Annex 5.7

E-GOVERNMENT PROGRAM BACKGROUND AND IMPLEMENTATION FRAMEWORK

This section provides background material and information relating to this RFP. Nothing in this section shall be construed as a representation on the part of the Ministry of Digital Economy and Entrepreneurship (Modee) as to the Modee's future conduct or the project schedule.

E-Government Program Background

E-Government is a National Program initiated by His Majesty King Abdullah II. The purpose of e-Government program is to enhance the performance of government in terms of service provision, efficiency, accuracy, time and cost effectiveness, transparency, customer –centricity, customer satisfaction, cross-Governmental integration, and the way government is perceived.

The e-Government Program will support government transformation, using ICT tools to achieve the ultimate National goals of public sector development. This transformation process requires a focal point of contact to coordinate the efforts between Government entities and support them with best practices and subject matter expertise. The Ministry of Digital Economy and Entrepreneurship is responsible for the e-Government Program which facilitates and provides support services to Government entities in the areas of Program Management Office (PMO), project management, change management, technical management and support services, risk management, quality management and others. The role of the e-Government program is to plan, facilitate, manage and supervise the implementation of e-government through: Business Process Re-engineering (BPR) towards better and more efficient processes, human performance development (including knowledge transfer and training), organizations review and re-structuring to achieve greater efficiency. Additionally, the e-Government deploys best practices and latest technologies to enable Government stakeholders to implement new processes and create a knowledge-based community.

The scope of e-Government Program includes:

- Planning of the e-Government Portfolio (including selecting priority e-Services)
- Guiding and instigating Change Management efforts
- Determining technological standards for products and services integrated with e-Government Infrastructure (Portal, Secure Government Network)
- Establishing Technical and Information Security Standards, Program and Project Management methods, Change Management standards, procedures and tools, and reporting requirements for e-Government Projects across the Government entities
- Describing standards for e-Government Infrastructure (e-Government Architecture Framework (eGAF*)*, IIF, Reference Architecture) and developing other technology-oriented initiatives in order to establish a service-oriented and collaborative environment for e-Services.
- Developing and supporting e-Government strategy and providing support to its operations.

The e-Government Program has recently completed its 1st Wave of e-services (five Fast Track projects).

The 2nd wave of e-services, which started in 2006, comprises a number of cross-organizational e-services.

Government Service Bus

This solution will enables the integration between services including Government-to-Government (G2G), Government-to-Business (G2B) in an architecture that will allow the government entities to exchange data through web services, and will enable the exchange of data between government entities and the non-government entities (non SGN connected businesses).

Summary

IBM WebSphere Data Power SOA Appliances are purpose-built, easy-to-deploy network devices that simplify, secure, and accelerate your XML and Web services deployments while extending your SOA infrastructure. The Data Power Appliance provides many core functions to applications, such as service-level management, routing, data and policy transformations, policy enforcement, access control, and hardened security—all in a single “drop-in” device.

Data Power provides the following key benefits.

- Platform for Vertical e-Services integration: Web services from different government entities (service providers) can be securely exposed using Data Power.
- Cross Organizational e-Services Platform: Data Power provides role-based access control to ensure the right level of secure access for cross-organizational e-Services.
- Composite e-Services integration platform: Data Power is the service composition layer that exposes composite services to service consumers.
- Shared e-Services integration platform: Data Power supports modular service integration architecture.

When deploying this IBM appliance in your network, you secure your enterprise at the Application Layer vs. at the Network Layer. DataPower is a next-generation appliance that operates on MESSAGES instead of PACKETS. This enables offloading security checks and structural checks from the service providers, there by simplifying integration while minimizing performance degradation.

