Organisational structure for the e-government coordination and interoperability framework: a case study of Tunisia

Hatem Ben Sta
Higher Institute of Management,
University of Tunis,
SMART Lab, 41,
Avenue de la Liberté, Cité Bouchoucha,
Le Bardo 2000, Tunis, Tunisia
Email: hatem.bensta@gmail.com

Abstract: A clearly defined institutional framework for e-government planning and implementation is the main precondition for the development of e-services. Usually one of the main tasks of this coordination is to set up an organisational framework enabling planning and implementation of e-government development. The main risks regarding developments of the e-government architecture for e-services in Tunisia are that different technology projects managed by different organisations and regulated by different laws are creating a set of incompatible components of the state information system, which might need extra efforts of system development in the future. This is why the establishment of a clearly defined institutional framework and coordination mechanisms are of utmost importance. Sustainable and interoperable e-service development and data exchange are based on a clear organisational setup for developing and running the systems. The following description intends to provide a framework for the organisational setup in e-government services development and implementation.

Keywords: interoperability framework; interoperability; organisational structure; e-government; e-GIF; e-Government Interoperability Framework; NIF; national e-GIFs.


Biographical notes: Hatem Ben Sta is currently an Associate Professor at the Higher Institute of Informatics, University of Tunis El Manar. He is an Active Member of the Research Laboratory “Optimisation Strategy and Smart IT”. He received his PhD in Computer Science with very honourable from Ecole Centrale de Paris in 2006.

1 Introduction

Today, public administrations are striving to leverage modern information and communications technologies to improve the quality of their services to citizens and
businesses (Scholl and Klischewski, 2007; Osimo, 2008), to provide multiple communication channels and to make their internal and cross-organisation operations more efficient, even if this requires changing their modus operandi (Janssen and Cresswell, 2005; Niehaves, 2007). Since the late 90s, most countries have released their eGovernment strategies defining their milestones and action plans and have thereafter made significant progress on e-government at all levels of public administration (Capgemini, 2007). However, it soon became apparent that absence of common technological standards and interoperability guidelines yielded considerable leeway to governmental authorities and let them be focused on their own requirements and define inflexible information systems according to their own assumptions and interpretations (Hovy, 2008). Interoperability has thus become the key issue in the agenda of the public sector (CEC, 2006b) since providing one-stop services calls for collaboration within and across public authorities, while i2010 (CEC, 2006a, 2006b) explicitly addresses interoperability as one of the four main challenges for the creation of a single European information space and essential for ICT-enabled public services. Achieving interoperability requires resolution at various distinct interoperability levels: political context, legal, organisational, semantic and technical, as argued by IDABC (2004, 2008a), Gottschalk (2009), Panetto (2007), Papazoglou and Ribbers (2006), MODINIS (2007) and Scholl and Klischewski (2007). e-Government Interoperability Frameworks (e-GIFs) pose today as the cornerstone for the resolution of interoperability issues in the public sector and the provision of one-stop, fully electronic services to businesses and citizens. Such interoperability frameworks aim at outlining the essential prerequisites for joined-up and web-enabled Pan-European e-Government Services (PEGS), covering their definition and deployment over thousands of front-office and back-office systems in an ever extending set of public administration organisations (Charalabidis et al., 2007b). They further provide the necessary methodological support to an increasing number of projects related to the interoperability of information systems in order to better manage their complexity and risk and ensure that they deliver the promised added value (Ralyte et al., 2008). In this direction, the present paper presents also the baseline of the organisational structure for the e-government coordination and interoperability framework of Tunisia and gives some elements that have released and conducts a comparative analysis of some findings and compliance with the guidelines of the European interoperability framework (EIF). The scope of the analysis is to indicate the similarities and differences in the National e-GIFs (NIFs) philosophy and implementation and to produce a set of recommendations for any interesting party beginning to design or maintain an e-GIFs.

This paper is structured as follows: Sections 2 describes the Background of e-government, interoperability, standards interoperability framework in e-government, Section 3 describes the way in which organisations have agreed or should agree, to interact with each other, and how standards should be used, some criteria the public policy development, Section 4 draw the possible institutional framework for e-government development in Tunisia, Section 5 introduces the organisational setup of the implementation of the interoperability framework, and finally Section 6 showing the discussion and the conclusions of the research.
2 Background

This Section provides a background about e-government, its adoption barriers and readiness measurement index; it will also provide background on interoperability in e-government and its existing frameworks.

2.1 E-government

Deloitte and Touche (2003) defined e-government as “the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees”. These technologies can improve the government management, its interaction with industry, business, and empower the citizen through the better access to information. As a result, the government can increase transparency, convenience, revenue growth, and/or cost reductions (World Bank). The definition identifies four types of e-government: government to government (G2G), government to employee (G2E), government to citizens (G2C), and government to business (G2B) (Siau and Long, 2005).

- **The government to government (G2G) e-Government**: The objectives of G2G are to improve the cooperation and collaboration between governments of different physical locations and levels. This type of e-government has the role of guaranteeing the integration of systems and sharing of databases of local or federal governments. It also has to ensure the cooperation and collaboration through enforcement of laws, public safety and emergency management.

- **The government to employee (G2E) e-government**: This type’s goal is to ensure and enhance the effectiveness of government administration, internally, as well as its efficiency. The role it has to play is to organise the internal operational processes to implement and adopt the best practices in governance. Regarding the administration employees, it has to provide services such as training, payroll management.

