ sơ cá nhân cư trú.

19. Các ưu đãi trong hệ thống UID được liên kết hướng tới một cơ chế tự làm loại bỏ. Chắp vá qua nhiều cơ sở dữ liệu ở Ấn Độ đã khuyến khích các cá nhân cung cấp thông tin cá nhân khác nhau cho các cơ quan khác nhau. Kể từ khi việc chống trùng lắp trong hệ thống UID đảm bảo rằng người dân chỉ có một cơ hội để cung cấp thông tin trong cơ sở dữ liệu, cá nhân được khuyến khích cung cấp dữ liệu chính xác. Biện pháp này có thể trở nên đặc biệt khả dụng khi lợi ích và quyền lợi được liên kết với UID.

20. **Xác nhận Aadhaar**[19] là quá trình trong đó số nhận dạng duy nhất, cùng với dữ liệu nhận dạng cá nhân của chủ sở hữu (Dữ liệu nhận dạng cá nhân), được gửi đến CIDR tại UIDAI cho phù hợp, sau đó CIDR xác minh tính đúng đắn trên cơ sở phù hợp với thông tin nhận dạng chủ sở hữu của Aadhaar sẵn có. UIDAI hoặc xác nhận giấy tờ chứng minh hoặc xác nhận các thông tin được

[19] Aadhaar Operating Model - http://www.uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

cung cấp bởi cư dân. Để bảo vệ sự riêng tư của cư dân, dịch vụ xác nhận Aadhaar phản hồi chỉ với cầu trả lời "có/không"; không có dữ liệu nhận dạng cá nhân được đề cập trong các phản hồi.

21. Các dịch vụ xác nhận có sẵn cho các cư dân để chứng minh nhận dạng của mình ở bất cứ đâu, bất cứ lúc nào và bằng nhiều cách khác nhau. Một nhà cung cấp dịch vụ có thể chọn một trong hai phương thức xác nhận một yếu tố hoặc đa yếu tố. Aadhaar, tự nó, không phải là một yếu tố xác nhận. Aadhaar, cùng với các thuộc tính cá nhân (tên, địa chỉ,...) hoặc Mật khẩu dùng một lần (OTP) hoặc một/nhiều thuộc tính sinh trắc học (dấu vân tay, võng mạc,...), có thể được sử dụng để cung cấp xác nhận một yếu tố. Ngoài ra, ba thuộc tính có thể được sử dụng kết hợp cho một quá trình xác nhận đa yếu tố.

22. Dịch vụ xác nhận gồm nhiều loại[20] khác nhau tùy thuộc vào các thuộc tính sử dụng.

a. **Loại 1**: Nhân khẩu học. Loại này sử dụng các thuộc tính cá nhân (tên, địa chỉ, ngày tháng năm sinh/tuổi, giới tính, điện thoại di động, email) đơn lẻ hoặc kết hợp. Nó có thể được sử dụng định kỳ để kiểm tra tính hợp lệ của chứng chỉ, hoặc làm sạch các dịch vụ cơ sở dữ liệu của nhà cung cấp bằng cách loại bỏ trùng lặp.

b. **Loại 2**: OTP. Loại này sử dụng mật khẩu dùng một lần được chuyển giao cho một số điện thoại di động hoặc địa chỉ email theo yêu cầu của người dân hoặc của ứng dụng. Nó có thể được sử dụng để xác thực người dân trên Internet và các giao dịch điện thoại di động, cũng như trong trường hợp triển khai công nghệ sinh trắc học gặp khó khăn hoặc không thực tế.

c. **Loại 3**: sinh trắc học. Loại này sử dụng dấu vân tay và/hoặc quét võng mạc. Nó đòi hỏi người dân phải có mặt để cho phép dấu vân tay và võng mạc chụp trên một thiết bị. Loại này được sử dụng khi xác nhận sinh trắc học được coi là thiết yếu trong quá trình nhận dạng và xác thực khách hàng (KYC), giao dịch tài chính, theo dõi tại nhà,...

d. **Loại 4**: đa yếu tố. Loại này sử dụng quét sinh trắc học và OTP/điện thoại di động. Vì đây là phương thức xác nhận đa yếu tố, do đó, có sự đảm bảo hơn.

23. Các tính năng[21] của dịch vụ xác nhận Aadhaar bao gồm khớp nối dữ liệu nhân khẩu học và sinh trắc học. Nó cũng cung cấp sử dụng OTP, "có/không" phản hồi, yêu cầu chữ ký số/phản hồi, mã phản hồi, phản hồi theo thời gian, phản hồi tự kiểm chứng, mã hóa và xáo trộn.

---

[20] Aadhaar Authentication Framework - http://www.uidai.gov.in/images/authDoc/d2_authentication_framework_v1.pdf

[21] Aadhaar Enabled Service Delivery http://uidai.gov.in/images/authDoc/whitepaper_aadhaarenabledservice_delivery.pdf

24. **Cách thức xác nhận Aadhaar**. Hầu hết các hệ thống xác nhận hiện tại đều được mô tả như "địa phương" (ví dụ, các dịch vụ hợp thức hoá và/hoặc các dịch vụ liên quan theo từng tình huống) và "hủy bỏ" (trong đó có một yếu tố nhận dạng sẵn có có thể bị thu hồi và cấp lại do hết hạn sử dụng, kết hợp hay lý do chính đáng khác). Với những giao dịch huỷ bỏ như thế này, hệ thống xác nhận địa phương đi kèm với một tập hợp các điểm mạnh và hạn chế. Các hệ thống xác nhận Aadhaar, mặt khác, có thể được mô tả mang tính chất "toàn cầu" do các ứng dụng của nó thể hiện qua các tình huống, các nhà cung cấp dịch vụ và các dịch vụ. Đây cũng là đặc tính "không thể bị hủy bỏ" vì các yếu tố xác định Aadhaar, như dấu vân tay và quét võng mạc, nhìn chung không thể bị thu hồi hoặc thay thế. Toàn cầu, không thể bị hủy bỏ/hệ thống xác nhận vĩnh viễn đi kèm với thiết lập của riêng của họ về những điểm mạnh và hạn chế. Trong mô hình xác nhận, yếu tố xác nhận toàn cầu-không thể thu hồi Aadhaar cùng tồn tại và tăng cường yếu tố địa phương-hủy bỏ được thực hiện bởi các cơ quan sử dụng xác thực. Người ta cho rằng một phương pháp tiếp cận như vậy có thể tạo ra hệ thống xác nhận chính xác hơn và đáng tin cậy hơn so với những hệ thống chỉ dựa vào một trong hai mô hình toàn cầu-không thể thu hồi hoặc mô hình địa phương-hủy bỏ. Xác nhận Aadhaar đã được thiết kế với mục đích tăng cường hệ thống xác nhận của các nhà cung cấp dịch vụ, chứ không phải là một sự thay thế. Trong khi mô hình không uỷ nhiệm cho sự tồn tại hoặc sử dụng xác nhận riêng của một nhà cung cấp dịch vụ (nếu một nhà cung cấp dịch vụ mong muốn, thì có thể chỉ sử dụng xác nhận Aadhaar của chính mình), các nhà cung cấp dịch vụ được khuyến khích sử dụng xác nhận Aadhaar kết hợp với xác nhận địa phương của họ để làm cho hệ thống xác nhận tổng thể mạnh hơn và đáng tin cậy hơn. Đây được gọi là chế độ liên hoàn của xác nhận Aadhaar.

25. Aadhaar và xác định nhận dạng được sử dụng bởi các nhà cung cấp cung cấp dịch vụ chủ yếu phục vụ cho việc thiết lập hiện diện và bằng chứng chuyển giao, thông tin KYC, và như là một hệ thống thông tin người dân làm trung tâm.

26. Trong trường hợp thiết lập sự hiện diện và bằng chứng chuyển giao, xác nhận đối tượng hưởng lợi là một cách sử dụng phổ biến của dịch vụ xác nhận để đảm bảo rằng các dịch vụ được cung cấp theo quyền lợi của cá nhân. Nó hỗ trợ theo dõi trong trường hợp tiền lương/chi tiêu được liên kết với số ngày thực tế hưởng lợi như báo cáo theo chương trình. Chương trình cũng tạo điều kiện cho các giao dịch tài chính như khi một ngân hàng thẩm định một khách hàng sử dụng Aadhaar cũng như thông tin nhận dạng liên quan đến ngân hàng (số tài khoản/ID người sử dụng cùng với mật khẩu dùng một lần OTP,...) trước khi cho phép chuyển tiền hoặc rút tiền.

27. Trong trường hợp thiết lập các thông tin KYC, nhận dạng và xác minh địa chỉ là một yêu cầu quan trọng để đăng ký khách hàng mới hoặc mở một tài khoản mới cho một cá nhân. Các nhà

cung cấp dịch vụ trong tất cả các trường hợp như vậy có thể xác minh danh tính và địa chỉ sử dụng xác nhận Aadhaar. Điều này dự kiến sẽ giảm đáng kể chi phí của KYC trong việc cung cấp các dịch vụ này. Nó cũng có thể được sử dụng như chứng minh nhận dạng (POI) cho các yêu cầu liên quan đến bảo mật như nhập cảnh vào các lĩnh vực như cảng hàng không; và trong các kiểm nghiệm khác nhau (y tế hoặc học tập), nơi một số lượng lớn các mạo nhận được báo cáo mỗi năm. Việc đăng ký xác nhận trong dữ liệu nhân khẩu học và xác minh địa chỉ trong cơ sở dữ liệu cung cấp dịch vụ có thể giúp đỡ trong việc làm sạch và quản lý dữ liệu.

28. Aadhaar là một khái niệm chung để liên kết cơ sở dữ liệu liên quan. Nó cho phép thể hiện quan điểm về Nhà nước của người dân trên khắp các chương trình, ví dụ, số lượng các chương trình truy cập bởi một cư dân. Nó cung cấp một liên kết tiềm năng của Janani Suraksha Yojana (JSY), chương trình của chính phủ để giảm tỷ lệ trẻ sơ sinh và bà mẹ tử vong; Dịch vụ Tích hợp phát triển trẻ em (ICDS); và Sarva Shiksha Abhiyan (SSA), một chương trình giáo dục. Việc kết nối các dịch vụ sẽ tạo thuận lợi cho việc theo dõi sức khỏe và giáo dục cho tất cả các cơ sở dữ liệu trẻ em, chăm sóc sức khỏe và hồ sơ bệnh nhân (cấp địa phương, khu vực và quốc gia); văn phòng tín dụng sẽ có thể tận dụng các thông tin đánh giá của khách hàng; có thể là một kỹ năng về đăng ký và theo dõi các cá nhân thông qua vòng đời; và các tổ chức lớn sẽ có quan điểm về khách hàng qua dịch vụ được cung cấp bởi các ngân hàng, các công ty bảo hiểm,…

29. UIDAI đã xác định một mô hình hoạt động mở rộng với các thành phần chủ chốt, vai trò, trách nhiệm và nghĩa vụ của các thành phần này trong mô hình xác nhận Aadhaar[22]. Bất kỳ cơ quan muốn sử dụng xác nhận Aadhaar để kích hoạt dịch vụ của mình có thể đăng ký như là một Tổ chức xác nhận (AUA) và tham gia vào một thỏa thuận với UIDAI. Các AUA lần lượt có thể cần phải tham gia với một Tổ chức xác nhận dịch vụ (ASA). ASA là một cơ quan đã thiết lập kết nối đường truyền bảo mật cho CIDR ở UIDAI để truyền tải yêu cầu nhận dạng thay cho AUAs và nhận phản hồi từ CIDR. Các ASAS xây dựng và duy trì kết nối bảo mật của mình cho CIDR phù hợp với các tiêu chuẩn và thông số kỹ thuật theo quy định của UIDAI. AUA được tùy chọn tự kết nối với CIDR hoặc thông qua một ASA hiện có. Hơn nữa, một cơ quan muốn sử dụng xác nhận Aadhaar có thể chọn để trở thành một AUA hoặc nó có thể chọn để truy cập các dịch vụ xác nhận thông qua một AUA hiện có. Trong trường hợp sau, nó trở thành một tiểu AUA của AUA đã tham gia cùng.

