THE REPUBLIC OF UGANDA

Uganda e-Government Interoperability Framework (e-GIF)

Project: THE REPUBLIC OF UGANDA CONSULTANCY SERVICES FOR THE DEVELOPMENT OF A GOVERNMENT ENTERPRISE ARCHITECTURE (GEA) AND E-GOVERNMENT INTEROPERABILITY FRAMEWORK (E-GIF)

Project duration: 10 November 2020 – 09 September 2021

May 6, 2021

Table of Contents

1. Executive Summary

1.1. The need

Uganda is modernising its e-Government by introducing digital public services. The Government of Uganda (GoU) has developed a number of ICT systems in the Government. At the edge the e-Citizen portal www.ecitizen.go.ug provide one stop access for all GOU public services.

There are currently a lot of ICT systems available from which many appear to be doing similar if not duplicated functions. It implies not only duplication of functions but also wasting already scarce resources. Isolated and largely disparate digital systems are not sharing data and information with each other. Citizens and businesses carry information from one organisation to another using paper documents like certificates, proofs, receipts, evidence etc. For the GOU agencies that have built applications that offer digital services, sharing of information between these GOU agencies is limited.

For this reason, there should be efforts to harmonize GOU digitization efforts to avoid digital fragmentation of services and data. To guarantee digital information sharing, we need to set up and run interoperable systems which ensure effective communication between digital components such as devices, networks, and data repositories.

Government organisations' information systems are developed for a specific purpose to meet the exact requirements of the respective organisation's core mandate. Interoperability of government systems ensures that the valuable information across the government systems is shared to collectively support delivery of more useful and productive services and integration of the government business processes. Interoperability is the ability of making systems and organisations operate together (inter-operate).

The objective of this eGovernment Interoperability Framework, hereinafter: **e-GIF**, is to outline the main principles and general guidelines enabling development and implementation of shared electronic services for citizens, businesses, and MDA/LGs in the Ugandan Government.

1.2. Approach

The e-GIF uses the terminology and structure of the European Interoperability Framework (EIF)[1], the content is adjusted to the GoU national policies, strategies, and guidelines.

Interoperability is both a prerequisite for and a facilitator of the efficient delivery of public services. The Interoperability framework aims to improve:

- cooperation between MDA/LGs aiming at the establishment of public services,

[1] https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

- information exchange between MDA/LGs to fulfil legal requirements or political commitments,
- sharing and reusing information among MDA/LGs to increase administrative efficiency and reduce administrative burden on citizens and businesses.

Most e-GIF underlying principles are inspired by the EIF: subsidiarity and proportionality, openness, transparency, reusability, technological neutrality and data portability, user-centricity, inclusion and accessibility, security, privacy, administrative simplification, preservation of information, assessment of effectiveness and efficiency.

For achieving the **interoperability by design** paradigm, the e-GIF implements a model that includes:

- four layers of interoperability: legal, organisational, semantic, and technical
- a cross-cutting component of the four layers: integrated public service governance
- a back-ground layer: interoperability governance.

MDA/LGs need to agree on a common approach to interconnect information systems and services. The e-GIF proposes a conceptual model that must be used as the baseline for that common approach that comprises loosely coupled components interconnected through shared infrastructure.

Cross-border services is quite a new challenge for GOU. There are initiated several sectorial cross-border based projects such as Northern Corridor Integration Projects (NCIP) and African Union Health Information Exchange (AfricaCDE HIE). The e-GIF SHOULD consider the needs cross-border services.

To ensure interoperability of GOU information systems, several common infrastructure components must be established in the GOU with very clear ownership, lead and responsibility.

2.Introduction

The National Vision 2040[2] stipulates that ICT has enormous opportunities that Uganda can exploit to transform the economy through: build robust and trusted high speed ICT infrastructure; manufacturing of ICT products; improving availability of digital content and e-products, automation of Government processes and inter-agency connectivity & innovation; development of platforms on which the private sector can co-create with the Government, offering new value-added services to the public; and establishment of incubation centres among others.

Digital Uganda Vision (DUV)[3] has declared a vision (*A Digitally Empowered Society and Knowledge Economy*) and mission *(To Transform Uganda into a digitally enabled society that is innovative, productive, and competitive).* The DUV is an overarching 20-year ICT development framework that is aligned to the Uganda Vision 2040. It aims to harmonise Uganda's transformative policies, strategies, initiatives, and other governance frameworks for the expedient realisation of national development aspirations.

GoU e-Government Interoperability Framework (e-GIF) provides an implementation strategy for the Ugandan Government to adopt in its effort to digitalize the entire public sector. It supports achieving goals of the Nation Vision 2040, Digital Uganda Vision, and other GoU ICT priorities.

The main objective of the Government of Uganda through National Information Technology Authority – Uganda (NITA-U) is to transform the delivery of public services by creating an environment which will help government information systems to inter-operate and share information in an integrated and seamless manner, regardless of the underlying technology or application in use, or regardless of which vendor the system or technology has been procured from.

The e-GIF sets out the government's technical polices and specifications for achieving interoperability and IT systems coherence across government. The e-GIF defines essential prerequisites and guidelines for integrating government systems to offer online services to citizens and businesses and to share data across the government.

Adherence to the e-GIF standards and guidelines is mandatory. The focus of government organisations should be to take advantage of the opportunities provided by increased interoperability to implement information systems that are citizen-centric and service- based to meet the growing demands of a whole-of government approach for citizens and businesses.

The GoU Interoperability Framework gives guidance, through a set of recommendations, to MDA/LGs on how to improve governance of their interoperability activities, establish cross-

[2] http://www.npa.go.ug/uganda-vision-2040/

[3] https://ict.go.ug/initiatives/digital-uganda-vision/

organisational relationships, streamline processes supporting digital services, and ensure that existing and new legislation do not compromise interoperability efforts.

This document serves as the second version of the national e-GIF and will work as the reference for government organisations. The e-GIF uses the terminology and structure of the EIF, the content is adjusted to the GoU national policies, strategies, and guidelines.

2.1. Context of e-GIF

GoU e-GIF is an important part of activities for building the e-Government Enterprise Architecture (GEA). By GEA we mean the structure of e-Government components, their inter-relationships, and the principles and guidelines governing their design and evolution over time. We distinguish the following steps/levels in the GEA lifecycle:

- **Strategy of building an information society**. The strategy will be fixed in vision papers of the Government, and in legislation
- **e-GIF**. The e-GIF provides an implementation strategy for the GEA. It defines basic interoperability guidelines in the form of common principles, models, and recommendations for interacting between public institutions.
- **e-Government Interoperability Reference Architecture (GIRA**). The GIRA is a reference architecture focused on the interoperability of digital public services. It is composed of the most salient Architecture Building Blocks needed to promote interactions between MDA/LGs.
- **Implementation of GEA.** This phase gives an implementation plan and road map highlighting the required activities, resources and timelines as well as cross-government governance structures to ensure compliance and uptake of the developed GIRA.
- **Governance of GEA.** Building, monitoring, managing, and steering of the implemented GEA. Building the GEA is an iterative process. Some components need to be renewed; some components need to be added sometimes. Sometimes it is reasonable to start a new lifecycle from the beginning.

2.2. Definitions

2.2.1. Interoperability

Interoperability is the ability of making systems and organisations operate together (inter-operate). In the following document the term "interoperability" is used in a broad way. It considers not only technical but also social, political, and organisational factors. We are

following the definition of the European Commission[4], which has been accepted in governmental context internationally:

"Interoperability is the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their ICT systems."

2.2.2. Public Service

In this document, we follow the service-oriented principle. It means all the activities of any organisation are services. Service can be:

- A repeatable activity: a discrete behaviour that a component of organisation may be requested or otherwise triggered to perform.
- An element of behaviour that provides specific functionality in response to requests from actors or other services.

A **GoU public service** comprises any public sector service supplied by MDA/LGs, either to one another or to businesses or citizens of Uganda.

2.2.3. GoU Interoperability Framework

The **GoU Interoperability Framework (e-GIF**) is the agreed approach to the delivery of GoU public services in an interoperable manner. It defines basic interoperability guidelines in the form of common principles, models, and recommendations.

2.3. The e-GIF Purpose

Interoperability is both a prerequisite for and a facilitator of the efficient delivery of public services. The interoperability framework aims to improve:

- **cooperation** between MDA/LGs aiming at the establishment of public services
- **exchanging information** between MDA/LGs to fulfil legal requirements or political commitments
- **sharing and reusing information** among MDA/LGs to increase administrative efficiency and reduce administrative burden on citizens and businesses

The e-GIF is oriented to:

- **improving** public service delivery to citizens and businesses by facilitating the one-stop shop delivery of public services

---

[4] https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

- **reducing costs** for MDA/LGs, businesses, and citizens through efficient and effective delivery of public services.

The objective of the e-GIF in its current phase is to focus on the principles, mechanisms and components enabling user centric services – both for civil servants, businesses, and citizens. Information systems must be designed to logically interoperate.

The e-GIF is a set of agreements and guidelines aimed at ensuring the provision of services for institutions, enterprises, and citizens. The GoU interoperability framework serves as:

- a guidance for elaborating concepts for countrywide information systems – interoperability enablers
- a guidance for IT project managers in the MDA/LG for elaborating concepts for the information systems of their institutions
- a list of requirements for public procurements.

The specific objectives of the GoU interoperability framework are the following:

- to facilitate the transformation of institution-based MDA/LG into a service-centred one, where all citizens can communicate with the state without needing to know its hierarchical structure and division of roles of government institutions
- to reduce public sector IT expenses through a wide use of common rules and solutions
- to improve the interoperability of new IT projects through coordinated use of centrally developed common infrastructure services and open standards
- to improve the coordination and management of state information systems and to accelerate the development of IT solutions
- to contribute to the co-development of the state information systems
- to allow autonomous development for all systems within the principles of organisational, semantic, and technical interoperability
- to endorse free competition among various vendors while procuring.

The report contains:

- the list of underlying principles
- the principles for achieving interoperability on legal, organisational, semantic, and technical levels
- the Public Service conceptual model

The primary target group of the interoperability framework is officials in public sector with following roles:

- Permanent Secretaries
- Agency Accounting Officers
- Chief executive officers (CEO),

- Heads of Finance,
- Chief Information Security Officers (CISO),
- Chief Information Officers (CIO),
- Head of IT.

eGIF is also a guideline for private sector managers and project leaders who offer development and administrative services to the public sector.

The National Information Technology Authority Uganda (NITA-U), responsible for planning and development of the state information system, is also in charge of designing the Interoperability framework and the related documents.

Public and private sector working groups covering sub-topics of the interoperability framework will be formed to advise the coordination body in the process of developing interoperability guidelines.

2.4. Scope and Structure of the e-GIF

The e-GIF is applicable to all MDA/LGs in Uganda. It lays out the basic conditions for achieving interoperability at all levels of the administration. This document is addressed to all those involved in defining, designing, developing, and delivering public services in Uganda.

