THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT

e-GOVERNMENT AGENCY

Document Title

e-Government Interoperability Framework – Standards and Technical Guidelines (e-GIF)

Document Number

eGA/EXT/GIF/001

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr.Jabiri Bakari	CEO – eGA		

Table of Contents

1. OVERVIEW

1.1. Introduction

The delivery of e-Government services involves interaction between actors, citizens, businesses and administrations, in a diverse setting, not only in terms of technology, but also in terms of how the relationships and the processes are organized and of how the necessary data and information are structured and handled. Such type of interaction within Government as a whole is derived by applying some common set of minimum standards and technical guidelines referred to as e-Government Interoperability Framework (e-GIF).

The e-Government Interoperability Framework (e-GIF) has been derived from the e-Government Enterprise Architecture as referred in *e-Government Architecture Vision - Standards and Technical Guidelines*.

1.2. Rationale

One of the objectives of the e-Government standards and guidelines is to integrate various Public Institutions in the government, such that citizens/businesses/ employees deal with one face of the government rather than individual Public Institutions for availing services. However, this requires making ICT systems and the processes they support interoperable based on well accepted standards – which are the core aims of e-GIF. e-GIF provides the Government the ability to share information and integrate information and business processes by use of common standards.

1.3. Purpose

e-GIF provides the know how to achieve interoperability of data and information within and outside the government. It enables any Public Institution to provide and receive information and integrate its processes with other Public Institutions using predetermined standards. There are multiple benefits that should be expected from e-GIF.

i. It will enable better decision making by combining data from different Public Institutions.

ii. It will also eliminate patchwork of ICT solutions in different Public Institutions that are unable to "talk" or exchange data.

iii. It will improve coordination between various Public Institutions and non-government agencies. It will enable prudent utilization of government resources by pre-empting redundancy and waste of resources due lack of coordination.

iv. It will enable the government service delivery to become more citizen-centric by breaking down the silos and allowing seamless flow of information across various Public Institutions.

v. It will lead to cost savings by improving the current systems, reducing reliance on single vendors and experience reusable from one Public Institution to another.

vi. Overall e-GIF is expected to result in better governance of e-Government initiatives in Tanzania.

2. e-GOVERNMENT INTEROPERABILITY FRAMEWORK (e-GIF)

2.1. eGovernment Interoperability Framework

e-GIF provides a framework to the Government to share, collaborate and integrate information and organisation processes by use of common standards. The diagram below demonstrates the e-GIF framework for the Government.

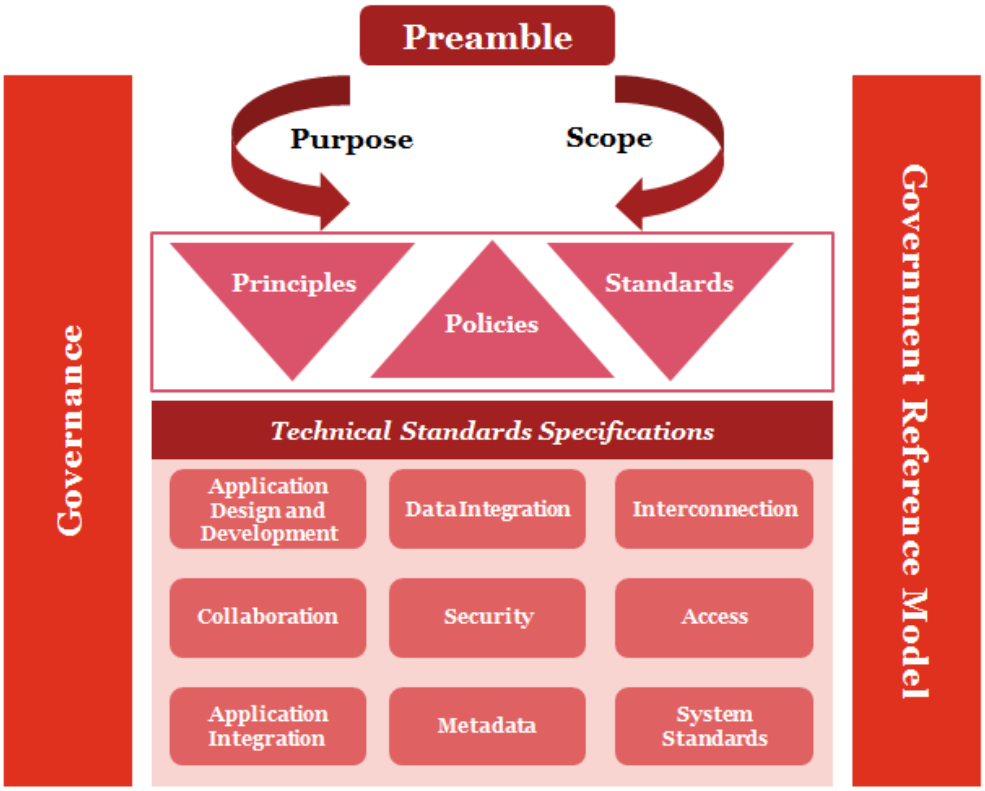


Figure II: eGovernment Interoperability Framework

A. Structure of eGovernment interoperability Framework

i. Preamble

This covers purpose and scope of the e-GIF. The overarching purpose of e-GIF in Tanzania is to improve economic growth and equity by enhancing access to information and its effective use, thereby improving delivery of services to benefit stakeholders – citizens, businesses and also Government (intra-government and inter-government).

ii. Principles

These define the guiding basis for defining the standards. The Government has a set of objectives and priorities for e-government. Based on these objectives and priorities, a set of directions are required to define policies and e-Government standards. The following key e-GIF principles:

a) Interoperability

Rationale: to ensure that policies reinforce and standards defined facilitate interoperability,

Implications:

i. eliminating patchwork of ICT solutions in different government offices those are unable to "talk" or exchange data

ii. bringing in the ability to effectively interconnect, collaborate, access and facilitate data integration in order to communicate between different stakeholders (Government to Government-G2G, Government to Citizen-G2C, and Government to business-G2B etc.).

b) Share, Re-Use and Collaborate

Rationale: to propagate sharing, re-use and collaboration

Implications:

i. Identifying common components (including existing Government policies, standards, application, technology etc. wherever relevant) across the interoperability domain and defining policies, standards, and procedures to ensure reusability of artefacts. For e.g. defining data structure, data sets at a government level.

ii. Choosing standards that will enable more flexibility and reduce the administrative burden.

c) Scalability

Rationale: to ensure that standards meet the changing and growing Public Institutions needs

Implications:

i. Requirements and the applications and technologies will scale up, adapt and respond to such requirement changes and demand fluctuations.

d) Confidentiality

Rationale: to ensure that the confidential information and data are properly classified and adequately protected whether for government, citizens or businesses.

e) Adherence to open standards

Rationale: to provide for choice of vendor to promote competitiveness and opportunity to look at integrated platforms.

Implications: The attributes of open standards such as platform independence, vendor neutrality and ability to use across multiple implementations and the model for establishing open standards will finally allow for sustainable information exchange, interoperability and flexibility.

iii. Policies

These include eGovernment Policy and National ICT policy, act as enforcement guidelines for implementing the principles and standards. Guidelines and Technology standards establish direction and technical requirements which govern the acquisition, use and management of ICT resources for the ICT initiatives undertaken by Public Institutions.

Mwongozo wa matumizi bora, sahihi na salama ya vifaa na mifumo ya TEHAMA serikalini, provides directives covering various aspects of e-GIF which are to be followed by Public Institutions. These directives include both organizational level guidelines and even those relating to different technical standard areas:

a) Overall e-GIF Guidelines
b) Application and technology Guidelines
c) Data and meta data Guidelines
d) Security Guidelines
e) Data protection guidelines

iv. Standards

These are foundations upon which to develop new technologies and an opportunity to share and enhance existing practices.

v. Government Reference Model

This coexist with e-GIF coherently, so that both the initiatives complement each other and reduce redundancy through shared principles, artefacts etc.

vi. Governance

This is the key to implement and maintain interoperability initiatives. Leading practices suggest clearly, that all successful e-GIF have a clearly defined governance mechanism. The implementation of e-GIF includes creating and educating e-GIF framework (standards/ policies/ principles) across all Public Institutions maintaining standards by updating it continually and ensuring compliance to standards across government.

vii. Technical Standards Specifications

There are nine technical standards areas namely Interconnection, Data Integration, Access, Collaboration, Application Design and Development, Application Integration, System Standards, Meta Data and Security identified under e-GIF. The table below covers 9 areas.

Table I: Technical Standards Specifications

Service Area	Technical Areas
1. Interconnection	Recommended interoperability standards to enable interconnection and communication between different Public Institutions over networking environment. Interconnection covers interoperability components/infrastructure and technical specifications required to enable communication between different systems and the exchange of information over the networking environment. Interconnection is used when Public Institutions each have their own clients and must

Service Area	Technical Areas
	interconnect with other Public Institutions to provide a comprehensive service. Based on understanding of the Tanzania environment, the interconnection standard is vital for successful interoperability among the different Public Institutions. The section below describes the way in which the interconnection part of e-GIF is organized. The interconnection standard is segmented into following areas: **telecom level, Public Institution level and integrated system.** Telecom Level is further divided into three major sections for interconnection: i. Access Transmission Network Standard ii. Fixed Line Next-Generation Network Standard (FL-NGN) iii. 2nd, 3rd and 4th Generation Mobile Network Standard Public Institution Level is further divided into three major sections for interconnectivity: i. Physical Infrastructure Layer Standard ii. Institutional Level IP Network Layer Standard iii. Protocol Layer Standard Integrated System is further divided into two areas: i. Internet Service Providers Standard ii. Financial Services Connectivity Standard **Components** Interconnection –Telecom i. Access Transmission Network

Service Area	Technical Areas
	ii. Fixed Line Next Generation Network iii. Next Generation Mobile Network Standards Interconnection- Public Institution i. Physical Layer Infrastructure ii. Application Layer Protocols iii. Transport Layer Protocols
2. Information access and presentation	Recommended interoperability standards to enable users to effectively access information and service electronically in an interoperable data presentation format. Access relates to provision to be made to enable users to effectively access information and service electronically via a range of delivery channels (e.g. World Wide Web) and devices (e.g. personal computers, mobile phones, PDAs) for their needs via a range of delivery channels. This is realized by using components as per technical specifications standards to enable delivery of service, user interfaces and interaction models. This is also connected with security standards to ensure security of access, integrity of data and privacy requirements. **Components** i. Access Token ii. Animation iii. Compression iv. Kiosk v. Mobile devices vi. Scripting vii. Smart Card viii. Directory Access

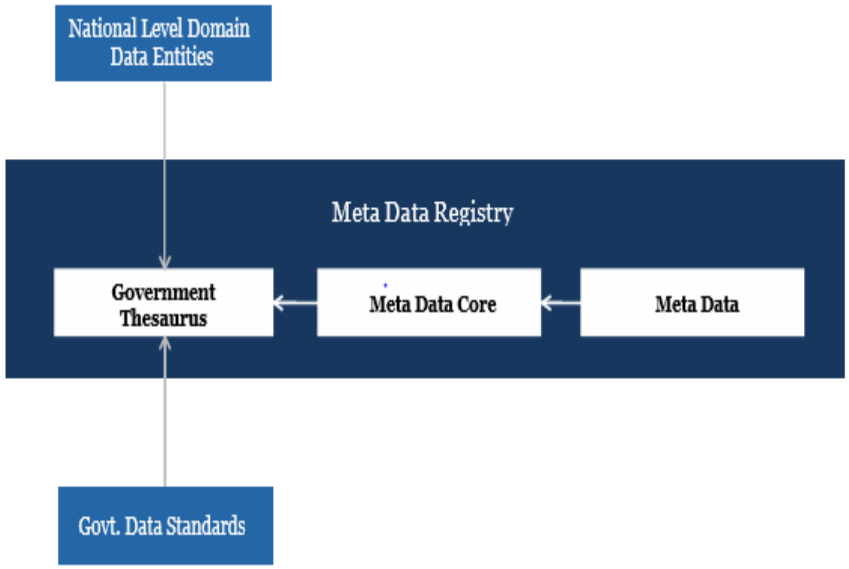
Service Area	Technical Areas
	ix. Web Access standard x. Web browser xi. Work stations
3. Collaboration	Recommended interoperability standards to enable users to collaborate, share information and services electronically. Collaboration covers components and technical specifications required to enable users to collaborate, to share information and services electronically e.g. Email, video conferencing etc. **Components** i. Email System ii. Enterprise Content Management iii. IP Telephony iv. Video Conferencing
4. Data integration	Recommended interoperability standards to enable data interchange and transformation. Data Integration provides for aggregation of data from disparate sources and facilitates inter organisational communication. Use of standards for representation of data and suitable converters such as Optical Character Recognizing (OCR) engines enable aggregation. It covers components and technical specifications required to support the recognition of data (text, images, maps and multimedia.), codes, recognition methods, interpretation formats, converters and filters. **Components** i. Character and encoding for information interchange ii. Data description

Service Area	Technical Areas
	iii. Data exchange & Transformation iv. Data exchange Formats v. Ontology-based information exchange vi. Data modelling language vii. Data integration meta language viii. Minimum interoperable character set ix. Digitization x. Data Definition for Smart Cards
5. Application integration	Recommended interoperability standards to enable multiple Public Institutions applications to interact and integrate both internally and externally for information sharing and exchange. It facilitates development and deployment of e-Services composing services from multiple applications. Application standards includes standards and specification pertaining to design and development of Application. The conformance to the standards and their use will ensure longer lifecycle of applications. These standards are not protocols or specification, these standards are typically a recommended approach and guideline to design/procure and implement applications of various types. It is important to have key recommendations in terms of application design and development because for the Public institutions have legacy applications, new application design and development are be based on latest standards. There will be tremendous growth in applications in the coming years due to operationalize business process re-engineering (BPR) and moving towards e-Services. These application standards will serve as a guidance to ensure interoperability.

Service Area	Technical Areas
	Development and deployment of e-Services will require multiple applications to be composed to provide services. Composing applications requires Application integration. Application integration may also use services running on a legacy system through a thin-client browser or a service that enables the execution of multiple application functions from an integrated user interface. The methods used to achieve this integration include web services, message oriented middleware, remote procedure calls and object request brokers. **Components** i. Message oriented Middleware ii. Object request brokers iii. Remote procedure calls
6. Application Design & Development	Recommended interoperability standards to facilitate application design and development for computers and mobile devices. **Components** i. Application Development For Handheld Devices ii. Application development framework iii. Business Rules, Logic and Objects iv. Commercial, off-the-shelf applications(COTS) v. Geographic information system vi. Modeling design and development vii. Programming language for Application Development viii. Reporting tools ix. Software configurations Management (SCM)

Service Area	Technical Areas
	x. Service Oriented Architecture xi. Smart Card Applications
7. Security management	Recommended interoperability standards to enable secure exchange of information as well as the secure access to public sector information and services. Security covers components and technical specifications needed to enable the secure exchange of information as well as the secure access to public sector information and services. **Components** i. Access management ii. Anti-Spam iii. Anti-Virus/Anti Spyware iv. Desktop Firewall v. Digital Signature vi. Email Security vii. Encryption Algorithm viii. Enterprise Firewall ix. Identity , Authentication, authorization and privacy x. Identity management xi. Intrusion detection and prevention xii. IP Encapsulation security xiii. IP security xiv. Layer 2 Security xv. Proxy server xvi. Public key infrastructure xvii. Remote Security

Service Area	Technical Areas
	xviii. Secure transport xix. Virtual Private Network xx. XML security standards xxi. Physical Security
8. Business services including data & metadata	Recommended interoperability standards pertaining to specific business areas like Finance (e.g. XBRL), e-Health (e.g. HL7, SNOMED Clinical Terms), e-Learning (e.g. SCORM), HR (e.g. HR-XML), e-News, e-Payment (e.g. PCI DSS, PCI PED, EMV, 3D secure etc.). There are various standards bodies, business communities and other groups working on specifications for the exchange of specific content-related information. They fall into two broad classes: one represents particular business objects, such as invoices; the other class defines a transaction, for example the submission of an invoice or a deposit into a particular account. Some specifications focus on common business objects and some on standardizing complex transactions. Further, some proposed specifications include a single schema for a single business object, while others are frameworks that propose rules and structure for classes of schemas and may include more than one individual schemas. This will include some of the important business area which usually require standardisation. For the government data to be truly interoperable defining the standards and policies governing the data and the metadata used across the Public Institutions applications and services is very much essential. **Data & Metadata** The metadata and data standards and continuously being developed as e-Government initiatives emerge. The standards

Service Area	Technical Areas
	are developed as per a defined process which ensures coordination *(Refer to Information Architecture – Standards and Technical Guidelines).* Broadly the data entities should be categorized as: **Generic (Common) Data Entities** –These are the common data entities that will be useful for information exchange across the Public Institutions. Some of the generic data entities include Person, Person Name, Company, Address, Party Address, Party Identifier etc. **Public institutions Specific Data Entities**- These are the data entities specific to the business process of the Public Institutions and based on the National Level Domain Data Entities identified. Some of the specific data entities includes Vehicle, Vehicle Type, Vehicle Owner, Driving License, License Category for Department of Transport. A thesaurus reflecting the generic and the special segment will be developed as illustrated below. 

