



Uganda e-Government Interoperability Framework (e-GIF)

e-GIF-2026

April 15, 2026

Table of Contents

1. Executive Summary	7
2. Introduction	8
2.1. The need for a Renewed e-GIF	8
2.2. Approach	10
2.3. The e-GIF Purpose.....	11
2.4. Scope and Structure of the e-GIF	12
3. Context of e-GIF.....	15
3.1. TOGAF based approach	15
3.2. Data Space Model.....	15
3.2.1. Shift from Centralized to Federated Architecture	16
3.2.2. Strengthened Trust and Security.....	16
3.2.3. Interoperability by Design	16
3.2.4. Strategic and Global Alignment.....	17
3.3. AI for interoperability and interoperability for AI	17
3.3.1. Principles for AI Implementations	17
3.3.2. Ethical Framework: Ethics-by-Design and Transparency.....	18
3.3.3. Governance Model: Policy as Code.....	18
3.3.4. Risk Management and Resilience	18
3.4. Catalogues based interoperability governance	19
3.5. Definitions.....	20
3.5.1. Interoperability	20
3.5.2. Data Space	20
3.5.3. Public Service.....	21
3.5.4. Dataset	21

3.5.5.	Information System	21
3.5.6.	Registry	21
3.5.7.	API	21
3.5.8.	Enabler	21
3.5.9.	Shared services	22
3.5.10.	Data Space Model	22
3.5.11.	GoU Interoperability Framework	22
3.6.	Stakeholders of digital Uganda ecosystem	22
3.6.1.	Principal stakeholders	22
3.6.2.	Stakeholder roles	23
4.	Underlying Principles	26
4.1.	Principle 1: Subsidiarity and Proportionality	27
4.2.	Principle 2: Openness	28
4.3.	Principle 3: Transparency	29
4.4.	Principle 4: Reusability	29
4.5.	Principle 5: Technological Neutrality and Data Portability	30
4.6.	Principle 6: User-Centricity	30
4.7.	Principle 7: Inclusion and Accessibility	31
4.8.	Principle 8: Security and Privacy	32
4.9.	Multilingualism	33
4.10.	Principle 10: Administrative Simplification	33
4.11.	Principle 11: Preservation of Information	34
4.12.	Principle 12: Assessment of Effectiveness and Efficiency	34
5.	Interoperability Layers	35
5.1.	Interoperability Governance	36

5.1.1.	Barriers of Interoperability Governance	36
5.1.2.	Governance on the Interagency Level	36
5.1.3.	Financing.....	39
5.1.4.	Monitoring, Conformance, and Enforcement	40
5.1.5.	Standards and specifications	40
5.2.	Integrated Public Service Governance.....	41
5.2.1.	Governance on the Administration Level.....	42
5.2.2.	Interoperability Agreements	42
5.3.	Legal Interoperability	43
5.3.1.	Interoperability and Digital Checks.....	43
5.3.2.	Data-Centric Legal Definitions.....	43
5.3.3.	Legal Framework for AI and Automated Decisions.....	44
5.3.4.	Recommended Framework Legislation.....	44
5.3.5.	Compliance with Key National Acts.....	44
5.4.	Organisational Interoperability	45
5.4.1.	Business Process Alignment and Optimization	45
5.4.2.	Multi-Level Governance and Relationships	45
5.4.3.	Service Lifecycle and Change Management.....	45
5.4.4.	Capacity Building and Communities of Practice.....	46
5.4.5.	AI-Enhanced Coordination.....	46
5.5.	Semantic Interoperability.....	46
5.5.1.	Data as a Strategic Public Asset.....	46
5.5.2.	Metadata Standards and Findability.....	47
5.5.3.	Base Registries as the Semantic "Source of Truth"	47
5.5.4.	Base registries	48

5.5.5.	AI-Driven Semantic Alignment.....	49
5.5.6.	Semantic Readiness for Data Spaces.....	49
5.6.	Technical Interoperability	50
5.6.1.	Service-oriented architecture.....	51
5.6.2.	API-First and Event-Driven Architecture.....	51
5.6.3.	Federated Data Space and Decentralization	51
5.6.4.	Cloud-Native and Zero-Trust Security	52
5.6.5.	Technical Conformance and Observability.....	52
5.6.6.	Legacy System Transition.....	52
6.	The Conceptual Model for Integrated Public Services Provision	53
6.1.	Introduction	53
6.2.	Model overview.....	54
6.3.	Shared Enablers and Reusable Building Blocks.....	55
6.4.	Internal information sources and services	55
6.5.	Base registries	56
6.6.	Open data.....	56
6.7.	Interoperability Governance Catalogues	57
6.8.	External information sources and services.....	57
6.9.	Security and privacy.....	58
7.	Governance of Interoperability Framework	60
7.1.	Institutional Roles.....	60
7.2.	Assessment and Approval Procedures	60
7.3.	Monitoring and the Observatory	60
7.4.	Incremental Architecture Methodology.....	60
7.5.	Role of sectors and administrations	61