The e-GIF may be used for building domain-specific interoperability frameworks in Uganda. These frameworks should remain compatible with the e-GIF, and where necessary, extend the scope of the e-GIF to capture the specific interoperability requirements of the domain in question.

The e-GIF is oriented to the development of a GoU public services ecosystem in which owners and designers of systems and public services become aware of interoperability requirements, MDA/LGs are ready to collaborate with each other and with businesses and citizens, and information flows seamlessly across Uganda.

The e-GIF's scope covers three types of interactions:

- A2A (MDA/LG to MDA/LG), which refers to interactions between MDA/LGs.
- A2B (MDA/LG to business), which refers to interactions between MDA/LGs and businesses.
- A2C (MDA/LG to citizen), which refers to interactions between MDA/LGs and citizens.

The e-GIF content and structure is presented below:

- Chapter 3 presents a set of 12 **principles** intended to establish general behaviours on interoperability. The Chapter gives 29 requirements/recommendations for MDA/LGs.
- Chapter 4 presents a layered **interoperability model,** which organises in layers the different interoperability aspects to be addressed when designing public services. The Chapter gives 27 requirements/recommendations for MDA/LGs.

- Chapter 5 outlines a **conceptual model** for interoperable public services. The model is aligned with the interoperability principles and promotes the idea of 'interoperability by design' as a standard approach for the design and operation of public services. The Chapter gives 15 requirements/recommendations for MDA/LGs.
- Chapter 6 stipulates the rules of **e-GIF governance**. The e-GIF handles information systems from the point of view of the state as a whole. The maintenance of the e-GIF document will be handled through the Inter-Agency Digital Technical Implementation Committee and the e-Government working groups with the leadership of the Secretariat at the Ministry of ICT and National Guidance. Chapter gives 5 requirements/recommendations for e-GIF governance.
- Chapter 7: Abbreviations
- Chapter 8: Glossary

The requirements and recommendations are numbered within a every chapter throughout and highlighted with green boxes.

The most important conclusions and requirements have been provided in text boxes. They are numbered within a chapter throughout.

The key words of this document "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" should be interpreted as specified by the Internet Engineering Task Force (IETF)[5]. To highlight the relevance of these words, they have been provided in block capitals and their meaning is as follows:

Meaning	Words expressing the meaning
Required/obligatory. Absolute requirement	*MUST, REQUIRED, SHALL*
Recommendation. There may exist valid reasons circumstances to ignore an item, but the full implications must be understood and carefully weighed before choosing a different course.	*SHOULD, RECOMMENDED*
Acceptable/allowed.	*MAY, OPTIONAL*
Not recommended. Acceptable only under reasons or circumstances.	*SHOULD NOT, NOT RECOMMENDED*
Prohibited. Absolute prohibition.	*MUST NOT, SHALL* NOT

[5] Internet Engineering Task Force (IETF) RFC 2119: „Key words for use in RFCs to indicate requirements levels ": https://tools.ietf.org/html/rfc2119

3.Underlying Principles

This chapter sets out the general principles of good administration that are relevant to the process of establishing public services. The interoperability principles are fundamental behavioural aspects to drive interoperability actions. This chapter sets out the general interoperability principles, which are relevant to the process of establishing GoU information systems and services.

The twelve underlying principles of the e-GIF are grouped into four categories:

- Principles setting the context for GoU actions on interoperability (principle 1).
- Core interoperability principles (principles 2 to 5).
- Principles related to generic user needs and expectations (principles 6 to 9).
- Foundation principles for cooperation among MDA/LGs (principles 10 to 12).

The e-GIF is based on the following principles:

1. Subsidiarity and proportionality
2. Openness
3. Transparency
4. Reusability
5. Technological neutrality and data portability
6. User-centricity
7. Inclusion and accessibility
8. Security
9. Privacy
10. Administrative simplification
11. Preservation of information
12. Assessment of effectiveness and efficiency

3.1. Principle 1: Subsidiarity and Proportionality

Subsidiarity. The subsidiarity principle implies that GoU ICT policy decisions are taken as closely as possible to the public institutions, entrepreneurs, and citizens. In other words, the central government does not act unless central action is more effective than action taken at local level. Application of subsidiarity principles means that centralised solutions are used as little as possible.

Proportionality. MDA/LG-s do not force central solutions in their areas of government, which would mean that an institution may lose control of business processes. Neither does the central government prescribe technical solutions for local governments. At the same time, the subsidiarity principle does not restrict public sector institutions' cooperation in working out joint standard solutions.

3.1. Information systems SHOULD support the existing organisational structures and their objectives.

3.2. MDA/LGs MUST align their frameworks and strategies with the e-GIF.

3.3. GoU information technology related political decisions SHOULD be enforced only if they are more efficient than the ones made in public sector institutions.

We distinguish between three types of activities: centralised, use of standard solutions, and decentralised.

Centralised. GoU has decided to centralise:

- Coordination activities (ICT policy and legislation, standardisation, interoperability framework, security framework, reference architecture)
- eID and PKI ecosystem
- Secure data exchange: data between institutions are exchanged through a central solution
- Catalogue of interoperable resources (institutions, systems, public services, data services, assets)
- Citizen portal
- Secure and centralised government authentication gateway for services requiring user authentication and authorisation
- Centralised payment system
- Open data portal
- Common semantic assets and classifications

Standard solutions. A solution which can be used by several authorities or persons for performing the tasks in their domain. In Uganda standard solutions can be used for example for:

- Document management systems
- Public Financial Management & Accounting
- Human resources systems
- Systems for implementation functions of municipalities
- E-mail and notification services
- Collaboration services

Decentralised solutions. Where possible, the decentralised approach SHOULD implemented.

3.2. Principle 2: Openness

The concept of openness mainly relates to data, specifications, and software. Open government data refers to the idea that all public data should be freely available for use and reuse by others, unless restrictions apply e.g. for protection of personal data, confidentiality, or intellectual property rights.

An administrative body of Uganda SHALL be obliged to ensure that public information is proactively published on its own (appropriate) electronic resource. Proactively published public information shall be open and equally available for any person. It is inadmissible to charge a fee or to introduce any other restriction on accessing the proactively published public information, except as provided for by law. In addition, legal reforms MAY be considered to limit legal restrictions to access to information as much as possible.

3.4. The MDA/LGs MUST publish the data they own as open data unless certain restrictions apply.

The use of open-source software technologies and products can help save development cost, avoid a lock-in effect, and allow fast adaptation to specific business needs because the developer communities that support them are constantly adapting them. MDA/LGs SHOULD not only use open-source software, but also whenever possible contribute to the pertinent developer communities. Open source is an enabler of the underlying principle on reusability.

3.5. The MDA/LGs SHOULD ensure a level playing field for open source software and demonstrate active and fair consideration of using open source software, considering the total cost of ownership of the solution.

The **level of openness of a specification/standard** is decisive for the reuse of software components implementing that specification. If the **openness** principle applies in full:

- all stakeholders could contribute to the development of the specification and a public review is part of the decision-making process
- the specification is available for everyone to study
- intellectual property rights to the specification are licensed on FRAND[6] terms, in a way that allows implementation in both proprietary and open-source software,[7] and preferably on a royalty-free basis.

The positive effect of open specifications is demonstrated by the internet ecosystem. However, MDA/LGs MAY decide to use fewer open specifications if open ones do not exist or do not meet functional needs. In all cases, specifications MUST be mature and sufficiently supported by the market, unless they are being used to create innovative solutions.

---

[6] FRAND: fair, reasonable, and non-discriminatory.

[7] This fosters competition since providers working under various business models may compete to deliver products, technologies and services based on such specifications.

3.6. The MDA/LGs MUST give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.

3.3. Principle 3: Transparency

Transparency in the e-GIF context refers to:

- Enabling **visibility** inside the administrative environment of a MDA/LG. This is about allowing other MDA/LGs, citizens, and businesses to view and understand administrative rules, processes, data, services, and decision-making.
- Ensuring **availability of interfaces** with internal information systems. MDA/LGs operate many often heterogeneous and disparate information systems in support of their internal processes. Interoperability depends on ensuring the availability of interfaces to these systems and the data they handle. In turn, interoperability facilitates reuse of systems and data, and enables these to be integrated into larger systems.
- Securing the right to the **protection of personal data**, by respecting the applicable legal framework for the large volumes of personal data of citizens, held and managed by MDA/LGs.

3.7. The MDA/LGs SHOULD ensure internal visibility and provide external interfaces for GoU public services.

3.4. Principle 4: Reusability

Reuse means that MDA/LGs confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevance to the problem at hand, and where appropriate, adopting solutions that have proven their value elsewhere. This requires the MDA/LG to be open to sharing its interoperability solutions, concepts, frameworks, specifications, tools, and components with others.

Reusability of IT solutions (e.g. software components, Application Programming Interfaces, standards), information and data, is an enabler of interoperability and improves quality because it extends operational use, as well as saving money and time. These existing standards and specifications CAN and SHOULD be used more widely beyond the domain for which they were originally developed.

3.8. MDA/LGs SHOULD reuse and share solutions and cooperate in the development of joint solutions.

3.9. MDA/LGs MUST reuse and share information and data unless certain privacy or confidentiality restrictions apply.

3.5. Principle 5: Technological Neutrality and Data Portability

When establishing information systems and services, MDA/LGs SHOULD focus on functional needs and defer decisions on technology as long as possible in order to avoid imposing specific technologies or products on their partners and in order to be able to adapt to the rapidly evolving technological environment. MDA/LGs should render access to public services independent of any specific technology or product. Legislation MUST NOT prescribe specific technologies.

3.10. MDA/LGs SHALL NOT impose any specific disproportionate technological solutions for citizens, businesses and other MDA/LGs when establishing information systems and services.

3.11. When developing functionality of information systems, technological decisions MUST be made as late as possible.

The principle requires that data can be easily transferred amongst different systems to avoid lock-in, support the free flow of data and ensure a level playing field. Data portability is the ability to move and reuse data easily among different applications and systems.

3.12. MDA/LGs MUST ensure that data is easily transferable between systems and applications.

3.13. Information systems interfaces MUST be API-centric and created in a technology neutral way, using open standards and specifications (XML, WSDL, SOAP, REST etc). Technical Interoperability Agreement MUST be set up where acceptable formats are specified.

3.6. Principle 6: User-Centricity

Users of GoU public services are meant to be any MDA/LG, citizen or business accessing and benefiting from the use of these services. User needs SHOULD be considered when determining which public services should be provided and how they should be delivered.

Therefore, as far as possible, user needs and requirements SHOULD guide the design and development of public services, in accordance with the following expectations:

- A **multi-channel** service delivery approach, meaning the availability of alternative channels, physical and digital, to access a service, is an important part of public service design, as users may prefer different channels depending on the circumstances and their needs.
- A **single point** of contact SHOULD be made available to users, to hide internal administrative complexity and facilitate access to public services, e.g. when multiple bodies must work together to provide a public service.
- **Users' feedback** SHOULD be systematically collected, assessed and used to design new public services and to further improve existing ones. Feedback tools should be easy to identify and utilise. User feedback should be regarded as a priority for continuous service quality improvement.