Service Area	Technical Areas
	The Thesaurus will be updated as per an established process with maintenance tools. This include: i. **Data Standards:** The e-Government Interoperability Framework (e-GIF) mandates the adoption of XML and the development of XML schemas as the cornerstone of the government interoperability and integration strategy. A key element in the development of XML schemas is an agreed set of Data Standards (DS). The data standards provide the detailed description of the data entity structure and its data elements. The detail may also include as appropriate high level representation for access and use. ii. **Meta Data Core:** These are core set of Metadata that may be described using XML. To publish and make available and facilitate access, metadata about data standards as per elements and qualifiers is recommended for use. RDF standards may also be used. These Metadata will be used for any type of document. iii. **Meta Data:** These will comprise attributes about data additional to the Dublin core in accordance with the elements and qualifiers e.g. in library management, Contact, document form, citation, channels etc. These Metadata can be domain specific which will get reflected on any document including data standards. iv. **National level Domain Data Entities:** It is envisioned creation and maintenance of

Service Area	Technical Areas
	national level data domain entities in accordance with a coordinated process. These data entities will establish and keep up to date the data entities. The entities are domain specific e.g. Tax Administration, Transport, Land Reforms & Management, Municipality, Judiciary, Telecom Regulations etc. v. **Meta Data Registry:** The Meta data core, Meta Data will be held in a Registry (Meta Data Registry) which may be conceptually understood as a catalogue in a Library of books. By using tools the registry should be searched for selection and retrieval in application development thus enabling reuse. Adding resources to the Registry enables collaboration. There are tools to manage the master data that is stored in the database and keep it synchronized with the transactional systems. vi. The meta data standards given in this document is a structure with details on Meta data core, sample meta data, sample data standards structure and initial set of Government Thesaurus with common entities. The following should be entrusted to the Meta data working group which covers: a. Endorsement of Elements and its adoption b. Develop a Government wide Thesaurus c. Define National Level Domain entities (Public Institution wise or common)

Service Area	Technical Areas
	d. Develop and enhance government Data Standards e. Develop a registry. **Components** i. Finance ii. Workflow and Web Services iii. e-Health iv. e-Learning v. Legal vi. HR vii. E-News
9. System standards	Recommended interoperability standards and guidelines pertaining to application, web, portal and database servers, hardware platform, storage devices, desktop, mobile and server operating systems, ICT operations management, backup and recovery etc. This will include standards pertaining to system software and hardware such as server O/S, database server, portal servers etc. **Components** i. Application Servers ii. Backup Recovery iii. Business Intelligence iv. DB Connectivity and access technology v. DBMS vi. Desktop O/S

Service Area	Technical Areas
	vii. Directory Services viii. Hardware Platforms ix. ICT Operations Management x. Mobile O/S xi. Portal servers xii. Server O/S xiii. Storage Devices xiv. Web Server

B. Deployment of eGovernment Interoperability Framework (eGIF)

Nationwide infrastructure, will be deployed by the government so that the information governed by e-GIF flows across the Public Institutions. e-GIF will be a vital element for managing e-Government interconnectivity, data integration, e-Services access and content management. It will also facilitate exchange of information effectively with other equally interoperable bodies, changing internal systems and practices, to make them interoperable. The custodian of the e-GIF will be the e-GIF Working Group as defined in the Process and Governance for Enterprise Architecture. This group will work with the security architecture working group to document systems, security controls, and the environment topologies, conduct awareness on security for every Public Institution.

Standards for eGIF are based on the objective and principles of e-GIF. Any policy and standards defined in e-GIF shall be consistent and compliant with the existing e Government policies and standards wherever relevant. Whenever a new version of e-GIF is released or enhanced/revised, it is mandatory to train the e-GIF working group committee members who shall in turn be mandated to train the concerned/identified ICT resource in each Public Institutions across government.

The standards for eGIF are aligned with the World Wide Web (WWW) standards. The guidelines for XML Schemas that will be used for all new applications will continuously be developed by the Working groups. These guidelines will include mandatory requirements for XML Schema structure and content. Also, working with data owners,

will be developed and government wide data set and centralization of Meta data will be done. The Meta data standards are primarily based on the international Dublin Core model (ISO 15836).

e-GIF has dimensions, as demonstrated in the diagram below:

i. Business process or organizational interoperability;
ii. Information or semantic interoperability; and
iii. Technical interoperability.

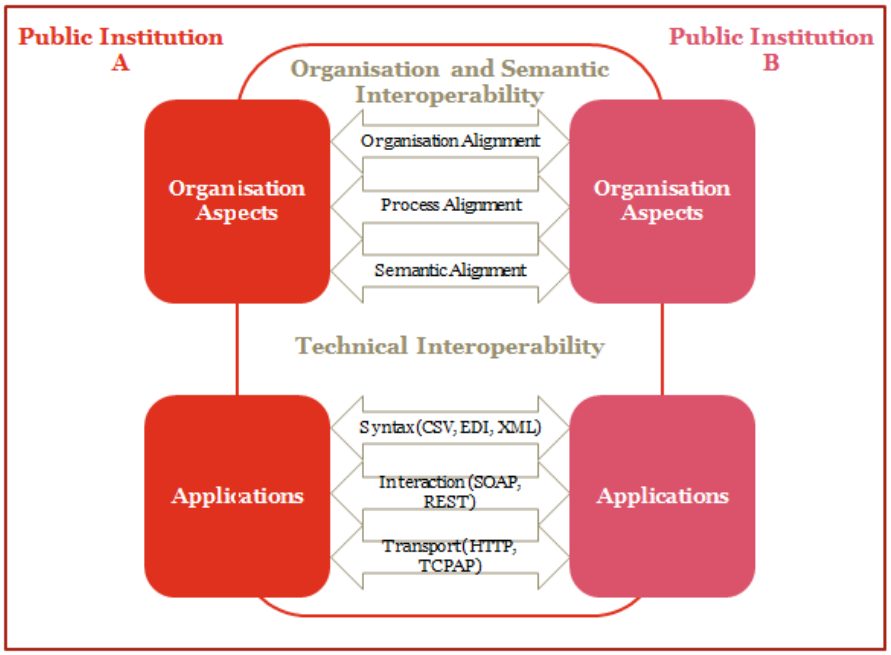


Figure II: Dimensions of e-GIF

Table II: Dimensions of e-GIF

Business Process or Organizational interoperability	Relates to the collaboration between entities in the development, deployment and delivery of e- Government services, and to the interaction between services, and supporting processes. Specifically, business process or organizational interoperability deals with defining Public Institution's goals, common methods, modelling business processes, defining shared services etc. *Refer to Appendix – Illustration No.1 Typical Interaction Points.*

Information or semantic interoperability	Relates to the communities of practice and to the negotiation of meaning that occurs within them. It is also concerned with ensuring that the exact meaning of information from various applications are understandable by any application even though if the application was not developed for this purpose. For e.g. semantic interoperability services can be used when a citizen relocates his home and business from one region to another by means of single interaction. Linking the user's name to their business and retrieving residential and business addresses, telephone numbers etc. will ensure interoperability. In some countries a common words thesaurus is prepared for commonly used terms, for example in accounting and administration functions all Public Institutions make use of terms such as Acquisitions, Contracting out, e- Procurement, Outsourcing, Procurement and Tendering.
Technical interoperability	Technical interoperability is the most common and basic aspect of interoperability. This is necessary to ensure that all the hardware and software components of the network and information system should physically communicate and transfer information successfully. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services etc.

2.2. e-Government Interoperability Framework (e-GIF) Standards

A. Principles

2.2.1. Public institutions will adopt design principles of e-GIF that are described in *Section 2.1 A. ii.*

B. Technical Standards

e-GIF Technical Standards are based on nine components Technical Standard Specifications of figure II. Each component has:

i. One or more requirement/specification that needs to be followed to ensure interoperability.

ii. The standards table that briefly represents the standards/requirements/ status and enforcement policies. For additional information on each component/standard, the details of the standards with resource locator (source) to the relevant standard are provided in the section below. The hyperlinks for the detailed standards/requirement for each component have also been provided in the Reference and Links guideline column.

2.2.2. Interconnection

Table III: Detailed standards/requirement for each component provided in the Reference and Links

Standards Proposed	**Mandatory/ Recommended**	**Reference & Guidelines**
Interconnection –Telecom		
Access Transmission Network		
Coarse Wave Division Multiplexing (CWDM) should be the standard for transmitting multiple wavelength signals through the same fibre optic cable.	Mandatory	***CWDM*** http://www.itu.int/itudoc/itu-t/aap/sg15aap/history/g.694.2/index.html
FTTB (Fibre To The Building), FTTH (Fibre To The Home), FTTD (Fibre To The Desk) should be the stand for	Recommended	Section 4.1.1.2 FTTx of ITU

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Interconnection –Telecom		
RING topology with Failover/Auto-Recovery function		
Fixed Line Next Generation Network		
ADSL2 should be the standard to address the bandwidth increase. ADSL2+ should be considered in near future.	Mandatory	***ADSL (ITU G.992.2)*** http://www.itu.int/rec/T-REC-G.992.2/en ***ADSL2+ (ITU G.992.5)*** http://www.itu.int/rec/T-REC-G.992.5/en
VDSL2 should be the standard for HDTV, VoD, VC, high speed Internet access and advanced voice services including over a standard copper telephone cable.	Recommended	VDSL2 (ITU-T G.993.1) http://www.itu.int/rec/T-REC-G.993.1/en
Passive optical network (PON) should be the standard to enable a single optical fibre to serve multiple premises.	Mandatory	***EPON (IEEE 802.3av)*** http://www.ieee802.org/3/av/ ***GPON (ITU-T G.984)*** http://pmcs.com/products/optical_networking/ftth_pon/
WiMAX should be considered for wireless broadband voice, data and video transfer at large distances. It is recommendatory to use WiMAX for area that are hard to reach with	Recommended	The fixed WiMax standard IEEE 802.16-2004 (also known as 802.16d). The 802.16 includes two

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Interconnection –Telecom		
fixed line as well as business that demand higher bandwidth than CDMA 1x EV-DO connectivity.		sets of standards, 802.16-2004 (802.16d) for fixed WiMAX and 802.16- 2005(802.16e) for mobile WiMAX.
Next Generation Mobile Network		
Mobile Broadband should be the standard followed for a range of data applications. It is Recommended to use 3G mobile access radio such as WCDMA as much as possible in order to elevate the limitation of upgrading to HSPA without significant upgrading cost. 4G networks must be based on an all Internet protocol (IP) packet switching instead of circuit-switched technology, and use OFMDA multi-carrier transmission methods or other frequency-domain equalization (FDE) methods instead of current spread spectrum radio technology.	Recommended	***GSM/WCDMA-HSPA+Network*** http://www.3gpp.org/
CDMA2000 1X (IS-2000 - also known as 1x and 1xRTT) should be the core CDMA2000 wireless air interface standard.	Mandatory	***CDMA 1x EVDO rev 0*** http://cdg.org/news/press/2009/Aug17_09.asp
CDMA2000 1xEV-DO (Evolution-	Mandatory	

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Interconnection –Telecom		
Data Optimized), often abbreviated as EV-DO should be the telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access.		***CDMA 1x Rev A*** http://cdg.org/news/press/2009/Aug17_09.asp

Interconnection –Public Institutions

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Physical layer infrastructure		
A 19-inch rack should be used for mounting multiple equipment modules.	Mandatory	
Cat 6 or better should be used for physical infrastructure within a 100m length.	Mandatory	***Cat 6 Cable (TIA/EIA-568-B)*** http://www.tiaonline.org/standards
Information outlet with Cat 6 or better should be used to terminate cables to end users.	Mandatory	***Information Outlet (TIA/EIA-568 –A or B)*** www.tiaonline.org/standards ***Information Outlet (ISO/IEC 11801)*** http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45020
A Copper patch panel with Cat 6 or better should be used for the termination of Copper cable connections	Mandatory	***Copper Patch panel (TSB-40-A)*** www.tiaonline.org/standards
A Copper patch cord with Cat 6 or better cable should be used to connect circuits on a patch panel to switches or from outlets to end devices.	Mandatory	***Copper Patch Cords (TIA/EIA-568-B)*** www.tiaonline.org/standards
Fibre optic should be used for carrying data above 100m length.	Mandatory	***Optical Fibre Cables (TIA/EIA-568-B.3)***

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
		www.tiaonline.org/standard
A fibre pigtail should be used to extend fibre optic cables or to terminate fibre core cables on fibre patch panel.	Mandatory	***Fibre Pigtail (TIA/EIA-604-10-A)*** www.tiaonline.org/standards – Fibre Pigtail (IEC 61754-20)
A fibre patch panel should be used for distributing and rearranging fibre cable connections and circuits.	Mandatory	***Fibre Patch Panel (TIA/EIA-568-B.3)*** www.tiaonline.org/standards
A fibre patch cord should be used to attach one device to another for signal routing.	Mandatory	***Fibre Patch Cords (TIA/EIA-568-B.3)*** www.tiaonline.org/standards
A Data Centre should house computer systems and associated components, such as telecommunications and storage systems.	Mandatory	
Disaster recovery process, policies and procedures should be planned for recovery or continuation of technology infrastructure.	Mandatory	***Disaster recovery guidelines (ISO/IEC 24762)*** www.iso.org/iso/catalogue_detail.htm?csnumber=41532
Load Balancing should be	Recommended	

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
considered to distribute workload evenly across two or more links in order to get optimal resource utilization, maximize throughput, minimize response time and avoid overload.		
Infrastructure of data centre should include systems that are important for the safety of data centre such as fire suppression, control etc. that should be available in a data centre.	Mandatory	***Data centre infrastructure (TIA-942)*** www.tiaonline.org/standards The TIA-942 specification references private and public domain data center requirements for applications and procedures such as: i. Network architecture ii. Electrical design iii. File storage, backup and archiving iv. System redundancy v. Network access control and security vi. Database management

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
		vii. Web hosting viii. Application hosting ix. Content distribution x. Environmental control xi. Protection against physical hazards (fire, flood, windstorm) xii. Power management
Public Institution Level IP Network		
All ICT equipment should be IPv6 Compatible. It is Recommendatory to have a managed switch so as to control and have security from anybody walking in to the Enterprise's LAN.	Recommended	-
Application Layer Protocols		
Border Gateway Protocol should be used as the core routing protocol of the internet.	Mandatory	***BGPv4 (RFC 4271)*** http://www.rfc-editor.org/rfc/rfc4271.txt
DNS should be used for resolution of names that locate computers assigned with IP addresses.	Mandatory	***DNS (RFC 1034)*** http://www.rfc-editor.org/rfc/rfc1034.txt
DHCP should be used by devices (DHCP clients) to obtain configuration information for	Mandatory	***DHCP IPv4 (RFC 2131)*** http://www.rfc-editor.org/rfc/rfc2131.txt

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
operation in a network dynamically.		***DHCP IPv6 (RFC 3315)*** http://www.rfc-editor.org/rfc/rfc3315.txt
File Transfer Protocol (FTP) should be used to exchange and manipulate files over an Internet Protocol computer network, such as the Internet.	Recommended	***FTP (RFC 0959)*** http://www.rfc-editor.org/rfc/rfc959.txt
FTPS should be used for exchanging and manipulating files over internet securely.	Recommended	***FTPS (RFC 4217)*** http://www.rfc-editor.org/rfc/rfc4217.txt
GPRS Tunnelling Protocol (GTP) should be considered to carry General Packet Radio Service (GPRS) within GSM and UMTS networks.	Recommended	***GTP*** www.3gpp.org/ftp/Specs/html-info/29060.htm
Hypertext Transfer Protocol (HTTP) should be used to distribute and collaborate, hypermedia information systems.	Mandatory	***HTTP (RFC 2616)*** http://www.rfc-editor.org/rfc/rfc2616.txt
HTTPS should be used to distribute and collaborate hypermedia information systems securely.	Mandatory	***HTTPS (RFC 2818)*** http://www.ietf.org/rfc/rfc2818.txt
IMAP should be used for accessing mailboxes.	Mandatory	***IMAP (RFC 1203)*** http://www.rfc-editor.org/rfc/rfc1203.txt
Internet Relay Chat (IRC) should be considered for the use of real-time	Recommended	***IRC (RFC 2813)*** https://www.rfc-

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Internet text messaging or synchronous conferencing.		editor.org/rfc/rfc2813.txt
Light Weight Directory Access Protocol should be used for querying and modifying directory services running over TCP/IP.	Mandatory	***LDAP (RFC 4510)*** https://www.rfc-editor.org/rfc/rfc4510.txt
Megaco (H.248) should be considered for controlling Media Gateways on IP networks and the public switched telephone network (PSTN).	Recommended	***Megaco*** https://www.itu.int/itudoc/itu-t/com13/ipexpert/ipmedia/71391.html
Media Gateway Control Protocol should be considered for controlling media controllers on IP and telephone Networks similarly as Megaco.	Recommended	***MGCP*** http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8651&lang=en
MIME (Multipurpose Internet Mail Extensions) should be used for formatting non-ASCII messages so that they can be sent over the Internet.	Mandatory	***MIME (RFC 2633)*** http://www.rfc-editor.org/rfc/rfc2633.txt
The multiprotocol BGP should be considered to enable multicast routing policy within and between BGP autonomous systems because it adds features to BGP.	Recommended	***MP-BGP(RFC 4760)*** http://www.rfc-editor.org/rfc/rfc4760.txt
Simple Network Management Protocol (SNMP) should be used to monitor network systems and	Mandatory	***SNMP (RFC 3411)*** http://www.rfc-editor.org/rfc/rfc3411.txt

