THE REPUBLIC OF UGANDA

e-Government Interoperability Framework Reference Architecture

GIRA-2026

May 15, 2026

Table of Contents

1. Introduction

1.1. Background

The Ugandan e-Government Interoperability Framework Reference Architecture (GIRA-2026) is a structured architectural blueprint that GOU use to ensure that digital systems, services, and institutions can seamlessly exchange data, integrate processes, and work together across all sectors. Renewal of the Government Enterprise Architecture (GEA) and e-Government Interoperability Framework (e-GIF),[1] GIRA-2026 represents a significant evolution of the 2021 version.[2]

GIRA-2026 takes account of experiences, guidelines, and initiatives of United Nations[3], OECD[4], EU[5], World Bank[6], UN led GovStack initiative[7], EU member states and other countries, especially in Africa. The GIRA uses the terminology of TOGAF[8] and the European Interoperability Reference Architecture (EIRA©)[9] The content is adjusted to the GoU national policies, strategies, and guidelines.

Relationship to the Government Enterprise Architecture (GEA): GIRA-2026 provides the structure and principles governing the inter-relationships between Uganda's e-government components, including its institutions, people, systems, and datasets. While the GEA serves as the overarching blueprint for optimizing fragmented architectural processes into an integrated environment, GIRA-2026 focuses specifically on the interoperability of digital public services.

Relationship to the e-Government Interoperability Framework (e-GIF): the GIRA serves as the technical implementation strategy for e-GIF. It translates high-level principles into actionable

---

[1] GIRA is crucial part of GEA. Sometimes (for example in TOR) the general term GEA is used instead of GIRA.

[2] https://www.nita.go.ug/projects/uganda-enterprise-architecture-and-interoperability-framework

[3] https://publicadministration.un.org/egovkb/en-us/

[4] https://read.oecd.org/10.1787/f64fed2a-en?format=pdf

[5] https://interoperable-europe.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira

[6] https://wwhttps://govstack.global/about/ w.worldbank.org/en/programs/govtech

[7] https://govstack.global/about/

[8] https://www.opengroup.org/togaf

[9] https://interoperable-europe.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira

designs, ensuring that its architectural views correspond directly to the four layers of interoperability: **legal, organisational, semantic, and technical**.

Key New Characteristics of GIRA-2026 comparing with GIRA-2021 illustrated in Figure 1 and described below:

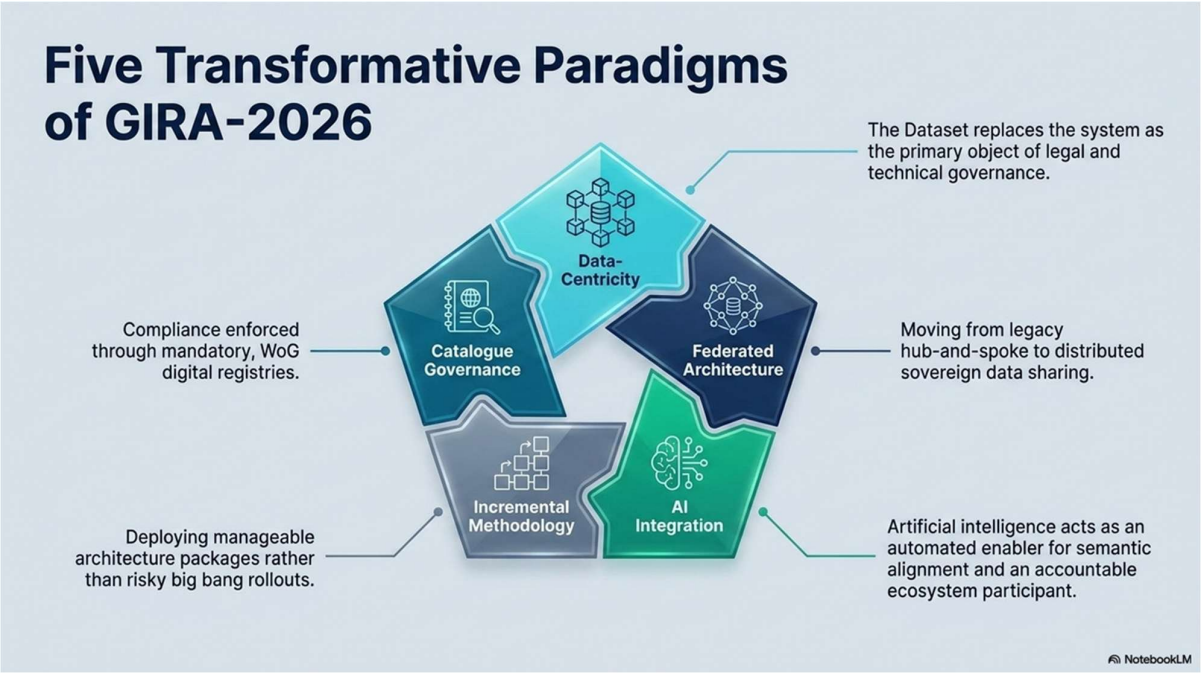

Figure 1 Five Transformation Paradigms of GIRA-2026

- **Data-Centric Paradigm**: Uganda is transitioning from a "system-centric" approach to a data-centric model, where the Dataset is the primary object of governance, ensuring digital continuity regardless of the underlying hosting system.
- **Federated Data Space:** Moving away from centralized "hub-and-spoke" models toward a Federated Data Space architecture, utilizing distributed Sovereign Connectors. This ensure that data remains at its source while being securely accessible. It eliminates **Single Points of Failure (SPOF)**.[10]

[10] Multiple organisations and initiatives are developing specifications, standards, and building blocks for dataspaces, such as the International Data Spaces Association (IDSA): https://internationaldataspaces.org/ , the Gaia-X European Association for Data and Cloud AISBL: https://gaia-x.eu/ , the Eclipse Dataspace Working Group (EDWG): https://dataspace.eclipse.org/, the Data Spaces Support Centre (DSSC): https://dssc.eu/, Nordic Institute for Interoperability Solutions (NIIS): https://www.niis.org/ (with the release of X-Road 8 "Spaceship"). The initiatives work together to keep specifications and standards aligned, thereby avoiding the creation of multiple overlapping or competing specifications.

- **AI-Enhanced Interoperability:** Artificial Intelligence (AI) is integrated as a driver for automating semantic alignment and as a compliant participant that must adhere to transparency and ethical standards.
- **Whole-of-Government Integration:** The GIRA-2026 is designed to eliminate "ICT islands" by mandating the use of Shared Enablers (like Secure Data Exchange, UgPass and the National Payment Switch) and ensuring that all new systems are API-first by default.
- **Catalogues based governance.** For interoperability governance the interconnected system of catalogues SHOULD be used. Compliance to e-GIF should no longer be voluntary. e-GIF-2026 and GEA shall be enforced with the use of Catalogues.

GIRA has four main characteristics:

- **Common terminology to achieve coordination**: It provides a common understanding that can be used by people working for public administrations in various architecture and system development tasks.
- **Reference architecture for delivering digital public services:** It offers a framework to categorise (re)usable Solution Building Blocks (SBBs) of an eGovernment solution. It focused on the design of end-to-end interoperable digital public services. It allows portfolio managers to rationalise, manage and document their portfolio of solutions.
- **Technology- and product-neutral and a service-oriented architecture (SOA) style:** The GIRA adopts a service-oriented architecture style and promotes ArchiMate® as a modelling notation. The GIRA ABBs can be seen as an extension of the model concepts in ArchiMate®.
- **Alignment with e-GIF-2026 and TOGAF®.** The GIRA is aligned with the Ugandan Interoperability Framework (e-GIF). The views of the GIRA correspond to the interoperability levels in the GIF: legal, organisational, semantic, and technical. The GIRA reuses terminology and paradigms from TOGAF® such as architecture building blocks and views. This not only assures a high level of quality but also allows architects to easily understand the GIRA and relate it to existing work.

The GIRA has the objective to respond to the above needs by supporting users in the following scenarios:

- **Design**: accelerate the design of eGovernment solutions that support the delivery of interoperable digital public services (across borders and sectors).
- **Assess**: provide a reference model for comparing existing architectures in different policy domains and thematic areas, to identify focal points for convergence and reuse.
- **Communicate and share:** help documenting the most salient interoperability elements of complex solutions and facilitate the sharing of (re)usable solutions.
- **Discover and reuse**: ease the discovery and reuse of interoperability solutions.

The update from GIRA-2021 to GIRA-2026 was guided by lessons learned and evolving policy prioritiesin today's digital landscape:

- The update drew on the existing GIRA-2021 framework, incorporating feedback from its formal evaluation, implementation monitoring, and broader stakeholder consultations**.** The

update addresses technological advances (e.g. on data spaces, AI, IoT interoperability), political shifts and evolving strategic priorities such as digital sovereignty.

1.2. Methodology: frameworks, standards, tools

In this section we will list and describe shortly main frameworks, standards and tools that been applied for building the GIRA-2026:

- The Uganda e-Government Interoperability Framework (e-GIF-2026),
- The Open Group Architecture Framework (TOGAF),
- The Architecture Development Method (ADM),
- The Enterprise Architecture Modelling Language ArchiMate®,
- Archi®, a modelling toolkit for creating ArchiMate models and sketches,
- The European Interoperability Reference Architecture (EIRA©)

GIRA-2026 methodological approach is illustrated in Figure 2.

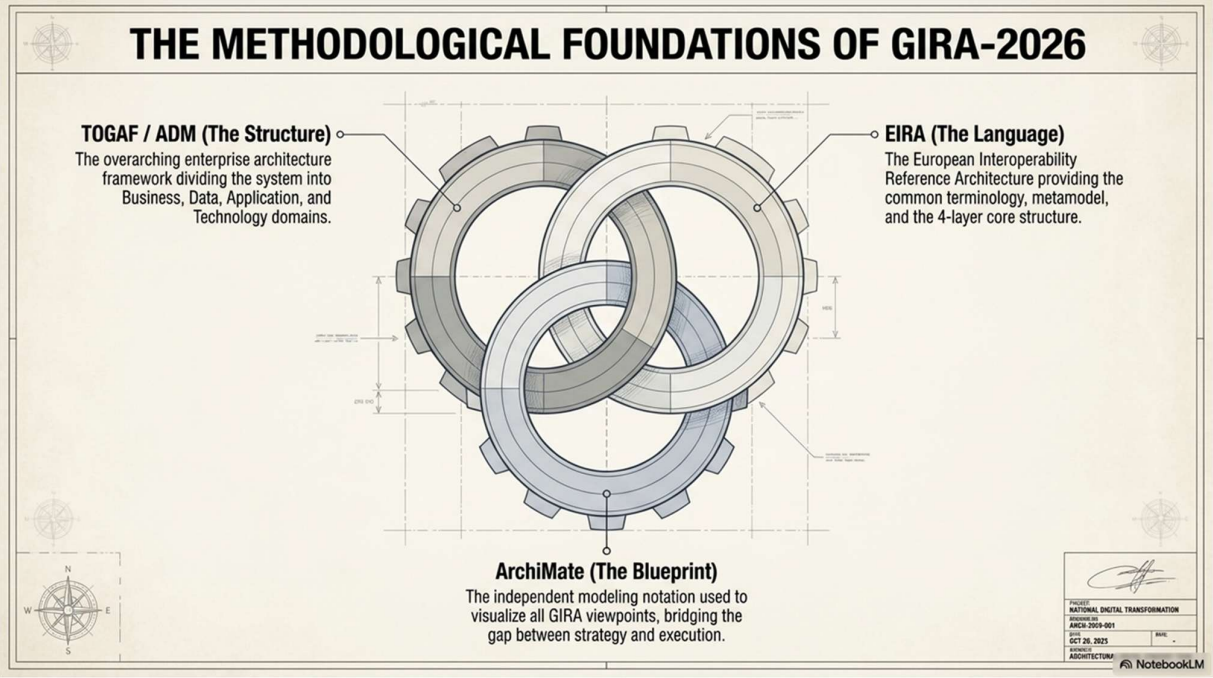

Figure 2 The methodological approach of GIRA-2026

e-GIF.[11] The Ugandan Interoperability Framework (e-GIF) is the agreed approach to the delivery of the Government of Uganda's (GOU's) public services in an interoperable manner. It defines the basic interoperability guidelines in the form of common principles, models, and recommendations. The GIRA is aligned with the e-GIF. The views of the GIRA correspond to the interoperability levels in the e-GIF: legal, organisational, semantic and technical interoperability.

TOGAF®.[12] The Enterprise Architecture framework TOGAF® is used by GOU for developing Government Enterprise Architecture. TOGAF is a generic framework. The TOGAF standard considers an "enterprise" to be any collection of organizations that have common goals.

Although the TOGAF documentation works together as a whole, it is expected that organizations will customize it during adoption, and deliberately choose some elements, customize, exclude, and/or create others.

TOGAF is based on four interrelated areas of Framework of specialization called architecture domains:

- **Business architecture** which defines the business strategy, governance, organization, and key business processes of the organization
- **Data architecture** which describes the structure of an organization's logical and physical data assets and the associated data management resources
- **Applications architecture** which provides a blueprint for the individual systems to be deployed, the interactions between the application systems, and their relationships to the core business processes of the organization with the frameworks for services to be exposed as business functions for integration
- **Technical architecture**, or technology architecture, which describes the hardware, software, and network infrastructure needed to support the deployment of core, mission-critical applications

GIRA reuses terminology and paradigms from TOGAF® such as architecture patterns, building blocks and views. This not only assures a high level of quality but also allows architects to easily understand EIRA© and relate it to existing work.

[11] Uganda e-Government Interoperability Framework (e-GIF). https://www.nita.go.ug/projects/uganda-enterprise-architecture-and-interoperability-framework

[12] https://www.opengroup.org/togaf/10thedition

ADM. The TOGAF ADM forms the core of TOGAF. It is a reliable, proven method for developing an Enterprise Architecture that meets the business needs of an organisation, utilising the other elements of TOGAF, and other architectural assets available to the organisation.

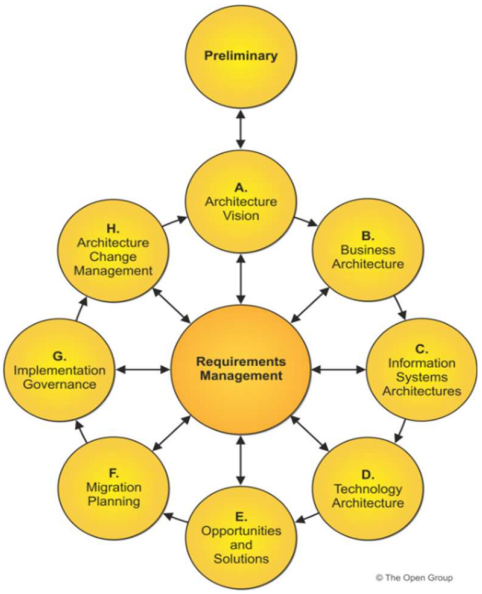

Figure 3 Basic structure of the ADM

The ADM is a generic method for architecture development, which has been designed to deal with most system and organisational requirements. However, it will often be necessary to modify or extend the ADM to suit specific needs.

The basic structure of the TOGAF ADM is shown in Figure 3. Throughout the TOGAF ADM cycle, there needs to be frequent validation of outputs against original expectations, both those from the whole TOGAF ADM cycle, and those from the phases of the method.

The ADM is iterative over the whole process, between phases and within phases; for each iteration of the ADM, a fresh decision must be taken on:

- The breadth of coverage of the enterprise to be defined
- The level of detail to be defined
- The extent of the time horizon aimed at, including the number and extent of any intermediate time horizons
- The architectural assets to be leveraged in the GOU

ArchiMate®.[13] The ArchiMate® modelling language is an open and independent Enterprise Architecture standard that supports the description, analysis and visualisation of architecture within and across business domains. ArchiMate is one of the open standards hosted by The Open Group® and is fully aligned with TOGAF®. ArchiMate® aids stakeholders in assessing the impact of design choices and changes. All views and viewpoints of GIRA are visualised by using the ArchiMate® language. ArchiMate 3.2 Notation is presented in Figure 4.

Archi®.[14] The Archi® modelling toolkit is targeted toward all levels of Enterprise Architects and Modellers. It provides a low cost to entry solution to users who may be making their first steps in the ArchiMate® modelling language, or who are looking for an open source, cross-platform ArchiMate® modelling tool for their company or institution and wish to engage with the language within a TOGAF® or others Enterprise Architecture framework. GIRA is modelled by using Archi®.

[13] https://www.opengroup.org/archimate-forum/archimate-overview

[14] https://www.archimatetool.com/

EIRA.[15] The European Interoperability Reference Architecture (EIRA©) is an architecture content metamodel defining the most salient ABBs needed to build interoperable e-Government systems. The EIRA© provides a common terminology that can be used by people working for public administrations in various architecture and system development tasks.

[15] https://interoperable-europe.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/release/610

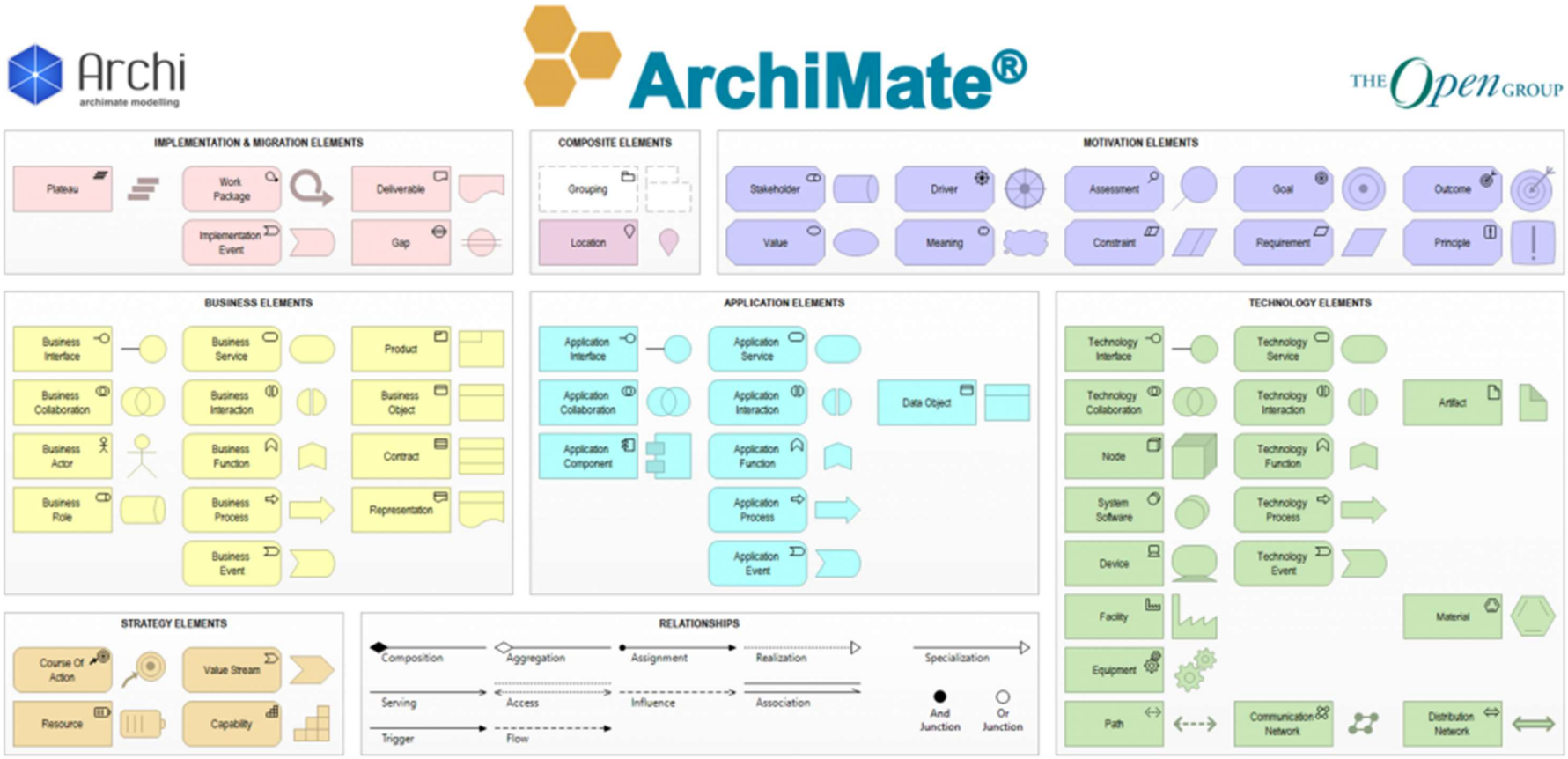

Figure 4 ArchiMate 3.2 Notation (taken from https://www.archimatetool.com/resources/)

1.3. Context

The Ugandan GIRA is an important part of the activities for building an 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.

The purpose of an Enterprise Architecture is to optimize the fragmented architectural processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the delivery of the business strategy.

The Enterprise Architecture framework TOGAF® is used by the GOU for developing a Government Enterprise Architecture. TOGAF® is generic framework. The TOGAF® standard considers an "enterprise" to be any collection of organizations that have common goals.

The core of TOGAF® is Architecture Development Method (ADM). ADM is a multi-phase, iterative approach to develop and use an Enterprise Architecture to shape and govern business transformation and implementation projects.

We distinguish the following steps/levels in the GEA lifecycle illustrated in Figure 5:

- **Preliminary Phase**. The strategy of the Ugandan e-Society and e-Government has been fixed in vision papers and legislations. For GIRA-26 Preliminary phase was renewed in Regulatory and Policy Review report.[16]
- **e-GIF**. e-GIF provides the implementation strategy for GEA. It defines basic interoperability guidelines in the form of common principles, models, and recommendations for interactions between public institutions. In terms of TOGAF®, e-GIF covers all phases of the ADM cycle, primarily the Vision phase. The purpose of e-GIF is to describe the strategic level of GEA as it depicted in Figure 5 (left side).
- **e-Government Interoperability Reference Architecture (GIRA**). 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 public administrations. GIRA covers, in terms of TOGAF®, the core phases of ADM: business architecture, information systems architecture and technology architecture Figure 5(right side) mainly. The ADM vision phase will be reviewed and refined.
- **Security architecture.** Security architecture is the viewpoint of GEA. All phases of ADM cycle contain security and privacy aspects.
- **Implementation plan of GEA.** This step results in the implementation plan and roadmap highlighting the required activities, resources and timelines as well as cross-government governance structures to ensure compliance and uptake of the developed GIRA. In terms of ADM, it covers phases E and F.

---

[16] Regulatory and Policy Review Report. Internal report of "Renewal of Uganda's GEA and e-GIF" project (2026). 33p

- **Governance of GEA.** Building, monitoring, managing, and steering of the implementation of GEA is in focus of this step. Building GEA is an iterative process. Some components might need to be renewed; some components might need to be added. Sometimes it is reasonable to restart a new lifecycle from the beginning. In terms of ADM, it covers phases G and H.

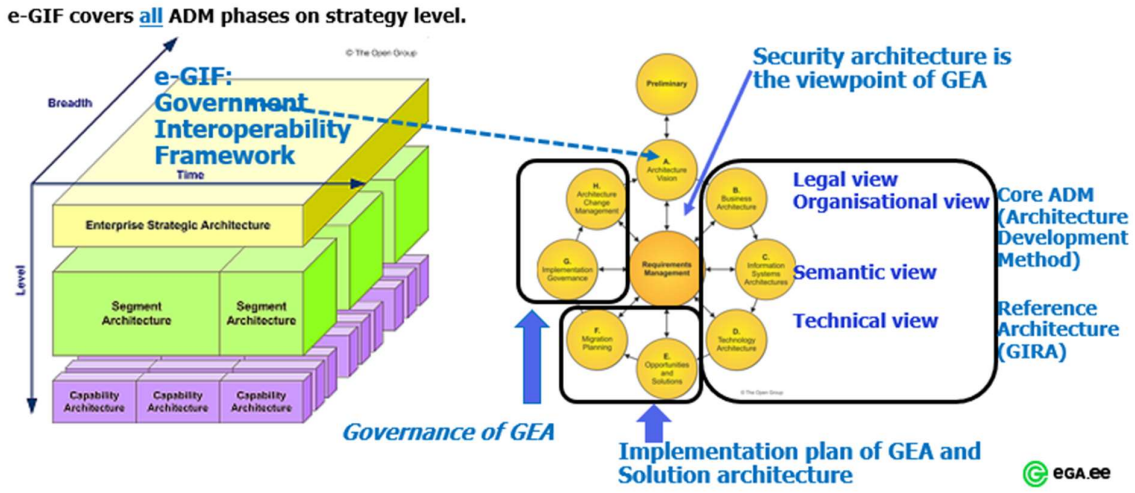

Figure 5 e-GIF covers all ADM phases on strategy level. The GIRA covers the core components of ADM: business, information systems and technology architectures.

1.4. Benefits

The use of the GIRA will provide the following benefits, which are explained in the subsequent sections:

- Proving a controlled vocabulary
- Decoupling functionalities in Architectural Building Blocks
- Accelerating the development cycle
- Supporting portfolio management decision making
- Supporting public policy formulation

1.4.1. Providing a controlled vocabulary

Being a controlled vocabulary, the GIRA provides a common language of Architecture Building Blocks for the design and comparison of the solution architectures of eGovernment solutions. Architects can easily understand the functionality of other solutions that are based on the GIRA as well as the interfaces to other solutions where those are documented in the same language.

1.4.2. Decoupling functionalities in Architectural Building Blocks

Each Architecture Building Block in the GIRA provides decoupled functionality meaning that the ABBs are autonomous and unaware of the other Architecture Building Blocks within the same context. The autonomous nature of the ABBs is an absolute necessity for reusability, provided that the interfaces are clearly defined. The decoupling also helps in rationalisation exercises where one Solution Building Block can be exchanged with another Solution Building Block, if they both "realise" the same Architecture Building Block.

1.4.3. Accelerating the development cycle

The development cycle is accelerated by the increased application of the principles of service-oriented architecture (SOA). Architects are guided naturally towards service-oriented architecture when using GIRA. It enables consumption of the system's services by other systems and vice versa without additional investments. Development time of new services is often much higher than integration costs of existing services. In addition, reuse at service level helps avoiding costs which are typically associated with the reuse of applications or components and accelerates the development cycle of new solutions.

1.4.4. Supporting portfolio management decision making

Portfolio managers are, through the common language, provided with a classification schema that allows:

- discovery of systems with identical or overlapping functionalities inside the organisation which might be phased out, and
- identification of Solution Building Blocks that could be made more generic

Architects can learn how to make Solution Building Blocks more generic. The GIRA identifies the ones with high interoperability relevance that should be implemented as modular services. The central functionalities need to be developed and maintained only once, and competing solutions providing the same functionalities can be replaced by more generic ones.

1.4.5. Supporting public policy formulation

The GIRA supports public policy formulation in the form of impact assessments where possible impacts to available solutions are examined during the public policy preparation phase. The assessments are carried out on initiatives expected to have significant economic, social, or environmental impacts. These can be:

- Legislative initiatives
- Non-legislative initiatives such as financial plans and recommendations for the negotiations of agreements)
- Implementing and delegating acts

1.4.6. Support B2B and B2C interactions and cross border data exchange

The GIRA can also be used for B2B (business to business) and B2C (business to citizens) interactions. The GIRA facilitates these interactions by providing a unified digital ecosystem, shared standards, and foundational building blocks that the private sector can adopt or integrate with. GIRA-2026 is ready for its expanding for cross border data exchange and use by private sector as depicted in Figure 6.

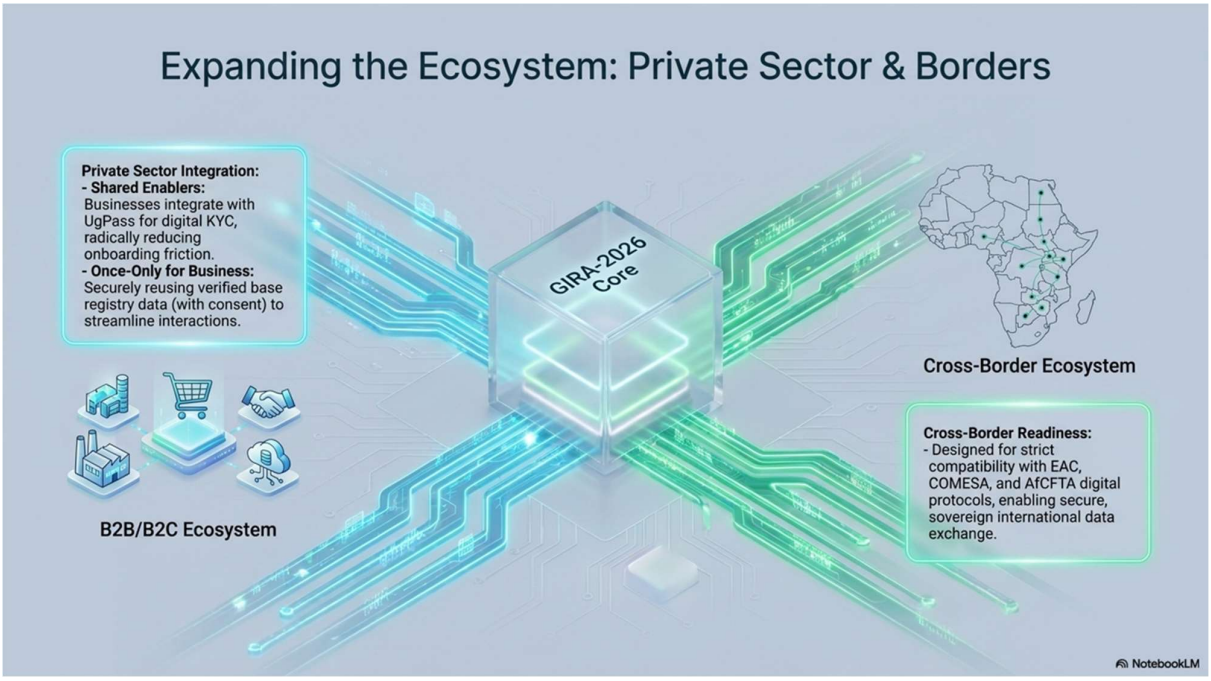

Figure 6 Readiness for cross border and private sector

1.4.6.1. Use of Shared Enablers.

GIRA provides the private sector with "digital rails" through mandatory shared enablers that simplify and secure private-sector transactions.

- **Digital Identity (UgPass):** By integrating with the national eID and PKI ecosystem, businesses can perform Digital KYC (Know Your Customer), reducing the cost and time of onboarding customers for private services.
- **National Payment Switch:** This enabler provides interoperability between different bank accounts and payment instruments, facilitating seamless B2B payments and B2C e-commerce transactions.
- **Trust Services:** GIRA's standards for electronic signatures and seals ensure that digital contracts between businesses or between businesses and consumers have the same legal standing as handwritten ones.

1.4.6.2. Standardization of the Digital Economy.

GIRA creates a predictable environment for the private sector by establishing common technical and semantic standards.