8. Abbreviations	62
9. Glossary	64

1.Executive Summary

The Ugandan e-Government Interoperability Framework (e-GIF) 2026 is one of the strategies for achieving the goals of f Uganda Vision 2040. It serves as the operational engine of the Government Enterprise Architecture (GEA), facilitating a "Whole-of-Government" (WoG) integrated environment. The objective is to ensure that data and services flow seamlessly between entities to improve service delivery and ensure that government acts as a single, coherent platform for its citizens.

Expected results of e-GIF are reduction of duplication of IT systems and data sets, faster service delivery, Improved government efficiency, better quality and security of data etc.

e-GIF-2026 is a mandatory framework for all public sector institutions in Uganda. It applies to all Ministries, Departments, and Agencies (MDAs) and Local Governments (LGs). All digital initiatives, procurement, and system developments within these entities MUST conform to the principles and recommendations contained herein.

This 2026 revision is necessitated by the rapid evolution of the technological landscape and the requirement to transition from a system-centric to a data-centric model. Emerging technologies — specifically Data Space, Artificial Intelligence (AI), and Cloud-native architectures — are now core components of the digital government ecosystem. E-GIF-2026 ensures that Ugandan e-government remains flexible, prevents vendor lock-in, and maintains resilience against global geopolitical and cybersecurity shifts.

2.Introduction

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

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

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

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

The GoU Interoperability Framework gives guidance, through a set of recommendations, to MDA/LGs on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting digital services, and ensure that existing and new legislation do not compromise interoperability efforts.

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

The process of updating the e-GIF was led by lessons learned and new policy priorities, ensuring it stays relevant and actionable in today's digital landscape:

- **Build on the e-GIF-2021:** The update process built on the current e-GIF and consider feedback collected through the evaluation of the e-GIF, the observatory of the implementation of the e-GIF, as well as additional stakeholder feedback.
- **Respond to change:** It addresses technological advances (e.g. on data spaces, AI, IoT interoperability), political shifts and evolving strategic priorities such as digital sovereignty.

2.1. The need for a Renewed e-GIF

The e-GIF arises from the need to provide a common legal, organisational, semantic and technical foundation for the seamless exchange of data and services across public administrations in Uganda and African countries. In an environment where governments,

businesses and citizens increasingly rely on cross-border digital interaction, the absence of shared standards and specifications, reference architectures and coordination mechanisms can lead to fragmentation, inefficiency and duplication of effort.

According to the assessment in the Terms of reference Ugandan e-GIF-2021 have significantly improved government efficiency and service delivery. Some notable successes include:¹

- Standardization and Integration,
- Enhanced Service Delivery,
- Improved Decision Making,
- Increased Transparency and Accountability,
- Cybersecurity Enhancement.

Despite these successes, the evolving technological landscape and changing government priorities necessitate a renewal of the e-GIF:

The Rationale for Renewal Uganda is transitioning from fragmented "ICT islands" toward a unified digital ecosystem. The e-GIF-2026 renewal is caused by the rapid emergence of Artificial Intelligence (AI), blockchain, and cloud-native patterns, as well as the need for deeper integration across nine critical sectors Agriculture, Industry, Services, Health, Education, Transport and communication, Finance and insurance, Tourism, Information and communication technology (ICT).

Architectural Shift: Data Spaces and AI. The renewed e-GIF adopts a **Federated Data Space Model**, moving away from centralized traffic controllers to distributed Sovereign Connectors. This ensures that data remains at its source while being securely exchangeable. Furthermore, the framework introduces the principle of "AI for Interoperability," utilizing machine learning and LLMs to automate semantic alignment and legal drafting.

Catalogues based governance. For interoperability governance the interconnected system of catalogues SHOULD be used. Compliance to e-GIF SHOULD be no longer voluntary and e-GIF-2026 and GEA SHALL be enforced through Catalogues.