- As far as possible, under the legislation in force, users should be able to provide data **once only**, and MDA/LGs SHOULD be able to retrieve and share this data to serve the user, in accordance with data protection rules.
- Users SHOULD be asked to provide only the **information that is necessary** to obtain a given public service.

3.14. A user SHOULD be able to choose an agreeable type of a service channel: service bureau, post, telephone, e-mail, and other Internet channels.

3.15. A person identified with an electronic ID or with other secure means MUST be able to apply for any electronic public service.

3.16. Citizen portal MUST acts as single contact point for public services. It is RECOMMENDED that multiple MDA/LGs work together to provide aggregated services via the citizen portal. MDA/LGs can create their own portals at the edge but consume services of integration platform.

3.17. Users' feedback SHOULD be systematically collected, assessed, and used as the basis for further service improvement. Mechanisms to involve users in analysis, design, assessment, and further development of GoU public services SHOULD be put in place.

3.18. Data MUST be provided by users only once, and MDA/LGs SHOULD be able to retrieve and share this data considering data protection rules and legislation.

3.19. Institution based approach MUST be replaced with a user-based approach. Institutions MUST provide information at their own initiative.

3.7. Principle 7: Inclusion and Accessibility

Inclusion is about enabling everyone to take full advantage of the opportunities offered by new technologies to access and make use of public services, overcoming social and economic divides and exclusion.

Accessibility ensures that people with disabilities, the elderly and other disadvantaged groups can use public services at service levels comparable to those provided to other citizens.

Inclusion and accessibility MUST be a part of the whole development lifecycle of a GoU public service in terms of design, information content and delivery. It should comply with e-accessibility specifications widely recognised at the international level.

Inclusion and accessibility usually involve multi-channel delivery. Traditional paper-based or face-to-face service delivery may need to co-exist with electronic delivery.

Inclusion and accessibility can also be improved by an information system's ability to allow third parties to act on behalf of citizens who are unable, either permanently or temporarily, to make direct use of public services.

3.20. MDA/LGs SHALL ensure that all public sector websites and public services are accessible to all citizens, including persons with disabilities and special needs.

2.21. The interfaces of GoU public sector information systems, websites, and services SHALL comply at least with WCAG (Web Content Accessibility Guidelines) quality criteria - level AA.

3.22. Public sector institutions MUST provide information in open formats. Citizens do not have to make extra expenses to use information (for example, obtain own software).

3.8. Principle 8: Security

Citizens and businesses must be confident that when they interact with public authorities they are doing so in a secure and trustworthy environment and in full compliance with relevant regulations.[8] MDA/LGs must guarantee the citizens' privacy, and the confidentiality, authenticity, integrity and non-repudiation of information provided by citizens and businesses.

User data should be stored securely, acquisition of usernames and passwords should be done securely, data provided should be used for only the reasons submitted. Confidentiality of personal data must be maintained.

Security and privacy are primary concerns in the provision of public services. When MDA/LGs and other entities exchange official information, the information should be transferred, depending on security requirements, via a secure, harmonised, managed and controlled network. Transfer mechanisms should facilitate information exchanges between MDA/LGs, businesses and citizens. Appropriate mechanisms should allow secure exchange of electronically verified messages, records, forms and other kinds of information between the different systems; should handle specific security requirements and electronic identification and trust services such as electronic signatures/seals creation and verification; and should monitor traffic to detect intrusions, changes of data and other type of attacks.

Security and privacy are discussed in more detail in section 5.9.

3.23. GoU SHOULD define a common security framework, adopt data protection legislation, and establish processes for public services to ensure secure and trustworthy data exchange between MDA/LGs and in interactions with citizens and businesses.

3.24. GoU information systems MUST guarantee confidentiality, integrity, authenticity, availability and provability of data and services.

[8] The Data Protection and Privacy Act

3.9. Principle 9: Privacy

Privacy refers to any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Citizens and businesses MUST be confident that when they interact with public authorities they are doing so in a secure and trustworthy environment and in full compliance with relevant regulations. MDA/LGs MUST guarantee the citizens' privacy, and the availability, confidentiality, authenticity, integrity and non-repudiation of information provided by citizens and businesses.

3.25. Citizens SHOULD be supplied by services through which they can check and, if necessary, correct the data collected about them by the public sector.

3.26. Citizens SHOULD be supplied by services through which they find out who, and for what purposes, has used the data collected about them in the public sector.

3.10. Principle 10: Administrative Simplification

Where possible, MDA/LGs SHOULD seek to streamline and simplify their administrative processes by improving them or eliminating any that do not provide public value. Administrative simplification can help businesses and citizens to reduce the administrative burden of complying with legislation or obligations. Likewise, MDA/LGs should introduce services supported by electronic means, including their interactions with other MDA/LGs, citizens and businesses.

Digitisation of public services should take place in accordance with the following concepts:

- **digital-by-default**, whenever appropriate, so that there is at least one digital channel available for accessing and using a given GoU public service
- **digital-first,** which means that priority is given to using public services via digital channels while applying the multi-channel delivery concept and the no-wrong-door policy, i.e. physical and digital channels co-exist.

3.27. MDA/LGs MUST simplify processes and use digital channels whenever appropriate for the delivery of public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on MDA/LGs, businesses and citizens.

3.11. Principle 11: Preservation of Information

Legislation should require that decisions and data are stored and can be accessed for a specified time[9]. This means that records and information in electronic form held by MDA/LGs for the purpose of documenting procedures and decisions must be preserved and be converted, where necessary, to new media when old media become obsolete. The goal is to ensure that records and other forms of information keep their legibility, reliability and integrity and can be accessed as long as needed, subject to legal, security and privacy provisions.

To guarantee the long-term preservation of electronic records and other kinds of information, formats should be chosen to ensure long-term accessibility, including preservation of associated electronic signatures or seals. In this regard, the use of qualified preservation services can ensure the long-term preservation of information.

3.28. Uganda MUST formulate a long-term preservation policy for information in electronic form.

3.12. Principle 12: Assessment of Effectiveness and Efficiency

MDA/LG should ensure that solutions serve businesses and citizens in the most effective and efficient way and provide the best value for taxpayer (including donor funds/grants) money. There are many ways to take stock of the value of interoperable services, including considerations such as minimum:

- return on investment,
- total cost of ownership,
- level of flexibility and adaptability,
- reduced administrative burden,
- efficiency,
- reduced risk,
- transparency,
- simplification,
- improved working methods,
- and level of user satisfaction.

Various technological solutions SHOULD be evaluated when striving to ensure the effectiveness and efficiency of a GoU public service.

3.29. MDA/LGs MUST evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits.

---

[9] National Records and Archives Act,2001. http://library.health.go.ug/publications/local-government/national-records-and-archives-act2001

4. Interoperability Layers

This chapter describes an **interoperability model** which is applicable to all digital public services and may also be considered as an integral element of the **interoperability-by-design** paradigm. It includes:

- **four layers** of interoperability: legal, organisational, semantic, and technical.
- a cross-cutting component of the four layers, '**integrated public service governance**'.
- a background layer, '**interoperability governance**'.

This model follows the terminology of the EIF. TOGAF and EIF methodology is adjusted to the needs of Uganda. The model is depicted below:

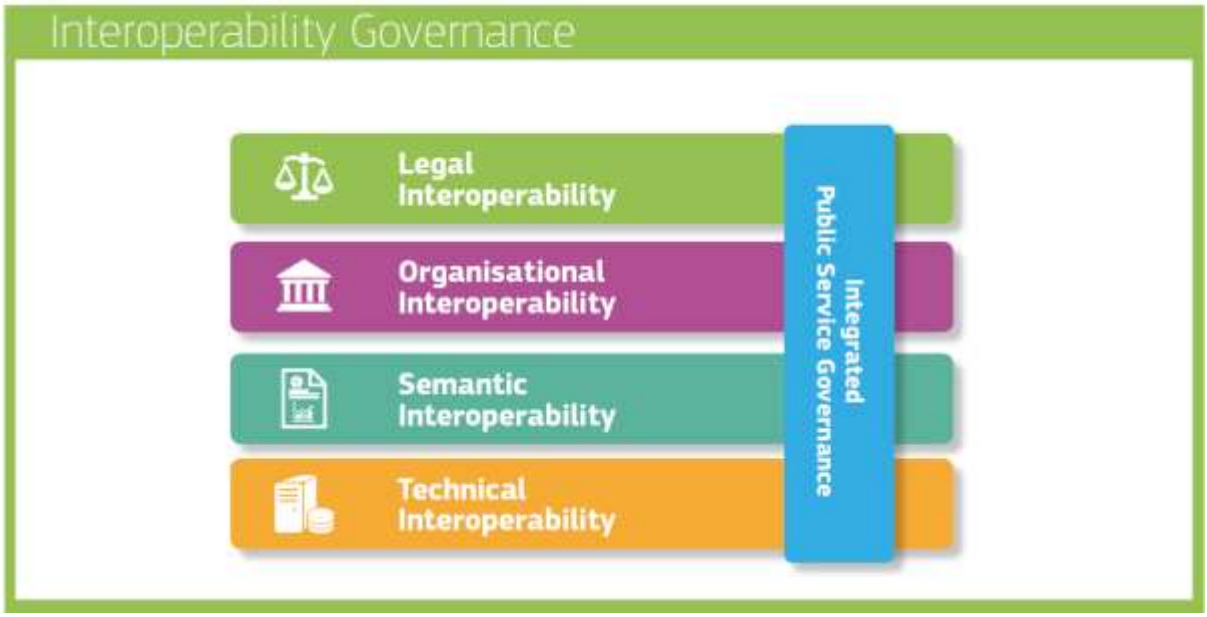

Figure 1. Interoperability model (picture is taken from the EIF)

4.1. Interoperability Governance

4.1.1. Barriers of Interoperability Governance

Interoperability governance refers to decisions on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements, and other aspects of ensuring and monitoring interoperability at government level.

GoU information systems and services operate in a **complex and changing environment**. Political support is necessary for cross-sectoral efforts to facilitate cooperation between MDA/LGs. Interoperability between MDA/LGs at different administrative levels will only be successful if MDA/LGs give enough priority and assign resources to their respective interoperability efforts.

As information systems are constantly changing, it is necessary continuously improve the skills IT personal. The possible **lack of necessary in-house skill sets** is another barrier when implementing interoperability policies. Uganda SHOULD include interoperability skills in their interoperability strategies, acknowledging that interoperability is a multi-dimensional issue that needs awareness and skills in legal, organisational, semantic, and technical areas.

The implementation of information systems and services often relies on components that are common to many GoU information system owners. The sustainability of these components SHOULD be guaranteed over time. **Interoperability should be guaranteed in a sustainable way** and not as a one-off target or project. As common components and interoperability agreements are the results of work done by MDA/LGs at different levels (local, regional, national), coordination and monitoring require a holistic approach.

