
iGovTT
intelligent • integrative • innovative

Date: 04/02/2013

National Information and Communication Technology Company Limited

Policy on e-Government Inter-Operability Framework

Consulting Unit

TABLE OF CONTENTS

1. Introduction

The e-Government Interoperability Framework (e-GIF) sets out the government's technical policies and specifications for achieving interoperability and simplifying Information and Communication Technology (ICT) systems integration across the public sector. The definition of Interoperability within Trinidad and Tobago is based on the definition used by the International Organization for Standardization (ISO) as follows:

> *[Interoperability is the] ability of two or more systems (computers, means of communication, networks, software and other components of information and communications technology) to interact and exchange data according to a defined method, in order to obtain the expected results.*

The main aim of interoperability in government is to achieve loose coupling between systems. This means that systems interoperate by exchanging agreed messages that are independent of their internal workings. In this way, systems remain independent, and any part of the interoperable network can be replaced without impact on the other parts as long as the new system implements the agreed interfaces.

1. Importance of Government Interoperability

e-Government interoperability is becoming increasingly important for developing countries as enhanced government efficiency and effectiveness coupled with the delivery of basic public services to all citizens are essential components required for achieving the Millennium Development Goals. Interoperability is also important as it reduces cost and risk for government systems while aligning them to the global Internet revolution.

2. Purpose

The e-GIF ensures that information can be readily located and passed between Government bodies and between the public and private sectors, while adhering to privacy and security obligations.

Government of the Republic of Trinidad and Tobago (GoRTT) is in the process of developing citizen-focused services. In order for this to be successful, information from several parts of Government may be required within a single transaction. The e-GIF will help to make this possible. In the medium and long term, the e-GIF will also accelerate the development of projects involving interoperability between systems by reducing the need to negotiate the standards to be used.

3. Objectives

The objectives of this Policy are to:

- Improve the image of Government domestically and internationally;
- Build citizen trust;
- Ensure technical consistency and integration;
- Reduce reliance on proprietary interfaces;
- Support multiple channels of service delivery;
- Achieve potential cost efficiencies; and
- Create conditions for broader e-Government implementation and achieving joined-up government.

In order to achieve these objectives, GoRTT will:

- Establish and maintain a set of technical standards to be used for inter-working between Public Sector Organisation (PSO) systems, between PSO systems and the wider citizenry, and between PSO systems and business communities;
- Establish a governance regime for the maintenance of these standards; and
- Establish a compliance regime with an exemption mechanism for times when it is impractical to adhere to this policy.

4. Context

Legislation and guidelines relevant to this Policy include:

- Constitution of the Republic of Trinidad and Tobago
- Civil Service Act, No. 45 of 1979
- Freedom of Information Act, No. 26 of 1999, as amended
- Tobago House of Assembly Act, No. 37 of 1980
- Vision 2020
- ***fastforward***
- Data Protection Act, No 13 of 2011
- Electronic Transactions Act, No 6 of 2011
- Policy on Content and Presentation Design Standards
- Policy on Network Security and Access Control
- Policy on Risk Management (Draft)
- Policy on Electronic Records Management (Draft)
- Policy on Content Management (Draft)
- Policy on Protection of Personal Privacy and Data Security
- Policy on Multi-Channel Delivery of Services (Draft)

5. Scope of Application

This Policy is aimed at the Managers, Communication Specialists, IT Professionals, or any persons responsible for the design, development, procurement, maintenance, approval and implementation of software, hardware, technical solutions, content or business services for Government (including ministries, departments and agencies in the public sector).

The scope of the e-GIF extends to systems that participate in the exchange of information between:

- Government to Citizens (G2C);
- Government to Businesses (G2B); and
- Government to Government (G2G).