[22] Aadhaar Xác nhận Operating model - http://www.uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

30. Thiết bị đầu cuối là các thiết bị sử dụng bởi AUAs (cả chính phủ và phi chính phủ) để cung cấp dịch vụ cho người dân. Ví dụ như các thiết bị vi ATM, máy thanh toán tiền bằng thẻ (POS), thiết bị đầu cuối của hệ thống định vị (PDS), và MGNREGA (một chương trình đảm bảo quyền hoạt động), thiết bị đầu cuối và các thiết bị bảo mật truy cập. Các thiết bị này có thể lưu trữ các ứng dụng của AUA và hỗ trợ cơ chế sinh trắc học để thu thập thông tin sinh trắc học của người dân cho mục đích xác nhận. Bất kỳ tính năng bổ sung của các thiết bị đầu cuối có thể phụ thuộc vào nhu cầu cụ thể của các dịch vụ được cung cấp bởi AUA. Các thiết bị này phải phù hợp với thông số kỹ thuật của UIDAI để bảo vệ tất cả các thông tin sinh trắc học và nhân khẩu học được cung cấp bởi các cư dân. Thiết bị đầu cuối được đăng ký với hệ thống Aadhaar để quản lý khóa mã hóa và được gọi là thiết bị đầu cuối đã đăng ký. Thiết bị đầu cuối công cộng không được đăng ký.

31. **Thông số kỹ thuật thiết bị sinh trắc học.** Các thiết bị đầu cuối được sử dụng trong xác nhận Aadhaar sinh trắc học có khả năng lưu giữ dấu vân tay và hình ảnh võng mạc của các cư dân tại thời điểm cung cấp dịch vụ. Các UIDAI đã xác định thông số kỹ thuật[23] dựa trên các tiêu chuẩn mở để dữ liệu lưu giữ được bằng cách sử dụng thiết bị sẽ đảm bảo dữ liệu có chất lượng cao và cho kết quả chính xác hơn.

32. Hệ thống sinh trăc học dựa trên dấu vân tay là yếu tố chính của việc chống trùng lắp của UIDAI và nhận dạng duy nhất của người cư trú. Dấu vân tay, công nghệ sinh trắc học lâu đời nhất, có thị phần lớn nhất trong tất cả các phương thức sinh trắc học trên toàn cầu. Ngành công nghiệp vân tay cũng có một loạt các nhà cung cấp và cơ sở của các chuyên gia có kinh nghiệm cần để thực hiện các giải pháp quản lý nhận dạng duy nhất ở quy mô mà Ấn Độ yêu cầu. Gương mặt là sinh trắc học được lưu lại phổ biến nhất, và thường xuyên được sử dụng trong kiểm tra thủ công. Tuy nhiên, xét từng yếu tố, nhận diện khuôn mặt tự động không cung cấp độ chính xác cao, và chỉ có thể được sử dụng để bổ sung cho phương thức sinh trắc học đơn giản.

33. **Thiết bị sinh trắc học chứng nhận cho ứng dụng UID.** UIDAI đã thông qua một quá trình cấp giấy chứng nhận cho các thiết bị sinh trắc học để đảm bảo phù hợp với quy định của UIDAI. UIDAI đã giao trách nhiệm thực hiện các quy trình chứng nhận để triển khai các tiêu chuẩn kiểm tra và chứng nhận chất lượng (STQC) thuộc Sở Công nghệ thông tin (DIT). Cơ quan này cung cấp dịch vụ đảm bảo chất lượng trong lĩnh vực điện tử và CNTT thông qua mạng lưới các phòng thí nghiệm và các trung tâm trên toàn quốc. Một danh sách các nhà cung cấp thiết bị sinh trắc được

---

[23] Biometric Devices Specifications for Aadhaar Xác nhận - http://stqc.gov.in/sites/upload_files/stqc/files/New%20Revision%20_May_%201%20STQC%20UIDAI%20BDCS-03-08%20UIDAI%20Biometric%20Device%20Specifications%20_Xác nhận_.pdf

chứng nhận có thể được các nhà cung cấp dịch vụ sử dụng cho nhận dạng sinh trắc học. Các nhà cung cấp muốn để có được thiết bị sinh trắc học được chứng nhận phải thực hiện theo các quy trình cấp giấy chứng nhận xác định bởi STQC được công bố trên cổng thông tin UIDAI[24].

34. **Dịch vụ nhận dạng ngón tay tốt nhất.** Dựa trên kết quả của một loạt các tổ chức phân tích bằng chứng (PoC) nghiên cứu về xác nhận sinh trắc học Aadhaar, dịch vụ này được nghiên cứu rằng một cư dân được lấy dấu vân tay để xác định nhận dạng có thể đưa ra chất lượng các dấu vân tay khác nhau trên tất cả các ngón tay. Vì vậy, độ chính xác hoặc các cơ hội khớp các dấu vân tay có thể khác nhau do những khác biệt này. Sự thay đổi này cũng có thể xảy ra vì cách thức mà các cư dân thường tương tác với một máy quét dấu vân tay điển hình, và các ngón tay khác nhau sẽ chứa lượng thông tin nhận dạng khác nhau tùy thuộc vào kích thước của ngón tay và tính phổ biến của hình dạng vân tay. Do đó, UIDAI cung cấp quy trình chứng nhận ngón tay tốt nhất (BFD) là dịch vụ web không quốc tịch được gọi là bởi ứng dụng chuyển giao dịch vụ của nhà cung cấp dịch vụ nhằm phát hiện ngón tay của cư dân có độ chính xác cao nhất và mang lại kết quả khớp lệnh thành công. Sau đó, người dân có thể sử dụng các dấu tay tốt nhất để đảm bảo tỷ lệ thành công cao trong nhận dạng sinh trắc học.

35. **Phần mềm và lập trình kỹ thuật sinh trắc học.** UIDAI đã công bố trên cổng thông tin công cộng về Bộ công cụ phát triển phần mềm (SDK) của Aadhaar và thông số kỹ thuật[25] của giao diện lập trình ứng dụng (API) nhằm cung cấp giao diện thống nhất trên nhiều phương thức (gương mặt, dấu vân tay và võng mạc) cho các nhà phát triển SDK từ các nhà cung cấp thiết bị sinh trắc học để tiếp xúc với chức năng của các phương thức khác nhau của hệ thống Aadhaar. Điều này thúc đẩy các nhà cung cấp trung lập do việc sử dụng các API tiêu chuẩn và các tiêu chuẩn mở sẽ loại bỏ các tính năng độc quyền. Nó cũng thúc đẩy khả năng tương tác bằng cách sử dụng giao diện tiêu chuẩn, định nghĩa định dạng dữ liệu phổ biến, và các giao thức trên các thành phần với chức năng tương tự. API mở cho phép các thuật toán tốt nhất sẽ được sử dụng cho các mục đích đặc biệt. API cho thấy kiểm tra chất lượng, phân khúc, trình tự, khai thác và phù hợp với chức năng khớp nối.

36. Xác nhận Aadhaar hỗ trợ sử dụng đối với nhiều yếu tố. Những yếu tố này gồm dữ liệu nhân khẩu học, dữ liệu sinh trắc học, PIN, mật khẩu dùng một lần OTP, … Việc bổ sung nhiều yếu tố sẽ tăng mức độ xác nhận phụ thuộc vào các yếu tố. Những ứng dụng xác nhận Aadhaar cần lựa chọn

---

[24] Biometric Device Certification Process - http://uidai.gov.in/biometric-devices/180.html

[25] Aadhaar Biometric SDK API Specification version 2 - http://uidai.gov.in/images/aadhaar_biometric_sdk_api_2_0.pdf

những yếu tố phù hợp theo yêu cầu. Tuy nhiên, không phải tất cả các yếu tố đều được thực hiện xem xét trong một lần.

37. UIDAI công bố trên cổng thông tin điện tử công cộng về các tiêu chí API[26] trong xác nhận Aadhaar được dùng bởi AUA và ASA để tích hợp dịch vụ xác nhận thành dịch vụ ứng dụng chuyển giao. Những tiêu chí này gồm định dạng dữ liệu API, quy định kỹ thuật, và quy định về bảo mật.

38. Dịch vụ xác nhận Aadhaar được mở rộng khi dịch vụ được tiến hành thông qua giao thức truyền siêu văn bản an toàn (HTTPS). Việc sử dụng định dạng dữ liệu mở trong ngôn ngữ đánh dấu khả mở (XML) và sử dụng rộng rãi khi HTTP cho phép thông qua và triển khai xác nhận Aadhaar.

39. Để các đại lý cung cấp dịch vụ tăng cường dịch vụ xác nhận Aadhaar trong chuyển giao dịch vụ, họ sẽ nắm bắt và lưu trữ số Aadhaar 12 chữ số (UID) với người xác nhận duy nhất (khách hàng hoặc người hưởng lợi, ...) trong hệ cơ sở dữ liệu chuyển giao dịch vụ. Quá trình mà số UID của người dân được bao gồm trong cơ sở dữ liệu chuyển giao dịch vụ của nhà cung cấp dịch vụ nhằm cho phép xác nhận dựa trên Aadhaar trong suốt quá trình chuyển giao dịch vụ được đề cập tới như việc triển khai Aadhaar[27].

40. Trong tương lai, Aadhaar có thể định dạng cơ sở, cơ sở hạ tầng nhận dạng toàn cầu mà các tổ chức đăng ký, chính phủ, và các nhà cung cấp dịch vụ khác trên khắp đất nước có thể xây dựng các ứng dụng dựa trên nhận dạng của họ. Những tính năng này, đến lượt nó, được dự kiến sẽ phục vụ cho nhiều lợi ích chuyển đổi trong phát triển và tăng trưởng công bằng thông qua nhận dạng hợp lệ. Dần dần, sẽ dẫn đến việc hướng đến mục tiêu tốt hơn bằng cách phát triển các chương trình của chính phủ và khu vực tư nhân, đảm bảo rằng tất cả các hồ sơ ảo, trùng lặp và giả mạo được đào thải ra khỏi cơ sở dữ liệu để có thể tránh được kết quả nhận dạng bị rò rỉ. Trong bối cảnh đó, những tính năng này sẽ làm tăng phạm vi và hiệu quả của việc cung cấp nhiều hàng hóa và dịch vụ như PDS, tài chính ngân hàng, viễn thông, y tế, bảo hiểm, giáo dục,... và không cần kiểm tra KYC về cư trú. Quá trình triển khai, tuy nhiên, nhất thiết phải được tiến hành trước bởi việc số hóa và tập trung hoá dữ liệu.

---

[26] Aadhaar Authentication API Specifications - http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf

[27] Aadhaar seeding - http://uidai.gov.in/images/aadhaar_seeding_v_10_280312.pdf

41. Số hoá dữ liệu nghĩa là thu thập dịch vụ chuyển giao dữ liệu theo định dạng điện tử (cơ sở dữ liệu/Excel hoặc những định dạng tương tự) từ nơi nhận được dữ liệu theo yêu cầu của ngôn ngữ truy vấn theo cấu trúc (SQL) chuẩn. Công việc này quan trọng do dữ liệu nhận dạng cá nhân từ từ trở nên cố định thông qua đa hệ thống. Aadhaar cũng là kênh thông tin nhận dạng cá nhân chuẩn hoá đầu tiên và dữ liệu Aadhaar có thể được sử dụng để làm sạch những dữ liệu đã có.

42. Tập trung hoá dữ liệu là quản lý dịch vụ chuyển giao và tiếp cận dữ liệu sẵn có. Mục tiêu của quá trình triển khai/tiện ích để có thể truy cập dịch vụ chuyển giao dữ liệu và tất cả các thông tin liên quan ít nhất để ở chế độ chỉ cho phép đọc (read-only). Ví dụ, trong dữ liệu quản lý chế độ hưu trí có thể sẵn có trong kho dữ liệu giữa các khu vực. Quan điểm thống nhất của toàn bộ dữ liệu có thể tạo điều kiện cho bộ phận phúc lợi xã hội của nhà nước để cải thiện cung cấp dịch vụ trong các chương trình của mình, trong khi cũng có thể để đảm bảo rằng cùng một người không được hưởng lợi ích gấp đôi từ hai khu vực khác nhau. Trong trường hợp cung cấp dịch vụ dữ liệu đã được số hóa và tập trung hoá, không có hành động được yêu cầu từ khía cạnh triển khai.

