# WEST BANK AND GAZA

# HIGH LEVEL TECHNICAL ASSESSMENT ON E-GOVERNMENT

**January, 2016**

WORLD BANK GROUP

## Standard Disclaimer:

This volume is a product of the staff of the International Bank for Reconstruction and Development/ The World Bank. The findings, interpretations, and conclusions expressed in this paper do not necessarily reflect the views of the Executive Directors of The World Bank or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

## Copyright Statement:

# Contents

## List of Figures



## List of Tables

## List of Abbreviations

| | |
|---|---|
| BPEL | Business Process Execution Language |
| BPMN | Business Process Model and Notation |
| CA | Certifying Authority |
| CMMI | Capability Maturity Model Integration |
| CMS | Content Management System |
| COBIT | Control Objectives for Information and related Technology |
| DoD | Database of Databases |
| ETSS | Embedded Technology Skill Standards |
| FAQs | Frequently Asked Questions |
| G2B | Government-to-Business |
| G2C | Government-to-Citizen |
| G2G | Government-to-Government |
| IAAS | Infrastructure as a Service |
| ICT | Information and Communication Technologies |
| IT | Information Technology |
| ITEE | Information Technology Engineers Examination |
| ITIL | Information Technology Infrastructure Library |
| ITSM | IT service management framework |
| ITSS | Skill Standards for IT Professionals |
| KPI | Public Key Infrastructure |
| MOE | Ministry of Education |
| MOF | Ministry of Finance |
| MOH | Ministry of Health |
| MOI | Ministry of Interior |
| MOJ | Ministry of Justice |
| MOLG | Ministry of Local Government |
| MONE | Ministry of National Economy |
| MOSA | Ministry of Social Affairs |
| MOT | Ministry of Transportation |
| MTIT | Ministry of Telecommunications and Information Technology |

| | |
|---|---|
| NIST | National Institute of Standards and Technology |
| OCTAE | Operationally Critical Threat, Asset and Vulnerability Evaluation |
| OTP | One-Time Password |
| PA | Palestinian Authority |
| PAAS | Platform as a Service |
| PalCERT | Palestinian Cybersecurity Emergency Response Team |
| PLC | Palestinian Legislative Council |
| PMBOK | Project Management Body of Knowledge |
| PPP | Public-Private Partnership |
| RFI | Requests For Information |
| RFP | Requests For Proposals |
| RFQ | Request For Quotations |
| RSS | Rich Site Summary |
| SAAS | Software as a Service |
| SLA | Service Level Agreements |
| TOGAF | The Open Group Architecture Framework |
| UISS | Users Information System Skill Standards |
| USAID | United States Agency for International Development |
| W3C | World Wide Web Consortium |
| WB&G | West Bank and Gaza |
| WFMC | Workflow Management Coalition |

# 1. Executive Summary

The Palestinian Authority (PA) is in the early phase of its e-government journey and aims to utilize ICT to deliver services to its citizens and businesses to improve social well-being and facilitate economic development. The PA aims to serve 12.1 million Palestinians in the West Bank (2.7 million), the Gaza Strip (1.7 million), and the remaining 7.7 million Palestinians who are dispersed among 28 different countries. Many Palestinians are refugees, including more than one million in the Gaza Strip, 750,000 in the West Bank, and about 250,000 in Israel. Of the Palestinian population residing abroad, otherwise known as the Palestinian diaspora, more than half are considered stateless, lacking citizenship in any country. The combination of the ongoing Israeli-Palestinian conflict as well as the diaspora situation makes implementation of e-government projects in the West Bank and Gaza (WB&G) unique and complex.

A review of e-government documentation and stakeholder interviews reveals that the PA has made reasonable progress on e-government amidst a challenging environment, but it is still in the nascent phase in terms of delivering benefits to its constituents. There are numerous challenges for the successful implementation of e-government, including geopolitical conflict, insufficient legislation to facilitate electronic transactions, limited budget to support e-government projects, inadequate policies and standards, and limited capacity within the e-government unit under the Ministry of Telecommunications and Information Technology (MTIT).

The most challenging barriers to e-government implementation, which are the dispersion of the Palestinian population and the Israeli-Palestinian conflict, also serve as the most pressing reasons for implementing e-government since it would enable the government to better perform its responsibilities and provide e-services to Palestinians. Through the utilization of ICT, the government would be able to digitally unite, communicate, and serve its citizens and businesses. The successful provision of citizen-centric information and implementation of basic e-services will provide an excellent opportunity to increase the effectiveness and efficiency of the PA's service performance. The PA views e-government not as a luxury but as an essential necessity from the governance, economic, and social perspectives. E-government solutions and e-services are expected to provide improved reach and services to Palestinians within the West Bank and Gaza, as they face difficulties in reaching public offices because of the movement and access restrictions. E-government is also expected to connect and serve Palestinian refugees across the globe.

The PA has identified e-government as one of its key national priorities. In 2005, President Abbas appointed a ministerial committee for e-government, which oversaw the completion of the e-government strategic plan. Based on the e-government policy document drafted by MTIT, the e-government vision aims "to provide a better life for our citizens by being a government that empowers citizens to participate in government; connects citizens, the private sector and institutions to drive economic growth and meet community challenges; and delivers real public value through citizen-centric government services." However, the e-government program has suffered setbacks because of various internal and external challenges.

With the OECD's support, a report entitled *Modernizing the Public Administration: The Case of E-government in the Palestinian Authority* was published in 2011 to illustrate the potential impact of e-government policies when integrated within the public administration reform agenda. In addition, MTIT and OECD jointly drafted an "E-government Policy Document" and an "E-government Implementation Roadmap" in 2011 to design and implement the building blocks and principles identified as drivers for growth. Appendix A provides a summary of the report's key points.

MTIT has requested a high-level technical assessment on the enabling environment, to better understand the current roadblocks to fulfilling the e-government vision. The key points of the assessment include:

1. Legislation: With regard to legislation related to e-government, an Electronic Transaction (e-Transaction) Law and a Right to Access to Information Law have been drafted and are pending the cabinet's approval. The two laws are deemed essential for the implementation of e-government services.

2. E-government Strategy: While an e-government strategy document was drafted in 2011, there is a need to review and update the strategy document to ensure that policies and programs are revised according to new priorities, for example, the National Development Plan 2014-2016. In addition, an implementation master schedule should be drafted to ensure projects are better managed and monitored.

3. Leadership and Organizational Capacity: There is positive recognition across government ministries that MTIT should continue to take a leadership role in driving the e-government agenda. However the e-government unit within MTIT is inadequately staffed and the unit's officers require further training in both technical and soft skills, for example, project management.

4. Governance: The e-government Ministerial Committee, formed in 2014, is responsible for the overall strategy. However, the governance structure is deemed to be less effective as it lacks comprehensive oversight of all e-government projects. The committee should also undertake the coordination of grants and loans from multilateral and bilateral agencies to ensure alignment and adoption of shared ICT infrastructure and avoid overlaps in effort.

5. Policies and Standards: Defining policies and adopting globally used IT standards are essential for implementing e-government projects. The current policy document, developed by MTIT with the support of the OECD, does not extend to technology-related aspects, such as sharing IT infrastructure, public key infrastructure (PKI), digital security, e-payment, and information security. IT standards play an important and integral part in facilitating the choice and adoption of technologies. MTIT has successfully implemented the Palestinian e-government interoperability framework, named Zinnar, which aims to establish the necessary foundation for the interoperation of heterogeneous information systems in the different governmental ministries in WB&G. Beyond the establishment of Zinnar, there are inadequate standards established in all other areas; for example, in project management, IT service management, and risk assessment frameworks.

6. Infrastructure: The PA already enjoys a commendable technological infrastructure: a government network through which all ministries are currently connected to the Government Computer Center. MTIT aims to move the data center onto a private government cloud by 2016. The PA has yet to establish a disaster recovery site. From a shared software infrastructure perspective, MTIT, with the support of the Estonian government, has put in place X-Road, which is a platform to facilitate data exchange between different databases and information systems.

7. Government-to-Government Services: Several shared government-to-government (G2G) systems are available throughout all ministries. These include an e-mail platform and ministry websites provided by the MTIT, and financial, HR applications, and payroll system provided by the Ministry of Finance. In addition, various ministries, MOJ, MOSA, MOE, MOF, MOH, MOI, MOLG, MONE, and the Council of Ministers Cabinet Secretariat, are currently implementing ministry-specific initiatives.

8. Government-to-Citizen/Government-to-Business: The PA's ministries have generally been focused on establishing ministry-specific information, while MTIT has focused on implementing a G2G infrastructure, such as the Government Computer Center, Zinnar and X-Road. A handful of ministries in the West Bank have started to publish citizen-centric information online, for example, guidelines on transacting public services on their websites.

While there are many barriers towards the implementation of e-government, MTIT can deliver visible e-government success by focusing its attention on the following recommended initiatives, which are divided into 4 tracks.

1. Develop a Palestinian national portal (Track 1). This citizen-facing track would focuses on the delivery of quality information and services for citizens and businesses. A national portal, with an e-government on social media sub-program, would require technical assistance for an estimated period of 4 to 6 months, and portal implementation for a period of 12 to 18 months. MTIT should involve citizens to help co-design the National Portal so as to better align with citizens' needs and expectations. MTIT could organize brainstorming sessions and developer hackathons to tap into the creativity of citizens.

2. MTIT should pursue strategy review and elaboration, and develop monitoring and evaluation mechanisms. This is in addition to implementing key legislation, policies and standards (Track 2), over a 6-12 month timeframe and put in place common e-service enablers (Track 3). The latter would require technical assistance in the form of consultation to draft the necessary policies, propose the technical standards and architectures, and draft the bidding documents. The implementation timeframe is estimated to be at least 6 months for the consultation and 12 to 18 months for implementation.

3. To facilitate the projects mentioned above, a strong and adequately staffed team in the e-government unit is essential (Track 4). MTIT should consider experienced new hires from the private sector and/or secondment of IT staff from other ministries to strengthen the unit.