- **Common Terminology and Standards:** By following GIRA's controlled vocabulary and open standards (like XML, JSON, and REST APIs), businesses can design their own systems to be compatible with both the government and other GIRA-compliant private partners, reducing integration costs and technical debt.
- **Interoperability by Design:** Private service designers are encouraged to join communities of practice across administrations to co-create assets and reuse existing solution patterns, ensuring that new B2B/B2C services are interoperable from the start.

1.4.6.3. Participation in the Data Space Ecosystem.

The transition to a Federated Data Space allows trusted private partners to become active participants in the national data ecosystem.

- **Secure Data Sharing:** Businesses can use GIRA-compliant Sovereign Connectors to share data with other businesses while maintaining absolute control via machine-readable Usage Control Policies (ODRL).
- **Once-Only Principle for Business:** The architecture ensures that once data is verified in a base registry, it can be reused securely by businesses (with proper consent), preventing citizens from having to resubmit the same information to different private service providers.

1.4.6.4. Practical Applications: Digital Invoicing.

1. A core example of GIRA supporting B2B and B2C is the implementation of Digital Invoices.

- **Automation:** By utilizing the secure data exchange and common data formats, digital invoices allow the economy to conduct transactions fully digitally and instantly across both the public and private sectors.
- **Cashless Economy:** These standards support the broader national effort to achieve a cashless economy, improving transaction accuracy and administrative efficiency for all business entities.

1.4.6.5. Benefits for Private Stakeholders.

According to the e-GIF stakeholder mapping, GIRA-compliant interactions offer specific contributions and benefits for the private sector:

- **ICT Providers:** Gain market alignment and can offer new solutions based on existing technical interoperability, allowing them to compete on quality and cost.
- **Businesses:** Experience reduced administrative burdens, easier procedures for interacting with government, and more control over the reuse of their data.

- **Service Designers:** Benefit from access to proven interoperability solutions and faster design cycles.

1.5. Scope and Structure

This document is addressed to all those experts involved in defining, designing, developing, delivering, and governing public services. The GIRA is applicable to all MDAs in Uganda.

The reference architecture is a guideline for the following users within MDAs and the private sector:

- **Architects**, Enterprise Architects as well as Solution Architects who are responsible for the design of solution architectures
- **Business analysts** responsible for assessing and studying the impact of changes in the (external) environment on IT systems
- **Portfolio managers** responsible for maintaining of assets related to the design and implementation of eGovernment solutions and for making investment decisions on these assets.
- **Service providers.** Reuse of existing data and solutions. Lower ICT cost through market mechanisms.
- **Service designers.** Access to interoperability solutions. Efficient assessments through alignment. Faster design cycles and improved service quality.
- **Policy makers.** Policies and measures that promote sustainable digital transformation of the public sector.
- **ICT providers.** Existing and new solutions. Existing technical interoperability. Competition on quality and cost.

The GIRA can be used for building domain-specific architecture frameworks in Uganda. These frameworks should remain compatible with the GIRA, and where necessary, extend the scope of the GIRA to capture the specific ABBs of the domain in question.

The GIRA 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, MDAs 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 to MDA), which refers to interactions between MDAs.
- A2B (MDA to business), which refers to interactions between MDAs and businesses.
- A2C (MDA to citizen), which refers to interactions between MDAs and citizens.

- **Support to B2B and B2C interactions.** It must be noted that the GIRA can also be used for B2B (business to business) and B2C (business to citizens) interactions. It is described in more details in section 1.4.6.

The GIRA content and structure is presented below and visualised in Figure 7:

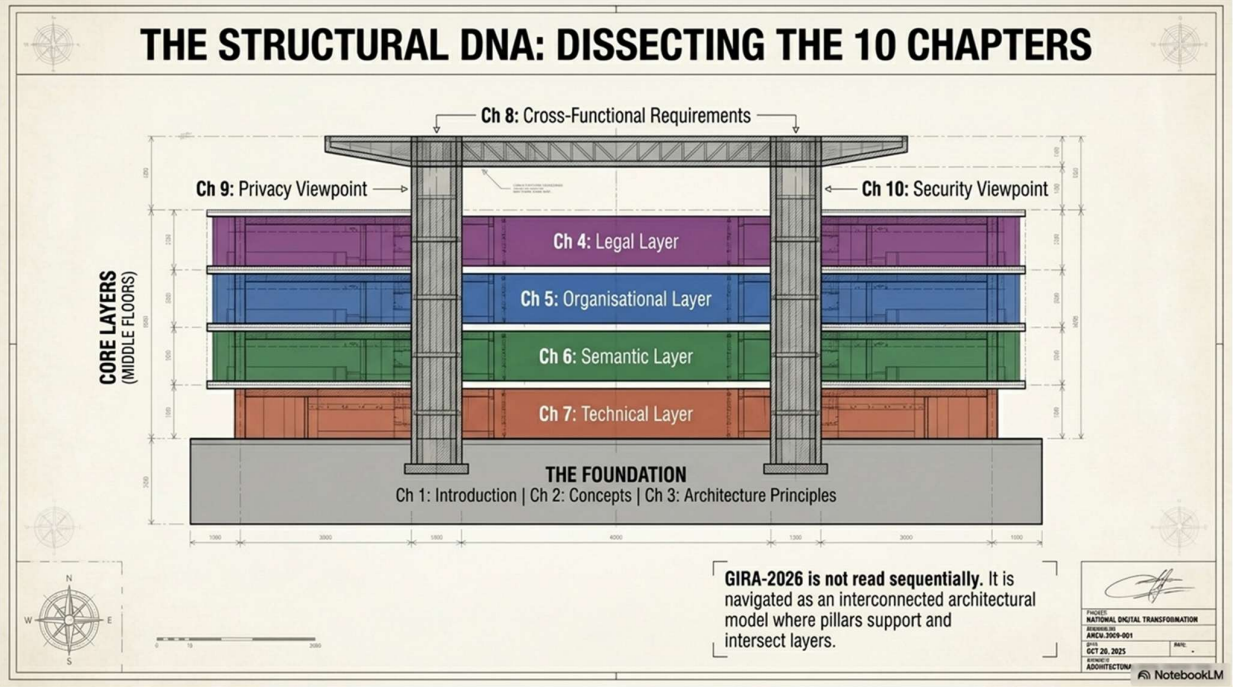

Figure 7 GIRA-2026 visualised structure

Chapter 1 provides an overview of the GIRA. It includes background information, methodology, context in building the GEA, and benefits.

Chapter 2 provides 6 key viewpoints. The focus is on new changes in the conceptual model: shift from centralized to federated architecture, strengthened trust and security, AI.

Chapter 3 provides six types of architecture principles:

- The e-GIF-2026 underlying principles
- Digital Public Service Strategy
- Digital Public Service Design
- Digital Public Service Operations
- Improvement architecture
- Solution Architecture Principles

Chapter 4 provides baseline and target legal reference architecture.

Chapter 5 provides baseline and target organisational reference architecture.

Chapter 6 provides baseline and target semantic reference architecture.

Chapter 7 provides baseline and target technical reference application architecture.

Chapter 8 provides cross-functional requirements.

Chapter 9 is dedicated to the horizontal privacy viewpoint.

Chapter 10 gives viewpoint to the security architecture.

Chapter 11 gives definitions

2. Key concepts

2.1. Ontology viewpoint

The ontology of enterprise architecture defines a common vocabulary for sharing information in a domain. They provide a standardized, machine-interpretable definition of basic concepts within the domain, and of relations among them. The general ontology of the GIRA (based on EIRA© methodology) is depicted in Figure 8.

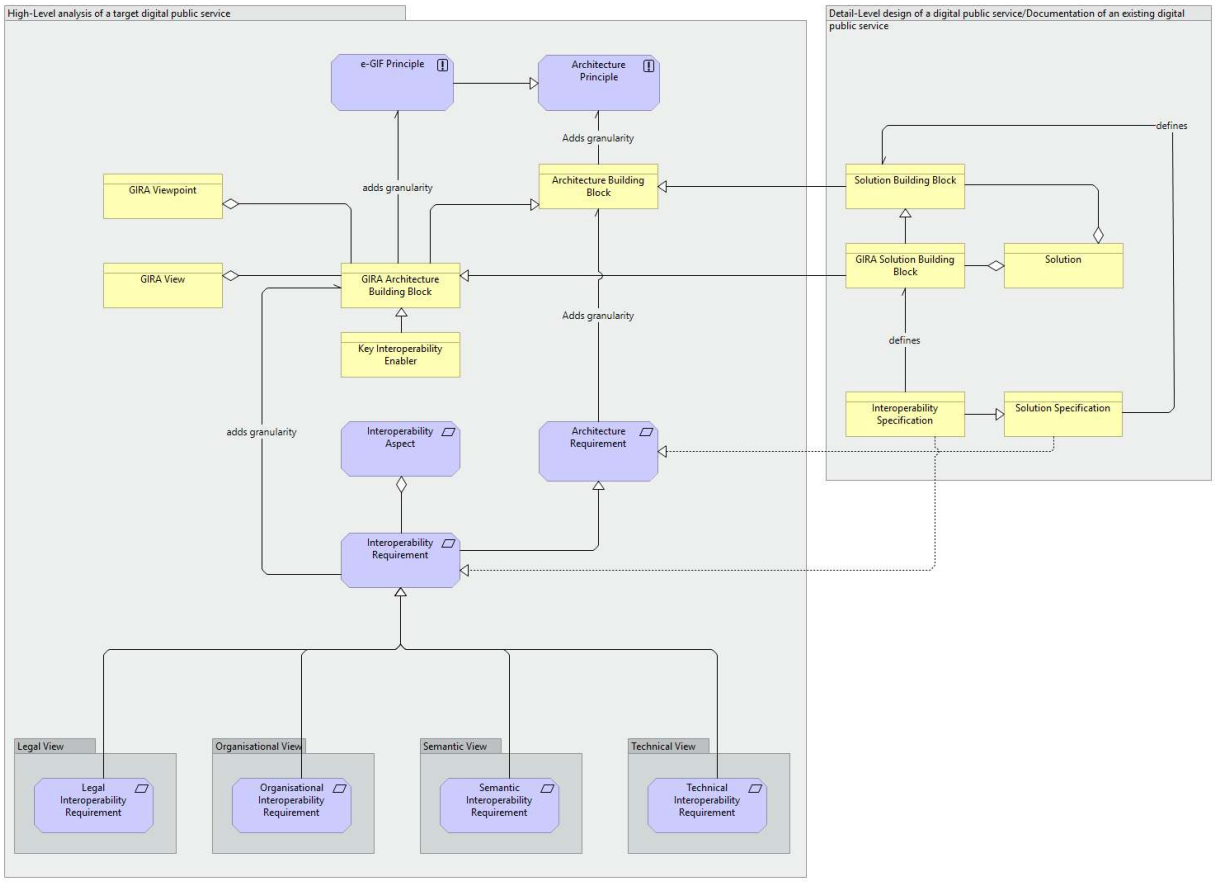

Figure 8 General ontology of the GIRA

The key concepts of the GIRA are defined as follows:

e-GIF interoperability level. The e-GIF-2026 is a set of guidelines for developing public services. They cover legal, organizational, semantic, and technical interoperability. Each level deserves special attention when a new GOU public service is established.

e-GIF principle. The e-GIF outlines 12 underlying principles of the GOU public services. These general principles of good administration are relevant to the process of establishing public services.

They describe the context in which GOU public services are decided and implemented. They complement one another regardless of their different natures, e.g., legal or technical.

GIRA view. The GIRA consists of several views, including one view for each of the e-GIF interoperability levels. The GEA views contain a graphical notation of the GIRA ontology.

GIRA viewpoint. The GIRA provides several viewpoints that conform to the GIRA views, the viewpoints provide a perspective with a specific stakeholder's concern in mind.

Architecture Building Block. Based on the TOGAF® definition, an Architecture Building Block (ABB) is an abstract component that captures architecture requirements and that directs and guides the development of Solution Building Blocks. An ABB represents a (potentially re-usable) component of legal, organizational, semantic, or technical capability that can be combined with other Architecture Building Blocks. An Architecture Building Block describes generic characteristics and functionalities. Architecture Building Blocks are used to describe reference architectures, solution architecture templates or solution architectures of specific solutions.

Solution Building Block. Based on the TOGAF® definition, a Solution Building Block is a concrete element that defines the implementation and fulfils the required business requirements of one or more Architecture Building Blocks. From the technical view, a Solution Building Block is a specific product or software component and may be either procured or developed.

Reference Architecture. Architecture is the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. A reference architecture is a generalized architecture of a solution, based on best practices, domain neutral and, occasionally, with a focus on a particular aspect. The goal of a reference architecture is reusability; it reduces the amount of work, reduces errors and accelerates the development of solutions. A reference architecture is based in a reference model and in a style. The model covers the ontology of the components and their interrelationships, and in the case of the GIRA, it is ArchiMate®. The architecture style covers the architecture design principles and patterns and in the case of the GIRA it is "Service Oriented Architecture" (SOA). The focus of the GIRA is interoperability in GOU institutions.

Solution Architecture. Based on TOGAF®, a solution architecture is "a description of a discrete and focused business operation or activity and how information systems / technical infrastructure support(s) that operation. A Solution Architecture typically applies to a single project or project release, assisting in the translation of requirements into a solution vision, high-level business and/or IT system specifications, and a portfolio of implementation tasks". Within the context of the GIRA, the solution architecture describes the specific architecture of a solution. It can be derived from a solution architecture template.

Solution. A solution consists of one or more Solution Building Blocks to meet a certain stakeholder need. Within the context of the GIRA, a solution is usually an Interoperable GIRA Solution developed by public bodies that facilitates the delivery of electronic public services of information between public bodies, Citizens or Businesses, in support of the implementation and advancement of GOU public policies.

2.2. Key Interoperability Enablers viewpoint

The Key Interoperability Enablers viewpoint covers all e-GIF-2026 interoperability aspects: legal, organisational, semantic and technical. Ensuring interoperability when preparing legal instruments, organisation business processes, data/information/knowledge exchange, services and components that support Ugandan interoperable digital 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 public administrations, the business processes, and by the emergence of new technologies. This viewpoint is illustrated in Figure 9.

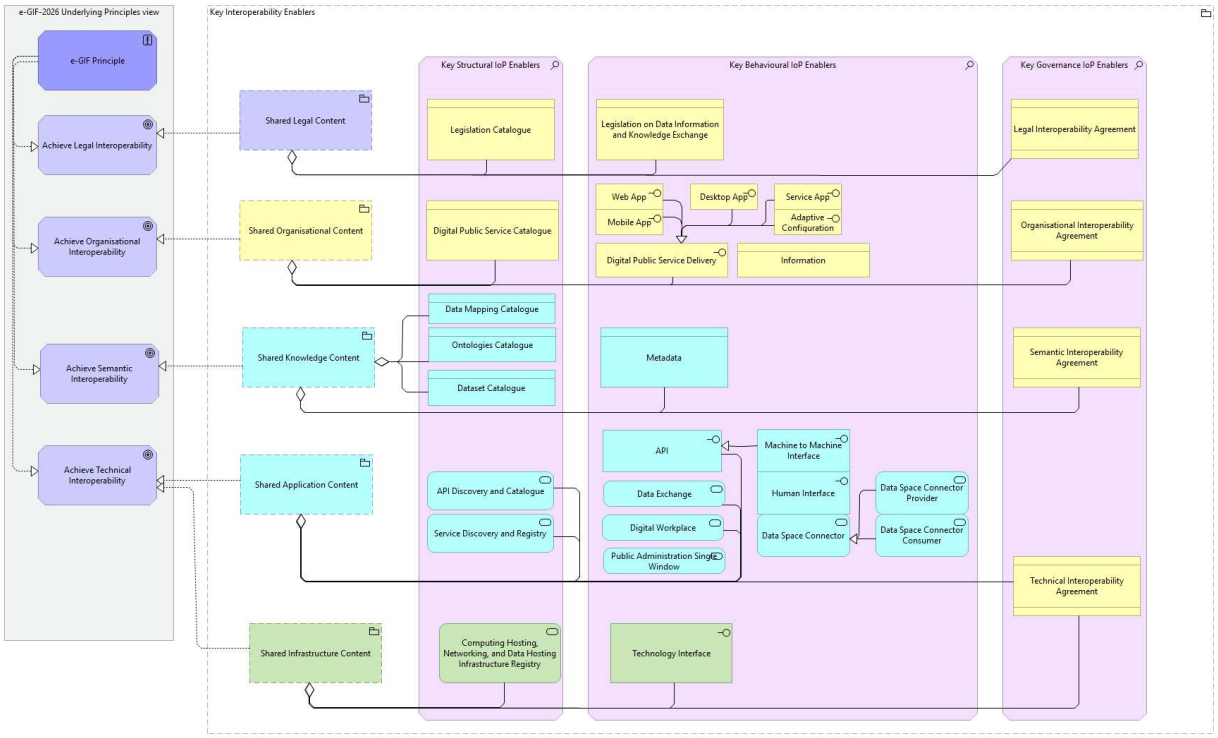

Figure 9 Key Interoperability Enablers viewpoint

2.3. Behavioural viewpoint

The Interoperability Behavioural viewpoint is in the European Interoperability Reference Architecture (EIRA) and its Ugandan adaptation GIRA. This viewpoint uses the ArchiMate© motivation extension to assess the behavioural interoperability readiness of a solution - specifically its ability to support the exchange of data, information, and knowledge with internal and external peers as illustrated in Figure 10. This viewpoint selects the specific Architecture Building Blocks (ABBs) from each of the four layers that are necessary to enable the efficient and effective exchange of information required for the delivery of integrated public services:

Legal Behavioural Interoperability: Focuses on the legal resources,[17] including legislation, that support the exchanging capabilities of data, information, or knowledge, ensuring they can be provisioned and consumed across different administrations and across borders.

Organisational Behavioural Interoperability: Focuses on the service delivery model, which acts as the enabler for data, information, or knowledge to be provisioned and consumed across different Ministries, Departments, and Agencies (MDAs).

Semantic Behavioural Interoperability: Focuses on metadata as the key enablers that ensure the meaning of data, information, or knowledge is preserved and understood when provisioned and consumed across heterogenous systems.

Technical Behavioural Interoperability: Focuses on the technical interfaces (such as APIs, data exchange, dataspace connectors) that provide the physical and logical means for data, information, and knowledge to be exchanged between digital public services and their users or other systems.

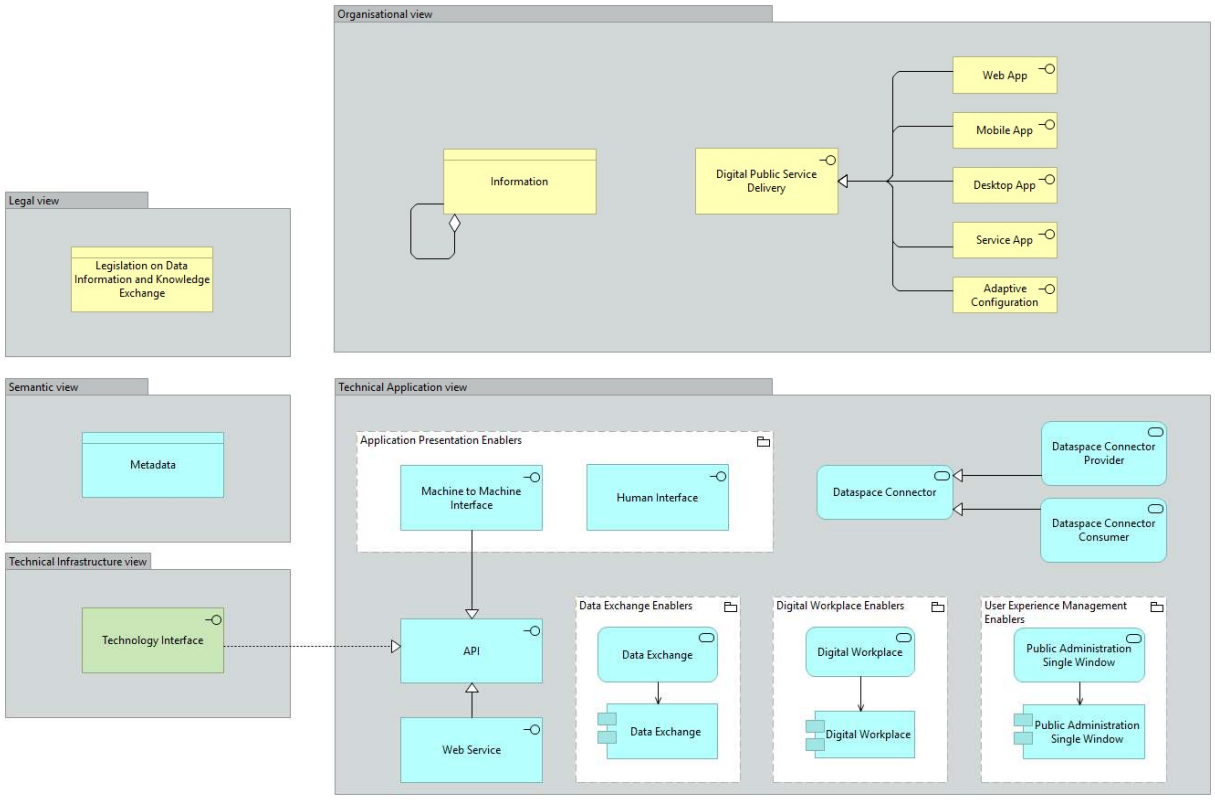

Figure 10 Interoperability Behavioural viewpoint

[17] Legal resources is a broader term. It refers to all materials that help understand, interpret, apply, or research the law. IT includes legislation (laws), court decisions (case law), legal textbooks and commentaries, guidelines, policy documents, legal databases (e.g., online law libraries). It may include both binding and non-binding materials.

2.4. High level viewpoint

The model in Figure 11 describes the architecture layers for every GOU administration as it is defined in e-GIF-2026. Additionally, every institution MUST have a crosscutting component of the four layers, an **"integrated public service governance"**. At the country level an additional background layer **"interoperability governance"** is needed. Comparison of content of the layers is depicted in Figure 12.

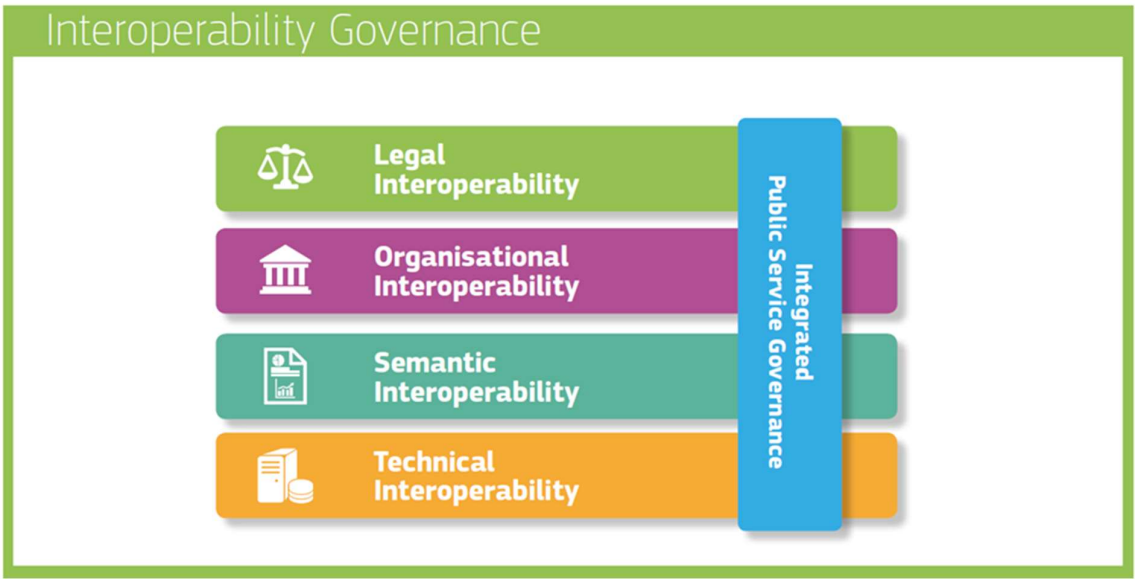

Figure 11 Interoperability model (picture taken from the e-GIF-2026 and the EIF)

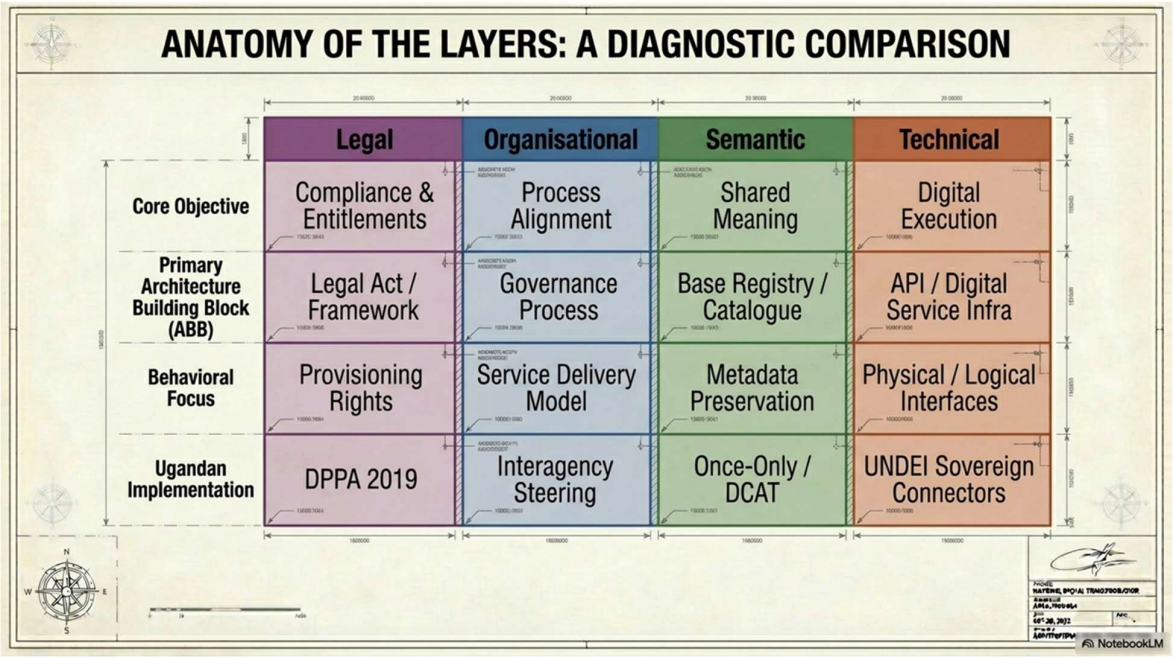

Figure 12 Comparison of content of the layers

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 the government level.

The high-level viewpoint of Ugandan interoperability reference architecture in a more formalised way is depicted in Figure 13.

The GIRA provides a set of Architecture Building Blocks, important to facilitate the interoperability of any GOU solution. Each view is represented by the Architecture Building Blocks needed to deliver an interoperable solution. The GIRA high level viewpoint is aligned with the terminology and recommendations of the eGIF-2026 and the EIRA©.

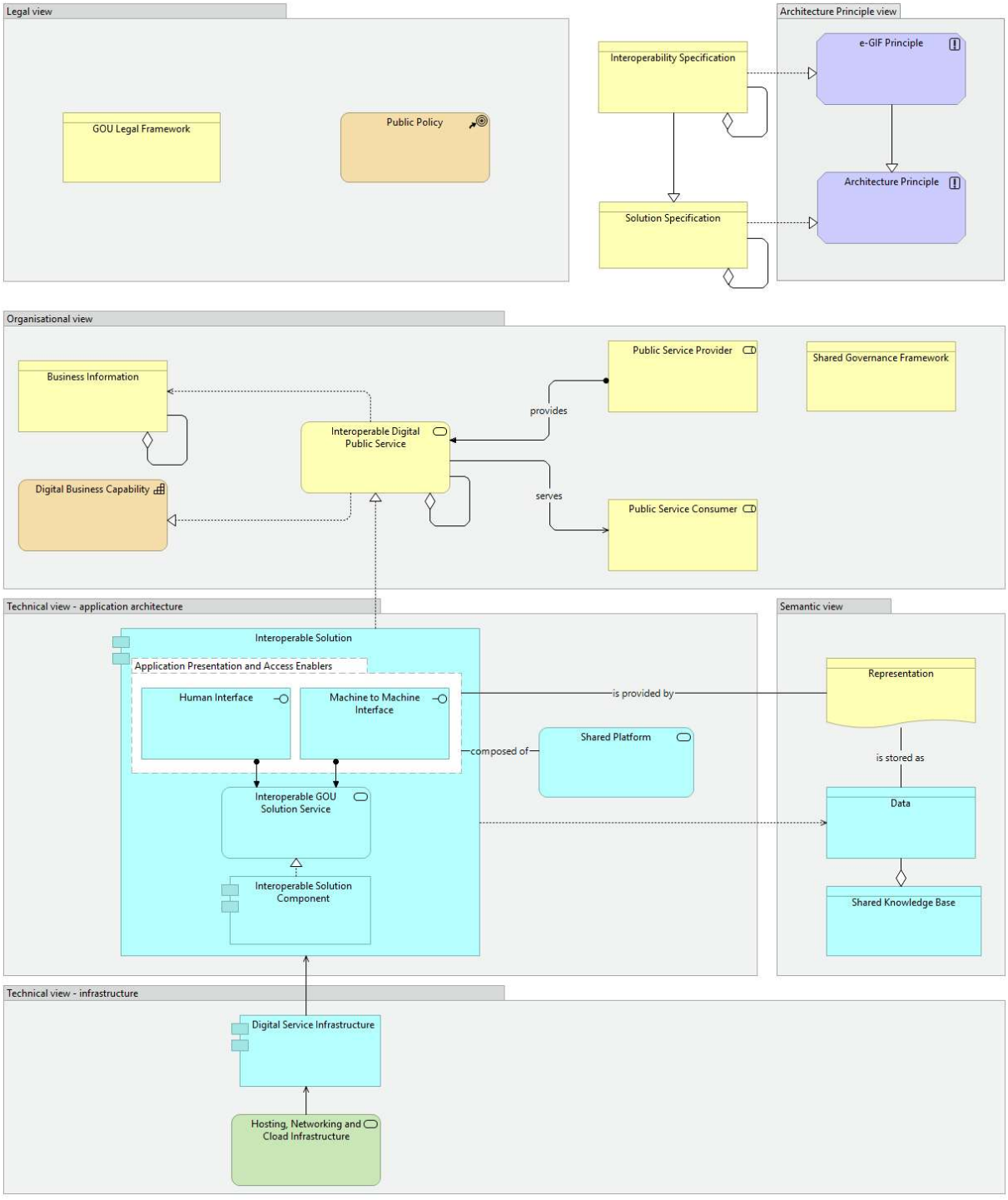

Figure 13 High level viewpoint

The high-level viewpoint is structured according to the following architectural views:

- **The Legal view.** The Legal view models the most salient public policy development enablers and implementation instruments that shall be considered to support the End-to-End design of interoperable digital public services. The legal view core ABBs are:
    - Legal Act ABB: is formalising a set of rules on a subject, potentially including requirements concerning digital public services.
    - Shared Legal Framework ABB: is setting legal (re)usable resources with convergence power, in relation to public policy goals attainment, enabling interoperability from a legal perspective.
    - Public Policy ABB: is a Course of Action allowing public authorities to bring social change in the medium and long term, in each area.
- **The Organisational view.** A Public Service can be an aggregation of other Public Services, serving Consumers and being provided by a Service Provider. The Public Service is realized by a Business Capability, which can be an aggregation of other Business Capabilities. The Organisational view core ABBs are:
    - Digital Public Service Delivery[18] Model ABB: is a Business Collaboration representing a collection of concepts related to the way in which the public sector delivers digital technologies to citizens and businesses.
    - Digital Public Service ABB: is a Business Service supporting the realization of a Public Administration digital business capability, provisioned via a digital service delivery mode by, or on behalf of, a public administration.
    - Digital Business Capability ABB: is a Capability enabling public administrations to digitally perform an administrative function.
- **The Semantic view.** The Semantic view models the most salient Architecture Building Blocks that should be considered to support semantic aspects for the End-to-End design of interoperable digital public services.
- **The Technical - Application view.** The application view contains the most important application Architecture Building Blocks that need to be considered to support technical aspects for the end-to-end design of Interoperable GOU Solutions. The technical view core ABBs are:
    - Interoperable Digital Solution ABB: is an Application Component enabling the delivery of a digital public service, in fulfilment of a shared legislation framework, being managed according to a shared governance framework, accessing semantic assets in a shared knowledge base and using digital resources of a shared platform enabling cross-organisation exchange of data, information, and knowledge indistinctly between the GOU public administrations, businesses and citizens.
    - Shared platform ABB: is an Application Component setting technical (re)usable resources with convergence power, in relation to public policy goals attainment, enabling interoperability from a technical perspective cross level in a GOU public

[18] OECD Digital transformation of public service delivery: https://read.oecd-ilibrary.org/governance/government-at-a-glance-2017/digital-transformation-of-public-service-delivery_gov_glance-2017-72-en#page2

administration. Examples: Digital Authentication and Electronic Signatures Solutions (UGPass), Data Space Infrastructure, Secure Data Exchange infrastructure, Catalogues, Integration Service (UGHub), SMS Gateway, NITA-U National Data Centre, Electronic One Stop Centre Web Portal (eBiz) for businesses, etc.