- **The government to citizen (G2C) e-government**: has the role to improve the quality of services provided to citizens and the relationship between government and citizen. This is done by proving access to information varying from general information to specifics such as information on education and learning, policies, and loans.

- **The government to business (G2B) e-government**: aims to provide services of better quality to businesses like eradicating duplicated data and reducing the cost of transactions.

2.2 E-government stages

The United Nations defined a five stages model for e-government, namely

- emerging
- enhanced
- interactive
- transactional
- connected.
• **Stage 1**: In this stage, the government is present online through websites by providing static information for users; they are mainly official information about universities, government ministries, departments and agencies.

• **Stage 2**: In the enhanced stage, the websites become dynamic, updating data frequently and providing links for users to archived information.

• **Stage 3**: The online presence becomes more interactive; users are able to download documents such as application forms for passports, and car license.

• **Stage 4**: The transactional stage takes the online government to a further level by allowing the users to upload documents such as applications for car license, or passport, as well as making online transactions like paying taxes online, and doing e-banking.

• **Stage 5**: In the last stage, all government services are available online and accessible through a one-stop portal. At the portal, all the government services are integrated. Here, we talk about
  i. horizontal integration, which is among government agencies
  ii. vertical integration between local and central agencies of the government
  iii. connection between the government and its citizens
  iv. connection between all the players from government, private sector, academic institutions and civil society (United Nations, 2008).

### 2.3 UN e-government readiness index

To measure a country’s e-government readiness, the United Nations defined a measurement index consisting of three components: human capital index, online services index, and telecommunication infrastructure index. The values of the indices vary between zero for the lowest index value and one (1) for the highest one (United Nations, 2010)

• **The human capital index** has two measurement parameters, which are adult literacy rate, and combined gross enrolment ratio for primary, secondary and tertiary schools.

• **The online services index** is composed of four measurement parameters, emerging information services, enhanced information services, transaction services, and connection approach.

• **The telecommunication infrastructure index** is composed of five measurement parameters,
  i. estimated internet users per 100 inhabitants
  ii. mobile subscribers per 100 inhabitants
  iii. main fixed telephone lines per 100 inhabitants
  iv. personal computers per 100 inhabitants
  v. total fixed broadband per 100 inhabitants.
2.4 E-government adoption barriers

In their research paper, Ebrahim and Irani (2005) identified e-government adoption barriers defined in the literature as being the IT infrastructure, security and privacy, IT skills, operational costs, and organisational barriers. The IT infrastructure represents the key barrier for e-government adoption; it encompasses problems related to networks like the capacity and bandwidth, interoperability incompatibility between systems, shortage of Enterprise Architecture, and so on. Trust, privacy protection and security are aspects that affect the adoption where virus, worms and hackers are constant threats facing online applications and services; protection of personal data and ensuring secure transaction are a must for e-government. A successful implementation of e-government system also requires highly skilled staff in IT, but the public sector is generally suffering from a shortage of the skilled staff mainly because of the difference in salaries between the public and private sector. The organisational barriers are represented by the lack of coordination and collaboration between departments and agencies. Reluctance for change is another factor that is omnipresent when it comes to adoption of new strategies and technologies accompanied with the non-commitment of high and senior managers. Cost is another factor that hampers the e-government adoption; it covers the cost of implementation, maintenance of the infrastructure, development of systems and training, among other costs.

2.5 Interoperability

Identified as one of the factors affecting the e-government adoption (Ebrahim and Irani, 2005), the interoperability was defined as being “The ability of systems, units or forces to provide services to, and accept services from, other systems, units or forces and to use the services so exchanged to enable them to operate effectively together without altering or degrading the information exchanged” (DoD Missile Defense Agency). There are two types of interoperability, organisational interoperability and technical interoperability. The organisational interoperability deals with modelling business processes by aligning information architecture with organisational goals and helping business processes to cooperate (European Journal of ePractice, 2008). It is also about the collaboration of companies and administrations that wish to exchange information and cooperate despite having different internal structures and processes. The technical Interoperability has been defined by Mowbray and Zahavi as the “ability to exchange functionality and interpretable data between two software entities” (cited by Guijarro, 2007) and it is divided into two groups:

- **Application interoperability**: Includes issues regarding telecommunication network access level and network interconnection level.
- **Semantic interoperability**: Deals with the interpretation of data using XML schemas, and representation and exploitation of knowledge by means of ontologies and agents.

2.6 Standards for technical interoperability

Many standards exist for technical interoperability; the well-known standards are as follows
• **American National Standards Institute (ANSI):** Promotes the international use of US standards, policies and technical positions in standards organisation at national and international level. It also advocates the adoption of international standards at the national level when is needed (ANSI).

• **Dublin Core MetaData Initiative (DCMI):** has the mission to provide simple standards to help and facilitate searching, finding, sharing and management of information (DCMI).

• **European Telecommunication Standards Institute (ETSI):** Produces globally-applicable standards for information and communication technologies which include fixed, mobile, radio, converged, broadcast and internet technologies. The institute is officially recognised by the European Union as a European Standards Organisation (ETSI).

• **Institute of Electrical and Electronics Engineers (IEEE):** Aims to enhance global prosperity by promoting engineering process of creating, developing, integrating, sharing, and applying knowledge about electrical and information technologies and sciences for the profession and human benefit.