The PA is at a key moment in its e-government journey. It is an opportunistic time to drive modernization of its public administration and public service delivery through use of ICT, offer better services to citizens, and promote economic growth.

# 2. Study Methodology

The methodology for this study is based on a three-step approach that consists of the following activities:

- Review of West Bank and Gaza (WB&G) e-government documents: This is to gain familiarity of previous attempts at designing and implementing e-government and to identify challenges and best practices applicable to WB&G, based on legislation, policies, standards, and infrastructure and capacity aspects.

- Stakeholder interviews: Conduct consultations with key stakeholders to gather their understanding and suggestions for implementation. This includes gathering information on the e-government enabling environment from the Ministry of Telecommunications and Information Technology, and understanding the prioritized e-government initiatives from the Ministry of National Economy, Ministry of Health, Ministry of Social Affairs, Ministry of Finance, Ministry of Justice, Ministry of Education, Ministry of Local Government, Ministry of Interior, Ministry of Transport, and the Council of Ministers.

- Time bound recommendations: Propose recommendations on e-government initiatives, based on short-term (less than 12 months) and mid-term (12 to 24 months) implementation timeframes.

# 3. E-government Enabling Environment

## 3.1 Legislation

Many Palestinian officials interviewed expressed the need for adoption of the e-Transaction Law, which specifies coverage of the e-signature legislation. The e-signature is viewed as a necessity for the implementation of e-government services. The PA's national e-government strategy also identified e-signature as the highest priority for e-government laws. This legislation has not yet been passed by the Palestinian Legislative Council (PLC) because of the PLC's limited activity in the past few years.

However, global e-government experience has shown that the lack of an e-Transaction Law (and e-signature), while considered an important foundation for e-government, should not be viewed as an impediment to e-government implementation. Many governments have implemented useful e-services in the absence of e-signature by developing citizen-centric information and redesigning e-services to eliminate the need for e-signature. For example, a driver's license e-service could be designed as follows:

- The applicant completes an application form online.
- The online form is processed by the Ministry of Transport.
- A driver's license with a handwritten signature is issued when the applicant collects the license.

In this way, e-services may be designed to avoid legislative hurdles, and citizens may benefit from the convenience brought about by an e-government program.

The right of free access to information and transparency of public information is currently not protected by legislation, because this law has also not been passed by the PLC.

Apart from the above-mentioned laws, a Privacy Act is missing and needs to be considered in the context of e-government implementation. A Privacy Act regulates the handling of personal information about individuals, including the collection, use, storage, and disclosure of personal information, and access to and correction of that information. In addition, a Cyber Crime Act has been identified by MTIT as another important law that needs to be drafted. A Cyber Crime Act would address legal issues concerning online interactions that could potentially include cybersquatting, cybersex, child pornography, identity theft, and illegal access to data.

**Proposed Actions**

- The legislation needed for e-government should be addressed as soon as possible to facilitate the implementation of transaction e-services.
- The e-Transaction Law, which is viewed as the highest priority, and the right of free access to information law, have not been passed because of the inactivity of the Legislative Council. The appropriate ministries could consider jointly making the case to the PA President to explain the situation and benefits that would arise as a result of passing these laws.
- MTIT could also work with the MOJ to initiate the drafting of the Privacy Act and Cyber Crime Law, in order to lay the legislative foundation for e-government.

## 3.2 E-government Strategy

Since 2005, the Palestinian Authority has included e-government as a national priority in all its main policy documents and strategies. The Ministerial Committee for E-government, established under the impetus of President Abbas, produced a first comprehensive e-government strategic plan in 2005. The document was part of the Palestinian Authority's vision to provide a better life for its citizens by being a government that:

- Empowers citizens to participate in government;
- Connects citizens, the private sector, and institutions to drive economic growth and meet community challenges; and
- Delivers real public value through citizen-centric government services.

This broad consideration has been kept at the heart of the PA's e-government vision and policies, and is reflected in later documents, such as the "2010 Administrative Development Plan of the Ministry of Planning," which again focused on "a public sector that provides citizens with high quality services and value for money." This plan stressed that the e-government strategy should, over time, help improve the efficiency and effectiveness of public service delivery; it also states that the MTIT has an important role to play in driving these initiatives forward.

There is a need to review and update the e-government strategy document to ensure that strategies and programs are revised according to new priorities, for example, the National Development Plan 2014-2016. In addition, an implementation master schedule should be drafted to ensure projects are better managed and monitored.

In the stakeholder discussion with MTIT, it emerged that the immediate priority for the e-government strategy has been redirected towards realizing visible benefits in the government-to-citizen (G2C) and government-to-business (G2B) domains. The purpose is to bring immediate benefits for citizens, since demonstrative content and e-services will provide concrete examples and benefits of e-government and, consequently, drive demand for such services across the public sector. The authority had focused extensively on the back-end, that is, government-to-government (G2G) services, over the past year and this effort has laid a relatively good foundation for G2C and G2B e-service implementation.

MTIT also intends to build a national e-government portal that empowers and connects citizens and delivers public value. The portal could unify all the authority's content and e-services, and enable the government to better serve Palestinians in the West Bank, Gaza, and in other countries as part of its diaspora. The national portal could be highly symbolic as the next major step toward e-government in particular, and as the first step in transforming governance. It could also be used as a vehicle to drive greater awareness, interest, and use of e-government by citizens and businesses.

In addition to a national portal, MTIT could consider working with the ministries to better utilize social media platforms to empower, connect, and deliver public value. Social media platforms, such as Facebook and YouTube, could be utilized for public service delivery with no additional investment in hardware and system software.

**Proposed Actions**

- To review and update the e-government strategy document.
- Draft a master schedule for implementation of projects.
- The implementation of a mobile-friendly Palestinian national portal is essential in achieving the e-government vision of "an efficient and effective public administration capable of delivering high quality services that concretely helps to improve peoples' lives through modern ICT solutions."
- Social media platforms could be utilized as channels for public service delivery.

### 3.3 Leadership and Organizational Capacity

There appears to be a high level of recognition across government ministries that MTIT should play a leadership role in driving the e-government agenda. From a coordination perspective, the other government ministries are relatively aware of the shared services and platforms available from MTIT that they could use to implement their e-government efforts.

Managing and implementing an e-government program spanning all of the ministries will require significant capability and capacity. While partners, vendors, and other third party entities, for example, NGOs and academia, may implement individual application projects, it will be challenging for MTIT to manage, coordinate, and implement these complex activities given the limited resources of the e-government unit. The e-government unit has an estimated five full-time equivalent staff, with several of its officers serving only 50 percent capacity as their duties straddle MTIT's IT management and e-government responsibilities.

The e-government unit staff could also benefit from more training and experience in several areas, for example, IT policy, standards, and implementation. An enhanced e-government unit is required to cover the key responsibilities of stakeholder engagement, portfolio management, ICT procurement, common infrastructure and application operations and maintenance, formulating standards and guidelines, while maintaining and mandating quality assurance and security. Skills areas, such as process reengineering, project management, infrastructure and application architecture, design, quality assurance, organizational change management, portfolio management standards and capabilities, are either largely absent or are only basic in nature within MTIT and most ministries.

Even though MTIT has a unit for e-government, the authority's ICT and e-government activities are largely driven by individual ministries with limited sharing of infrastructure, resources, applications, and talent between each other and with the MTIT. MTIT could consider operationalizing the shared infrastructure with standardized operating procedures (SOPs), and actively communicate these to the ministries with a view to educating and enticing them to participate to reap the benefits of economies of scale and scope.

**Proposed Actions**

- The Palestinian e-government program will require significant capability and capacity to manage and implement. There is inadequate staffing in the e-government unit. The unit's staff has limited training and experience in IT policy, standards and implementation know-how.
- MTIT to consider operationalizing the shared infrastructure through establishing SOPs.
- A proposed list of additional people is listed in the table below, and the needed skills and training on standards and processes may be found in Table 6.

## 3.4 Governance

The E-government Ministerial Committee, formed in 2014, should be responsible for the overall strategy, to coordinate and manage e-government budgets, integrate and redefine government policies and processes, endorse standards, and integrate schedules and plans.

Many of the ICT and e-government projects are currently funded by multilateral agencies. However, the scope of funding and sponsorship varies from project to project, and is dependent on agreement with those agencies. MTIT could define a clear strategy and governance structure to drive and manage the funding and sponsorship needed by e-government and other ICT projects, develop an e-government portfolio to have clear oversight on all upcoming and ongoing projects, and carefully monitor these engagements to prevent wastage of funds from potential scope-of-work overlaps.

Insufficient governance has led to funding agencies and sponsoring firms frequently driving their strategy, technical solutions, and implementation in siloes. The situation is accentuated by the development grants and loans from multilateral and bilateral agencies, which mostly work independently. The agencies usually attempt to develop end-to-end capacity and capability to avoid constraints, regardless of the availability of central or common ICT infrastructure. This naturally results in wastage of financial resources because of duplication, repetition, or redundancies. It is not uncommon for individual ministries' product and technology selection, as well infrastructure architectures, to be largely driven by the funding agency or sponsoring firm. This has often resulted in the deployment of systems that are difficult to interoperate with other governmental systems, and are cumbersome to enhance or scale for whole-of-government adoption.

**Proposed Actions**

- For the governance structure to be deemed effective, clear oversight on all e-government projects is needed to facilitate better coordination of grants and loans from multilateral and bilateral agencies.
- MTIT needs to work with the ministries and their funding agencies to formulate the requirements and design the system or e-service while leveraging the available common infrastructure, such as the Government Computer Center and X-Road.

## 3.5 Policies

Defining and adopting policies are essential for implementing e-government projects. These policies would typically cover the areas of information security, IT service management, public records, information access and protocols, interoperability and integration, e-governance workflow, and IT governance. Such policies will help streamline the adoption of ICT within the government, and implementing these policies will also serve to better enhance citizen experience and improve the adoption of e-government initiatives.