Interoperability governance is the key to a **holistic approach** on interoperability, as it brings together all the instruments needed to apply it.

4.1. The coordination body SHALL ensure holistic governance of interoperability activities across administrative levels and sectors.

4.1.2. Governance on the Interagency Level

The President, Cabinet of Ministers are responsible for providing political leadership in support of all ICT related policy interventions. This is important in driving cross-sectoral implementation of the e-GIF. Cabinet can secure the support for changes at the highest possible level with strategic decisions and monitor the implementation progress.

The Parliament is responsible for enacting appropriate and effective legislations that create a conducive legal and regulatory environment for the success of the e-GIF. In addition, Parliament has a role of guiding the financial resource allocation for implementation of the e-GIF. The Parliament is also the place where info-political concepts and decisions are discussed and passed. This is not about technology but about important conceptual decisions of the society – privacy and protection of personal data, avoiding digital divide, public-private cooperation and engagement of the academia, civil society, and NGO-s etc.

The Policy Coordination Committee (PCC) chaired by the Prime Minister is responsible for coordinating policy and monitoring progress of the implementation of the Digital Uganda Vision (DUV). Usually, the role of the committee is also to discuss strategic issues of eGovernment - strategies, action planning, regulations, and budgeting. Also, recommendations on priorities and responsibilities of different government institutions are made by the Coordination Committee. Other important stakeholders (below) should be included to the work of the PCC. It is most important to engage all stakeholders into the strategic decision-making process. The PCC is legally a government committee advised by the Prime Minister and the Ministry of Information and Communication Technology and National Guidance in their decision-making process.

The Inter-Ministerial Steering Committee (IMSC) shall be responsible for the Strategic Direction and Oversight of the DUV including ensuring effective implementation of decisions made by the Cabinet and the PCC.

The Inter-Agency Digital Technical Implementation Committee shall be responsible for promoting cross-cutting priorities and policies on a program-based approach. It advises on issues for central coordination of programs; promotes intra-sectoral and program linkages. It will also address any identified challenges and (or) constraints requiring higher levels of action and attention. This Committee shall also have representation from the private sector and development partners who will articulate issues arising from their different forums.

The Ministry of Information and Communications Technology and National Guidance (MoICT&NG) shall provide supervisory oversight and policy guidance to MDA/LGs, Local Governments, and other stakeholders in the implementation of the DUV. Ministry is responsible for the formation of information society in Uganda. In addition, the Ministry is responsible for supervising its agencies on the implementation and reporting on progress to Cabinet for all ICT interventions including the e-GIF.

The National Information Technology Authority (NITA-U) is an autonomous statutory body to coordinate, implement and regulate Information Technology services in Uganda. NITA-U is responsible for technical operational support, standards as well as building and maintaining the e-Government enablers, like the PKI ecosystem, Secure Data Exchange ecosystem, citizen portal, metadata management and other cross- government systems and services.

4.3. The National Information Technology Authority (NITA-U) acts as central implementation unit and is responsible for interoperability enablers.

Ministries, departments, other agencies and public institutions (MDA/LG) are responsible for their own business processes. They may choose to implement technologies by themselves, with respect to commonly agreed principles.

The principles of information policy and supportive legislation will be developed by the policy and coordination actor, by engaging stakeholders. The key investments and other large-scale financing decisions should also be coordinated on the Cabinet level.

4.4. It is RECOMMENDED to centralise development of the policies and decentralise the implementation.

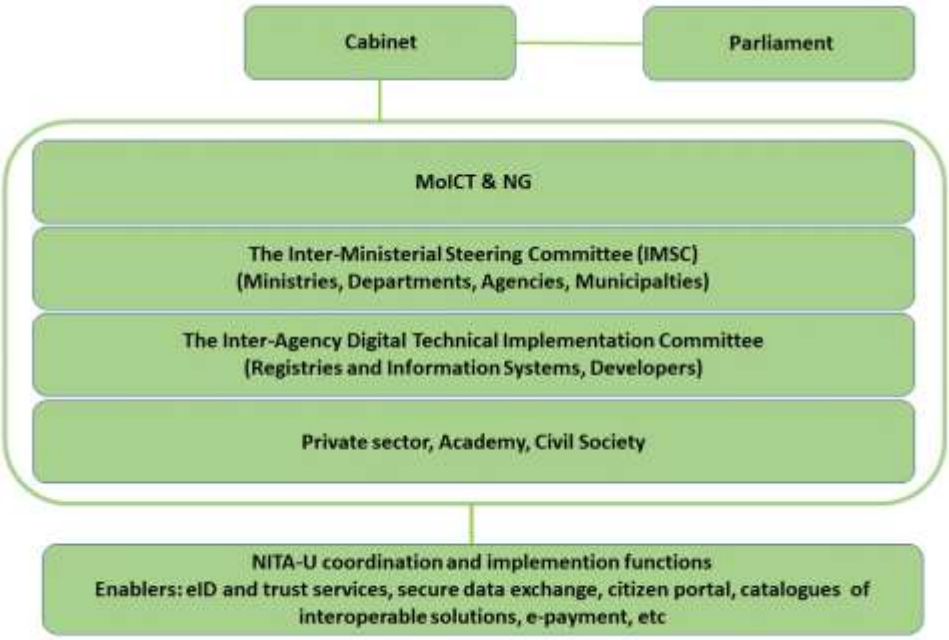

Figure 2. Institutional Framework. NITA-U supports preparing and implementation of strategical and political decisions. MDA/LGs, registries and information systems, developers, private sector, Academy, etc are involved.

Other important stakeholders:

- Universities and other research and development institutions
- ICT industry associations
- Software and hardware companies
- Banks and telecom companies
- Digital identity and trust services providers
- Open data communities
- Open source software communities
- Civil Society organizations

Other community organisations

- International activities, stakeholders, donors, partners
- Smart Africa
- World Bank
- UNDP

Typical strategy level tasks, usually regulated by the Government are:

- Collecting and analysing data about ICT systems in the government
- e-Government budget planning with the Ministry of Finance and donors

- Developing and approving legal acts related to e-Government
- Preparing e-Government strategies and action plans
- Monitoring Action Plan development
- Cooperation with CIOs, training courses for CIOs
- Planning and coordinating international cooperation on e-Government

The usual central implementation level tasks focusing on the implementation of an e-government interoperability platform are:

- Data exchange layer and monitoring
- Portal
- Interoperability platform management system - metadata
- Infrastructure
- Network
- eID
- Certificaion Authority
- Mobile and payment gateway
- Cloud

4.1.3. Financing

For a e-government development and operation, sustainable financing must be secured. The financing Ugandan e-Government will be mainly by the government. The financing will be provided through five annual budgeting. Development of e-government is partially dependent on international donor funding. The main donor organisations supporting digital transformation in Uganda include UNDP, World Bank and USAID. The Ministry of Finance, Planning and Economic Development (MOFPED) is coordinating activities with donor.

Private sector, development partners and civil society organisations shall be engaged to contribute towards the financing of e-Government components.

E-government financing can be broadly described as follows:

- Government (or donors) cover from their investment budget development of cross government IT systems (hardware, software).
- Operational costs (maintenance, support, further developments, etc.) are covered from the MDA/LG budgets.

The Government of Uganda charges Non-Tax Revenue (NTR) fees for government services and business. For example, there are state fees to Motor-Vehicle Registration, transfer; business registration; land search; land transfer, certification services etc.

4.1.4. Standards and specifications

The government adopts and draw up standards and specifications for government data and technology processes. The seven principles[10] that will be used for adopting and drawing standards by the Uganda government:

- **Standards must meet user needs** - Government IT specifications are based on user needs, expressed in terms of capabilities with associated open standards for software interoperability, data, and document format. Security, risk and privacy aspect MUST be considered.
- **Standards must give suppliers equal access to government contracts** - Standards can be implemented by a diverse range of suppliers. In selecting open standards for government IT specifications, the government removes barriers to competition, such as lock-in.
- **Standards should support flexibility and change** - The government's IT and data and the standards upon which they are built, are enablers for change, giving services the freedom to evolve according to changing user needs, expectations, and technology innovation.
- **Standards must support sustainable cost** - Decisions are based on the most economical solution for the public sector as a whole and costs are sustainable.
- **Decisions on standards selection are well informed** - Effective selection of standards for government IT specifications is a result of pragmatic and informed decision making, taking the consequences for citizens, users, and government finances into account.
- **Select standards using fair and transparent processes** - The selection and adoption process for open standards and open standards-based profiles in government IT is transparent, allowing engagement with the public and subject matter experts.
- **Specify and implement standards using fair and transparent processes**- Government IT procurement, specifications, implementation plans and agreed exemptions from the open standards policy are open and transparent.

Public sector agrees in cooperation with other concerned parties, on the minimum set of public sector open standards, compliance with which is compulsory for the public sector. The choice and assessment of standards is public and balanced.

NITA-U is charged to:

- set, monitor and regulate standards for information technology planning, acquisition, implementation, delivery, support, organisation, sustenance, disposal, risk management, data protection, security and contingency planning;

[10] These principles are adopted from UK open standards policy: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

- regulate and enforce standards for information technology hardware and software equipment procurement in all government ministries, departments, agencies and parastatals; and
- protect and promote the interests of consumers or users of information technology services or solutions.

NITA-U Standards Catalogue contains a complete list of standards that have been developed in collaboration with the Uganda National Bureau of Standards (UNBS) through consensus by industry, consumers, government departments, research organisations, universities and private institutions. List of recommended standards will be published on the web by NITA-U and reviewed regularly.

4.5. MDA/LGs SHOULD implement open standard principles by using open source and proprietary software. The principles support equal access to government IT contracts and improve flexibility and ability when cooperating with other government organisations, citizens, and businesses.

4.6. MDA/LGs SHOULD follow an agreed minimum set of open standards. The choice and assessment of the standards is public and balanced. The list of standards will be reviewed once a year.

4.2. Integrated Public Service Governance

GoU service provision often requires different MDA/LGs to work together to meet end users' needs and provide **public services in an integrated way**. When multiple organisations are involved, there is a need for coordination and governance by the authorities (NITA-U) with a mandate for planning, implementing and operating GoU shared services. Services SHOULD be governed to ensure integration, seamless execution, reuse of services and data, and development of new services and **'building blocks**.[11]

4.2.1. Governance on the Administration Level

Focusing here on the governance part, this SHOULD cover all layers: legal, organisational, semantic, and technical. Ensuring interoperability when preparing legal instruments, organisation business processes, information exchange, services and components that support GoU public services is a continuous task, as interoperability is regularly disrupted by changes to the environment, i.e. in legislation, the needs of businesses or citizens, the organisational structure of MDA/LGs, the business processes, and by the emergence of new technologies. It requires, among other things, organisational structures and roles and responsibilities for the delivery and operation of public services, service level agreements, establishment, and management of interoperability agreements, change management procedures, and plans for business continuity and data quality.