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
network-attached devices for conditions that warrant administrative attention.		
The Network News Transfer Protocol (NNTP) should be used for transporting Usenet news articles between servers.	Recommended	***NNTP (RFC 3977)*** http://www.rfc-editor.org/rfc/rfc3977.txt
The Network Time Protocol (NTP) should be used for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.	Mandatory	***NTP (RFC 1305)*** http://www.rfc-editor.org/rfc/rfc1305.txt
POP (Post Office Protocol) should be used to retrieve e-mail from a mail server.	Mandatory	***POP (RFC 1939)*** http://www.rfc-editor.org/rfc/rfc1939.txt
The Routing Information Protocol (RIP) should be used to route packets in local and wide area networks.	Mandatory	***RIPv2- RFC 2453*** http://www.rfc-editor.org/rfc/rfc2453.txt
Remote Procedure Call (RPC) should be used to execute procedures in another address.	Recommended	***RPC*** http://rfc-editor.org/rfc/rfc5531.txt
Real-time Transport Protocol (RTP) should be used to deliver audio and video over the Internet.	Recommended	***RTP(RFC 3550)*** http://www.rfc-editor.org/rfc/rfc3550.txt
Real Time Streaming Protocol should be used, for controlling streaming data over an Internet	Recommended	***RTSP(RFC 5560)*** http://rfc-editor.org/rfc/5560.txt

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Protocol network.		
SCP should be used to allow clients to have multiple conversations over a single TCP connection.	Recommended	***SCP*** www.w3.org/Protocols/HTTP-NG/http-ng-scp.html
The Session Description Protocol (SDP) should be used for describing streaming media initialization parameters in an ASCII string.	Recommended	***SDP(RFC 4566)*** https://www.rfc-editor.org/rfc/rfc4566.txt
The Session Initiation Protocol (SIP) should be considered for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP).	Recommended	***SIP (RFC 3261)*** http://www.rfc-editor.org/rfc/rfc3261.txt
Simple Mail Transfer Protocol (SMTP) should be used for transmitting electronic mails (e-mail) across Internet protocol networks.	Mandatory	***SMTP (RFC 5321)*** http://www.rfc-editor.org/rfc/rfc5321.txt
Simple Object Access Protocol, XML-based messaging protocol should be used for encoding standards for web services messages.	Mandatory	Simple Object Access Protocol, XML-based messaging protocol should be used for encoding standards for web services messages.
Secure Shell should be used for exchanging data between two	Mandatory	***SSHv2***

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
networked devices securely.		http://www.rfc-editor.org/rfc/rfc4251.txt
Telnet (teletype network) should be used on the Internet or local area networks to provide a bidirectional interactive communications facility.	Mandatory	***Telnet (RFC 854)*** http://www.rfc-editor.org/rfc/rfc854.txt
Trivial File Transfer Protocol should be used to transfer small amounts of data between hosts on a network.	Recommended	***TFTP (RFC 1350)*** http://www.rfc-editor.org/rfc/rfc1350.txt
Extensible Messaging and Presence Protocol (XMPP) should be considered to be used in extensible instant messaging (IM) and in the near future for message oriented middleware.	Recommended	***XMPP (RFC 3920)*** http://rfc-editor.org/rfc/rfc3920.txt
Transport Layer Protocols		
Data gram Congestion Control Protocol (DCCP) should be used to enforce reliable connection setup, teardown, congestion control, and feature negotiation.	Recommended	***DCCP*** i. http://www.rfc-editor.org/rfc/rfc4340.txt ii. http://www.rfc-editor.org/rfc/rfc5595.txt iii. http://www.rfc-editor.org/rfc/rfc5596.txt
Explicit Congestion Notification (ECN) should be used for an end-	Mandatory	***ECN*** *i.* http://www.rfc-

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
to-end notification of network congestion without dropping packets		editor.org/rfc/rfc3168.txt
Resource Reservation Protocol (RSVP) should be considered for the use of reserving resources across a network for an integrated services internet.	Recommended	***RSVP (RFC 2205)*** i. http://www.rfc-editor.org/rfc/rfc2205.txt
Stream Control Transmission Protocol (SCTP) should be used for transporting packets in a network.	Recommended	***SCTP (RFC 4960)*** i. http://www.rfc-editor.org/rfc/rfc4960.txt
Transmission Control Protocol (TCP) should be used for communication between server and a single client.	Mandatory	***TCP (RFC 793)*** i. https://www.rfc-editor.org/rfc/rfc793.txt
User Datagram Protocol (UDP) should be used for broadcasting or multicasting of data.	Mandatory	***UDP (RFC 0768)*** i. https://www.rfc-editor.org/rfc/rfc768.txt
Xpress Transport Protocol (XTP) should be used for high-speed networks for error control, flow control, and rate control.	Recommended	i. XTP ii. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=558148
Internet Layer Protocols		
Internet Control Message Protocol (ICMP) should be used by networked computers' operating	Mandatory	***ICMP (RFC 0792)*** https://www.rfc-editor.org/rfc/rfc792.txt

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
systems to send error messages.		
Internet Group Management Protocol (IGMP) should be used for managing the IP multicast groups by IP hosts and adjacent multicast routers to establish multicast group memberships.	Mandatory	***IGMP (RFC 3376)*** http://rfc-editor.org/rfc/rfc3376.txt ***IGMP (RFC 4604)*** http://rfc-editor.org/rfc/rfc4604.txt
Internet Protocol (IP) should be used for delivering packets.	Mandatory	***IPv4(RFC 791)*** http://www.rfc-editor.org/rfc/rfc791.txt ***IPv6(RFC 2460)*** http://www.rfc-editor.org/rfc/rfc2460.txt
Intermediate System (IS)-IS should be used by network devices (routers) to determine the best way to forward data grams through a packet-switched network.	Mandatory	***IS-IS (RFC 1142)*** http://www.rfc-editor.org/rfc/rfc1142.txt
Multi-Protocol Label Switching(MPLS)-OAM should be used to monitor network operation in order to detect network faults and measure its performance	Mandatory	***MPLS-OAM (ITU-T Y.1731)*** www.itu.int/itudoc/itu-t/aap/sg13aap/recaap/y1731/
Multi-Protocol Label Switching-traffic switching- MPLS-TE should	Mandatory	***MPLS-TE (RFC 2702)***

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
be used to replicate and expand MPLS-enabled network upon the traffic engineering capabilities of Layer 2 ATM and Frame relay networks.		http://www.rfc-editor.org/rfc/rfc2702.txt
Multicast source discovery protocol (MSDP) should be used to connect multiple PIM Sparse-Mode (PIM-SM) domains together or other protocols.	Recommended	***MSDP (RFC 3618)*** http://www.rfc-editor.org/rfc/rfc3618.txt
Protocol Independent Multicast (PIM) should provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet.	Recommended	***PIM-SM (RFC 2362)*** http://www.rfc-editor.org/rfc/rfc2362.txt ***PIM-DM (RFC 3973)*** http://www.rfc-editor.org/rfc/rfc3973.txt
Quality of Service (QoS) should be used to provide different priority to different users or data flows or guarantee a certain level of performance to a data flow in accordance with requests from the application program.	Mandatory	***QoS(IEEE 802.1p)*** http://www.ieee802.org/1/pages/802.1D.html
Resource Reservation Protocol-Traffic engineering (RSVP-TE) should be used to support the reservation of resources across an IP network. It runs on both IPv4	Mandatory	***RSVP-TE (RFC5151)*** http://www.rfc-editor.org/rfc/rfc5151.txt

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
and IPv6.		
Source Specific Multicast (SSM) should be used to deliver multicast packets from a specific source address requested by the receiver.	Mandatory	***SSM(RFC 4607)*** http://www.rfc-editor.org/rfc/rfc4607.txt
Virtual Router Redundancy Protocol (VRRP) should be used to increase the availability of the default gateway servicing host on the same subnet.	Mandatory	***VRRP (RFC 3768)*** http://www.rfc-editor.org/rfc/rfc3768.txt
Link Layer Protocol		
Address Resolution Protocol (ARP) should be used to map an IP address to a MAC address.	Mandatory	***ARP (RFC 5494)*** http://rfc-editor.org/rfc/rfc5494.txt
Fibre distributed data interface(FDDI) should be the standard for data transmission in a local area network that can extend in range up to 200 kilometres (124 miles).	Recommended	***FDDI*** www.t13.org/Documents/UploadedDocuments/meetings/d97003.doc
Layer 2 Tunnelling Protocol (L2TP) should be used to support virtual private networks (VPNs).	Mandatory	***L2TP (RFC 3931)*** http://www.rfc-editor.org/rfc/rfc3931.txt
Multiprotocol Label switching (MPLS) should be the mechanism used to direct and carry data from one network node to the next.	Mandatory	***MPLS (RFC 3031)*** http://www.rfc-editor.org/rfc/rfc3031.txt
Neighbour Discovery Protocol (NDP)	Recommended	***NDP (RFC 4861)***

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
should be used for discovery of other nodes on the link, information about the paths to other active neighbour nodes.		http://rfc-editor.org/rfc/rfc4861.txt
Open Shortest Path First (OSPF) should be used to route packets in an IP network dynamically.	Mandatory	***OSPF v3 (RFC 5340)*** http://www.rfc-editor.org/rfc/rfc5340.txt ***OSPFv2 (RFC 5709)*** http://www.rfc-editor.org/rfc/rfc5709.txt
Point to Point (PPP) protocol should be used to establish a direct connection between two networking nodes and provide Authentication.	Mandatory	***PPP (RFC 1661)*** http://www.rfc-editor.org/rfc/rfc1661.txt
The Inverse Address Resolution Protocol (InARP/RARP) should be used for mapping MAC address to an IP address.	Mandatory	***RARP (RFC 2390)*** http://rfc-editor.org/rfc/rfc2390.txt
Rapid Spanning tree Protocol (RSTP) should be used to provide faster spanning tree convergence after a topology change and respond to changes within a second.	Mandatory	***RSTP (IEEE 802.1w)*** http://www.ieee802.org/1/pages/802.1w.html
Spanning Tree Protocol (STP) should be used to ensure a loop-free topology for any bridged LAN.	Mandatory	***STP (IEEE 802.1D)*** http://www.ieee802.org/1/pages/802.1D-2003.html

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
VLAN trunk should be used for allowing multiple bridged networks to transparently share the same physical link.	Mandatory	***Vlan Trunk (IEEE 802.1 Q)*** http://www.ieee802.org/1/pages/802.1Q.html

Interconnection –Telecom and Public Institution

Standards proposed	Mandatory/ Recommended	Reference / Guidelines
Internet Service Provider Standards		
.tz Web hosting should be used to make websites accessible through browsers.	Mandatory	
.tz domain should be used to convert domain names to IP addresses.	Mandatory	
Electronic commerce should be considered as the main interface for buying and selling of products in the near future.	Recommended	***xCBL*** http://www.xcbl.org/ ***UBL*** http://oasis-open.org/committees/ubl/lsc/
Financial Interconnectivity System Standards		
Wireless communication should be employed as a convenient and high efficient	Mandatory	***Interactive Financial Exchange Forum*** http://www.ifxforum.org/html/standard/ifxstandar

Standards proposed	Mandatory/ Recommended	Reference / Guidelines
communication/interconnectivity method.		d.html
EMV standard should be used for interoperation of Integrated Cards ("Chip cards") and IC capable POS terminals and ATMs, for authenticating credit and debit card payments.	Recommended	The organization responsible for developing and maintaining the standard http://www.emvco.com/

2.2.3. Data Integration

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
Character and encoding for information interchange		
i. American Standard Code for Information Interchange (ASCII) should be used as the minimum set of characters for data interchange. ii. Unicode should be used for language(Swahili) support iii. UCS Transformation Format (UTF-8) should be used for encoding Unicode ISO 8859-1	Mandatory	***ASCII*** http://www.columbia.edu/kermit/ascii.html ***UTF*** http://www.ietf.org/rfc/rfc2279.txt ***Unicode*** http://www.unicode.org/versions/Unicode5.2.0/
Data Description		

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
i. Resource Description Framework (RDF) model should be used to define models for describing interrelationships among resources in terms of named properties and values. ii. Extensible Markup Language Version 1.1 and above should be used for Structured data description iii. Extensible Name and Address Language Version 2 (xNAL) should be used for defining name and address iv. Extensible Customer Information Language xCIL should be used to capture specifying formats for citizen information elements such as name, address etc. v. Extensible Customer relationship Language xCRL should be used to define relationship between Public Institutions	Mandatory	***RDF*** http://www.w3.org/RDF/ ***XML 1.1*** http://www.w3.org/TR/xml11/#sec-intro ***xNAL*** http://www.oasis-open.org/committees/ciq/ciq.html#4 http://www.oasis-open.org/committees/ciq/download.html ***XCIL*** http://www.oasis-open.org/committees/ciq/ciq.html#7 ***xCRL*** http://www.oasis-open.org/committees/ciq/download.shtml

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
Data exchange & Transformation		
i. XML Metadata Interchange (XMI) Format should be encouraged as an open information interchange model. ii. ISO 8601 should be followed for data elements and interchange formats *iii.* Extensible cascaded style sheet Language transformations (xSLT) should be used for transforming XML documents into other XML document.	Mandatory	***XMI*** http://www.omg.org/spec/XMI/ ***xSLT*** http://www.w3.org/TR/xslt
Data exchange Formats		
i. Standards Used for Data exchange formats include: a. Public institutions should adopt ANSI X12 and UN/EDIFACT electronic data interchange (EDI) standards for international	Mandatory	***XML/EDI*** http://www.eccnet.com/xmledi/ ***UN/EDIFACT*** http://www.unece.org/cefact/cf_plenary/plenary98/docs/98cf4.pdf ***PDF/UA*** http://pdf.editme.com/pdfua

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
compatibility. XML/EDI should be considered for future use for using XML for Electronic data interchange through XML b. PDF should be used for accessing non-editable documents c. MS office document type such as Doc, XLS, and PPT should be used for inter-departmental information interchange between users of Microsoft office product. In the future, Open document format for office application should be considered. d. Tagged Image File Format (TIFF/IT) should be used for facsimile and		***PDF/E*** http://pdf.editme.com/PDFE http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42274 ***Open format for office application*** http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office ***TIFF*** https://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf http://www.remotesensing.org/libtiff/ http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=2181

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
scanned documents(especially useful for archiving and digitization) e. Graphic Interchange Format (GIF) and Joint Photographic Experts Group (JPEG) for raster based colour documents, drawings, graphic image, photographs etc. f. Rich Text Format(RTF) should be used for editable word processing documents format for text and graphics interchange g. Initial Graphics Exchange Specification (IGES) and DXF should be used for computer aided design documents		***GIF89a*** http://www.w3.org/Graphics/GIF/spec-gif89a.txt ***JPEG*** http://www.jpeg.org/jpeg/index.html ***RTF*** http://www.microsoft.com/downloads/details.aspx?FamilyId=DD422B8D-FF06-4207-B476-6B5396A18A2B&displaylang=en ***MPEG Standards*** http://mpeg.chiariglione.org/standards ***SMTP Standards*** http://datatracker.ietf.org/doc/rfc5335/ ***MIME Standards*** http://datatracker.ietf.org/doc/rfc2045/ http://datatracker.ietf.org/doc/rfc2046/

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
h. Moving Picture Experts Group (MPEG) should be used for moving images and audio i. PST and CSV should be used as a standard for inter-departmental information interchange. (usually through Email exchange) j. Computer Graphics Metafile (CGM) and Scalable Vector Graphics (SVG) for editable vector based graphics, 2D content, raster images and font text. k. HTM should be used for publishing/presentation on the web through popular		***WebCGM 2.0*** http://www.w3.org/TR/2007/REC-webcgm20-20070130/ ***HTML4.01*** http://www.w3.org/TR/html4/

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
browser l. AVI and MP3/MP4 format should be used for audio streaming files.		
Ontology-based information exchange		
i. For formal descriptions of the meaning of terminology used in web document for the automatic processing of such documents. OWL should be used with RDF for adding semantics.	Recommended	***OWL*** http://www.w3.org/TR/owl-semantics/ http://www.w3.org/TR/owl2-overview/
Data Modelling		
i. For data modelling, business modelling, object modelling and component modelling standardized general-purpose modelling language UML Should be used to specify, visualize, modify, construct and document the artefacts.	Mandatory	***UML*** http://www.omg.org/spec/UML/
Data integration meta language		
i. XML signatures ii. XML encryption	Recommended	***XMLSig*** http://www.w3.org/TR/xmldsig-core/

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
iii. XML signature and encryption iv. XML key management where a PKI environment is used v. XML security assertion mark-up vi. XML access control		***XML-Encryption*** http://www.w3.org/TR/xmlenc-core/ ***XML-Key Management Specification(XKMS)*** http://www.w3.org/TR/xkms2/
Minimum interoperable character set		
i. Minimum Interoperable Character Set is required to define the minimum character sets to be used for the content to be interchanged in between related parties, e.g. agencies and departments as well as third parties such as suppliers.	Mandatory	***UTF-8*** http://datatracker.ietf.org/doc/rfc3629/
Digitization		
This is the way to convert hard-copy or non-digital records into digital format.	Mandatory	Text only, black and white-Format TIFF PDF/A containing TIFF or JPEG 2000 TIFF JPEG 2000PDF/A containing TIFF or JPEG 2000
Data Definition for Smart Cards		

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
The following standards are Recommendatory for data definition aspects for smart card applications: i. ISO/IEC 7816-6 ii. ISO/IEC 7812-1 Additionally the following standards should be considered for review for future versions: i. EN 1546-3 ii. EN 1546-4	Recommended	ISO/IEC 7816-6:2004 http://www.iso.org/iso/catalogue_detail.htm?csnumber=38780 – ISO/IEC 7812-1 :2006 http://www.iso.org/iso/catalogue_detail.htm?csnumber=31443