In order to ensure current and future interoperability, e-GIF compliance shall be a mandatory part of any public sector procurement. However, the policy recognizes that there are cases where systems are built or procured with no immediate intention to implement external interfaces. **In this regard, ministries, departments and agencies in the public sector must note that the increasing emphasis being placed on providing seamless services to citizens will eventually result in a need for interoperability in their systems.**

1. Compliance, Exemption and Migration

Compliance with the e-GIF is mandatory for all Government ministries, departments and public sector agencies. However, some projects may be exempted from compliance, for example if their systems need to comply with industry-specific technical standards such as those issued by the International Civil Aviation Organisation. In such cases, requests for exemption must be made to the Interoperability Working Group (IWG) **(See Section 10**).

In other cases, systems may need to interoperate using the same software that incorporates a proprietary interface. Under these circumstances, approval to use this interface can be given within the organisation without the need to involve the IWG. However, the IWG should be informed of this decision [1].

2. Legacy Systems

A "legacy system" refers to a system that is already in operation. Not all legacy systems used within Government will initially comply with the e-GIF. In such cases, there are four circumstances under which migration towards the e-GIF should be considered:

- The legacy system is being replaced. In this case, the new system should adhere to the e-GIF;
- A legacy system is undergoing an upgrade. In this case, all parts of the system involved in the upgrade should comply with the e-GIF. Consideration should be given to moving other parts of the system towards e-GIF compliance at the same time;
- A new interoperability requirement is identified. In this case, the systems involved should move to e-GIF standards; and
- A security risk has resulted in a standard being withdrawn. In this case, owners of systems using that standard should assess the risk and take appropriate action.

[1] One purpose of the e-GIF is to reduce the reliance on specific proprietary solutions. Care must be taken that use of proprietary interfaces does not result in increased vendor lock-in.

6. Process for Review [2]

The drafting of a new version of the e-GIF will be done under the control of the Interoperability Working Group **(See Section 10).** New drafts will be put out to a wider consultation. The IWG will decide whether feedback requires a new consultation process. At the end of the process, the e-GIF will be published with any further changes.

The e-GIF specifications will inevitably change and must have the capability to change quickly when required. The change management process will ensure that the e-GIF remains up to date and is aligned to the requirements of all stakeholders and to the potential of new technology and market developments. The diagram below describes a consultation process for this document that will encourage participation and innovation.

7. e-Government Manual

The e-GIF comprises the **e-Government Manual** which contains a set of guidance documents, standards and specifications each of which can be viewed as independent, stand-alone documents. At present, two key components of the e-GIF have been completed: the e-Government Omnibus Technical Standards (e-GOTS) and the Policy on Content and Presentation Design Standards. The diagram below highlights the state of readiness of each component of the e-GIF.

In Development

Already Developed

[2] e-GOTS is necessary for the e-GIF to be implemented/executed. In this light, the review process of both documents is necessary to ensure streamlined continuity.

8. Completed Components of e-Government Manual

This section presents the completed components of the e-Government Manual as follows:

- The e-Government Omnibus Technical Standards (e-GOTS); and
- The Policy on Content and Presentation Design Standards.

A synopsis of each component is presented, while the full build out of each can be viewed via the links provided.

1. e-Government Omnibus Technical Standards (e-GOTS)

The set of e-Government Omnibus Technical Standards forms a key part of the e-GIF and identifies the standards that systems should comply with in order to be compliant with the e-GIF. Standards are categorised into five main categories: Networking, Data Integration, Application / Presentation, Security and Web Services. These categories correspond with layers in the model presented in the e-GIF. A specific standard may fit into more than one category.

1. *Networking*

Networking and interconnection form the first layer of interoperability. Networking within the e-GIF is based on the use of TCP/IP networking. Interconnectivity involves the use of high-level standards such as HTTP for web access and FTP for file transfer. Proprietary protocols may be used within a single network, or to link two networks using the same proprietary technologies. Allowing networks to interoperate without adding a layer of security is not advisable. In this regard, the security layer serves to protect the networking and interconnection layer.