43. Có hai cách triển khai dịch vụ chuyển giao dữ liệu theo Aadhaar: cách thức từ trên xuống và cách thức hữu cơ. Cách thức sử dụng dữ liệu sẵn có trong nhận dạng và xác thực cư dân (KYR+) và hồ sơ nhận dạng điện tử/UID như nguồn thông tin đầu vào trong khi sau đó yêu cầu nhà cung cấp dịch vụ liên hệ với cư dân, hoặc ngược lại, cho mục đích cập nhật thông tin cá nhân thông qua quá trình được quyết định bởi nhà cung cấp dịch vụ. Việc hoàn tất thủ tục triển khai được theo dõi bởi tổ chức xác nhận nhân khẩu học/sinh trắc học, đặc biệt không có dịch vụ cơ sở dữ liệu nào được cập nhật trực tiếp.

44. Một số thử thách thường phải đối mặt trong suốt quá trình triển khai và tìm hiểu về những trở ngại gây ra bởi việc triển khai sớm trong quá trình lên kế hoạch. Những trở ngại thường thấy như: việc hoàn tất dữ liệu không được lưu trong dịch vụ chuyển giao cơ sở dữ liệu, những thông tin tương tự thông qua các nguồn dữ liệu khác nhau không hoàn toàn khớp nhau; dữ liệu trong dịch vụ chuyển giao dữ liệu theo ngôn ngữ địa phương, tất cả dữ liệu được yêu cầu không sẵn có; và những công cụ quy định không xử lý được dữ liệu có dung lượng lớn.

45. Quá trình triển khai thường liên quan đến chiết xuất dữ liệu, kết hợp và khớp nối dữ liệu. Với những hoạt động thực thi, UIDAI đã phát triển một công cụ trong nhà có thể được sử dụng bởi các nhà cung cấp dịch vụ sau khi ký hợp đồng thống nhất rằng công cụ đó không được sử dụng với mục đích khác ngoài mục đích dự kiến ban đầu.

46. **Khuôn khổ triển khai điều chỉnh Aadhaar.** UIDAI thiết kế và triển khai lĩnh vực trọng tâm chủ trì bởi UIDAI, với tên gọi Khuông khổ triển khai điều chỉnh Aadhaar[28] (RASF) với mục tiêu khởi động nỗ lực triển khai để thông qua dịch vụ chuyển giao Aadhaar sớm hơn. Nhà cung cấp dịch vụ có thể cung cấp lĩnh vực trọng tâm nhằm triển khai dịch vụ chuyển giao cơ sở dữ liệu bằng cách yêu cầu triển khai bổ sung và hợp thức hoá dữ liệu; hoạt động này được thực hiện bởi người dùng có thẩm quyền từ nhà cung cấp dịch vụ.

47. Nhà cung cấp dịch vụ của Chính phủ và khu vực tư nhân như nhà cung cấp trong lĩnh vực ngân hàng[29], bảo hiểm[30], thị trường vốn[31], viễn thông[32], LPG[33], và đướng sắt [34] đã cập nhật tiêu chuẩn KYC của họ bao gồm Aadhaar là chứng chỉ KYC hợp lệ.

48. For stakeholders wishing to leverage the Aadhaar Identity solution in their service delivery applications, the UIDAI has created a support group and a set of artifacts. The support structure includes an applications group at the UIDAI, and empanelled consultants and software vendors to help service providers build necessary processes and applications. Further, there are detailed support documents for guidance on leveraging and integrating the Aadhaar solution such as:

a. Ứng dụng đang triển khai và sẵn sàng cho các nhà cung cấp cung cấp dịch vụ.
b. Khuôn khổ xác nhận, mô hình hoạt động và hướng dẫn.
c. Tiêu chí, danh mục kiểm tra và hoạt động mẫu để trở thành một AUA hoặc ASA.
d. Giải pháp triển khai Aadhaar cho dịch vụ chuyển giao cơ sở dữ liệu cung cấp dịch vụ để ứng dụng vào số Aadhaar.

49. UIDAI đã xác định quá trình đăng ký cho việc lựa chọn thành phần tham gia chủ chốt (ASA, AUA, nhóm AUA,…) trong việc cung cấp các dịch vụ xác nhận cho chính phủ và các tổ chức tư nhân. Quá trình này đơn giản đủ để các tổ chức áp dụng, nhưng đồng thời, nó bao gồm việc kiểm tra và cân bằng cần thiết để đảm bảo rằng các cơ quan được lựa chọn cho vai trò này có khả năng cung cấp các dịch vụ chuyển giao. UIDAI xác định rõ quá trình từng bước trong việc áp dụng cho vị trí này và cung cấp các tài liệu hỗ trợ áp dụng cho từng thành phần tham gia.

---

[28] Remote Aadhaar Seeding Framework - http://uidai.gov.in/images/uidai_rasf_v06_27022013.pdf

[29] http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7367

[30] http://www.irda.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo1322&flag=1

[31] http://www.sebi.gov.in/cms/sebi_data/attachdocs/1344851126270.pdf

[32] http://www.dot.gov.in/as/2011/as_14.01.2011.pdf

[33] http://uidai.gov.in/images/FrontPageUpdates/aadhaar_news_release_28_june.pdf

[34] http://www.indianrail.gov.in/id_proof.doc

50. **Nâng cao nhận thức kỹ thuật và áp dụng.** UIDAI đã thiết lập một cổng thông tin công cộng[35] để xây dựng nhận thức về kỹ thuật và cung cấp hỗ trợ kỹ thuật cho các cơ quan sử dụng trong cả hai khu vực công và tư nhân. UIDAI công bố tài liệu kỹ thuật trên cổng thông tin một cách thường xuyên nhắm vào các chuyên gia phần mềm làm việc trong lĩnh vực công nghệ và quan tâm đến việc kết hợp xác nhận Aadhaar vào các ứng dụng của họ.

51. **Dịch vụ nhận dạng và xác thực khách hàng điện tử eKYC.** Tổng cục nhận dạng duy nhất Ấn Độ UIDAI đã triển khai dịch vụ eKYC thông qua đó các nhà cung cấp dịch vụ có thể thực hiện quá trình eKYC với sự chấp nhận của người cư trú. Trong quá trình eKYC, người dân ủy quyền cho UIDAI qua xác nhận Aadhaar bằng cách sử dụng dữ liệu sinh trắc học hoặc mật khẩu dùng một lần OTP để cung cấp dữ liệu nhân khẩu học của họ, cùng với bức ảnh họ đã được mã hóa và chữ ký số, tới các nhà cung cấp dịch vụ. Điều này giúp các nhà cung cấp dịch vụ thực hiện eKYC không cần giấy tờ về cư dân trong thời gian thực như một phần của quá trình cung cấp dịch vụ của họ bằng cách sử dụng chức năng eKYC. Điều này có thể cho phép các nhà cung cấp dịch vụ thực hiện cung cấp dịch vụ ngay lập tức cho người dân, nếu không sẽ mất vài ngày để kích hoạt chờ xác minh các tài liệu eKYC, số hóa, … Ngoài ra loại bỏ được chi phí lặp KYC, xử lý và lưu trữ giấy tờ, và nguy cơ giả mạo tài liệu POI và PoA.

52. **Cầu thanh toán bằng Aadhaar (Aadhaar là một địa chỉ thanh toán).** UIDAI thực hiện cầu thanh toán bằng Aadhaar (APB) sử dụng thanh toán Aadhaar trên cơ sở: một hệ thống chuyển tiền tới mọi công dân trên cơ sở số Aadhaar. Hệ thống này tạo điều kiện chuyển liền mạch cho tất cả các thanh toán chương trình phúc lợi tới Tài khoản ngân hàng truy cập bằng Aadhaar (AEBA) của người hưởng lợi. Tại thời điểm Aashaar mở cửa đăng ký, người dân cung cấp chi tiết tài khoản ngân hàng hiện có của họ hoặc yêu cầu mở một tài khoản mới có thể được gắn vào số Aadhaar của họ cho tất cả các khoản thanh toán chương trình phúc lợi. APB duy trì một kho lưu trữ các số Aadhaar cư dân với số tài khoản ngân hàng chính tương ứng được sử dụng để nhận được khoản thanh toán an ninh và quyền lợi xã hội của các cơ quan chính phủ khác nhau. APB sử dụng số Aadhaar bắt buộc như là từ khóa chính cho tất cả các thanh toán. Điều này có thể loại bỏ xác nhận giả và ảo từ hệ thống và đảm bảo rằng lợi ích đến được với những người hưởng lợi dự kiến.

53. Giải pháp UIDAI về tài chính sử dụng sự kết hợp của Aadhaar như một địa chỉ thanh toán và eKYC để tạo tài khoản ngay lập tức với các cơ sở hạ tầng thanh toán Aadhaar. Các quỹ có thể tiếp cận với cư dân thông qua số Aadhaar, dù cho họ có tài khoản ngân hàng hay không. Nếu họ

---

[35] UIDAI public facing portal – http://uidai.gov.in/

có tài khoản ngân hàng truy cập bằng Aadhaar (AEBA), tiền có thể được chuyển vào đó. Nếu họ không có, một tài khoản ngay lập tức có thể được tạo ra trên cơ sở số Aadhaar với một khoản ghi nợ được đóng băng. Số tiền này được chuyển giao và ghi có vào tài khoản vừa lập sẽ được kích hoạt trong lần rút tiền đầu tiên trên cơ sở chức năng eKYC.

II. Ét-xtô-nia

1. Ét-xtô-nia là một trong những nước phát triển về điện tử triển trên thế giới. Câu chuyện thành công đáng kinh ngạc xuất phát từ mối quan hệ giữa một chính phủ có tầm nhìn xa, một lĩnh vực CNTT chủ động, và một dân số nhanh nhạy, am hiểu công nghệ. 78% dân số trong độ tuổi từ 16-74 sử dụng Internet[36] (theo số liệu của Ét-xtô-nia). 71% các hộ gia đình có khả năng kết nối Internet (theo số liệu của Ét-xtô-nia năm 2011) và tất cả các trường học ở Ét-xtô-nia được kết nối Internet.

2. Ét-xtô-nia không có hồ sơ nhận dạng cá nhân cấp quốc gia - cả hồ sơ giấy và hồ sơ điện tử. Do đó, Ét-xtô-nia triển khai hệ thống định danh điện tử để nhận dạng cư dân của mình và cư dân bên ngoài có mặt trong lãnh thổ bằng cách sử dụng thẻ ID như giấy tờ nhận dạng.

3. Thẻ ID có hai chức năng chính. Một là hình thức nhận dạng theo nhận dạng cơ thể - được sử dụng như một ID thường xuyên trong các tình huống thông thường, bất cứ nơi nào thường phải chứng minh danh tính, tuổi tác... Chức năng thứ hai là để định danh điện tử - nó cho phép người dân sử dụng thẻ này để xác thực điện tử đến các trang web và mạng lưới, và/hoặc để ký chữ ký điện tử trong thông tin liên lạc và giao dịch theo yêu cầu.

4. CMND điện tử đầu tiên được phát hành năm 2002; đã được phát hành cho 130.000 cư dân trong năm đầu tiên[37]. Tính đến tháng 1 năm 2012, hơn 1,1 triệu người ở Ét-xtô-nia (gần 90% dân số) đã có thẻ ID[38]. Thẻ ID Ét-xtô-nia được sử dụng để cung cấp dịch vụ nhận dạng phụ và nó là giấy tờ nhận dạng bắt buộc của người dân từ 15 tuổi trở lên. Thẻ có thể được sử dụng cho các văn bản có chữ ký điện tử, để nhận dạng cá nhân, và phục vụ chức năng mã hóa dữ liệu. Thẻ có hai chứng chỉ ở định dạng X.509 v3 và hai từ khoá liên quan được bảo vệ bởi mã PIN được lưu trên thẻ ID: (a) chứng nhận định danh điện tử cá nhân, ký và mã hóa dữ liệu; và (b) chứng nhận chữ ký điện tử, cho phép chủ thẻ phát hành chữ ký điện tử. Trên thẻ ID ban hành sau ngày

---

[36] Who, where and why uses the Internet - http://www.stat.ee/dokumendid/68627

[37] eID in action: Estonia - http://ec.europa.eu/idabc/en/document/4487/5584.html

[38] e-Estonia - http://Estonia.eu/about-Estonia/economy-a-it/e-Estonia.html

01/01/2007, giấy chứng nhận có giá trị cho đến khi hết hạn ghi trên thẻ, nghĩa là, năm năm; và không có nhu cầu gia hạn giấy chứng nhận[39] Thẻ mang các tập tin điện tử cá nhân có chứa thông tin cá nhân của người dân[40]. Đây là một thẻ thông minh và phù hợp với tiêu chuẩn ISO / IEC 7816. Thẻ ID được tạo ra với chức năng vừa là một ID vật lý và một ID điện tử và có thể có giá trị lên đến mười năm. Trong trường hợp khẩn cấp (ví dụ, mất thẻ), giấy chứng nhận có thể bị đình chỉ, nếu cần - vô hiệu hóa khả năng sử dụng thẻ cho các xác nhận và giao dịch điện tử.