With regard to e-government policies, the PA's e-government policy document was developed by MTIT with the support of the OECD in 2011. Based on the findings of the OECD's report *Modernizing the Public Administration: The Case of E-government in the Palestinian Authority*, the policy document calls for a digital administration that is regulated, seamless and reliable, supportive, and accessible and ubiquitous. These are

important aspects of e-government policy, although they appear to be predominantly focused on addressing the administration reform process.

The current policy document does not extend to technology-related aspects, such as sharing IT infrastructure, public key infrastructure (PKI), digital security, and information security. Policies related to electronic service delivery and for e-payments would also be necessary considerations to advance e-government implementation. E-governance management policies, including procurement, budget, and public-private partnerships, also need to be considered. These aspects are outlined below.

### *3.5.1 Technology-Related Policies*

Shared IT Infrastructure Policy

Policy should spell out clearly the guidelines and standards to be adopted for building and operating data centers, including primary data centers and disaster recovery centers. Ministries could be mandated to deploy or migrate their ministry-specific applications in these shared data centers as soon as they are available.

A cloud computing architecture also needs to be set out clearly. Adoption of a cloud-based infrastructure model has the potential to speed up the delivery of e-services, and optimize ICT investment by the government. Policy should also provide clear guidelines on cloud directory and publication of services, criteria definition for adoption of various cloud models (IAAS, PAAS and SAAS), scaling of cloud, connectivity to the cloud infrastructure, securing the government cloud, and charge-back models for building and operating the cloud.

e-Security and PKI Policy

Policy should cover the promotion of e-signatures for the purpose of authentication and non-repudiation in e-government, establishing legal validity for signing forms electronically, set up of certifying authorities' (CA) organizational structure to promote and regulate e-signature adoption, ensuring interoperability between e-signature certificates issued by different CAs, and providing clear guidelines on usage and procurement of digital certificates for e-government projects.

Information Security Policy

E-government initiatives are built by integrating technology and services from various providers. These include software vendors, data center facility providers, network service providers, original equipment manufacturers, IT service providers, and so on. The development and operation of these programs are carried out by people from diverse organizations, often spread across multiple geographies. In order to secure all aspects of e-government, an information security policy providing clear guidelines on securing all aspects of an e-government service to ensure confidentiality, integrity, and availability of the e-services should be adopted with key risks identified at the outset. This should be accompanied by risk mitigation plans, and application of technology controls in accordance with policies and procedures.

### *3.5.2. Electronic Service Delivery Related Policies*

Mandatory Electronic Service Delivery Policy

Policy should provide actionable and concrete guidelines on how PA ministries should ensure the enablement of their services into electronic versions. The focus should not be simply on automation, but also on process reengineering, simplification of processes and forms, reduction in approval levels and time cycles, electronic payments, online status tracking, service level agreements (SLA) on response time, and to ensure that electronic delivery of services is a mandatory public service offering by the respective ministries.

Multichannel Access Enablement Policy

Policy should aim to provide actionable and concrete guidelines on how to enable G2C and G2B services over different access channels – web, mobile devices, one-stop centers at the postal office, walk-in centers at government offices, and so on. The emphasis should be on moving away from a ministry-centric silo approach to a "one government" mode of service delivery.

e-Payment Policy

Many e-services require an e-payment solution. Policy should enable online receipt of payments from citizens, investors, and businesses and their routing and disbursement to various partner departments. Policy should provide guidelines on setting up and operating electronic payment gateways, the types of payment that needs to be supported, accounting and reconciliation procedures in government departments to account for funds received through electronic channels, and associated dispute-handling mechanisms. Such a policy could jointly be developed by the Central Bank, MTIT, and other ministries that will facilitate electronic payments.

### *3.5.3 E-Governance Management Policies*

Procurement Policy

Policy could provide guidelines on how hardware, software, and ICT services should be procured in a public tendering process. It should also provide guidelines on how ministries should prepare, evaluate, and award e-government related tenders, requests for information (RFI), requests for proposals (RFP), and request for quotations (RFQ), in collaboration with MTIT's subject experts.

E-government Budgetary Allocations Policy

Policy should provide guidelines on how much budgetary allocation should be made available for e-government projects for each ministry, and how the ministry should utilize the budget. Policy should also provide guidelines on charge-back models, that is, payments made by various ministries to MTIT for using common infrastructure.

Public-Private Partnership policy for ICT

Many successful e-government initiatives across the world are built and operated on a public-private partnership (PPP) model. Private sector involvement brings in management and technology expertise, and raises quality. It also helps to reduce financial and operational risks. If the PA decides to adopt a PPP approach towards implementing e-government projects, clear guidelines would be needed on the role of commercial entities. PA would also need to specify controls to ensure that national security of ICT assets would be retained, while commercial entities build and operate the services.

### *3.5.4 Quality Assurance Policies*

E-government projects are built by leveraging and integrating different technology components with changes in government processes. Clear guidelines are essential on how different aspects of the ICT system or e-service should be verified to conform to expectations in a standards compliant manner. Aspects that should be verified include functionality, performance and scalability, security, usability, conformance to standards, and documentation quality.

## 3.6 Standards

IT standards play an important and integral part in facilitating the choice and adoption of technologies. A standards-based approach towards e-government implementation would facilitate revision in choices in response to changes in market and technology conditions. It is imperative that an internationally proven standards framework is adopted when building e-government systems, as its services include mission critical public service delivery systems which impact a high number and wide variety of stakeholders.

A standards-based approach should not only be restricted to technology, but it should be adopted across all aspects and phases of e-government initiatives. Some of the well-known and internationally accepted standards used in e-government initiatives across the world are listed in Annex B on standards. These could be considered for adoption by WB&G for its e-government projects.

Governmental entities also need to adopt a set of agreed standards to exchange data messages, in order to facilitate the data exchange between e-government systems and services. MTIT has successfully implemented the Palestinian e-government interoperability framework, named Zinnar, as illustrated in Figure 1. Zinnar aims to establish the necessary foundation for the interoperation of heterogeneous information systems in the different governmental ministries in WB&G. Zinnar was accredited by the cabinet in March 2013, and an interoperability framework national team comprising 17 members across different ministries was formed to ensure interoperability between the different ministries and institutions in accordance with the standards and norms listed in Zinnar. However, the team appears to have ceased to function because of funding challenges.

Zinnar consists of five components:

i. Ontology Server: Contains an accurate description of the data exchanged in e-government services.

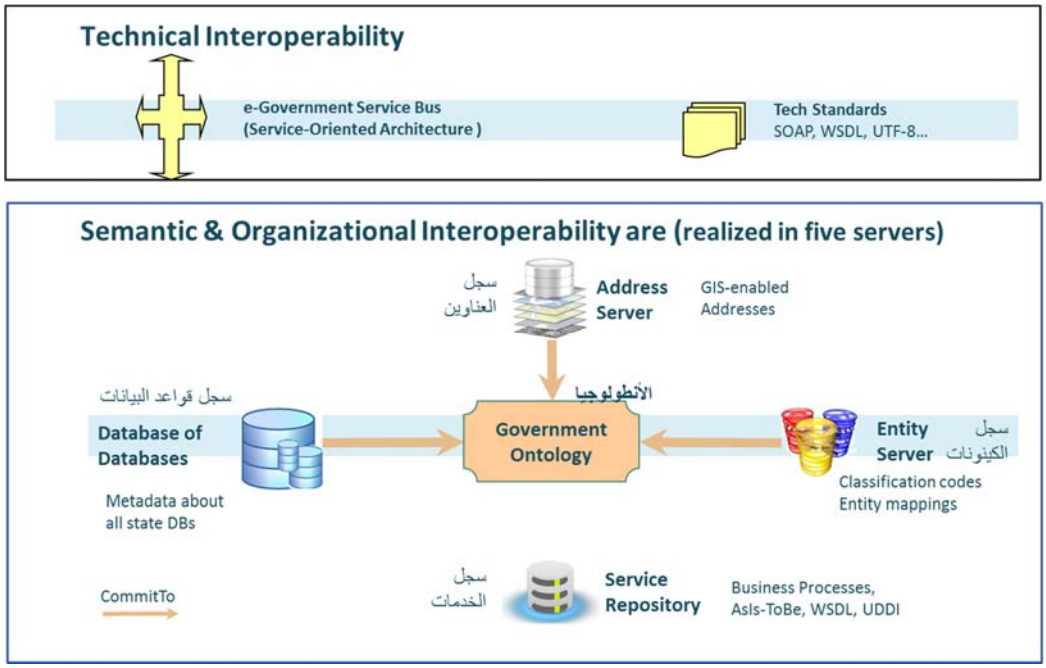
ii. Entity Server: Provides standard entity classifications that must be used when exchanging data messages.

iii. Address Server: A repository of addresses that would contain all the addressing information.

iv. Service Repository: Contains information about all the services provided by the PA's institutions (metadata, detailed description, repository).

v. Database of Databases (DoD): Contains information about all the services provided by the Palestinian government institutions.

**Figure 1. Zinnar – Palestinian E-government Interoperability Framework**




Beyond the establishment of Zinnar for interoperability purposes, there appears to be a lack of established standards in all other areas. These areas include technology and architecture, for example, enterprise architecture, IT service management, and risk assessment frameworks. There also does not appear to be standards established for e-government workflow and documentation. No software development standards are established for IT governance, project management, and software development lifecycle model. Annex C – Standards, details indicate the IT standards that MTIT could consider in the course of its e-government implementation.

**Proposed Actions**

- Given that X-Road and Zinnar are in place and cloud infrastructure will be made available in 2016, MTIT should consider introducing a shared IT infrastructure

policy to facilitate the adoption of these shared infrastructure across the whole-of-government.

- The Information Security Policy e-Security and PKI policies are two other critical policies to be drafted to safeguard the confidentiality, integrity, and availability of the online information and e-services.
- The e-government unit's staff should be adequately trained in project management skills, so as to ensure upcoming e-government projects are well managed.