- **The Technical -Infrastructure view.** The Technical -Infrastructure view provides an architecture content metamodel for the most important cross-sectorial infrastructure services, along with the supporting hosting and networking facilities, which shall be considered to support technical aspects for the end-to-end design of interoperable GOU solutions. The difference with the application part of the technical view is that the Architecture Building Blocks in the infrastructure view are relevant to solutions in any sector of the government.

2.5. Conceptual model viewpoint

The GOU e-GIF-2026 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 GIRA is aligned with the e-GIF conceptual model. This model in terms of ArchiMate is depicted in Figure 14.

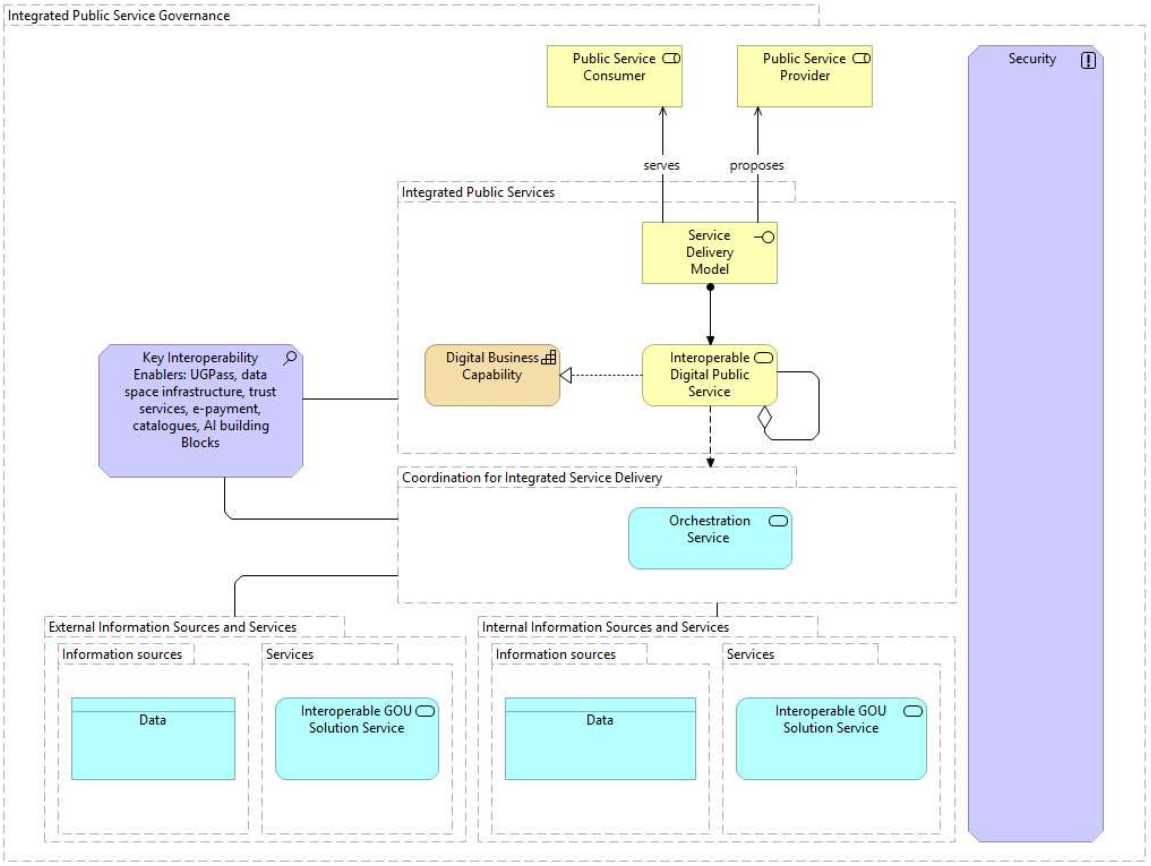

Figure 14 Conceptual model for integrated public services

The Conceptual Model promotes reusability as a driver for interoperability (interoperability by design), recognising that the GOU's public services should reuse information and services that already exist and may be available from various sources inside or beyond the organisational boundaries of the MDAs. Information and services should be retrievable and be made available in interoperable formats. Security and privacy requirements should be considered and measures for the provision of each public service according to risk management plans. Trust services should ensure secure and protected data exchange in public services.

The renewed aspects of Conceptual Model arising from need to shift to the Data Space model and add AI enabler. The most prominent changes are characterised in following sections.

2.5.1. Shift from Centralized to Federated Architecture

The GovStack Architecture[19] distinguishes five types of Whole-of-Government architecture patterns as sown inFigure 15:

- Wild - Fragmented Point-to-Point Integration Architecture
- Monolithic - Fully Centralized Monolithic Architecture
- Centralized Service Oriented Architecture - Oriented around a Central Gateway
- Semi-Decentralized Service Oriented Architecture - Oriented around decentralized domain gateways
- Fully Decentralized Event Driven Microservice Architecture - Oriented around domain messages and their message rooms

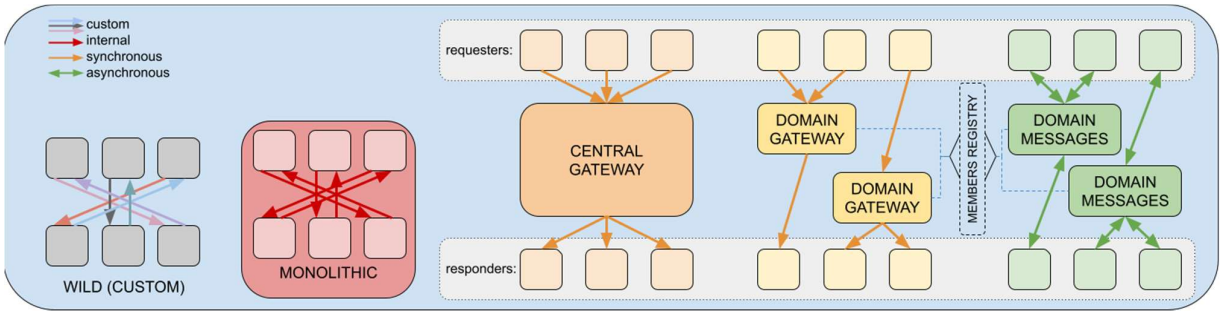

Figure 15 Five architecture patterns by GovStack

Domain/sector/MDA is important for governance because the people responsible for the domain - domain experts know the terminology, data classifications, workflows, and business rules best.

[19] https://specs.govstack.global/architecture/4-interoperability-architecture/4.3-architecture-patterns

Patterns deeper analyse (by Kristo Vaher)[20] shows weaknesses and strengths these patterns. Each administration should choose a pattern that suits him. Recommended patterns for Uganda:

- Sector specific systems could use internally central gateway approach. But their Domain Gateway Should be interacted with the other sectors by using sovereignty connectors.
- On WoG level Uganda moves away from centralized "hub-and-spoke" models toward a Federated Data Space architecture, utilizing distributed Sovereign Connectors to ensure data remains at its source while being securely accessible.
- The wild and monolithic architecture can be used if possible: for example, in open data ecosystem

To achieve the resilience and sovereignty required by a modern digital state, the Government of Uganda SHOULD transit its integration layer from the legacy centralized UGHub to the Ugandan National Data Exchange Infrastructure (UNDEI). This change is not merely cosmetic; it represents a fundamental architectural evolution required to achieve the goals of GIRA-2026 and e-GIF-2026.This infrastructure serves as the Secure Data Exchange ABB, utilizing a federated model of Sovereign Connectors to ensure that data remains at its source. The following points summarize the key justifications for this transition:

1. Moving from a "Hub" to a Federated Data Space. The current name, "UGHub," signifies a centralized "hub-and-spoke" model where all data must pass through a single facility. This creates several business and technical risks that the new infrastructure (UNDEI) addresses:

- **Eliminating Single Points of Failure (SPOF):** A centralized hub acts as a bottleneck and a high-value target for cyberattacks. Transitioning to UNDEI signals a shift to a distributed infrastructure where data remains at its source with the custodial agency, enhancing national resilience.
- **Enabling Data Sovereignty:** Independent ministries often reject centralized models due to concerns over losing control of their data. UNDEI utilizes Sovereign Connectors, allowing MDAs to "grant access" rather than "give up" their data, thereby ensuring absolute control through machine-readable usage policies.

2. Decoupling Data Exchange from Service Orchestration. Renaming to UNDEI allows for a clear functional separation of duties within the national architecture as depicted in Figure 16:

- **UNDEI as the Secure Layer:** This component will focus exclusively on the Secure Data Exchange (SDE) layer, providing the "digital rails" for secure peer-to-peer data transport.
- **UGHub as the Orchestration Logic:** The term UGHub can be repurposed to refer specifically to the Orchestration Component, which defines the sequence and conditions (workflows) in which services invoke one another to realize useful functions.

[20] https://interopframework.com/architecture-comparisons-v2.pdf

- **Business Function Alignment:** According to international standards like GovStack, technical changes should be driven by business functions rather than programmer preference. Decoupling these functions ensures that data ownership (a business function of UNDEI) is not compromised by service complexity (the logic function of UGHub).
- If Uganda decides to continue with the historical name "UGHub", for maintain a clear architecture the transport and logic tiers should be separated.
    - We use term UGHub/UNDEI (UNDEI – Ugandan National Data Exchange Infrastructure) for Ugandan WoG Secure Data Exchange (SDE) layer which ensures peer-to-peer transport between UNDEI members.
    - The term UGHub/orchestration denotes platforms used for orchestration services. Technically it is previous UGHub solution which can be used/reused on central and sectoral levels.

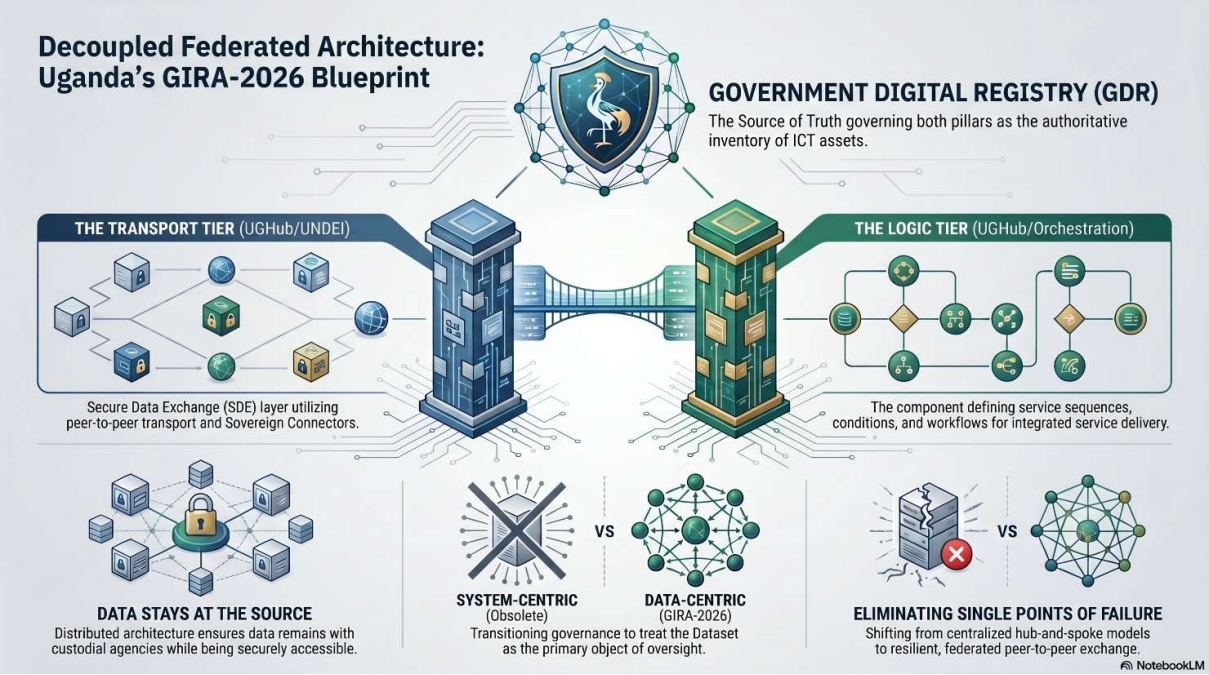

Figure 16 Decoupled Federated Architecture

3. Strengthening Trust through Non-Repudiation. A critical limitation identified in the current hub model is the absence of non-repudiation.

- **Evidence of Exchange:** UNDEI is designed to implement "Evidence of Exchange" receipts signed via the National PKI.
- **Legal Certainty:** Renaming the facility to an "Infrastructure" emphasizes its role as a legally binding foundation that provides undeniable proof of origin and receipt for every transaction.

4. Facilitating Cross-Border and Regional Integration. Uganda's strategic visions (Vision 2040 and the Digital Transformation Roadmap) emphasize regional integration.

- **Compatibility:** While the current hub model does not natively support cross-border exchange, UNDEI is explicitly designed to be compatible with EAC, COMESA, and AfCFTA digital protocols.
- **Global Standard Positioning:** Transitioning to a "National Data Exchange Infrastructure" aligns Uganda with international best practices for Federated Research Infrastructures and European Health Data Spaces, positioning the nation as a leader in the regional data economy.

5. Terminology Alignment and Silo-Busting. Standardized terminology is a key requirement for building the Ugandan GEA.

- **Eliminating Jargon:** Renaming helps eliminate communication silos between MDAs that may operate with domain-specific "jargon".
- **The "Data-Centric" Paradigm:** Renaming signals to all stakeholders that the government is moving away from a "system-centric" view (where the hub is just a piece of software) to a "data-centric" view where data is treated as a strategic public asset regardless of the underlying hosting system.

2.5.2. Strengthened Trust and Security

Cryptographic Non-Repudiation: Implementing "Evidence of Exchange" receipts signed via the National PKI. This ensures undeniable proof of origin and receipt for every transaction.

Data Sovereignty: MDAs maintain absolute control over their primary registries, using machine-readable Usage Control Policies (ODRL)[21] to dictate how, when, and by whom their data is used.

Privacy by Design: Ensuring data is only accessed for specific, authorized purposes.

2.5.3. Interoperability by Design

Mandatory Standards: Interoperability is a pre-requisite for all new IT projects, not an afterthought.

Semantic Layer: Reuse a meaning of data from Base Registries, implement DCAT[22] for metadata to ensure all systems "speak the same language" natively.

Reusable Blocks: Using standardized, open-source connector stacks to lower the barrier for MDA and LGs participation.

---

[21] ODRL Information Model 2.2: https://www.w3.org/TR/odrl-model/

[22] Data Catalog Vocabulary: https://www.w3.org/TR/vocab-dcat-3/

2.5.4. Strategic and Global Alignment

Once-Only Principle: The architecture is the primary engine ensuring citizens only provide information to the government once.

Cross-Border Ready: Designed to be compatible with EAC (East African Community) and AfCFTA digital protocols, facilitating secure data exchange across borders.

NITA-U's Role: Shifting from an "Operator" of a central hub to a "Scheme Regulator" of the Data Space standards and trust framework

2.5.5. AI enabler

In the Conceptual Model for Integrated Public Services, AI is integrated through the following mechanisms:

- **Conversational Interfaces:** The architecture recommends replacing traditional menu-based portals with AI-driven conversational interfaces to improve user experience.
- **AI-Enabled Shared Enablers:** AI is explicitly incorporated as a reusable building block for document intelligence and decision support systems.
- **Human-in-the-Loop (HITL):** For any service utilizing AI for decision support, the architecture mandates a human-in-the-loop requirement to ensure accountability.
- **Reproducibility and Continuity:** GIRA-2026 requires that digital continuity be considered for AI reproducibility and within cloud/edge pipelines.

The integration of Artificial Intelligence into public administration marks a strategic shift from legacy static architectures to **agent-based infrastructure**. This transition positions AI as a **"compliant participant"** within the digital ecosystem, designed to enhance the capacity of systems to exchange and interpret information across all interoperability layers. The e-GIF-2026 framework moves beyond basic automation toward determinism, orchestration, and trust as the primary goals for AI-driven public services.

2.5.5.1. Principles for AI Implementations

Recommended principles for AI implementations:[23]

- **The Principle of Non-Dependency.** AI is an additive layer, not a structural foundation. Systems must be architected to function deterministically without artificial intelligence.
- **The Principle of Retained Authority.** Autonomy is delegated, not absolute. For all critical processes, architecture must enforce a mandatory "break point" for human review.
- **The Principle of Radical Observability.** If it cannot be traced, it cannot be automated.

[23] https://specs.govstack.global/ai-readiness/principles-for-ai-implementations

- **The Principle of Semantic Unity.** Interoperability is a linguistic, not just technical, requirement. To prevent fragmentation, systems must strictly adhere to shared vocabularies and data contracts.
- **The Principle of Bounded Delegation.** Identity must be bound by scope and time. Simple session authentication is insufficient for autonomous agents.
- **The Principle of Executable Governance.** Policy must be machine-readable and self-enforcing. Governance cannot rely on manual compliance. Regulatory rules (e.g., data retention, access limits) must be translated into "Policy-as-Code" and enforced automatically by the infrastructure at the API Gateway level.
- **The Principle of Contextual Alignment**. Architecture must engineer trust to overcome cultural resistance. Technical design must account for local "data hugging" cultures and legal frameworks.

2.5.5.2. Ethical Framework: Ethics-by-Design and Transparency

To foster integrity and public confidence, administrations must adopt an **"ethics-by-design"** approach, integrating human values throughout the entire AI lifecycle:

Algorithmic Transparency: Transparency is expanded to include **algorithmic explainability.** Any automated or AI-assisted decision that affects citizen rights or benefits must be understandable, auditable, and aligned with the rule of law.

Human-in-the-Loop (HITL): Complex decision-support systems must maintain a mandatory **human-in-the-loop** requirement to ensure meaningful human oversight and accountability for automated outcomes.

Bias and Fairness: AI components, such as those used for intelligent service personalization, must undergo rigorous **bias testing** to ensure inclusivity and prevent the marginalization of disadvantaged groups.

2.5.5.3. Governance Model: Policy as Code

Governance of AI-ready systems is managed through a "**Policy as Code"** model, where regulatory requirements are embedded directly into the orchestration and integration fabric.

Mandatory Registration: All AI-enabled components, including document intelligence and multilingual assistants, must be registered in the **Catalogue of Interoperable Solutions** to ensure statutory recognition and oversight.

Model Cards: To ensure traceability, every AI service must publish model cards that detail the model's intent, data provenance, and performance characteristics.

2.5.5.4. Risk Management and Resilience

Administrations must maintain comprehensive risk registers specifically for the legal, organizational, and technical dimensions of AI:

- **Monitoring and Drift Detection:** Implementation requires continuous observability, utilizing AI-driven tools to detect "semantic drift" (changes in data meaning over time) and performance anomalies in real-time.
- **Incident Escalation:** Robust procedures must include rollback or disable protocols for automated decisions and mandatory incident post-mortems to facilitate cross-border and cross-sectoral learning.
- **Sovereignty and Exit Strategies:** To mitigate the risk of vendor lock-in, administrations should prioritize open-source AI models and develop risk-based exit strategies to ensure service continuity regardless of external provider shifts.

2.5.5.5. Recommendations

Service Catalogue. For autonomous agents to navigate a complex government landscape, they require a centralized directory/catalogue. Just as a human needs a contact list to find the right department, a software agent needs a "Phonebook" to discover which services are available and how to use them. Governments must therefore implement a centralised Catalogue system.

The "Human-in-the-Loop" Handover Protocol. Autonomy is not absolute. There will always be edge cases where an AI agent lacks the confidence or the authority to proceed. To handle this safely, Uganda must standardize the "Human-in-the-Loop" protocol. This is a technical handshake that defines exactly how a machine delegates back to a civil servant when it encounters ambiguity.

Procurement and Vendor Requirements. To ensure that new systems are compatible with this agentic future, we must update the legal language of our contracts. The most powerful lever for change is the procurement requirement. The specific, non-negotiable clauses into all future tenders to mandate AI Readiness SHOULD be inserted, like:

- Delivered software must provide Open API 3.1 specifications. This ensures that every new piece of software comes with a machine-readable manual by default.
- System must comply with GIRA requirements. This shifts the burden of proof to the vendor, requiring them to demonstrate interoperability before the contract is signed.

2.6. Interoperability Specification viewpoint

An Interoperability Specification is a document formulated as an agreed normative statement in design terms on a legal, organisational, semantic, or technical attribute. It can refer to existing standards or specifications.

The Interoperability specification viewpoint models the most salient Architecture Building Blocks that shall be considered when providing interoperability specifications. It provides an overview of Architecture Building Blocks from the different views and depicts them as a taxonomy of interoperability specifications. Each GIRA view has Architecture Building Blocks that support interoperability.

Each view's interoperability specifications serve to define the interoperability aspects of catalogues and registries. Given the linked nature of the GIRA views, the interoperability specifications from all

views can be considered to affect each individual catalogue or registry. However, the focus in each case is kept within the specific view to best capture the level of detail that each view's specifications deal with.

An Interoperability Specification is a Specification and can be composed of other Interoperability Specifications. This viewpoint selects Architecture Building Blocks from the five different views highlighting the interoperability specification related Architecture Building Blocks of the GIRA.

Interoperability Specification viewpoint is depicted in Figure 17.

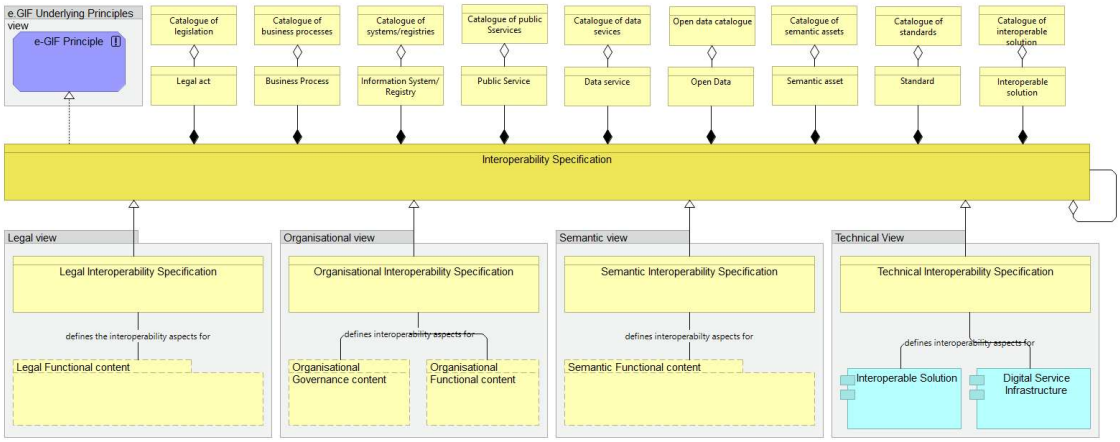

Figure 17 Interoperability Specification viewpoint

3.Architecture Principles

The Architecture Principles define the underlying general rules and guidelines for the use and deployment of all IT resources and assets across the GOU. They reflect a level of consensus among the various elements of the GOU and form the basis for making future IT decisions.

The GIRA's architecture principles aligned with the GOU Interoperability Framework (e-GIF-2026). The European Library of Architecture Principles (ELAP)[24], the OECD Digital Government Policy Framework[25], EU strategies and digital governments development trends have been considered in the selection of the most suitable to the GOU's context principles. Six types of architecture principles are distinguished as depicted in Figure 18:

- The e-GIF-2026 underlying principles
- Digital Public Service Strategy
- Digital Public Service Design
- Digital Public Service Operations
- Improvement architecture
- Solution Architecture Principles

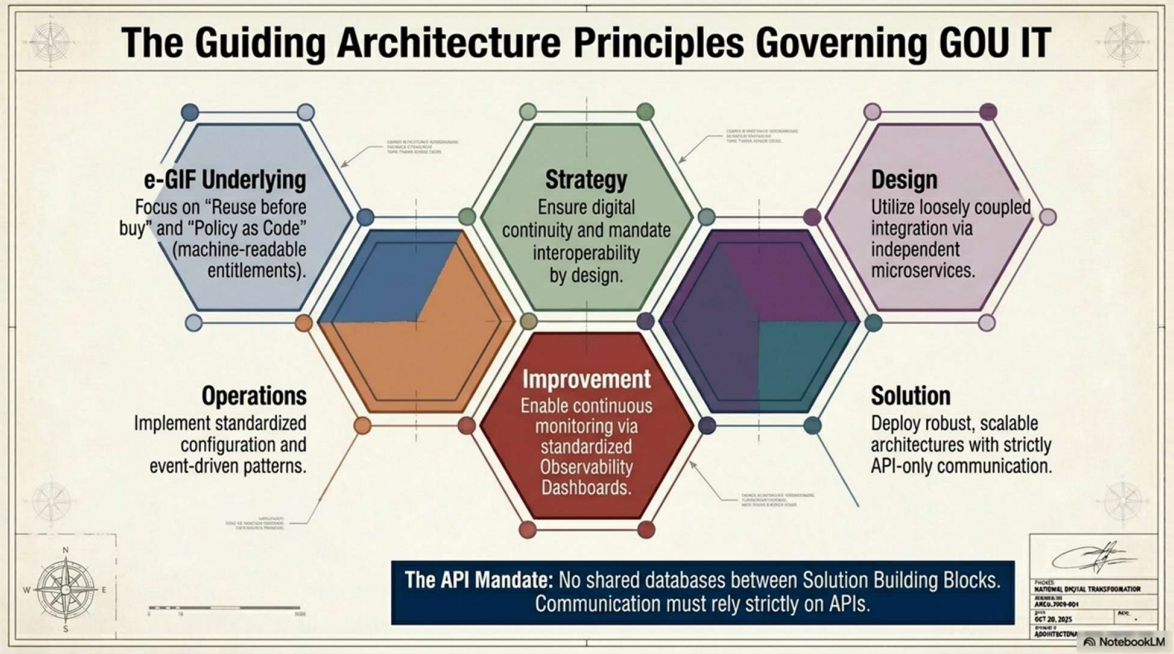

Figure 18 GIRA-2026 Architecture Principles

---

[24] https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elap/release/120

[25] https://read.oecd.org/10.1787/f64fed2a-en?format=pdf

3.1. Interoperability underlying principles

Public sector interoperability enables administrations to cooperate and make public services function across sectors and across organisational boundaries. The interoperability principles are fundamental behavioural aspects to drive interoperability actions. The twelve underlying principles and requirements arising from them are thoroughly described in the e-GIF-2026. Here they are briefly presented:

- **Subsidiarity and proportionality.** The subsidiarity principle requires GOU decisions to be taken as closely as possible to the citizen.
- **Openness.** In the context of interoperable public services, the concept of openness mainly relates to data, specifications and software.
- **Transparency.**
    - Enabling visibility inside the administrative environment of a public administration. This is about allowing other public administrations, citizens, and businesses to view and understand administrative rules, processes, data, services, and decision-making.
    - Transparency additionally applies to automated decision making, AI and algorithmic outputs, and data sharing policies.
    - Ensuring the availability of interfaces with internal information 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 Administrations.
- **Reusability.** This requires the Administration to be open to sharing its interoperability solutions, concepts, frameworks, specifications, tools, and components with others.
- **Technological neutrality and data portability.** When establishing information systems and services, Administrations SHOULD focus on functional needs and defer decisions on technology as long as possible, to avoid imposing specific technologies or products on their partners and to be able to adapt to the rapidly evolving technological environment.
- **User-centricity.** User needs SHOULD be considered when determining which public services should be provided and how they should be delivered.
- **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. Equitable access to digital services includes also:
    - AI model fairness.
    - Accessible machine generated summaries.
    - Cross language support in automated processing.
- **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.
- **Privacy.** Administrations MUST guarantee the citizens' privacy, and the availability, confidentiality, authenticity, integrity and non-repudiation of information provided by citizens and businesses.
- **Multilingualism.** Multilingualism and linguistic neutrality come into play not just at the level of the user interfaces, but at all levels of design of public services. The multilingual AI tools and multilingual data-exchange layers SHOULD be considered in service interfaces.

- **Administrative simplification.** Administrations SHOULD seek to streamline and simplify their administrative processes by improving them or eliminating any that do not provide public value.
- **Preservation of information.** Records and information in electronic form held by Administrations, for the purpose of documenting procedures and decisions, must be preserved and be converted, where necessary, to new media when old media become obsolete.
- **Assessment of effectiveness and efficiency.** Administration 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.