Solution components and features

The below sections lists the used components and the utilized features within the Data Power appliance during the implementation of the Edge ESG to help meet Modee requirements:

- **Logging**

  IBM Data Power appliance offers a bunch of different options when it comes to logging. MODEE’s main concerns when it came to logging were:

  - The ability to troubleshoot a problem when one arises: As for this point in the solution IBM Data Power offers a feature called ‘debug probe’, this feature can be enabled to log the messages temporarily and then view them at each stage within the policy execution, this also offers information like the requested and source URL/IP which should be sufficient when a problem arises at the message level.
  - Being able to view and track events as they occur (mostly errors): As for this DataPower’s out of the box logging behavior should suffice, it offers the ability to filter the logs based on the component from which they originated and the ability to increase and decrease the level of logging details based on the current need.

- DataPower auditing: Out of the box, DataPower offers the ability to log any administrational actions, by which user where they performed and when (this also included some lower level relevant action logging).

- **Security using SSL certificates**

When it comes to SSL, the solution includes two different implementations:

- Standard SSL over HTTP (for G2G services)
  In this scenario DataPower is issued a certificate which the service consumers should trust and accordingly be able to authenticate DataPower boxes and perform transport layer encryption. As for between DataPower and the service providers, DataPower should receive a copy of the public certificate of the entities it will connect to in order to trust them.

- SSL with mutual authentication (for G2B services)
  As for this scenario the communication with the backend services is still done in the same manner but the communication with the consumers is done differently. In this case the first part still stands true where DataPower is still issued a certificate which the service consumers should trust but the difference is that the service consumers themselves should also be issued certificates which the DataPower should receive (public certificates) in order to perform a mutually authenticated connection.

Mutual authentication or **two-way authentication** (sometimes written as 2WAY authentication) refers to two parties authenticating each other at the same time. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

- **Web services proxy**

A 'Web Service Proxy' provides security and abstraction for remote web services. It is the object where most of the implementation will be performed and where the majority of the other features are contained. A Web Service Proxy makes it easier to implement certain features for web services based on a WSDL file.

- **WSRR integration**

DataPower offers the option to obtain the service WSDLs, the SLAs and configuration files in general from WSRR. This has multiple benefits the solution by offering automated, scalable capabilities to optimize resources in an SOA environment. Through advanced metadata systems, WSRR integration enables enterprises to manage applications, services, and service consumers in order to apply consistent operational policies and enforce lifecycle governance.

- **Message Transformation (XSLT)**

XSLT (Extensible Stylesheet Language Transformations) is an XML structured language used for transforming XML documents into other XML documents, or other formats.

Within DataPower XSLT is the language of choice and it is used to implement any custom logic which doesn't come with DataPower out of the box. XSLT as a language along with its extensions offer a big range of possibilities when it comes to implementing custom logic.

- **AAA for security enforcement**

AAA stands for 'Authenticate, Authorize and Audit'. In this solution the AAA action in a DataPower policy is what is used to authenticate the consumer's identity against LDAP and to authorize the user based on an LDAP group membership.

Secure Government Network

The Secure Government Network (SGN) is a large initiative linking all government entities to a secure Government Network as a part of a recently developed Connectivity Strategy. The main role of the SGN is to provide connectivity to government entities. Currently, the following services are provided through the SGN:

- File sharing/exchange between government's entities connected through the SGN.
- E-mail services (electronic services that include email messaging solution, calendar, personal communications tools, etc.).
- Inter-application communication

The entities currently connected to the SGN are:

Ministry of Digital Economy and Entrepreneurship
Ministry of Planning
Municipality of Greater Amman
Ministry of Industry and Trade
Ministry of Finance
Prime Ministry
Ministry of Foreign Affairs
Ministry of Public Works and Housing
Civil Status and Passport Department
Department of Land and Survey
Income and Sales Tax Department
Central Bank of Jordan
Ministry of Tourism and Antiquities
Civil service bureau
Drivers and Vehicles Licensing Department
Department of Borders and Residence