• **International Organisation for Standardisation (ISO):** The world’s largest developer and publisher of international standards, with 162 members, as one member per country. It is a non-governmental organisation forming a bridge between the public and private sectors (ISO).

• **Internet Engineering Task Force (IETF):** has the mission to make the internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the internet (IETF).

• **Organisation for the Advancement of Structured Information Standards (OASIS):** A non-profit consortium that drives the development, convergence and adoption of an open standard for the global information society, it produces worldwide standards for security, Cloud computing, SOA, web services, the smart grid, electronic publishing, emergency management, and other area (OASIS).

• **Unicode Consortium:** Enables people all around the world to use computers in any language. Its members develop the Unicode standards, Unicode locales (CLDR)

• **XML.org:** Hosted by OASIS, it is an online community gathering place for those interested and involved in standards and specification related to XML. It features focus areas for OASIS standards, and advances the use of open standards by providing technical and educational information, collaborative workspaces, and discussion areas (XML organisation).

### 2.7 Interoperability framework and enterprise architecture

Supporting the two types of interoperability, two types of Interoperability frameworks exist.

1. The interoperability framework is a set of policies, technical standards, specifications and guidelines (Valdes et al., 2008) to enable the seamless flow of
information between different administrations in the delivery of e-services (Guijarro, 2007).

ii The enterprise architecture is a tool for taking that basic interoperability further to the organisational-wide level, achieving IT and business alignment (Valdes et al., 2008). The result of this alignment contributes to interoperability at the organisational level between different administrations (Guijarro, 2007).

2.8 Interoperability frameworks in e-government

There are two main interoperability frameworks in e-government, e-GIF, and the Federal Enterprise Architecture (FEA); they represent reference frameworks in e-government interoperability, and have been adopted by non-negligible number of countries all over the world. Table 1 presents a non-exhaustive list of countries which have adopted one of the two frameworks. The rank indicates the United Nations’ e-government readiness index as of 2010 (United Nations, 2010).

<table>
<thead>
<tr>
<th>Country</th>
<th>South Korea</th>
<th>USA</th>
<th>Canada</th>
<th>UK</th>
<th>New Zealand</th>
<th>Denmark</th>
<th>Australia</th>
<th>Mauritius</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank 2010</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>14</td>
<td>7</td>
<td>8</td>
<td>77</td>
</tr>
<tr>
<td>Framework</td>
<td>Both</td>
<td>FEA</td>
<td>FEA</td>
<td>e-GIF</td>
<td>e-GIF</td>
<td>e-GIF</td>
<td>FEA</td>
<td>e-GIF</td>
</tr>
</tbody>
</table>

2.8.1 e-Government Interoperability Framework

A framework developed by the UK and published for the first time in 2001 as part of the Cabinet Office strategy to ensure the support of business transformation of the government by IT, helping to deliver more efficient public services (Cabinet Office, 2005). Thus the goal of the e-GIF is to establish policies, standards and technical specifications to achieve interoperability of IT and system coherence (Valdes et al., 2008) in the public sector. The policies and standards cover interconnection, data integration, content management metadata, e-services access, and business areas. Figure 1 represents the architecture of the framework (Cabinet Office, 2005). The Architecture of e-GIF framework is composed of five elements, Technical Standards Catalogue (TSC), Government Data Standards Catalogue (GDSC), e-Government Metadata Standards (e-GMS), and Government Category List (GCL):

- **e-Government Metadata Standard (e-GMS):** Is the component that defines the structure of metadata used in the public sector and the rules directing these metadata based on the Dublin Core standard (Valdes et al., 2008) to ensure the interoperability, standardisation of data is a must.

- **Government data standards catalogue (GDSC):** As e-GIF mandates the use and development of XML schemas for the interoperability and integration strategy, an agreed set of data standards are needed. The GDSC contains these agreed standards to be used in the development of XML schemas and exchange process. The framework recommends the use of these standards at the business level for storing data.
- **XML schemas**: Because data exchange involves several processes in government, the component includes XML schemas agreed to be used in the public sector to define common data.

- **Government category list (GCL)**: Contains controlled vocabulary list for e-GMS, such as Integrated Public Sector Vocabulary (IPSV) representing the subject element of e-GMS (ESD standards).

- **Technical standards catalogue (TSC)**: In this catalogue, the minimal set of technical standards are defined conforming to technical policies defined in e-GIF. The standards enclose the interconnections, data integration, content management metadata, e-service access, and business areas.

For the good management of the e-GIF Framework, responsibilities and roles have to be identified. In the case of e-GIF, main functions have been identified to ensure its good functioning.

- E-government unit in the Cabinet Office has the main authority for implementation and maintenance of the framework.

- Public sector organisations such as government departments and their agencies, local authorities and other involved bodies’ role are to ensure that e-GIF is compliant with their organisational, e-business and IT strategies.

- The industry is involved in the maintenance and development since the government works in partnership with the industry. The industry participates in the development of the policies and specifications for the interoperability.

- Citizens are encouraged to give comments, propositions that can help improve the framework, they are at the centre of e-government system since its aims are to serve their needs efficiently.

- **Other groups**: all working groups affected by the framework and its standards are part of the management process.