5. Chứng nhận điện tử được phát hành cùng với chương trình về thẻ ID và đã được chứng nhận theo chỉ thị về chữ ký số của Châu Âu số 1999/93/EC[41].

6. Ngoài việc nhận dạng vật lý để cung cấp dịch vụ, các dịch vụ định danh điện tử chính được chuyển giao gồm chữ ký điện tử (ký trên các văn bản điện tử), nhận dạng (định danh điện tử của người dân), và mã hóa tài liệu. Chúng được sử dụng bởi các nhà cung cấp dịch vụ trong chính phủ và khu vực tư nhân như các dịch vụ phụ trợ phổ biến cho phép cung cấp dịch vụ.

7. Các dịch vụ định danh điện tử cá nhân xác nhận cư dân điện tử tại thời điểm chuyển giao dịch vụ điện tử sử dụng giấy chứng nhận nhận dạng cá nhân trên hồ sơ nhận dạng điện tử. Chứng nhận nhận dạng cá nhân có chứa các thông tin về người cư trú và người cư trú có thể chứng minh bản thân bằng cách nhập mã PIN. Máy tính để bàn và các ứng dụng web sử dụng thông tin này để xác định người sử dụng tại thời điểm cung cấp dịch vụ

8. Chữ ký điện tử cho phép người dân ký trên các văn bản điện tử bằng cách sử dụng chứng nhận chữ ký và một cặp từ khoá trên văn bản điện tử (thẻ ID hoặc điện thoại di động) ngoài chứng nhận nhận dạng. Luật Chữ ký điện tử của Ét-xtô-nia (DSA)[42] được thông qua vào năm 2000 đảm bảo rằng chữ ký điện tử của người cư trú được đưa ra với cặp từ khóa ký trên CMND điện tử với giấy chứng nhận hợp lệ có tính ràng buộc pháp lý và có giá trị như một chữ ký tay. Ét-xtô-nia là một trong số ít các nước châu Âu, nơi các chức năng chữ ký điện tử không phải là tùy chọn.

9. Giấy chứng nhận có tên và số ID cá nhân của chủ thẻ, giấy chứng nhận nhận dạng cũng chứa một địa chỉ thư điện tử chính thức duy nhất cho mỗi chủ thẻ. Ét-xtô-nia cung cấp một địa

---

[39] http://www.id.ee/index.php?id=31015

[40] Personal Data File on the card - https://eid.eesti.ee/index.php/General_information_for_developers#Using_the_personal_data_file

[41] European Digital Signature Directives 1999/93/EC - http://www.columbia.edu/~mr2651/ecommerce3/2nd/statutes/ElectronicSignaturesDirective.pdf

[42] Estonia Digital Signatures Act (DSA - 2000) - http://www.legaltext.ee/text/en/X30081K4.htm

chỉ email chính thức đến từng người dân. Địa chỉ email được sử dụng cho liên lạc chính thức của chính phủ, nhưng nó cũng có thể được sử dụng cho liên lạc riêng tư. Địa chỉ email của một công dân có định dạng "firstname.lastname_NNNN@eesti.ee", trong đó NNNN đại diện cho bốn chữ số ngẫu nhiên. Mỗi chủ thẻ cũng có thể nhận email tại địa chỉ "ID_CODE@eesti.ee" với ID_CODE đại diện cho số ID cá nhân của công dân. Ét-xtô-nia không cung cấp dịch vụ thư điện tử cho công dân của mình; thay vào đó, địa chỉ email hoạt động như bước chuyển tiếp, và công dân chỉ định một tài khoản email để nhận tin nhắn. Tất cả các địa chỉ email được niêm yết công khai trên hệ thống chứng nhận về đăng ký dịch vụ quốc gia của các nhà cung cấp dịch vụ Ét-xtô-nia.

10. Chính phủ triển khai thực hiện cơ sở hạ tầng xác nhận đáng tin cậy tại Ét-xtô-nia, nhận được sự chấp nhận cao của công dân và các doanh nghiệp, do đó trở thành một thành công về mặt hiệu quả và thể hiện hiệu quả sử dụng trong cuộc sống hàng ngày.

11. Cơ sở hạ tầng định danh điện tử là một lĩnh vực rất nhạy cảm trong quản lý hành chính của Ét-xtô-nia, nó đã được thiết kế để có độ tin cậy cao và cung cấp hỗ trợ kỹ thuật toàn thời gian. Các giải pháp kỹ thuật được dựa trên công nghệ đã được chứng minh cung cấp bởi phần mềm và các nhà cung cấp trong nước. Giải pháp là khả năng mở rộng, linh hoạt và dựa trên tiêu chuẩn cho việc cho phép mở rộng ra các dịch vụ khác cũng như hướng đến có thể sử dụng qua biên giới.

12. Con dấu kỹ thuật số là một dịch vụ cho phép các tổ chức pháp lý (ví dụ, các công ty) ký trên các văn bản kỹ thuật số. Nó có giá trị tương đương với thẻ ID cho các công ty. Điều này khẳng định rằng tài liệu đó là do công ty đã ký và các tài liệu này không được thay đổi trong thời gian tạm thời. Chữ ký (với số lượng lớn) có thể được gắn vào hoá đơn, đơn đặt hàng thanh toán, xác nhận, chứng chỉ, sao kê của ngân hàng (ví dụ, ngân hàng SEB cung cấp một sao kê có con dấu điện tử tự động)... Công ty được cấp một mật USB có giấy chứng nhận X.509 và, tương tự như chữ ký số, khi con dấu được sử dụng, một tài liệu chứa theo định dạng DigiDOC có thể được tạo ra có chứa các dữ liệu được ký.

13. Các tài liệu định danh điện tử cung cấp các chức năng để mã hóa và giải mã hồ sơ điện tử sử dụng giấy chứng nhận nhận dạng. Chức năng này chủ yếu dành cho việc vận chuyển an toàn các tập tin trong một môi trường không an toàn (ví dụ như Internet), trái ngược với lưu trữ dữ liệu dài hạn.

14. Tại Ét-xtô-nia, việc sử dụng định danh điện tử được quy định bởi DSA120 và Luật về tài liệu nhận dạng[43], trên cơ sở đó các thẻ ID Ét-xtô-nia được ban hành. Ét-xtô-nia đưa ra chương trình thẻ căn cước điện tử vào tháng Hai năm 1999 khi Quốc hội Ét-xtô-nia thông qua Luật Tài liệu nhận dạng. Luật có hiệu lực từ ngày 01/01/2000, và thiết lập các hướng dẫn quốc gia về việc tạo ra một chứng minh thư quốc gia bắt buộc đối với các công dân của Ét-xtô-nia và người nước ngoài thường trú từ 15 tuổi trở lên. Trước đó, Ét-xtô-nia không có một tài liệu nhận dạng cá nhân quốc gia nào.

15. Luật Tài liệu nhận dạng cũng khẳng định rằng các dữ liệu nhân khẩu học và sinh trắc học của cư dân không bị trùng lặp và được sử dụng cá nhân hoá thẻ định danh điện tử cho các cá nhân cũng được nhập vào hệ thống đăng ký quốc gia theo quy định của Luật Đăng ký Dân số[44].

16. Các quy định cụ thể liên quan đến chữ ký số, DSA, đã được thông qua một cách riêng biệt bởi Quốc hội Ét-xtô-nia (Riigikogu) vào ngày 08/3/2000, và có hiệu lực vào ngày 15/12/2000. Luật này quy định khuôn khổ và quy định cần thiết để quản lý hiệu quả cơ sở hạ tầng mã khóa công khai (PKI) và cơ sở hạ tầng chữ ký số. Mục tiêu chính của DSA là để cho chữ ký điện tử có một mức độ tin cậy và đảm bảo như chữ ký tay. Theo quy định chữ ký tay và chữ ký điện tử có giá trị tương đương ở cả hai khu vực công và tư nhân. DSA cũng khẳng định rằng bộ phận dịch vụ công cộng phải chấp nhận các tài liệu bằng chữ ký số. DSA yêu cầu mỗi chữ ký số được nhận dạng duy nhất dùng trong ký kết, ràng buộc các cá nhân với các dữ liệu đã ký kết, và đảm bảo rằng các dữ liệu được ký không thể giả mạo mà không cần hủy bỏ hiệu lực hồi tố chữ ký riêng của mình.

17. **Quy tắc và quy định đối với các nhà cung cấp dịch vụ chứng nhận.** Một trong những thành phần cốt lõi của DSA là việc thành lập các quy tắc và các quy định liên quan đến các nhà cung cấp Giấy chứng nhận Dịch vụ (CSP) nơi ban hành giấy chứng nhận kỹ thuật số cho người dùng và quản lý dịch vụ bảo mật liên quan. DSA đưa ra một số yêu cầu về tài chính và thủ tục nghiêm ngặt để đảm bảo rằng các CSP được thành lập và quản lý đúng cách để thực hiện chức năng của mình với các tiêu chuẩn cao nhất có thể.

18. **Quy tắc và quy định đối với các nhà cung cấp dịch vụ con dấu điện tử.** DSA cũng quy định các dịch vụ cung cấp con dấu số được cung cấp bởi Các nhà cung cấp dịch vụ con dấu điện tử (TSP). TSP cũng phải tuân theo luật và những quy định như CPS. Con dấu số đơn giản là một mảnh thông tin một mẩu thông tin minh chứng cho sự xuất hiện của một sự kiện tại một thời điểm

---

[43] Estonia Identity Documents Act (1999) – http://www.legislationline.org/documents/id/5718

[44] Estonia Population Register Act (2000) – http://www.legaltext.ee/text/en/X40051K5.htm

cụ thể. DSA không định nghĩa con dấu số một cách chi tiết, nhưng nó đảm bảo rằng dữ liệu của con dấu là không thể giả mạo hoặc sửa đổi mà không cần vô hiệu hoá con dấu.

19. **Luật Bảo vệ dữ liệu cá nhân.** Luật Bảo vệ dữ liệu cá nhân quy định việc sử dụng các dữ liệu cá nhân và cơ sở dữ liệu chứa dữ liệu cá nhân của các tổ chức công và tư. Cơ quan Điều tra Bảo vệ dữ liệu là cơ quan chính phủ giám sát việc đáp ứng các yêu cầu và tuân thủ khi thực thi, nếu cần thiết. Chiến lược bảo vệ dữ liệu và thẻ ID tại Ét-xtô-nia là thẻ chứa dữ liệu cá nhân càng ít càng tốt. Thay vào đó, dữ liệu có thể được lưu giữ trong cơ sở dữ liệu tại cơ quan có liên quan, và một người có thể sử dụng thẻ như là cơ sở dữ liệu chính (phương pháp uỷ quyền) để truy cập dữ liệu của mình trong cơ sở dữ liệu. Yêu cầu của các bên thứ ba (ví dụ, đại diện chính quyền) đối với dữ liệu cá nhân đã đăng nhập và các bản ghi có sẵn trực tuyến cho các cá nhân theo yêu cầu (thông qua cổng thông tin của công dân).

20. **Chứng nhận nhận dạng kỹ thuật số.** Thường được gọi là Digi-ID, đây là một tài liệu kỹ thuật số để nhận dạng cá nhân trong một môi trường điện tử và để phát hành một chữ ký điện tử. Không giống như thẻ ID, Digi-ID không được thiết kế để nhạn diện cá nhân trực quan; do đó, nó không kèm theo ảnh - chỉ gồm tên, mã số cá nhân và ngày hết hiệu lực. Ngoài ra, các tập tin dữ liệu cá nhân sẽ để trống trên thẻ Digi-ID, trừ trường số tài liệu. Mã hóa, là một thẻ thông minh tương tự như chứng minh nhân dân. Trong khi việc phát hành thẻ ID có thể mất đến một tháng, thẻ Digi-ID được phát hành trong vòng vài phút từ các điểm dịch vụ của Cục bảo vệ Công an và Bộ đội biên phòng.