Integrated public service governance on administration SHOULD include as a minimum:

- the definition of organisational structures, roles & responsibilities and the decision-making process for the stakeholders involved

[11] A 'building block' is a self-contained, interoperable, and replaceable unit encapsulating an internal structure.

- the imposition of requirements for:
    - aspects of interoperability including quality, scalability and availability of reusable building blocks including information sources (base registries, open data portals, etc.) and other interconnected services
    - external information/services, translated into clear service level agreements (including on interoperability)
- a change management plan, to define the procedures and processes needed to deal with and control changes
- a business continuity/disaster recovery plan to ensure that digital public services and their building blocks continue to work in a range of situations, e.g. cyberattacks or the failure of building blocks.

4.7. MDA/LGs SHOULD ensure interoperability and coordination over time when operating and delivering integrated public services by putting in place the necessary governance structure.

4.2.2. Interoperability Agreements

Organisations involved in the GoU public service provision should make **formal arrangements** for cooperation through **interoperability agreements**. Setting up and managing these agreements is part of public service governance.

Agreements should be detailed enough to achieve their aim, i.e. to provide GoU public services, while leaving each organisation the maximum feasible internal and national autonomy.

At semantic and technical levels, but also in some cases at organisational level, interoperability agreements usually include standards and specifications. At legal level, interoperability agreements are made specific and binding via GoU legislation or via bilateral and multilateral agreements.

Other types of agreements can complement interoperability agreements, addressing operational matters. For example, memoranda of understanding (MoUs), service level agreements (SLAs), support/escalation procedures and contact details, referring, if necessary, to underlying agreements at semantic and technical levels.

Since delivering a GoU public service is the result of collective work with parties that produce or consume parts of the service, it is critical to include appropriate change management processes in the interoperability agreements to ensure the accuracy, reliability, continuity and evolution of the service delivered to other MDA/LGs, businesses and citizens.

4.8. MDA/LGs SHOULD establish interoperability agreements at all layers, complemented by operational agreements and change management procedures.

4.3. Legal Interoperability

Each MDA/LG contributing to the provision of a GoU public service works within the national legal framework. Legal interoperability is about ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together. This MIGHT require that legislation does not block the establishment of GoU public services and that there are clear agreements about how to deal with differences in legislation, including the option of putting in place new legislation.

The first step towards addressing legal interoperability, is to perform 'interoperability checks' by screening existing legislation to identify interoperability barriers: sectoral or geographical restrictions. It SHOULD check the use and storage of data, different and vague data license models, over-restrictive obligations to use specific digital technologies or delivery modes to provide public services, contradictory requirements for the same or similar business processes, outdated security and data protection needs, etc.

Coherence between legislation, in view of ensuring interoperability, SHOULD be assessed before adoption and through evaluating their performance regularly once they are put into application.

4.9. Administration SHOULD ensure that legislation is screened by means of 'interoperability checks', to identify any barriers to interoperability.

Bearing in mind that GoU public services are clearly meant to be provided - amongst others - from digital channels, ICT must be considered as early as possible in the law-making process.

Proposed legislation should undergo a **'digital check'**:

- to ensure that it suits not only the physical but also the digital world (e.g. the Internet)
- to identify any barriers to digital exchange
- to identify and assess its ICT impact on stakeholders

This will facilitate interoperability between public services at lower levels (semantic and technical) as well, and increase the potential for reusing existing ICT solutions, so reducing cost and implementation time.

4.10. When drafting legislation to establish public service, seeking to make it consistent with relevant legislation, MDA/LGs MUST perform a 'digital check' and consider data protection requirements.

4.11. All IT related legislation MUST pass approval process in catalogue of information systems. Catalogue of information systems and approval authorities approvement rules SHALL be provided for in the relevant legislation.

Listed below are the core e-Government areas where new legislation needs to be created and existing legislation needs to be supplemented / improved:

- Interoperability
- Electronic identification and electronic signature
- Databases / registries

- Archiving
- Access to information
- Information and Communications Technology (ICT)
- Public procurement and Public-Private-Partnership (PPP)
- Intellectual property
- Incentives for use of e-services
- Security and privacy

MDA/LGs SHALL fulfil requirements existing e-Government related legal acts. Important acts (as of 2020) related to the interoperability:

- The Access to Information Act 2005
- Electronic Transactions Act 2011
- National Databank Regulations 2019
- E-Government Regulations 2015
- Electronic Transactions Regulations 2013
- National Payment Systems Act 2020
- The National Information Technology Authority-Uganda (NITA-U) Act 2009
- Electronic Signatures Act 2011
- Registration of Persons Act 2015
- Data Protection and Privacy Act 2019
- Communications Act 2013
- The Computer Misuse Act 2011

4.4. Organisational Interoperability

This refers to the way in which MDA/LGs align their business processes, responsibilities, and expectations to achieve commonly agreed and mutually beneficial goals. In practice, organisational interoperability means documenting and integrating or aligning business processes and relevant information exchanged. Organisational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user focused.

Business Process Alignment

In order for different administrative entities to be able to work together efficiently and effectively to provide public services, they may need to align or improve their existing business processes or define and establish new ones.

Aligning business processes implies documenting them in an agreed way and with commonly accepted modelling techniques, including the associated information exchanged, so that all MDA/LGs contributing to the delivery of public services can understand the overall (end-to-end) business process and their role in it.

4.12. MDA/LGs SHOULD document business processes using commonly accepted modelling techniques (like BPMN, UML, Archimate, Gantt charts, LEAN etc) and agree on how these processes SHOULD be aligned to deliver a GoU public service.

Organisational Relationships

Service orientation, upon which the conceptual model for public services is conceived, means that the relationship between service providers and service consumers must be clearly defined.

This involves finding instruments to formalise mutual assistance, joint actions, and interconnected business processes as part of service provision e.g. MoUs and SLAs between participating MDA/LGs.

4.13. MDA/LGs SHOULD clarify and formalize organisational relationships for establishing and operating public services.

4.5. Semantic Interoperability

Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'. In the E-GIF, semantic interoperability covers both semantic and syntactic aspects.

- The **semantic** aspect refers to the meaning of data elements and the relationship between them. It includes developing vocabularies and schemata to describe data exchanges and ensures that data elements are understood in the same way by all communicating parties.
- The **syntactic** aspect refers to describing the exact format of the information to be exchanged in terms of grammar and format.

A starting point for improving semantic interoperability is **to perceive data and information as a valuable public asset**.

4.14. MDA/LGs SHOULD perceive data and information as a public asset that SHOULD be appropriately generated, collected, managed, shared, protected, and preserved.

An information management strategy SHOULD be drafted and coordinated at the highest possible level (corporate or enterprise) to avoid fragmentation and set priorities.

4.15. An information management strategy SHOULD put in place at the highest possible level to avoid fragmentation and duplication. Management of metadata, master data and reference data SHOULD be prioritized.

Key prerequisites for achieving semantic interoperability are agreements on reference data, in the form of taxonomies, controlled vocabularies, thesauri, code lists and reusable data structures/models. Approaches like **data-driven-design**, coupled with **linked data** technologies, are innovative ways of substantially improving semantic interoperability.

The single identifier of objects. Information about some objects like persons, addresses, land properties are used in many services. For interoperability is important to use same identifiers for these objects in all information systems of Uganda.

4.16. All objects in government information systems MUST have a specified single identifier. All information systems MUST use the same identifier.

Classifications. In order to understand process and categorize data in information systems in a standardised way, data need to be classified and tagged. Government agencies cannot communicate and exchange data properly without using the same names/codes (e.g. codes of cities, countries, banks, currencies, goods declared for example for customs etc.) The use of classifications facilitates the standardisation of data, enables information exchange between information systems (data providers and data receivers), and allows the comparison and analysis of the published data. All classifications need to be published in the catalogue of semantic assets.

4.17. The same data in all information systems MUST be coded by using standard classification. All classifications MUST be published in the catalogue of semantic assets.

Uniform addresses. Every administrative unit, infrastructure object, building and certain part of those must have a uniform and unambiguous address.

4.18. All address objects MUST be described by a uniform and unambiguous set of data.

Data standards. According to the once only principle, data are collected by base registries only once. Base registries will establish syntax and semantic those data and describe it in the catalogue of information systems. Secondary registries and information systems are using the same syntax and semantics.

4.19. Data standards SHALL be established and maintenance by owners of base registries and SHALL be published in the catalogue of information systems. Other MDA/LGs SHALL be following these standards.

Robust, coherent, and universally applicable information standards and specifications are needed to enable meaningful information exchange among public organisations.

4.6. Technical Interoperability

Technical interoperability covers the applications and infrastructure linking systems and services. Aspects of technical interoperability include interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols.

A major obstacle to interoperability arises from legacy systems. Historically, applications and information systems were developed in a bottom-up fashion, trying to solve organisation, domain-specific and local problems. This resulted in fragmented ICT islands which are difficult to interoperate.

Due to the size of MDA/LG and the fragmentation of ICT solutions, the plethora of legacy systems creates an additional interoperability barrier in the technical layer.

Technical interoperability SHOULD be ensured, whenever possible, via the use of formal technical specifications.

4.20. MDA/LGs SHOULD use open specifications, where available, to ensure technical interoperability when establishing public services.

Once Only principle. The proposed model[12] ensures the principle that information is supplied to information consumers only once from the authentic source responsible for handling the information and there is no other information source for the same information. According to the "once-only" principle, public bodies SHOULD take action to share data with each other, respecting privacy, and data protection rules. This calls for a generic and scalable solution to interconnect different systems. Data is kept only in a database, where it serves as master data. Availability requirements MAY lead to the copying of data, but in this case, it must be considered that data MAY be outdated.

4.21. Technical solutions of MDA/LGs MUST support fulfilling the once only principle.

Society as a service-centred organisation. All the activities of officials, entrepreneurs, citizens and software/information system are viewed as services. End users see services from a joint service room. They are not interested in the organisation that provides the service, but in the service itself. Although the private and public sector act according to fairly different business rules, the users of their services are the same. Hence, it is practical that the private and public sector develop and manage the services jointly.

4.22. Technical solutions MUST support service-centred approach.

Separation of front-end and back-end systems. In public sector information systems, front-end and back-end systems SHOULD be architecturally clearly separated. All public sector registers and databases are considered to be "back-end systems". The task of the back-end systems is data management and provision of network services; they do not deal with authentication and authorisation. Hence, there is no need to build components of end user authentication and authorisation into back-end systems. Web services of back-end systems are made available for the end-user only through service intermediaries (front-end systems).

4.23. MDA/LGs SHOULD separate front-end and back-end systems.

Reuse of components and infrastructure services. A full component-based service model for MDA/LGs allows the establishment of public services by reusing, as much as possible, existing service components.

For helping building software solution NITA-U SHALL develop common usable infrastructure services. MDA/LGs SHALL use these instead developing own solutions.