2. *Data Integration*

The Data Integration category includes standards relating to the format of the data being transferred. It includes standards for character sets and character encodings, as well as file format types and standards

for data message formatting, data message definition and data transformation.

In general, information from databases will be exchanged in an agreed XML format. There are some cases where other formats may be appropriate. No standards are provided for native database formats since a variety of these types of databases are in use and the exchange of data will be done by agreement between the parties. For interworking within the Government space, some proprietary protocols are allowed which permits the full power of applications that are in use throughout GoRTT to be realized. However, more open formats are specified for use when interoperating with the public.

3. *Application/Presentation*

This category includes standards for applications and presentation, including those for VoIP, data modelling and email. Only the basic VoIP standards have been included. Further standards should be added when they are required for a specific VoIP project and detailed investigation is undertaken.

4. *Security*

This category includes standards to enable secure access to public sector information and secure exchange of information. The standards aim to ensure that information cannot be intercepted, that the receiver of the information can identify the sender and detect whether the information has been tampered with, and that the sender cannot validly claim that the information has been modified by the receiver (non-repudiation).

Many insecure protocols have secure equivalents or additional privacy layers that can be added. For example, HTTP and FTP can be used with SSL or TLS; SMTP email can be used with PGP; and SSH can be used instead of Telnet.

5. *Web Services*

A Web Service is defined by the W3C as "a software system designed to support interoperable machine-to-machine interaction over a network".

The W3C Web service definition encompasses many different systems, but in common usage the term refers to clients and servers that communicate using XML messages that follow the SOAP standard. In such systems, there is often machine-readable description of the operations offered by the service written in the Web Services Description Language (WSDL) and sometimes a service registry defined by the Universal Description, Discovery and Integration (UDDI) standard.

It should be noted that these SOAP-based web services are not the only way to invoke procedures on a remote server. Often, services can be invoked in a stateless manner using an HTTP "GET" request, or a series of such requests. Such HTTP requests can result in the running of a procedure on a server, with the

result being returned in any desired format (XML, HTML or some other format). Such services are often referred as "RESTful" services, where REST stands for "representational state transfer". RESTful services are simpler to implement than SOAP-based services. Security can be added using many of the security standards in this catalogue. SOAP-based services have the benefit of a more defined security architecture, increasing the chances that different services will be using the same set of standards.

6. *Classifications*

Standards are classified in terms of the maturity of their use within GoRTT's systems.

Since technology changes, standards have their own lifecycles. Within the context of the e-GIF, standards will be classified in one of four stages of a lifecycle as follows:

Stage 1: Classification "U"

A "U" Classification indicates that a standard is under observation. This means that the standard is listed in the e-GOTS but that active review and assessment is on-going. Any entity wishing to use this standard must consult the Interoperability Working Group (IWG).

This usually occurs in two types of cases:

- A suggestion is made that a new standard should be added to the e-GOTS; and
- The IWG has decided that a new standard should be monitored.

Stage 2: Classification "A"

An "A" classification indicates that the standard has been adopted. The scope of its use will be described in the catalogue entry for the standard. For example, a standard may be approved for use in Government-to-Government (G2G) communications, but not Government-to-Consumer (G2C) or Government-to-Business (G2B). The standard description may qualify this further, for example stating that Government systems should accept data in a particular format from the public, but that it should not generate data in that format.

Stage 3: Classification "D"

A "D" classification indicates that the standard (or a particular version of a standard) is 'deprecated'. It may still be in use within Government, but should not be used for new applications. In most cases it will have been replaced by a new version or standard.

Stage 4: Classification "W"

A "W" classification indicates that a standard has either been withdrawn or that it has been considered and subsequently rejected. Government systems will no longer use this standard. If the standard is still in use, plans must be in place to migrate away from it. The catalogue entry for a standard with a

classification of "W" will indicate the reason for its withdrawal or rejection.