3.2. Digital Public Service Strategy Principles

- **Digital First/Digital by design.** Making public services digital makes them more accessible, reduces administrative burdens and time, and allows faster responses to individuals and organizations.
- **Data-driven public sector.** A data-driven public sector recognises and takes steps to govern data as a key strategic asset in generating public value through their application in the planning, delivering and monitoring of public policies, and adopts rules and ethical principles for their trustworthy and safe reuse.
- **Government as a platform.** A government acts as a platform for meeting the needs of users when it provides clear and transparent sources of guidelines, tools, data and software that equip teams to deliver user-driven, consistent, seamless, integrated, proactive and cross-sectoral service delivery.
- **Open by default.** A government is open by default when it makes government data and policy-making processes (including algorithms) available for the public to engage with, within the limits of existing legislation and in balance with the national and public interest.
- **User-driven.** A government becomes more user-driven by awarding a central role to people' needs and convenience in the shaping of processes, services and policies; and by adopting inclusive mechanisms for this to happen.
- **Proactiveness.** Proactiveness represents the ability of governments and civil servants to anticipate people's needs and respond to them rapidly, so that users do not have to engage with the cumbersome process of data and service delivery.
- **Data Sovereignty**. Ability of stakeholders involved in the delivery of public services to have full control over the shared data.
- **Digital sovereignty and autonomy.** Digital sovereignty and autonomy. Digital infrastructures, products and services safeguard the GOU's security, strategic assets and interests, while respecting Ugandan values and requirements, and preventing external stakeholders to the monopoly (lock in) to the solutions.
- **Trustworthy and secure**: Systems must be backed by robust technical and legal frameworks and tools, so they work using reliable information and gain the trust of users.
- **Open and transparent**: Institutions should strive to make their data open by default and improve engagement with citizens to encourage transparency and accountability.
- **Social participation**. Promoting Civic Participation and Transparency of Government Decision-Making Processes covering policies concerning ICT.
- **Care from cradle to grave.** A full life cycle cost of ownership (including retirement costs) should form part of the business case.

3.3. Digital Public Service Design Principles

- **Once only**. The Once Only Principle entails that citizens and businesses provide diverse data only once in contact with public administrations, while public administration bodies take actions to internally share and reuse these data always in respect of data protection regulations and other constraints.
- **Service Orientation**. Service orientation is a way of thinking in terms of services and service-based development and the outcomes of services. Applications/microservices SHOULD get data of other applications/microservices over services. Direct access to the data of other applications/microservice SHOULD be avoided.
- **User-centricity**. User-centricity refers to putting the users' needs at the centre when determining which public services should be provided and how they should be delivered.
- **Proactiveness**. Proactiveness refers to proactive services, which are public services that a public institution delivers following its own initiative, without prior request from an individual.
- **Reuse, before buy, before build.** Re-use first: existing IT systems and services, already acquired, should be re-deployed prior to considering buying new systems, or at worst case, building new systems.
- **Policy as Code.** Wherever feasible, policies, rules, and entitlements should be expressed in machine-readable form, enabling consistency, automation, and transparency across systems
- **Loosely coupled integration**. Each organization serves a unique part of the application process. Loosely coupled architecture is an architectural style where the individual components of an application are built independently from one another. Each component or microservice, is built to perform a specific function in a way that can be used by any number of other services. A loosely coupled system is one[26]
    - in which components are weakly associated (have breakable relationships) with each other, and thus changes in one component do not affect the existence or performance of another component.
    - in which each of its components has, or makes use of, little or no knowledge of the definitions of other separate components.
    - Loose coupling is the opposite of tight coupling.

3.4. Digital Public Service Operations

- **Security by Design** (SbD). Security should be built into a product by design, instead of being added on later by third-party products and services.
- **Data Interoperability.** Datasets metadata machine-readable format, vocabularies reused, and reference to other datasets and their metadata. Data format should be readable for machines without the need for specialised or ad hoc algorithms, translators, or mappings. Data does not exist in isolation but is highly dependent upon other data that is available from other parties. Data should also be reused, when possible, to prevent collecting the same data twice and introducing duplication, with the risk of inconsistency. Controlled vocabularies define the terms in a specific domain, standardising their interpretation. These concepts are the foundation for data, providing definitions and meaning to them. It is important for users of

[26] Loose Coupling: https://en.wikipedia.org/wiki/Loose_coupling

data to have access to these definitions, so they can correctly interpret the data. The usage of standardised methods for the representation of metadata (RDF, OWL, DAM+OIL, JSON LD). In the metadata of datasets, references are made to the metadata of other datasets that the dataset depends upon. The data model of the dataset refers to the data model and the specific data elements and definitions that are reused from other datasets. The data itself includes identifiers to data in other datasets that the data depends upon.

- **Data Reusability.** Metadata and data should be well-described so that they can be replicated and/or combined in different settings.
- **Data Accessibility.** Data and metadata availability through standardised mechanism and ensure its long-term availability Data retrieval should be mediated without specialised or proprietary tools or communication methods.
- **Trust.** Trust entails the reliance of citizens on trustworthy and verifiable digital government applications and services.
- **Preservation of Information.** Decisions and data are stored and can be accessed for efficient retrieval and use.

3.5. Improvement Architecture

- **Innovation.** Innovation entails rethinking organizations and processes and changing behaviour so that public services are delivered more efficiently to people.
- **Emerging technologies.** Supporting cooperation in the adoption of emerging technologies (for example Artificial intelligence, Internet of things, Data analytics, Automation and Robotics, Cloud computing, etc).

3.6. Solution Architecture Principles

Although the Solution Architecture is out of scope of the Reference Architecture, it is appropriate to state some general principles here. It is recommended to outline cross-functional (non-functional) requirements for solution architecture, for example on basis of UN GovStack initiative.[27] The same document gives following principles for building blocks design:

- **Open**
  - Based on open standards
  - Based on Digital Development Principles, see https://digitalprinciples.org/ and https://digitalinvestmentprinciples.org/.
  - Built on open-source software (where possible).
  - Supports open development, see https://standard.publiccode.net/.
  - No vendor lock-in.
  - Cloud native (Docker/Docker Compose/OCI containers).
  - Code is openly developed and available to anyone, via Github or Gitlab.
- **Sustainable**
  - Stewardship is critical, see https://publiccode.net/codebase-stewardship/ .

[27] Architecture and Nonfunctional Requirements: https://docs.egovstack.net/v1.1.0/Architecture_and_NonFunctional_Requirements_v1.1.0.pdf

    - Continuous funding for maintenance, development and evolution.
    - Attractive to ICT industry and individual developers in deployment environment (incentives must be aligned).
    - Lower cost than commercial solutions due to shared development costs.
    - Uses microservices-based architecture instead of monolithic.
- **Secure**
    - Blocks are audited and certified before being made available.
    - Development processes and standards enforce quality and security.
    - Different certification levels reflect level of standards-compliance.
    - Regular security scanning and auditing.
    - Public ratings and reviews.
    - Comprehensive logging and exception handling.
- **Accessible**
    - Meets users where they are: web, mobile, SMS and/or voice. UI supports accessibility technologies, e.g., screen readers.
    - SSO allows for signing in once for multiple services.
    - Shared ownership of code.
    - Deployment and development processes and standards are open to contributors.
    - Community-driven development tools for documentation and support.
    - Blueprints, templates and documentation.
- **Flexible**
    - Blocks can be reused in multiple contexts.
    - Each block is autonomous: blocks are interoperable, blocks are easy to set up.
    - Standardized configuration and communications protocols connecting blocks.
    - Blocks can be provided as a service (ICT opportunity).
- **Robust**
    - Operates in low-resource environments: occasional power, low bandwidth, low-reliability connectivity.
    - Easily scalable for high availability and reliability.
    - API-only based decoupling.
    - Asynchronous communications pattern decoupled through rooms is ideal.
    - Eventual consistency for data.

4. Legal view

The GIRA Legal View models the most important public policy development enablers and implementation instruments that shall be considered to support the End-to-End design of interoperable digital public services.

Figure 19 illustrates the most important ABBs of legal architecture.

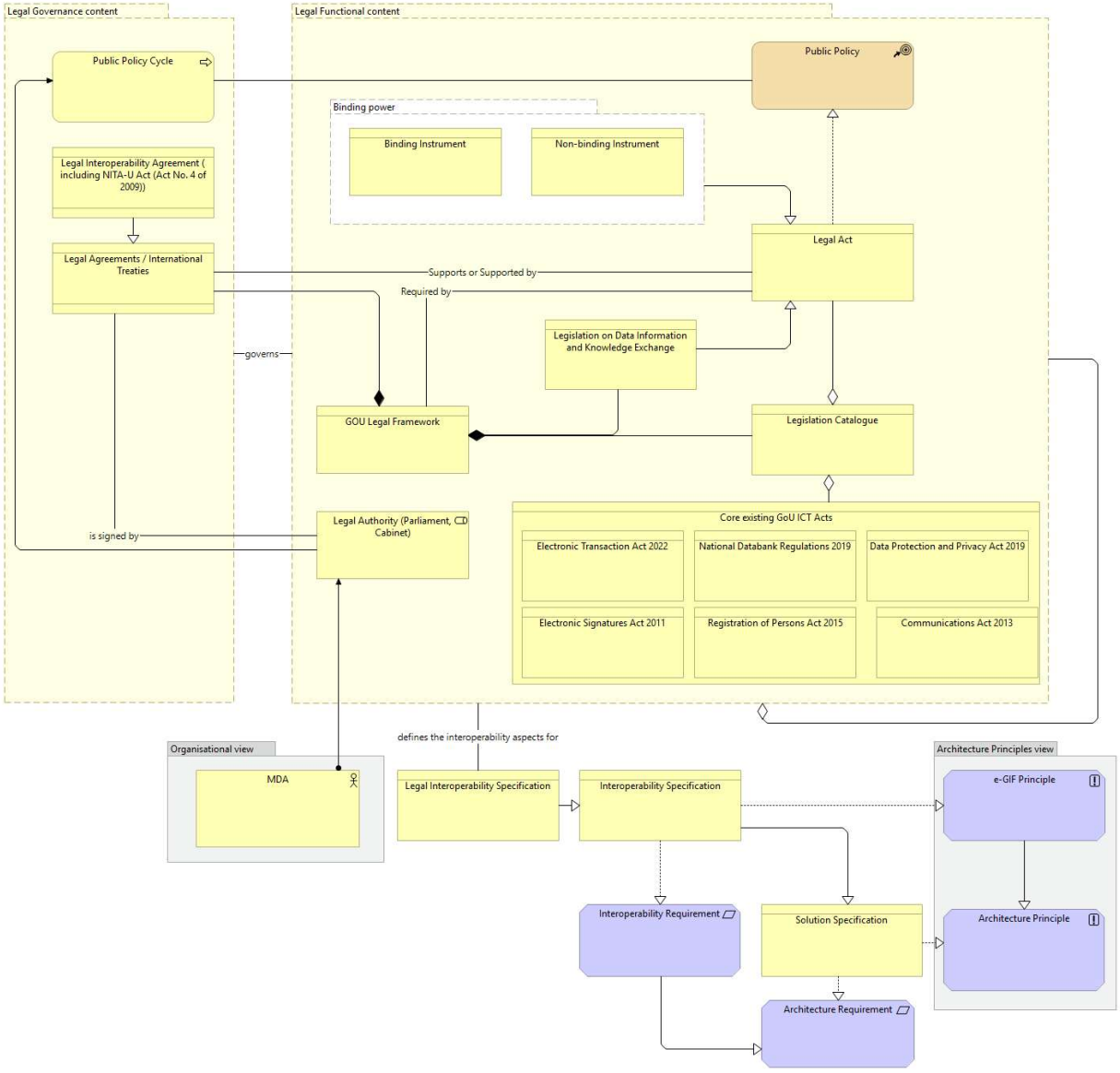

Figure 19 GIRA Legal view

4.1. Baseline legal interoperability architecture

Uganda has a legal framework for e-government in place. The focus should be on ensuring that the existing legislation is properly implemented and relied on NITA-U e-government regulations.

NITA-U is the designated authority for eGovernment development in Uganda. However, its current mandate requires legislative clarification in two respects: first, to define the boundaries of its regulatory role and prevent regulatory overreach; and second, to strengthen its authority to promote, coordinate, and enforce interoperability standards across government

The basic legal framework for enabling interoperability appears to be in place, including essential rules about datasets, information systems and their interoperability. Although the essential basics of recognising electronic transactions and identities is handled via the relevant laws, the laws do not make it mandatory for government agencies. Additional rules may need to be issued.

Uganda has recent data protection legislation, which introduces the modern best practice of general data protection legal framework rather than provisions in various sectoral laws.

ICT related legal acts:

- **The Access to Information Act 2005 (ATIA) in Uganda**[28] grants citizens, residents, and non-residents the right to access information held by public bodies, promoting government transparency, accountability, and citizen participation. Article 41 of the 1995 Constitution, allowing access to records in government ministries, departments, and local governments, subject to exemptions like national security, cabinet secrets, and personal privacy. It defines the right to access information held by the state, including the right for citizens to request and receive that information in **electronic formats.**
- **Electronic Transactions Act 2011**:[29] Its primary goal is to provide for the use, security, facilitation and regulation of electronic communications and transactions; to encourage the use of e-Government services and to provide for related matters.
- **Electronic Signature Act 2011**[30] The Act regulates the use of electronic signatures and related digital authentication methods in Uganda. It aims to establish legal recognition, standards, and procedures for electronic signatures, digital signatures, and public key infrastructure (PKI). Defines essential terms such as electronic signature, digital signature, advanced electronic signature, secure signature creation device, private and public keys, and certificates. Clarifies the legal equivalence of digital signatures to handwritten signatures and their enforceability

[28] http://judiciary.go.ug/files/downloads/access%20to%20informatioinformation%20Act2005.pdf

[29] https://www.nita.go.ug/publication/electronic-transactions-act-2011-act-no-8-2011

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

- **Electronic Signatures Regulations 2013 - SI 43 of 2013**[31]. It outlines the regulations and requirements for electronic signatures, certification service providers, licensing, and related procedures in Uganda.
- **Data Protection and Privacy Act 2019**: This Act protects the constitutional right to privacy by regulating the collection and processing of **personal information** and establishing the Personal Data Protection Office (PDPO)
- **Computer Misuse Act 2011**:[32] It defines cybercrime offenses and explicitly recognizes **electronic evidence**, ensuring such evidence cannot be denied legal validity solely due to its digital format.
- **National Information Technology Authority, Uganda (NITA-U) Act 2009**:[33] This legislation established NITA-U as the autonomous statutory body responsible for coordinating, implementing, and regulating IT services among other functions.
- **Uganda Communications Act 2013:**[34] This Act consolidated previous laws to establish the Uganda Communications Commission (UCC) as the consolidated regulator for the telecommunications and broadcasting sectors.
- **Registration of Persons Act 2015**:[35] This Act harmonized laws on the registration of individuals to establish a **national identification register**, which serves as a critical platform for digital identity in Uganda.
- **National Payment Systems Act 2020:**[36] It provides a comprehensive legal basis for electronic payment systems, including mobile money, and introduced a "sandbox" for testing innovative fintech solutions.
- **Regulation of Interception of Communication Act 2010:**[37] This law supplements general criminal provisions by providing legal standards for the monitoring and interception of communications within the digital space.

---

[31] https://www.nita.go.ug/sites/default/files/2025-06/Electronic%20Signatures%20Regulations%202013%20-%20SI%2043%20of%202013.pdf

[32] https://ulii.org/ug/legislation/act/2015/8-3

[33] https://www.nita.go.ug/sites/default/files/2025-06/NITA-U%20Act%20%28Act%20No.%204%20of%202009%29.pdf

[34] https://www.ucc.co.ug/files/downloads/UCC%20Act%202013.pdf

[35] https://ulii.org/ug/legislation/act/2015/7-6

[36] https://ulii.org/akn/ug/act/2020/15/eng@2020-09-04

[37] https://ulii.org/akn/ug/act/2010/18/eng@2010-09-03/source.pdf

- **NITA-U (National Databank) Regulations 2019 (No. 109):**[38] This is the central regulation for government data management. It defines the **national databank** as a system managed by NITA-U resulting from the integration of various databases to facilitate real-time access to information by authorized persons. It mandates that every data controller links its database as prescribed by NITA-U and requires NITA-U to maintain a **database register.**
- **NITA-U (E-Government) Regulations 2015 (SI No. 27):**[39] This regulation expounds out matters on government interoperability, e-government services and also matters meant to improve access and sharing of Government information and services.
- **National Records and Archives Act 2001:** [40]This Act specifically mentions records in electronic form and tasks the state with following good practices for managing public records in any format.

4.2. Crucial components of the target legal interoperability architecture

Uganda has a Legal Framework for e-government in place, but continuous improving and amendment of it is needed. The gaps are related primarily to the absence of a comprehensive governance framework for Whole of Government (WoG) interoperability, including clear rules governing the creation, management, and reuse of shared digital assets across government institutions. Initial proposals to address these shortcomings are outlined in the following proposals:

- **Legislation about WoG.** Uganda SHOULD consider creation of framework law about digital government including rules for establishing information systems and enablers, supervision of creating and operating these systems.
- **Legislation about interoperability governance.** Uganda SHOULD consider development of legislation about registry of interoperability governance including rules and procedures of assessment and approval of public sector IT systems.
- **Legislation of secure data Exchange.** Uganda has National databank regulation from 2019. But it doesn't cover all aspects of secure data exchange. Uganda SHOULD consider renewal of legislation about secure data exchange connection with the transition to the federated data exchange concept.
- **Legislation about Legislation Catalogue/Registry/Gazette.** Current Gazette presents legal acts in pdf format. Uganda should reform this Gazette and establish legislation which sets the rules for business processes, machine readable formats of acts, metadata for legal acts, search and navigation, ensuring AI readiness

---

[38] https://demo.nita.go.ug/sites/default/files/2025-02/The%20NITA-U%20%28%20National%20Data%20Bank%29%20Regulations%202019_0.pdf

[39] https://pmlawhub.com/wp-content/uploads/2026/01/NITA-U-E-Government-Regulations-2015-SI-No.-27-of-2015.pdf

[40] https://ulii.org/akn/ug/act/2001/12/eng@2001-06-15

- **Legislation about digital archiving.** Uganda SHOULD consider legislation of digital archiving of datasets.
    - **Review of legislation processes.** All new digital government related legislation should be reviewed/checked before approval, looking at the following aspects: Digitalisation, Data protection, Interoperability. The review should be carried out by public bodies and by a Coordination body as depicted in Figure 20

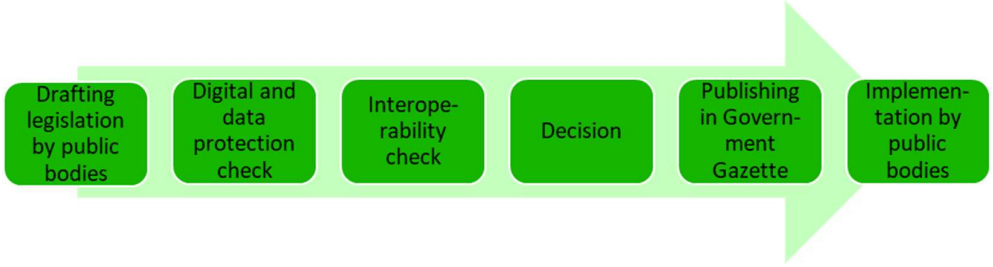

Figure 20. Legislation reviews process

4.2.1. Digital and data protection check

When drafting legislation to establish a public service and seeking to make it consistent with relevant legislation, public bodies must perform a 'digital check' and consider data consumers protection requirements.

Bearing in mind that Ugandan public services are provided also via digital channels, ICT must take it into account in the law-making process.

The proposed legislation should undergo a **'digital check'**:

- to ensure that it suits not only to 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 also facilitate interoperability between public services at lower levels (semantic and technical) and increase the potential for reusing existing ICT solutions, thereby reducing the cost and implementation time.

4.2.2. Interoperability check

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 for issues concerning the use and storage of data, conflicting 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. The performance of legislation should be audited once it is applied.

4.2.3. AI supported law-making process.

AI tools will be used during the law-making process to suggest harmonized language, detect inconsistencies, and ensure multilingual semantic alignment. The architecture also mandates algorithmic transparency, ensuring that automated or AI-assisted decisions are explainable and auditable.

5.Organisational View

Organisational Architecture refers to the way in which public bodies 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 exchanged information. Organisational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user focused.

Organisational Architecture is regulated by legal acts (listed in section 4.1) and specified with following policy documents:

- Uganda Vision 2040[41]
- Digital Uganda Vision (DUV) 2040:[42]
- Fourth National Development Plan (NDP IV):[43]
- Digital Transformation Roadmap (2023/24 – 2027/28)[44]
- Digital Government Strategy (2022–2027):[45]
- National ICT Policy:[46]
- MoICT&NG Strategic Plan (2025/26 – 2029/30):[47]
- NITA-U Strategic Plan (2020–2025):
- Big Data Utilization Strategy:[48]
- National Information Security Framework (NISF) 2014
- National Cybersecurity Strategy (2022-2026): [49]

---

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

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

[43] https://create.finance.go.ug/publicationsresources/fourth-national-development-plan-ndpiv

[44] https://ict.go.ug/site/documents/Digital%20Transformation%20Roadmap.pdf

[45] https://www.nita.go.ug/sites/default/files/2025-07/Digital-Strategy.pdf

[46] https://empowerconsult.co.ug/wp-content/uploads/2023/06/NITA-U_Final-Draft-National-ICT-Policy.pdf

[47] https://ict.go.ug/site/documents/ict-strategic-plan-202526-202930.pdf

[48] https://www.n-ix.com/big-data-strategy/

[49] https://ega.ee/wp-content/uploads/2022/08/Ugandan-national-cybersecurity-strategy.pdf

- Uganda AI Vision 2040[50]
- Uganda national AI landscape assessment[51]
- Uganda e-Government Interoperability Framework (e-GIF)[52]
- e-Government Interoperability Framework Reference Architecture (GIRA)[53]

The Organisational view models the most important Architecture Building Blocks that shall be considered to support organisational aspects for the End-to-End design of interoperable digital public services.

Figure 21 illustrates the most important ABBs of organisational architecture.

[50] https://www.nita.go.ug/sites/default/files/2025-07/e-GIF.pdf/ugandaai2040.org/

[51] https://ict.go.ug/site/documents/uganda-national-ai-landscape-assessment.pdf

[52] https://www.nita.go.ug/sites/default/files/2025-07/e-GIF.pdf

[53] https://www.nita.go.ug/sites/default/files/2025-07/GIRA.pdf

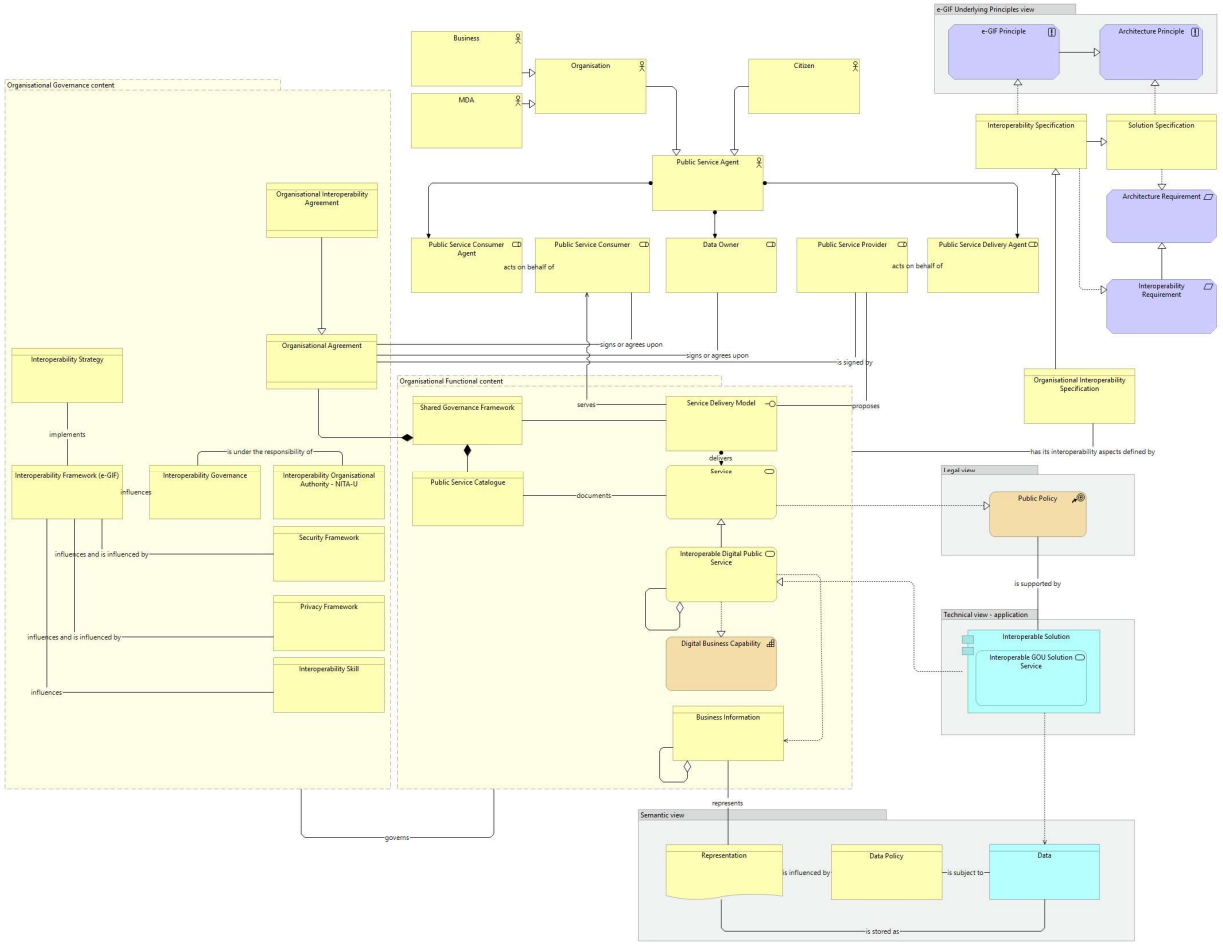

Figure 21 GIRA Organisational View

5.1. Stakeholders and Governance on the Interagency Level

Citizens. The GIRA's primary beneficiaries that will benefit from an easier life.

Businesses. Businesses are waiting for easier procedures to interact with the government.

Civil Servants. Benefits for Civil Servants include easier business processes and improving capacity and access to registries.

The President, Cabinet of Ministers, Ministry of ICT and National Guidance 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. Ministry of ICT and National Guidance 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 digital transformation in Uganda. The central coordination of WoG planning and implementation is responsibility of Ministry. 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.

Ministries, departments, other agencies and Municipalities 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.

Figure 22. 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
- Catalogues
- AI
- Infrastructure
- Network
- eID
- Service portal
- Certification Authority
- Mobile and payment gateway
- Cloud

5.2. Integrated Public Service Governance

There is a need for high level coordination of the e-government activities between the various units of the government. NITA-U SHOULD have the legal rights and competence to take binding decisions in implementation of ICT policy and operating enablers and shared services.

All government institutions are using technology to modernise their processes. The idea of the coordination is not to centralise all decision making and technical capacities. Vice versa, the idea is to support innovation and service delivery modernisation in every government institution.

The tools of coordination are policies, legislation and regulations, budgeting, monitoring, common standards. Standards are needed to allow nation-wide re-use of data, data exchange, re-use of the software solutions and rapid development of the online services.

The Interoperability Governance viewpoint models the Architecture Building Blocks that refer to decisions on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability at interagency level. As such, it does not include operational Architecture Building Blocks like interoperability agreements.

Interoperability governance is the key to a holistic approach on interoperability, as it brings together all the instruments needed to apply it. The organizational view in Figure 23Figure 23 illustrates the most important ABBs of Governance viewpoint.

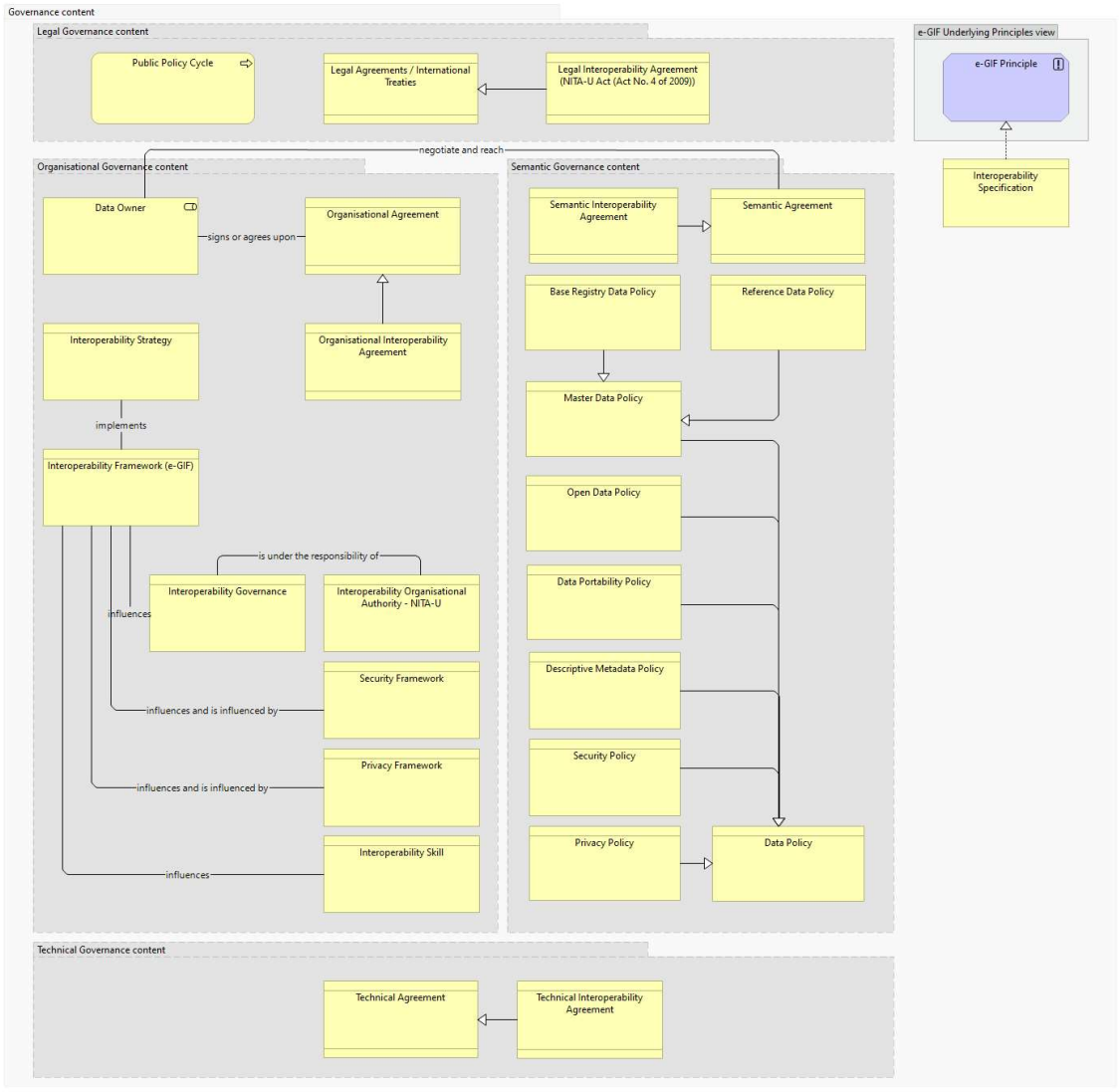

Figure 23 Interoperability Governance viewpoint

5.3. Crucial Components of the Target Organisational Interoperability Architecture

5.3.1. Organisational and Governance processes

According to e-GIF-2026 principle of Subsidiarity and Proportionality coordination activities, including catalogues of interoperability governance, SHOULD be centralised.[54] For achieving organisational interoperability following mechanisms SHOULD be established:

- **Mandatory Catalogue Registration:** Any registry or system not registered in the legally binding Catalogue System (CatIS/GDR or similar) officially "does not exist" in the legal domain and is ineligible for state funding.
- **Enforcement procedures**: NITA-U and the Ministry of Finance enforce compliance by denying funding to any project that refuses to use Shared Enablers like UgPass or the National Data Centre.
- The responsibility for Catalogues-based Interoperability Governance should be established.