General Intelligence Department
Ministry of Interior
Amman Chamber of Commerce
Amman Chamber of Industry
Companies Control Department
Amman Medical Center
Royal Hashemite Documentation Center
Management & Development of Orphans Fund Corporation
General Supplies Department
Vocational Training Corporation
Joint Procurement Department
Prince Hamza Hospital
Public Transport Regulatory Commission
Supreme Judge Department
Crisis Management Centre
Royal Jordanian Geographic Center
Ministry Of Labor
Jordan Customs
Audit Bureau
Jordan Parliament
Ministry Of Higher Education
Government Tenders Directorate
Investment Commission
Ministry of justice
Ministry of Health
Ministry Of Education
The Jordanian Senate
Hussein Cancer Center
Ministry Of Municipal Affairs
National Library
Social Security Corporation
Ministry of Agriculture
Ministry of Social Development
Ministry of Culture
Ministry of Energy
Legislation and Opinion Bureau
Palace of Justice
Ministry of Environment
Department of Statistics
General Budget Department
National Aid Fund
Jordan Museum
Scientific Research Support Fund

Housing and Urban Development Corporation
Ministry of Public Sector Development
Ministry of Parliamentary Affairs
Jordan News Agency(Petra)
Ministry of Transport
Civil Defense Directorate
Operating Fund, Training and Vocational and Technical Education
Jordan Atomic Energy Commission
Anti-Corruption Commission
Ministry of Awqaf Islamic Affairs and Holy Places
Jordan Armed Forces
Postal Saving Funds
Energy & Mineral Regulatory Commission
The authority of the Aqaba Special Economic Zone
Jordan Ombudsman bureau
Cities and Villages Development Bank
Royal Cultural Center
Social Security Investment Fund
Natural Resources Authority
Civil Aviation Regulatory Commission
Department of Palestinian Affairs
Jordan Institution for Standards and Metrology
Free Zones Corporation
Development and Employment Fund
Royal Hashemite Court
Telecommunications Regulatory Commission
Independent Electoral Commission
Inspection Department/ MOI Branch
National Institute for Training (Previous: Institute of Public Administration)
Department of Antiques
Jordan Securities Commission
Ministry of Water & Irrigation
Jordan Medical Council
Jordan Enterprise development Corporation
General Directorate of the Gendarmerie
IFTAA
Constitutional Court
Government Financial Management Information System Building
The Higher Council For Youth
e-Fwateercom

The following diagram illustrates the current SGN architecture:

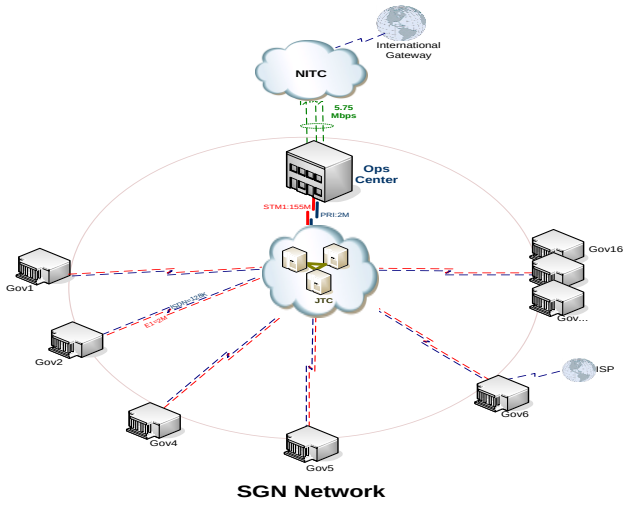


Figure 13: current SGN architecture

Upon request, Modee will provide the winning bidder with related document(s) describing in detail Connectivity Strategy and detailed requirements related to SGN.

Identity Management Solution

The Project of Identity Management Solution (IDM) is a running a project that is scheduled for delivery in Dec 2019.
This project is owned and run by Ministry of Digital Economy and Entrepreneurship , being implemented by the Italian company; OmniTech and local company; JBS.

IDM solution is hosted on-premise and it handles the both citizen and government employee access to government services through government portal, including authentication and digital signature; remote signing and smart card signature. It mainly provides the following functionalities:

- Strong User Authentication and Digital Signature
- Ensuring the user's mobility with Single Sign-On Capabilities
- Support different authentication methods and multichannel authentication, including Mobile Applications
- Compatibility with standard protocols (e.g. SAML, Open ID Connect, standard well-known digital signing protocols)
- Digital Signature engine to support transaction approval and document signing.
- Integration with the existing Card Management System, eGov National Portal, PKI Infrastructure.
- Self-service user profile management.