2.2.4. Security

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
Access management		
i. The system should support operating systems, application servers, database management systems, identity management and directory services. ii. The system should have APIs for identification and authentication.	Mandatory	***Access management*** http://www.2ab.com/pdf/AccessManagement.pdf

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
iii. The access management should encrypt user-ids and passwords during transmission. In addition, passwords must be stored in an encrypted or one- way hash format.		
Anti-Spam		
i. Anti-spam product should be compatible with standards adopted for operating systems and electronic mail systems.	Mandatory	***Access management*** http://www.2ab.com/pdf/AccessManagement.pdf
Anti-Virus/Anti Spyware		
i. They should be able to provide protection against various kinds of attacks from virus, worms, Trojan horse etc. ii. Anti-virus and anti-spyware products should be compatible with the standards adopted for operating systems.	Mandatory	
Desktop Firewall		
i. Technologies must support standards approved in various categories such as	Mandatory	***Firewall (RFC-3360)*** http://rfc-editor.org/rfc/rfc3360.txt

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
operating systems and network protocols.		
Digital Signature		
i. Secure Hash Algorithm should be used as a standard for digital signature. ii. Provides authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality.	Mandatory	***RFC 4359 (SHA)*** http://www.rfc-editor.org/rfc/rfc4359.txt http://www.w3.org/PICS/DSig/SHA1_1_0.html
Email Security		
i. S/MIMEv3 should be the standard used for a secure mail to transport for a source to a destination.	Mandatory	***S/MIME (RFC 3851)*** http://rfc-editor.org/rfc/rfc3851.txt
Encryption Algorithm		
i. Triple DES and DES standards should be used for encryption algorithm.	Recommended	***DES RFC 4772*** http://www.rfc-editor.org/rfc/rfc4772.txt http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf – 3DES
Enterprise Firewall		

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
i. The firewall should support various layers of TCP/IP protocol stack. ii. The firewall should support approved standards of operating systems, network protocols, data transport, electronic mail systems and application technologies.	Mandatory	***Firewall (RFC-3360)*** http://rfc-editor.org/rfc/rfc3360.txt
SwIPe		
i. Security Network Protocol (SwIPe) should be the standard used for IP security at the network layer for confidentiality, integrity and authentication of network traffic.	Mandatory	***SwIPe*** http://www.crypto.com/papers/swipe.id.txt
Cryptographic algorithm		
i. MD5 algorithm should be used for cryptographic hash function.	Mandatory	***MD5 (RFC 1321)*** http://www.rfc-editor.org/rfc/rfc1321.txt
User Level Security		
i. Authentication, Authorization and Accounting (AAA) and TACACS should be the	Mandatory	***AAA (RFC 4962)*** http://rfc-editor.org/rfc/rfc4962.txt

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
standards used for user level security.		***TACACS (RFC 1492)*** http://rfc-editor.org/rfc/rfc1492.txt
Identity, Authentication, authorization and privacy		
i. Security Assertions Markup Language (SAML1.1) should be the framework for exchange of authentication and authorization information ii. X.509 should be the standard for identity certificates. iii. Platform for Privacy Preferences Project (P3Pv1.0) should the standards adopted for enabling web sites to express privacy practices in a standardized form that can be automatically retrieved and interpreted by user agents, such as browsers.	Mandatory	***P3P v1.0*** http://www.w3.org/TR/P3P/ ***SAML*** http://saml.xml.org/saml-specifications#samlv11 ***X.509*** ***RFC 4158*** http://rfc-editor.org/rfc/rfc4158.txt ***RFC5280*** http://rfc-editor.org/rfc/rfc5280.txt
Identity Management		
i. Identity Management should enable encryption of user-ids and passwords during transmission. In addition, passwords should be stored	Mandatory	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51625

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
in an encrypted or one-way hash format. ii. It should have APIs for identification and authentication. Technologies should be vendor neutral and support operating systems, database management systems, application servers, access managers and directory services.		
Intrusion detection and prevention		
i. Technologies must support approved standards in various categories such as operating systems, and firewalls	Mandatory	***IDS/IPS*** http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1517609
IP Encapsulation security		
i. Encapsulating Security Payload(ESP) should be used for communicating secure data transmission, confidentiality, data origin authentication, connectionless integrity, an anti- replay, and traffic flow confidentiality	Mandatory	***ESP (RFC 4303)*** https://www.rfc-editor.org/rfc/rfc4303.txt
IP Security		

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
i. The standard for securing internet protocol communications by authentication or encrypting should be IPSec.	Mandatory	***IP SEC (RFC 4301)*** http://rfc-editor.org/rfc/rfc4301.txt
Layer 2 Security		
i. Layer 2 tunnelling protocol (L2TP) should be used to support a secure communication in VPN on data link layer.	Mandatory	***L2TP (RFC 3931)*** http://www.rfc-editor.org/rfc/rfc3931.txt
Proxy server		
i. Evaluates the request according to its filtering policies. ii. Proxy servers should be compatible with LDAPv3 and should be able to integrate with adopted standards for directory services	Mandatory	
Public key infrastructure		
i. PKI should be used for communicating confidential information in banking sectors and other Public Institutions.	Mandatory	***PKI*** http://www.oasis-pki.org/resources/techstandards/
Remote Security		

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
i. SSH should be used for secure remote login when data is being accessed by Public Institutions.	Mandatory	***SSHv2/3*** http://www.rfc-editor.org/rfc/rfc4251.txt
Secure transport		
i. TLS/SSL should be the standards used for a secure transport of data from a source to a destination.	Mandatory	***Secure Socket Layer*** https://tools.ietf.org/html/rfc6101***Transport Layer Security (RFC 5246)*** http://rfc-editor.org/rfc/rfc5246.txt
Virtual Private Network(VPN)		
i. The VPN must use vendor neutral, standards-based, APIs for identification and authentication ii. The VPN should allow encrypting user-ids and passwords during transmission. In addition, passwords must be stored in an encrypted or one- way hash format iii. The technology should be compatible with adopted standards for PKI, proxy servers, firewalls and operating systems.	Mandatory	***RFC 4026 VPN*** http://www.rfc-editor.org/rfc/rfc4026.txt ***RFC 2764 IP based VPN*** http://www.rfc-editor.org/rfc/rfc2764.txt

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
XML security standards		
i. XML-DSIG should be used for representing and verifying web signatures ii. WS – Security should be the standards for security of messages transmitted between web services components. *iii.* WS- I Basic Security Profile Version 1.0 should be used for Web Services-Interoperability	Mandatory	***XML-Signature*** www.w3.org/TR/xmldsig-core/ ***WSS*** www.oasis-open.org/committees/wss/ ***WS-I*** http://www.ws-i.org/Profiles/BasicProfile-1.0-2004-04-16.html
Physical Security		
i. It includes different kinds of methods and equipment for securing an environment such as: a. IP-based surveillance cameras, access control (card or biometric) devices.	Mandatory	***IP based Surveillance*** http://www.onvif.org/ http://www.onvif.org/Documents/Specifications/tabid/284/Default.aspx ***Codec*** www.itu.int/rec/T-REC-H.264
Security of Smart Cards		
i. ISO/IEC 7816-8: 2004 Identification cards – Integrated circuit	Mandatory	Security Standards for Smart cards namely CC, ETSI, FIPS and EMVCo

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
cards Security inter industry commands ii. ISO/IEC 7816-9: 2004 Identification cards – Integrated circuit cards Commands for card management iii. ISO/IEC 7816-11: 2004 Identification cards – Integrated circuit(s) cards Personal verification through biometric methods and Integrated circuit cards iv. ISO/IEC 7816-15: 2004 Identification cards - Integrated circuit cards Cryptographic information application v. ISO 9564-1: 2002 Banking -- Personal Identification Number (PIN) management and security Basic principles and requirements for online PIN handling in ATM and POS systems vi. ISO 9564-2:Banking -- Personal Identification Number management and		–ISO/IEC 7816-8:2004 http://www.iso.org/iso/catalogue_detail.htm?csnumber=37989 –ISO/IEC 7816-9:2004 http://www.iso.org/iso/catalogue_detail.htm?csnumber=37990 –ISO/IEC 7816-11:2004 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31419 –ISO/IEC 7816-15:2004 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35168 –ISO 9564 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29374 –ISO 9564-2:2005 http://www.iso.org/iso/catalogue_detail.htm?csnumber=36289 –ISO 9564-3:2003

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
security Approved algorithm(s) for PIN encipherment vii. ISO 9564-3: 2003 Banking -- Personal Identification Number management and security Requirements for offline PIN handling in ATM and POS systems viii. ISO 9564-4: 2004 Banking -- Personal Identification Number management and security Guidance for PIN handling in open networks		http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35124 –ISO/TR 9564-4:2004 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36761

2.2.5. Access

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
Access Token		
i. American Standard Code for Information Interchange (ASCII) should be used as the minimum set of characters for data interchange.	Mandatory	***FIPS – 197*** http://csrc.nist.gov/publications/PubsFIPS.html

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
ii. All hardware tokens must have an inherent unique identity that should be tamper proof and with access restricted only to applications offered by the token vendor or another trusted organization. No other access should be permitted iii. The authentication should require a two-factor authentication key wherein the hardware token requiring per-session local activation (with a password or biometric). iv. The token design should be FIPS compliant.		
Animation		
i. SVG 1.1 (.svg), as per W3C specifications. ii. SVG tiny1.2 as per W3C specifications for mobile specification iii. GIF (.gif), as per GIF89a specification	Recommended	***SVG 1.1 specifications*** http://www.w3.org/TR/SVG11/http://www.w3.org/TR/SVG/ ***SVG tiny 1.2*** http://www.w3.org/TR/SVGTiny12/

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
Compression		
i. The following standards should be used for compacting the files. a. GNU ZIP (.gz). b. Tape Archive TAR Pack (.tar). c. Compact TAR Pack (.tgz ou .tar.gz).	Mandatory	***GZIP*** http://www.gnu.org/software/gzip/ ***TAR*** http://www.gnu.org/software/tar/
Kiosks		
i. The kiosk machine should support the Content management and personalization technologies used for delivering services. ii. The Kiosk should support the application for a minimum period of 5 years. ***iii.*** Transponder on the server side should have the capability to effect the required transformation of	Recommended	-

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
content for delivering it through kiosks.		
Other delivery channel		
i. Information Access covers components and technical specifications required to enable users to access Public Sector information and services electronically via a range of delivery channels like Hypertext Web Content, Document, Spreadsheet, Presentation, Character Sets and Encoding	Recommended	***HTML*** http://www.w3.org/TR/html401/ ***XHTML*** http://www.w3.org/TR/xhtml1 ***RTF*** http://msdn.microsoft.com/library/?url=/library/enus/dnrtfspec/html/rtfspec.asp?frame=true ***PDF*** http://www.adobe.com/products/acrobat/adobepdf.html ***Word Document*** http://www.microsoft.com/office/word/default.asp

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
		Excel http://www.microsoft.com/office/excel/default.asp
Mobile devices		
i. Application schedule be compatible for delivering service with mobile devices such as PDA's Wi-Fi, Digital TV etc. *ii.* Transponder on the server side should have the capability to effect the required transformation of content for the target delivery device	Recommended	***OMA Standards*** http://www.openmobilealliance.org/Technical/PublicMaterial.aspx
Scripting		
i. ECMA 262 should be the standards for server side scripting. ECMA Script is a vendor- neutral scripting language *ii.* Java Script should be the standards for client side	Mandatory	***ECMA-262*** www.ecma-international.org/publications/standards/Ecma-262.HTM

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
scripting		
Directory Access		
i. LDAP v3 – Lightweight Directory Access Protocol version 3 should be the standard to locate and access information stored in directories	Mandatory	http://datatracker.ietf.org/doc/rfc4510/ http://datatracker.ietf.org/doc/rfc4517/ http://datatracker.ietf.org/doc/rfc4523/ http://datatracker.ietf.org/doc/rfc4512/ http://datatracker.ietf.org/doc/rfc4514/
Web access standard		
i. Web content accessibility guidelines (WCAG) should be the standard for making information accessible to people with special needs. ii. WCAG is part of the series of web accessibility guidelines published by the w3c's web accessibility initiative.	Mandatory	Web access Standard http://www.w3.org/WAI/
Web browser		
i. Web browsers should support HTM L4.01,	Mandatory	-

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
XHTML1.0, CSS 2.1,ECMAScript and Dom level 3 *ii.* Extensible Style sheet Language (XSL) is the language for defining how a browser will display XML content to the user.		
Workstation		
i. A workstation is high level performing equipment used for technical and scientific applications. ii. Desktops, lap top and other computer terminal used by end users /employees daily should comply with configuration so as to serve the application needs for a minimum period of 3 years.	Mandatory	
Biometric data interchange		
For Biometric Data Interchange the following standards are: i. ISO/IEC 19785-2 Information Technology -	Mandatory	***ISO/IEC 19785-1*** http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41047

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
Common Biometric Exchange Formats Framework ii. ISO/IEC 19794-7 Information Technology - Biometric data interchange formats iii. ISO/IEC 10918-4: 1999 Information Technology - Digital compression and coding of continuous-tone still images iv. ISO/IEC 15444-2:2004 Information Technology - JPEG 2000 image coding system		***ISO/IEC 19785-2*** http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41048 ***ISO/IEC 19794-1*** http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38745

2.2.6. Collaboration

Standards Proposed	Mandatory / Recommended	Reference & Guidelines
Email System		
i. Internet standards (STD) for mailing:- a. **SMTP:**-Internet standard for electronic	Mandatory	***SMTP Standards*** http://datatracker.ietf.org/doc/rfc5335/ http://datatracker.ietf.org/doc

mail transmission around IP networks b. **POP3**:- Application layer internet standard protocol used by local e-mail clients to retrieve email from a server over TCP/IP. c. **IMAP4rev1**: Protocol for retrieving e-mails over TCP/IP d. **The Message Transfer Agent** (MTA) in e-mail systems should be LDAP enabled. e. Appropriate rules and policies set in the email to protect the same from spams and other intrusions. f. Any web access to e-mail should be provided only if adequate access security preventing unauthorized access and leakage of mail.		/rfc5336/ ***MIME Standards*** http://datatracker.ietf.org/doc/rfc2045/ http://datatracker.ietf.org/doc/rfc2046/ http://datatracker.ietf.org/doc/rfc2047/ http://datatracker.ietf.org/doc/rfc2048/ http://datatracker.ietf.org/doc/rfc2049/ ***POP3 Standards*** http://datatracker.ietf.org/doc/rfc1939/ http://datatracker.ietf.org/doc/rfc1957/ http://datatracker.ietf.org/doc/rfc2445/ ***IMAP4*** http://www.ietf.org/rfc/rfc2060.txt http://www.ietf.org/rfc/rfc2342.txt http://www.ietf.org/rfc/rfc2971.txt www.w3.org/XsL
IP Telephony		
IP telephony should comply withH.323 and the Session	Recommended	http://www.rfc-editor.org/rfc/rfc3661.txt

Initiation Protocol (SIP) protocols to provide audio-visual communication sessions on any packet network.		http://www.rfc-editor.org/rfc/rfc2805.txt http://www.rfc-editor.org/rfc/rfc5125.txt http://www.rfc-editor.org/rfc/rfc3015.txt http://www.rfc-editor.org/rfc/rfc4666.txt
Videoconferencing		
i. Simultaneous audio & video transmission through telecommunication technologies. ii. Also used to share documents, computer-displayed information, and whiteboards.	Recommended	***G series*** http://www.itu.int/net/itu-t/sigdb/speaudio/Gseries.htm ***G.722*** ***H.261*** http://www.itu.int/rec/T-REC-H.261-199303-I/en ***Q.931*** http://www.itu.int/rec/T-REC-Q.931-199805-I/en ***H.263*** http://www.itu.int/rec/T-REC-H.263-200501-I/en

2.2.7. Application design and development

Standards proposed	Mandatory / Recommended	Reference & Guidelines
Application Development For Handheld Devices		

Standards proposed	Mandatory / Recommended	Reference & Guidelines
i. Technologies must be compatible with the standards adopted for mobile operating systems. ii. There are specialised application development platforms for handheld devices. iii. Public institutions developing or purchasing new, wireless departmental or enterprise applications that will be accessed primarily via wireless phones and PDAs must utilize these customized application development platforms	Recommended	***Application for handheld devices:*** http://www.wapforum.org
Application development framework		
i. Provide the Public Institutions with distinct approaches to address different application needs/ requirements. ii. Public institutions should utilize an enterprise framework in the development of applications and services.	Mandatory	-

Standards proposed	Mandatory / Recommended	Reference & Guidelines
iii. Technologies should provide capability for reuse of existing components and services iv. Technologies should provide support for creating of web services and should be compatible with standards adopted for web services.		
Business Rules, Logic and Objects		
i. There should be Meta data for every document /object ii. For naming and design rules for schema design Universal Business Language (UBL) should be used. iii. W3C standards and Uniform Resource Name (URN) should be used for namespaces i.e. defining each element type and attribute name in an XML document.	Recommended	***UBL:*** http://docs.oasis-open.org/ubl/os-UBL-2.0-update-delta.zip ***URN:*** i. http://tools.ietf.org/html/rfc1737 ii. http://tools.ietf.org/html/rfc2141 iii. http://tools.ietf.org/html/rfc3406 iv. http://www.ietf.org/rfc/rfc4350.txt
Commercial, off-the-shelf applications(COTS)		
i. The COTS application should comply with open standards, industry standards in a manner that it interoperates	Recommended	There are no predefined standards for COTS except open standards. The evaluation and selection process for COTS