The e-GOTS in its entirety can be accessed by double-clicking this image:

2. Policy on Content and Presentation Design Standards

The Policy on Content and Presentation Design Standards provides homogenous guidelines for the development of GoRTT web sites and portals to:

- Encourage enterprise wide, consistency of functionality of Internet web interfaces and end user experience;
- Improve usability of web sites by the public;
- Assure a seamless interaction of Ministry and statutory agency web sites and the e-Government Portal interface; and
- Ensure standardization of software tools used with web sites.

The Core Design Principles and Guidelines contained in the policy include:

- Accessibility;
- Navigation;
- Usability ;
- Format and Layout (including scripts and dynamic pages, graphics, and multimedia);
- Colour and Typography (including type fonts, type size and settings, margins and justification);
- Site Content (including editorial standards, privacy statement and terms of use, and language options);
- External Content and Links; and
- Domain Names.

The Policy on Content and Presentation Design Standards in its entirety can be accessed by double-clicking the image below:

9. Components of e-Government Manual to be developed

The sections below outline the components of the e-Government Manual which still need to be developed. The purpose and outline of each component is presented, accompanied by examples where appropriate.

1. Meta-Data Policy

A Metadata Policy, with suitable infrastructure, helps with indexing and searching Government information resources by adding context to a search. Dublin Core is a widely accepted metadata standard that could be referenced by GoRTT. The metadata policy will provide a set of metadata elements and descriptions of these elements, suitable for use within Government.

1. *Metadata Profile and Binding*

A **Metadata Profile** defines the appropriate content of metadata and how this metadata will be implemented throughout Government. The Profile can be used when creating metadata records that provide information about which elements should be used in a specific context (such as when applying metadata to a web page), application schema etc. While primarily used to describe digital data, the Profile can also be used to describe other resources including textual documents and various other non-digital elements.

A **Metadata Binding** describes how to encode the metadata in different formats. The Metadata Binding states how different records will encode their metadata, for example, a web page will encode its metadata as <meta> elements, while an XML Schema might use a Resource Description Framework (RDF). The UK is one Government that has implemented a Dublin Core-based metadata policy and associated profiles and bindings.

2. Data Standards Catalogue

XML formats are a set of common schemas used to describe data items commonly used within Government, such as names and addresses. Having a common set of definitions helps interoperability and reduces systems-development effort since the same definitions will be used for all interoperability requirements. In addition to a set of schemas, it is valuable to have the definitions in a syntax-independent format. This is referred to as the **Data Standards Catalogue**.

The purpose of the Data Standards Catalogue is to provide a means by which common data can be standardised. The benefits are as follows:

- Maintenance and design of existing systems is faster for all common elements and therefore costs less;
- Interchange of common data between systems is defined and simplified so that integration across systems costs less and data can be combined to create added value;
- Non database systems (usually web based systems) can use common formats for their data (using xml schema) so that the interchange of data across websites is defined; and
- A set of generic data entry standards can be produced.

1. *Policy on XML Naming and Design Rules*

A policy on XML Naming and Design Rules (NDR) will be developed to help promote consistency in XML

implementations. This helps developers as they are able to work with consistent formatting within an XML schema. The policy will be developed around the information presented below.

The main technology for data integration is XML. The benefits and advantages of XML are as follows:

- XML is an open standard, maintained by the World Wide Web Consortium (W3C), which also maintains the HTML standard;
- XML is widely supported by all major software vendors;
- XML knowledge and skills are readily available;
- XML technologies allow document and message formats to be described and documents and messages to be validated automatically against the defined formats;
- The descriptions of document and message formats are modular, allowing portions of them to be reused;
- XML documents are human readable;
- XML documents can be multi-purpose; and
- XML documents can be displayed using stylesheets.

As an example, the e-GOTS is defined as an XML document. Free tools can be used to edit this document. The web display of the formats is created by a client-side web application that operates directly on the XML document using stylesheets. Another stylesheet is used to create the PDF format.