4.24. MDA/LGs SHALL use common infrastructure services established and administrated by NITA-U.

[12] Model is described in chapter 5

Service oriented architecture. In the elaboration of the state IT architecture, principles of Service Oriented Architecture (SOA) SHALL be followed. In case of service-oriented architecture, different systems provide diverse information services through the so-called "service interfaces", which CAN be used by other information systems. Descriptions of these interfaces have to contain sufficient information for the identification and use of a service without the need for the service-using system to "know" anything about the internal architecture, platform etc. of the service-providing system. In case of SOA, the service publisher and the actual service provider do not necessarily have to be the same, while from the point of view of the service user, this does not make any difference. There are no restrictions as to technologies to be used for the application of SOA.

4.25. Service oriented architecture MUST be followed by MDA/LGs.

Linking business processes via aggregated services. Information systems communicate with each other via aggregated services. If, for the performance of a business process in one agency, data is needed from or workflow has to be carried out in another agency, aggregated services are made use of. Agencies SHOULD ensure that the data and services they offer could be used as aggregated services. Aggregate service or complex service is combined from reliable basic services (for example, results of one basic service are used as input for other). The user perceives a complex service as one service. In the case of aggregate services, special attention must be paid to security related risks that are linked with service using rights as well as to the danger of combining data.

4.26. MDA/LGs SHALL be able to aggregate data services.

Data centres. Government data centre is used to host computer systems and associated components, such as telecommunications and storage systems. Government data centre SHOULD use cloud technologies.

4.27. Critical solutions SHOULD be hosted in a centralised cloud data centre.

5. The Conceptual Model for Integrated Public Services Provision

5.1. Introduction

This chapter proposes a conceptual model for integrated public services. It is relevant to all governmental levels: local, government bodies, ministerial, national. The model exposes modular and comprises loosely coupled service components interconnected through shared infrastructure. The terminology and the main idea for the GoU model is taken over from the EIF and best practices of other countries. The model is adjusted to the needs of Uganda.

5.1. MDA/LGs SHOULD use the conceptual model for public services to design new services or reengineer existing ones and reuse, whenever possible, existing service and data components.

MDA/LGs need to identify, negotiate, and agree on a common approach to interconnecting service components. This will be done at different administrative levels according to organisational set-up. Access boundaries for services and information SHOULD be defined through interfaces and conditions of access.

There are well-known and widely used technical solutions, e.g. web services, to do this, but implementing them at a state level will require concerted efforts by MDA/LGs, including common or compatible models, standards, and agreements on common infrastructure.

5.2. GoU MUST decide on a common scheme for interconnecting loosely coupled service components and put in place and maintain the necessary infrastructure for establishing and maintaining public services at the state level.

5.2. Model overview

The conceptual model promotes the idea of **interoperability by design**. It means that for the GoU public services to be interoperable, they should be designed in accordance with the proposed model and with certain interoperability and reusability requirements in mind. The model promotes reusability as a driver for interoperability, recognising that the GoU public services should reuse information and services that already exist and may be available from various sources inside or beyond the organisational boundaries of MDA/LGs. Information and services should be retrievable and be made available in interoperable formats.

The basic components of the conceptual model are presented below.

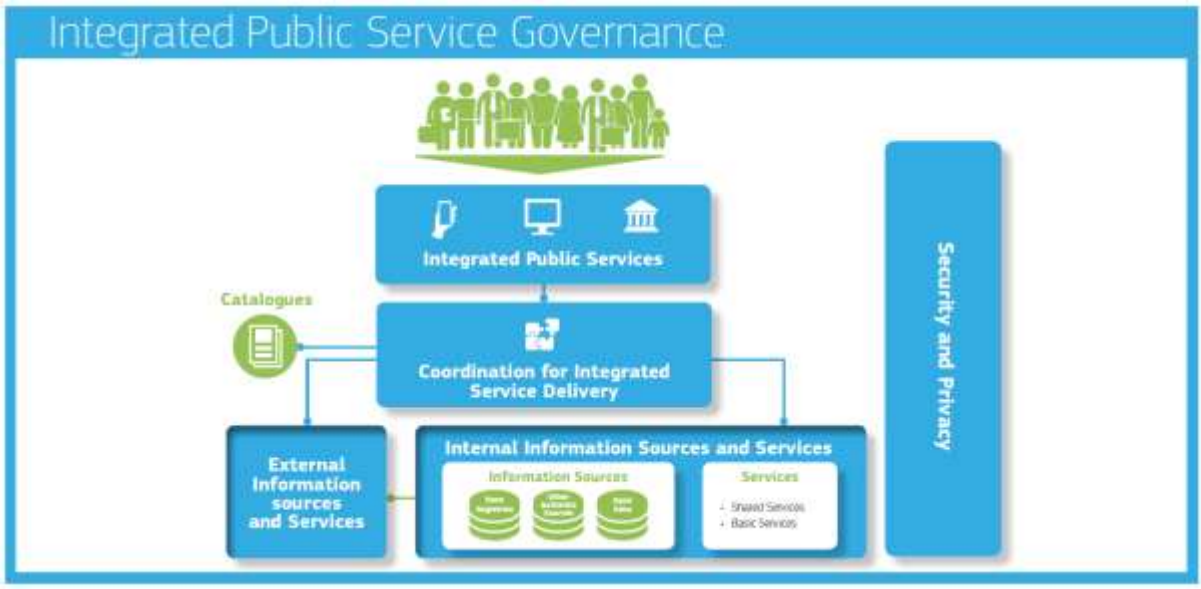

Figure 3. Conceptual model for integrated public services (taken from EIF)

The model's structure comprises:

- 'integrated service delivery' based on a 'coordination function' to remove complexity for the end-user.
- a 'no wrong door' service delivery policy, to provide alternative options and channels for service delivery, while securing the availability of digital channels (digital-by-default).
- reuse of data and services to decrease costs and increase service quality and interoperability.
- catalogues describing reusable services and other assets to increase their findability and usage.
- integrated public service governance.
- security and privacy.

5.3. Coordination function

The coordination function ensures that needs are identified, and appropriate services are invoked and orchestrated to provide a GoU public service. This function should select the appropriate sources and services and integrate them. Coordination can be automated or manual.

Process phases of integrated public service provision

The following process phases are part of 'integrated public service provision' and executed by the coordination function.

- **Need identification**: This is prompted by a public service request by a citizen or business.

- **Planning**: This entails identifying the services and information sources needed, using the available catalogues, and aggregating them in a single process, considering specific user needs (e.g. personalisation).
- **Execution**: This entails collecting and exchanging information, applying business rules (as required by the relevant legislation and policies) to grant or reject access to a service and then providing the requested service to citizens or businesses.
- **Evaluation**: After service provision, users' feedback is collected and evaluated.

5.4. Internal information sources and services

MDA/LGs produce and make available a large number of services, while they maintain and manage a huge number and variety of information sources. These information sources are often unknown outside the boundaries of a particular administration (and sometimes even inside those boundaries). The result is duplication of effort and under-exploitation of available resources and solutions.

Information sources (base registries, open data portals, and other authoritative sources of information) and services available not only inside the administrative system but also in the external environment can be used to create integrated public services as building blocks.

Building blocks (information sources and services) should make their data or functionality accessible using service-oriented approaches.

5.3. Develop a shared infrastructure of reusable services and information sources that CAN be used by all MDA/LGs.

MDA/LGs SHOULD promote policies for sharing services and information sources in three main ways:

- **Reuse:** When designing new services or revising existing ones, the first step should be to investigate whether existing services and information sources can be reused.
- **Publish:** When designing new services and information sources or revising existing ones, reusable services and information sources should be made available to others for reuse.
- **Aggregate:** Once appropriate services and information sources are identified; they should be aggregated to form an integrated service provision process. The building blocks should exhibit native capability of being combined ('interoperability by design'), to be ready for mash-up in different environments with minimum customisation. This aggregation is relevant to information, services, and other interoperability solutions (e.g. software).

The reusable **building block** approach finds a suitable application by mapping solutions against the conceptual building blocks of a **reference architecture** [13] that allows reusable

[13] It is RECOMMENDED to develop interoperability architecture document for Uganda

components to be detected, which also promotes rationalisation. The result of this mapping is a **cartography** [14] of solutions, including their building blocks that CAN be reused to serve common business needs and ensure interoperability.

More specifically, to avoid duplication of effort, extra costs and further interoperability problems, while increasing the quality of services offered, the conceptual model features two types of reuse.

- **Reuse of services**: Different types of services can be reused. Examples include basic public services, e.g. issuing a birth certificate, and shared services like electronic identification and electronic signature. Shared services may be provided by the public sector, the private sector or in public-private partnership (PPP) models.
- **Reuse of information**: MDA/LGs already store large amounts of information with a potential for reuse. Examples include master data from base registries as authoritative data used by multiple applications and systems; open data under open use licences published by public organisations; other types of authoritative data validated and managed under the aegis of public authorities. Base registries and open data are discussed in more detail in the next section.

5.5. Base registries

Base registries are the cornerstone of GoU public service delivery. A base registry is a trusted and authoritative source of information, which CAN and SHOULD be digitally reused by others, where one organisation is responsible and accountable for the collection, use, updating and preservation of information. Base registries are reliable sources of basic information on data items such as people, companies, real-estate etc. This type of information constitutes the **'master data'** for MDA/LGs and GoU public service delivery. 'Authoritative' here means that a base registry is the 'source' of information, i.e. it shows the correct status, is up-to-date and is of the highest possible quality and integrity.

In case of base registries, a single organisational entity is responsible and accountable for ensuring data quality and for having measures in place to ensure the correctness of the data. Such registries are under the legal control of MDA/LGs, whereas operation and maintenance CAN be outsourced to other organisations if required. There are several types of base registries, e.g. population, businesses, vehicles, cadastres. For the MDA/LGs, it is important to obtain a high-level overview of the operation of base registries and of the data they store (a registry of registries).

In case of distributed registries there MUST be a single organisational entity responsible and accountable for every part of the register. Additionally, a single entity MUST be responsible and accountable for the coordination of all parts of the distributed registry.

[14] Ideas of the European cartography MAY be used: https://ec.europa.eu/isa2/solutions/eira_en

A **base registry framework** describes the agreements and infrastructure for operating base registries and the relationships with other entities.

Access to base registries should be regulated to comply with privacy and other regulations; base registries are governed by the principles of information stewardship.

The **information steward** is the body (or possibly individual) responsible and accountable for collecting, using, updating, maintaining and deleting information. This includes defining permissible information use, complying with privacy regulations and security policies, ensuring that information is current and ensuring the accessibility of data by authorised users.

Base registries SHOULD draw up and implement a **data quality assurance plan** to ensure the quality of their data. Citizens and businesses SHOULD be able to check the accuracy, correctness and completeness of any of their data contained in base registries in line with the data protection and privacy act.

A guide to the terminology used and/or a glossary of relevant terms used in each base registry SHOULD be made available for both human and machine-readable information purposes.