*The e-GIF framework is compliant with international standards; it proposes for each specification the available international standards that can be used. For instance, regarding character sets and alphabets in e-service access specifications, two possible standards are specified which are UNICODE and ISO/IEC 10646-1:2000.*

**Figure 1** Architecture of e-GIF (see online version for colours)

*Source: Cabinet Office (2005)*
2.8.2 Federal enterprise architecture (FEA)

In 1999, the US published the Federal Enterprise Architecture Framework (CIO Council, 1999), aiming to provide federal agencies with an enterprise architecture (EA) builder; it contains a variety of approaches and definitions to help develop and document an EA but does not define the contents of these EAs. The framework provides a logical arrangement to organise and classify architectural description. Later on, in 2002, the USA developed the Federal Enterprise Architecture (Figure 2) as the new reference architecture that provides to agencies a common language and frameworks to analyse, describe investments, and improve collaboration within the federal government. It is composed of five reference models that help analysis and identifying duplicate investment across agencies (Office of Management and Budget, 2007).

**Figure 2** Architecture of FEA

![Architecture of FEA](source: Office of Management and Budget (2007))

2.8.3 Architecture of FEA

- **Performance reference model (PRM):** the model offers a common language that allows the Enterprise Architecture of an agency, to measure the performance and objectives’ achievement of the agency (Office of Management and Budget, 2007).

- **Business reference model (BRM):** Provides a framework that helps to have a functional view of the lines of business in the government.

- **Service component reference model (SRM):** Provides a classification of service components regarding the capabilities they offer to business functions. Seven service components domains are identified in this model,
  
  i. customer services defines the capabilities related in a direct way to a customer who can be internal or external, customer driven functions or activities or business interaction
  
  ii. process automation services describe the capabilities that help to automate management and process activities for better business management
iii the business management services present the capabilities and services needed by project, planning and programs for the management within business operations in a successful way

iv digital services domain represents the capabilities that support the distribution of electronic media and intellectual capital across the business and extended enterprise

v business analytical services represents the capabilities helping the extraction, aggregation, and representation of information, to ease evaluation of business and analysis of decisions

vi back offices domain defines the capabilities helping to manage the enterprise planning and transactional-based functions

vii support services domain which includes cross functional capabilities possible to be leveraged independently from service domain objectives or missions.

• Data reference model (DRM): Is the mechanism of FEA to identify what the federal government has as data and how it can be shared to respond to the requirements of business and missions. It provides guidance to enterprise architects and data architects for implementing repeatable processes to enable data sharing in accordance with federal government-wide agreements (Office of Management and Budget, 2005). It has three standardisation areas (Office of Management and Budget, 2007).

• Technical reference model (TRM): Defines a hierarchical framework describing how standards and technologies support delivery, exchange and construction of service components. The service areas in TRM are: service access and delivery, service platform and infrastructure, component framework, and service interface and integration.

The framework was developed by the Office of Management and Budget’s (OMB), Office of E-Government (E-Gov) and Information Technology (IT), with the support of the General Services Administration (GSA) and the Federal Chief Information Officers (CIO) Council. Table 2 presents the framework focuses on TRM description on the access channel rather than standards since the objective of the framework is not to provide technical interoperability but organisational interoperability.

<table>
<thead>
<tr>
<th>Service area</th>
<th>Service access and delivery</th>
<th>Service platform and infrastructure</th>
<th>Component framework</th>
<th>Service interface and integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service category</td>
<td>Access channel</td>
<td>Support platforms</td>
<td>Security</td>
<td>Integration</td>
</tr>
<tr>
<td></td>
<td>Delivery channels</td>
<td>Delivery servers hardware/infrastructure</td>
<td>Presentation/ interface</td>
<td>Interoperability interface</td>
</tr>
<tr>
<td></td>
<td>Service requirements</td>
<td>software engineering</td>
<td>Business logic data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service transport</td>
<td>data/storage</td>
<td>interchange data</td>
<td>management</td>
</tr>
</tbody>
</table>
2.9 Interoperability strategies

From the two frameworks, two strategies in interoperability can be identified, technology first strategy, and business first strategy (Valdes et al., 2008):

i The technology first strategy sets as a priority to build the national wide interoperability framework (IF), in order to provide the basic and technical interoperability as fundamental stage then plan to define and implement the Enterprise Architecture which will be at the advanced stage.

ii The business first strategy prioritise building enterprise architecture and reference models first, by implementing data, infrastructure and service layers, then agencies can implement their own interoperability frameworks (as an advanced stage).

2.10 Adoption criteria for an interoperability framework

In their research paper aiming to identify a national IF for Chilean government (Valdes et al., 2008) performed a survey on e-GIFs adopted by different countries, they found that the criteria that affect the selection of a specific framework are:

- **Target**: The interoperability frameworks are either developed to ensure a technical interoperability for the public sector or a communication and information exchange across government agencies in order to align IT with business.

- **Strategy**: The government may prioritise ensuring business interoperability or prioritise technology first, this will match the target of the framework; the government may also inspire to apply both of the strategies.

- **Governance structure**: The structure of the government affect the implementation of the IF, in case of a federal government, the framework is set as a guidance to be followed, whereas in a centralised government implementation is meant to be at a national wide, agencies or administrations are obliged to conform to the specification of the frameworks in their implementation.

- **Coverage**: Closely related to the governance structure when selecting an IF, the government should verify what is the coverage of the specifications provided by the framework, does it provides enough specifications and guidance to be implanted at national-wide or is there specific adaptation to undertake in order to adopt it.