This e-GIF revision therefore responds both to an institutional demand - ensuring that Ugandan policies are implemented coherently across sectors and institutions - and to an operational need, providing the framework, shared vocabulary and governance model that enables truly interoperable public services throughout the Ugandan administrations and sectors and ensure cross border data exchange.

¹ Terms of reference for renewal of the Ugandan e-GIF and GEA 2025

2.2. Approach

e-GIF takes account of experiences, guidelines, and initiatives United Nations², OECD³, EU⁴, World Bank⁵, UN led GovStack initiative⁶, EU member states, other countries in word, especially in Africa. The e-GIF uses the terminology and structure of TOGAF⁷ and the European Interoperability Framework (EIF)⁸ the content is adjusted to the GoU national policies, strategies, and guidelines. The European Commission is developing a new version of the EIF to reflect new digital technologies, new policy priorities, and lessons from implementation across Member States.⁹ The new version aims to “address practical needs arising in the implementation and delivery of interoperable digital public services” are reflected also in this framework.

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

- cooperation between MDA/LGs aiming at the establishment of digital public services,
- information exchange between MDA/LGs to fulfil legal requirements or political commitments,
- sharing and re-using data and information among MDA/LGs to increase administrative efficiency and reduce administrative burden on citizens and businesses.

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

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

² <https://publicadministration.un.org/egovkb/en-us/>

³ <https://read.oecd.org/10.1787/f64fed2a-en?format=pdf>

⁴ <https://interoperable-europe.ec.europa.eu/interoperable-europe/nifo>

⁵ <https://www.govstack.global/about/> [w.worldbank.org/en/programs/govtech](https://www.worldbank.org/en/programs/govtech)

⁶ <https://govstack.global/about/>

⁷ <https://www.opengroup.org/togaf>

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

⁹ <https://living-in.eu/news/shape-new-generation-european-interoperability-framework>

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

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

Cross-border services is quite a new challenge for GOU. There are initiated several sectorial cross-border based projects such as EAC projects and AfCFTA projects respectively. MDAs SHOULD consider the needs cross-border services.

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

2.3. The e-GIF Purpose

The e-GIF is oriented to:

- **improving** public service delivery to citizens and businesses by facilitating the one-stop shop delivery of public services.
- **reducing costs** for MDA/LGs, businesses, and citizens through efficient and effective delivery of public services.

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

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

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

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

1. to facilitate the transformation of institution-based MDA/LG into a service-centred one, where all citizens can communicate with the state without needing to know its hierarchical structure and division of roles of government institutions.
2. to reduce public sector IT expenses through a wide use of common rules and solutions.
3. to improve the interoperability of new IT projects through coordinated use of centrally developed common infrastructure services and open standards.

4. to improve the coordination and management of Government information systems of Uganda and to accelerate the development of IT solutions.
5. to contribute to the co-development of the state information systems.
6. to allow autonomous development for all systems within the principles of organisational, semantic, and technical interoperability.
7. to endorse free competition among various vendors while procuring.

The report contains:

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

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

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

2.4. Scope and Structure of the e-GIF

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

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

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

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

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

The e-GIF content and structure is presented below:

- Chapter 3 present the context of e-GIF-2026 and presents the new paradigms of e-GIF-2026: Data Space Model, AI, and Catalogues based interoperability governance. Chapter gives 4 recommendations.
- Chapter 4 presents a set of 12 **principles** intended to set up general behaviours on interoperability. The Chapter gives 32 requirements/recommendations for MDA/LGs.
- Chapter 5 presents a layered **interoperability model**, which organises in layers the different interoperability aspects to be addressed when designing public services. The Chapter gives 23 requirements/recommendations for MDA/LGs.
- Chapter 6 outlines a **conceptual model** for interoperable public services. The model is aligned with the interoperability principles and promotes the idea of 'interoperability by design' as a standard approach for the design and operation of public services. The Chapter gives 21 requirements/recommendations for MDA/LGs.
- Chapter 7 stipulates the rules of **e-GIF governance**. The e-GIF handles information systems from the point of view of the state as a whole. The maintenance of the e-GIF document will be handled through the Inter-Agency Digital Technical Implementation Committee and the e-Government working groups with the leadership of the Secretariat at the Ministry of ICT and National Guidance. Chapter gives 4 requirements/recommendations for e-GIF governance.
- Chapter 8: Abbreviations
- Chapter 9: Glossary