21. **Thẻ cư trú điện tử.** Cấp cho người nước ngoài cư trú tại Ét-xtô-nia không phải là công dân của Liên minh châu Âu, thẻ cư trú điện tử mang dữ liệu của giấy phép cư trú. Trong điều khoản của dịch vụ điện tử sẵn có, các chức năng của thẻ cư trú và chứng minh nhân dân là như nhau. Sự khác biệt chính là CMND được cấp cho công dân của Ét-xtô-nia và EU có thể được sử dụng như một tài liệu du lịch tại EU, trong khi thẻ cư trú không thể được sử dụng để đi du lịch bên ngoài Ét-xtô-nia. Một khác biệt nữa là các thẻ cư trú cũng mang một con chip không tiếp xúc với dấu vân tay và hình ảnh khuôn mặt của người dùng.

22. **Định danh điện tử qua điện thoại di động.** Điện thoại di động thâm nhập thị trường Ét-xtô-nia với tỷ lệ hơn 100%, chính phủ giới thiệu dịch vụ định danh điện tử qua điện thoại di động và chữ ký số nhằm thúc đẩy việc thông qua định danh điện tử để truy cập dịch vụ điện tử. ID điện thoại di động là một tài liệu điện tử nhận dạng cá nhân mà có thể được sử dụng để nhận dạng cá nhân điện tử và chữ ký điện tử với một điện thoại di động, nơi mà các điện thoại di động với các chức năng của SIM cùng lúc được sử dụng là thẻ ID và đầu đọc thẻ. Để sử dụng một ID điện thoại

di động, một SIM chuyên dụng là cần thiết để kích hoạt dịch vụ. Nó có thể thu được bằng cách ký một hợp đồng dịch vụ với một nhà điều hành điện thoại di động. ID điện thoại di động có thể trở thành có thể sử dụng sau khi đã được kích hoạt trong môi trường ứng dụng điện tử của Ban bảo vệ của Công an và Bộ đội biên phòng, nơi mà các chứng chỉ cần thiết được yêu cầu. Không giống như các văn bản khác, chứng nhận ID điện thoại di động sẽ không được lưu trên SIM. Không giống như thẻ ID, ID điện thoại di động không được sử dụng để mã hóa tài liệu - nếu không, các nhà điều hành điện thoại di động và dịch vụ DigiDoc có thể xem được dữ liệu đã giải mã.

23. ID điện thoại di động được phát hành bởi các nhà mạng điện thoại di động của Ét-xtô-nia như Elisa, EMT[45], Tele2 tại các cửa hàng tại địa phương. Cư dân tiếp cận nhà mạng di động để cấp ID điện thoại di động tại các cửa hàng địa phương gần nhất. Cư dân xuất trình thẻ ID của họ có giấy chứng nhận hợp lệ để nhận được ID điện thoại di động. Một cư dân đã ký hợp đồng (hợp đồng thuê bao ID điện thoại di động[46]) với các nhà điều hành điện thoại di động để có được ID điện thoại di động. Chính phủ đã giao trách nhiệm phát hành ID điện thoại di động cho các nhà khai thác điện thoại di động trên toàn quốc.

24. **Chứng nhận kích hoạt ID điện thoại di động.** Các cư dân phải kích hoạt dịch vụ trên điện thoại của họ cùng với SIM chuyên dụng. Để kích hoạt dịch vụ ID điện thoại di động hoặc xin cấp chứng chỉ, các cư dân phải truy cập trang web của Cục bảo vệ Công an và Bộ đội biên phòng[47] và nộp đơn xin cấp giấy chứng nhận mới. Để có được giấy chứng nhận cho ID điện thoại di động, cư dân phải điền vào một mẫu đơn trực tuyến trên trang web của cảnh sát và nhập vào thẻ vào đầu đọc thẻ và làm theo hướng dẫn.

25. Các nhà điều hành điện thoại di động tính cước cho dịch vụ ID điện thoại di động. Các chi phí bao gồm lệ phí đăng ký một lần và lệ phí hàng tháng. Nếu ID điện thoại di động được sử dụng bên ngoài của Ét-xtô-nia, mỗi giao dịch ID điện thoại di động được tính vào chi phí của việc gửi một tin nhắn văn bản theo danh sách giá của gói.

26. Chính phủ thực hiện 4 quy trình hoạt động để triển khai định danh điện tử bằng điện thoại di động. Gồm:

---

[45] EMT website - https://www.emt.ee/en/mugavusteenused/mobiil-ID#open-4077133-tab-5

[46] Mobile ID Subscription agreement - https://www.emt.ee/en/era-arve

[47] Police Web Site for activation of the Mobile ID - http://www.politsei.ee

a. **Quy định về SIM.** Cư dân có thể đến bất kỳ nhà cung cấp dịch vụ cung cấp dịch vụ ID điện thoại di động để đăng ký số SIM mới. Các nhà cung cấp dịch vụ chuyển tiếp các ứng dụng cho Nhà điều hành mạng di động (MNO) và thông báo cho cư dân địa phương đến nhận SIM. Các MNO xác định người dùng thông qua thẻ ID và trên cơ sở xác nhận thành công, sẽ chuyển thẻ SIM đến tay người dân, hoặc cài đặt phần mềm vào SIM của công dân nếu cần. Là một phần của quá trình xác nhận, SIM được gắn vào một thiết bị bảo mật tạo chữ ký duy nhất (SSCD) cho mỗi một cư dân; các SSCD có thể sau đó được sử dụng để cấp giấy chứng nhận đủ điều kiện. Giấy chứng nhận SSCD được khai báo đã kích hoạt cho một SIM cụ thể và được thực hiện có sẵn cho tất cả các TSP. MNO cung cấp một mã số duy nhất cho các cư dân để kích hoạt giấy chứng nhận đủ điều kiện.

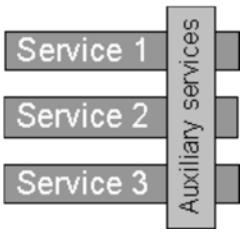
b. **Kích hoạt chứng nhận/đăng ký cho người sử dụng.** Mục đích của quá trình kích hoạt chứng nhận là tạo mới và kích hoạt chứng nhận đủ điều kiện. Người sử dụng yêu cầu kích hoạt chứng nhận đủ điều kiện của họ bằng cách sử dụng điện thoại di động có SIM mới. Cơ quan quản lý đăng ký (RA) yêu cầu xác nhận tới điện thoại di động của người sử dụng để nhận thông tin cá nhân. Người sử dụng sẽ xác nhận thông tin và báo lại bằng cách nhập mã kích hoạt xác nhận thiết bị của mình. Cơ quan quản lý đăng ký sẽ nhận những thông tin đã được người dùng xác nhận đó và nhập thông tin bổ sung gồm chứng nhận thiết bị và chuyển yêu cầu kích hoạt chứng nhận tới cơ quan xác nhận có thẩm quyền. CA sẽ tạo mới và kích hoạt chứng nhận đủ điều kiện để công bố.

c. **Sử dụng.** Nhà cung cấp dịch vụ yêu cầu dịch vụ nhận dạng từ TSP và sử dụng Hệ thống thông tin di động toàn cầu (GSM) để nắm số lượng và/hoặc mã nhận dạng cá nhân. TSP phân loại yêu cầu và gửi tới điện thoại di động của người sử dụng. Người sử dụng xác nhận yêu cầu bằng cách nhập mã PIN. TSP nhận dữ liệu do người sử dụng cung cấp và kiểm tra hiệu lực của mã và của chứng nhận. Nhà cung cấp dịch vụ sẽ nhận dịch vụ liên quan đến nhận dạng từ TSP.

d. **Huỷ bỏ.** Người sử dụng có thể ngừng sử dụng ID di động vì một số lý do như: Người sử dụng không sử dụng được dịch vụ, mất SSCD, chứng nhận hết hạn, hoặc người sử dụng vi phạm hợp đồng giữa họ với CA. Trong trường hợp thu hồi chứng chỉ, RA thông báo cho CA chứng nhận thu hồi, CA ngay lập tức thu hồi giấy chứng nhận, và danh mục huỷ chứng nhận (CRL) sẽ được cập nhật. Trong trường hợp SIM bị chặn do mất mát, thiệt hại, giấy chứng nhận thiết bị được đưa ra khỏi danh sách các SSCD hợp lệ có sẵn cho tất cả các TSP.

27. **Sự tương kết.** Những dịch vụ phụ trợ được thiết kế để đảm bảo có thể phù hợp với những dịch vụ đã có sẵn và hệ thống chuyển giao dịch vụ chính trong kế hoạch của nhà cung cấp dịch vụ tại Ét-xtô-nia để kích hoạt các tính năng chữ ký số, định danh điện tử và mã hoá dữ liệu. Yêu cầu về sự tương kết được đáp ứng bởi:

a. **Sử dụng tiến độ chuẩn.** Tiến độ công việc chuẩn được tạo ra bằng việc thông qua ứng dụng thể thức văn bản chung đối với từng nhà cung cấp dịch vụ độc lập (DigiDoc) và nguồn cung cấp dịch vụ công cộng trung tâm có thể kết nối với cơ sở dữ liệu quốc gia.



b. **Chủ yếu cung cấp số nhận dạng duy nhất cho người dân Ét-xtô-nia.** Cơ sở dữ liệu trung tâm số nhận dạng duy nhất phân bổ cho người dân Ét-xtô-nia được thiết lập nhằm cung cấp xác nhận cho chủ sở hữu thẻ (như, ứng dụng chữ ký). Cơ sở hạ tầng trung tâm quốc gia, số nhận dạng duy nhất cho từng người dân Ét-xtô-nia được sử dụng để phục vụ việc xác nhận điện tử.

c. **Nguồn cung cấp dịch vụ công cộng trung tâm để kết nối với cơ sở dữ liệu quốc gia.** Để nhận dạng và xác nhận nhiều dịch vụ khác nhau thông qua cơ sở hạ tầng hợp nhất, nguồn cung cấp dịch vụ công cộng trung tâm được gọi là X-Road đã được tạo ra. Dựa vào Internet, X-Road kết nối cơ sở dữ liệu công cộng và hệ thống thông tin, những công cụ được chủ yếu phát triển bởi nhà nước (ví dụ, Trung tâm cổng thông tin của nhà nước) và Trung tâm X-Road (quản lý và điều khiển cổng thông tin) với Trung tâm xác nhận đối với thẻ nhận dạng điện tử.

d. **Trung tâm một điểm truy cập dịch vụ công cộng (Cổng thông tin công dân điện tử).** Thẻ định danh điện tử của công dân được bảo mật vì nhiều mục đích truy cập được cung cấp bởi một điểm truy cập: Cổng thông tin công dân điện tử.

e. **Tiến độ chuẩn sử dụng định dạng văn bản chung (DigiDoc).** Để ký chữ ký số trên văn bản, một phương thức kết nối sử dụng tiến độ chuẩn trong định dạng văn bản chung gọi là DigiDoc được sử dụng. Định dạng DigiDoc được dựa trên tiêu chuẩn Chữ ký điện tử tiên tiến theo ngôn ngữ đánh dấu khả mở XML (XAdES). Tiêu chuẩn XAdES xác định định dạng có thể lưu trữ dữ liệu được chấp nhận, chữ ký, và bảo mật phù hợp với chữ ký điện tử, do đó, có thể đưa ra cách hiểu chung.