- **E-government stage**: With an e-government at early stages, it is more appropriate and advisable to implement and ensure technical interoperability first; organisational interoperability requires more maturity in administration and business management to be able to cooperate across agencies which means that there is an alignment between IT and business within the agencies.
3 Comparative analysis framework

According to the EIF (IDABC, 2008b), an Interoperability Framework describes the way in which organisations have agreed, or should agree, to interact with each other, and how standards should be used. In other words, it provides policies and guidelines that form the basis for selection of standards and may be adapted according to the socio-economic, political, cultural, linguistic, historical and geographical situation of its scope of applicability in a specific circumstance/situation. Typically, an e-GIF includes the context, the technical content, the management processes and the tools (UNDP, 2007).

Extending the EIF in terms of providing a comparative analysis framework for NIFs that remains in compliance with its underlying principles, the levels of analysis upon which the national NIFs can be compared based on the following criteria:

1. The ‘Systems’ Level on the basis of deploying the following supporting infrastructures which store and manage the artefacts of the ‘Standards and specifications level’:
   a. certification tools for examining compliance with the framework and providing specific guidelines for amendments when a certification of a public site or information system fails
   b. services and processes directory containing services and processes descriptions
   c. XML schemas and core components repository
   d. web services repository and registry
   e. systems reference repository with explicit definitions for systems and their topology
   f. access and collaboration tools for seeking and retrieving the eGIF specifications and posting change requests and comments in a bidirectional communication.

2. The ‘standards and specifications’ Level, which includes the paper-based specifications in alignment with the three levels of interoperability: organisational, semantic and technical.
   a. an organisational interoperability guidelines for service documentation, business process alignment, business process reengineering and legal issues
   b. organisational interoperability assets containing: service descriptions and metadata, service workflow diagrams and web services definitions, as well as transformation and reengineering patterns
   c. semantic interoperability guidelines
   d. semantic interoperability assets (IDABC, 2005) including dictionaries/code lists; thesauri and nomenclatures; taxonomy that includes constant and enumeration definitions; Mapping tables for defining intersections, correspondences, and gaps between constants and enumerations together with guidelines for mapping types onto each other syntactically and semantically; global or local ontologies for describing e-government knowledge
e syntactic interoperability assets with XML schemas libraries, core components libraries and metadata standards
f technical interoperability guidelines and standards
g guidelines and specifications for designing and implementing integration mechanisms (web services)
h guidelines for authentication and security mechanisms
i guidelines for websites design
j certification framework for organisations, systems, data and people.

3 The ‘Coordination’ Level, which mainly deals with long-term envisioning, raising awareness and ensuring maintenance:
   a coordination strategy that includes: vision and strategy for interoperability and e-government, goals and metrics and guidelines (maturity matrix and roadmap for PA)
   b coordination activities with marketing and communication plan and coordination and acceptance mechanisms
   c training activities which embrace skills management and training process as well as the training material
   d maintenance procedure referring to the change management – versioning processes.

The methodological approach for the analysis of the e-GIFs bears the following steps:
- the contents of the e-GIFs are retrieved and studied
- a detailed comparison of the e-GIFs is conducted on the basis of the aforementioned levels: systems, standards and specifications, coordination
- a discussion around similarities and differences of the various approaches, as well as best practices and lessons learnt, follows on the comparison matrix.

As far as the e-GIFs research is concerned, it must be noted that apart from the information published in the eGIFs official websites (until September 2008), the findings of relevant work undertaken by Guijarro (2007), Charalabidis et al. (2007a, 2007b, 2008), the MODINIS Study on Interoperability (2007) and the UNDP Study (2007) have also been taken into account.

4 Possible institutional framework for e-government development in Tunisia

4.1 Coordination and implementation of e-government

There is a need for some changes in the organisational development of e-governance in Tunisia. For a smooth planning, management and implementation of e-governance systems, at least two central coordinating bodies should be nominated. There should be
an organisation responsible for general coordination of e-government and another organisation responsible for the implementation of e-government central technology components. There are two important decisions to be made:

- to define who is responsible for the coordination framework of e-governance
- to define who can be responsible, at the government level, for the implementation of horizontal e-governance interoperability issues.

4.2 Coordination and planning of e-government

On the one hand, the government needs to specify the status and functions of the coordination institution. Today this role is (at least partially) fulfilled by the e-Government Unit at the Presidency of the Government and by the Ministry of Information and Communication Technologies. It would be important that the main coordination actions are performed by a single institution. International practice shows that cross-government coordination should be done at the highest level of government.

The questions to be addressed are the following:

- Who is responsible for the legal framework? Who would have the responsibility to determine the need for new legislation and provide the drafts?
- What is the financial model of running e-governance systems and deciding on the cost of the services?
- Who is responsible for the address system?
- Who is responsible for electronic ID planning and implementation?
- Who is responsible for data security frameworks?
- Who will collect metadata?
- Who will manage e-governance geographic coordinate definitions?

Currently, some of these tasks are done by the e-Government Unit at the Presidency of the Government, some by the Ministry of Information and Communication Technologies and some tasks are not fulfilled. It is recommended that at least tasks 1, 2 and 6 will be fulfilled by the e-Government Unit at the Presidency of the Government.

4.3 Implementation of interoperable e-Governance

The other important body responsible for the implementation of e-governance architecture should focus on the technical implementation:

- central portal management
- monitoring of infrastructure services
- registering and monitoring of the implementation of the e-government service bus
Organisational structure for the e-government coordination

- development and use of data protection measures
- advising and helping all government bodies in their service optimisation and implementation processes.