## 3.7 Infrastructure

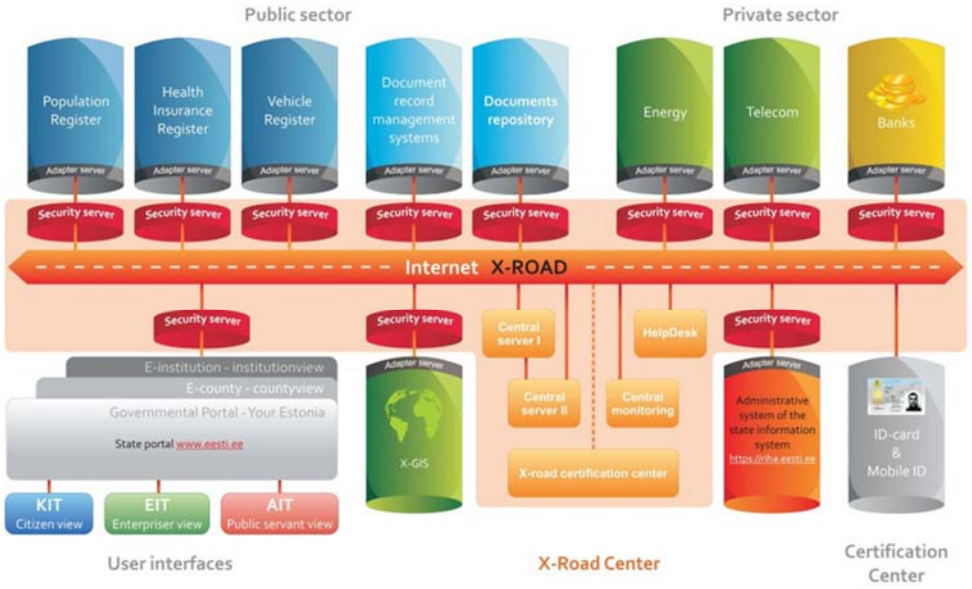
Stakeholder interviews and secondary sources show that the PA already enjoys a commendable technological infrastructure: a government network through which all ministries are currently connected to the Government Computer Center. MTIT is planning to virtualize the center by the end of 2015, and aims to move the data center onto a private government cloud setup by 2016.

A disaster recovery site for the Government Computer Center is also needed but is not currently available. In the case of an emergency or any situation that mandates the shutting down of the center, there would be no backup and continuity, putting some critical government services at risk. A business continuity plan also appears to be absent.

An IT service management framework (ITSM) for deployment is also lacking. The study did not reveal the existence of robust operating procedures for IT service management (such as adoption of ITIL standards) in order to plan, design, and operate all aspects of IT services delivery.

MTIT, with the support of the Estonian government, has put in place X-Road, which is a platform to facilitate data exchange between different databases and information systems. MTIT is currently conducting pilot programs with nine ministries to utilize X-Road to facilitate data exchange between them. The pilots include the provision of a citizen registry for the Ministry of the Interior, and a births and deaths registry for the Ministry of Health, for data exchanges. Technical details on X-Road may be found in Appendix D.

**Figure 2. Layered Structure for X-Road**




To facilitate the development of e-services, the approach of undertaking a "build once, reuse always" for common e-service enablers is important. Common e-service enablers such as e-signature, citizen e-authentication, and e-payments are necessary but have yet to be established in WB&G from the policy, technical, and operational perspectives.

**Proposed Actions**

- A whole-of-government ICT application infrastructure to complement the Government Computer Center's hosting services, will enable ministries under PA to develop and deploy their e-services and mobile applications in a cost-effective and rapid manner.
- Such shared application infrastructure provides common enablers needed by most e-services. The common e-service enablers could include citizen authentication, enterprise authentication, content management, electronic payment services, data services, notification services, etc.

# 4. E-government Services and E-government in Gaza

## 4.1 Government-to-Government

Several shared Government-to-Government [G2G] systems are available throughout all ministries. These include an e-mail platform and ministry websites provided by the MTIT, and financial, HR applications, and payroll system provided by the Ministry of Finance. Various ministries are also currently implementing several other initiatives, including:

- The Ministry of Justice (MOJ) is connecting all its courts and will provide them with a complete case management system to automate their processes. MOJ has also setup a Justice Information Center, in order to facilitate citizens' access to legal information. Additionally MOJ has a Document Management Archive System, which automates its five departments; namely arbitration, complaint, endorsement, translation, and archiving.

- The Ministry of Social Affairs (MOSA) has started the process of automating its programs and has built an Internet presence, which provides program information on cash transfers, emergency assistance, orphans, disability, economic empowerment for the disabled, custom exemption for people with disabilities, and so on.

- The Ministry of Education (MOE), in collaboration with the MTIT, has connected many schools to the Internet. MOE is working on a network for all school management information system.

- The Ministry of Finance (MOF), is developing the electronic workflow of documents to allow greater accountability and transparency of all of the procedures related to the payment of current and former public employees (payroll and pensions). The new system will allow all public employees access, through the website, to their personal information.

- The Ministry of Health (MOH) is developing its Health Information System (HIS), which aims to standardize patient administration and management procedures across hospitals and primary health care centers. Patient information will be made more accessible to health care professionals through improved handling of medical records. The HIS will also be critical to developing new health standards by setting up new protocols, new guidelines and monitoring systems.

- The Ministry of Interior (MOI) has implemented the citizen identification number database, which is connected and used by many ministries for citizen identification prior to service delivery.

- The Ministry of Local Government (MOLG) has carried out a study to compile a list of priority services to be digitized at the municipality level.

- The Council of Ministers Cabinet Secretariat is preparing an electronic compliance system for its unit of complaints at the secretariat, and the units of complaints at the Palestinian ministries.

- The Ministry of National Economy (MONE) aims to implement an online company registration system that would enable applicants to register a company online and track registration. The system would cover name checking and reservations. The applicant would be able to conduct an online search to ensure the proposed company name was not currently in use, following which the user would be able to reserve the name for the ministry's approval. Once the name has been approved, the applicant would be able to do online filing for the company. A company registration certificate could also be generated electronically as a PDF document sent to the applicant via email.

## 4.2 Government-to-Citizen/Government-to-Business

A high-level assessment of the e-service maturity and implementation priorities of various PA ministries' was conducted with the Director Generals and/or the Head of IT departments of the Ministry of Justice (MOJ), the Ministry of Interior (MOI), the Ministry of Education (MOE), the Ministry of National Economy (MONE), the Ministry of Health (MOH), the Ministry of Local Government (MOLG), the Ministry of Foreign Affairs (MOF), the Ministry of Social Affairs (MOSA), the Ministry of Transportation (MOT) and the Council of Ministers in West Bank **.** In general, ministries have largely focused on establishing ministry-specific information, while MTIT has focused on implementing a G2G infrastructure, such as the Government Computer Center, Zinnar, and X-Road.

A handful of ministries in the West Bank have started to publish citizen-centric information online, for example, guidelines on transacting public services on their websites. They have not embarked on e-service implementation owing to in the legislation issues, for instance, the failure to pass the e-Transaction Law, as well as the lack of common e-service enablers such as e-payment and online citizen authentication. There is currently no national portal to provide a single window for all government information and services to Palestinian citizens. In addition, there is no mobile service available to citizens.

## 4.3 E-government in Gaza

Owing to access restrictions, assessment of the status of e-government in Gaza solely relied on a secondary document, E-government *Project - Current Status*.

In Gaza, common enablers for e-government services, such as single sign-on and e-payment, have been implemented. In 2014 there were 40,546 employees and 131,266 citizens using single sign-on for e-government services. With regard to e-payment, direct debit and electronic stamps are available and 53,884 transactions had been made on the e-payment system by 2014.

An e-portal for government e-services has been established in Gaza, as illustrated in Figure 4, and 53 e-services had been implemented by 2014. The e-portal is available on the Internet, and on smartphones via Android and iPhone operating systems.

**Figure 3. E-portal for Government E-services in Gaza**


*Source*: ww.eportal.gov.ps.

Smartphone applications have also been developed in Gaza. These include the Government Data Application, which provides a service for government personnel to inquire about government e-services. The WB&G Government Portal App, designed for citizens, also provides access to various content and e-services.

**Proposed Actions**

- MTIT should also focus on a two-phase implementation approach for the portal. Phase 1 should consist of delivering citizen-centric information to provide higher clarity about various government services.
- Phase 2 could consist of e-service implementations that require the usage of common e-service enablers; such as online citizen authentication, e-signature, and e-payments.
- Instead of developing a new portal, MTIT could consider scaling the e-portal implemented by the Gaza e-government team to incorporate content and e-services needed by Palestinians in West Bank and the diaspora.
- MTIT should involve the citizens to help co-design the national portal and e-services, so as to better align with the citizen's needs and expectations.
- Prioritized G2C and G2B e-services can be found on tables 5 and 6.

## 5. Recommendations

Recommendations are divided into four concurrent tracks described below. While there are many barriers towards the implementation of e-government, MTIT can deliver visible e-government success by focusing its attention on developing citizen-facing deliverables in the form of a Palestinian National Portal, as described in Track 1. This track focuses on the delivery of quality information and services for the citizens and businesses. A Palestinian National Portal, with an e-government on social media sub-program, would require technical assistance for consultation, for an estimated period of four months, and portal implementation, for a period of 12 to 18 months, through open tender. MTIT should involve the citizens to help co-design the National Portal and e-services so as to better align with the citizen's needs and expectations. MTIT could organize various types of sessions with citizens and businesses to tap on their creativity; such as brainstorming, hackathons, boot camps, etc. These sessions should also be sufficiently focused on the disenfranchised sections of the population; such as citizen who are rural, less educated, disabled, etc.

To pave the way for end-to-end e-transactions with authentication, e-payments, and e-signature, MTIT should pursue strategy review, legislation, policies and standards, as described under Track 2, over a 6-12 month timeframe, and put in place common e-service enablers, as described under Track 3. The latter would require technical assistance in the form of consultation to draft the necessary policies, propose the technical standards and architectures, and draft the bidding documents. The implementation timeframe is estimated to be at least 6 months for the consultation and 12 to 18 months for implementation.