28. Vai trò tổ chức chính theo yêu cầu đối với hoạt động định danh điện tử bằng di động/cơ sở hạ tầng mã khoá công cộng không dây gồm:

a. **Nhà điều hành mạng di động.** Nhà điều hành mạng di động cung cấp SIM mới cho người dân khi có ứng dụng mới hơn cho điện thoại di động. SIM gồm chức năng tạo chữ ký bảo mật theo Chỉ thị số 1993/93 EC[48].
b. **Tổ chức đăng ký.** Tổ chức quản lý đăng ký RA chịu trách nhiệm về việc đăng ký và kích hoạt định danh điện tử qua điện thoại di động của người sử dụng.
c. **Tổ chức chứng nhận.** Cơ quan có thẩm quyền chứng nhận CA quản lý việc kích hoạt, đình chỉ, và huỷ bỏ chứng nhận.
d. **Nhà cung cấp dịch vụ tin cậy.** Nhà cung cấp dịch vụ tin cậy hoạt động như trung tâm trung gian trong hệ cơ sở hạ tầng mã khoá công cộng không dây wPKI. Nhiệm vụ chính gồm chấp nhận xác nhận và ký giao dịch từ nhà cung cấp dịch vụ, chuyển yêu cầu tới nhà điều hành mạng di động, và kiểm tra hiệu lực của chứng nhận và chữ ký.
e. **Nhà cung cấp dịch vụ/bên tín nhiệm.** Nhà cung cấp dịch vụ là bên thứ ba quan tâm tới xác nhận và/hoặc chữ ký số của người sử dụng.

29. Chương trình thẻ định danh điện tử của Ét-xtô-nia là trách nhiệm của toàn thể Uỷ ban di trú công dân (CMB) của Chính phủ Ét-xtô-nia. Đây là trách nhiệm phát hành văn bản nhận dạng tới công dân và người nước ngoài cư trú tại Ét-xtô-nia theo yêu cầu của Luật nhận dạng quốc gia Ét-xtô-nia. Uỷ ban CMB là một tổ chức tiếp nhận đơn đăng ký cấp thẻ từ người dân.

30. **Quan hệ công tư.** Quá trình được quản lý thông qua mối quan hệ công tư chặt chẽ với hai tổ chức tư nhân chính. AS Sertifitseerimiskeskus (SK), là tổ chức cổ phần được thành lập năm 2001 giữa hai ngân hàng lớn nhất Ét-xtô-nia (Hansapank, Eesti Ühispank), và tổ chức viễn thông (Eesti Telefon and EMT) hoạt động như một trung tâm xác nhận. TRÜB Baltic AS, một chi nhánh của tổ chức dịch vụ tài chính TRÜB và có trụ sở tại Thuỵ Sỹ, là công ty tự phát hành thẻ dưới dạng nhận diện trực quan và điện tử. TRÜB tiếp nhận đơn đăng ký cấp thẻ từ Uỷ ban CMB và phát hành thẻ, in và tạo bản khắc dữ liệu cá nhân trên thẻ, tạo ra từ khoá trên mạch và phát hành chứng nhận.

31. Chức năng của SK giống của cơ quan quản lý chứng nhận về dự án thẻ định danh điện tử của Ét-xtô-nia và quản lý toàn bộ dịch vụ điện tử, gồm giao thức truy cập nhanh các dịch vụ thư mục (LDAP), giao thức kiểm tra chứng thực trực tuyến (OCSP), và những dịch vụ chứng nhận khác

[48] SSCD Specification – Directive 1993/93 EC – http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

có liên quan. SK quản lý kênh phân bổ tới người sử dụng cuối cung thông qua các cửa hàng bán lẻ. SK chịu trách nhiệm về duy trì và phát triển phần mềm định danh điện tử được cài đặt trên thiết bị của ngườ dùng để truy cập dịch vụ định danh điện tử theo yêu cầu của chính phủ. Trách nhiệm này tương tự như trách nhiệm đối với gói cài đặt phần mềm nhận dạng điện tử, hướng dẫn và hướng dẫn bằng hình ảnh được công bố trên cổng thông tin công cộng của chính phủ. SK, thay mặt chính phủ, triển khai trung tâm liên lạc và cung cấp dịch vụ hỗ trợ qua thư điện tử tới người dân.

32. Nhằm tiến hành và quản lý chữ ký số, các tổ chức và chi nhánh sau có liên quan:

a. **Nhà cung cấp dịch vụ chứng nhận.** Theo Luật DSA của Ét-xtô-nia, nhà cung cấp dịch vụ chứng nhận xác định nhận dạng cá nhân bằng tên và mã ID. Các nhà cung cấp dịch vụ chứng nhận phải là tổ chức pháp lý đáp ứng đủ các yêu cầu pháp lý cụ thể.

b. **Nhà cung cấp dịch vụ theo dấu thời gian.** Luật DSA cũng quy định công việc của các nhà cung cấp dịch vụ tin cậy. Các yêu cầu đối với nhà cung cấp dịch vụ tin cậy gần như giống với với yêu cầu đối với các nhà cung cấp dịch vụ chứng nhận CSPs. Theo luật DSA, dấu thời gian là một đơn vị dữ liệu chứng minh một dữ liệu cụ thể có hiệu lực trong một khoảng thời gian nhất định.

33. **Cơ quan quản lý hệ thống thông tin Ét-xtô-nia**[49] được biết đến như RIA phối hợp hoạt động phát triển và quản lý hệ thống thông tin chính phủ; cơ quan này tổ chức các hoạt động liên quan đến bảo mật thông tin và giải quyết các vấn đề phát sinh về bảo mật xảy ra trong mạng lưới máy tính của Ét-xtô-nia. RIA tư vấn cho các nhà cung cấp dịch vụ công cộng làm thế nào để quản lý hệ thống thông tin của họ theo yêu cầu và điều hành chúng. Cơ quan này cũng chịu trách nhiện cung cấp hỗ trợ kỹ thuật và cơ sở hạ tầng CNTT chia sẻ cấp quốc gia, và các dịch vụ cho cơ quan chính phủ chịu trách nhiệm chuyển giao dịch vụ nhận dạng.

34. **Phần mềm nhận dạng điện tử.** Chính phủ Ét-xtô-nia cung cấp phần mềm được cài đặt trên các thiết bị kết nối mạng của người dân (như máy tính xách tay, máy tính để bàn,…). Phần mềm, ở đây được hiểu là phầm mềm nhận dạng điện tử, cho phép người dân sử dụng thẻ ID của mình để truy cập dịch vụ điện tử công và tư, ký văn bản bằng chữ ký điện tử và mã hoá văn bản để chuyển dữ liệu an toàn. Chính phủ cung cấp trên trang web công cộng[50] các bước để cài đặt phần mềm định danh điện tử trên thiết bị. Trong suốt quá trình cài đặt, có 3 chương trình sẽ được cài trên máy tính:

---

[49] Estonia Information System's Authority - https://www.ria.ee/about-Estonia-information-systems-authority/

[50] Estonia government Web Site for installing ID-software - https://installer.id.ee/?lang=eng

a. **Tiện ích thẻ ID.** Tiện ích này được người dân dùng để kiểm tra chức năng thẻ ID và hiệu lực chứng nhận, và để gia hạn nếu cần, thay đổi và khoá mã PIN và mã mở khoá cá nhân (PUK), và định dạng địa chỉ thư điện tử @eesti.ee.
b. **Ứng dụng DigiDoc3.** Ứng dụng này dùng để ký chữ ký số sử dụng thẻ ID và ID điện thoại di động, để kiểm tra hiệu lực của chữ ký điện tử, mở và lưu văn bản trong ngăn dữ liệu ký. Ngăn chứa dữ liệu ký là các tập tin có đuôi .bdoc hoặc .ddoc.
c. **Mã hoá DigiDoc3.** Ứng dụng này cho phép người dân bảo mật thông tin để truyền thông tin bằng cách sử dụng thẻ ID và để xem các văn bản bảo mật (đã được mã hoá). Những văn bản này được mã hoá bằng cách sử dụng xác nhận thẻ ID và bổ sung vào ngăn chứa dữ liệu bảo mật bằng tập tin có đuôi .cdoc.
d. **Ứng dụng nối trình duyệt.** Đây là ứng dụng được cài đặt trên thiết bị của người dân khi truy cập cổng thông tin lần đầu tiên. Yêu cầu kết nối chứng nhận của người dân và phản hồi mã PIN để nhận dạng được thực hiện trước khi cho phép họ kết nối với nhà cung cấp dịch vụ.

35. **Cổng thông tin điện tử.** Địa chỉ cổng thông tin http://digidoc.sk.ee; tất cả các chủ sở hữu thẻ được miễn phí truy cập cổng thông tin này. Chức năng của cổng thông tin tương tự như chương trình ứng dụng – một người có thể sử dụng ứng dụng này để tạo ra và xác định chữ ký điện tử. Ngoài ra, cá nhân có thể sử dụng ứng dụng này để có văn bản có chữ lý của nhiều người. Chỉ với vài thao tác chuột, người sử dụng có thể chỉ định người ký cần thiết trên văn bản, và những người này có thể ký trên cùng một cổng thông tin. Mỗi người sử dụng có một hướng dẫn văn bản mà không ai có thể nhìn thấy; tuy nhiên, bất cứ ai cũng có thể gửi văn bản có chữ ký của người sử dụng.

36. SK, cùng với các đối tác của mình, chuyển giao chữ ký số hoàn chỉnh được biết đến là DigiDoc[51]. Đây là một hệ thống toàn cầu nhằm yêu cầu, tạo lập và xác nhận chữ ký số. Nó được kết nối với bất kỳ phần mềm mới hoặc sẵn có nào. Các phần của hệ thống là chương trình ứng dụng riêng biệt, một cổng thông tin điện tử và dịch vụ trang web dựa trên giao thức truy suất đối tượng đơn giản (SOAP)[52] để có thể dễ dàng kết hợp chức năng của chữ ký số, xác nhận chữ ký và xác nhận với hệ thống thông tin khác. Dịch vụ này được dùng trong nhiều môi trường và nền tảng khác nhau với hỗ trợ mã hoá SOAP 1.0.

---

[51] DigiDoc Specification – http://www.sk.ee/upload/files/DigiDocService_spec_eng.pdf

[52] SOAP – Simple Object Access Portal – http://www.w3.org/TR/soap/

37. SK dựa trên định dạng văn bản DigiDoc theo chuẩn chữ ký XML (DSig) standard. Tháng 2/2002, Tổ chức quản lý tiêu chuẩn viễn thông châu Âu (ETSI) phát hành mở rộng XML-DSig thành ETSI TS 101 903, được gọi là Chữ ký điện tử tiên tiến theo ngôn ngữ đánh dấu khả mở XAdES[53]. Định dạng văn bản DigiDoc là một tệp dữ liệu của XAdES, gồm nhiều tệp mở rộng. The tệp dữ liệu XAdES về XAdES-X-L (ví dụ, mở rộng dài hạn) được sử dụng trong hệ thống DigiDoc nhưng chức năng đánh dấu thời gian (timemarks) được dùng thay cho dấu thời gian (timesptamp), ký và thời gian xác định hiệu lực chứng nhận theo phản hồi của OSCP. Dữ liệu này cung cấp thông tin về văn bản đã ký như sau:

a. Chứng nhận sử dụng để ký
b. Thời gian ký
c. Địa điểm ký
d. Vai trò của người ký và giải pháp
e. Tích hợp với thông tin hiệu lực chứng nhận trong chữ ký
f. Phản hồi của OCSP
g. Chứng nhận phản hồi OCSP

38. Trên cơ sở định dạng văn bản, một thư viện được thành lập theo ngôn ngữ chương trình C và kết hợp với:

a. Định dạng văn bản DigiDoc
b. Dịch vụ kiểm tra hiệu lực OCSP của SK
c. Liên kết với thẻ ID của người sử dụng bằng cách dùng liên kết nguyên bản CPS của hệ điều hành Windows hoặc qua hệ thống PKCS#11.

39. **Cổng thông tin công dân điện tử (eCitizen Portal).** Thẻ ID của người dân được bảo mật nhằm cung cấp dịch vụ định danh điện tử bằng cổng một điểm dừng: Cổng thông tin công dân điện tử. Thẻ ID được sử dụng với mục đích xác nhận tại Cổng thông tin công dân điện tử. Sau khi xác nhận, hiệu lực chứng nhận của công dân có thể được xác nhận bằng dịch vụ OCSP; dấu thời gian được đưa vào ứng dụng dịch vụ điện tử. Sử dụng X-Roads, cổng mạng, và tin nhắn ứng dụng được trao đổi ở chế độ an toàn.