5.4. MDA/LGs SHALL make authoritative sources of information available to others while implementing access and control mechanisms to ensure security and privacy in accordance with the relevant legislation.

5.5. MDA/LGs SHALL develop interfaces with base registries and authoritative sources of information, publish the semantic and technical means and documentation needed for others to connect and reuse available information.

5.6. MDA/LGs SHALL match each base registry with appropriate metadata including the description of its content, service assurance and responsibilities, the type of master data it keeps, conditions of access and the relevant licences, terminology, a glossary, and information about any master data it uses from other base registries.

5.7. MDA/LGs SHALL create and follow data quality assurance plans for base registries and related master data.

5.6. Open data

The focus of open data policy is on releasing **machine-readable** data for use by others to stimulate transparency, fair competition, innovation and a **data-driven economy**. To ensure a level playing field, the opening and reuse of data MUST be non-discriminatory, meaning that data must be interoperable so that can be found, discovered, and processed.

GOU SHALL establish Open Data policy/framework[15] and update it regularly. Open data working group with the participation of the private sector, academy and SCO SHOULD be established.

5.8. MDA/LGs SHOULD establish procedures and processes to integrate the opening of data in their common business processes, working routines, and in the development of new information systems.

There are currently many barriers to the use of open data. It is often published in different formats or formats that hinder easy use, it can lack appropriate metadata, the data itself can be of low quality, etc. Ideally basic metadata and the semantics of open datasets SHOULD be described in a standard format readable by machines.

5.9. MDA/LGs SHALL publish open data in machine-readable, non-proprietary formats. They SHALL ensure that open data is accompanied by high quality, machine-readable metadata in non-proprietary formats, including a description of their content, the way data is collected and its level of quality and the licence terms under which it is made available. The use of common vocabularies for expressing metadata is RECOMMENDED.

Data CAN be used in different ways and for various purposes and open data publishing SHOULD allow this. Nevertheless, users might find problems with datasets or might comment on their quality or might prefer other ways of publishing. Feedback loops can help in learning more about the way datasets are used and how to improve their publication.

For reuse of open data to reach its full potential, legal interoperability and certainty is essential. For this reason, the right for anyone to reuse open data should be communicated clearly, and legal regimes to facilitate the reuse of data, such as licences, should as far as possible be promoted and standardised.

5.10. MDA/LGs MUST communicate clearly the right to access and reuse open data. The legal regimes for facilitating access and reuse, such as licences, SHOULD be standardised as much as possible.

5.7. Catalogues

Catalogues help others to find reusable resources (e.g. services, data, software, data models). Various types of catalogue exist, e.g. directories of services, libraries of software components, open data portals, registries of base registries, metadata catalogues, catalogues of standards, specifications, and guidelines. Commonly agreed descriptions of the services, data, registries and interoperable solutions published in catalogues are needed to enable interoperability between catalogues.

5.11. NITA-U SHOULD put in place catalogues of public services, public data, and interoperability solutions and use common models for describing them.

[15] https://www.ict.go.ug/wp-content/uploads/2018/06/Open-Data-Policy-First-Draft-vX.pdf

5.8. External information sources and services

MDA/LGs need to exploit services delivered outside their organisational boundaries by third parties, such as payment services provided by financial institutions or connectivity services provided by telecommunications providers. They need also to exploit external information sources such as open data and data from international organisations, chambers of commerce, etc. Moreover, useful data can be collected through the Internet of Things (e.g. sensors) and social web applications.

5.12. Where useful and feasible to do so, external information sources and services SHOULD be used while developing GoU public services.

5.9. Security and privacy

Security and privacy are the primary concerns in the provision of public services. MDA/LGs SHOULD ensure that:

- they follow the **privacy-by-design** and **security-by-design** approach to secure their complete processes (including supply chain), infrastructure and building blocks
- public sector organisations **manage information security** systematically and methodically
- services **are not exposed to threats** which might interrupt their operation and cause data leakage or data damage
- they are compliant with the legal requirements and obligations regarding **data protection and privacy**[16] acknowledging the risks to privacy from advanced data processing and analytics
- they are compliant with the legal requirements and obligations regarding the **use of electronic communications and transactions**[17]

[16] Data Protection and Privacy Act 2019. https://www.nita.go.ug/sites/default/files/publications/Draft%20Data%20Protection%20and%20Privacy%20Regulations%202019.pdf

[17] Electronic Transactions Act 2011 (Act No. 8 of 2011) https://www.nita.go.ug/publication/electronic-transactions-act-2011-act-no-8-2011

- they are compliant with the legal requirements and obligations regarding the use of **electronic signatures** and **public key infrastructure** for authenticity and security[18]

They SHOULD also ensure that data controllers and data processors comply with data protection legislation, by covering the following points:

- **'Risk management plans'** to identify risks, assess their potential impact and plan responses with appropriate technical and organisational measures. Based on the latest technological developments, those measures must ensure that the level of security is commensurate with the degree of risk
- **'Business continuity plans'** and **'Back-up and recovery plans'** to put in place the procedures needed for functions to operate after a disastrous event and bring all functions back to normal the earliest possible
- A **'data access and authorisation plan'** which determines who has access to what data and under what conditions, to ensure privacy. Unauthorised access and security breaches should be monitored, and appropriate actions should be taken to prevent any recurrence of breaches
- An **Information Security Plan** to protect personal information and sensitive MDA/LGs data. This plan can mitigate threats against MDA/LG, as well as help ADM protect the integrity, confidentiality, and availability of your data.
- Use of **qualified trust services** to ensure the integrity, authenticity, confidentiality, and non-repudiation of data.

The National Information Security Policy (NISP)[19] is carrying the main idea of mandatory minimum collection of security controls (the baseline) for any Uganda private or public sector organisation processing personal data, owning, or operating protected computers or official communications.

5.13. MDA/LGs SHOULD consider the specific security and privacy requirements and identify measures foreseen by the National Information Security Framework for the provision of each public service.

NISF MUST follow the ISO/IEC 27000 family security standards, Government Enterprise Architecture (GEA) and e-Government Interoperability Reference Architecture (GIRA). The relationship between GEA, e-Government Enterprise Security Architecture (GESA), Information Security Management System (ISMS), ISMS security standards and NISP visualised by the simplified diagram in Figure 4.

---

[18] Electronic Signatures Act 2011 (Act No. 7 of 2011) https://www.nita.go.ug/sites/default/files/publications/Electronic%20Signatures%20Act%202011%20%28Act%20No.%207%20of%202011%29.pdf

[19] https://www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf

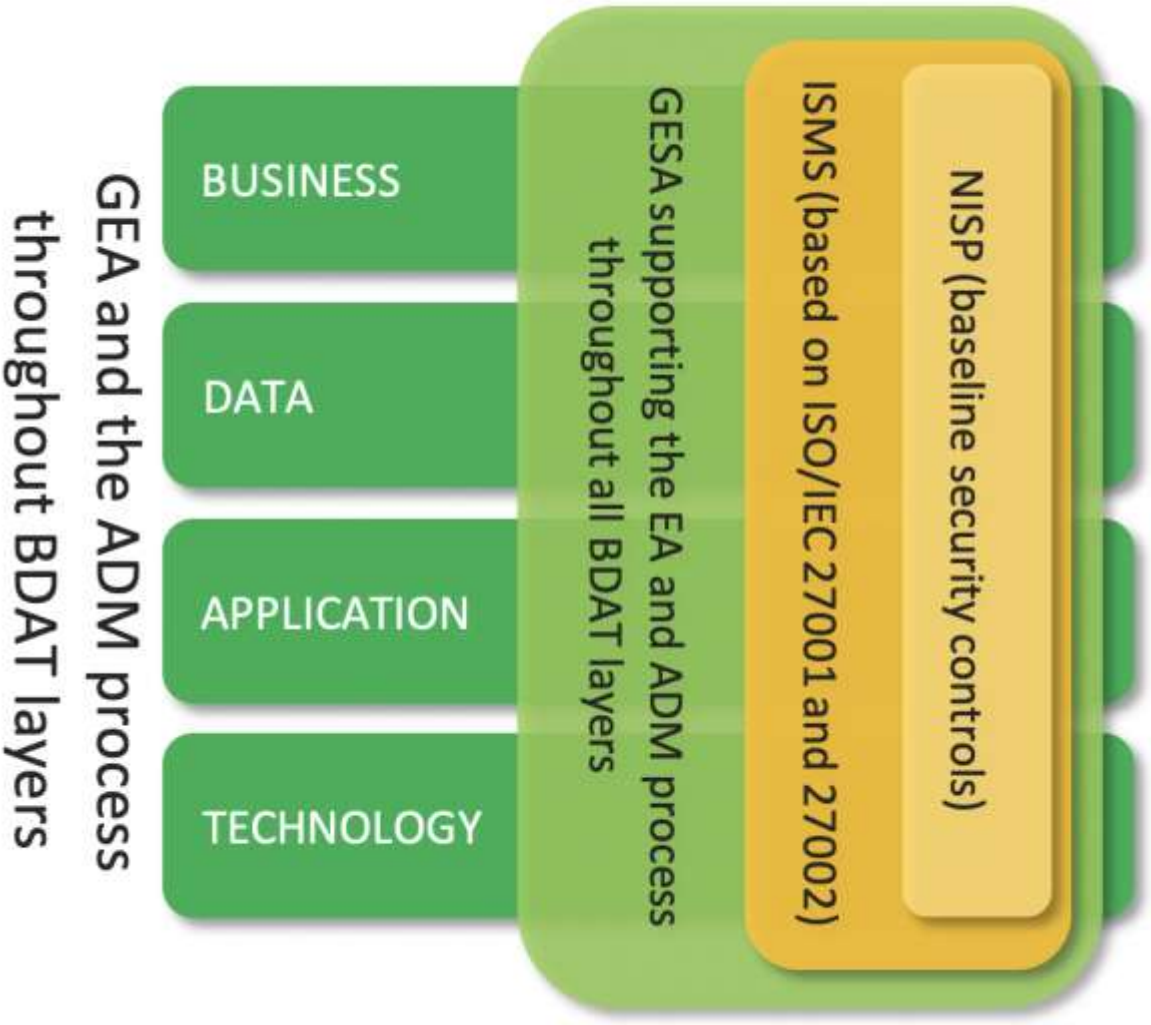

Figure 4. The relationship of components NISF Uganda. (BDAT – Business, Data, Application, Technology; ADM – Architecture Development Method; GESA – e-Government Enterprise Security Architecture)

5.14. NISF MUST align with ISMS (ISO/IEC 27001) requirements and support GESA and GEA concepts.

When MDA/LGs and other entities exchange official information, the information SHOULD be transferred, depending on security requirements, via a secure, harmonised, managed and controlled secure data exchange layer. Transfer mechanisms should facilitate information exchanges between MDA/LGs, businesses and citizens that are:

- **registered and verified**, so that both the sender and the receiver have been identified, authenticated, and authorised through agreed procedures and mechanisms
- **encrypted**, so that the confidentiality of the exchanged data is ensured
- **time stamped**, to maintain accurate time of electronic records' transfer and access
- **logged**, all electronic records to be archived, thus ensuring a legal audit trail

Appropriate mechanisms SHOULD allow secure exchange of electronically verified messages, records, forms and other kinds of information between the different systems; SHOULD handle specific security requirements and electronic identification and trust services such as electronic signatures/seals creation and verification; and SHOULD monitor traffic to detect intrusions, changes of data and other type of attacks. Information MUST also be appropriately protected during transmission, processing, and storage by different security processes such as:

- defining and applying security policies
- security training and awareness
- physical security (including access control)
- security in development
- security in operations (including security monitoring, incident handling, vulnerability management, cryptographic controls)
- security reviews (including audits, technical checks and security testing).