Standards proposed	Mandatory / Recommended	Reference & Guidelines
with complementary products from other vendors ii. Availability and access to training and all round support iii. The application should allow iv. Parameterization and customization for local needs e.g. payroll v. Minimum or no locking with proprietary products		should be done based on Specification and requirements of the organization
Geographic Information System		
i. Technology/ software products that comply with Open Geospatial Consortium (OGC) Open GIS Specifications and protocol such as include Web Map Service (WMS) and Web Feature Service (WFS). ii. Describes any information system that integrates, stores, edits, analyses, shares, and displays geographic information	Recommended	***WFS*** http://www.opengeospatial.org/standards/wfs ***WMS*** http://www.opengeospatial.org/standards/wms ***CSW*** http://www.opengeospatial.org/standards/cat ***OWS*** http://www.opengeospatial.org/standards/common ***WPS*** http://www.opengeospatial.org/standards/wps

Standards proposed	Mandatory / Recommended	Reference & Guidelines
		Simple Features http://www.opengeospatial.org/standards/sfa ***GML*** http://www.opengeospatial.org/standards/geoxacml
Modelling design and development		
i. The standards (frameworks) adopted for application design and development should be compatible with the technologies used for implementing applications. ii. Process Modelling should be done using BPMN standards, for workflow iii. For Notation specifying business process behaviour based on Web Services Business Process Execution Language(BPEL4WS) for Web Services iv. Entity-Relationship diagram (ERD) should be the diagramming notation for	Recommended	***BPMN*** i. http://www.bpmn.org/ ii. http://www.bpmi.org/ ***UML*** i. www.UML.org ***XMLv1.0*** i. http://www.w3.org/TR/2002/WD-xml11-20020425/ ***WML*** i. http://www.openmobilealliance.org/tech/affiliates/wap/wap-238-wml-20010911-a.pdf

Standards proposed	Mandatory / Recommended	Reference & Guidelines
data modelling for relational data bases. v. UML 2.0 and above (Unified modelling language) should be the standard used for requirement specification for application development vi. XML Schema v1.0 should be used for creating tags to define the structure, content and semantics of XML documents(define, transit, validate, and interpret data) vii. WML v2.0 – Wireless Markup Language version 2.0 should be used for development of content for mobile/pda.		
Programming language for Application Development		
i. Scripting languages should allow Code portability, code collaboration, and browser compatibility and should follow ASCII as the basis. ii. Languages for development of mobile applications should be thus compatible with mobile network standards (such as GSM,	Recommended	-

Standards proposed	Mandatory / Recommended	Reference & Guidelines
CDMA, TDMA and packet-switched) and data standards (such as GPRS, IS95B and 3G). iii. Technologies used should be compatible with the application development framework adopted as standards. The application would include web application as well. iv. Various technologies exist to support the basic frameworks and programming languages used for application development that will support or improve the software user's work.		
Reporting tools		
i. They should be platform independent ii. They should provision for integrating with Swahili language/provide language support iii. The reporting tools should support database connectivity, spreadsheet	Recommended	-

Standards proposed	Mandatory / Recommended	Reference & Guidelines
connectivity and access mechanisms accepted as standards. iv. Version control features and change control features should be available.		
Software configurations Management (SCM)		
i. The SCM tool should provide for all parts of the software development, deployment and maintenance lifecycle ii. The technology should enable project set up execution and monitoring features. iii. It should provide features for collaborative work	Recommended	-
Service Oriented Architecture		
i. It is recommended to use W3C standards for web services ii. UDDI version 3 used for describing publishing, and discovering network-based software components. iii. WSDL v 1.1 used for specifying the location of the service and the operations, or methods, the service exposes	Mandatory	***Web Service standards and specification*** i. www.W3c.org ***UDDI*** i. http://www.oasis-open.org/specs/index.php#uddiv3.0.2 ***WSDL***

Standards proposed	Mandatory / Recommended	Reference & Guidelines
iv. SOAPv1.2 and above should be used to for Web Services transport. v. ebXML Version 2.0 (now ISO/TS 1500 series) used for Standard Message Service Specification vi. WSRM 1.1 should be used for message delivery to applications or Web services. vii. Web Services Business Process Execution Language should be used to describe business process activities as web services and define how they should be connected to accomplish specific tasks. viii. Basic Profile Version 1.0 as defined by the Web Services Interoperability Organization (WS-I) should be used as web services basic interoperability profile.		i. http://www.w3.org/TR/2001/NOTE-wsdl-20010315#_introduction ***SOAP*** i. http://www.w3.org/TR/soap12-part1/ ***ebXML*** i. www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf ii. http://www.ebxml.org/geninfo.htm ***WSRM*** i. http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.1-spec-os-01-e1.pdf ii. http://docs.oasis-open.org/ws-rx/wsrm/200608/wsrm-1.1-spec-cd-04.html
Smart Card Application		

Standards proposed	Mandatory / Recommended	Reference & Guidelines
i. The following standards are Recommendatory for smart card applications design and development: a. ISO/IEC 7816-4 b. ISO/IEC 7816-5 c. ISO/IEC 7816-7 d. ISO/IEC 7812-2 e. ISO/IEC 7813 f. EN 1332-1 g. EN 1332-4	Recommended	**Overall** http://www.tiresias.org/research/standards/smartcards.htm#international ***ISO 7816*** http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx ***ISO 7812*** ISO/IEC 7812-1:2006 Identification cards -- Identification of issuers -- Part 1: Numbering system ***ISO/IEC 7812-2:2007 Identification cards*** -- Identification of issuers -- Part 2: Application and registration procedures ***ISO 7813*** http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43317 ***EN 1332*** http://www.tiresias.org/research/standards/smartcards.htm#international

2.2.8. Application integration

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Message oriented Middleware		
i. JMS and MSMQ may be used for application integration based on the platforms deployed.	Recommended	***Message oriented Middle ware (AMQP)***
Object request brokers (ORB)		
i. CORBA or COM /DCOM should be used as ORB ii. Web applications should use Resource Discover Framework standards	Recommended	***ORB*** http://www.service-architecture.com/web-services/articles/corba.html http://www.omg.org/gettingstarted/orb_basics.htm http://www.omg.org/spec/
Remote procedural calls		
i. Any RPC used for non-web based application should be developed using interface description language (IDL) ii. For all web enabled application XML-RPC should be used.	Recommended	***RPC*** http://ietf.org/rfc/rfc5531.txt ***XML-RPC*** http://www.xmlrpc.com/spec

2.2.9. System Standards

Standards proposed	Mandatory / Recommended	Reference & Guidelines
Application Servers		
i. Application servers should provide support for various standards adopted for web services ii. Application servers should be compatible with data connectivity and access technologies, application development frameworks and database management systems	Mandatory	There are open standards such as Soapad which provides open-source, open standards for application server. However an e-GIF standard does not provide the choice of application server.
Backup Recovery		
i. Technologies should be compatible with standards adopted for categories such as operating systems, database management systems and storage. ii. Production databases shall be periodically tested for recoverability. iii. Metadata (database schemas, structures, data definitions, etc.) shall be backed up along with the data.	Mandatory	Apart from ensuring the requirement mentioned in the table it is important to concentrate on the process of maintenance of database, routine of backup and recovery and the health of the data. It is not just the data files that need to be part of the backup

		process backup of transaction log must also be done for critical systems.
Business Intelligence		
i. Technologies should support database connectivity and access technologies accepted as standards. ii. Technologies should provide support Graphical Interfaces for summarizing data, e.g. desktop dashboards. iii. Technologies should provide support for ad-hoc and —canned queries. ***iv.*** Technologies should provide support for guided report creation as well as programmatic control of report creation.	Recommended	Any tools which supports Online analytical processing (OLAP) should support Multidimensional OLAP (MOLAP), Hybrid OLAP (HOLAP) and Relational OLAP (ROLAP) depending on the nature of reporting system that needs to be developed.
DB Connectivity and access technology		
i. Frameworks and models used for database connectivity and access purposes should be based on the standards of the database environment identified.	Mandatory	Some platform specific standards are: –Java Database Connectivity (JDBC) is a standard SQL database access interface. JDBC is an API for the Java programming –ADO.NET is a set of computer software components that should be used by

		programmers to access data and data services based on Microsoft .NET Framework. –Microsoft's ActiveX Data Objects (ADO) is a set of Component Object Model (COM) objects for accessing data sources.
Database Management System		
i. Database Management system should provide support for the basic properties of a database transaction: (ACID) Atomicity, Consistency, Isolation, and Durability ii. Database Management System should provide for security of the data and built-in audit capabilities iii. Database technologies shall support iv. industry or de facto standards for database connectivity mechanisms such as Java Database Connectivity (JDBC), Open Database Connectivity (ODBC) or Object Linking and Embedding Database (OLEDB) v. Database Management System should be XML enabled and must provide capability for web service standards. vi. The version/release levels of all database management systems and	Mandatory	***DBMS*** http://www.ansi.org http://www.iso.org

related tools used to develop or support Public Institution mission critical applications shall have vendor or equivalent level support. vii. Public institutions should preferably have database for transactional and analytical processing in separated DBMS source viii. Database cluster, the clustering software should support heterogeneous Operating systems from different OEM's. ***ix.*** The Volume Manager and File system should support heterogeneous Storage models from different OEMs.		
Desktop O/S		
i. Desktop operating system should provide graphical user interface and should be compatible with the hardware platform.	Mandatory	
Hardware Platforms		
i. Public institutions should consider deploying 64 bit hardware platforms ***ii.*** X86 instruction set architecture should be used. X86-32 for the 32 bit hardware platforms, and x86-64 for the 64 bit hardware platforms.	Mandatory	
ICT Operations Management		
i. Technologies should be compatible with standards adopted for categories such as operating systems, database management systems, and storage	Mandatory	***ICT operations management*** http://www.itlibrary.org/

application servers. ***ii.*** The systems should be compatible with Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON).		
Mobile/OS		
i. Mobile operating system should provide for graphical user interface. ii. Mobile operating systems should provide support for the adopted standards for application development frameworks for handheld devices.	Recommended	
Portal Servers		
i. Portal servers must adhere to Organization for the Advancement of Structured Information Standards (OASIS) Web Services for Remote Portlets (WSRP) specifications.	Mandatory	***Organization for the Advancement of Structured Information Standards (OASIS)*** http://www.oasis-open.org
Server OS		
i. Operating system should be providing graphical user interface, should be compatible with the hardware platform and should upgrade based on requirements and support. ii. POSIX standards for O/S should be applicable iii. Operating system should be based on the requirement of the application or system to function	Mandatory	***POSIX, IEEE Standards Association*** http://standards.ieee.org/regauth/posix

iv. Server O/S should minimize server operating system configuration variations as this helps to reduce risks and support and maintenance costs v. Server O/S should configure all servers supporting mission critical applications, including desktop applications, to minimize service interruption.		
Storage Devices		
i. Storage hardware used should adhere to the storage interface available/adopted ii. Local Redundant Array of iii. Independent Disks (RAID)/ Storage Area Network (SAN)/ Network-attached storage (NAS) should be used as the system storage technology. iv. Optical disks and tapes are also a suitable choice from the available latest technology and this should be considered.	Mandatory	-
Web Server		
i. A web server provides World Wide Web services on the Internet. If a web server is used internally and not by the public it may be known as an "intranet server." ii. It is responsible for accepting HTTP requests from clients and serving them HTTP responses along with optional data content.	Mandatory	Web Server http://www.ietf.org

2.2.10. Business areas specifications

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Specification for specific business area- Finance		
i. XBRL should be used for XML based forms and tax taxonomy ii. RIXML also can be considered to prepare financial content	Recommended	***XBRL*** http://www.xbrl.org ***RIXML*** www.rixml.org
Specification for specific business area- workflow and web services		
i. Wf-XML should be used to exchange information among workflow management system ii. Specification Schema and OASIS Business Transaction Protocol should also be considered to provide coordination between different system	Recommended	***Wf-xml*** http://www.wfmc.org/standards/***ebXML*** http://www.ebxml.org/ ***OASIS BTP*** http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=business-transaction
Specification for specific business area- e-Health		
i. HL7 should be adopted ii. SNOMED Clinical Terms should be used	Recommended	***HL7*** http://www.hl7.org/implement/standards/index.cfm ***SNOMED CT*** http://www.ihtsdo.org/snomed-ct/
Specification for specific business area- e-learning		

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Following standard should be followed i. IMS standards for Content Packaging Information Model, XML Binding, Test Interoperability, Digital repositories, Simple sequencing, Learning design ii. SCORM *iii.* IEEE 1484.12.1: 2002 LOM *iv.* BS7988	Recommended	***IMS Project*** http://www.imsglobal.org/ ***SCORM*** http://www.scorm.com/scorm-explained/technical-scorm/ ***BS7988*** http://www.bsi-global.com/
Specification for specific business area- HR		
i. HR-XML should be considered for human resources exchange application	Recommended	***HR-XML*** http://www.hr-xml.org/
Specification for specific business area- legal		
i. Legal XML should be considered if schema suitable for Tanzania is available	Recommended	***Legal-XML*** http://www.legalxml.org/
Specification for specific business area- e-News		
i. News XML should be considered to broadcast eNews	Recommended	***NITF*** http://www.iptc.org/
Specification for specific business area- e-payment		

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
i. PCI should be considered for cardholder data and PIN security for Online payments as well as best practices for payment application development ii. European Master Card and VISA (EMV) should be considered for physical and electronic requirements of payment system IC cards iii. 3D Secure should be considered for further identity verification	Recommended	***ISO 8583*** http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31628 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=23632 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35363

Enterprise Content Management

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Enterprise Content Management		
i. ISO 15836: 2009 - Information and documentation -- metadata element set. ii. Open Archives Initiative Protocol for Metadata Harvesting 2.0 (OAI-PMH) for metadata collection. Protocol Version 2.0 of	Recommended	***–EMC content management products*** http://africa.emc.com/enterprise-content-management/index.htm?nav=1 ***–Open Text*** http://www.opentext.com/ ***-ISO 15836***

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
2002-06-14 iii. RSS (RDF Site Summary) Version 1 iv. RSS (Really Simple Syndication) Version 2 v. OpenURL 0.1 (migrating to 1.0) for context-sensitive linking vi. ISO 23950:1998 Information and documentation – Information retrieval (Z39.50) – Application service definition and protocol specification		http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52142 ***–OAI-PMH 2.0*** http://www.openarchives.org/OAI/openarchivesprotocol.html***–RSS Version 1*** http://web.resource.org/rss/1.0/ ***–ISO 23950*** http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=27446

Network Architecture

Network Architecture contains the framework of the physical components of the network. It contains the principle and procedure of the components.

Standards proposed	Mandatory/ Recommended	Reference & Guidelines
Network Components ii. Network interface cards iii. Switches iv. Repeaters v. Bridges vi. Routers	Recommended	***Network interface cards*** i. http://standards.ieee.org/about/get/802/802.3.html ii. www.ietf.org/rfc/rfc2640.txt ***Switches***

		i. https://datatracker.ietf.org/doc/rfc4665/ ii. https://datatracker.ietf.org/doc/rfc4031 ***Routers*** i. http://standards.ieee.org/about/get/802/802.3.html ii. www.ietf.org/rfc/rfc2640.txt

Open Source Software

Open-source software (OSS) is computer software that is available in source code form for which the source code and certain other rights normally reserved for copyright holders are provided under a software license that permits users to study, change, and improve the software.

The Open Source Definition is used by the Open Source Initiative to determine whether or not a software license should be considered open source. The distribution terms of open-source software must comply with the following criteria:

Table IV: Criteria for Distribution of Open-Source software

Criteria	Definition
Free Redistribution	The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.
Source Code	The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well- publicized means of obtaining the

	source code for no more than a reasonable reproduction cost preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a pre-processor or translator are not allowed.
Derived Works	The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.
Integrity of The Author's Source Code	The license may restrict source-code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.
No Discrimination Against Persons or Groups	The license must not discriminate against any person or group of persons.
No Discrimination Against Fields of Endeavour	The license must not restrict anyone from making use of the program in a specific field of endeavour. For example, it may not restrict the program from being used in a business, or from being used for genetic research.
Distribution of License	The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.
License Must Not Be Specific to a Product	The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the

	same rights as those that are granted in conjunction with the original software distribution.
License Must Not Restrict Other Software	The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.
License Must Be Technology-Neutral	No provision of the license may be predicated on any individual technology or style of interface.

To comply with the Open Standards Requirement, an "open standard" must satisfy the following criteria. If an "open standard" does not meet these criteria, it will be discriminating against open source developers.

Table V: Criteria Open Standard

Criteria	**Standards**
No Intentional Secrets	The standard MUST NOT withhold any detail necessary for interoperable implementation. As flaws are inevitable, the standard MUST define a process for fixing flaws identified during implementation and interoperability testing and to incorporate said changes into a revised version or superseding version of the standard to be released under terms that do not violate the OSR.
Availability	The standard MUST be freely and publicly available (e.g., from a stable web site) under royalty-free terms at reasonable and non-discriminatory cost.
Patents	All patents essential to implementation of the standard MUST: i. be licensed under royalty-free terms for unrestricted use, or

	ii. be covered by a promise of non-assertion when practiced by open source software
No Agreements	There MUST NOT be any requirement for execution of a license agreement, NDA, grant, click-through, or any other form of paperwork to deploy conforming implementations of the standard.
No OSR-Incompatible Dependencies	Implementation of the standard MUST NOT require any other technology that fails to meet the criteria of this requirement.