40. Để thông qua dịch vụ chữ ký số trong vùng, phần mềm và kỹ thuật cung cấp cho các bên bắt buộc phải phù hợp chặt chẽ với các ứng dụng. Chính phủ không thể tìm ra ứng dụng chung trong nội địa hoặc tiến hành đáp ứng yêu cầu. Nhưng vẫn ra quyết định để không phụ thuộc vào

[53] XAdES – http://www.openxades.org

nhà cung cấp kỹ thuật hoặc phần mềm nước ngoài nhằm cung cấp và đảm bảo hỗ trợ cho cơ sở hạ tầng quốc gia quan trọng này. Việc phụ thuộc vào nhà cung cấp nước ngoài có thể dẫn đến tác động bất lợi thường ngày của quốc gia kể từ đó về sau. Do những cân nhắc này, mô hình phần mềm đặt riêng đặc biệt đã được xây dựng để cung cấp cho Ét-xtô-nia và những bộ phận cấu thành chữ ký số.

41. Có thể xác định hiệu lực của chữ ký số mà không cần thông tin bổ sung nào; người xác định sẽ tin tưởng vào tổ chức phát hành chứng nhận của người ký và chứng nhận phản hồi OCSP.

42. Các tài liệu nguyên bản đi cùng với chữ ký, xác nhận hiệu lực và chứng nhận được nén trong ngăn dữ liệu với "SignedDoc" như là các thành phần cốt yếu.

43. Khuôn khổ hệ thống DigiDoc gồm thư viện cơ sở, thư viện trung gian, dịch vụ web và ứng dụng cung cấp cho người sử dụng cuối cùng.

a. Thư viện phần mềm. Thư viện DigiDoc luôn sẵn sàng sử dụng cho tất cả những người xây dựng với ngôn ngữ lập trình C trong thư viện chương trình và Mô hình thành phần của hệ điều hành Windows (COM). Nó có thể được kết nối với bất kỳ phần mềm mới hoặc sẵn có nào. Ví dụ, người sử dụng có thể bổ sung hỗ trợ DigiDoc vào phần mềm kế toán, hệ thống quản lý văn bản, trang web và ứng dụng nội bộ, hoặc tương tự.
b. Máy chủ OCSP. Về khía cạnh máy chủ, DigiDoc cung cấp một máy chủ OCSP phù hợp RFC2560, điều hành trực tiếp bởi trung tâm cơ sở dữ liệu chứng nhận CA và cung cấp xác nhận hiệu lực đối với chứng nhận và chữ ký.
c. Để đảm bảo hiệu lực của chứng nhận, thông tin hiệu lực của chứng nhận được kiểm tra từ cơ sở dữ liệu trực tiếp hơn là từ danh mục huỷ chứng nhận (CRL) và giá trị thời gian trong phản hồi của OCSP có thể là thực. Để có được chữ ký điện tử hiệu lực dài hạn, một hệ thống truy cập bảo mật được sử dụng trong mô hình. Tất cả phản hồi của OCSP và những thay đổi trong chứng nhận hiệu lực sẽ được truy cập an toàn để duy trì hiệu lực của chữ ký điện tử.

44. Mô hình bảo mật DigiDoc. Một trong những vấn đề thách thức nhất trong quản lý hệ thống chữ ký số là câu hỏi về hiệu lực của chữ ký sau khi được chứng nhận. Thường thì những tranh cãi về hiệu lực chứng nhận chữ ký của người ký tại thời điểm ký sẽ được xử lý bởi người xác nhận. DigiDoc dựa trên XadES mở, bằng chứng chứng nhận hiệu lực của người ký được duy trì tại thời điểm tạo chữ ký. Bằng chứng này được duy trì định dạng trong phản hồi OCSP và được lưu trữ trong văn bản đã ký.

45. Dịch vụ DigiDoc cung cấp phương pháp xác nhận bằng điện thoại và ký bằng điện thoại có tên là Xác nhận bằng điện thoại di động, Ký trên điện thoại di động và tạo chữ ký trên điện thoại di động. Cả ba phương pháp đều chấp nhận mã xác nhận cá nhân đối với người sử dụng điện thoại và/hoặc số điện thoại như dữ liệu đầu vào. Sử dụng số điện thoại để xác nhận người dùng được khuyên là không nên vì số điện thoại được công khai và có thể phát sinh những vấn đề liên quan đến bảo mật. Thay vào đó, việc dùng cả số điện thoại và mã nhận dạng cá nhân được khuyên dùng do những thông tin này không công khai và là lựa chọn an toàn hơn.

46. Cơ sở hạ tầng công cộng không dây[54]. ID di động dựa trên quy định về cơ sở hạ tầng mã khoá công cộng không dây wPKI được thực hiện thông qua cơ sở hạ tầng PKI. Với wPKI, điện thoại di động hoạt động như một thẻ đọc thông minh hiển thị. Liên kết giữa máy tính cá nhân/dịch vụ và điện thoại di động thông qua chữ ký số trên di động/ xác nhận dịch vụ trên di động và cổng thông tin đi động của nhà cung cấp dịch vụ mạng.

47. Cổng thông tin di động sử dụng kỹ thuật cập nhật phần mềm từ xa (OTA)[55] để kết nối và chạy ứng dụng trên SIM của điện thoại di động mà không kết nối trực tiếp với thẻ. Dịch vụ DigiDoc gửi xác nhận/yêu cầu chữ ký (yêu cầu wPKI[56]) đến cuối hệ thống của nhà điều hành mạng, bù lại, sẽ gửi yêu cầu tới cổng thông tin/máy chủ OCSP. Cổng thông tin OTA truyền yêu cầu trong một tin nhắn ngắn gọn và gửi tới Trung tâm dịch vụ tin nhắn ngắn (SMSC) để truyền tới điện thoại di động của người dùng. Cổng thông tin OTA nhận yêu cầu dịch vụ bằng giao diện lập trình ứng dụng (API) của Cổng thông tin OTA. Cổng thông tin OTA duy trì cơ sở dữ liệu thẻ phát hành và kích hoạt với chi tiết như nhà cung cấp SIM, số thẻ nhận dạng, trung tâm nhận dạng di động quốc tế (IMSI) và số nhận dạng di động quốc tế (MSISDN). Cổng thông tin OTA có một thư viện chứa các định dạng sử dụng trong các loại SIM để định dạng yêu cầu dịch vụ thành tin nhắn dễ hiểu trên điện thoại di động của công dân. Cổng thông tin OTA gửi tin nhắn tới trung tâm SMSC bằng cách sử dụng các tiêu chí phù hợp như mô tả tại GSM 03.48. SMSC sẽ gửi tin nhắn có độ dài tối đa 160 ký tự từ và đến điện thoại di động. Nếu điện thoại di động tắt máy hoặc ra khỏi vùng phủ sóng, tin nhắn sẽ được lưu và gửi lại khi điện thoại di động mở máy hoặc nằm trong vùng phủ sóng. Liên kết giữa SIM và Cổng thông tin OTA được thực hiện bằng cách trao đổi tin nhắn thông qua kênh SMS.

---

[54] wPKI Specification - http://www.signature.lt/KK/wPKI-specification.pdf

[55] Over-The-Air Technology - http://www.gemalto.com/techno/ota/

[56] WPKI Mobile Transactions - http://wpki.eu/doku/lib/exe/fetch.php/wiki:baltic_wpki_standard_draft-0.3.pdf

48. Điện thoại di động có giai đoạn 2+ trong tiêu chuẩn GSM[57] và có bộ dụng cụ ứng dụng SIM (STK)[58] với ứng dụng hỗ trợ dịch vụ OTA theo tiêu chuẩn GSM[59].

49. Ngày nay ở Ét-xtô-nia, việc dùng thẻ ID điện tử làm bằng chứng nhận dạng ngày càng được sử dung phổ biến. Việc này chủ yếu theo yêu cầu thời gian đối với những người muốn thay đổi suy nghĩ, thiếu ứng dụng, có thể không khuyến khích người dùng ngay từ lần sử dụng đầu tiên, vàchi phí cao hơn cho đầu dọc thẻ ID. Thẻ ID được sử dụng rộng rãi cho xác nhận hiệu lực thẻ ID trong hệ thống thông tin công cộng và nó có chi phí thấp hơn một chiếc vé giấy. Chức năng ID điện tử của thẻ ngân hàng thường được sử dụng nhiều hơn thẻ ID. Khi công dụng của thẻ ID có hiệu quả về mặt chi phí hơn đối với ngân hàng và đảm bảo tính bảo mật cho công dân, xu hướng kinh tế chung có thể hỗ trợ chuyển dịch từ thẻ ngân hàng sang thẻ ID điện tử trong ứng dụng dịch vụ công cộng.

50. Chính phủ Ét-xtô-nia tiến hành các biện pháp sau để cải tiến việc ứng dụng định danh điện tử đối với người dân:

a. Khuyến khích ID điện tử cho người dân, chính phủ đã ban hành trên cổng thông tin công cộng phần mềm ID và cài đặt trên các thiết bị kết nối mạng. Đoạn hướng dẫn bằng hình ảnh về cài đặt phần mềm cũng được cập nhật nhằm hướng dẫn cụ thể hơn cho người dân.
b. Cổng thông tin công cộng cũng cung cấp hướng dẫn bằng hình ảnh đối với ký văn bản bằng chữ ký số sử dụng thẻ ID hoặc ID di động với dịch vụ DigiDoc.
c. Dịch vụ thử nghiệm cài đặt bởi chính phủ cho những người dân muốn kiểm tra hoạt động phần mềm ID và đầu đọc thẻ liệu có hoạt động không; dịch vụ này tạo ra quyền truy cập dịch vụ nhận dạng điện tử.
d. Chính phủ cũng thiết lập trung tâm liên lạc và hỗ trợ bằng thư điện tử cho công dân cần hỗ trợ cài đặt phần mềm hoặc dịch vụ nhận dạng điện tử.
e. Chính phủ cung cấp văn bản liên quan đến Digidoc[60] và các dịch vụ khác có thể hữu ích cho người cung cấp dịch vụ với mong muốn truy cập chức năng chữ ký số trong chuyển giao ứng dụng.

---

[57] GSM 11.11 Digital Cellular Telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface - http://www.etsi.org/deliver/etsi_gts/11/1111/05.03.00_60/gsmts_1111v050300p.pdf

[58] SIM Application Toolkit - http://www.gemalto.com/techno/stk/

[59] GSM 11.14 Digital Cellular Telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for Subscriber Identity Module - Mobile Equipment (SIM-ME) interface - http://www.etsi.org/deliver/etsi_gts/11/1114/05.04.00_60/gsmts_1114v050400p.pdf

III. Bỉ

Web Site chính thức : http://eid.belgium.be/en/

1. Bỉ có ba loại văn kiện định danh điện tử theo luật định: định danh điện tử (eID) cho công dân trên mười hai tuổi, định danh điện tử cho trẻ em dưới mười hai tuổi, và thẻ cho người nước ngoài sinh sống tại Bỉ.

2. Chứng minh nhân dân là bằng chứng cho việc thông tin cá nhân của công dân đã được nhập vào trong Đăng ký dân số quốc gia tại Bỉ. Các công dân có thể sử dụng thẻ này để chứng minh quốc tịch và danh tính của họ. Tất cả các công dân Bỉ sẽ tự động nhận được một chứng minh thư điện tử ở tuổi mười hai. Và được cung cấp bởi cơ quan đăng ký tại địa phương. Các công dân trên 15 tuổi được yêu cầu phải mang chứng minh nhân dân ở mọi lúc mọi nơi.

3. Tại Bỉ, định danh điện tử (eID) đã được thực hiện bằng cách sử dụng chứng minh thư điện tử. Thẻ định danh điện tử (eID) của Bỉ là loại thẻ thông minh với một con chip được tích hợp. Con chip có chứa chứng thực và chứng nhận chữ ký cùng với mã PIN cho mỗi chứng nhận.

4. Thẻ định danh điện tử (eID) được sử dụng để cung cấp nhận dạng và xác thực điện tử và các dịch vụ chữ ký số. Chứng nhận xác thực được sử dụng để xác nhận danh tính của công dân tại thời điểm đăng nhập vào một trang web với định danh điện tử (eID) của công dân. Chứng nhận chữ ký cho phép hiển thị chữ ký số của công dân. Công dân có đủ điều kiện để sử dụng chữ ký số của họ từ 18 tuổi trở đi. Họ sẽ đến văn phòng đăng ký tại địa phương để kích hoạt chứng nhận chữ ký trên thẻ.