5.3.2. Nomination of coordination and supervisors' organisations for Catalogues based interoperability governance

Building an organization to enforce the implementation of Catalogues in Uganda involves a multi-level governance structure that integrates political leadership, technical implementation, and financial enforcement.

- Appointment of controller, authorized processor and supervisors of the Catalogues System and corresponding register data.
- Creating regulation about GDR.
- Interoperability Skill Building: The community of practitioners should be established to ensure that officials across all sectors have the necessary skills in legal, organisational, semantic, and technical interoperability areas
- Fund, staff and train the registry management team
- Appointment of coordinating bodies for governance and operation of this multi-level registry.
- Each administration MUST appoint an accountable interoperability leader
- Data providers and information systems owners must be legally responsible for the availability and integrity of the data services they register in the Catalogues

[54] Requirement 4.3 of e-GIF-2026 says: GoU information technology related political decisions SHOULD be enforced only if they are more efficient than the ones made in public sector institutions.

5.3.3. Business Process Alignment

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 public bodies contributing to the delivery of public services can understand the overall (end-to-end) business process and their role in it.

Public bodies should document business processes using commonly accepted modelling techniques (such as BPMN, UML, ArchiMate, Gantt charts, LeanIX, etc.) and agree on how these processes should be aligned.

5.3.4. AI-supported Process Alignment

Public administrations will utilize AI-driven process mining to identify redundant processes or overlapping mandates across agencies. AI chatbots will serve as digital assistants for cross-departmental coordination and to interpret complex digital legislation for employees

5.3.5. Interoperability Skills

Interoperability skills involve expertise in organising, implementing, and managing interoperability in digital public services. The Interoperability Skill ABB is an interoperability enabler as it helps to achieve organisational interoperability.

5.3.6. Supervision of Information Systems

The aim of supervision is to:

- Create the capability for the supervision of information systems. The supporting instruments (described in 7.4.4) for describing information systems, public services, data services and semantic asset should be established.
- Improve the interoperability of new IT projects through the coordinated use of centrally developed common infrastructure services and open standards
- Improve the coordination and management of state information systems and accelerates the development of IT solutions.

5.3.7. Modernisation of PSC

Point of Single Contact (PSC) (named also an e-government portal, service portal or citizen portal) is portal that allows service consumers to get the information they need and complete administrative procedures online. The Ugandan PSC is a one-stop online centre for government online services. Its main objective is to enhance government service delivery to citizens, businesses and to public bodies. The benefits include making government services more accessible, reducing access costs and queueing at Government offices, make transparency, and increasing transaction convenience with the GOU

5.3.8. eID and PKI ecosystem capacity

Digital identity is the cornerstone of e-government. Simply by owning electronic identification, citizens will be able to carry out secure electronic transactions and take full advantage of e-government, cutting out paperwork.

5.3.9. Capacity for building and managing the secure data ecosystem

A Secure Data Exchange ecosystem and the technical platform support public sector bodies to resolve data exchange tasks more efficiently and securely. Public bodies will use a standardized approach for providing and consuming all services.

5.3.10. Capacity for the Data Centre and Government Cloud

A high-security government data centre is needed to ensure the presence of high availability and high-quality cloud services and cover the need for the accommodation of resources of public bodies.

5.3.11. Modernisation of Open Data Ecosystem

Public bodies should publish open data in machine-readable, non-proprietary formats. They should 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 license terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.

Public bodies must clearly communicate the right to access and reuse open data. Legal regimes for facilitating access and reuse, such as licenses, should be standardized as much as possible.

5.3.12. Implementation e-GIF and GIRA

Improving the organisational interoperability is a continuous process. The implementation strategy for achieving organisational interoperability is formulated by the GOU e-GIF. Recommended activities include:

- Continuous improvement of the implementation and supervision of organisational interoperability aspects: frameworks, agreements, policies, standards.
- MDAs SHOULD document business processes using commonly accepted modelling techniques and agree on how these processes SHOULD be aligned to deliver a GoU public service.
- MDAs SHOULD clarify and formalise organisational relationships for establishing and operating public services.
- Establishment of policies and framework listed in the e-GIF and GIRA
- Supervision of information systems/registries over compliance with legislation, e-GIF, GIRA.

6. Semantic view

The Semantic view models the Architecture Building Blocks that should be considered to support semantic aspects for the End-to-End design of interoperable digital public services. Semantic interoperability view in Figure 24Figure 24 illustrates the most important ABBs of data architecture.

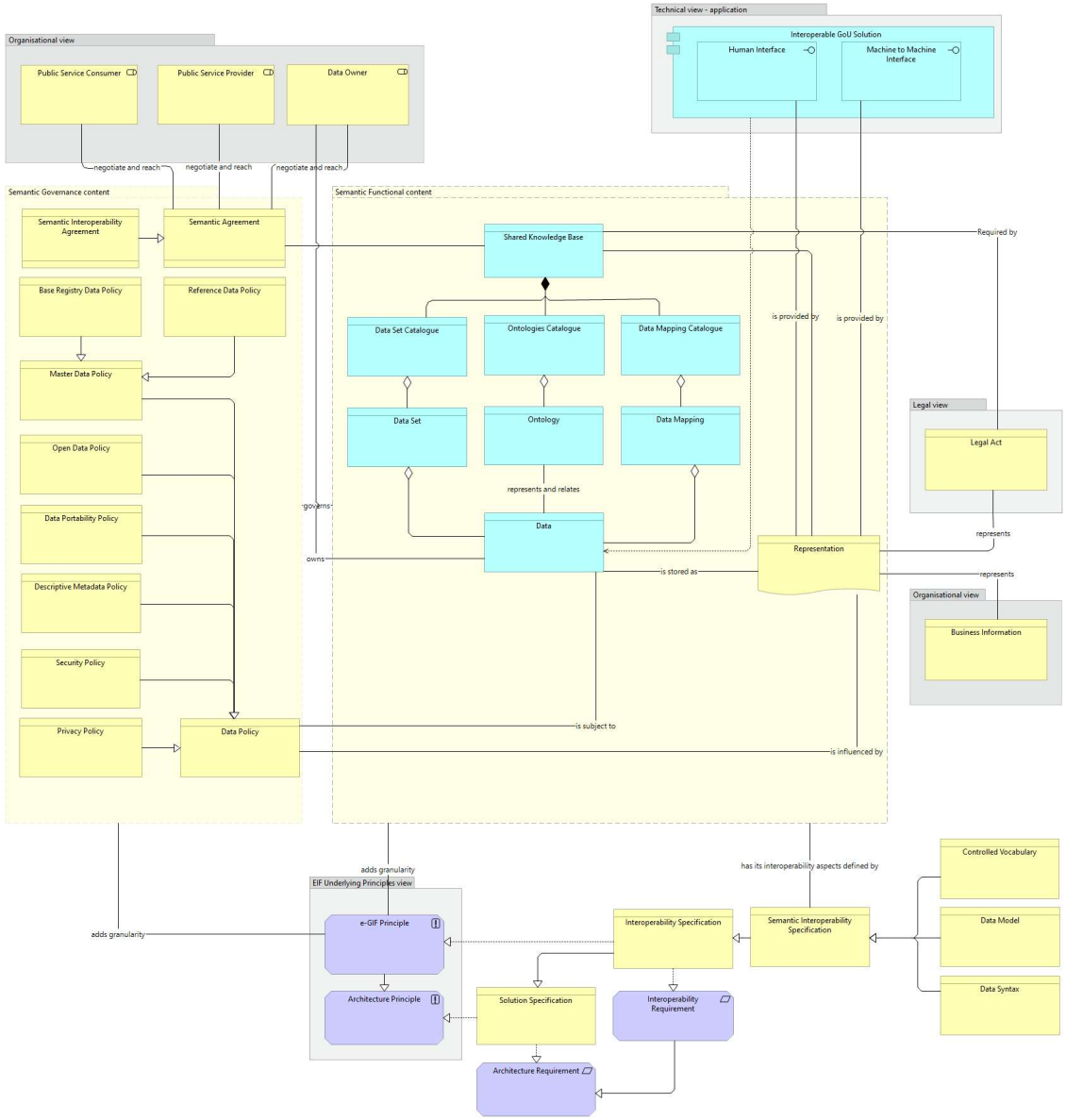

Figure 24 Semantic interoperability view

Semantic (data) 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 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.

6.1. Baseline semantic architecture

6.1.1. Core registries

Core registries provide basic information used across nearly all government sectors:

- **National Identification Register**. Managed by National Identification & Registration Authority (NIRA),[55] it serves as the critical platform for digital identity in Uganda. NIRA is responsible for:
    - Registration of births, deaths, marriages, adoption orders
    - Issuing National Identification Numbers (NINs) and National ID cards
- **Business Registry**.[56] Authoritative source for information on companies and economic operators. The Uganda Registration Services Bureau (URSB) maintains registries for:
    - Business and company registration
    - Intellectual property (trademarks, patents, copyrights, industrial designs)
    - Civil registrations (including births, deaths, marriages, adoptions, divorces)
    - Insolvency and receivership records
- **National Land Information System (NLIS)**[57] includes Uganda's central land registry, covering:
    - Land titles (freehold, leasehold, mailo[58])
    - Parcel information
    - Land records digitization

[55] https://www.nira.go.ug/home

[56] https://www.registrall.com/company-registries/uganda

[57] https://mlhud.go.ug/ugnlis/

[58] https://en.wikipedia.org/wiki/Mailo

    - Land transactions and cadastral information
- **Government Land Registry**: Registry is managed by the Uganda Land Commission (ULC)[59] and it includes:
    - Government-owned land titles
    - Public land allocation records
    - Land fund and restitution programs
- **National Population and Housing Census Registry.** Uganda Bureau of Statistics (UBOS)[60] managed registry through periodic censuses that provide:
    - Population data
    - Housing and socio-economic statistic

Sector-Specific Priority Registries. The Digital Transformation Roadmap identifies several priority registries for integration to eliminate data silos:

- **National Health Facility Registry.**[61] Responsible: Ministry of Health A comprehensive registry of all 6,426 registered health facilities in Uganda, including:
    - Government, private, and PNFP health facilities
    - Facility levels (clinic, HC II, HC III, HC IV, hospitals, etc.)
- **Education:** Includes the Education Management Information System (EMIS) to facilitate data exchange across the teaching and learning system.
- **Agriculture:** Registries for standardized geospatial, weather, and commodity data models.
- **Justice, Law and Order (JLOS):** Includes the Electronic Court Case Management Information System (ECCMIS), Prisons Management Information System (PMIS), and the Electronic Policing Information System (ePIS).
- **Finance:** The Security Interest in Movable Property Registry (SIMPO), which facilitates borrowing using movable property

Digitalised systems. A significant number of Government registries and services are still not digitalised. Portfolio of Government System Services[62] lists nearly 400 items.

Integration Service (UGHub). A considerable number of institutions (146) have created a readiness to share data and communicate throw UGHub platform. UGHub includes a centralized

[59] https://ulc.go.ug/

[60] https://www.ubos.org/

[61] https://nhfr.health.go.ug/

[62] https://oldsite.nita.go.ug/portfolio-government-system-services (not available 2026-03-30). Full inventory to be maintained in the upgraded GDR

Semantic and Systems Catalogue that enables efficient discovery, classification, and management of systems and their associated services for streamlined operations.

6.1.2. Government Digital Registry

The Government Digital Registry (GDR)[63] was established under the mandate of MoICT&NG as Uganda's centralised platform for the inventory and governance of ICT assets, systems, and processes across all MDAs. In its current form, the GDR enables MDAs to register their digital systems and provides MoICT&NG with a baseline view of the government's digital estate.

The GDR is directly aligned with and operationalises the Project Charter for the Inventory of Government Processes and Systems, a formal MoICT&NG (Ministry of ICT and National Guidance) initiative with the following scope:

- Design, develop, and test a comprehensive inventory platform to profile all government systems, business processes, and IT infrastructure across MDAs
- Train IT officers in all MDAs on the platform, targeting complete MDA system profiling within 60 days of deployment
- Conduct review, analysis, and validation of submitted data — generating a status of digitisation report and rationalisation roadmap
- Centralise approval of new ICT systems at MoICT&NG, introducing a mandatory clearance process before procurement or funding

GDR propose is to: [64]

- Provide the Government of Uganda with visibility over existing digital systems
- Reduce duplication of ICT investments
- Improve coordination, interoperability, and planning of e-Government services
- Support implementation of Uganda’s Digital Transformation Strategy

[63] https://gdr.ict.go.ug/

[64] https://bbegmedia.com/ict-ministry-launches-digital-registry-to-coordinate-e-government-services/

6.2. Crucial components of the target semantic interoperability architecture

6.2.1. Digitisation, digitalisation, digital government

Digitisation is the process of turning physical data into digital data. Scanning of historical data about the population would be an excellent example in this respect. Public bodies should digitise all the needed documents.

Digitalisation is the incorporation of digital technologies into business/social processes, with the goal of improving them. Public bodies should interact with citizens, businesses, and other public bodies digitally.

Digital government refers to the use of digital technologies, as an integrated part of governments' modernisation strategies, to create public value. It relies on a digital government ecosystem comprised of government actors, non-governmental organisations, businesses, citizens' associations, and individuals, which supports the production of and access to data, services, and content through interactions with the government.[65] Implementation of the GIRA supports creating a digital government.

6.2.2. Interoperability between registries

To achieve interoperability between registries the government is transitioning from a system-centric to a data-centric model, treating the Dataset as the primary object of governance. Core mechanism for achieving semantic interoperability between registries are:

- **Base Registries as "Sources of Truth":** Owners of foundational registries (e.g., NIRA for identity) are the authorities for syntax and semantics in their domains; all secondary systems must adhere to these standards.
- **Single Identifiers:** To ensure cross-sector traceability, information about core objects (such as persons, land, and addresses) must use the same specified single identifier across all government systems.
- **Metadata Standards**: All datasets must be described using international standards (like W3C DCAT-3) to ensure they are discoverable and "findable" across the government

6.2.3. Semantic Readiness for Data Spaces, and cross border data exchange

For moving toward a federated architecture, semantic assets must be designed for broader integration.

[65] https://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

6.2.4. AI supported Semantic Interoperability

AI models will automate the mapping of equivalent concepts between heterogeneous data schemas and detect hierarchies in taxonomies. AI translation tools will ensure that metadata and data meanings remain equivalent across English and Ugandan local languages to prevent "semantic drift".

6.2.5. Catalogues

Data about data (metadata) must be properly managed and made publicly available. Catalogues help others to find reusable resources (e.g., services, data, software, data models). Various types of catalogues 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. Various Catalogues should be interconnected and communicate with each other as depicted in Figure 25.

Catalogues provide trustworthy assistance and a tool for the developers, administrators, and users of Ugandan information systems. Catalogues are a supplementary instrument for coordinating Ugandan information systems. All objects of catalogues must be reviewed and approved by a coordination body.

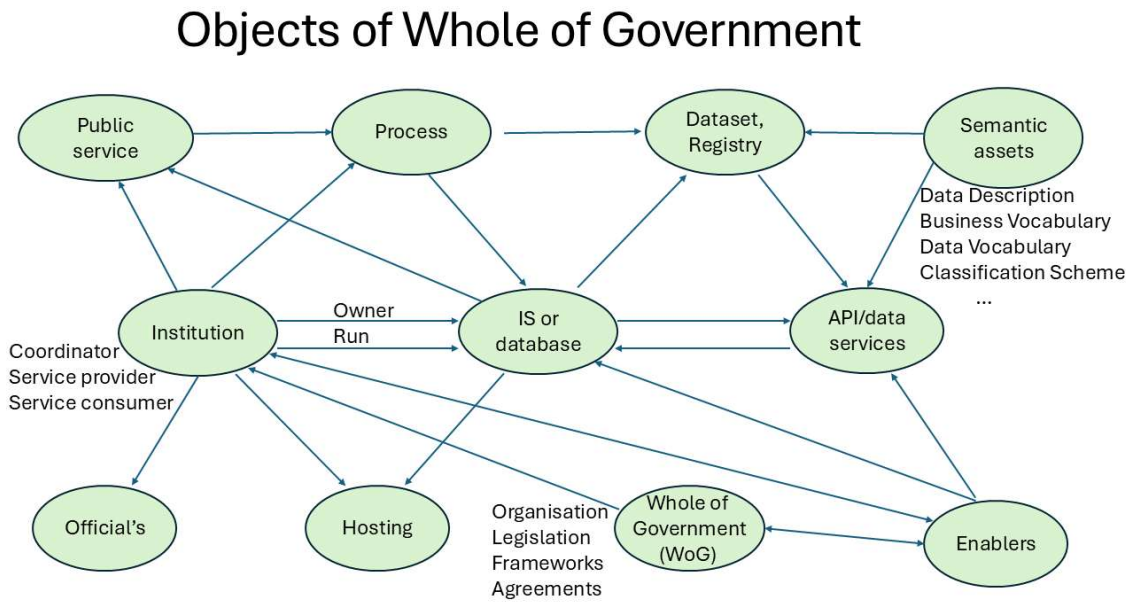

Figure 25 Catalogues system

Every specification MUST reuse, if possible, WoG objects as depicted in Figure 25. For example, Service portal MUST reuse information about institutions, public services and Data services from Catalogues.

Catalogues system is a tool for the coordinated activities of several bodies. The main stakeholders of Catalogues system are depicted in.

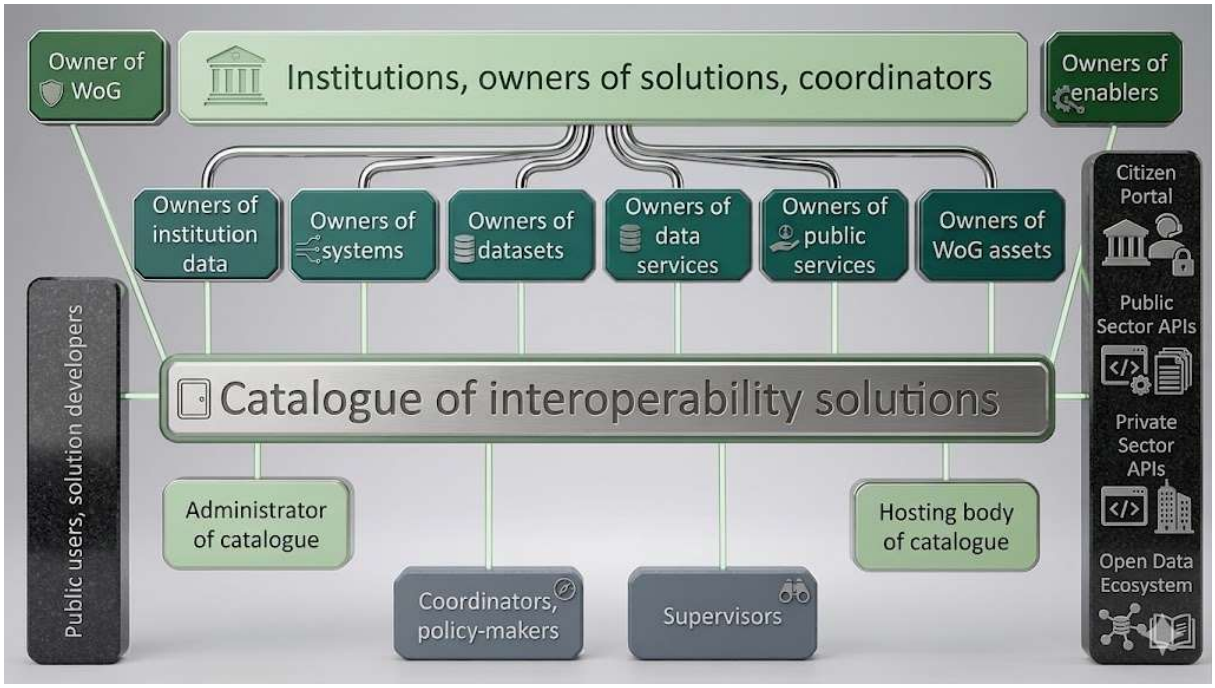

Figure 26 Stakeholders of Catalogues System

Administrator of catalogue is the e-government implementation or coordination body. The owner assigns the responsible administrators who are responsible for the integrity and availability catalogue system.

Coordinators and supervisors see all Catalogues System data, including data hidden from public users. They use Catalogues for making decisions in the WoG governance domain. Usually, they have special roles in workflow processes. For example, they assess:

- Compliance of documentation of registers and information systems with the legislation
- Compliance of documentation of datasets, registers and information systems, services with the interoperability framework (and/or other documents)
- Fulfilment of the once-only principle
- Fulfilment of requirements of the conceptual model of e-services
- Fulfilment of privacy and security requirements
- Compliance with agreements and standards
- Whether all datasets, registers and systems are complete and up to date
- Level of security of registers and systems

Public users include developers, journalists, scientists, students, etc. Public users can read, list, search and download public data. Sensitive data are hidden from public users. Public users cannot change any data. Developers of services and developers of systems are very important groups of public users, who reuse data from other registers. Developers can find all needed information (descriptions of systems, structure and meaning of data, descriptions of services) from Catalogues

System. There is no need for additional contacts with developers of other systems. For newcomers, Catalogues data serves as examples and teaching material.

External systems. Catalogue system SHOULD supports migrating from one instance to another, the configurable elements of the application (forms, views, roles, workflow definitions) can be downloaded in bulk from one instance of the application and then uploaded to another. The citizen portal may be most important external system. The citizen portal can reuse descriptions of public services and institutions and present this information to citizens and businesses. These features ensure downloading data as open data. Downloaded data can be used for generating statistics, for analytics, etc.

Stakeholders co-create the content of the catalogue. Institution experts submit data about institutions, owners of registers data about their registers, owners of consumer organisations about their information systems, owners of services about their services, owners of interoperable assets about their assets. Coordinators and supervisors use the catalogue, and they register their decisions in the catalogue.

Government Digital Registry is described in section 6.1.2. During project draft catalogue system CatIS was launched.[66] CatIS instance is a test and demonstration deployment of the CatIS software, not a national system (however it can be used for it). CatIS is hosted as a sandbox. It was used for: Training, Demonstrations, Architecture exploration.

Current GDR lacks transparency and openness. CatIS publishes no sensitive data in public catalogues. CatIS includes all WoG objects depicted in Figure 25 and stakeholders in Figure 26. It would be important to make comparative analyse of GDR and CatIS and if needed, add new data structures and functionalities to GDR. It is important to use single catalogue system and avoid duplication in data capture.

Catalogues system/GDR SHOULD become a comprehensive, legally authoritative, Whole-of-Government digital governance platform that registers, governs, validates, and monitors all government information systems, datasets, public services, Data services (API), processes, and ICT investments across all MDAs and Local Governments; enforces compliance with national interoperability, security, and data protection standards; and provides the structured approval gateway through which all digital investments and data infrastructure establishments must pass before recognition, funding, or operationalisation.

The organisation for Catalogues-based Governance should be decided and nominated.

6.2.6. Once-only principle

The once-only principle ensures that users should be able to provide data once only, and public bodies should be able to retrieve and share this data to serve the user. According to the "once-only" principle,

[66] https://upmind.ee/ug/catis

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 copying of the data, but in this case, it must be considered that data may be outdated.

6.2.7. The single identifier of objects

Information about some objects such as persons, addresses, and land properties are used in many services. For interoperability it is important to use the same identifiers for these objects in all information systems of Uganda

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

6.2.8. Classifications

To understand processes and categorize data in information systems in a standardized way, data needs 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.

The same data in all information systems must be coded by using standard classification.

6.2.9. Uniform addresses

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

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

6.2.10. Data standards

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

Data standards should be established and maintained by the owners of the base registries and should be published in the catalogue of information systems. Other public bodies should follow these standards.

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

7.Technical View

In terms of implementation, application and technical architecture have a close relationship. Therefore, we shall look at them together. In the GIRA, this topic is covered by applications and infrastructure views. We do not consider all e-government activities but only activities for achieving 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

7.1. Baseline Technical Architecture

7.1.1. UGPass

Digital Authentication and Electronic Signatures Solutions (UGPass) is a digital authentication and electronic signature platform that empowers individuals, businesses, and government entities to seamlessly sign and authenticate documents online. Designed with security, efficiency, and digital trust, UGPass eliminates the need for physical presence in signing or verifying documents, enabling a more productive and paperless future.[67]

UGPass offers a robust suite of services to meet the needs of modern digital workflows:

- Digitally Authenticate Yourself: Prove your identity securely and reliably online.
- Sign and Seal Documents: Create electronic signatures that are legally binding and tamper-proof.
- Trusted Subscriber Services: Leverage verified digital identities for seamless service access.
- Integrate with Existing Systems: Easily connect UGPass with your organization's digital ecosystem.
- Adhere to Legal Standards: Ensure compliance with national and international laws governing electronic signatures and digital trust.

7.1.2. Internet

NITA-U provides reliable and high-speed Internet Bandwidth services to all government entities in Uganda through the National Backbone Infrastructure (NBI). This service is designed to ensure seamless connectivity, enabling government offices to operate efficiently and deliver services to citizens effectively.

[67] https://www.nita.go.ug/services/e-government-services/digital-authentication-and-electronic-signatures-solutions-ugpass

7.1.3. The SMS Gateway

The SMS Gateway service is provided by the Uganda government's IT body, designed to facilitate efficient and secure communication across all government departments and agencies. This service is pivotal in enhancing the interaction between government entities and the public, as well as within the governmental framework itself.[68]

7.1.4. Leased lines

Leased lines are dedicated and rented communication links that provide reliable, high-speed connectivity between two or more locations. These lines are designed to facilitate private data transfer, secure communication, and seamless internet access for government entities. As part of the technical services offered by the National Information Technology Authority - Uganda (NITA-U), leased lines are tailored to meet the specific needs of government bodies, ensuring efficient and uninterrupted operations.[69]

7.1.5. UMCS

Unified Messaging and Collaboration System (UMCS) is a government of Uganda platform designed to revolutionize communication and collaboration across all government sectors. UMCS is fully operational Software as a Service (SaaS) with over 140 fully onboarded and utilizing the service. With a comprehensive suite of features tailored to enhance productivity and streamline workflows:[70]

- **Email Services**: Enjoy a government-grade email system that guarantees secure, reliable, and seamless communication. UMCS email services are built to handle the volume and sensitivity of governmental correspondence with ease.
- **Audio & Video Conferencing**: Break down geographical barriers with our high-definition audio and video conferencing capabilities. Host meetings, conduct briefings, or engage in policy discussions without the need for physical presence, all while maintaining clarity and professionalism.
- **Content Sharing & Collaboration**: Collaboration is at the heart of UMCS. Share documents, brainstorm in real-time, and manage projects with tools designed to boost productivity. Our platform supports multiple users working on the same content simultaneously, ensuring that ideas flow freely and decisions are made swiftly.
- **Secure Drive Storage**: Data security is paramount. UMCS provides a secure drive where government documents, sensitive information, and project files can be stored, accessed, and

[68] https://www.nita.go.ug/services/e-government-services/sms-gateway

[69] https://www.nita.go.ug/services/technical-services/leased-lines

[70] https://www.nita.go.ug/services/e-government-services/unified-messaging-and-collaboration-system-umcs

managed with stringent security protocols in place, ensuring compliance with data protection standards.

7.1.6. Website Domain & Hosting

Empowering Ugandan government institutions and bodies with reliable, secure, and efficient digital solutions. Website Domain & Hosting service is specialised specifically for the unique needs of public sector entities, ensuring that your online presence is professional, accessible, and optimized for performance[71]. Features:

- Domain Registration
- Customized Hosting Solutions
- Website Management
- Security Measures
- Performance Optimization
- Support and Training

7.1.7. UGHuB

Integration Service (UGHub), spearheaded by the NITA-U, is a groundbreaking initiative designed to streamline data sharing across government systems. By facilitating seamless, secure, and efficient information exchange among Ministries, Departments, and Agencies (MDAs), UGHuB is transforming service delivery, enhancing decision-making, and fostering innovation across Uganda's public and private sectors.[72]

UGHuB is a Data Integration Platform that connects disparate government systems, enabling real-time data sharing and collaboration. It addresses the challenges of heterogeneity, security, and inefficiency in government service delivery by providing a unified, vendor-neutral platform for integration.

Key Features:

- **Vendor-Neutral Integration.** The platform supports seamless integration with any system, regardless of the underlying technology. Built on the robust WSO2 technology stack, UGHub offers unmatched flexibility and compatibility.

---

[71] https://www.nita.go.ug/services/e-government-services/unified-messaging-and-collaboration-system-umcs

[72] https://www.nita.go.ug/services/e-government-services/integration-service-ughub

- **Secure Hosting in the Government Data Centre.** Entirely hosted within the Government of Uganda's data centre, the platform ensures top-notch data security and operational sustainability.
- **API Management.** UGHub provides comprehensive API management tools that allow entities to easily create, share, and consume APIs, enabling real-time data interactions.
- **Identity and Access Management.** Advanced identity and access management systems ensure secure authentication and authorization, giving entities full control over their data accessibility.
- **Semantic and Systems Catalogue.** A centralized catalogue enables efficient discovery, classification, and management of systems and their associated services for streamlined operations.
- **Reporting, Analytics, and IoT.** With robust reporting and analytics capabilities, the platform offers actionable insights. Additionally, support for the Internet of Things (IoT) opens avenues for future innovation and integration.

7.1.8. My-UG

My-UG is FREE Wi-Fi and a centralized digital service platform developed and managed by the NITA-U.[73] As part of its mandate to streamline and enhance the delivery of government services, NITA-U offers My-UG as a key technical service to all government bodies in Uganda. This platform is designed to facilitate seamless integration, data sharing, and service delivery across various government entities, ensuring efficiency, transparency, and accessibility for both public institutions and citizens.