To facilitate the projects mentioned above, a strong and adequately staffed team in the E-government Unit is essential. MTIT should consider experienced new hires from the private sector and/or secondment of IT staff from other ministries to strengthen the unit.

| Track | Project Name | Timeframe |
|---|---|---|
| 1 | **Palestinian National Portal**<br>Technical Assistance Consultancy<br><br>Portal Implementation | <br>4 – 6 months<br><br>12-18 months |
| 2 | **Strategy, Legislation, Policies and Standards**<br>Technical Assistance Consultancy on E-government Strategy<br><br>Passing of Legislations<br><br>Technical Assistance on Policies and Standards | <br>6 months<br><br>6 - 12 months<br><br>6 months |
| 3 | **Common e-Service Enablers** | |

| | | |
|---|---|---|
| | Technical Assistance Consultancy on e-Service Enablers<br><br>Common e-Service Deployment | 6 months<br><br>12-18 months |
| 4 | **E-government Unit** | 6-12 months |

The involvement of the private sector in the e-government program would be key. MTIT should tap on the academia's and ICT industry's experience and expertise, and involve them for the provision of infrastructure and e-services through open tenders.

### 5.1 Track 1: Palestinian National Portal

To achieve the e-government vision of "an efficient and effective public administration capable of delivering high quality services that concretely helps to improve peoples' lives through modern ICT solutions," it would be instrumental to have a mobile-friendly Palestinian National Portal to serve as the service delivery platform. In addition, the usage of the national portal could also be seen as a strong signal and commitment of the PA's new effort towards e-government, and used widely for communication purposes.

The Palestinians could utilize their mobile devices to access a "one-stop shop" acting as a convenient online venue for people to remember, where all government-related information and services might be found. Palestinians could receive news and positive messages from PA, hence creating a digital bridge to foster bonding. Palestinians could also use the portal as a feedback channel, where users could provide comments and suggestions on policies, processes, and transactions affecting their daily lives. The portal needs to facilitate faster access to information and services and offer an easier way to find the information and services citizens want through a well-developed navigation structure and easy-to-use search tool. The portal would ease the lives of Palestinians, because users would not be required to travel to a government office during specified office hours, unless the nature of the service is not appropriate for delivery via the portal. Users would be able to access services at any time, from anywhere through multiple devices. To encourage citizens to co-design e-services, the National Portal could serve as the central open data repository to the government's publicly-available data.

For Palestinian businesses, the portal could be an "online showcase center," where Palestinian businesses could demonstrate their products and services to the international business community, to promote economic opportunities. The portal could also provide "partnership sourcing," where investors, international traders, and firms could source business ventures and partnerships with Palestinian businesses.

For the PA, the portal could serve as marketing and branding tool to frame a more positive perception by the media. The portal should also be a "national communications platform," which ministries could utilize to communicate and engage with citizens and businesses community. Ministries could also gather user feedback via the portal (integrated with the feedback system currently planned by the Council of Ministers). The

portal governance structure comprising representatives from various ministries and institutions would be a key forum to review the feedback, respond with resolutions, and develop future phases of user-focused services.

In terms of implementation, PA should "Think Big, Start Small, and Scale Fast." The portal vision should be broad and inspiring. Implementation should be undertaken in small logical arrangements, both to reduce big mistakes and cater for rapid advances in technology. As the portal is scaled in terms of capability and infrastructure components, the vision and the strategies should be continually reviewed and the development plan amended as necessary. In addition, the implementation team should learn and revise, as this would be PA's first foray into developing a portal of such significance. There could be regulatory, policy, and process blind spots. Having the structure and flexibility to learn, improvise, and implement is essential.

The portal implementation team should also focus on putting the user at the center of its universe. It should offer a wide array of user capabilities, cultivating rather than forcing use, and treating value for users as the top priority. The benefits for the country, the PA, citizens, and businesses can only be realized by addressing user needs first.

*Meeting rapid changes in user expectations.* The portal's users may expect websites to provide interaction and connection, in addition to just information. Users may also expect interactions to occur between themselves and the PA, where they can provide feedback on hard-to-understand regulations, confusing policies, and unclear processes. Users also expect such portals to provide connection capability, where like-minded users could seek out each other to form partnership or alliances.

*Putting the user at the center.* This is more than just a priority principle; as there are also social design and technical architectural considerations. Many users already have web identities and presences, for example, there were 966,960 Palestinian Facebook users in December 2012[1] Users are usually attached to their existing web identities and associated networks and commercial portals. Therefore it would be logical for the portal to consider leveraging social profiles from these social networking portals for login authentication, for example, Facebook, Twitter, or LinkedIn could be used for login.

*Mobilize the portal.* Mobile access to the portal cannot be an afterthought. Many portal implementations focus on providing portal access first through a desktop or laptop-based Internet browser, then devising a catch-up strategy for mobile access. This would result in a poorly planned and developed mobile portal solution.

*Farming approach.* The project team must incorporate a mobile strategy into the planning and governance at the outset of the portal's program. User-centric portals are transforming the way governments govern, deploy, and manage portal deployments. Traditionally, governments form a governance structure, create a vision, define objectives, policies, priorities and key performance metrics, and delegate responsibilities

[1] Source – www.InternetWorldStats.com

for portal management. The portal is subsequently implemented in structured phases with ongoing monitoring of its use and performance over time. The traditional lore holds that a deliberate and meticulously planned approach is necessary for portal success. However, the "build it and they will come" belief has a place in an evolved portal strategy. While governance and planning are still vitally important, governments are not able to predict completely the local and international business communities' response to their portal implementations.

Rather than forcing users down a certain path of design or usage, the PA should provide an adaptive environment that fosters collaboration and creativity, and let users discover its purpose for themselves. PA should consider the establishment of a steering committee to push for the adoption of a farming approach, whereby officials identify, cultivate, and promote product use of the portal, while weeding out problems and addressing risks.

MTIT should also focus on a two-phase implementation approach for the portal. Phase 1 should consist of delivering citizen-centric information to address confusion or lack of clarity about various government services. In addition, providing frequently asked questions (FAQs) for services, and "how-to-apply" guides that should be drafted in a step-by-step sequence using easy to understand language, would greatly benefit citizens. This phase could also include three or four in-demand e-services, for example, application for driving licenses, and for non-convicted persons. Phase 2 could consist of e-service implementations that require the usage of common e-service enablers, such as online citizen authentication, e-signature, and e-payments.

Instead of developing a new portal, MTIT could consider scaling the e-portal implemented by the Gaza e-government team to incorporate content and e-services needed by Palestinians in the West Bank and the diaspora. If this option is deemed inappropriate, a new portal could be conceptualized through technical assistance for consultation, with consideration placed on cross-referencing content and services from both portals to provide convenience to the users.

Tables 5 and 6 provide a list of prioritized content and services from various ministries, gathered during the stakeholder interviews and from the list of prioritized e-government services identified by USAID. This could serve as a starter list for content to be published in Phase 1 of the portal's implementation. The full list may be found in Appendix C.

**Table 1.Content and Services: G2C**

| Ministry | G2C Content and e-Services |
|---|---|
| Ministry of Justice | Endorsement e-services that certifies someone to act on behalf of another person to conduct a certain task. Application for Non Convicted Person, which is necessary for job applications, university applications and for membership application into business associations and organizations. |
| Ministry of Interior | Application for birth certificate, application for death certificate, application for a new passport and to renew passport. |
| Ministry of Health | Mobile services for an appointment to see a doctor, vaccination reminders, emergency health texts to alert for epidemics, and health insurance validation (public health insurance). |
| Ministry of Education | Linkage to the e-Learning Portal, Scholarship Application and the e-School website. |
| Ministry of Finance | Property tax payment and fees. |
| Ministry of Social Affairs | Application for social support for new born, disabled, death, health insurance, food supply, waiving school fees, and cash transfer. |
| Ministry of Local Government | Request for e-statement of account, which indicates the applicant's status on any outstanding fees owed to the government. |
| Ministry of Transport | Application for driving license.<br><br>Traffic advisory services for accidents, traffic jam alerts, and traffic awareness. |
| Council of Ministers | Complains and feedback service for whole-of-government. |

**Table 2. Content and Services: G2B**

| Ministry | G2B Content and e-Services |
|---|---|
| Ministry of National Economy | Online company registration which enables the applicant to register company online and track registration issuing steps which covers the following<br>– Name check and reservation. The applicant can conduct an online search to ensure the proposed company name is not currently used, following which the user can reserve the name for the ministry's approval.<br>– Once the name has been approved, the applicant is able to do online filing for the company.<br>– Company registration certificate could be generated electronically as a PDF document sent to the applicant via email.<br>Trademark information, search for trademarks and online registration form to apply for trademark.<br>An e-objection service, which enables applicants to object to registrations, e.g. company and trademark.<br>Factory set-up registration form, Certificate of Origin form, import license form, trader registration form. |
| Ministry of Transport | Vehicle registration services include<br>• Dealership for new vehicles;<br>• Personal import for used vehicles; and<br>• Company import for used vehicles. |
| Ministry of Health | Application for health-related professionals, e.g. doctors and pharmacists.<br>Application to setup healthcare services, e.g. clinics, NGO healthcare centers and hospitals. |
| Ministry of Local Government | Application for building-related licenses. |

### *5.1.1 Sub-Track: E-government on Social Media*

Government ministries cannot afford to ignore the social media channels that citizens depend on. Citizens globally are increasingly adopting social media, and increasingly have pervasive access to mobile and broadband. Instead of a "go to where the-government is" approach, a "go to where the citizen is" approach via social media could further heighten the success of the PA's effort to provide services to its citizens.

There is significant potential to leverage social media platforms such as Facebook to support the delivery of e-government services to the Palestinians. According to *Internet World Stats*, there were 1,687,739 Palestinian Internet users in December 2014 at 60.6 percent penetration, and 966,960 Facebook users in December 2012, at 36.9% penetration.

Few ministries are currently taking full advantage of the new opportunities that social media offers. Some of the challenges they face are a lack of manpower or resources to implement programs, the frustration of having to handle social media interactions manually, and difficulty in making appropriate use of the information they find. In addition, some see social media as just a one-way broadcast channel, and ignore the potential for citizen engagement and mutual collaboration.