5. Định danh điện tử (eID) trẻ em sử dụng dịch vụ Hello Service[61] cung cấp cho trẻ em sự bảo vệ đặc biệt trong trường hợp khẩn cấp. Dịch vụ này có thể giúp liên hệ với cha mẹ (hoặc gia đình, bạn bè, hàng xóm, vv) qua điện thoại nếu một đứa trẻ đang trong tình trạng khó khăn. Khi dịch vụ được kích hoạt, những người tìm thấy đứa trẻ mất tích sẽ có một số điện thoại để gọi; ứng dụng tự động gọi số đã được chỉ định. Một người sử dụng có thể chỉ định lên đến bảy con số. Nếu không có ai trả lời, cuộc gọi được tự động chuyển đến số khẩn cấp của Child Focus luôn sẵn sàng 24 giờ một ngày.

---

[60] DigiDoc Service Specifications – http://www.sk.ee/upload/files/DigiDocService_spec_eng.pdf

[61] Hello Service – http://www.halloouders.be/

6. Để sử dụng định danh điện tử (eID) với các nhà cung cấp dịch vụ của chính phủ và khối tư nhân, các công dân phải có một máy tính với hệ điều hành được hỗ trợ và một đầu đọc thẻ gắn vào máy tính.

7. Để sử dụng định danh điện tử (eID) với các nhà cung cấp dịch vụ của chính phủ và khối tư nhân, các công dân phải có một máy tính với hệ điều hành được hỗ trợ và một đầu đọc thẻ gắn vào máy tính.

8. Cơ quan dịch vụ công của liên bang Bỉ về Công nghệ thông tin và truyền thông (Fedict) đã phát triển phần mềm đơn giản cho hệ điều hành hỗ trợ cài đặt phần mềm định danh điện tử (eID) trên máy tính được gọi là eID QuickInstall[62]. Phần mềm này hiện có sẵn để tải về trên trang web của cổng thông tin công cộng của chính phủ Bỉ cho định danh điện tử [63]. Công dân có thể cài đặt phần mềm bằng cách làm theo hướng dẫn hiển thị trên màn hình khi chạy chương trình. Phần mềm kiểm tra cấu hình của máy tính và cài đặt trình điều khiển cho đầu đọc thẻ và phần mềm định danh điện tử (eID). Khi cài đặt thành công phần mềm, sử dụng dịch vụ thử nghiệm[64] được cung cấp bởi Fedict sẽ đọc dữ liệu trên thẻ để kiểm tra xem tất cả mọi thứ có đang làm việc như đã thiết kế hay không. Phần mềm này cũng cung cấp cơ chế để cài đặt bản cập nhật thường xuyên cho phần mềm.

9. Định danh điện tử (eID) làm việc với một mã PIN và mã mở khoá cá nhân (PUK). Mã PIN do chính phủ cấp và được niêm phong trong thư kín từ chính quyền địa phương khi thu thập các định danh điện tử (eID). Mã PIN là một số 12 chữ số và có thể được cập nhật bởi công dân. Bức thư cũng bao gồm mã mở khoá cá nhân (PUK). Các công dân được khuyến cáo đến văn phòng đăng ký tại địa phương với mã PIN và mã mở khoá cá nhân (PUK) và sau đó sẽ được sử dụng để kích hoạt các vi mạch trên thẻ định danh điện tử (eID)với sự hỗ trợ từ các nhân viên. Mã PIN là mã số cá nhân sử dụng bởi các công dân mỗi khi có ứng dụng cung cấp dịch vụ dựa trên định danh điện tử (eID) được truy cập; và cũng có thể được sử dụng để cấp chữ ký số. Mã mở khoá cá nhân (PUK) là chỉ để kích hoạt hoặc bỏ chặn các định danh điện tử (eID).

---

[62] QuickInstall software - http://eid.belgium.be/en/using_your_eid/installing_the_eid_software/

[63] Belgium eID government public portal - http://eid.belgium.be/en/

[64] eID Installation Testing Service - http://www.test.eid.belgium.be/

10. Fedict đã thiết lập dịch vụ trực tuyến riêng của mình để hỗ trợ công dân trong việc giải quyết các vấn đề về cài đặt và sử dụng phần mềm. Các công dân có thể điền vào một biểu mẫu liên lạc trên trang web của Fedict[65] để thông báo các vấn đề.

11. Dịch vụ công cộng liên bang Nội vụ cùng với Bộ Ngoại giao, Ngoại thương và Hợp tác phát triển và Cảnh sát Liên bang đã thiết lập dịch vụ DOC STOP[66] miễn phí và dịch vụ CheckDoc để bảo vệ sự riêng tư của dữ liệu trên thẻ và ngăn chặn gian lận nhân dạng. DOC STOP giúp tránh rủi ro của sử dụng gian lận cũng như những hậu quả tài chính không không mong muốn. Nó cho phép công dân có thể khoá thẻ chứng minh ngay lập tức nếu nó bị mất hoặc bị đánh cắp. Các công dân sẽ phải gọi một số điện thoại miễn phí DOC STOP để trình báo thẻ bị mất hoặc bị đánh cắp và để khoá lại. Dịch vụ này hoạt động 24 giờ mỗi ngày quanh năm.

12. CheckDoc[67] cho phép xác minh trong thời gian thực tính hợp lệ của giấy tờ tùy thân tại Bỉ; nó cũng xác định các giấy tờ tùy thân bị đánh cắp, bị mất, hết hạn, hợp lệ hoặc chưa bao giờ được sử dụng. Để sử dụng dịch vụ, công dân hoặc tổ chức sử dụng phải điền vào một mẫu đơn và truy cập vào trang web với tên người dùng và mật khẩu được cung cấp khi đăng ký thành công.

13. Cổng thông tin chính phủ cung cấp một danh sách các ứng dụng của khu vực công và tư nhân hỗ trợ định danh điện tử (eID)[68].

14. Fedict đã lựa chọn phần mềm nguồn mở (OSS) và hợp tác tích cực với các nhà phát triển. Các mã nguồn cho các sáng kiến định danh điện tử (eID) là cho các bên quan tâm có thể xem các phần mềm, đề xuất và/hoặc cải thiện. Trong sự giao thoa chéo này các chuyên gia trên toàn thế giới có thể thực hiện việc sửa đổi, cải thiện sự ổn định và chất lượng của các mã nguồn. Để phù hợp với cách tiếp cận này, Fedict đã tạo ra một Hướng dẫn của các nhà phát triển định danh điện tử (eID) (Belgium eID Developers' Guides[69]). Chúng chứa các hướng dẫn cho việc phát triển các ứng dụng định danh điện tử (eID) bằng các ví dụ cụ thể.

15. Fedict đang xúc tiến việc sử dụng định danh điện tử (eID) bằng các ứng dụng của cả khu vực công và tư bằng cách cung cấp các nhà phát triển với các khối hợp nhất định danh điện tử

---

[65] Fedict Service Desk Contact Form – http://eid.belgium.be/en/contact/contactform.jsp

[66] Doc Stop Service – https://www.docstop.be/DocStop/docstop_en.jsp

[67] Check Doc Service – https://www.checkdoc.be/CheckDoc/

[68] Available eID Applications – http://eid.belgium.be/en/available_eid_applications/

[69] Belgium eID Developers' Guides – http://eid.belgium.be/en/binaries/UPD_Developers_Guide_tcm406-112228.pdf

(eID) (Belgium eID building blocks[70]), các khối cơ bản của ứng dụng định danh điện tử (eID). Nó cung cấp dịch vụ cho các cơ quan chính phủ trong việc tích hợp các Eid vào các ứng dụng riêng của họ. Các dịch vụ được cung cấp bởi Fedict có sẵn trên cổng thông tin công cộng của họ trong phần nhận dạng và bảo mật[71].

16. Các khối hợp nhất định danh điện tử (eID) bao gồm:

a. **Phần mềm eID and Applet**[72]. Phần mềm eID và Applet eID. Các phần mềm eID đảm bảo việc sử dụng các eID trên máy tính của công dân. Phần mềm cung cấp giao diện người dùng và nhận thẻ vào đầu đọc thẻ như là một chứng minh thư điện tử. Các mã nguồn có sẵn như là một dự án mã nguồn mở[73] và Fedict duy trì một danh sách gửi thư trực tuyến và các cuộc thảo luận để hỗ trợ phát triển[74].

b. **Dịch vụ chữ ký số** (Digital Signature Service[75]). Dịch vụ chữ ký số là một dịch vụ có thể được sử dụng bởi các ứng dụng web để áp dụng hoặc kiểm tra chữ ký số đối với một eID. Dịch vụ chữ ký số hỗ trợ các định dạng tài liệu khác nhau và cung cấp tất cả các tương tác cần thiết cho người sử dụng. Chữ ký được áp dụng thông qua dịch vụ chữ ký số tuân thủ thông số kỹ thuật và Chỉ thị Châu Âu 2009/767 / EC về chữ ký điện tử tiên tiến theo ngôn ngữ đánh dấu khả mở (XAdES). Các mã nguồn có sẵn như là một dự án mã nguồn mở [76].

c. **Nhà cung cấp danh tính nhận dạng điện tử**[77]. Các nhà cung cấp danh tính của eID cho phép một ứng dụng web có thể truy cập bằng cách sử dụng eID. Khối hợp nhất này có chứa tất cả các chức năng cần thiết để chứng thực một cách chính xác cho người sử dụng một ứng dụng với một eID. Các mã nguồn có sẵn như là một dự án mã nguồn mở[78].

---

[70] Belgium eID Building Blocks – http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/

[71] Identification & Security Section – http://www.fedict.belgium.be/en/identificatie_beveiliging/

[72] Belgium eID Software and applet – http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/eID_software/

[73] Belgium eID Building Block Source Code – http://code.google.com/p/eid-mw/

[74] Belgium Developers Help and Support – http://groups.google.com/group/eid-mw

[75] Belgium Digital Signature Service – http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/digital_signature_service/

[76] Belgium DSS Source code – http://code.google.com/p/eid-dss

[77] Belgium eID Identity Provider – http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/eID_identity_provider/

[78] Belgium eID Identity Provider Source Code – http://code.google.com/p/eid-idp

d. **Quick Key Toolset**[79]. EZ key hoặc Quick Key Toolset có nghĩa là một thẻ thông minh của Java có thể hoạt động giống như một eID. Bằng cách này, các EZ key chính là chìa khoá mở cửa cho tương lai, khi định danh điện tử phụ thuộc ít hơn vào các nhà cung cấp. Các mã nguồn có sẵn như là một dự án mã nguồn mở[80].

17. Fedict cũng cung cấp một bộ công cụ phát triển phần mềm định danh điện tử (eID Software Developmen Kit[81]) để cho phép các nhà phát triển sử dụng nội dung của thẻ eID từ các ứng dụng máy tính để bàn. Bộ công cụ phát triển phần mềm (SDK) bao gồm các eID Middleware[82] và được dựa trên tiêu chuẩn mã hoá công khai (PKCS) # 11.

18. Fedict[83] chịu trách nhiệm phát triển phần mềm cho thẻ nhận dạng điện tử. Và xác định và thực hiện chiến lược của chính phủ điện tử liên bang. Thông tin sáng tạo và công nghệ thông tin được sử dụng để giúp các dịch vụ công cộng liên bang khác nhau để cải thiện danh mục dịch vụ của họ. Kết lại, Fedict tạo ra công nghệ để đáp ứng các nhu cầu của công chúng nói chung, doanh nghiệp và cán bộ công chức.

---

[79] Belgium Quick Key tool set - http://eid.belgium.be/en/developing_eid_applications/eid-bouwstenen/quick_key_tool_set/

[80] Belgium Quick Key tool set source code - http://code.google.com/p/eid-quick-key-toolset

[81] Belgium eID Software Development Kit (SDK) - http://eid.belgium.be/en/developing_eid_applications/eid_software_development_kit/

[82] Belgium eID Middleware SDK 4.0 - http://code.google.com/p/eid-mw/wiki/SDK40

[83] Fedict - http://www.fedict.belgium.be/en/over_fedict/

[i] ISO 27001 – http://www.27000.org/iso-27001.htm
[ii] ISO 27002 – http://www.27000.org/iso-27002.htm
[iii] ISO 27003 – http://www.27000.org/iso-27003.htm
[iv] ISO 27004 – http://www.27000.org/iso-27004.htm
[v] ISO 27005 – http://www.27000.org/iso-27005.htm