Open Standards Compliance

To assist Public Institutions in recognizing and adopting standards that conform to this Requirement, the OSI defines two levels of compliance:

i. OSR Compatible

This indicates that the owner of the standard has self-certified that their standard complies with this Requirement, and all Compliance Criteria. Anyone may ask the OSI to review an OSR Compatible standard; if the OSI finds that the standard is incompatible, the owner must either modify the standard or stop using the OSR Compatible mark.

ii. OSR Conformant

This indicates the OSI has reviewed a standard, as submitted by the owner, and certified that it fully conforms to the OSR. The OSI may charge a fee to offset the costs of this certification.

Reference / Guidelines – The Open Source Initiative http://opensource.org/

2.3. e-GIF Metadata & Data Standards

2.3.1. Meta Technologies/ Standards

Metadata technologies/standards are technologies, specification and tools that are used to create, maintain and manage Metadata Framework.

Table VI: Metadata & Data Standards

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Government Thesaurus		
i. Sample lists of dictionary data entity / data elements are provided below. a. Person b. Company c. Person Name – title, first/given i. name, middle name, last/family ii. name d. Party Address e. Party ContactMethod - telephone number, email address f. Person Gender g. Person Marital Status h. Person Birth Date i. Citizenship Certificate j. Driving License Number k. Permanent Account	Mandatory	The Government would require to maintain a catalog of generic and Public Institution specific data entities and its data element which are of nationwide interest to the Government for achieving interoperability. These data entities would facilitate seamless information exchange across departments and provide citizens and businesses with better access to public services. The Data Entity Catalog provides the initial list of these generic and Public Institutions/departments data entities and its elements. The catalog

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Number l. Date & Time ii. For each of the above dictionary entities there will be a meta data attribute		provides a details of these data entities with respect to the data elements of these entities, the XML data definition of these elements, the data entity attributes that includes the nature of the data entity indicating whether it is a shared data or codification table, the owner of the data, the storage system indicating if the data entity will be stored in Govt. database or in respective owner system.
Meta Data Core		
i. Meta data core based standards are listed below: a. Title b. Creator/Author c. Subject and Keywords d. Description e. Publisher f. Contributor g. Date h. Resource Type	Mandatory	Refer to the meta data core details below.

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
i. Format j. Resource Identifier k. Source l. Language m. Relation n. Coverage o. Rights Management p. Accessibility q. Addressee r. Aggregation s. Audience t. Digital signature u. Disposal v. Location w. Mandate x. Preservation y. Status		
Meta data		
i. Apart from the core there should be: a. other Meta data domain specific or generic) and that will be used to define Data standards or for any documentation or b. Extension elements that may be required to	Mandatory	

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
provide information about how the meaning of an element have been refined, or about how the value (specific content) of an element should be interpreted. A sample list of Meta data are provided below i. Prepared by ii. Based on iii. Is part of iv. Is Basis For v. requires vi. required by vii. created viii. modified ix. valid till x. available from xi. replaces xii. Function xiii. Alternative xiv. Versions xv. Status xvi. Comments		

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Meta data Technologies/ Standards		
i. XrML should be used to specify metadata for resources by leveraging the standard methodology developed by the Dublin Core Metadata Initiative. ii. Open Archives initiative harvesting protocols(OAI-PMH)should be considered for Metadata Harvesting iii. MIX 2.0 should be considered as the Technical Metadata for Digital Still Images Standards iv. ANSI/NISO Z39.87 - Data Dictionary should be considered for Technical Metadata for Digital Still Images v. ODRL 1.1 should be considered for the standardisation of expressing rights information over content	Recommended	Refer to metadata Technologies section below.

Standards Proposed	Mandatory/ Recommended	Reference & Guidelines
Meta data Registry		
i. Meta data registry should organize standards concept and data items and should maintain these standards in conformity with ISO11179 standards	Mandatory	Refer to meta data registry section below

2.3.1. Meta data Core

The Public Institution should lay down core sets of metadata for their information resources or design search interfaces for information systems. To start with, Dublin core Meta data standards should be followed by the Government by defining the 15 core attributes for every resource/artefact/document given below before building any application. Each of the attributes have to have a value to be defined by the central Meta data working group, The attribute together with the value forms the meta data. The following tables provide details/description to the Meta data core for the list mentioned below. It is recommended to add to this list as and when more applications are developed and more data are captured.

Table VII: Details / Descriptions to Metadata core (Title)

TITLE

Element	Title
Label:	Title
Definition:	A name given to the resource.
Obligation:	Mandatory

Description:	i. Title enables the user to find a resource with a particular title or carry out more accurate searches. It is commonly used as the key point of reference in the list of search results. ii. It should be the formal title. If the resource does not have a formal title, then it is Recommended to create a meaningful title. The Meta tag should be customer focused: make it brief and meaningful rather than clever and catchy. iii. For an alternative title, add any form of the title used as a substitute or alternative to the formal title of the resource, including a name by which the resource is normally known, abbreviations and translations. If a resource's official or formal title is one which members of the public would find incomprehensible, it is Recommendatory that an additional, meaningful name be given to it. iv. The title should be in the same language as the resource.
Examples:	i. If the resource is an e-mail and the subject line is unclear, give a meaningful title as the main title, and use the original subject line as the alternative title. ii. For an e-mail with an informal and uninformative subject line a. Title: Payroll Application Milestone b. Alternative: PR pilot test Monday
Reference:	Title – http://purl.org/dc/elements/1.1/title Alternative http://purl.org/dc/terms/alternative

Table VIII: Details / Descriptions to Metadata core (Creator/Author)

CREATOR/AUTHOR

Element	**Creator**

Label:	Creator
Definition:	An entity primarily responsible for making the content of the resource.
Obligation:	Mandatory
Description:	i. Creator enables the user to find resources that were written or otherwise prepared by a particular individual or organization. ii. Enables a resource to be tracked when the division creating it has been disbanded or the Creator has moved on. It is often best to depersonalize the Creator and give the job title rather than the person's name. iii. Give full contact details if possible, especially when they are not to be given elsewhere. There are, however, situations where the Creator has legal responsibilities and obligations, and personal names may be needed for audit trails. a. Acronyms may be meaningless to users. Use the full official title of the organization, or link to a glossary or explanatory note. b. Not to be confused with Publisher & Contributor. Creator is responsible for the intellectual or creative content of the resource; Publisher is the person or organization that makes (releases) the resource available. Whereas a Contributor plays an important role (contributes to the resource) but does not have primary or overall responsibility for the content.
Reference:	http://purl.org/dc/elements/1.1 /creator

Table IX: Details / Descriptions to Metadata core (Subject and Keywords)

SUBJECT AND KEYWORDS

Element	**Subject**

Label:	Subject/Keywords
Definition:	Topic of the resource
Obligation:	Mandatory
Description:	i. Enables the user to search by the topic of the resource. ii. It must be identified and used as the source for one or more values for the unrefined Subject element. iii. It should reflect the main idea/subject of the resource. iv. Not be confused with Type & Coverage. Type indicates what the subject matter is and Coverage contains the contents of the resource to the extent of time and place.
Reference:	http://purl.org/dc/elements/1.1/subject

Table X: Details / Descriptions to Metadata core (Description)

DESCRIPTION

Element	**Description**
Label:	Description
Definition:	Summary content of the resource
Obligation:	Mandatory
Description:	i. Helps user in identifying the resource needed. ii. It should be kept simple and precise and shouldn't contain repeated information that would be covered in other elements. iii. It is capable of covering key outcomes, abstract and events occurred etc.
Reference:	http://purl.org/dc/elements/1.1/description

Table XI: Details / Descriptions to Metadata core (Publisher)

PUBLISHER

Element	**Publisher**

Name:	
Label:	Publisher
Definition:	An entity responsible for making the resource available.
Obligation:	Mandatory
Description:	i. Enables users to find a resource published by a particular organization or individual. It should also be referred to by those wanting to re-use or republish the resource elsewhere, or to purchase a copy of the resource. ii. The publisher is the person or organization a user needs to contact in order to obtain permission to republish the information contained in the resource or to obtain copies in a different format. A publisher has certain legal rights and responsibilities regarding the resource, so should always be named. iii. Not to be confused with Creator/Contributor – The publisher is the entity that releases the resource and the user would contact to obtain new copies or discuss copyright issues; the creator, and to some extent the contributor, are responsible for the content of the resource.
Examples:	Publisher: Ministry of Local Government

Table XII: Details / Descriptions to Metadata core (Contributor)

CONTRIBUTOR

Element Name:	**Contributor**
Label:	Contributor
Definition:	An entity responsible for making contributions to the content of the resource.
Obligation:	Mandatory

Description:	i. Enables users to retrieve a resource which has been contributed to by a particular person or organization. ii. Include all individuals or organizations that played an important or significant role in creating the content of the resource but do not qualify as Creators. iii. Not to be confused with Creator – Creator is the person or group responsible for the intellectual or creative content of the resource; Contributor plays an important role but does not have primary or overall responsibility for the content.
Reference:	http://purl.org/dc/elements/1.1/contributor

Table XIII: Details / Descriptions to Metadata core (Date)

DATE

Element Name:	**Date**
Label:	Date
Definition:	i. The date the resource was released or made available. ii. A date associated with an event in the life cycle of the resource.
Obligation:	Mandatory
Description:	i. Enables the user to find the resource by limiting the number of search hits according to a date. ii. Dates need to appear in a format that is recognizable to people all over the world and that should be interpreted by computer software. The W3C format allows accurate searching and makes it clear which is the year, month or day. The format is _yyyy-mm-dd', where _yyyy' is the year, _mm' is the month and _dd' the day. iii. Not be confused with Coverage & Disposal– Date refers to dates relevant to the information resource itself, not the information held within the resource; coverage Is the extent he resource covers whereas Disposal – Use the Disposal review refinement to indicate when the decision to keep a resource needs to be made.
Reference:	http://purl.org/dc/elements/1.1/date

Table XIV: Details / Descriptions to Metadata core (Resource Type)

RESOURCE TYPE

Element Name:	**Resource Type**
Label:	Type
Definition:	The nature or genre of the content of the resource.

Obligation:	Mandatory
Description:	i. Enables the user to find a particular type of resource. ii. Not to be confused with Format – Format refers to the physical format of the resource, including the software application used to create, read and edit it; Type refers to the content of the resource and Subject – refers to what the resource is about.
Examples:	Type: Text
Reference:	http://purl.org/dc/elements/1.1/type

Table XV: Details / Descriptions to Metadata core (Format)

FORMAT

Element Name:	**Format**
Label:	Format
Definition:	The physical or digital manifestation of the resource.
Obligation:	Mandatory
Description:	i. Allows the user to search for items of a particular format. ii. Not to be confused with Type – Format looks at the physical format of the resource and includes hard or electronic copy, and the software needed to access the resource; Type considers the content and describes the category of the information in the resource.
Reference:	http://purl.org/dc/elements/1.1/format

Table XVI: Details / Descriptions to Metadata core (Resource Identifier)

RESOURCE IDENTITIFER

Element Name:	**Resource Identifier**
Label:	Identifier

Definition:	An unambiguous reference to the resource within a given context.
Obligation:	Mandatory
Description:	i. Allows a user to search for a specific resource or version. ii. Identification codes automatically allocated by records and content management systems should be used. iii. Identifiers should be made more unique by prefixing them with national codes that are/will be released by the government. iv. Not be confused *with Location* – *Location* indicates the physical location of the resource, not its electronic file path or URL.
Reference:	http://purl.org/dc/elements/1.1/identifier

Table XVII: Details / Descriptions to Metadata core (Source)

SOURCE

Element Name:	**Source**
Label:	Source
Definition:	A reference to a resource from which the present resource is derived.
Obligation:	Mandatory
Description:	i. Enables the user to find resources that have been developed using the content of a particular resource. ii. The described resource may be derived from the Source resource in whole or in part. iii. Not to be confused with Relation – Do not use Source if it is more appropriate to put this data in the Relation element, i.e. it may be more accurate to use the Relation refinement Is version of.
Reference:	http://purl.org/dc/elements/1.1/source

Table XVIII: Details / Descriptions to Metadata core (Language)

LANGUAGE

Element Name:	**Language**
Label:	Language
Definition:	A language of the intellectual content of the resource.
Obligation:	i. Mandatory
Description:	ii. Enables users to limit their searches to resources in a particular language. iii. The use of language codes simplifies the inputting of the Language element. Most systems should be set so that the name of the language is displayed in full, which is more user-friendly. iv. It will be more important for resources that will be loaded onto the internet. It is an invaluable means for people to limit their searches to items that are relevant to their own needs.
Reference:	http://purl.org/dc/elements/1.1/language

Table XIX: Details / Descriptions to Metadata core (Relation)

RELATION

Element Name:	**Relation**
Label:	Relation
Definition:	A reference to a related resource.
Obligation:	Recommendatory
Description:	i. Enables the user to find other resources that are related to a resource, or to group together individual resources which then form a collection. ii. Not be confused with Source –relation describes other document that is next to kin to this resource or documents that are part of this document, whereas source is a term where the resource could be found.

Reference:	http://purl.org/dc/elements/1.1/relation

Table XX: Details / Descriptions to Metadata core (Coverage)

COVERAGE

Element Name:	**Coverage**
Label:	Coverage
Definition:	The extent or scope of the content of the resource.
Obligation:	Mandatory
Description:	i. Enables the user to limit the search to items about a particular place or time. Can be thought of as a sub-section of the Subject element. ii. Not to be confused with Date – The Coverage refinement Temporal refers to the time period covered by the content of the resource, not its creation or publication date. Subject – Coverage contains information about the geographical and time aspects of the content of the resource. It should be thought of as a sub-section of the Subject element. There may be times when it is appropriate to enter the same data in both elements. Location – Location describes the physical whereabouts of the resource; it has nothing to do with what the resource is about.
Reference:	http://purl.org/dc/elements/1.1/coverage

Table XXI: Details / Descriptions to Metadata core (Rights Management)

RIGHTS MANAGEMENT

Element Name:	**Rights Management**
Label:	Rights Management
Definition:	Information about rights held in and over the resource.
Obligation:	Mandatory

Description:	i. Indicates who has the right to see, copy, redistribute, republish or otherwise make use of all or part of the resource. ii. Not to be confused with Accessibility – Accessibility indicates whether particular users will be able to access or use the resource; Rights indicates if they are allowed to. Audience – Audience tells you who the content is designed for; Rights is the place to list the individuals or groups who are allowed to see the resource.
Reference:	http://purl.org/dc/elements/1.1/rights

Table XXII: Details / Descriptions to Metadata core (Accessibility)

ACCESSIBILITY

Element Name:	**Accessibility**
Label:	Accessibility
Definition:	Indicates the resource's availability and usability to specific groups.
Obligation:	Mandatory
Description:	i. Enables those unable to use all information resources to limit the search to items meeting their requirements. ii. Not to be confused with Audience – Accessibility indicates whether particular users will be able to physically access or use the resource; Audience indicates those users for whom the content is designed. iii. Rights indicate who is allowed to see the resource; Accessibility indicates who is actually able to see it.

Table XXIII: Details / Descriptions to Metadata core (Addressee)

ADDRESSEE

Element Name:	**Addressee**
Label:	Addressee

Definition:	The person (or persons) to whom the resource was addressed.
Obligation:	Mandatory
Description:	i. Enables the user to identify the person(s) to whom the resource was dispatched. ii. Note that this does not provide evidence that the intended person actually received or read it, nor that they had the right or ability to access it. It is likely that in practice this element will mainly be used when describing e-mails. It is also applicable to other types of correspondence or any resource which is distributed. iii. Includes those listed in _cc' and _bcc' lists. Use the Addressee copy refinement to list person(s) to whom the resource was copied. iv. Not to be confused with Audience & rights – Audience refers to the wider sector of the population for whom the resource was intended; Addressee refers to the person or group to whom it was actively sent and rights refers to the person or group who have the right to see the resource, whether or not it has actually been sent to them.
Examples:	Addressee : Xyz@ega.org

Table XXIV: Details / Descriptions to Metadata core (Aggregation)

AGGREGATION

Element Name:	**Aggregation**
Label:	Aggregation
Definition:	The resource's level or position in a hierarchy.
Obligation:	Mandatory

Description:	i. Aggregation allows searches to be restricted to resources at a particular level. It also helps indicate which actions should be carried out on the resource. ii. It shows the extent to which the resource is part of a larger resource or collection, and defines where in a hierarchy it belongs. An example of this could be a folder containing individual records, where all actions that are performed on the folder, such as a change in the security classification, automatically affect each record in the folder.
Examples:	Aggregation: EGIF Folder

Table XXV: Details / Descriptions to Metadata core (Audience)

AUDIENCE

Element Name:	**Audience**
Label:	Audience
Definition:	A category of user for whom the resource is intended.
Obligation:	Mandatory
Description:	i. Enables the user to indicate the level or focus of the resource, as well as enabling filtering of a search to items suited to the intended audience. ii. Do not use Audience unless the resource is prepared with a particular group in mind. If it is for general release, leave it blank. iii. Not to be confused with Accessibility, Rights and Addressee – Audience indicates which users the content is aimed at; Accessibility indicates whether particular users will be able to access or use the resource whereas Rights informs the user of a list of individuals or groups who are allowed to see the resource and Addressee refers to the person(s) to whom the resource was actually sent.
Examples:	Audience: Citizens

Reference:	http://purl.org/dc/terms/audience

Table XXVI: Details / Descriptions to Metadata core (Digital Signature)
DIGITAL SIGNATURE

Element Name:	**Digital Signature**
Label:	Digital Signature
Definition:	Authentication information used for the verification of resources in transactions.
Obligation:	Mandatory
Description:	i. The National Archives will examine what metadata is likely to be created by digital signature technology and how far it is of relevance/use in records management when the adoption of this technology is advanced.