2. *XML Schemes*

XML and Web services are widely used to promote the interoperability between systems. Unfortunately, the W3C specification for XML Schema is large and complex leaving it nearly impossible to completely understand it in its entity. Additionally, the W3C does not offer any guidance with respect to best practices or guidelines for implementing XML Schemas within enterprise environments. The purpose of this policy will be to state the best practices and guidelines that should be followed by Government to ensure consistency across the XML Schemas that are designed. These schemas will describe data that can be exchanged between systems across Government.

This document should address many of the common features and issues pertaining to XML Schema. As the W3C XML Schema specification continues to evolve and mature, this document will be modified appropriately to keep pace with industry standard best practices and guidelines. A policy on XML Naming will help promote consistency in XML implementations. This helps developers as they know they are dealing with consistent formatting within an XML schema.

3. **Guidance Documents**

Guidance documents should be produced when new technologies are deployed within Government, describing best practices in the use of the technology. These documents are administrative instruments that assist projects with similar technologies to follow the direction of previous projects. The accumulation of these documents creates a library that government Ministries and Agencies can access

when developing similar systems. Guidance documents also play a key role in the development of interoperable systems.

10. Management of the Technical Standards

1. Interoperability Working Group (IWG)

An Interoperability Working Group (IWG) will be formed to manage the e-GIF and to ensure that it remains relevant. The IWG will comprise representatives from the public sector, private sector, and relevant trade bodies[3]. It will be the main body responsible for recommending approvals of new versions of the e-GIF and e-GOTS. The IWG will report to the delegated authority, i.e. the body with responsibility for ICT governance in the public service, who will formally publish new releases of the e-GIF and e-GOTS. The terms of reference of the IWG will be to:

- Advise the Government Chief Information Officer on the on-going development and management of the Interoperability Framework and e-Government Manual;
- Update the Interoperability Framework and e-Government Manual to reflect technology advancement and application requirements;
- Monitor the effectiveness of the Interoperability Framework and suggest necessary enhancements;
- Promote and facilitate the adoption of the Interoperability Framework; and
- Encourage project teams in government to recommend changes to the e-GOTS and create additional guidelines based on their use of the standards.

The IWG will require a secretariat within the Ministry with responsibility for ICT governance in the public service. The secretariat will convene and minute meetings of the IWG, maintain a mailing list of members, and make the physical changes to the e-GIF and e-GOTS documents.

Sub-committees of the IWG may be formed, either as on-going groups or for specific tasks or to create and maintain parts of the e-Government Manual.

The IWG shall be made aware when a new GoRTT project involves the use of standards that are not currently included in the e-GOTS. In this case, the IWG shall agree on the standards to be used.

1. *Technical Policies*

In order to promote interoperability, systems must, in general, use the standards described in the relevant section of the e-GOTS. However, in cases where all parties to an interoperability requirement already use the same proprietary standards, these standards may offer higher functionality and may be used in place of those described in the e-GOTS.

[3] It may be possible to combine the role of the IWG with that of another group, such as the National Infrastructure Task Force.

In all other cases, where a suitable standard is not contained in the e-GOTS, an application must be made to the Interoperability Working Group (IWG) via the secretariat for inclusion of one or more new standards. The required standards must be described in terms of the current Omnibus Technical Standards. This means that the name and version (where applicable) of the standard should be given, with a description, main category and sub-category, usage guidance, references to external documents, reference to any relevant GoRTT documents, a rationale for selection, and the scope of the standard (G2C, G2B and/or G2G). The IWG will then consider the request and make any necessary changes to the e-GIF and e-GOTS.

Where a standard exists in the e-GOTS, but is not suitable for a specific purpose, application must be made for exemption. Such an application may trigger a revision of the descriptions in the e-GOTS at the next scheduled revision.