Key Features:

- **Unified Access Portal:** My-UG provides a single point of access for government employees to access shared resources, applications, and databases, reducing redundancy and improving workflow efficiency.
- **Secure Data Exchange:** The platform enables secure data sharing and communication between government agencies, ensuring compliance with national data protection and cybersecurity standards.
- **E-Government Services Integration:** My-UG integrates with existing e-government services, allowing for a cohesive digital ecosystem that supports service delivery to citizens.
- **User Management System**: A robust user management system ensures that access to sensitive information is restricted to authorized personnel, enhancing security and accountability.
- **Real-Time Analytics and Reporting**: Government bodies can leverage My-UG's analytics tools to generate real-time reports, monitor performance, and make data-driven decisions.

[73] https://www.nita.go.ug/services/technical-services/my-ug

7.1.9. NITA-U National Data Centre

The NITA-U National Data Centre offers a comprehensive suite of services tailored to meet the diverse needs of government entities and other stakeholders. These services are designed to enhance operational efficiency, ensure data security, and support the delivery of critical public services:

- **Infrastructure as a Service (IaaS).** Provides foundational building blocks such as servers, storage, and networking infrastructure. Enables government agencies to scale their IT resources without significant upfront capital investments. Ideal for hosting critical applications, databases, and citizen service platforms.
- **Platform as a Service (PaaS).** Offers a robust environment for developing, deploying, and managing applications. Handles backend tasks such as database management, operating system updates, and middleware integration. Empowers government developers to focus on creating innovative solutions for public service delivery.
- **Software as a Service (SaaS).** Provides access to ready-to-use applications such as email, collaboration tools, and enterprise resource planning (ERP) systems. Eliminates the need for on-premises software installation and maintenance, reducing operational overhead.
- **Backup as a Service (BaaS).** Delivers automated data backup and recovery solutions to ensure the protection of critical government data. Minimizes the risk of data loss due to hardware failure, cyberattacks, or natural disasters.
- **Disaster Recovery.** Offers robust disaster recovery solutions to ensure business continuity in the event of unforeseen disruptions. Supports government agencies in maintaining uninterrupted service delivery to citizens.
- **Infrastructure Highlights.** The NITA-U National Data Centre is equipped with cutting-edge infrastructure to ensure maximum uptime, security, and operational efficiency. Data Centre facility is designed to meet the highest international standards for data centre operations.

7.1.10. IP Transit

IP Transit (IPT) is a critical technical service offered by the NITA-U to facilitate seamless internet connectivity for all government bodies in Uganda. As the central authority responsible for coordinating and regulating Information Technology services across the government, NITA-U ensures that government entities have reliable, high-speed, and secure access to the internet and other digital resources. IP Transit serves as the backbone for interconnecting government networks to the global internet, enabling efficient communication, data exchange, and access to online services.[74]

7.1.11. Open Data

Open Data ecosystem includes key open data initiatives and sources:

[74] https://www.nita.go.ug/services/technical-services/ip-transit-ipt

- **Uganda Bureau of Statistics (UBOS):** Provides official data on population, censuses, business, and industry.[75]
- **SDG Open Data Portal**: Tracks Uganda's progress on Sustainable Development Goals via interactive maps and charts.[76]
- **Bank of Uganda Open Data**: A repository for economic and financial data.[77]
- **Uganda GeoPortal**: Offers geospatial data, satellite imagery, and maps.[78]

7.2. Technical Architecture - Application Architecture view

Application - Domain specific view contains the application Architecture Building Blocks that need to be considered to support technical aspects for the End-to-End design of Interoperable Solutions.

The view depicts application architecture of any MDA solution. The view does not reflect the use of infrastructure services in detail. Infrastructure view, supporting ABB **Digital Service Infrastructure,** is described in granularity in chapter 7.3.

Application Interoperability view in Figure 27Figure 27 illustrates the most important ABBs of application architecture.

[75] https://www.ubos.org/nso-open-data/

[76] https://sdgs.opm.go.ug/2025/08/11/ugandas-sdg-open-data-portal-advancing-transparency-and-sustainable-development/

[77] https://cb-uganda.opendataforafrica.org/

[78] https://uganda-africa.hub.arcgis.com/

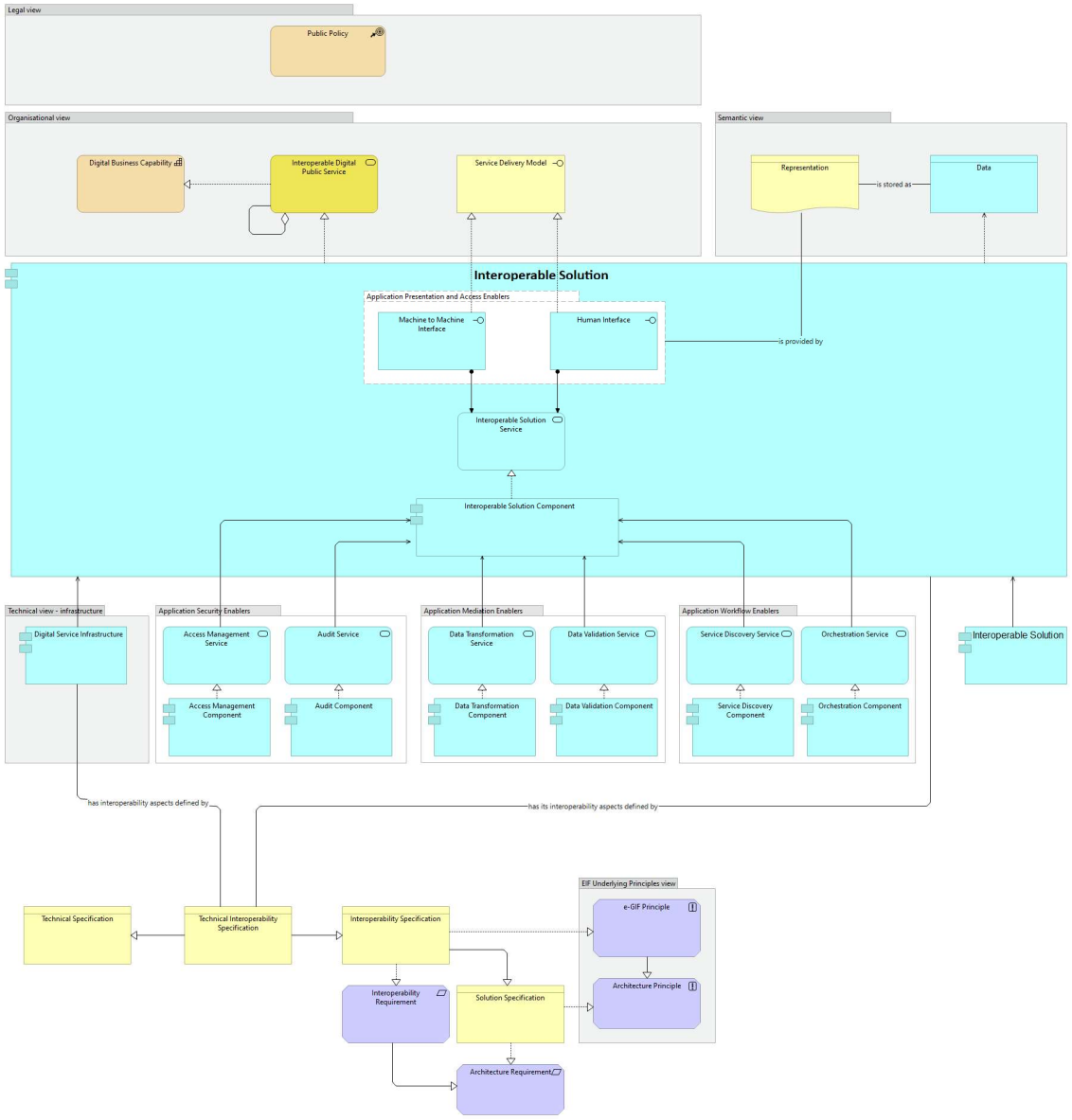

Figure 27 Application architecture view

7.3. Technical architecture – Infrastructure Architecture View

The GIRA Infrastructure view depicted in Figure 28Figure 28Figure 28 provides an architecture content metamodel for the cross-sectorial infrastructure services, along with the supporting hosting and networking facilities, which shall be considered in order to support technical aspects for the End-to-End design of Interoperable Solutions. The difference from the application part of the Application view is that the Architecture Building Blocks in the infrastructure view are considered to be relevant for solutions in any sector of government.

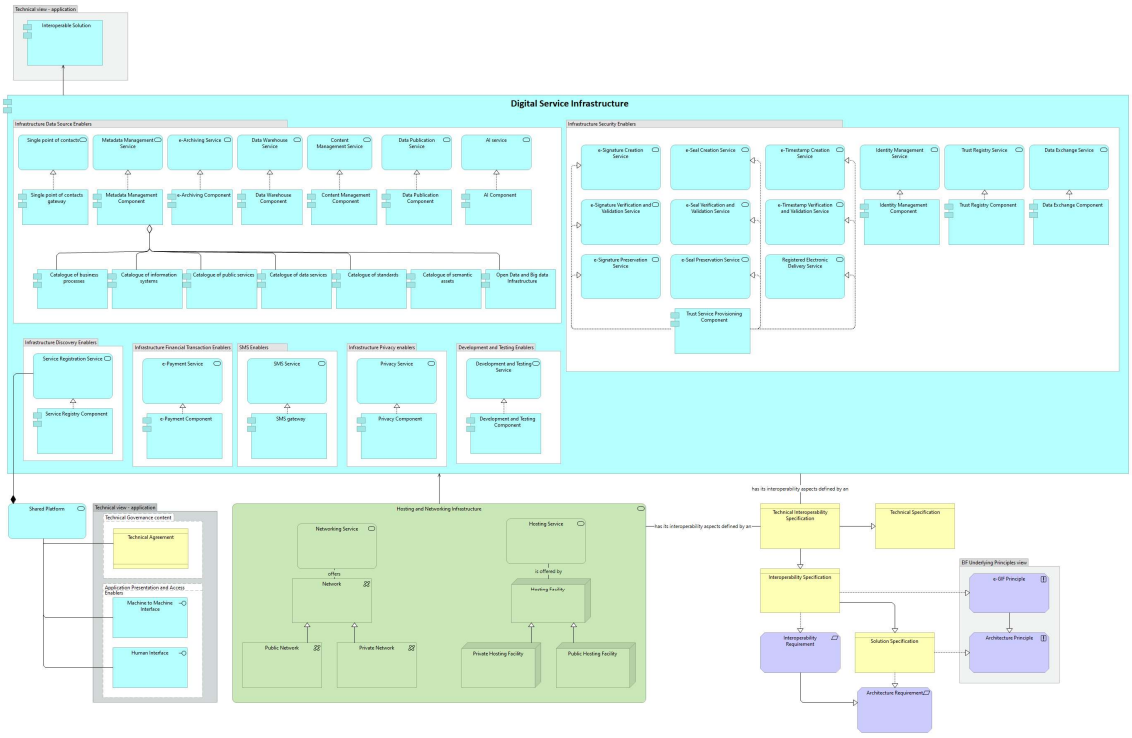

Figure 28 GIRA infrastructure view

7.4. Crucial components of application and technical interoperability architecture

7.4.1. Ugandan National Data Exchange Infrastructure

Uganda is currently using the UGHub platform (described in section 7.1.7) for data exchange that encapsulates technical and security details from public bodies. UgHub is excellent tool for service orchestration but for Data Space Model it's needs to supplement or replaced. UgHub is excellent tool for building sectoral gateways.

The Ugandan National Data Exchange Infrastructure (UNDEI) (also referred to as **Secure Data Exchange Ecosystem (SDE) or** the **Data Space Ecosystem)** represents the core integration

layer of GIRA-2026. It facilitates a secure, decentralized environment where government agencies, public institutions, and trusted partners share and access data without losing sovereignty over it.

Architectural Paradigm: Shift to Federated Data Sharing. The GIRA-2026 mandates a transition from the legacy "Hub-and-Spoke" model (where **UGHub** acted as a central traffic controller) to a **Federated Data Space**:

- **Decentralization:** Data remains at its original source with the custodial MDA, eliminating the need for central data silos.
- **Peer-to-Peer Exchange:** Integration is achieved through distributed nodes, removing the "Single Point of Failure" (SPOF) and performance bottlenecks associated with centralized processing.
- **Sovereignty:** MDAs retain absolute control over their primary registries, granting access rather than "giving up" data.

Security and Trust of SDE. To ensure the integrity of the Whole-of-Government (WoG) ecosystem, the Data Space incorporates:

- **Cryptographic Non-Repudiation:** Every technical exchange MUST generate "Evidence of Exchange" receipts signed via the **National PKI**, providing undeniable proof of origin and receipt for every transaction.
- **Zero-Trust Security:** Implementation of a security-by-design architecture where no device or user is trusted by default, regardless of their location on the government network.
- **Anomalies Monitoring:** Utilization of **AI-enhanced cybersecurity monitoring** to identify real-time anomalies in cross-sector and cross-border data exchanges.

Metadata and Interoperability Governance. The ecosystem is governed by a legally binding system of **Catalogues**:

- **Source of Truth:** All data services (APIs) and datasets within the Data Space MUST be registered in the **National Dataset Catalogue** and **API/Data Space Catalogue**.
- **Mandatory Registration:** Any data service or registry not registered in the central catalogue officially "does not exist" in the legal domain and is ineligible for state budget allocation.
- **Semantic Consistency:** The ecosystem reuses meanings from verified **Base Registries** and implements **W3C DCAT-3** metadata standards to ensure all systems "speak the same language" natively.

Strategic and Global Alignment

- **Once-Only Principle:** The Data Space is the primary engine for ensuring citizens provide information to the government only once, with data then being reused securely across the entire federated ecosystem.
- **Cross-Border Readiness:** The architecture is designed for compatibility with **EAC, COMESA, and AfCFTA** digital protocols, facilitating secure data exchange across national borders.
- **Regulatory Shift:** This architecture shifts NITA-U's role from an "Operator" of a central hub to a "**Scheme Regulator**" of the national Data Space standards and trust framework.

7.4.2. eID ecosystem

Digital identity is the cornerstone of digital government. Simply by owning an electronic identification, citizens will be able to carry out secure electronic transactions and take full advantage of e-government and cutting out paperwork.

A digital identity is information used by computer systems to represent an external agent – a person, organization, application, or device.[79] Digital identities allow access to services provided with computers to be automated and make it possible for computers to mediate relationships.

The Building Blocks associated with eID ecosystem:

- Registration Service
- Issuance Service
- Authentication Service
- Validation Service
- Single-sign-on (SSO) service
- Supervision and incident management service
- Support for users and eID supporting

Most of these functionalities are realised by UgPass (described in section 7.1.1)

7.4.3. Trust services and PKI infrastructure

Trust services are services provided by a trusted third party (Trust Service Provider) to commit authenticity of information or transaction.

From technical perspective trust services are based on PKI technology where digital signature is used for integrity and proof of authenticity. The Building Blocks for the Trust services ecosystem are:

- Key management - Registration and issuance services.
- e-Signature services (creation, verification, validation, preservation).
- e-Seal services (creation, verification, validation, preservation).
- Electronic Delivery service.
- Web-page identification service.
- Trusted List service.
- Certification authority services.
- Timestamping authority services.
- Accreditations and Assessment Body services.
- Supervision Bodies services.
- Support and notification service.

Most of these functionalities are realised by UgPass (described in section 7.1.1)

[79] https://en.wikipedia.org/wiki/Digital_identity

7.4.4. Catalogues

Interoperability governance conducted through WoG objects. WoG objects are institutions, officials, citizens, business, systems, datasets, services, semantic assets, which are interconnected and communicate with each other as depicted in Figure 25.

For interoperability governance the interconnected system of catalogues SHOULD be used. The system of catalogues should be used for several purposes:

As a Tool for Metadata Management and Discovery. At its core, a catalogue is defined as a repository for "data about data" (metadata). Its primary function in this context is to help developers, administrators, and users find reusable resources such as services, software components, and data models. This "findability" is intended to reduce duplication of efforts and decrease costs by promoting the reuse of existing assets.

As a Mandatory Governance Instrument. In the Ugandan Whole-of-Government (WoG) framework, a catalogue SHOULD be "legally binding" tool for coordination:

- **Approval:** All objects within national catalogues MUST be reviewed and approved by Coordination Body.
- **Statutory Status:** The sources state that if an information system is not registered in the central catalogue, it officially "doesn't exist" and will not be eligible for state funding.
- **Digital Checks:** The catalogue serves as the platform where assessment and approval workflows (such as "digital checks" and "interoperability checks") are recorded and preserved.

7.4.5. Point of single contact

Point of Single Contact (PSCs) is e-government portal that allow service providers to get the information they need and complete administrative procedures online. The Ugandan PCS is a one-stop online centre for Government online services. Its main objective is to enhance Government service delivery to citizens, non-citizens, businesses and to Government Ministries, Departments and Agencies (MDAs). The benefits include making Government services more accessible, reducing access cost and queuing at Government offices, transparency, timeliness and increasing convenience of transaction with the Government of Uganda ANYTIME and from ANYWHERE.

Ugandan PCS: https://ecitizen.go.ug/content/ecitizen-portal needs supplementation. Ideally, the PSC should take data about public services and institutions from the Catalogues.

The PSC should have three main topics areas: for Citizens, for Businesses, and for Visitors. It is recommended for the citizen portal to elaborate a personal secure environment for citizens, accessed by eID tools. The personal area may contain the following subareas:

- **Lifecycle area** containing articles on how to resolve important or frequently occurring issues (such as applying for family benefits) and advice on what to do in certain situations. The e-services, articles and contact details in the portal should be linked to make it easy for people to find information related to certain topics.

- **E-service area** allows people to survey the data which the government has collected about them.
- **Notification services**, e.g. breaks in electricity or water deliveries, expiration of a period of validity, etc.
- **Application area** allows people to fill in forms and then to forward them to the relevant institutions.
- **Secure document area** allows users to sign documents and forward them.

The portal sub-system allows end-users to access the e-services in a unified way as described below.

- **Citizen portal** – services for the public. Using the portal is convenient and secure and saves time. Citizens and foreigners alike can find information in the portal about their rights and obligations in communicating with the public authorities in Uganda. The thorough information the portal contains can be used to find answers to potentially problematic issues before they arise. Queries sent via the portal are answered directly by user support or passed on to the relevant department – users do not need to do this themselves. All questions can be submitted in one place, with a guaranteed response. Everybody can see the data about themselves. In addition, citizens can see who has looked at their personal data in registries. This helps to avoid type of misuse where "curious" officials look at the personal data.
- **Officials' portal** – services for government officials. The portal is a secure environment via which users are provided with convenient access to public sector information, services, and contact details. Officials get support from the portal to open their own resources via the central portal.
- **Companies' portal** – services for business users. The portal is a simple and secure way to obtain information about launching and running an enterprise and about communicating with public departments. If operating in a certain field is subject to specific requirements, the portal provides entrepreneurs with step-by-step instructions on what to do. For business operators, the portal represents a single online contact point.

7.4.6. e-Payment

The e-Payment component implements the functionality of executing payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device. The e-Payment component ABB is salient for technical interoperability because it provides the implementation of functionalities of executing payment transactions. Generally, the Building Block is supportive of multiple types of payment use cases where the Government is one of the parties:[80]

- **Government to people (G2P).** Payment where the payer is a government and the payee is an individual e.g. social benefits disbursement, government salary payments, Conditional and Unconditional Social Cash Transfers).
- **People to Government (P2G).** Payment where the payer is an individual and the payee is a government. P2G payments can be government initiated, for instance, in the case of payments for registrations for government services. For bill payments and payments for

[80] https://specs.govstack.global/payments/2-description

government services directly by the person, the system should provide the person with the flexibility to choose which payment instrument to use (e.g. mobile money, bank transfer or card payments). (e.g. payment of taxes, payment Registration for Postpartum and Infant Care, payment of school fees, driving license, utility payments).

- **Government to Business (G2B).** G2B payments include tax refunds, goods and services purchases, subsidies, contract payments, benefits, and loans.
- **Business to Government (B2G).** B2G payments include paying taxes and fees.
- **Government to Government (G2G).** Payments between two government entities (i.e. between Ministries/Departments and public sector institutions).

7.4.7. Digital invoice

Digital invoices are a critical component of Uganda's strategy to transition toward a digitally empowered society where the economy conducts transactions and pays invoices fully digitally, automatically, and instantly. This shift improves automation and efficiency in the following ways:

- **Reduction of Manual Paperwork**: Digital invoices support the national goal of making "unnecessary paperwork a thing of the past" in both the public and private sectors. By removing manual billing processes, officials and business owners have more time for high-value work.
- **Enhanced Revenue Administration**: The automation of revenue processes through systems like e-LogRev[81] and IRAS[82],which utilize digital invoicing and billing for local taxes,has already been credited with increasing local revenue collections. These systems improve administration, reduce opportunities for corruption, and help address widespread tax evasion.
- **Support for a Cashless Economy:** Implementing digital technologies for transactions is part of a broader effort to develop a national payments system and achieve a cashless economy. This improves the accuracy of filed tax returns and increases overall compliance.
- **Administrative Efficiency and Transparency**: Digital invoicing facilitates better service delivery by reducing transaction costs and lead times for the acquisition of goods and services. It also eliminates the need for physical visits to government offices, thereby reducing bureaucratic red tape.
- **Institutional Sustainability:** Within government entities like NITA-U, the automation of revenue collection and the development of automated billing systems are strategic interventions designed to increase operational efficiency and support financial sustainability.
- **Integration of "ICT Islands":** By utilizing the SDE secure data exchange, digital invoices can be part of an integrated end-to-end government business process, ensuring that data is provisioned and consumed across various MDAs without manual re-entry

[81] https://e-logrev.go.ug/dashboard/

[82] https://iras.go.ug/

7.4.8. Data Centre and Government Cloud

A high-security government data centre will be established, which will ensure the availability of high-availability and high-quality cloud services and cover the need for accommodation resources of public bodies.

A high-security government data centre SHOULD be established, which will ensure the availability of high-availability and high-quality cloud services and cover the need for the accommodation resources of Administrations.

	Private cloud	**Community cloud (e.g., Government cloud)**	**Public cloud**
Users	Used by a single organization	Used by a community of consumers	Used by the general public
Operating model	Owned and operated by the organization itself, a third party or combination of both	Owned and operated by one or more organization of the community or a third party	Owned and operated by a business
Location	May exist on and off premises	May exist on and off premises	Exists on the premises of the Cloud provider
SLA/Uptime	No guarantees, data redundancy is self-managed	Guaranteed by provider, data redundancy is managed by the provider	Guaranteed by provider, data redundancy is managed by the provider
Timeline	Longer timelines due to deployment and testing	Faster timeline, plug and play model	Faster timeline, plug and play model

Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organization, comprising multiple users (e.g., business units). It may be owned, managed, and operated by the organization, a third party (e.g., a CSP), or a combination of these. The physical location may be on or off premises. There are no guarantees on SLAs/Uptime and data redundancy is managed by the entity itself. Solutions development on private Clouds typically consume more time as all the deployment and testing needs to be done in-house.

Common examples of a private Cloud for the Governmental sector are the entity's own Clouds, that are typically serving the entity or an exclusive collection of entities.

Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared/aligned interests (e.g., mission, cyber security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination of these. The physical location may be on or off premises. The SLAs/Uptime are guaranteed by the service provider, and the data redundancy is managed by the provider as well. This model offers a "plug and play" model which allows for faster timelines for deployment of new solutions.

A common form of community Cloud for the Public sector is a government-owned community Cloud, which is often cited as "G-Cloud" or "Gov-Cloud". This is a Cloud typically fully owned by a government and provisioned for the exclusive use of Governmental entities. Operations for this Cloud could be done by a Governmental entity, a third party (e.g. a CSP) or a combination of these. It is typically located inside the country, mainly to protect data sovereignty.

Public Cloud: The cloud infrastructure is provisioned for open use by a variety of entities. It may be owned, managed, and operated by a business, academic, or government organization, or a

combination of these. It exists on the premises of the cloud provider. Public Cloud is typically served by global players (e.g. AWS, Google Cloud, Microsoft Azure) as well as by local players (e.g. local telecom and ICT players). The SLAs/Uptime are guaranteed by the service provider, and the data redundancy is managed by the provider as well. This model offers a "plug and play" model which allows for faster timelines for deployment of new solutions.

Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds). A multi-Cloud approach, a similar model, is a composition of two or more distinct cloud infrastructures but without necessarily connectivity or orchestration between them. Such an approach is globally endorsed.

Potential government investments in cloud computing for the public sector should be evaluated on a case-by-case basis. Each case should be assessed from 1) a cybersecurity perspective to make sure it satisfies the national cyber security requirements, 2) a technical perspective to ensure its technical viability and 3) a commercial perspective to ensure it represents the most cost-efficient solution available.

7.4.9. Open Data ecosystem

Open data is digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere. Ugandan public bodies agree to follow a globally agreed set of principles, formulated by the International Open Data Charter[83]. These principles will form the foundation for access to data and for the release and use of data:

- Open by default
- Timely and comprehensive
- Accessible and usable
- Comparable and interoperable
- For improved governance and citizen

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 that is readable by machines.

Public bodies 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 license terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.

[83] https://opendatacharter.net/principles/

Public bodies must clearly communicate the right to access and reuse open data. Legal regimes for facilitating access and reuse, such as licenses, should be standardized as much as possible.

Despite the progress (described in section 7.1.11), the open data movement in Uganda faces challenges, including legal bottlenecks, low internet penetration, and the need for improved data literacy. Uganda SHOULD develop frameworks/policies to enhance data access and transparency. Open Data catalogue/portal SHOULD be developed.

7.4.10. Data Analytics Service and Big data

The Data Analytics Service ABB is an Application Service analysing a great amount of raw data to make conclusions about specific information. Data analytics services enable the automation of mechanical processes and algorithms that work over raw data for human consumption.[84]

In September 2023 by the Ministry of ICT and National Guidance, the Big Data Utilization Strategy 2023-2027 enables data-driven decision-making to drive economic growth and improve public services.[85]

7.4.11. Chatbot

Chatbot acts as the first level of customer support to provide quick answers to simple questions. Machine learning should be utilised to provide better answers. Questions that the bot cannot answer yet should be redirected to a human support specialist who will either take over the chat or reply via e-mail. Sentiment analysis can be used to automatically direct the questions to the right competent authority.

7.4.12. Artificial Intelligence Service

Artificial Intelligence (AI) Service ABB is an Application Service applying advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions. AI Component ABB is an Application Component serving any current or future Digital Service Infrastructure (DSI) requiring artificial intelligence capabilities. It enables the implementation of functionalities for applying advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions.

---

[84] https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/chapter-4-eira-glossary

[85] https://www.itu.int/en/publications/ITU-D/pages/publications.aspx?parent=D-UGA-BIGDATA

7.4.13. UGHub/Orchestration

Functions of the Orchestration Component ABB is performed by UGHub Orchestration is an Application Component defining the sequence and conditions in which one service invokes other services to realize some useful function.[86] Orchestration must be under the control of a service provider; however, it may be technically outsourced.

After shifting into Federated Architecture, UGHub MAY be used as sectoral gateway. Orchestration SHOULD be distributed from central (as central gateway) to the sectors and MDAs

7.4.14. Analytics and feedback

The GOU should create digital tools and put into place the procedures to ensure that feedback from citizens will be used for further service development. It is recommended that procedures define how the feedback is analysed and used to improve services. Giving feedback should be easy and convenient for the citizen.

To measure the performance of public services, every (electronic) service must record the duration of procedures and user feedback. This information will be transmitted to a central repository, where it can be matched with a service in the catalogue of services. Based on the data collected, evidence-based decisions can be made on which services need to be improved and in what way:

- tools for web analytics,
- information about procedures,
- number of applications,
- processing time,
- satisfaction and feedback.

7.4.15. Stylebook

The basic purpose of a stylebook is to establish a set of standard rules or style of presentation, to be applied to governmental websites and services, to maintain consistency and improve communication. This means a common set of guidelines for designing government services that includes CVI (corporate visual identity), design elements, reusable technical components, content strategy and style guide. Following a standard stylebook will make it easier for citizens to navigate and use different government services and will allow for significant cost savings when building those services.

[86] https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/chapter-4-eira-glossary

7.4.16. Consent Service

In situations where a third party wishes to use data about a person that they don't have a legal basis to. The consent service can be used to ask for the permission from the person to allow data registers to share the data with the third party.

Users can see the permissions that they had given when their data has been accessed and revoke the privileges, if needed. The consent management ABB is depicted in *Figure 29*.

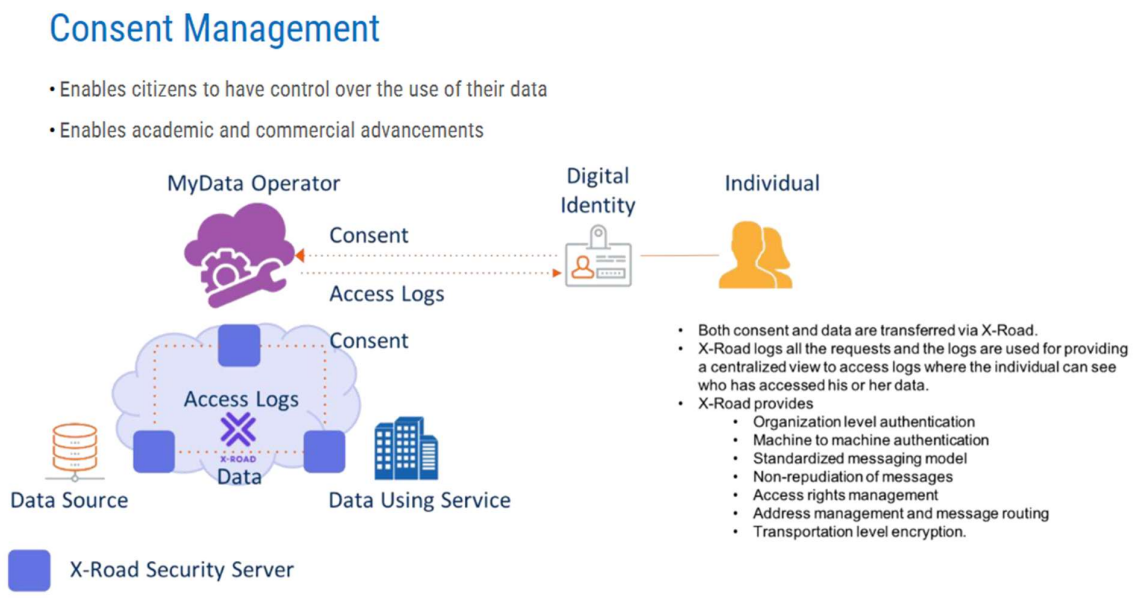

Figure 29 Consent Management ABB (Estonian case, internal report)

7.4.17. Spatial ecosystem

The interoperability of spatial systems means that relevant services are easy to use, and digital maps are accessible for all authorized users and for other information systems.