However, ministries such as MTIT (see Figure 5) and MOH (see Figure 6) are successfully utilizing Facebook by clearly identifying objectives, building processes, and integrating social media capabilities. Organizations that are face time and resource constraints may also find that social media channels can help to stretch their resources, by helping them to communicate effectively with a wide range of citizens and businesses.

**Figure 4. MTIT Facebook Page**


**Figure 5. MOH Facebook Page**


Ministries responsible for public safety also find that the real-time nature of social media can be invaluable in times of crisis. The bottom line is that ministries that listen carefully and interact in the social sphere can build trust, broaden constituent participation, and

better align services to citizen needs. Thus, MTIT could work with the ministries to embark on the following:

*i.* *Improving efficiency and reducing costs.* Social media offers a powerful and cost-effective channel for ministries to interact with their constituents. As such, it is relatively valuable for resource-constrained ministries that must provide consistent services with fixed or shrinking budgets. Ministries could, for example, use social media to post regular updates about the ministry's services to Twitter and Facebook. They could also create a YouTube channel with videos explaining the steps for a particular service, on how to form fill, the types of documents to attach, and the expected duration needed for application processing.

These simple steps could address many common questions and help citizens avoid making time-consuming mistakes, while also deflecting a large number of incoming queries and calls, and speeding the delivery of services to citizens not previously familiar with the service in need.

*ii.* *Improving trust in government.* Social media can increase transparency in government and help humanize otherwise opaque institutions. Where appropriate, using an employee's name on blogs or Twitter accounts can add a human face to government ministries. For local governments in particular, such a personalized touch can help to build essential trust that supports future budgets and funding. Beyond the one-way broadcast information, local governments could also use social media to respond in real time to citizen inquiries and complaints, and earn citizen's trust through better responsiveness.

*iii.* *Improving service to constituents.* Ministries could use social media to improve services to citizens by proactively reaching out to individuals on social media, to let them know about services or programs. By garnering feedback in the social sphere, ministries could take steps to better align services or programs to citizen needs.

*iv.* *Engaging citizens in collaborative government.* Social media brings new meaning to "government by the people and for the people" by making it easier for ordinary citizens to participate in meaningful ways with ministries that represent and serve them. Citizens who are not comfortable with searching for the relevant representative to discuss their issues or concerns, or calling representatives in person, may be more comfortable with posting their comment or suggestion on a social network

*v.* *Crisis response.* Social media can be a powerful tool in times of crisis. Ministries can both disseminate critical information to citizens in real time, and receive important new information from citizens. Ministries can also take the lead in addressing any misinformation that could put public safety or security at risk, by listening and responding to public sentiment.

### 5.2 Track 2: Strategy, Legislation, Policies and Standards

The e-government strategy requires review and update to align with the current national priorities. The current strategy also needs to be elaborated, and an actionable roadmap needs to be developed to implement the strategy. PA could also develop key performance

objectives and measurement mechanisms to help ensure that the strategy is meeting its goals and advancing towards the target.

Cloud hosting could also be an integral part of the strategy, given that MTITI currently does not have a backup/disaster recovery position, and the wide geographic spread of Palestinians. Cloud hosting could provide PA with continuity of operation and access to support different scenarios when access becomes challenging.

MTIT should also consult with stakeholders across the government in its efforts to renew the strategy; and co-create with citizens through various channels, such as focus group sessions, hackathons, etc.

The legislation needed for e-government should be addressed immediately. The e-Transaction Law, which is viewed as the highest priority, and the right of free access to information law, have not been passed because of the inactivity of the Legislative Council. The appropriate ministries could consider jointly making the case to the PA President to explain the situation and benefits that would arise as a result of passing these laws. Table 3 summarizes the legislation and actions needed.

**Table 3. Summary of Legislation and Action Needed**

| S/N | Legislation | Action |
|---|---|---|
| 01 | e-Transaction Law | Seek passage of the law |
| 02 | The Right of Free Access to Information Law | Seek passage of the law |

MTIT should also examine the technology related policies such as those concerned with electronic service delivery, e-government management, and quality assurance. The prioritized policies to facilitate a secure e-service delivery platform for citizen-centric transactional services are listed in the Table 4.

**Table 4. Prioritized Policies for E-government**

| S/N | Policy | Action |
|---|---|---|
| 01 | Shared IT Infrastructure Policy | Draft the policy |
| 02 | Information Security Policy | Draft the policy |
| 03 | e-Security and PKI Policy | Draft the policy |

It is also essential for internationally proven standards to be adopted when designing and building e-government services, as they include mission critical public service delivery systems which impact a high number and wide variety of stakeholders. The prioritized standard to facilitate a secure e-service delivery platform for transactional services are

listed in Table 5. Appendix B provides a list of other standards that could be considered for eventual implementation.

**Table 5. Prioritized Standards for E-government**

| S/N | Standard Category | Suggested Standards |
|---|---|---|
| 01 | Project Management Skills | e.g. PMBOK Guide and Standards |

## 5.3 Track 3: Common e-Service Enablers

A whole-of-government ICT application infrastructure to complement the Government Computer Center's hosting services will enable ministries under PA to develop and deploy their e-services and mobile applications in a cost-effective and rapid manner. Such shared application infrastructure provides common enablers needed by most e-services. The common e-service enablers could include citizen authentication, enterprise authentication, content management, electronic payment services, data services, notification services, and so on.

PA ministries could also benefit from lower operating costs through economies of scale and at the same time be assured of ICT system availability through a central application infrastructure. PA ministries do not need to invest in their own e-service infrastructure but instead could develop and deploy their e-services and mobile applications on the shared e-service application infrastructure. The application infrastructure could also be provided to the public sector ministries on a utility model, where ministries only need to pay for the shared e-service enabler(s).

The PA's X-Road could serve as a de facto shared e-service interoperability platform, which could be scaled into an application infrastructure platform. X-Road could go far beyond its existing interoperability capabilities by incorporating the following common e-service enablers to facilitate the publishing of content and development of e-services:

### *5.3.1 Digital Signature*

An e-signature is an author identification and verification mechanism used in an electronic system. This could be a scan of a real hand-written signature, or any kind of electronic authenticity stamp. It is a generic term that covers various authenticity measures. An e-signature is also the electronic equivalent of a handwritten signature. e-signatures have appealed to governments and businesses around the world for the following reasons:

- Accelerated transactions: The requirement for handwritten signatures often results in lengthy delays in transactions. e-signatures make possible long-distance transactions, in which parties may be in different time zones or in different countries. In addition, digital signature greatly reduces the amount of travel for in-person meetings, the cost of courier service, and the number of days and salaried hours needed to complete transactions.

- Reduction in the amount of paper: Many governments and organizations still seek "the paperless office" because of the desire to cut down on the time, staffing, and storage space required to handle paper-based transactions.

A digital signature is a type of electronic signature. It refers to the encryption and decryption technology used as the foundation for a variety of security implementations. Based on public and private key cryptography, digital signatures are used in secure messaging, public key infrastructure, virtual private networks, and electronic signatures. Contrary to what the name might suggest, a digital signature alone is not a type of electronic signature. Rather, digital signature encryption can and should be used by electronic signature applications to secure the data and verify the authenticity of a signed record. A digital signature alone also does not capture a person's intent to sign a document, and be legally bound to an agreement or contract.

The most full-featured and, arguably, the most secure type of e-signature, relies on public-key cryptography to authenticate identity. Public key cryptography involves a pair of mathematically related keys:

- The "private key," known only by the signer, can be used to sign a message that only the corresponding "public key" holder can verify.

- The public and private keys are large, randomly generated prime numbers, and it is computationally infeasible to distinguish one from the other. By issuing and managing public and private keys, public key infrastructure (PKI) enables strong authentication, integrity, and nonrepudiation.

- Because the crypto functions bind mathematically with a hash (a unique representation) of the document, any change negates the signature (the hash of the document being the document encoded with a one-way hash algorithm).

PKI could also provide a higher level of assurance of signer identity and authentication, as a certification authority vouches for the certificate holder. The primary risk related to a digital signature is the compromise of the private key.

### *5.3.2 Online Citizen Authentication*

The purpose of online citizen authentication is for PA ministries to provide a trusted domain for digital transactions that is convenient for access to public services by citizens anytime, from anywhere, on any device, or through any online channel, such as online access via the Web and mobile devices. Authentication is a real-time process of corroborating a claimed digital identity, yielding a specified or understood level of confidence. This trust is established by a combination of identity proofing and identity creation:

- Identity proofing involves the corroboration of real-world identity prior to digital identity creation. Identity proofing can be done through in-person presentment, or through different online methods.

- A digital identity is created for a citizen (a person with a real-world, civil identity) when some information corresponding to something uniquely possessed by this citizen is associated with, and is bound to, that digital identity, so that that identity can subsequently be used for authentication to systems.

Citizens could authenticate by providing some evidence for proof of possession (typically derived from the thing possessed), and an authentication service verifies that evidence, based on the corresponding information bound to the citizen's digital identity.

Authentication is typically seen as a "gateway event," something that happens only at login to a particular device, system, or domain. However, this is changing. Increasingly, governments are recognizing a need for post login "step-up" authentication, or trust elevation, when a citizen attempts a high-risk action or high-value financial transaction.

How citizens authenticate online, and the technical methods employed, are other critical pieces. The traditional username-password approach is subjected to a variety of cyber hacks and attacks. Online citizen authentication must be secure, flexible, and interoperable and it may need to factor multi-authentication methods when appropriate. For example, if PA wants to offer citizens secure access to a website on tax matters for sensitive data such as individual tax records, a higher identity assurance should be required. PA may need to consider incorporating a one-time password (OTP)-based mechanism in addition to the initial user e-ID password entry.

MTIT could evaluate and possibly leverage the online authentication mechanism in the “single sign on” module implemented by the Gaza e-government team, in order to avoid duplication of effort.