11. Glossary of Common Terms

Term	Definition
Data	Information in numerical form that can be digitally transmitted or processed
Dublin Core	An open organisation, incorporated in Singapore as a public, not-for-profit company which supports shared innovation in metadata design and best practices across a broad range of purposes and business models
Extensible Markup Language (XML)	Allows users to create customised tags, enabling the definition, transmission, validation, and interpretation of data between applications and organisations
File Transfer Protocol (FTP)	Uses the Internet's TCP / IP Protocols to enable data transfer
GET	A method for retrieval of information that is identified by the Request-URI.
Hyper Text Transfer Protocol (HTTP)	Defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands, each command is executed independently. Refer to RFC 2616
Information and Communication Technology (ICT)	Unified communications integrating telecommunications (telephone lines an wireless signals), computers as well as enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information
International Organization for Standardization (ISO)	The World's largest developer of voluntary International Standards. Founded ir 1947, have published more than 19,500 International Standards covering almost all aspects of technology and business.

Internet Protocol (IP)	Specifics the format of packets and the addressing scheme. This allows the user to address a package and direct it to another system, but there is no direct link between the sender and recipient
Interoperability	The ability of two or more systems (computers, means of communication networks, software and other components of information and communication technology) to interact and exchange data according to a defined method, in order to obtain the expected results.
Interoperability Working Group (IWG)	Representatives from public, private sector and relevant trade bodies responsible for recommending approvals of new versions of the eGIF and eGOTs reporting to the agency with responsibility for ICT governance in the public service
Metadata	Descriptions identifying how, when and by whom a particular set of data was collected and how it was formatted
Millennium Development Goals	The United Nations resolution adopted on September 18, 2000 during the fifty-fifth session of the General Assembly
Naming and Design Rules (NDR)	These are formal rules associated with how data elements are structured within a process of creating exchange documents between organizations. Naming and Design Rules are a set of guidelines and naming conventions that go beyond what a single data exchange standard specification will permit.
Network	A group of two or more computer systems linked together
Pretty Good Privacy (PGP)	A common method employed to encrypt messages being transmitted via the Internet
Protocols	An agreed upon format for transmitting data between devices which can be implemented either in hardware or software
Representational State Transfer (REST)	An architectural style for large-scale software design
Resource Description Framework (RDF)	A general framework for describing a website's metadata, it provides interoperability between applications that exchange machine-understandable information on the Internet. Refer to RFC 3870
Secure Shell (SSH)	A cryptographic network protocol for secure data communication exchange using a secure channel between two networked devices. Refer to RFC 4252
Secure Sockets Layer (SSL)	A security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. Refer to RFC 6101
Simple Mail Transfer Protocol (SMTP)	A protocol for sending email messages between servers and is generally used to send messages from a mail client to a mail server
Simple Object Access Protocol (SOAP)	An XML-based messaging protocol used to encode information in messages before sending them over a network and is independent of any operating system
Stylesheets	A fil e or form that defines the layout of a document

Telnet	A terminal emulation program for TCP / IP networks which runs on your device and connects to a server on the network to execute commands as though they were entered directly on the server console
The e-Government Interoperability Framework (e-GIF)	The government's technical policies and specifications for achieving interoperability and simplifying Information and Communication Technolog (ICT) systems integration across the public sector
Transmission Control Protocol (TCP)	Enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent. Refer to RFC 793
Transport Layer Security (TLS)	A protocol that guarantees privacy and data integrity between client / server applications communicating over the Internet. Refer to RFC 2246
Universal Description, Discovery and Integration (UDDI)	A web-based distributed directory that enables, businesses to list themselves on the Internet and resultant listings through search engines
Uniform Resource Identifier (URI)	A string of characters used to identify a name or resource.
Voice over Internet Protocol (VoIP)	A category of hardware and software that enables use of the Internet as a transmission medium for telephone calls by sending voice data in packets using IP
Web Services Description Language (WSDL)	An XML-formatted language used to describe a web service's capabilities as collections of communication endpoints capable of exchanging messages
World Wide Web Consortium (W3C)	A software system designed to support interoperable machine-to-machine interaction over a network