Currently, the ministries are working with different IT systems, but the specific development tasks are mainly defined by the existence of financial means and less by national development strategies for back-office integration, which should focus on interoperability between different components.

In Tunisia, several central components of e-governance are already implemented and new services are planned. Looking at the functionalities needed for the implementation of service-oriented architecture at the government level, a set of five basic aspects should be outlined:

1. administrative and technical implementation and maintenance of a data exchange layer (e-government service bus)
2. government portal
3. enabling technical infrastructure and security
4. administration of the implementation process (in the legal sense)
5. implementation and management of e-ID of citizens.

4.3.1 Details and explanations

The following explanations focus on different functionalities and roles of institutions. The descriptions are based on international practices and 20 years of experience coordinating and implementing e-GIFs in Estonia.

It should be mentioned that the international best practices are from countries where e-government coordination is done at the highest government level, such as the President’s or Prime Minister’s office (State Chancellery). It is important that e-government coordination and public administration reforms are handled together in the highest possible government structure. All changes in public management are difficult. Successful e-government development is a matter of reforms and changes in public administration.

There is a need to establish clear coordination mechanisms with relevant budgeting structures that will form the basis for stable and transparent development, give guarantees for decision-makers and permit greater donor input to the process. This mechanism exists only partly in Tunisia and there is a need for adjustments and clear legal definition of the roles and responsibilities.

It is important to find ways to establish a special budget line for ICT expenses in the state budget for expenses such as hardware, software, IT development work and running costs at the government agencies. Even if these ICT budgets of ministries are small, it would create stability for the Chief Information Officers and transparency for managers and donors. The budget for some shared services and coordination activities of the coordination centre can be centralised.
The tasks and responsibility areas of different government institutions regarding e-government should be fixed by a governmental decision. It is obvious that the central coordination unit cannot be directly responsible for all ICT development issues, although it should have an overall coordination role. For example, the development of basic ICT infrastructure (e.g., telecom regulation, network infrastructure, public key infrastructure, infrastructure-related legislation and international cooperation) is assigned to the Ministry of Information and Communication Technologies, e-health questions are the task of the Ministry of Health, ICT in education and e-learning questions are under the Ministry of Education, etc.

An active role of an ‘e-Government Council’ is very important in the launch phase of the Coordination Centre. Such a council could be used to increase the presence of the private sector, the academic sector and international organisations. One of the important roles of the council, among basic ICT policy/strategy issues, is trust-building and support.

It is important to keep technical issues and strategy planning issues (coordination and implementation) in separate units. For instance, the coordination tasks could be allocated to the e-Government Unit at the Presidency of the Government and the implementation to the data centre of the Ministry of Information and Communication Technologies. It would be good to avoid the situation where the same government institution is planning and implementing projects as well as supervising and auditing them, as this might cause a conflict of interests.

International examples demonstrate that coordination actions under the Prime Minister’s office are much more efficient than under the line ministries. There are several reasons for that – coordination questions are related to a wide horizontal change management, which is not easy to handle at the ministry level. All ministries (except for the Ministry of Finance) are basically working in a vertical-hierarchical manner. However, ICT coordination should be dealt with in a horizontal and in a networked manner. The Prime Minister’s role also includes ‘coordination’ with different political parties of the government, which might help to build wider consensus and organisational interoperability.

It is important to find ways to increase salaries of civil servants, working in the field of e-government (ICT). The goal is to get a critical mass of competence in the central government, which will be reflected in the efficiency of ICT investments and a systematic approach towards systems development.

The head of the central e-government coordination unit should have (or to be able to build) strong professional reputation among private sector actors, the academic circle and ministerial CIOs (a scientific degree in ICT or a related field would be an advantage). It would be important that the management of coordination unit is not too close to politics – examples from several countries show that there is a high risk to lose stability of coordination.

It is also important not to overemphasise the technical aspect of the field. The staff of the central coordination unit should be aware of the basic principles and possibilities of ICT – but it does not mean that they should be programmers, hardware specialists, etc. Not all members of the unit need to be highly educated ICT professionals.
Different models of coordination are possible, depending on the legal structure of the country and ways to share the roles between policy-making and implementation. Moreover, several practical aspects are important regarding the best position and mandate of the central coordination unit.

The following are the issues often discussed when the decisions are made:

- What is the scope of activities of the central coordination unit? Will the central coordination unit be specifically focused on e-government or responsible for a more broad scope of information society?

In practice, having a broader scope might be important. Usually, there is no special information society unit in the government and in practice, the additional activities focused on information society are very tightly connected with e-government concepts and activities.

- What are the tools for coordination? What tasks and rights should the central coordination unit have?

There are basically two main tools for coordination – law and money. It might be important that the central coordination unit has:

- a possibility to launch new legislative initiatives and approve e-government-related legal acts, prepared by other governmental institutions
- in cooperation with the Ministry of Finance, the possibility to support e-government-related budget planning and implementation
- the right to ask for information from government institutions regarding e-government situation, plans, and projects.

### 4.3.2 Responsibilities of the main coordination bodies

#### A Central Coordination Unit

1. Responsible for ICT strategy planning, implementation and supervision processes. Dealing with public relations on information society issues.

2. Has a right to get information from government bodies about the use of ICT systems and about the results of systems development processes.

3. Responsible for drafting the ICT budget in the state budget in cooperation with the Ministry of Finance. The Unit supervises the most important development projects (at the steering committee level).