The main components of the IDM solution are:

1. Mobile Authentication, Single Sign On and Federation Domain
2. Smart Card, Digital Signature and PKI Domain

E-Government Contact Centre

The vision of the Contact Centre Initiative is to support the transformation of Government into a customer-centric organization – a paradigm shift in the way the public sector operates. The E-Government Contact Centre program aims to create a solution to support the interactions of each government entity with its stakeholders.

In order to reach that vision, the maturity model depicted below has been developed.

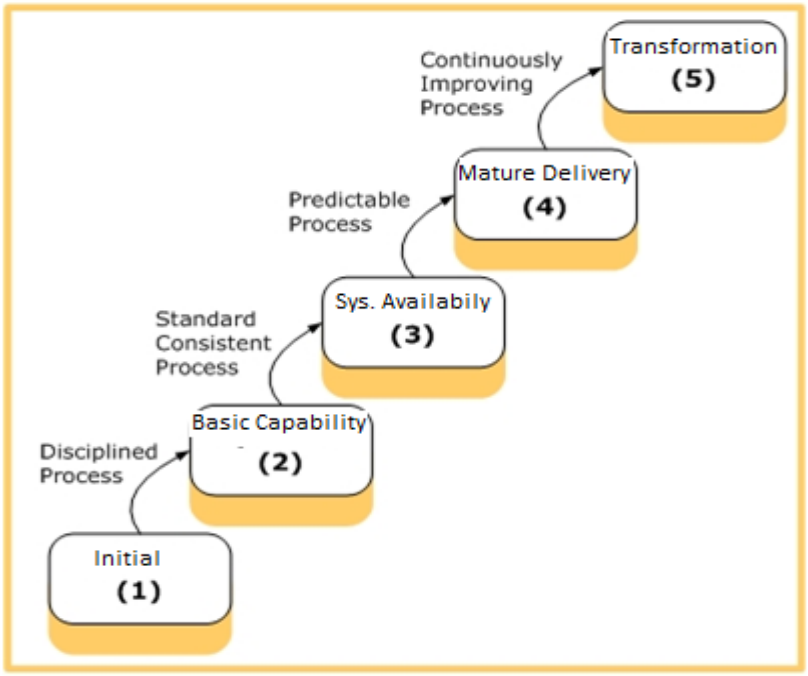


Figure 14: NCC Maturity Model and Roadmap

In its final maturity level, the Contact Centre should be seen as one of the access and delivery channels of the government including to traditional channels such as face-to-face or post and modern channels like the Internet. In addition, the Contact Centre will be a support method for modern channels.

eFAWATEERcom

Introduction

The eFAWATEERcom Integration Interface is a web service communication module that enables Banks, PSPs, and Billers to send and receive financial requests through the eFAWATEERcom network for the purpose of bills presentment and payment.

These requests are verified and processed in eFAWATEERcom system, which is responsible for handling all transactions in a secured environment.

eFAWATEERcom through its solution provides features for tracing the state of the transactions at all stages.

Moreover, eFAWATEERcom is integrated with several solutions for the purpose of reconciliation, reporting, clearing, and monitoring.

eFAWATEERcom Switch

eFAWATEERcom solution has the ability to connect different Banks and PSPs with different Billers, and at the same time, the solution integrates with the RTGS and the ACH for settlement.