### *5.3.3 e-Payment*

Increasingly, governments and donors are looking to transition their social transfer payments from cash to electronic payments and, in some cases, incorporate financial inclusion objectives into these payment schemes. This momentum toward e-payments rests on the promise of improving transparency, reducing leakage, and decreasing costs on the one hand, and facilitating value-added services for beneficiaries through financial access on the other. In this regard, MTIT could also evaluate and possibly leverage the e-payment mechanism implemented by the Gaza e-government team.

### *5.3.4 Portal Platform Enablers*

X-Road could be integrated with the following portal platform enablers to facilitate e-service related requirements for content publishing, collaboration, and connecting with the citizens.

- *Content management*: The e-service platform could offer a built-in content management system (CMS). A CMS is a structured system to manage content, with

support for role-based workflow, separation of presentation from content creation, and editorial approval and versioning processes.

- *Collaboration tools*: The e-service platform should have a collaboration suite comprising of message boards, blogs, and wikis, featuring Rich Site Summary (RSS) capabilities, tagging, common metadata, and social bookmarking. The collaboration suite should enable productive discussions and sharing of information amongst government officials and the business community, and the business community amongst themselves.

- *Social networking tools*: The e-service platform should have a suite of social networking tools, for example, instant messaging to enable users to connect with each other, create a "friend" lists, and the ability to customize the social networking tools based on their specific needs. In essence, the e-service platform should provide the user with the tools and framework for building a fully functional social network that can be customized to meet their needs.

### *5.3.5 Government Cloud*

The PA's move to the cloud in 2016 would enable to government to have a next generation whole-of-government infrastructure. It will provide efficient, scalable and resilient cloud computing resources; and could safeguard the country's valuable data in a conflict situation, which is of particular relevant for WB&G. The PA should acknowledge the differences between commercially-available public clouds, and private government cloud. The choice between one or the other, or a hybrid, is possible to cater to different levels of security and governance requirements. This could be implemented based on separate zones for high, medium or basic assurance.

PA could also further aggregate demand to maximize cost savings by identifying and providing common services, such as business analytics, customer relationship management and web content management, software-as-a-service and platform-as-a-service offerings on their government cloud. New central services such as government web service exchange and gateways to authentication and payment services will be added as the next phase of G-cloud. The existing X-Road could be integrated with the following portal platform enablers to facilitate e-service related requirements for content publishing, collaboration, and connecting with the citizens.

## 5.4 Track 4: E-government Unit

The Palestinian e-government program will require significant capability and capacity to manage and implement. It is clear that additional staff would be needed at the MTIT's E-government Unit. The unit currently has only five full time equivalents, of which several of its officers are serving only half time. The existing staff also have limited training and experience in IT policy, standards and implementation know-how. A proposed list of

additional staff required is listed in the table below, and the needed skills and training on standards and processes may be found in Table 6.

| Track | Additional Staff Required |
|---|---|
| Track 1 - Palestinian National Portal | 3 |
| Track 2 - Legislation, Policies, and Standards | 4 to 6 |
| Track 3 - Common e-Service Enablers | 2 to 3 |
| Track 4 - E-government Unit | 9 to 12<br><br>[Summation of Track 1- 3]. |

The E-government Unit should conduct a series of high-level visioning exercises to expose politicians i.e. Ministers on the value of e-government and ICT as enabler of social and economic development.

In addition, the Unit should work with the ICT industry to establish government skills training for government employees. The government employees should be trained in basic concepts on conceptualizing, planning, and managing e-government services. The e-government capacity building program would be designed for public officers who are involved in the provision of services in each Ministry.

Finally the Unit should conduct citizen outreach communications to create awareness on the e-services. The outreach activities would actively promote the availability of the National Portal and e-services; and communicate the benefits to the citizens through mass media and social media channels.

## Appendix A: Key Points from OECD's E-government Report

With reference to OCED's report on "The Case of E-government in the Palestinian Authority"; an updated e-government policy document could improve alignment with current PA priorities, and address some of the issues highlighted in this Report.

The report's proposed actions include the following:

[1] Update the e-government strategy by producing an e-government policy document that articulates the PA's new vision in the field of ICT in the public sector; and

[2] Involve all stakeholders in the process by creating *ad hoc* mechanisms for broad institutional involvement and wider public consultation.

The greatest drive for e-government comes from central government, and all Palestinian institutions perceive e-government as a priority. The co-ordination role of the MTIT could be reinforced to improve the implementation of e-services.

Proposed Actions include:

[1] Map administrative processes and existing applications in order to gain a clear picture of administrative workflows and institutional responsibilities; and

[2] Redefine the PA's e-government-related procedures with a "whole-of-government" approach and guarantee a more effective co-ordination role for the MTIT.

The enabling environment has a direct impact on a government's capacity to transform its stated goals into e-government services. The Palestinian Authority has recently established e-government teams of the MTIT to focus on this area.

Proposed Actions include:

[1] Prioritise legislative actions and infrastructure projects that enable the immediate delivery of key strategic services; and

[2] Develop a medium- and long-term plan to increasingly implement all the remaining legal and infrastructure reforms.

Basic e-government systems and applications are present in all ministries. Implementation could be improved by greater involvement of the private sector and by increasing the availability of dedicated funds.

Proposed Actions include:

[1] Increase awareness among the PA's public officials of the benefits and modalities to support a more direct inclusion of the Palestinian private sector in electronic service design and delivery; and

[2] New strategies based on the principles of good management (*i.e*. management by objective and performance-based budgeting) could increase the allocation and effective use of existing funds for e-government projects.

The delivery of user-centred services is a priority for the PA. More citizen engagement in policy formulation, and increased efforts to bridge the digital divide in the population would help transform this policy priority into practice.

Proposed Actions include:

[1] Creating focus groups, using online surveys and institutionalising public-private forums would allow greater involvement of Palestinians in policy making, and service identification and delivery; and

[2] Implement specific actions to increase access to the Internet and reduce the digital divide through ad hoc training programmes and infrastructure projects.

## Appendix B: Standards

**Table 6. Suggested Standards for IT Architecture**

| Technical/architecture | Suggested standards |
|---|---|
| IT service management | e.g. ISO/IEC 20000-1:2011 |
| Enterprise architecture framework | e.g. TOGAF, Zachman Framework |
| ICT skills development | e.g. Skill Standards for IT Professionals (ITSS), Users Information System Skill Standards (UISS), Information Technology Engineers Examination (ITEE), Embedded Technology Skill Standards (ETSS) |
| Risk assessment framework | e.g. NIST, OCTAVE, COBIT |

**Table 7. Suggested Standards for E-government Workflow and Documentation**

| E-government workflow/ documentation | Suggested standards |
|---|---|
| e-government workflow | e.g. Workflow Management Coalition (WFMC), BPMN, BPEL |
| e-government project documentation | e.g. ISO 9001 |
| Public records management | e.g. ISO 15489-1: 2001 |

**Table 8: Suggested Standards for Information Security**

| Information security | Suggested standards |
|---|---|
| Information security assurance | e.g. ISO/IEC 27001:2013 |
| Information access and transfer protocols | e.g.W3C Specifications: RFC 793 (TCP), 9/1981, RFC 794 (IPv4) 9/1981, and RFC 2460 (IPv6) 12/1998 |
| Public key infrastructure | e.g. X.509 |

**Table 9. Suggested Standards for Software Development**

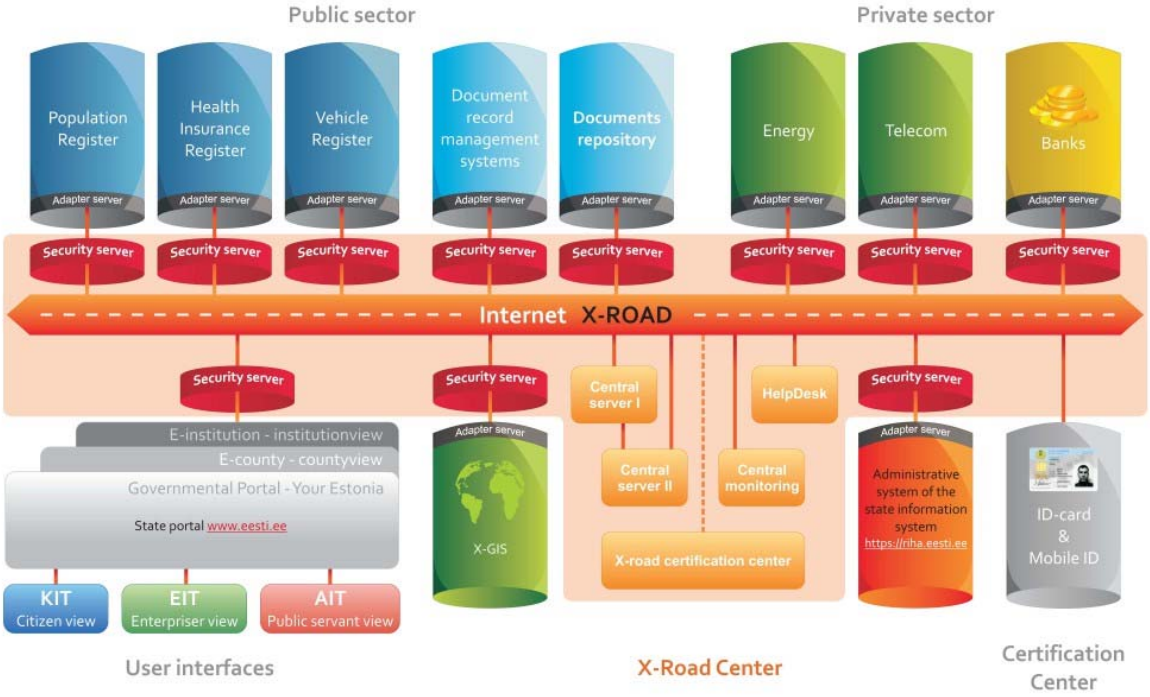
| Software development | Suggested standards |
|---|---|
| IT governance and management | e.g. COBIT |
| Project management skills | e.g. PMBOK Guide and Standards |
| System testing | e.g. ISO/IEC/IEEE 29119 |
| Software development lifecycle model | e.g. SEI Capability Maturity Model Integration (CMMI) |