4. Responsible for coordination of drafting of the main ICT-related legal acts (Digital Signature Act, Personal Data Protection Act, Telecommunications Act, Databases Act, etc.) The Unit should have a right to present opinions and approve all ICT-related legal acts. ICT-related acts are often initiated by ministries, e.g., Personal Data Protection Act – Ministry of Justice, Telecommunications Act and Digital Signature Act – Ministry of Communications, etc.

5. Has the right to initiate new ICT-related legal acts – e.g., Databases Act.
6. Responsible for management of the work of CIO working groups, planning and implementing CIO training activities.

7. Coordinates international cooperation activities in the field of ICT. Often international cooperation is performed in other ministries (e-health issues – Ministry of Health, e-business issues – Ministry of Economic Affairs, telecommunication and basic ICT infrastructure issues – Ministry of Information and Communication Technologies, etc.) but the central coordination should be performed by the Central Coordination Unit.

8. Initiates cross-government projects and programs.

9. Responsible for general guidance, recommendations and standards.

B. Chief Information Officer (CIO)

The Central Coordination Unit needs to have contact points in ministries to cooperate with them. CIOs should be nominated at the ministry level (normally he/she should be at the level of a Head of Department or an advisor to the ministry) with the following responsibilities:

1. Create and implement ICT action plan at the ministry level.

2. Plan and prepare for approval the annual ICT budget for the ICT Council of the ministry. The ICT budget should be in line with both the government ICT action plan and the ministerial action plan.

3. Implement different projects related to procurement, supervision of projects, ICT training issues of ministries, etc.

4. Organise ICT systems maintenance and user help desk.

5. Organise end user training on ICT issues.

CIO should be a member of the ICT workgroup of CIOs of ministries led by the Central Coordination Unit.

C. Ministerial level ICT Council

• headed by the head of administration.

• members of the ICT Council are the key persons of the main departments and sub-units of the ministry.

• topics and decisions of the Council are to be prepared by the CIO.

• the council should approve all strategic initiatives in the field of IT developments of the ministry:
  • initiate new projects
  • develop the annual ICT budget
  • prepare intermediate reports of ongoing projects
  • take decisions and responsibility of reengineering processes needed for the implementation of new projects.
Organisational structure for the e-government coordination

D Example: organisational chart of e-government coordination

5 Organisational setup of the implementation of the interoperability framework

When establishing the organisational setup for e-services interoperability framework, it is important to take the following aspects into account:

Avoid establishing a new institution. Use a suitable existing organisation that already has:

- some role of central implementation of e-government projects
- access to infrastructure
- availability of physical infrastructure (building, electricity, water and sewage, data connections)
• competence in hardware – data centre/cloud services and infrastructure
• role in monitoring and implementation of government networks
• knowledge of data security and close cooperation with CERT (Computer Emergency Response Team) for fighting cyber-attacks
• availability to train government officials and partners from private companies in various e-government topics
• skills and experience in government portal content development.

There are four main aspects to the organisational setup:

1 administrative and technical implementation and maintenance of the data exchange layer
2 government portal issues
3 enabling technical infrastructure
4 management and administration of implementation process (this is one of the main tasks and tools for coordination and planning).

A Administrative and technical implementation and maintenance require persons with the role of administration of technical components, including the establishment of physical connections of different government IT systems and databases.

B Governmental portal main activity is to develop a governmental web portal, which would be the main information source for citizens and businesses.

The activities include:
• development of web portal functionality, usability and layout, development of new applications (mobile applications, etc.)
• collecting, editing and publishing governmental information together with other ministries
• collecting, editing and publishing information about government services, providing service descriptions and service manuals for citizens and businesses in clear language
• linking electronic services to the service descriptions
• providing help to users, both institutional users and citizens.

It should be mentioned that the main workload for the portal comes from the editorial activities and portal development activities, but also from help desk activities.

C Enabling technical infrastructure

There is a need to manage and monitor internet connections for all government bodies and solve problems if a connection is broken or bandwidth is not sufficient. Also, there is a need to administer servers needed for the data exchange layer.
D  Management and administration of implementation process

In addition to the technical administration of the systems, there is a need to register government databases and IT systems, register electronic services, describe and distribute ontologies. This component is also important for the coordination and planning of e-government development and implementation. Cooperation with other government institutions is needed to get information about existing systems and future needs. Furthermore, there is a need for the administrative process with the approval of personal data protection administration and other relevant institutions when new systems and services are introduced.

E  Possible organisational setup and staff needed for the e-government technical (implementation) centre

The following descriptions can be handled as examples about possible institutional setup and staff needed for the e-government implementation centre. The descriptions are based on the Estonian experience of establishing and operating an e-government service oriented interoperability framework.

F  Interoperability Framework Centre

The activities of the centre are the following:
- development of governmental interoperability operation
- maintaining and monitoring governmental interoperability operation
- registering governmental databases, descriptions of governmental e-services
- assisting and advising other governmental institutions to connect databases to the interoperability centre and to develop electronic services.

The main responsibilities of the centre are:
- general development of the governmental interoperability solution
- planning, budgeting and managing unit activities
- cooperation with other ministries and governmental institutions.

G  Administrative system

This unit is responsible for the development and administration of the state information system.
Its daily activities are:
- registration of databases
- registration of services
- providing advice to other governmental institutions on how to describe, develop and register electronic databases and electronic services
- descriptions of ontologies and advice on their usages.