Common requirements for data protection SHOULD be agreed before providing aggregated services.

The provision of secure data exchange also requires several management functions, including:

- **service management** to oversee all communications on identification, authentication, authorisation, data transport, etc., including access authorisations, revocation, and audit
- **service registration** to provide, subject to proper authorisation, access to available services through prior localisation and verification that the service is trustworthy
- **service logging** to ensure that all data exchanges are logged for future reference and archived when necessary.

5.15. MDA/LGs SHOULD use foreseen by NITA-U trust services as mechanisms that ensure secure and protected data exchange in public services.

6. Governance of Interoperability Framework

The e-GIF handles information systems from the point of view of the state as a whole. The maintenance of the e-GIF document will be done by the Inter-Agency Digital Technical Implementation Committee and the e-Government working groups with the leadership of the Secretariat at the Ministry of ICT and National Guidance.

6.1. The Ministry of ICT and National Guidance coordinates the initiatives relating to the interoperability of the state information system and MUST ensure the modernity of the e-GIF. Interoperability architecture workgroup SHOULD be established.

Preparation of the interoperability framework and the related documents is supported by the NITA-U.

6.2. Specific structures, regulations and guidelines SHALL set up for supervision and coordination of e-GIF implementation.

Compliance to the e-GIF will be an integral part of IT project funding reviews by NITA-U and the Ministry of Finance, Planning and Economic Development (MoFPED). Any IT project by government organisations that is non-compliant to the e-GIF standards shall neither receive funding nor be sanctioned to proceed.

6.3. All IT projects SHALL be compliant with the e-GIF.

Full participation of MDA/LGs is essential for successfully delivering interoperability across the government. Although central direction from NITA-U will be provided where required, much of the action will take place in individual MDA/LGs. MDA/LGs shall have the following roles to play:

- Contribute to the continuous development and improvement of the e-GIF.
- Ensure that e-GIF compliance is a fundamental part of their organisational e-business and IT strategies
- Prepare a 'roadmap' for implementing the conformity with the e-GIF.
- Work with users of their data to identify those e-services that can be jointly provided as a result of data sharing.
- Ensure that they have the skills to define and use the specifications needed for interoperability.
- Establish a contact person who understands the rationale for interoperability and can respond fast to interoperability concerns in the respective government organisation.
- Budget for resources to support interoperability.
- Take the opportunity to rationalize processes (as a result of increased interoperability) to improve the quality of services and reduce the cost of provision.

MDA/LGs SHOULD analyse all the issues of interoperability in MDA/LG and they are encouraged to compile its interoperability framework (or similar) where principles and requirements are specified. These frameworks MUST be harmonised with GOU-e-GIF.

6.4. MDA/LGs are encouraged to set up their own framework that are harmonised with GOU e-GIF.

6.5. The framework should be updated at least five years or when a major change occurs.

7.Abbreviations

Abbreviation	Meaning
A2A	Administration to administration
A2B	Administration to business
A2C	Administration to Citizen
AI	Artificial Intelligence
AfricaCDE HIE	African Union Health Information Exchange
DUV	Digital Uganda Vision
e-GIF	e-Government Interoperability Framework
eID	Electronic IDentity
EIF	European interoperability framework
EU	European Union
GEA	e-Government Enterprise Architecture
GESA	e-Government Enterprise Security Architecture
GIRA	e-Government Interoperability Reference Architecture
GoU	Government of Uganda
ICT	Information and communication technology
IMSC	The Inter-Ministerial Steering Committee
IOT	Internet of things
ISMS	Information Security Management System
MDA/LG	Ministries Departments, Agencies and Local governments
MoICT&NG	The Ministry of Information and Communications Technology and National Guidance
MoU	Memorandum of Understanding
NCIP	Northern Corridor Integration Projects
NITA-U	National Information Technology Authority
NISP	National Information Security Policy
PCC	Policy Coordination Committee
PKI	Public Key Infrastructure
SLA	Service Level Agreement
SOA	Service Oriented Architecture
UgHub	Ugandan Data integration Platform
UNBS	Uganda National Bureau of Standards

8.Glossary

Term / acronym	Definition
Aggregate Public Services	A generic term used in the conceptual model for public services to refer to a set of basic public services accessed in a secure and controlled way before being combined and then delivered as a whole to end users.
Authentic Source	An authentic source is information that is stored only once and which is believed to be correct, so can serve as a basis for reuse.
Base registry	A base registry is a trusted and authoritative source of information, which CAN and SHOULD be digitally reused by others, where one organisation is responsible and accountable for the collection, use, updating and preservation of information.
Building block approach	An approach to building information systems from architecture to implementation in which the information system is designed as an assembly or aggregation of components that encapsulate data and functionalities in groups that can also be reused as 'building blocks' to build other public services or information systems.
Business Process	A business process is a sequence of linked activities that creates value by turning inputs into a more valuable output. This can be performed by human participants or ICT systems, or both.
Data Controller	Person, who alone, jointly with other persons or in common with other persons or as statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.
Data Processor	Data processor in relation to personal data, means a person other than employee of the data controller who processes the data on behalf of the data controller.
Data Repository	Any collection of data meant for use (processing, storage, querying, etc.) by an information system. Typically, a data repository contains additional structural and semantic information about the data in question, designed to aid the use of the data (data model, relationships between data elements, metadata, etc.). It may provide specific functionalities closely tied to the data stored in the repository (searching, indexing, etc.).
eGovernment	eGovernment is about using the tools and systems made possible by information and communication technologies (ICTs) to provide better public services to citizens and businesses.
Electronic Certification	Electronic certification is the application of an electronic signature, by a specifically authorised person or entity, in a specific context for a specific purpose. It is mostly used to indicate that a certain validation process has been executed and that a given result is being attested by the signer.
Electronic Signature	An electronic signature, or e-signature, refers to data in electronic form, which is logically associated with other data in electronic form and which is used by the signatory to sign. This type of signature provides the same legal standing as a handwritten signature as long as it adheres to the requirements of the specific regulation under which it was created

Formalised Specifications	Formalised specifications are either standards or specifications established by ICT industry fora or consortia.
Government Enterprise Architecture (GEA)	The structure of e-Government components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.
Information	Information is semantically enriched data, i.e. collections of data that have been given relevance and purpose.
Interface	An interface is a conceptual or physical boundary where two (or more) independent legal systems, organisations, processes, communicators, IT systems, or any variation/combination thereof interact.
Interoperability	The ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their ICT systems.
Interoperability Agreements	Written interoperability agreements are concrete and binding documents which set out the precise obligations of two parties cooperating across an 'interface' to achieve interoperability.
Interoperability Framework	An interoperability framework is an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.
Interoperability Governance	Interoperability governance covers the ownership, definition, development, maintenance, monitoring, promoting and implementing of interoperability frameworks in the context of multiple organisations working together to provide (public) services. It is a high-level function providing leadership, organisational structures and processes to ensure that the interoperability frameworks sustain and extend the organisations' strategies and objectives
Interoperability Levels	The interoperability levels classify interoperability concerns according to who/what is concerned and cover, within a given political context, legal, organisational, semantic and technical interoperability.
Legal interoperability	Ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together
Memorandum of Understanding	A bilateral or multilateral written agreement between two organisations which sets out a number of areas and means by which they will cooperate, collaborate or otherwise assist one another. The exact nature of these activities depends on the nature of the two organisations, the domain of activity in question, and the scope of the cooperation envisaged.
Orchestration	The aggregation and sequenced execution of sets of transactions involving use of other services and functionalities, according to business rules embodied in one or more documented business processes, with the ultimate goal of performing or providing some other value-added function or service. Orchestration is

	closely related to the concept of workflow. Usually, orchestration involves executing a set of processes, described in a standard language, by an 'orchestration engine', which is configurable and capable of executing all the requisite service calls and routing the inputs and outputs of processes according to rules described in that language.
Organisational Interoperability	Ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together
Public Data	Public data is information that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.
Public Service	Service can be: A repeatable activity: a discrete behaviour that a component of organisation may be requested or otherwise triggered to perform. An element of behaviour that provides specific functionality in response to requests from actors or other services.
Reusability	The degree to which a software module or other work product can be used in contexts other than its original, intended or main purpose.
Secure Data Exchange	This is a component of the conceptual model for public services. Its aim is to ensure that all data exchanges are done in a secure and controlled way.
Semantic interoperability	Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'.
Semantic Interoperability Assets	Semantic interoperability assets are a subset of interoperability assets and include any element of the semantic layer, such as nomenclatures, thesauri, dictionaries, ontologies, mapping-tables, mapping-rules, service descriptions, categories, and web services.
Service Level Agreement	A formalised agreement between two cooperating entities; typically, a service provider and a user. The agreement is expressed in the form of a written, negotiated contract. Typically, such agreements define specific metrics (Key Performance Indicators — KPIs) for measuring the performance of the service provider (which in total define the 'service level'), and document binding commitments defined as the attainment of specific targets for certain KPIs, plus associated actions such as corrective measures. SLAs can also cover commitments by the user, for example to meet certain notification deadlines, provide facilities or other resources needed by the service provider in the course of service provision, problem solving, or to process inputs given by the service provider to the user.
Service Orientation	Service orientation means creating and using business processes packaged as services.
Service Oriented Architecture (SOA)	Service oriented architecture is a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to

	offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations
Standard	A standard is a technical specification approved by a recognised standardization body for repeated or continuous application, with which compliance is not compulsory
Taxonomy	A taxonomy represents a classification of the standardised terminology for all terms used within a knowledge domain. In a taxonomy, all elements are grouped and categorised in a strict hierarchical way and are usually represented by a tree structure. In a taxonomy, the individual elements are required to reside in the same semantic scope, so all elements are semantically related with one another to one degree or another.
Technical interoperability	Technical interoperability covers the applications and infrastructure linking systems and services
GoU Interoperability Framework (e-GIF)	The agreed approach to the delivery of GoU public services in an interoperable manner. It defines basic interoperability guidelines in the form of common principles, models, and recommendations.
Vocabulary	A vocabulary is a set of terms (words or phrases) that describe information in a particular domain.
Workflow	The organisation of a process into a sequence of tasks that are performed by duly designated sets of actors fulfilling given roles in order to complete the process.