Table XXVII: Details / Descriptions to Metadata core (Disposal)
DISPOSAL

Element Name:	**Disposal**
Label:	Disposal
Definition:	The retention and disposal instructions for the resource.
Obligation:	Mandatory

Description:	i. Helps the user manage resources and ensure that they are not kept after they are needed or disposed of before their time. ii. It is Recommendatory that all web pages have a review date, so webmasters can easily locate pages before they become out of date and take necessary action, iii. Disposal in electronic records management systems (ERMS) is generally managed at the folder level. ERMS manage the disposal of resources to ensure they are only destroyed in accordance with an agreed disposal schedule and retained for periods consistent with the need to retain the resource.

Table XXVIII: Details / Descriptions to Metadata core (Location)

LOCATION

Element Name:	**Location**
Label:	Location
Definition:	The physical location of the resource.
Obligation:	Recommendatory
Description:	i. Enables the physical form of the resource to be found. Location will mainly be used for items held in a physical format. ii. This is especially relevant for items listed in a metadata base (a catalogue containing the metadata of resources but not the resources themselves) cause resources which are not available in electronic format might be referred to. iii. Not to be confused with Identifier – The URL or filename refers to an electronic, machine- readable pathway, not a physical location. Such information should go in the Identifier element. Coverage – This element concerns what the resource is about and not where the resource is.

Table XXIX: Details / Descriptions to Metadata core (Mandate)

MANDATE

Element Name:	**Mandate**
Label:	Mandate
Definition:	Legislative or other mandate under which the resource was produced.
Obligation:	Mandatory
Description:	i. Clarifies the legislative or other mandate for the business activity producing the records. ii. Not to be confused with Rights – Exemption from the data subject access provisions of the data protection act.

Table XXX: Details / Descriptions to Metadata core (Preservation)
PRESERVATION

Element Name:	**Preservation**
Label:	Preservation
Definition:	Information to support the long-term preservation of a resource.
Obligation:	Mandatory

Description:	Enables users now and in the future to read, interpret and use the resource. Preservation will mainly be used by records managers and others engaged in the long-term storage of official records. It will be used to support departmental migration activity, sustainability and archival preservation of the resource, and to preserve aspects of the provenance of the resource across transfer of custody between departments and to the Archives Record Management unit. A variety of approaches may have to be taken to sustain and preserve electronic resources and their components across technical platforms. Information on the technical environment that produced the original objects greatly improves the chances of such approaches being achieved successfully and may allow digital archaeological reconstruction where past management has been lacking (and costs are justified). Some of this information may need to be included in an archival description or custody documentation. As preservation strategies across government emerge, some of the refinements may need to be mandated in future for resources identified as being of long-term importance. Additionally, some will concern the original environment of the records (possibly requiring automatic capture at declaration stage) and others may be defined at the batch level for resources at platform or format migration. Not to be confused with Format – This provides information about the format of the resource for current processing; Preservation provides additional information intended to facilitate long-term preservation.

Table XXXI: Details / Descriptions to Metadata core (Status)

STATUS

Element Name:	**Status**
Label:	status
Definition:	The position or state of the resource.
Obligation:	Mandatory
Description:	i. Enables the user to search for a resource according to its status. It may also be used as a reference by a user who wants to know the resource's status. ii. The status of a resource includes the extent to which it has been developed or completed, the version number, purpose and approval. a. This data should apply to the described resource only, not to earlier versions.

Data Standards

The adoption of data standards for use across Public Institutions will enable easier, more efficient exchanging and processing of data. It will also remove ambiguities and inconsistencies in the use of data across the government ministries, departments & govt. agencies. These standards apply to all systems that are mandated in the e-GIF and are for use in all other public sector interfaces. Compliance with these standards should follow the e-GIF compliance policies.

Data Standard Template

Each data standard will be documented using the following template. The template is based on e-GIF (e- Governance Interoperability Framework) Standard of UK

Table XXXII: Data Standards Template

Metadata	**Value**
Name	The full name of the generic or common Data Type/Data Element
Description	A simple but unambiguous definition / description of the Data Type
Type	Generic or Specific Data Element

Is Part of	If the data element is a part of a parent data element
Has Part	The list of sub parts or the child data elements for this parent data
Data Format & Size	The required format of the data from the specific domain perspective. This will include the minimum and maximum number of characters if appropriate, and the structure of the data element
Version	The version number of this standard
UML	The UML representation of the data element
XML Schema ID	The identifier of the XML schema where the data standard is used. It is expected that a standard will only be used in one schema and all government schemas will be held on National Portal schema will show the pattern, i.e. the size and mask, of the standard. The XML schema will show the pattern, i.e. the size and mask, of the standard
Validations	Generic validations for Types and specific validations for Items. The validation rules to be applied for acceptance of data (e.g. first alpha character must be A, B or C).
Values	List of the acceptable values (e.g. Male, Female)
Default	For any list of values, the default value to be used unless otherwise
Owner	Name(s) of those Departments who own this standard
Based on	Origin of the standard (e.g. ISO, BSI, W3C etc)
Verification	Steps taken to establish the correctness of the Data Elements. Such steps taken for different level of verifications by departments will be detailed here
Comments	Additional notes
Status	The current status of the standard (Drafted or Agreed)
Date Agreed	The date this version was agreed as a Government Data Standard

Data Standard Catalog

The Data Standards Catalogue sets out the rationale, approach and rules for setting and agreeing at the set of Government Data Standards (GDS) to be used in the Govt. Data Schemas and other electronic interchanges of data involving the public sector, developed to support the e-GIF. These standards are defined at a logical

(business) level and not at a physical database storage level. However it is recommended that they be used for specifying data storage at the business level.

The data standards catalog provides a detailed description of the Govt. Data Standards of the common/generic data entities identified to be used across the Public Institutions. *The following sub section lists the data standards for some of the important common data entities as an example.*

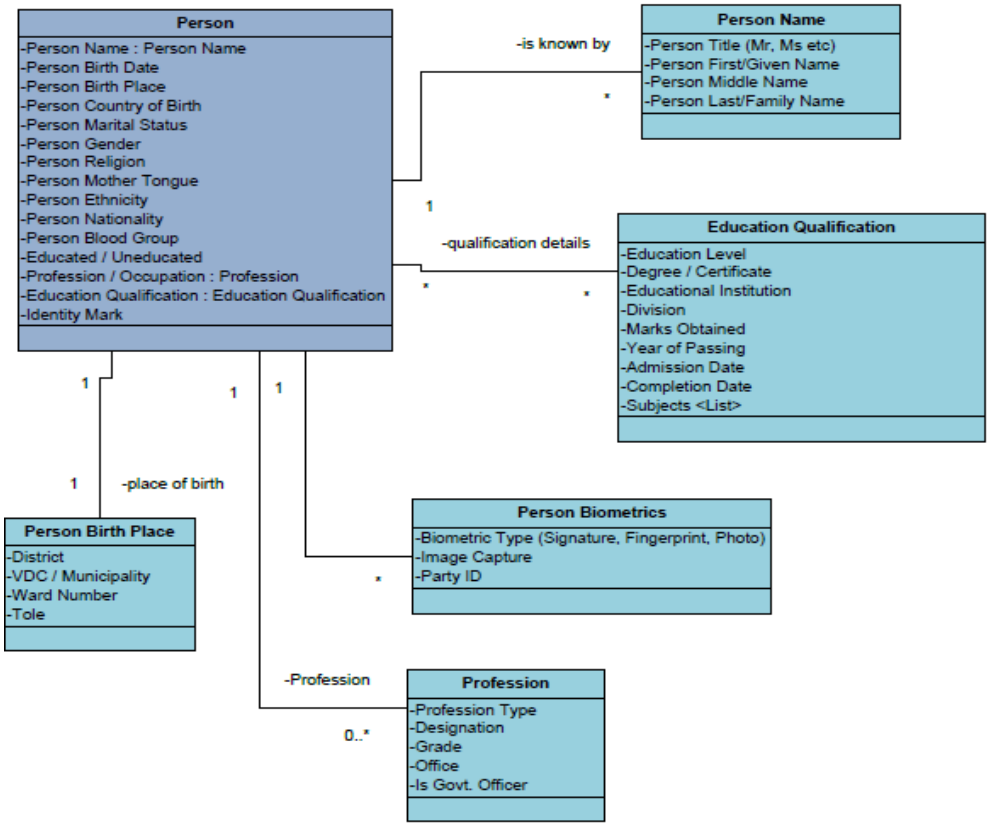
Table XXXIII: Data standards (Person)
PERSON

Metadata	**Value**
Name	**Person**
Description	This data entity is a composition of data elements that describes an individual or person for e.g. person name, birthdate, marital status, gender, religion, profession etc. Typically Citizens (including voters, taxpayers, land owners, vehicle owners, consumers), Govt employees will be classified as Person
Type	Generic Data Element
Is Part of	Party (Supertype)

Has Part	**Name of Data Element**	**Data Format**	**Maximum Size**
	Person Name	VarChar	99
	Person Birth Date	Date (dd/mm/yyyy)	10
	Person Place of Birth	VarChar	50
	Person Country of Birth	VarChar	50
	Person Marital Status	Integer (1 - Never Married,2 - Currently Married, 3- Widow / Widower, 4- Divorced, 5- Separated)	1
Data Format & Size	Person Gender	Char (M – Male, F – Female, T – Transgender)	1
Version	•Person Mother Tongue	VarChar	50
	•Person Religion	Integer	2
	•Person Nationality	VarChar	50
	•Person Blood Group	VarChar	10
	•Educated /Uneducated	Integer (Y or N)	1
	•Education Qualification	VarChar	50
	•Profession / Occupation	VarChar	50
	•Identity Mark	VarChar	50

Cover the format & size of individual child data elements in the Data Standard Catalog

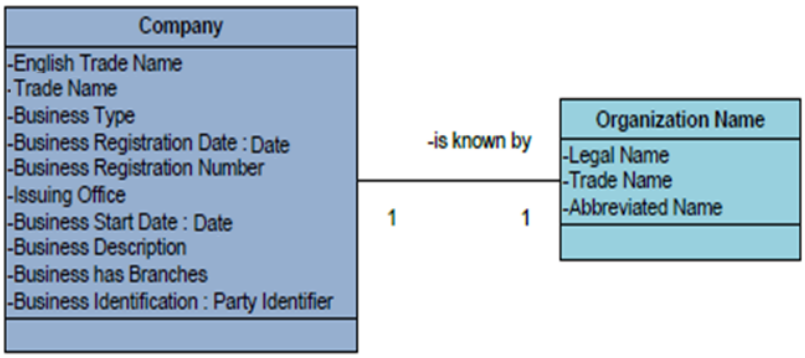
1.0

UML Diagram	
XML Schema ID	Refer to XML Schema (xsd) **PersonDescriptiveType** Refer to XML Definition **Person Structure**
Validations	Cover the validations of individual child data elements in the Data Standard Catalog
Values	Cover the values of individual child data elements in the Data Standard Catalog
Default Value	None
Owner	
Based on	
Verification	None
Comments	
Status	Drafted

Date Agreed	TBD

Table XXXIV: Data standards (Company)

COMPANY

Metadata	**Value**
Name	**Company**
Description	This data entity is a composition of data elements that describes a legal entity like company or organization e.g. organization name, business type, business registration number etc. Typically businesses like Private Limited Company / Public Limited Company / Partnership Firm / Charity Organization / Educational
Type	Generic Data Element
Is Part of	Party (Supertype)
Has Part	i. Organization Name ii. Business Type iii. Business Registration Date iv. Business Registration Number v. Registration Issuing Office vi. Business Start Date vii. Business Description
Data Format & Size	Cover the format & size of individual child data elements in the Data Standard Catalog
Version	1.0
UML Diagram	
XML	Refer to XML Schema (xsd) **CompanyDescriptiveType** Refer to XML Definition **Company** Structure

Schema ID	
Validations	Define the validations of individual child data elements in the Data Standard Catalog
Values	Refer to values of individual child data elements in the Data Standard Catalog
Default Value	None
Owner	
Based on	
Verification	None
Comments	
Status	Drafted
Date Agreed	TBD

Table XXXV: Data standards (Address)

ADDRESS

Metadata	**Value**
Name	**Address**
Description	The generic data element that captures the details of the postal address of a party.
Type	Generic Data Element
Is Part of	
Has Part	i. Address ID ii. Country Code iii. Development Region iv. Administrative Zone v. District vi. Constituency vii. Municipality Type viii. Municipality ix. Ward Number

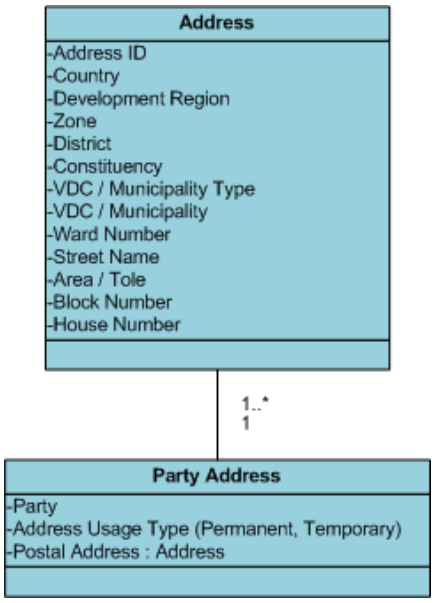
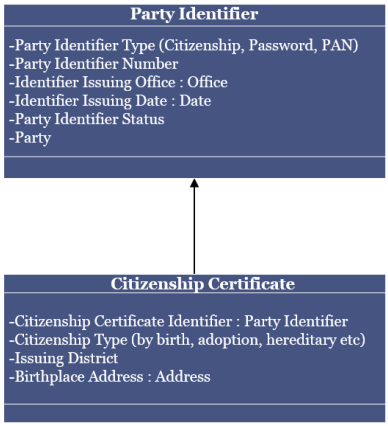
Data Format & Size	Cover the format & size of individual child data elements
Version	1.0
UML Diagram	
XML Schema ID	Refer to XML Schema (xsd) **AddressDescriptiveType** Refer to XML Definition **Address Structure**
Validations	Define the validations of the individual child data elements
Values	Refer to the values of the individual child data elements
Default Value	None
Owner	
Based on	As per the definition of the administrative units
Verification	None
Comments	
Status	Drafted
Date Agreed	

Table XXXVI: Data standards (Citizenship Certificate)

CITENZENSHIP CERTIFICATE

Metadata	**Value**
Name	**Citizenship Certificate**
Description	This is a specialized form of Party Identifier data element that captures citizenship certificate details of a citizen of Tanzania.

Type	Generic Data Element
Is Part of	Party Identifier (SuperType)
Has Part	i. Citizenship Certificate Identifier (extended from Party Identifier) ii. Citizenship Type (by birth, adoption, hereditary etc) iii. Citizenship Certificate Issuing District
Data Format & Size	*Cover the format & size of the individual child elements in the Data Standard Catalog*
Version	1.0
UML Diagram	
XML Schema ID	Refer to XML Schema (xsd) **PartyIdentifierDescriptiveType** Refer to XML Definition **CitizenshipCertificate** Structure
Validations	Define the validation of the individual child elements in the Data Standard Catalog
Values	Refer to the values of the individual child elements in the Data Standard Catalog
Owner	Ministry of Home Affairs
Based on	
Verification	***If Descendent*** i. Birth Certificate / Educational Certificate ii. Citizenship Certificates of Parents iii. Documents showing ownership of property in the District in family's name OR Migration Certificate issued by relevant

	authority Office ***If married to a Tanzania man*** i. Citizenship Certificate of Husband ii. Marriage Certificate iii. NOC from Country of Origin iv. Documents showing ownership of property in the District in Husband's family name OR Migration Certificate issued by relevant Office to Husband's family v. Recommendation Letter from Chairperson / Mayor / Municipality Secretary
Comments	
Status	Drafted
Date Agreed	TDB

Meta Data Technology

XrML

Description

XrML provides a universal method for securely specifying and managing rights (and associated conditions) for all kinds of resources including digital content and services. It supports content integrity and entity authentication and confidentiality within the specification. Encodes in XML, leverages standard XML schemas, namespaces, digital signatures etc. It's customizable, and extensible and offers lot of flexibility.

Standard Details

XrML 2.0 is used to specify metadata for resources by leveraging the standard methodology developed by the Dublin Core Metadata Initiative. It has four key components namely

i. Principal (person, device, application, etc.)

ii. Resource (work, service, name, etc.)
iii. Right (view, play, print, copy, forward, etc.)
iv. Condition (fee, time, geography, etc.).

Due to this interoperability is ensured as it should specify and "reach web services, allowing extended or more elaborate rights management for example seeking approval, reporting usage or tracking usage. Language should specify the trust environment before rights should be executed the rights expression should ensure confidentiality and integrity which is key in government sector. The details about the standards are provide in link mentioned in the resource locator below.

Reference Links: *- xrML http://ww.xrml.o/*

The Open Archives Initiative Protocol

Description:

The Open Archives Initiative Protocol for Metadata Harvesting (referred to as the OAI-PMH in the remainder of this document) provides an application-independent interoperability framework based on metadata harvesting. There are two classes of participants in the OAI-PMH framework:

a. Data Providers administer systems that support the OAI-PMH as a means of exposing metadata; and

b. Service Providers use metadata harvested via the OAI-PMH as a basis for building value-added services.