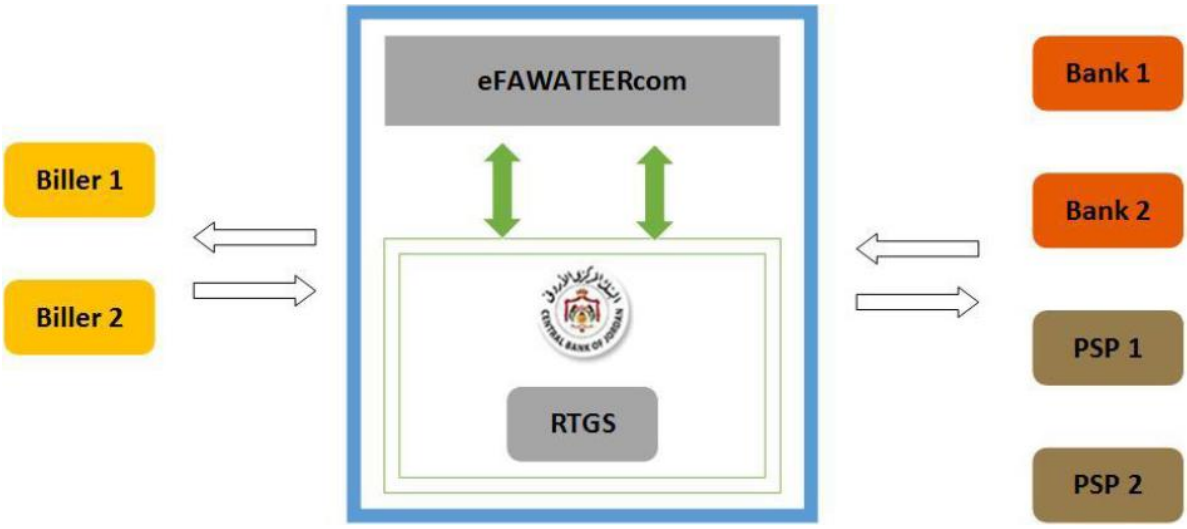


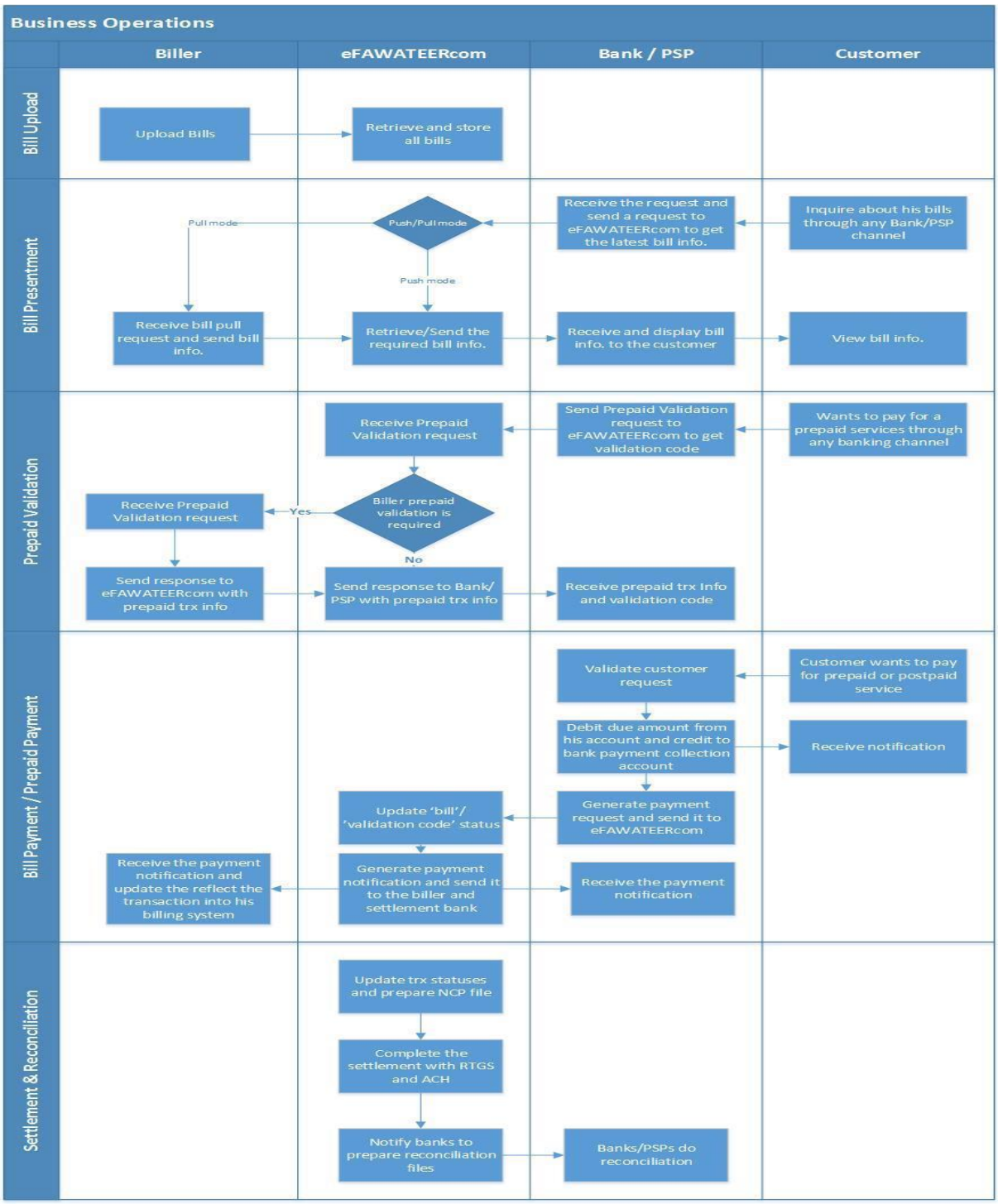
Figure 1 eFAWATEERcom Switch

Business Process Operations (BPOs) of eFAWATEERcom

The following workflow shows the main stages that eFAWATEERcom consists of:

- Bill Upload Process
- Bill Presentment (Bill Inquiry) Process
- Prepaid Process
- Payment Process
- Settlement and Reconciliation Processes

Note: The solution is capable of supporting different types of payments in addition to handling all payment statuses (New, Sent, and Completed).


Business Operations
Biller
eFAWATEERcom
Bank / PSP
Customer
Bill Upload
Upload Bills
Retrieve and store all bills
Bill Presentment
Pull mode
Push/Pull mode
Receive the request and send a request to eFAWATEERcom to get the latest bill info.
Inquire about his bills through any Bank/PSP channel
Push mode
Receive bill pull request and send bill info.
Retrieve/Send the required bill info.
Receive and display bill info. to the customer
View bill info.
Prepaid Validation
Receive Prepaid Validation request
Send Prepaid Validation request to eFAWATEERcom to get validation code
Wants to pay for a prepaid services through any banking channel
Receive Prepaid Validation request
Yes
Biller prepaid validation is required
No
Send response to eFAWATEERcom with prepaid trx info
Send response to Bank/ PSP with prepaid trx info
Receive prepaid trx Info and validation code
Bill Payment / Prepaid Payment
Validate customer request
Customer wants to pay for prepaid or postpaid service
Debit due amount from his account and credit to bank payment collection account
Receive notification
Update 'bill'/ 'validation code' status
Generate payment request and send it to eFAWATEERcom
Receive the payment notification and update the reflect the transaction into his billing system
Generate payment notification and send it to the biller and settlement bank
Receive the payment notification
Settlement & Reconciliation
Update trx statuses and prepare NCP file
Complete the settlement with RTGS and ACH
Notify banks to prepare reconciliation files
Banks/PSPs do reconciliation

Information Security

Information Security spans all phases of e-Government, and all layers of the e-Government enterprise architecture. It is both a guiding principle for e-Government and an attribute of the ICT infrastructure. Hence, it is a high priority to:

- Develop and execute an Information Security Roadmap for e-Government that covers important security issues
- Issue Information Security policies for the Government of Jordan
- Develop and apply information security standards, practices and measurements.
- Assess the security status of government entities and e-services and websites.

The information security unit have a number of projects and actions that will be delivered as part of the e-government program roadmap over the next 3 years.