The head of the unit is responsible for the development and accuracy of the administrative system of the state information system.

Data administrators (1–2) are responsible for registering electronic databases and electronic services to the system. They also advise other governmental institutions on how to describe, develop and register electronic databases and electronic services.

**H Technical implementation unit**

The unit is responsible for the 24/7 operation of the interoperability service. The daily activities are:
- administration of the system
- monitoring and maintenance of the system
- development of the monitoring and maintenance tools and systems
- advice to other governmental institutions.

The head of the implementation unit is also the top technical administrator of the system. His or her main responsibilities are:
- sustaining the work of the governmental interoperability system
- top administration of the system
- development and implementation of the monitoring and maintenance tools and systems.

Administrators (1–2) are responsible for the daily administrative activities of the system, monitoring of system activities, monitoring and controlling the online connectivity of the databases of other institutions, and providing advice to other governmental institutions. The number of administrators depends on the sustainability of the system and availability of remote monitoring tools.

**I Marketing, development and quality control unit**

The unit is responsible for interoperability architecture and service development.

The daily activities are:
- development of the governmental interoperability service, development of electronic services
- marketing and communication with service consumers and service providers (databases, institutional IT systems, etc.)
Organisational structure for the e-government coordination

- quality control of services and advice on the reuse of existing services and descriptions.

The head of the unit is also the main IT architect of the interoperability framework. His or her main responsibilities are:
- coordination of the development of the governmental interoperability service, development of electronic services
- coordination of the development of new technical solutions and channels
- cooperation with and advice to the other governmental institutions’ electronic services developers and software solutions developers
- preparation of terms of references for new technical solutions
- quality control of the services.

Developers (1–2) are responsible for service development as well as preparation, validation and deployment of major development works in cooperation with software development companies. They also provide advice to the other governmental institutions to develop electronic services.

An analyst (1) is responsible for analysing government services and the logic of procedures as well as the quality of services.

J Governmental portal

Governmental portal main activity is to develop the governmental web portal, which is the main information source for citizens and businesses.

The activities include:
- development of web portal functionality, usability and layout, development of new applications (mobile applications, etc.)
- collecting, editing and publishing governmental information together with other ministries
- collecting, editing and publishing information about government services and providing service descriptions and service manuals for citizens and businesses in clear language
- linking electronic services to the service descriptions
- providing help to users, both institutional users and citizens.

The director of the governmental portal is generally responsible for the portal’s operation. His or her main responsibilities are:
- general development of the governmental portal
- planning, budgeting and managing unit activities
- cooperation with other ministries, governmental institutions and units in the e-government implementation centre.
K Editorial unit
Editors (1–2) are responsible for:
- collecting, editing and publishing governmental information together with other ministries
- collecting, editing and publishing information about government services and providing service descriptions and service manuals for citizens and businesses in clear language
- development of the portal content, electronic democracy tools and other modern communication tools
- advising other governmental institutions on how to provide information about government activities and services.

L Development unit
Developers (1–2) are responsible for:
- portal development
- daily improvements
- preparation, validation and deployment of the major development works in cooperation with software development companies
- advising other governmental institutions to develop their portals/websites.

M Helpdesk unit
Helpdesk people (1–3) are responsible for:
- advising end users (citizens, businesses) on using the portal and governmental services
- advising governmental institutions on developing information and services.

The number of persons working for the help desk depends on the agreed working hours of the helpdesk.

N Data security unit (IT Baseline Security System implementation) with access to CERT (2017).

The main activities of the data security unit are related to the setup and advice on data security assessment and measures of different government IT systems. Moreover, there is a need to assess and provide advice on the central components of the interoperability framework. With the coordination of this unit, it might be possible to order data security audits for different components of e-government architecture. The CERT is the Research and Studies Telecommunication Centre (CERT, 2017).
6 Conclusion

Interoperability reaches all governmental organisations at the national and international level and constitutes a thriving research domain from all aspects – scientific, entrepreneurial, societal and political. Today, most countries internationally have created an interoperability framework, a strategic document containing specifications and standards to be followed in order to ensure interoperability among public administrations and their beneficiaries (citizens, businesses, other public administrations). It provides guidance to practitioners what to consider and to do in order to enable seamless interaction within their public administration as well as with other public authorities. However, in most cases, the scope of the NIFs needs to be extended applying best practices drawn from other NIFs in order to provide a thorough set of specifications covering the comparative analysis framework proposed in this paper.

This paper presents a practical approach to design and to recommend an Organisational Structure for the e-government coordination and interoperability framework. In one hand it defines the possible institutional framework for the e-government development in Tunisia as the coordination and implementation of e-government, the coordination and planning of e-government, the implementation of interoperable e-governance and the responsibilities of the main coordination bodies (Central Coordination Unit, Ministerial level ICT Council, CIO) on the other hand it gives some details about the organisational setup of the implementation of the interoperability framework as the administrative and technical implementation, the governmental portal, the enabling technical infrastructure, the management and administration of implementation process, the possible organisational setup and staff needed for the e-government technical centre, the interoperability framework centre, the administrative system, the technical implementation unit, the marketing development and quality control unit, the governmental portal, the editorial unit, the development unit, the help desk unit and the data security unit with access to CERT.

Acknowledgements

We thank the Presidency of Government, The General Directorate of Administrative Prospects and Reforms, the e-government unit for providing great information and research resources for this project.

References


Organisational structure for the e-government coordination


Websites