It must be possible for all agencies, enterprises and citizens to use digital maps which have been developed by the public sector on the basis on open GIS standards.

It must be possible to use geoinformation data sources to provide new e-services through open interfaces, and to add to the existing e-services links to geoinformation services, all without any significant additional costs. Authorized use of data must be ensured (e.g. objects falling into the category of nature conservation are only accessible for authorized users).

Spatial data infrastructure means a framework of administrative, technical and legal measures consisting of spatial data and spatial data sets, metadata thereof, network services and technologies, conditions of and agreements on sharing, access and use of data, coordination and monitoring mechanisms, administration processes and procedures.

Holders of information shall establish the following network services for the spatial data sets and services:[87]

- Discovery services making it possible to search for spatial data sets and services based on the content of the corresponding metadata and to display the content of the metadata.
- View services making it possible, as a minimum, to display, navigate, zoom in/out, pan, or overlay viewable spatial data sets and to display legend information and any relevant content of metadata.
- Download services, enabling copies of spatial data sets, or parts of such sets, to be downloaded and, where practicable, accessed directly.
- Transformation services, enabling spatial data sets to be transformed with a view to achieving interoperability.
- Services which allow to invoke spatial data services, including services for the organisation of e-commerce.

7.4.18. The address system

The system of address details is a set of common principles, which ensures a standardised identification of address objects, both in their location and in different information systems, and allows the comparison of addresses submitted at different times and based on different principles.

7.4.19. Document management system

Document management has 3 main components that all systems must support:

- hierarchical classification scheme based on the tasks of the institution (or common for the GOU).
- lifecycle management, which means that the system must be able to manage documents from their creation or receipt to their destruction or separation for transfer to another information system, which is an archive.
- system of access rights and restrictions, including tools for eID and e-signature

Basic functionality of the document management system SHOULD meet the requirements of MoReq.[88]

[87] https://inspire.ec.europa.eu/network-services/41

[88] MoReq: https://www.moreq.info/

8.Cross-Functional Requirements

This chapter defines the horizontal requirements that pervade all layers of the national architecture. GIRA-2026 moves away from the term "Non-Functional Requirements" to Cross-Functional Requirements (CFR) to emphasize that these constraints are directly tied to business functions and are not merely technical preferences.[89] The core CFR are depicted in Figure 30.

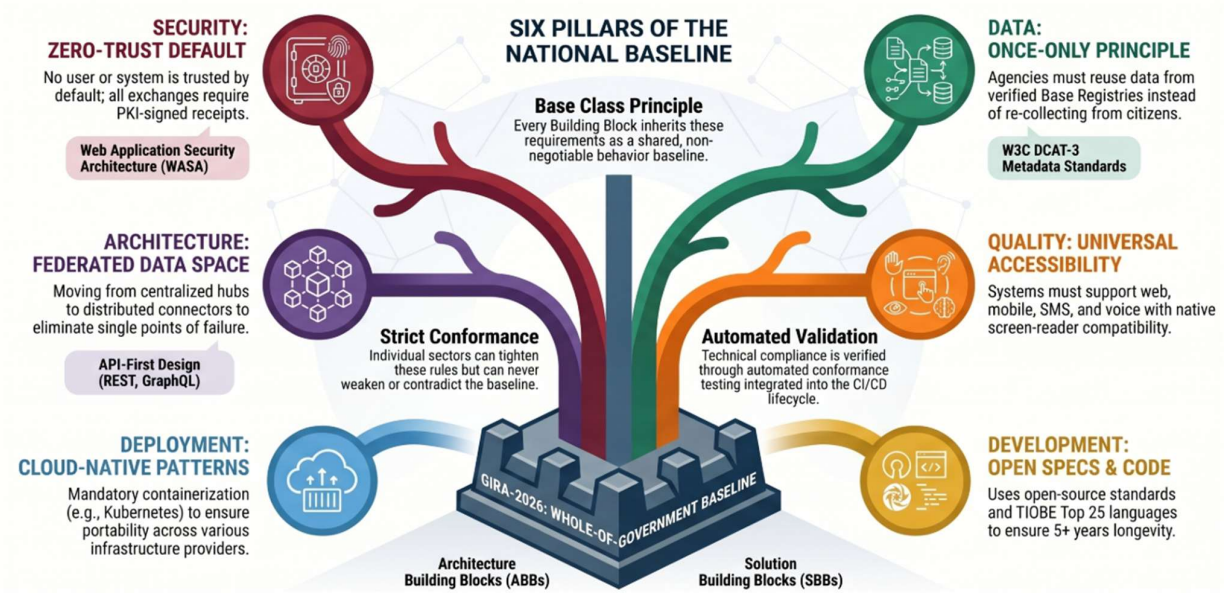

Figure 30 Cross-Functional Requirements

The GIRA-2026 adopts an "object-oriented" approach to specifications. The cross-functional requirements defined here serve as the baseline "base class" for the entire ecosystem.

- Mandatory Inheritance: Every Architecture Building Block (ABB) and Solution Building Block (SBB) inherits these CFRs as a shared behaviour baseline.
- Strict Conformance: Building Blocks can tighten or elaborate on these rules for specific domains (e.g., Health or Finance) but cannot contradict or weaken the cross-functional baseline.
- Validation: Any system meeting a GIRA-2026 Building Block specification automatically meets this cross-functional baseline, simplifying compliance and automatic testing.

Aligning with international best practices from the GovStack architecture, the Uganda GIRA-2026 organizes CFRs into six core sub-categories described in following sections.

[89] https://specs.govstack.global/architecture/6-cross-functional-requirements

8.1. Security

Zero-Trust Default: MDAs MUST implement a zero-trust model where no user or system is trusted by default.

Cryptographic Non-Repudiation: Technical exchanges MUST utilize receipts signed via the National PKI to provide undeniable proof of origin and receipt.

WASA Compliance: Web applications MUST adhere to the Web Application Security Architecture (WASA) framework.

8.2. Data

Data-Centricity: The Dataset is the primary object of governance; requirements apply to the information asset regardless of the hosting system.

Once-Only Principle: MDAs SHALL NOT request data from citizens that is already available in a verified national Base Registry.

Semantic Standards: All datasets MUST conform to W3C DCAT-3 and use specified single identifiers for core objects like persons and land.

8.3. Architecture

Federated Data Space: Architecture MUST move from centralized "hub-and-spoke" models to distributed Sovereign Connectors to eliminate Single Points of Failure (SPOF).

API-First Design: All new systems MUST expose functionality via secure, versioned, and well-documented APIs (REST, GraphQL, etc.).

AI Readiness: Building Blocks utilizing AI MUST ensure algorithmic transparency, making automated decisions explainable and auditable.

Communication between SBB. Building blocks MUST NOT use shared databases, file systems or memory for data exchange with other building blocks. Communication with other building Blocks (BB) MUST be realised only via API. More information: Amazon API Mandate: https://api-university.com/blog/the-api-mandate/ .

Secure Data Exchange. Data exchange between GOU information systems MUST take place inside the Secure Data Exchange (SDE)

8.4. Quality

Universal Accessibility: All public sector websites and services SHALL comply with WCAG 2.1 AA quality criteria: https://www.w3.org/TR/WCAG21

Observability Baseline: Every operational component MUST include built-in metrics for performance and reliability that feed into national monitoring dashboards.

Human-in-the-Loop (HITL): AI-driven administrative decisions MUST include a mandatory human-in-the-loop requirement to ensure accountability.

8.5. Deployment

Cloud-Native Default: Systems SHOULD be designed using cloud-native patterns (containerization, microservices) to ensure portability across the National Data Centre and edge infrastructures.

Digital Continuity: A long-term preservation policy MUST be applied to ensure electronic records remain legible and reliable over time, regardless of technological obsolescence.

8.6. Development

Open Specification Preference: MDAs MUST give preference to open standards and open-source software to prevent vendor lock-in.

Automated Testing: Technical compliance MUST be verified through automated conformance testing integrated into the CI/CD lifecycle.

Version control: All source code, configuration and infrastructure definitions are managed in Git or an equivalent distributed version control system.

Clear Code: All application source code and comments are clear, maintainable and written in English. Follow Best Practices for Public Code: https://standard.publiccode.net/

Use Top 25 Languages. Building blocks SHOULD be written using commonly used languages to ensure ongoing maintenance and support are as easy as possible. Building blocks MAY leverage less common languages, such as shell scripting where needed. Preference for TIOBE Top 25 Languages: https://www.tiobe.com/tiobe-index/

End-of-LIFE (EO)L SHOULD be at Least 5 Years. NO languages, frameworks, or dependencies SHOULD be used in a building block where that component has EOL of less than 5 years.

Containers: Building blocks MUST be deployable as a container orchestration (e.g. Kubernetes), and CI/CD pipelines.

Testing: The application must have passed security testing before going into production. According to the nature of the application and the risk analysis, implement measures to follow the recommendations given in the OWASP threat tables: https://owasp.org/www-project-top-ten/

9.Privacy Viewpoint

The Interoperability Privacy viewpoint in Figure 31 highlights the GIRA building blocks that are relevant when implementing the Data Protection and Privacy Act 2019 (DPPA) or assessing an existing architecture against the data protection principles. MDAs must indeed guarantee the citizens' privacy, and the confidentiality, authenticity, integrity, and non-repudiation of information provided by citizens and businesses.

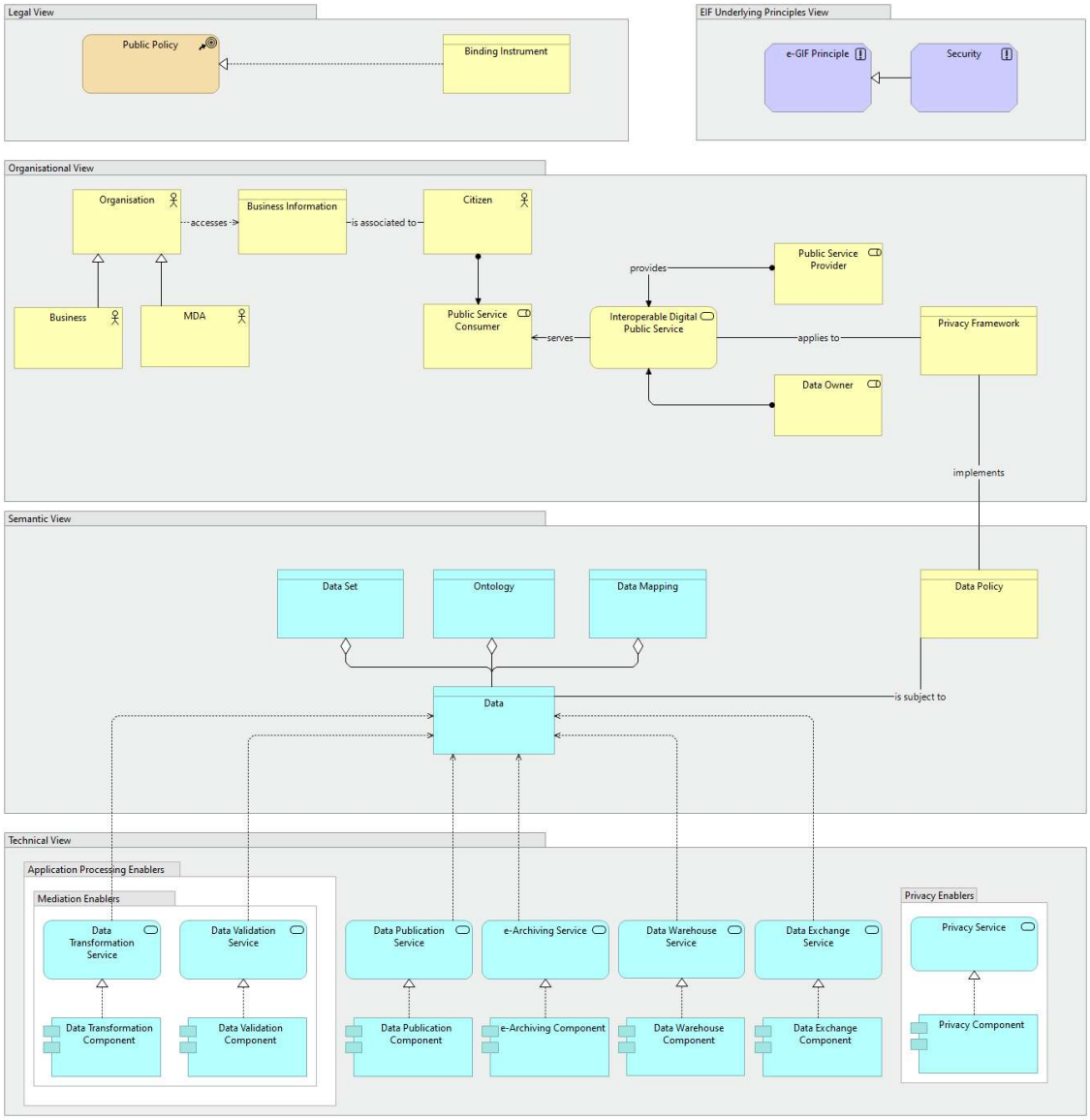

Figure 31 Privacy viewpoint

10. Security viewpoint

Security Architecture (SA) layers in the architecture will be present and pervade through all areas and layers, and cover access to data, systems, and services along with other dimensions of protection from threat, vulnerability exploitation and intrusion.

The Security Architecture viewpoint models the Architecture Building Blocks related to 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, e.g., the Regulation on electronic identification and trust services. The SA viewpoint of the GEA is illustrated in Figure 32.

Security is a primary concern in the provision of public services. When public administrations 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 administrations, 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 Framework is Agreed governance approach focusing on protection aspects on data, information and knowledge assets and organisational resources handling them. More specifically, the Security Framework comes in the form of the Web Application Security Architecture Framework (WASA Framework). It focuses solely on the security architecture of web applications that enable and run e-services. The WASA Framework is intended as an easy-reading guide and a practical Toolkit for GOU's public sector organisations who seek support for protecting their web application for two scenarios:

- Guidance for developing new secure web applications applying security-by-design principle from scratch
- Guidance on validating security controls of existing web applications (i.e., security assessment/auditing, security/penetration testing).

Combining two well-respected security methodologies, SABSA and OWASP ASVS, and customising to meet the needs of GOU, the WASA Framework derives from business attributes (requirements) technical security requirements of web applications while keeping the methodological overhead as slim as possible.

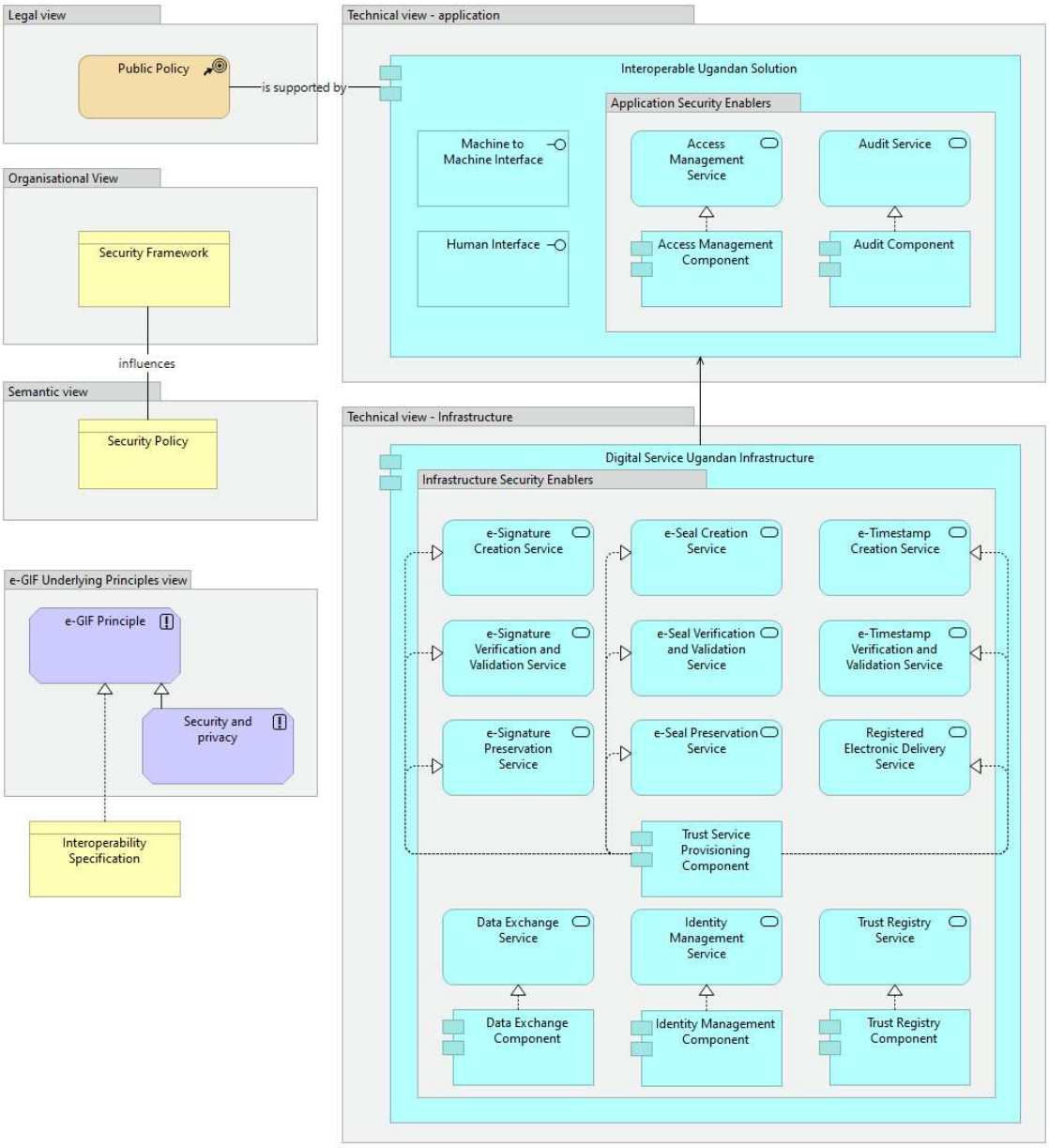

Figure 32 Security viewpoint

11. Definitions

Access Management Component. Implements the functionalities of allowing users to make use of IT services, data, and/or other assets. Access management helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorised users are able to access or modify the assets.

Access Management Service. Shares the functionality of allowing users to make use of IT services, data, and/or other assets. Access management helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users can access or modify the assets.

AI service. Artificial Intelligence as a Service is the third party offering of artificial intelligence outsourcing. AI as a service allows individuals and companies to experiment with AI for various purposes without large initial investment and with lower risk.

AI-readiness. AI-readiness is the extent to which Uganda's governance structures, data assets, digital infrastructure, workforce, and operational processes can support the responsible deployment and scaling of AI across government, in alignment with national development priorities and public trust.

Architecture Building Block. An Architecture Building Block (ABB) is a constituent of the architecture model that describes a single aspect of the overall model. An Architecture Building Block describes generic characteristics and functionalities. Architecture Building Blocks are used to describe reference architectures, solution architecture templates or solution architectures of a specific solution. Source TOGAF®: https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_8.

Architecture Principle. Architecture Principles define the underlying general rules and guidelines for the use and deployment of all IT resources and assets across the enterprise. They reflect a level of consensus among the various elements of the enterprise and form the basis for making future IT decisions. Source TOGAF® 9.2 The Open Group: https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap20.html#:~:text=Architecture%20Principles%20define%20the%20underlying,for%20making%20future%20IT%20decisions.

Architecture Requirement is a requirement of the highest possible level of granularity for an Architectural Building Block, formulated as an agreed normative statement of a To-Be GOU Public Service

Audit Component. Implements the functionality of providing support for the principle of accountability, which is holding the users of a system accountable for their actions within the system and is detecting policy violations. The audit policy defines the elements of an information system which need to be traced, for example to assure traceability of actions: what, how, when, where and with what.

Audit Service. Shares the audit functionality of providing support for the principle of accountability, which is holding users of a system accountable for their actions within the system, and detection of policy violations. The audit policy defines the elements of an information system which need to be traced, for example to assure traceability of actions: what, how, when, where and with what.

The Audit Service ABB is salient for technical interoperability because it defines the elements of an information system which need to be traced, for example to assure traceability of user actions. ADMs should ensure that 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.

Base Registry Data Policy. A Data Policy applying to a trusted authentic source of information under the control of an appointed public administration or organisation appointed by government.

Base registries are reliable sources of basic information on items such as persons, companies, , buildings, and are authentic and authoritative cornerstone of public services.

The Base Registry Data Policy ABB is salient for semantic interoperability because base registries include "authoritative sources of information", that need to be properly governed and made available. EIF's includes base registries in the conceptual model for integrated public services and describes it as "the cornerstone of Ugandan public service delivery".

Big data infrastructure. Big data infrastructure entails the tools and agents that collect data, the software systems and physical storage media that store it, the network that transfers it, the application environments that host the analytics tools that analyse it and the backup or archive infrastructure that backs it up after analysis is complete.

Binding Instrument. The Binding Instrument ABB is relevant for interoperability as, by being a specialisation of the Legal Act, it makes mandatory the implementation of the policy (and therefore the underlying interoperability implications).

Business. Economic operator with a legal entity entitled to perform a private activity for a profit. The Business ABB is salient for organisation interoperability because organisations can play the role of consumers of Public Services.

Business information. Organisationally constructed meaning describing business facts, assets, or opinions that are exchanged in the context of a public service to support its delivery. Examples include an invoice, a medical prescription, a driving license. The Business Information ABB is salient for organisational interoperability because it represents the entity being exchanged between organisations. Its interoperability needs to be guaranteed by means of organisational and semantic interoperability specifications.

Catalogue of business processes. Inventory of business processes with comprehensiveness and trustiness value.

Catalogue of data services. The repository ensures the interoperability of public sector information systems and the reuse of technical, organisational and semantic resources. The service repository is an addition to the metadata kept in the Database of Databases and includes specifications for all web services and a detailed description of government services (including business process descriptions). The repository describes the machine interface of services. This information is needed for establishing machine-machine data exchange.

Catalogue of information systems and registries. This component provides metadata about government registries and information systems: the name of; owner; type; list of services; information about registration and approval; technical architecture; legal acts; SLA; security

parameters; logical structure of data (data objects, data fields, parameters of fields).

Catalogue of legislation.

Catalogue of public services. The repository describes human interfaces of public services. This information can be used for building citizen portals.

Catalogue of semantic assets. The repository provides information about reusable components: semantic assets, guidelines, etc.

Catalogue of standards. NITA-U has developed a Standards Catalogue that contains a complete list of NITA-U standards available in the standards library. These standards have been developed through consensus by industry, consumers, government departments, research organizations, universities and private institutions.

Citizen. An individual is a principal that provides and/or consumes Public Services. A citizen has rights because of being born in Uganda or because of being given rights. The Citizen ABB is salient for organisation interoperability because citizens can play the role of consumers of Public Services.

Content Management Service. A Content Management System (CMS) is responsible for:

- developing Website templates and functionalities assigning appropriate user permissions and workflows providing trainings to the web working group
- developing tools and web controls to speed up and facilitate the work of the web working group
- giving support and advice to the web working group
- ensuring continuity of service and performance
- ensuring security and accessibility on the website
- ensuring disaster recovery processes and backup procedures
- setting up the website information architecture within the CMS
- setting up alert procedures and analytics on usage of the platform.

The Content Management Service ABB is salient for technical interoperability because it provides and shares the functionalities of dynamic creation, distribution, and analysis of contents (images, videos, etc.). Catalogues help others to find reusable resources (e.g., services, data, software, data models). Various types of catalogues 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.

Controlled Vocabulary. A controlled vocabulary is an organised arrangement of words and phrases used to index content and/or to retrieve content through browsing or searching. It typically includes preferred and variant terms and has a defined scope or describes a specific domain.

The Data Model ABB is salient for semantic interoperability because it ensures compatible interpretations of words and phrases used to index content and/or to retrieve content through browsing or searching.

Data. Data are symbols obtained through an encoding process of business information or a legal act.

Data Exchange Component. Implements the functionality that enables the secure exchange of messages, records, forms, and other kinds of data between different ICT systems.

Data Exchange Service. Shares the functionality that enables the secure exchange of messages, records, forms, and other kinds of data between different ICT systems.

Data mapping. Data mapping is an equivalence relationship between two data items with ontological value. Data mapping is used for a wide variety of tasks, including:

- Data mediation between a data source and a destination.
- Data transformation
- Identification of data relationships as part of data lineage analysis.
- Discovery of hidden sensitive data such as the last four digits of a social security number hidden in another user id as part of a data masking or de-identification project.
- Consolidation of multiple databases into a single database and identifying redundant columns of data for consolidation or elimination.

The Data Mapping ABB is a key interoperability enabler because it supports to achieve legal behavioural interoperability by enabling the exchange of data, information, and knowledge between digital public services.

Data Mapping Catalogue. Indexed inventory of data mappings with comprehensiveness and trustiness value. This ABB is a key interoperability enabler for sharing/PROVISIONING and reusing/CONSUMING Data.

Data Model. A collection of entities, their properties, and the relationships among them, which aims at formally representing a domain, a concept or a real-world thing

The Data Model ABB is salient for semantic interoperability because it ensures compatible interpretations of data exchange.

Data Owner. Data owners are either individuals or teams who make decisions such as who has the right to access and edit data and how it is used. Owners may not work with their data every day but are responsible for overseeing and protecting a data domain. Data owners are accountable for the quality, integrity, and protection of their data space.

The Data Owner ABB is salient for organisational interoperability because it is responsible for the management of the data generated or consumed by the public service. The identification of Data Owners is important for accountability since it clearly identifies a person/team responsible of controlling the compliance of data, and for the definition of policies and standards of public service data.

Data Policy. A set of broad, high-level principles which form the guiding framework in which data management can operate. The Data Policy ABB is important for semantic interoperability because it provides a guiding framework to manage data and information according to interoperability principles.

Data Portability Policy. The data portability policy implements the right to data portability. It regulates the exchange of data, allowing data subjects to obtain data that a data controller holds on them and to reuse it for their own purposes.

Individuals are free to either store the data for personal use or to transmit it to another data controller. The data must be received "in a structured, commonly used and machine-readable format".

The right to data portability applies:

- To personal data that an individual has given to a data controller.
- When the processing is carried out by automated means; and
- Where the processing is based on the individual's consent or for the performance or a contract.

The Data Portability Policy ABB is salient for semantic interoperability because it regulates how data can be exchanged and its reuse.

Data Publication Component. Implements the functionality of making data available for common use. The Data Publication Component ABB is salient for technical interoperability because it provides the implementation of the functionalities to make public data freely available for use and reuse by others unless restriction apply.

Data Publication Service. Shares the functionality of making data available for common use. The Data Publication Service ABB is salient for technical interoperability because it provides the functionalities to make public data freely available for use and reuse by others unless restriction apply

Dataset. The Semantic view models the most salient Architecture Building Blocks that should be considered to support semantic aspects for the End-to-End design of interoperable digital public services.

DataSet Catalogue. Indexed inventory of data sets with comprehensiveness and trustiness value. This ABB is a key interoperability enabler for sharing/PROVISIONING and reusing/CONSUMING Data. The Data Set catalogue ABB is a key interoperability enabler because it supports to achieve semantic structural interoperability by ensuring the provision/consumption of data by digital public services.

Data Syntax. Data Syntax is a set of rules defining the way in which data is put together with appropriate identifiers, delimiters, separator character(s), and other non-data characters to form messages. The Data Syntax ABB is salient for semantic interoperability because it provides the rules establishing how data must be written.

Data Transformation Component. Implements the functionality of conversion of data from one data representation to another. The Data Transformation Component ABB is salient for technical interoperability because it enables the implementation of the functionalities to transform internal data structures to common and agreed interoperable formats.

Data Transformation Service. Shares the functionality of conversion of one data representation to another. The Data Transformation Service ABB is salient for technical interoperability because it provides the functionalities to transform internal data structures to common and agreed interoperable formats.

Data Validation Component. Implements the functionality of referring to any activity aimed at verifying that the value of a data item comes from a given set of acceptable values. Data validation

may be followed by corrective actions, such as data editing or data imputation. In statistics, imputation is the process of replacing missing data with substituted values. The Data Validation Component ABB is salient for technical interoperability because it allows the implementation of the functionality to validate if data received (or to be sent) is compliant with common and agreed interoperable formats.

Data Validation Service. Shares the functionality of referring to any activity aimed at verifying that the value of a data item comes from a given set of acceptable values. Data validation may be followed by corrective actions, such as data editing or data imputation.

Data Warehouse Component. A data warehouse Component is part of the central repository where raw data is transformed and stored in query able forms. It is an information system that contains historical and commutative data from single or multiple sources. It simplifies reporting and analysis process of the organisation. The Data Warehouse Component ABB is salient for technical interoperability because it provides and shares the functionality for the short or medium-term preservation of records and information in electronic form to ensure their temporal legibility, reliability, and integrity, and to ease their management.

Data Warehouse Service. A data warehouse is a central repository where raw data is transformed and stored in query able forms. It is an information system that contains historical and commutative data from single or multiple sources. It simplifies reporting and analysis process of the organization. The Data Warehouse Service ABB is salient for technical interoperability because it provides and shares the functionality for the short or medium-term preservation of records and information in electronic form to ensure their temporal legibility, reliability and integrity, and to ease their management

Descriptive Metadata Policy. A Data Policy aiming at making data discoverable and identifiable. It may mandate elements such as title, abstract, author, and keywords.

The Descriptive Metadata Policy ABB is crucial for semantic interoperability because metadata facilitates opening and sharing data by providing the appropriate format, description of the content, high level of quality to achieve interoperability. 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 license terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.

Development and Testing Service. Development and testing service is a complicated process to design and testing an application or software to meet a particular business or personal objective, goal or process.

Digital Service Infrastructure. Infrastructure which enables networked services to be delivered electronically, typically over the internet, providing Ugandan interoperable services of common interest for citizens, businesses and/or public authorities, and which are composed of core service platforms and generic services. The Digital Infrastructure Service ABB is salient for technical interoperability because it a central element through which interoperability is ensured.

e-Archiving Component. Shares the functionality of enabling the permanent or long-term storage of selected (by an authority) electronic documents or information for preservation purposes like their enduring research value and memory aid.

The GIRA differentiates between document management, record management and e-archiving as follows:

- Document management is primarily about day-to-day use of electronic documents (create/update/delete/versioning) within the operational environment.
- Record management is primarily about ensuring that information (e.g., in form of an electronic document or database record) is available for business and legal purposes (e.g. to proof and track the handling of contracts). If an electronic document or information is becoming a record (an authority declares it as a record), that electronic document or information needs to be handled by the record management service (based on specific business or legal reasons (e.g., contract negotiation)).
- e-Archiving is primarily about storing records which have been selected (by an authority) for permanent or long-term preservation due to their enduring research value and as a memory aid. An electronic document or information which a) is managed by the document management service or the record management service and b) is no longer needed for business or legal purposes or day-to-day activities, and c) still has value for research purposes or as a memory aid, the electronic document should be managed by the e-archiving service.