## Appendix C: USAID's List of Top 10 Services

| Updated list of 10 Services | Ministry-in-charge |
|---|---|
| 1a) Smartcard/biometric ID to facilitate authenticated e-government services | MTIT and MOI |
| 1b) Citizen portal/service gateway | MTIT and related Ministries |
| 2a) SMS Gateway (cross-Ministry functionality) | MTIT and related Ministries |
| 2b) Central call center for G2C service information | MTIT and Ministries |
| 3) Car importation application and information | MoT |
| 4) Car purchase and maintenance services:<br>- Dynamometer car history<br>- Garage service information | MoT |
| 5) Traffic advisory services<br>- accidents<br>- traffic jam alerts<br>- traffic awareness | MoT |
| 6) Social support one-stop shop<br>- Cash transfer<br>- Emergency aid<br>- Small project loans<br>- Orphan aid<br>- Loans for the disabled<br>- Food aid | MoSA and others (MoF, MoI, etc.) |
| 7) Civil records<br>- Birth certificates<br>- Death certificates | MoH, MoI |
| 8) Health insurance validation (public health insurance) | MoH |
| 9) Property tax payment and pertinent sub-services<br>- assessment information<br>- TBC other sub-services | MoF |
| 10) Letter of good standing | Cross-cutting |

## Appendix D: About X-Road

X-Road is a platform, an independent data exchange layer between different databases and information systems. Platform independence is achieved by using the standardized SOAP protocol.




*Services*: X-Road services are Web services. Each service provider has a WSDL schema that describes all of its services.

*Service consumer*: Service consumer is an institutional organization that uses services provided by service providers. Consumer certificate does not allow provision of services.

*Service provider*: The service provider is a database that provides predefined Web services through x-road infrastructure. Service provider certificate does not allow using services of other service providers.

**Central server (PKI directory service)**

The central server provides information about X-Road users' public keys and IP addresses. The central server has the following services:

- DNS-SEC – resolving providers IP addresses and publishing X-Road consumers/producers public keys.
- NTP-SERVER – keeping security servers time up to date.
- Hash Repository service – storing all log hashes sent by security servers.

**i. Directory service (DNS-SEC)**

- **Functions of Directory Service:**
  - The Directory Service publishes certificate validity information.
  - The Directory Service manages and publishes access group rights for e-services.
  - The Directory Service is built on a DNS system with the DNSSEC security extensions. IT provides information about the institutions that have joined the system, about their Security Servers (e.g. IP addresses, certificates)
- **Features:**
  - The X-Road central institution operates one primary DNS server and as many secondary DNS servers as necessary. As a safeguard against communication problems with central servers, all Security Servers are equipped with a caching DNS server.
  - Directory Service manages access rights for e-service consumer groups. This feature facilitates the management of access rights to these services that have a large user-base.

**ii. Time-stamping service (NTP – Server)**

- **Functions of Time-stamp Service:**
  - Time-stamp Server has one main function: to store and time-stamp "digital fingerprints" of Security Server log entries.

- **Features:**
  - To ensure the evidentiary value of SOAP messages, X-Road is equipped with a time-stamping service, which is used in conjunction with secure logging mechanisms present in Security Servers.
  - The service, which time-stamps log entries, is called asynchronously at predetermined intervals. The number of issued time-stamps is independent of the number of transactions.

**Central services are needed for three purposes:**

- To ensure the evidentiary value of the exchanged data by providing the third party with a proof;
- To make the system scalable;
- To ensure the quality of service and detect any misuses of the system.

**Central services prime server provides the following management functions:**

- Management of secondary Central Server (IP adding, IP removing)
- Management of Security Servers: Allows addition and removal of Security Servers into X-Road or management following data related to the existing Security Servers:
    - Name of hosting organization.
    - IP address of Security Server.
    - Certificates import.
    - Manage e-mail address lists for error messages reports.
- Management of e-mail address lists for system wide error-messages.

**Management functions of secondary Central Server:**

- Request of IP address of prime Central Server.

**Certification authority server CA**

- CA server is an offline computer.
- Issuing certificates to X-Road consumers and producers.
- Information about producers IP addresses is also combined by CA server.
- Public keys and IP addresses are exported to central server using offline media (USB flash drive).

**Functions of Certification Service:**

- The certification service issues certificates to all institutions that use X-Road Security Servers.
- Generation of new key. Generates a key for DNS-SEC.
- Security Servers use certificates to authenticate their communication partners and to sign the SOAP messages exchanged.
- The certification service keeps a history (including current validity information) of all certificates ever issued.
- Certification keys can be stored in a hardware security module.

**Features of Certification Service:**

- The issued certificates database can be used to solve any disputes and to find out which institution was responsible for messages signed with a particular certificate.
- Certification Service works offline. Certificates created by the Certification Service will be loaded manually to the Directory Service and Security Servers
    - 

**Security server**

Security server is a dedicated proxy server for exchanging data between service consumers and providers. The security server's assignment is to:

- Forward queries to a right producer.
- Check if consumer's/producer's certificate is valid.
- Encrypt/decrypt data.
- Check if consumer has permission to access services.
- Log all queries.

The main functions of the security server are:

- Mediation and the provision of Web services over SOAP protocol provided by an information system. The security server must support SOAP attachments.
- Supports operations in synchronous and asynchronous modes. In the case of asynchronous mode of communication, the security server sorts the SOAP message and sends them to another Secure Server as soon as possible. Security servers maintain the order of messages and guarantee their delivery.
- Electronically signs all outgoing SOAP XML messages using the cryptographic keys for electronic signature, which are certified by a certification authority.
- Security Servers log and archive all exchanged SOAP XML messages. Messages are logged together with signatures. The message log is a cryptographic tamper-proof log that utilizes cryptographic hash functions to chain the messages together in a way that makes tampering detectable. In order to provide an evidentiary value, the log values must be time-stamped by a trusted third party, which in this case is the central institution. X-Road supports several time-stamping servers to increase the availability of the service.
- Encoding information exchanged with other security servers and message archives using the standard TLS protocol, using strong encryption algorithms (keys of at least 128 bits, an industry-standard algorithm, for example. AES). The security server checks the validity of the certificates with Central Services.
- Providing information about available services and service providers in X-Road system.
- Back-up and restore of archived messages.
- Sending an error message. The server will send an e-mail with error message to the list of e-mail addresses. The list is configurable. Error messages are divided into categories, with a separate category for global security problems;
- Security Servers are equipped with a caching DNS server as a safeguard against communication problems with central servers; all Security Servers are equipped with a caching DNS server.
- Performing load balancing with other Security Servers in same network.

The main features of the security server are:

- One Security Server can serve a more than one agency (required for ASP solutions).
- Administration of the Security Server is indivisible among administrators in different agencies.
- Administrators do not need additional software and hardware to administer the Security Server.

**Monitoring station**

- Monitoring stations provide X-Road servers (security and central servers) status information to system administrators.
- Monitoring Station also collects service usage information.
- Usage information contains only metadata (query time, user ID, user organization ID, database name and service name).

The monitoring service is used to check the status of system components. There are two levels of monitoring used.

**Functions of local monitoring stations, each of which continually:**

- Collects information (status information, error messages, and query information) from the Security Server.
- Status information contains detailed system information, such as CPU usage, memory usage, number of pending queries, and much more, giving the system administrator a complete and accurate overview of his server(s).

**Functions of central monitoring station that collects:**

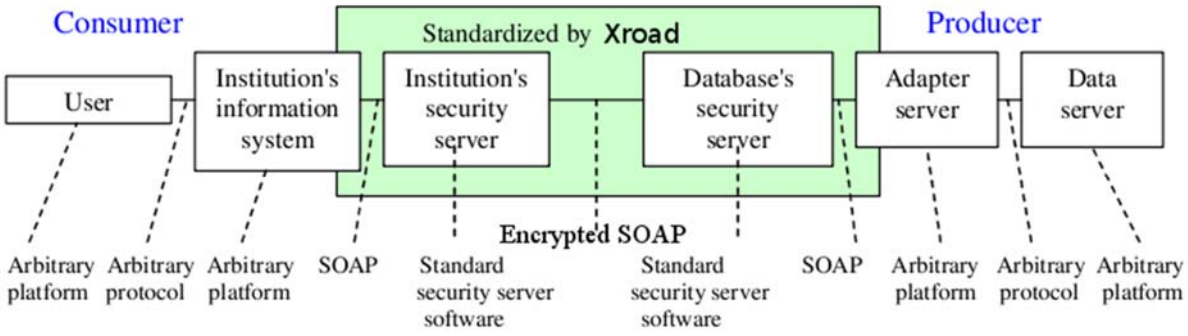
- Information from all gateways about the operation of X-Road in general.
- In addition, SNMP trap messages are used to transmit nonsensitive status and error information.

**Features of Monitoring Service**

- The monitoring system can detect suspicious activities (such as unwarranted queries to collect confidential information).
- With flexible alert rules, it is possible to monitor the average/expected number of queries (on hourly/daily/monthly basis) and notify the person(s) responsible when abnormal deviations are detected.

**Adapter server (process)**

Adapter server is a web service provider that modifies x-road queries to a database platform specific format.



**X-Road: overview**

- There are various databases and information systems in different platforms that need to cooperate.
- Extra interface from every database to every information system would be expensive.
- X-Road is a platform-independent secure standard interface between databases and information systems.
- Database is adapted to X-Road by setting up Adapter Server, which contains:
  - X-Road / SOAP server.
- Information systems implement:
  - X-Road / SOAP client.
  - X-Road rules.
- To secure the system, each party accesses X-Road via its Security Server.
- X-Road Security Server is a standard software solution that encrypts/decrypts outgoing/ingoing messages, filters ingoing messages as a firewall, and logs messages it receives.
- Traffic between Security Servers is encrypted with PKI.
- Security Servers have to be certified by X-Road Certification Authority.
- Certificates are available for verification from X-Road Central Servers.
- Central Servers are duplicated.