Standard Details:

This protocol mandates that individual archives map their metadata, a simple and common metadata set for this purpose. In other words, the relation of OAI compatibility to is that OAI standards allow a common way to provide content, and part of those standards is that the content has metadata that describes the items in Core format. The detailed specification and definitions are provided in the URL below.

Resource Locator

i. OAI-PMH

http://www.openarchives.org/OAI/openarchivesprotocol.html

ANSI/NISO Z39.87

Description:

This standard defines a set of metadata elements for raster digital images to enable users to develop, exchange, and interpret digital image files.

Standard Details:

The dictionary has been designed to facilitate interoperability between systems, services, and software as well as to support the long-term management of and continuing access to digital image collections.

Resource Locator:

i. ANSI/NISO Z39.87

http://www.niso.org/kst/reports/standards?step=2&gid=None&project_key=b897b0cf3e2ee5262 52d9f830207b3cc9f3b6c2c.

MIX2.0

Description:

The Library of Congress' Network Development and MARC Standards Office, in partnership with the NISO Technical Metadata for Digital Still Images Standards Committee and other interested experts, is developing an XML schema for a set of technical data elements required to manage digital image collections. This schema is currently referred to as "NISO Metadata for Images in XML (NISO MIX)".

Standard Details

This is an XML schema that provides a format for interchange and/or storage of the data specified in the Data Dictionary - Technical Metadata for Digital Still Images (ANSI/NISO Z39.87-2006). MIX is expressed using the XML schema language of the World Wide Web Consortium. MIX is maintained for NISO by the Network

Development and MARC Standards Office of the Library of Congress with input from users.

Resource Locator:

i. MIX2.0

http://www.loc.gov/standards/mix//

ODRL1.1

Description:

ODRL (Open Digital Rights Language) is an XML-based standard Rights Expression Language (REL) used in Digital Rights Management systems and open content management systems. ODRL is managed by an open organization that's open to public participation. ODRL explicitly support the use of right vocabularies from various sectors and communities. Its goal is to also support the reuse of other metadata vocabularies to supplement, e.g. the context element. For example, instead of using the context element to describe personal information, the vCard standard should be used. It has created a profile that supports Dublin Core Metadata Initiative (DCMI) metadata. It supports formal representation of ODRL data model in UML form which will improve ODRL data models.

Standard Details

ODRL is a standard language and vocabulary for the expression of terms and conditions over assets. ODRL covers a core set of semantics for these purposes including the rights holders and the expression of permissible usages for asset manifestations. Rights should be specified for a specific asset manifestation (i.e. format) or should be applied to a range of manifestations of the asset.

ODRL is focused on the semantics of expressing rights languages and definitions of elements in the data dictionary. ODRL defines a core set of semantics. Additional semantics should be layered on top of ODRL for third-party value added services with additional data dictionaries.

ODRL does not enforce or mandate any policies for DRM, but provides the mechanisms to express such policies. Communities or organisations, that establish

such policies based on ODRL, do so based on their specific business or public access requirements.

ODRL depends on the use of unique identification of assets and parties. The ODRL specification contains:

i. The model for the ODRL expression language.

ii. The semantics of the ODRL data dictionary elements.

iii. The XML syntax used to encode the ODRL expressions and elements.

iv. Additional ODRL data dictionaries should be defined.

Resource Locator:

i. ODRL1.1

http://www.w3.org/TR/odrl/

Meta Data Registry

Description

The Meta data core, Meta Data and Government thesaurus will be held in a Registry (Meta Data Registry). By using tools the registry should be searched for selection and retrieval in application development thus enabling reuse. Adding resources to the Registry enables collaboration. There are standards to manage the Meta data registry.

Standard Details

ISO 11179 provides the Framework for the specification and standardization of data/metadata elements. These standards are provided for data element repositories; work on Taxonomies, Thesaurus and Dictionary. It contains various sections such as:

i. **Framework** - This part of ISO/IEC 11179 introduces and discusses fundamental ideas of data elements, value domains, data element concepts, conceptual domains, and classification schemes essential to the understanding of this set of standards and provides the context for associating the individual parts of ISO/IEC 11179.

ii. **Classification for administered items**- This part of ISO/IEC 11179 provides a conceptual model for managing classification schemes. There are many structures used to organize classification schemes and there are many subject matter areas that classification schemes describe. So, this part also provides a two-faceted classification for classification schemes themselves.

iii. **Registry meta model and basic attributes**- This part of ISO/IEC 11179 specifies a conceptual model for a metadata registry, and a set of basic attributes for metadata for use when a full registry solution is not needed

iv. **Formulation of data definitions**- This part of ISO/IEC 11179 provides guidance on how to develop unambiguous data definitions. A number of

specific policies and guidelines are presented in ISO/IEC

v. **Naming and identification principles**- This part of ISO/IEC 11179 provides guidance for the identification of administered items. Identification is a broad term for designating, or identifying, a particular data item. Identification should be accomplished in various ways, depending upon the use of the identifier. Identification includes the assignment of numerical identifiers that have no inherent meanings to humans; icons (graphic symbols to which meaning has been assigned); and names with embedded meaning, usually for human understanding, that are associated with the data item's definition and value domain.

vi. **Registration**- This part of ISO/IEC 11179 provides instruction on how a registration applicant may register a data item with a central Registration Authority and the allocation of unique identifiers for each data item. Maintenance of administered items already registered is also specified in this document.

Resource Locator

i. ISO11179

http://metadata-stds.org/11179/

2.3.1.1. The governance and compliance of e-GIF shall be handled by the e-GIF working group as defined in the *eGovernment Process and Governance for Enterprise Architecture (eGA/EXT/ARC/009) document*. The e-GIF governance and compliance shall include the following:

Table XXXVII: e-GIF Governance and Compliance

Creation of e-GIF	i. Publication of e-GIF standards ii. Train the champions on e-GIF (e-GIF working group) iii. Release e-GIF Version (Standards) iv. Begin awareness/training for each Public Institution's on e-GIF (Training programs, Website, FAQs, etc)

Maintenance of e-GIF	e-GIF is a living document which needs to be updated at frequent intervals from document creation, proposals, approvals and release for usage to Public Institutions.
Monitoring	i. Ensuring compliance to standards defined in e-GIF for any major system upgrade, migration of systems or changeover of systems. This shall be done by e-GIF working group and relevant stakeholders: a. Validation of business case b. Validation of proposed solution c. Validation of preliminary and detailed architecture d. Validation of quality attributes and architecture trade-offs analysis e. Validation of implementation architectures f. Validation of architecture changes and post project implementation assessment
Compliance self-assessment	Self-assessment will require the respective Public Institution to ensure that the checklist of the e-GIF compliance is made available upfront and they report a self-assessment of compliance on the project to e-GIF working group at different stages of the project.
Review of compliance	A compliance team has to be formed by e-GIF Working Group to carry out e-GIF reviews of the projects to check for and ensure compliance with the envisaged standards, policies and criterion. The compliance teams should define a framework for compliance evaluation and distribute it to all Public Institutions so that they are aware of the compliance requirements/criteria.
Compliance Process	**Gather** – Collection of relevant and sufficient data/functional requirements of a project at the respective stage for which review is done. Then a comparison should be made with e-GIF standards based on a pre-defined compliance questionnaire (checklists).

	Analyse - Analyse the collected data and form initial compliance assessment. The analysis will also take into account the subjective environment, permissible exclusion, on the ground realities. **Validate -** Validate the analyses, further meetings/interviews should be conducted with the Public Institutions to firm up analysis. **Report** – Submission of compliance report and trigger exemption process is required. This should also be triggered, heard and resolved during the post implementation compliance review.

2.4. e-Government Interoperability Framework Technical Guidelines

2.4.1. Public institutions will take into consideration the dimensions for e-GIF (Organisational Interoperability, semantic interoperability and technical interoperability) as demonstrated in *figure II.* The security requirements for the information, the services, and the infrastructure should be identified and treated in accordance to the type of information, SLA's, and the outcome of the risk analysis.

2.4.2. Internal network security policie will be enforced across all Public Institutions. The policies will be updated and maintained by each Public Institution. The concerned Public Institutions will also set out a framework to assure the availability, integrity and confidentiality of e-Government services, specifically lay out procedures for identity registration, enrolment and authentication processes which are important for citizens to access e-Service. Adding to that,

key procedures pertaining to the above areas will be implemented and enforced.

2.4.3. The security policies, procedures and standards shall be enforced to protect the privacy of data. Suitable media should be used to store, transport, and process to provide the adequate level of protection needed.

2.4.4. Whenever data and information flows into /out of critical systems (as defined by a Public Institution) the Public Institution will ensure they monitor:

i. such flow whenever they occur,

ii. the information transmitted,

iii. the purpose of such information/data flow,

iv. parties involved in exchange and collection of such information

v. for how long the information is going to be held and under what circumstances.

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

3.1. This document takes effect once signed and approved in its first page.

3.2. This document is subject to review at least once every three years.

3.3. This Documents need to be complied with as directed in the most current version of "*Mwongozo wa Matumizi Bora, Sahihi na Salama ya Vifaa na Mifumo ya TEHAMA Serikalini".*

4. GLOSSARY AND ACRONYMS

4.1. Glossary

None

4.2. Acronyms

Abbreviation	Explanation
3DES	Triple Data Encryption Algorithm
ACID	Atomicity, Consistency, Isolation, and Durability

Abbreviation	Explanation
ADSL	Asymmetric Digital Subscriber Line
AMQP	Advanced Message Queuing Protocol
ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Automatic Teller Machine
AVI	Audio Video Interleave
B2B	Business-to-Business
BGP	Border Gateway protocol
BI	Business Intelligence
BPEL4WS	Business Process Execution Language for Web Services
BPMN	Business Process Modeling Notation
BPR	Business Process Re-Engineering
Cat 6	Category 6 UTP cable
CDB	Common Database
CDMA	Code Division Multi Access
CGM	Computer Graphics Metafile
CoBIT	Control Objectives for Information and related Technology
COM	Component Object Model
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off the Shelve
CSS	Cascading Style Sheet
CSV	Comma Separated Values
DBA	Data Base Administrator
DBMS	Data Base Management System
DCCP	Datagram Congestion Control Protocol

Abbreviation	Explanation
DCOM	Distributed Component Object Model
DES	Data Encryption Algorithm
DHCP	Dynamic Host Configuration Host protocol
DNS	Domain Name Services
DOM	Document Object Model
DRM	Digital Rights Management
DTD	Document Type Definition
EA	Enterprise Architecture
ebXML	E-business XML
ECN	Explicit Congestion Notification
EDI	Electronic Data Interchange
e-GIF	e-Government Interoperability Framework
ERD	Entity-Relationship Diagram
EVDO	Evolution Data Optimized
FDDI	Fiber Distributed Data interface
FTP	File Transfer Protocol
FTPS	Secure File Transfer Protocol
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GT	Government Thesaurus
GIF	Graphics Interchange Format
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSMA	Global System for Mobile communications Association
GTP	GPRS Tunneling Protocol

Abbreviation	Explanation
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
HSPA	High Speed Packet Access
ICA	International Compliance Association
ICT	Information and Communication Technology
ICMP	Internet Control Message Protocol
IDL	Interface Description Language
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPsec	IP Security Authentication Header
IRC	Inter Relay Chat
ISBN	International Standard Book Number
IS-IS	Intermediate System to Intermediate System
ISO	International Standards Organisation
ISSN	International Standard Serial Number
ITIL	Information Technology Infrastructure Library
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JDBC	Java Database Connectivity
JMS	Java Message Service

Abbreviation	Explanation
JPEG	Joint Photographic Experts Group
JVM	Java Virtual Machine
KPI	Key Performance Indicators
LDAP	Lightweight Directory Access Protocol
L2TP	Layer 2 Tunneling Protocol
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extensions
MIX	Metadata for Images in XML
MP-BGP	Multi-Protocol-Border Gateway Protocol
MPEG	Moving Picture Experts Group
MPLS	Multi-Protocol Label Switching
MPLS-OAM	Multi-Protocol Label Switching – Operation Administration and Maintenance
MPLS-TE	Multi-Protocol Label Switching -Traffic Engineering
MSAG	Multi-Service Access Gateway
MSDP	Multi Source Discovery Protocol
MSMQ	Microsoft Message Queuing
MTA	Message Transfer Agent
NAS	Network –Attached Storage
NDA	Non-Disclosure Agreement
GIDC	Government Information Data Centre
NDP	Neighbor Discovery Protocol
NISO	National Information Standards Organization
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OAI-PMH	Open Archives Initiative - Protocol for Metadata Harvesting

Abbreviation	Explanation
OASIS	Organization for the Advancement of Structured Information Standards
ODBC	Open Database Connectivity
ODRL	Open Digital Rights Language
OEM	Original Equipment Manufacturer
OGC	Open Geospatial Consortium
OLEDB	Object Linking and Embedding Database
ORB	Object Request Broker
OSPF	Open Shortest Path First
OS	Operating System
PDA	Personal Digital Assistant
PDF	Portable Document Format
POP	Post Office Protocol
POSIX	Portable Operating System Interface
PPP	Point to Point Protocol
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PST	Personal Storage Table
P3P	Platform for Privacy preferences
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RARP	Reverse Address Resolution Protocol
RDBMS	Relational Data Base Management System
RDF	Resource Description Framework
RFC	Request for Comments
RIP	Routing Information Protocol

Abbreviation	Explanation
RMON	Remote Network Monitoring
RPC	Remote Procedure Calls
RSTP	Rapid Spanning Tree protocol
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
RSVP	Resource Reservation protocol
RSVP-TE	Resource Reservation protocol-Traffic Engineering
SAM	Self-service Automated Machine
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SCTP	Stream Control Transmission protocol
SCM	Software Configuration Management
SCP	Session Control Protocol
SDLC	Software Development Life Cycle
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation protocol
SLA	Service Level Agreement
SMTP	Simple Mail Transfer protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
STP	Spanning Tree Protocol
SSH	Secure Shell
SSM	Source Specific Multicast
SVG	Scalable Vector Graphics
S/MIME	Secure/Multipurpose Internet Mail Extensions

Abbreviation	Explanation
TA	Transport Authority
TC	Trust Computing
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
Telnet	Teletype Network
TFTP	Trivial File Transfer Protocol
TIA	Telecommunication Industry Association
TIFF	Tagged Image File Format
UBL	Universal business Language
UDDI	Universal Description Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling language
UTP	Unshielded Twisted Pair
URN	Uniform Resource Name
VDSL	Video Digital Subscribers Line
VRRP	Virtual Router Redundancy Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAI	Web Access Initiative
WCAG	Web Content Access Guidelines
WCDMA	Wide Band Code Division Multiple Access
WIMAX	Worldwide Interoperability for Microwave Access
WFS	Web Feature Services
WML	Wireless Markup Language
WMS	Web Map Service
WSDL	Web Service Definition Language

Abbreviation	Explanation
WSRP	Web Service for Remote Portlets
WSRM	Web Services Reliable Messaging
WSS	Web Services Security
WS-I	Web Services-Interoperability
W3C	World Wide Web Consortium
XHTML	Extensible Hypertext Markup Language
XMPP	Extensible Messaging and Presence Protocol
XCIL	Extensible Customer Information Language
XLS	Excel Worksheets
XMI	XML Metadata Interchange
XML	Extensible Markup Language
XNAL	Extensible Name and Address Language
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformation
XTP	Xpress Transport protocol

5. RELATED DOCUMENTS

5.1. Mwongozo wa Matumizi Bora, Sahihi na Salama ya Vifaa na Mifumo ya TEHAMA Serikalini Toleo la 2

5.2. eGovernment Architecture Vision - Standards and Technical Guidelines *(eGA/EXT/AVS/001)*

5.3. eGovernment Application Architecture - Standards and Technical Guidelines *(eGA/EXT/APA/001)*

5.4. eGovernment Business Architecture - Standards and Technical Guidelines *(eGA/EXT/BSA/001)*

5.5. eGovernment Information Architecture - Standards and Technical Guidelines *(eGA/EXT/IFA/001)*

5.6. eGovernment Processes and Governance - Standards and Technical Guidelines *(eGA/EXT/PAG/001)*

5.7. eGovernment Integration Architecture - Standards and Technical Guidelines *(eGA/EXT/ITA/001)*

5.8. eGovernment Infrastructure Architecture - Standards and Technical Guidelines *(eGA/EXT/IRA/001)*

5.9. eGovernment Security Architecture - Standards and Technical Guidelines *(eGA/EXT/ISA/001)*

6. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	eGA	Creation of Document	February 2016

7. APPENDIX

Illustration No.1 - Typical Interaction Points

The Ministry of Social Welfare operates in a complex environment, where very often information on citizens is segregated amongst various Public Institutions or the private sector. The table below demonstrates the various interaction points between the Ministry of Social Welfare and other public and private institutions.

Table XXXIX: Typical Interaction Points

S.No.	Stakeholders to Ministry of Social Welfare	Description
1.	RITA	Notify on death, remarriage
2.	Immigration Department	Notify on departures
3.	Tanzania Police Force	Notify on admission of beneficiaries in Jail
4.	BRELA	Recording of objections to winding up
5.	Ministry of Labour	Pension Contributions by Employers and Employees
6.	Insurance Company	Perform assessment for Insurance Schemes
7.	Banks/ Post Office	Receiving payment instructions, sending acknowledgement, reconciliation and other reports
8.	Tanzania Revenue Authority	Submission of returns and contributions effected

This kind of cooperation across Public Institutions results in each institution being granted access to more information and is therefore better able to supervise and provide services.