The e-Archiving Component ABB is important for technical interoperability because it provides the implementation of the functionalities for the long-term or permanent preservation of records and information in electronic form in order to ensure their temporal legibility, reliability and integrity.

e-Archiving Service. Shares the functionality of enabling the permanent or long-term storage of selected (by an authority) electronic documents or information for preservation purposes like their enduring research value and memory aid.

e-GIF Principle. Underlying principle stipulated by the Uganda Interoperability Framework.

e-Payment Component. Implements the functionality of executing payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device. The e-Payment Component ABB is salient for technical interoperability because it provides the implementation of functionalities of executing payment transactions.

e-Payment Service. Shares the functionality of executing payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device. The e-Payment Service ABB is salient for technical interoperability because it enables the possibility of executing payment transactions by any means of telecommunication, digital or IT device.

e-Seal Creation Service. Shares the functionality of signing data in electronic forms on behalf of a legal person. **An 'electronic seal'** means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. The 'creator of a seal' is a legal person who creates an electronic seal.

e-Seal Preservation Service. Shares the functionality of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

e-Seal Verification and Validation Service. Shares the functionality of the verification of documents that are signed electronically.

e-Signature Creation Service. Shares the functionality of signing data in electronic form by a natural person. **An 'electronic signature'** means data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign.

e-Signature Preservation Service. Shares the functionality of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

e-Signature Verification and Validation Service. Shares the functionality of the verification of documents that are signed electronically.

e-Timestamp Creation Service. Shares the functionality of the verification of timestamps used for establishing evidence that a give piece of data existed at a given point in time. An **'electronic time stamp'** means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

e-Timestamp Verification and Validation Service. Shares the functionality of the verification of timestamps used for establishing evidence that a given piece of data existed at a given point in time.

Hosting and Networking Infrastructure. Shares the functionalities for i) hosting Interoperable Ugandan Solutions and ii) providing the necessary networks for operating these solutions.

Interoperability Framework (e-GIF). An agreed governance approach to interoperability for organisations that wish to collaborate towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, guidelines, and recommendations.

The Interoperability Framework ABB is an interoperability enabler because it helps achieve organisational interoperability by defining a set of rules, practices, and a commonly agreed approach to the delivery public services.

Interoperability Governance. Set of organising rules assuring the functioning of an Interoperability Framework. These rules include structures, roles, responsibilities, policies, standards, specifications, practices, decision making and operational procedures. The Interoperability Governance ABB is an interoperability enabler because it helps achieve organisational interoperability.

Interoperability Organisational Authority – NITA-U. An organisation having the powers to govern the interoperability of public administration. The Interoperability Organisational Authority ABB is an interoperability enabler because it helps achieve organisational interoperability by ensuring political and/or administrative governance of the interoperability capabilities of an organisation.

Interoperability Requirement. An Interoperability Requirement is a requirement of the highest possible level of granularity for a GIRA ABB, formulated as an agreed normative statement in functional terms on a legal, organisational, semantic, or technical attribute of a To-Be GOU Public Service

Interoperability Skill. Expertise in organising, implementing, and managing interoperability in digital public services. The Interoperability Skill ABB is an interoperability enabler because it helps achieve organisational interoperability by removing a barrier to implement interoperability policies.

Interoperable Solution. A solution developed by ADMs that facilitate the delivery of electronic Public Services between ADMs (or Citizens and Business) in support to the implementation and advancement of Public Policies.

Interoperable Solution Component. Interoperable GOU Solution Component represents the encapsulation of a functionality provided by an Interoperable GOU Solution. The Interoperable GOU Solution Component ABB is salient for technical interoperability because it is a central element of the e-GIF conceptual model for integrated public services. It represents all the functionalities provided by Interoperable Solutions.

Interoperable Solution Service. Represents an explicitly defined shared application behaviour of an Interoperable Solution. The Interoperable Solution service ABB is salient for technical interoperability because it is a central element of the e-GIF conceptual model for integrated public services. It represents the generalisation of all application services provided by Interoperable Solutions.

Interoperability Specification. An Interoperability Specification is a document formulated as an agreed normative statement in design terms on a legal, organisational, semantic, or technical attribute. It can refer to existing standards or specifications.

Interoperability Strategy. The overarching strategic plan in interoperability. The Interoperability Strategy ABB is an interoperability enabler because it helps achieve organisational interoperability by setting up the vision and principles for the development of the interoperability capabilities. The e-GIF implements Ugandan Interoperability Strategy.

Interoperable Digital Public Services. An Interoperable digital public service is a service provisioned by or on behalf of a MDA in fulfilment of a public policy goals servicing to users either citizens, businesses, or other public administrations. A GOU public service comprises any public service supplied by ADM, either to one another or to businesses and citizens. Once or more Digital Public Service can realize one Digital Business Capability.

The Public Service ABB is salient for organisational interoperability because it is the central element around which interoperability needs to be ensured.

GIRA Architecture Building Block is a requirement of an intermediate level of granularity, in alignment with at least one e-GIF principle, formulated as an agreed normative statement in functional terms on a legal, organisational, semantic, or technical attribute of a To-Be GOU Public Service.

GIRA Solution Building Block is a concrete component of an intermediate level of granularity, that it implements one or more GIRA Architecture Building Blocks of an GOU's Public Service, formulated as an agreed normative statement in design terms on a legal, organisational, semantic, or technical attribute of an GOU's Public Service. On the technical view, a Solution Building Block is a specific software component that it might be either procured or developed of a To-Be Interoperable GOU Solution or that it is integrated in an As-Is GOU Solution

GIRA View. The GIRA consists of several architecture views, including one view for each of the e-GIF interoperability levels. The GIRA views contain a graphical notation of the GIRA ontology.

TOGAF®: An architecture view is a representation of a system from the perspective of a related set of concerns. https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_17.

GIRA Viewpoint. The GIRA provides several viewpoints that conform to GIRA views. The viewpoints provide a perspective with specific stakeholder's concern in mind. TOGAF®: A specification of the conventions for a particular kind of architecture view. Source https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_18.

Hosting Facility. The equipment supporting the hosting of Interoperable Solutions and their components, usually embodied in a building. The Hosting Facility ABB is salient for technical interoperability because it provides all the equipment supporting the hosting of interoperable solutions and their components.

Hosting Service. Shares the functionalities of a hosting provider, typically a high availability and high-performance hosting infrastructure that is being comprised, among other elements, of back-end web server instances and application servers for hosting and serving both static and dynamic sites. The Hosting Service

Human Interface. A boundary set of means enabling the exchange of data between an individual and a service. This ABB is a key interoperability enabler for assessing compatible interfaces. The Human interface ABB is a key interoperability enabler because it supports to achieve technical behavioural interoperability by enabling the exchange of data, information, and knowledge between digital public services and individuals.

Identity Management Component. Implements the functionality of user authentication. `**Electronic identification'** means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. **'Authentication'** means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.

Identity Management Service. Shares the functionality of user authentication.

Interoperability Requirement is a requirement of the highest possible level of granularity for an GIRA ABB, formulated as an agreed normative statement in functional terms on a legal, organisational, semantic, or technical attribute of a To-Be GOU Public Service

Interoperability Specification. An Interoperability Specification is an agreed normative statement on a legal, organisational, semantic, or technical level. It can refer to existing standards or specifications.

Interoperable Solution Component. Interoperable Ugandan Solution Component represents the encapsulation of a functionality provided by an Interoperable GOU Solution.

Interoperable Solution Service. Represents an explicitly defined shared application behaviour of an Interoperable Ugandan Solution.

Key Interoperability Enabler. A Key Interoperability Enabler is a GIRA ABB, which is necessary to enable the efficient and effective delivery of public services across ADMs.

Legal Act. Formalised set of rules on a subject potentially including requirements concerning digital public services. The granularity of the requirements might be of high level or detail level.

Requirements of high-level granularity contain generic/abstract functional requirements like principles and/or recommendations with considerable degrees for transposition/execution and of not binding nature. On the other side, requirements of detail-level granularity imply a limited degree for transposition/execution, and they contain specific/concrete functionalities, solution components, data, procedures, and/or technical specifications or standards to be used.

The Legal Act ABB is salient for interoperability because it helps achieve legal interoperability by ensuring compatible legal/juridical certainty in the exchange of information.

Legal agreements/ International treaties. Under international law, a treaty is any legally binding agreement between states (countries). A treaty can be called a Convention, a Protocol, a Pact, an Accord, etc.; it is the content of the agreement, not its name, which makes it a treaty.

Legal Authority. It is an entity with entitled powers. The powers that a public administration exercises during the above-mentioned life cycle are of the following four types: Legislation, control (monitoring, enforcing, sanctioning, etc.), economic (taxes, subsidies, expenditures, funding, etc.) and (public service) provision.

The Legal Authority ABB is salient for interoperability because it supports legal interoperability by providing reliability and trustworthiness of the Legal Interoperability Agreement.

Legal Interoperability Agreement. A legal interoperability agreement is a legal resource formalising governance rules enabling collaboration between digital public services (NITA-U Act (Act No. 4 of 2009)).

The Legal Interoperability Agreement ABB is a key interoperability enabler because it supports legal interoperability by enabling the seamless exchange of data, information, and knowledge.

Legal Interoperability Specifications. A Legal Interoperability Specification is a document of the highest possible level of granularity on a GIRA SBB, formulated as an agreed normative statement in design terms. It can refer to existing standards or specifications.

The Legal Interoperability Specification ABB is relevant for interoperability because it helps achieve legal interoperability by addressing the core legal interoperability background for solutions.

Legislation Catalogue. Indexed inventory of legal documents with comprehensiveness and trustiness value.

This ABB is a key interoperability enabler because it supports to achieve legal structural interoperability by enabling sharing/provisioning and reusing/consumption of legislation on digital public services.

Legislation on data information and knowledge exchange. Legal act on the exchange of data, information, and knowledge between different agents (private and public) at national and/or cross-border level.

The Legislation on Data, information, and Knowledge Exchange ABB is a key interoperability enabler because it supports to achieve legal interoperability by ensuring legal/juridical certainty and determinacy in the exchange of data, information, and knowledge.

Machine to Machine Interface. A boundary set of means enabling the exchange of data between a service and other services.

Master Data Policy. A Data Policy applying to the authoritative, most accurate data that is available about key business entities, used to establish the context for business transactions and transactional data.

The Master Data Policy ABB is important for semantic interoperability because Master Data is used to establish the context for business transactions and transactional data by providing accurate data usually stored and available for reuse by other parties. Its management should be prioritised.

Metadata Management Component. Implements the functionalities for the i) creation, ii) storage, iii) categorisation and iv) retrieval of metadata.

The Metadata management Component ABB is essential for interoperability because it provides the implementation of the functionalities to manage metadata. e-GIF recommends prioritising it: "Put in place an information management strategy at the highest possible level to avoid fragmentation and duplication. Management of metadata, master data and reference data should be prioritised."

Metadata Management Service. Shares the functionalities for the i) creation, ii) storage, iii) categorisation and iv) retrieval of metadata.

Network. Transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet- switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. The Network ABB is salient for technical interoperability because it provides the network where can operate interoperable solutions (both public and private network).

Networking Service. Shares the functionalities provided by a network provider which is the combination of transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet- switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

Non-Binding Instrument. Legal means, involving no obligation, which are available to the ADM to carry out their tasks, like recommendations and opinions.

The Non-binding Instrument ABB is a key interoperability enabler as a specialisation of the Legal Act.

Ontology. An Ontology is a formal description of knowledge as a set of concepts within a domain and the axioms connecting concepts and allowing for logic inferences. When speaking about an ontology, we do not refer only to the terminology (or T-Box) but also to all the "assertions" about the concepts and roles (the A-Box), i.e., all the individuals or instances of concepts and roles of the terminology and as important, the rules for logic inference: the semantics "part".

The Ontologies ABB is salient for semantic interoperability because it is defined as a simplified, reusable, and extensible data model that captures the fundamental characteristics of a data entity in a context-neutral and syntax-neutral fashion.

Ontologies Catalogue. Indexed inventory of ontologies with comprehensiveness and trustiness value. This ABB is a key interoperability enabler (*) for sharing/PROVISIONING and reusing/CONSUMING Data. The Ontologies catalogue ABB is a key interoperability enabler because it supports to achieve semantic structural interoperability by ensuring the provision/consumption of ontologies by digital public services.

Open Data Policy. The rules and practice of publishing (raw) data in a way that is accessible, reusable, machine readable and licensed permissively. It can be generated by a wide range of parties,

including public authorities, the semi-public sector, businesses and the public. In the case of MDA, making their data available for public reuse supports economic development, openness, and transparency.

The Open Data Policy ABB is crucial for semantic interoperability because Open Data is a part of the basic components of the e-GIF conceptual model for integrated public services.

Orchestration Component. Implements the functionality of defining the sequence and conditions in which one service invokes other services to realise some useful function. The Orchestration Component ABB is a key for technical interoperability because it provides a set of various methods to manage existing business processes or define and establish new ones. BPM components also execute business process documented through accepted modelling techniques.

Orchestration Service. Shares the functionality of defining the sequence and conditions in which one service invokes other services to realize some useful function. The Orchestration Service ABB is important for technical interoperability because it provides the functionality of "automated" business processes coordination. The e-GIF Conceptual model for integrated public services foresees the concept a Coordination for Integrated Service Delivery. The Model comprises an "integrated service delivery" is based on a "coordination function", which is related to SOA principles such as choreography and orchestration, to manage internal business processes in order to remove complexity for the end-user. This function should select the appropriate sources and services and integrate them. Coordination can be automated or manual.

Organisation. An Organisation is a principal that provides and/or consumes Public Services.

The Organisation ABB is important for organisation interoperability because organisations can play the role both of providers of Public Services (mainly ADMs) and consumers of Public Services (ADM or businesses).

Organisational Interoperability Agreement. Organisational Agreement means any agreement to which the Company or any Restricted Subsidiary is a party pursuant to which, among other things, fees are paid to the Company or a Restricted Subsidiary in exchange for organisational, consulting or similar services.

Organisational Interoperability Requirement. An organisational interoperability requirement is an interoperability requirement that must be met to help achieve organisational interoperability.

Point of single contact. Point of Single Contact (PSCs) is e-government portal that allow service providers to get the information they need and complete administrative procedures online. The Ugandan PCS is a one-stop online centre for Government online services. Its main objective is to enhance Government service delivery to citizens, non-citizens, businesses and to Government Ministries, Departments and Agencies (MDAs). The benefits include making Government services more accessible, reducing access cost and queuing at Government offices, transparency, timeliness and increasing convenience of transaction with the Government of Uganda ANYTIME and from ANYWHERE.

Ugandan PCS: https://ecitizen.go.ug/content/ecitizen-portal

Privacy Component. Privacy Component implements the functionalities of storing, securing, anonymising, pseudonymising, rectifying and erasing personal data.

The Privacy Service ABB is important for interoperability because "security and privacy are primary concerns in the provision of public services" and, as stated in e-GIF: "Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses."

Privacy Service. Privacy Service shares the functionalities of storing, securing, anonymising, pseudonymising, rectifying and erasing personal data.

Privacy Framework. Agreed governance approach focusing on confidentiality aspects on data, information and knowledge assets and organisational resources handling them.

Privacy Policy. A privacy policy is a document that explains how an organisation handles any customer, client or employee information gathered in its operations.

The Data Policy ABB is crucial for semantic interoperability because it provides a guiding framework to ensure the privacy of data and information according to e-GIF interoperability principles.

Private Hosting Facility. A Hosting Facility, meaning the equipment supporting the hosting of Interoperable Solutions and their components, usually embodied in a build-in, which is owned by or dedicated to one organisation (e.g. data centre or private cloud). The Private Hosting Facility ABB is salient for technical interoperability because it provides all the equipment, dedicated to one organisation, supporting the hosting of interoperable solutions and their components.

Private Network. A network that is used for the only purpose of realising the physical communication among GOU and cannot be accessed by the public. The Private Network ABB is salient for technical interoperability because it provides the private network where can operate interoperable solutions.

EXAMPLE: Any private network

Hosts within enterprises that use IP can be partitioned into two categories:

Category 1: hosts that do not require access to hosts in other enterprises or the Internet at large; hosts within this category may use IP addresses that are unambiguous within an enterprise but may be ambiguous between enterprises.

Category 2: hosts that need access to a limited set of outside services (e.g., E-mail, FTP, remote login) which can be handled by mediating gateways (e.g., application layer gateways). For any hosts in this category an unrestricted external access (provided via IP connectivity) may be unnecessary and even undesirable for privacy/security reasons. Just like hosts within the first category, such hosts may use IP addresses that are unambiguous within an enterprise but may be ambiguous between enterprises.

A third category is what is called a 'public network' and consist of the following:

Category 3: hosts that need network layer access outside the enterprise (provided via IP connectivity); hosts in the last category require IP addresses that are globally unambiguous.

Public Hosting Facility. The equipment supporting the hosting of Interoperable Solutions and their components, usually embodied in a building, which is owned by a third party and shared between organisations (e.g., cloud services). The Public Hosting Facility ABB is salient for technical interoperability because it provides all the equipment, shared between organizations, supporting the hosting of interoperable solutions and their components.

Public Network. A network that can be accessed by the public (public administrations, businesses, and citizens) without specific authorisations. Interoperable Solutions can rely on Public Networks (e.g., the Internet) to realise the physical communication between nodes.

The Public Network ABB is salient for technical interoperability because it provides the public network where interoperable solutions can operate.

Public Policy. Set of principles followed by the authorities of Uganda.

Public Policy Cycle. The series of public policy phases that are regularly repeated to manage all aspects of a public policy.

The Public Policy Cycle ABB is important for legal interoperability because it impacts the design and formulation of public policies, which are implemented through legal acts. Interoperability principles need to be considered during the whole public policy cycle.

Public Service Agent. An agent that consumes or delivers a public service on behalf of a principal. The Public Service Agent is crucial for organisational interoperability because it acts on behalf of a Public Service Consumer Agent to consume a Public Service and Public Service Provider Agent to deliver a Public Service.

Public Service Catalogue. A catalogue of public services is a collection of descriptions of active public services that are provided by public administrations at any administrative level (i.e., local, regional, national). All public service descriptions published in a catalogue of public services conform to a common data model for representing public services. The Public Service Catalogue ABB is a key interoperability enabler because it supports to achieve organisational structural interoperability by ensuring the provision/consumption of front-office digital public services.

Public Service Consumer. A person, institution, or machine (on behalf of somebody) consuming public services.

Public Service Provider. A person, institution, or machine (on behalf of somebody) delivering public services.

Reference Data Policy. A Data Policy applying to data used to organise or categorise other data, or for relating data to information both within and beyond the boundaries of the enterprise. Usually, it mandates the use of codes and descriptions, or definitions.

Reference data consists typically of a small, discrete set of values that are not updated as part of business transactions but are usually used to impose consistent classification. Reference data normally has a low update frequency. Reference data is relevant across more than one business systems belonging to different organisations and sectors

The Reference Data Policy ABB is a key for semantic interoperability because Reference Data can be shared and reused (e.g., in the form of taxonomies or controlled vocabularies) between organisations to agree on some basic information.

Registered Electronic Delivery Service. Shares the functionalities that: (1) makes it possible to transmit data between third parties by electronic means and (2) provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, (3) and that protects transmitted data against the risk of loss, theft, damage, or any unauthorised alterations. These functionalities SHALL cover UgHUb solution.

Representation. The description of the perceptible configuration of business information or a Legal act. Representations can be classified in various ways; for example, in terms of medium (e.g., electronic or paper documents, audio, etc.) or format (HTML, ASCII, PDF, RTF, etc.).

Security Framework. Agreed governance approach focusing on protection aspects on data, information and knowledge assets and organisational resources handling them.

Security Policy. A privacy or security policy is a statement or a legal document (in privacy law) that discloses some or all the way a party gathers, uses, discloses, and manages a customer or client's data.

The Data Policy ABB is crucial for semantic interoperability because it provides a guiding framework to ensure the security of data and information according to e-GIF interoperability principles

Semantic Agreement. An agreement from a peer to the common ontology is the result of a matching or mapping process that is used to resolve their semantic discrepancies. The combination matching process consists of linguistic base, internal and external structure comparison. Result of a matching combination will be used to develop an agreement unit as a component of agreement. There are some assumptions for the agreement, such as using the same language for representation of schema/ontology, labels represent the meaning of concept, and there is no individual at the common ontology.

Semantic Interoperability Agreement. A Semantic interoperability agreement is a semantic resource formalising governance rules enabling collaboration between digital public services with ontological value.

The Semantic Interoperability Agreement ABB is a key interoperability enabler because it supports semantic governance interoperability by enabling collaboration between digital public services.

Semantic Interoperability Requirement. A semantical interoperability requirement is an interoperability requirement that must be met to help achieve semantic interoperability.

Semantic Interoperability Specification. Semantic interoperability enables organisations to process information from external sources in a meaningful manner. It ensures that the precise meaning of exchanged information is understood and preserved throughout exchanges between parties. In the context of the GOU e-GIF, semantic interoperability encompasses the following aspects:

- Semantic interoperability is about the meaning of data elements and the relationship between them. It includes developing vocabulary to describe data exchanges and ensures that data elements are understood in the same way by communicating parties.
- Syntactic interoperability is about describing the exact format of the information to be exchanged in terms of grammar, format, and schemas.

Semantic interoperability specifications support semantic interoperability by addressing the core semantic interoperability background for solutions.

The Semantic Interoperability Specification ABB is cruicial for semantic interoperability because it enables organisations to process information from external sources in a meaningful manner and ensuring that the precise meaning of exchanged information is understood and preserved throughout exchanges between parties.

Service Delivery Model. The way of delivering to public service consumers, or otherwise interacting with them, for the purpose of supplying specific public services with accessibility value. This involves

several management practices to ensure that the public services are provided as agreed between the public service provider and the consumer.

Service Discovery Service. Shares the functionality of locating a machine-processable description of a service-related resource that may have been previously unknown and that meets certain functional criteria. It involves matching a set of functional and other criteria with a set of resource descriptions. The goal is to find an appropriate service-related resource. The Service Discovery Service ABB is salient for technical interoperability because it allows to discover service available for reuses.

Service Discovery Component. Implements the functionality of locating a machine-processable description of a service-related resource that may have been previously unknown and that meets certain functional criteria. It involves matching a set of functional and other criteria with a set of resource descriptions. The goal is to find an appropriate service-related resource. The Service Discovery Component ABB is salient for technical interoperability because it allows to implement the functionality of sharing services available for reuse.

Service Registration Service. Implements the functionality of registering the system service within a catalogue to be discovered by other services. This ABB is a key interoperability enabler for sharing/PROVISIONING and reusing/CONSUMING back-office services. The Service Registration Component ABB is a key interoperability enabler because it supports to achieve technical interoperability by provisioning and consuming back-office services as stated in the e-GIF recommendation: "Put in place catalogues of public services, public data, and interoperability solutions and use common models for describing them."

Service Registry Component. Shares the functionality of registering the system service within a catalogue to be discovered by other services. The Service Registration Service ABB is a key interoperability enabler because it supports to achieve technical structural interoperability by ensuring the provision/consumption of back-office digital public services.

Shared Governance Framework. A shared legal framework is formed by [re]usable legal resources, with convergence power, in relation to public policy goals attainment, given by their functioning impact via communication and harmonisation, across the levels of a public administration (central, regional, local) towards the achievement of the public policy goals.

Shared Knowledge Base. A shared Knowledge Base is formed by usable data, information, and knowledge resources, with convergence power, in relation to public policy goals attainment, given by their impact in the enactment of common understanding from the existing organisational information, across the levels of a MDAs towards the achievement of the public policy goals.

Shared Legal Framework. A shared legal framework is formed by [re]usable legal resources, with convergence power, in relation to public policy goals attainment, given by their legally binding nature, across the levels of MDAs towards the achievement of the public policy goals.

Shared Platform. A shared platform is formed by [re]usable ICT resources (i.e., the platform), with convergence power, in relation to public policy goals attainment, given by the impact of the availability of common problem-solving instruments, across the levels of MDAs towards the achievement of the public policy goals.

Solution. A solution consists of one or more Solution Building Blocks to meet a certain stakeholder need. Within the context of the GIRA, a solution is usually an Interoperable GOU Solution that facilitates the delivery of electronic Public Services between ADMs or Citizens.

Solution Building Block (SBB) is a candidate solution which conforms to the specification of an Architecture Building Block (ABB). Source TOGAF®: https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_70

Solution specification. An Architecture Specification is a document of the highest possible level of granularity on a Solution Building Block, formulated as an agreed normative statement.

Technical Agreement. These agreements constitute a framework and a privileged forum to identify common interests, priorities, policy dialogue, and the necessary tools for Strategic & Technological collaboration.

Technical Interoperability Agreement. Technical Interoperability Agreement is the means through which Technical Authorities mandate specific Technical Interoperability Specifications, ensuring organisations (operating under different technical frameworks, policies, and strategies) can work together.

The Technical Interoperability Agreement ABB is a key interoperability enabler because it supports technical governance interoperability by enabling collaboration between digital public services.

Technical Interoperability Requirement. A technical interoperability requirement is an interoperability requirement that must be met to help achieve technical interoperability.

Technical Interoperability Specification. A specification contained in a document which lays down the characteristics required of a product such as levels of quality, performance, safety, or dimensions, including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing and test methods, packaging, marking or labelling and conformity assessment procedures. The Technical Interoperability Specification ABB is salient for technical interoperability because it assesses the characteristics required of a product to support interoperability solutions.

Technical Specification. A document that prescribes technical requirements to be fulfilled by a product, process, or service.

- Note 1 to entry: A technical specification should indicate, whenever appropriate, the procedure(s) by means of which it may be determined whether the requirements given are fulfilled.

- Note 2 to entry: A technical specification may be a standard, a part of a standard or independent of a standard.

The Technical Specification ABB is salient for technical interoperability because it assesses the characteristics required of a product to support technical solutions.

Trust Registry Component. Implements the functionality of the discovery of essential information about e.g., supervised/accredited trust service providers issuing certificates for electronic signatures, for electronic seals or for website authentication; supervised/accredited trust services for eSignature, eSeal or TimeStamp creation and validation; supervised/accredited trust services for eSignature or eSeal preservation; supervised/accredited trust services for electronic registered delivery.

Trust Registry Service. Shares the functionality of the discovery of essential information about e.g., supervised/accredited trust service providers issuing certificates for electronic signatures, for electronic seals or for website authentication; supervised/accredited trust services for eSignature, eSeal or TimeStamp creation and validation; supervised/accredited trust services for eSignature or eSeal preservation; supervised/accredited trust services for electronic registered delivery.

Trust Service Provisioning Component. Implements the functionalities encapsulating the trust services functionalities. A **'trust service'** means an electronic service normally provided for remuneration which consists of these functionalities:

i) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

ii) the creation, verification and validation of certificates for website authentication; or

iii) the preservation of electronic signatures, seals or certificates related to those services.

12. Abbreviations

Abbreviation	Meaning
ABB	Architecture Building Block
ADM	The Architecture Development Method
AI	The Artificial Intelligence
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
Archi	The modelling toolkit for creating ArchiMate models and sketches,
ArchiMate	The Enterprise Architecture Modelling Language
ASVS	Application Security Verification Standard
ATTA	Access to Information Act
BaaS	Backup as a Service
BPMN	Business Process Model and Notation
CatIS	Catalogue of interoperable solutions: eGA tools for achieving interoperability governance
CFR	Cross-Functional Requirements
CI/CD	Continuous Integration / Continuous Delivery
CIO	Chief Information Officer
CVI	Corporate Visual Identity
DAML+OIL	Semantic markup language for Web resources
DPPA	Data Protection and Privacy Act
DSI	Digital Service Infrastructure
DSSC	Data Spaces Support Centre
DUV	The Digital Uganda Vision
eBiz	Electronic One Stop Centre Web Portal
ECCMIS	Electronic Court Case Management Information System
EDWG	Eclipse Dataspace Working Group
eGA	e-Governance Academy
e-GIF	e-Government Interoperability Framework
eID	electronic IDentification
EIRA	The European Interoperability Reference Architecture
ELAP	European Library of Architecture Principles
ePIS	Electronic Policing Information System
FTP	File Transfer Protocol
GDR	Government Digital Registry
GEA	e-Government Enterprise Architecture
GIRA	The e-Government Interoperability Framework Reference Architecture
GOU	Government of Uganda
HITL	Human-in-the-Loop
HTML	Hyper Text Markup Language
IaaS	Infrastructure as a Service
ICT	Information and communication technology
IDSA	International Data Spaces Association
IMSC	Inter-Ministerial Steering Committee
IOT	Internet of Things
IPT	IP Transit

JLOS	Justice, Law and Order
LD	Linked Data
MDA/LG	Ministries Departments, Agencies and Local Governments
MoICT&NG	Ministry of Information and Communications Technology and National Guidance
MoReq	Modular Requirements for Record Systems National Backbone Infrastructure
My-UG	FREE Wi-Fi and a centralized digital service platform developed and managed by the NITA-U
NBI	National Backbone Infrastructure
NGO	Non-Governmental Organisation
NIIS	Nordic Institute for Interoperability Solutions
NITA-U	The National Information Technology Authority – Uganda
NIRA	National Identification & Registration Authority
NLIS	National Land Information System
OCI	Open Container Initiative
OECD	The Organisation for Economic Co-operation and Development
OWASP	Open Worldwide Application Security Project
OWL	W3C Web Ontology Language
PaaS	Platform as a Service
PCC	Policy Coordination Committee
PCS	Point of single contact
PDPO	Personal Data Protection Office
PMIS	Prisons Management Information System
PKI	Public Key Infrastructure
PSC	Point of Single Contact
RDF	Resource Description Framework
SA	Security Architecture
SaaS	Software as a Service
SABSA	Sherwood Applied Business Security Architecture
SBB	Solution Building Block
SbD	Security by Design
SDE	Secure Data Exchange
SDG	Sustainable Development Goals
SIMPO	The Security Interest in Movable Property Registry
SMS	Short Message Service
SSO	Single Sign-On
SOA	Service Oriented Architecture
SPOF	Single Points of Failure
TOGAF	The Open Group Architecture Framework
UBOS	Uganda Bureau of Statistics
UCC	Uganda Communications Commission
UgPass	Electronic Signatures Solutions
ULC	Uganda Land Commission
UMCS	Unified Messaging and Collaboration System
UML	Unified Modelling Language
UN	The United Nations

UNDEI	Uganda Data Exchange Infrastructure
UNDP	United Nations Development Programme
URSB	Uganda Registration Services Bureau
W3C	World Wide Web Consortium
WASA	Web Application Security Architecture Framework
WCAG	Web Content Accessibility Guidelines
WoG	Whole of Government
WSO2	Web Services (WS) Oxygen (O2). Company and software platform name