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

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

The key words of this document "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" should be interpreted as specified by the Internet Engineering Task Force (IETF)¹⁰. To highlight the relevance of these words, they have been provided in block capitals, and their meaning is as follows:

Meaning	Words expressing the meaning
Required/obligatory. Absolute requirement	<i>MUST, REQUIRED, SHALL</i>

¹⁰ Internet Engineering Task Force (IETF) RFC 2119: „Key words for use in RFCs to indicate requirements levels “: <https://tools.ietf.org/html/rfc2119>

Recommendation. There may exist valid reasons circumstances to ignore an item, but the full implications must be understood and carefully weighed before choosing a different course.	<i>SHOULD, RECOMMENDED</i>
Acceptable/allowed.	<i>MAY, OPTIONAL</i>
Not recommended. Acceptable only under reasons or circumstances.	<i>SHOULD NOT, NOT RECOMMENDED</i>
Prohibited. Absolute prohibition.	<i>MUST NOT, SHALL NOT</i>

3.Context of e-GIF

The TOGAF framework¹¹ (The Open Group Architecture Framework) and EIF are used as a basis of e-GIF-2026. The new added paradigms in e-GIF-2026 are Data Space Model, AI and Catalogues based interoperability governance.

3.1. TOGAF based approach

The TOGAF® Standard (The Open Group Architecture Framework) is a widely used, comprehensive framework for designing, planning, implementing, and governing enterprise information technology architecture. It provides a structured, iterative approach—centered on the Architecture Development Method (ADM)—to align business goals with IT strategy.

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

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

3.2. Data Space Model

A **data space** is a distributed, interoperable data-sharing environment where multiple participants retain control over their own data while using common standards, trust frameworks, and governance rules to exchange data securely and fairly. It enables sovereign, federated data sharing across organizations, sectors, or countries without centralizing the data. The Data Space model will be described in GIRA. The changes in infrastructure needed.

¹¹ <https://www.opengroup.org/togaf>

Some infrastructure components need to be supplemented, replaced, or moved to other functionalities.

3.1. The Data Space Model is the key architectural decision and conceptual shifts Uganda SHOULD be set up for the Uganda e-GIF 2026 integration layer.

3.2.1. Shift from Centralized to Federated Architecture

Transition: Moving away from the "Hub-and-Spoke" model (UG-Hub as a central traffic controller) to a Federated Data Space.

Decentralization: Data remains at the source with the custodial MDA. Integration is achieved through distributed Sovereign Connectors rather than a single central message bus.

Resilience: Elimination of the "Single Point of Failure" by enabling peer-to-peer data exchange between MDAs.

3.2.2. 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)¹² to dictate how, when, and by whom their data is used.

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

3.2.3. 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 DCAT¹³ 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.

¹² ODRL Information Model 2.2: <https://www.w3.org/TR/odrl-model/>

¹³ Data Catalog Vocabulary: <https://www.w3.org/TR/vocab-dcat-3/>

3.2.4. Strategic and Global Alignment

Once-Only Principle: The architecture is the primary engine for the Parish Development Model (PDM), 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.

3.3. AI for interoperability and interoperability for AI

The rapid integration of Artificial Intelligence into public administration creates both an opportunity and a necessity for rethinking interoperability and the methods for reaching it. On one side, AI can vastly improve the capacity of systems to exchange, interpret, and reuse information across legal, organisational, semantic, or technical boundaries. On the other hand, the growing diversity of AI tools, data, and governance models, risks producing new silos and incompatibilities between public sector organisations and member states. Therefore, Uganda SHOULD ensure that AI becomes a driver for interoperability rather than a new barrier.

AI-driven conversational services. GoU should consider the replacing menu-based portals with conversational interfaces.

3.2. AI SHOULD become a driver of interoperability

3.3. AI-driven conversational services: GoU SHOULD consider the replacing menu-based portals with conversational interfaces.

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.

3.3.1. Principles for AI Implementations

Recommended principles for AI implementations:¹⁴

- **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.

¹⁴ <https://specs.govstack.global/ai-readiness/principles-for-ai-implementations>

- **The Principle of Radical Observability.** If it cannot be traced, it cannot be automated.
- **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.

3.3.2. 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.

3.3.3. 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.

3.3.4. 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.

3.4. Catalogues based interoperability governance

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 1.

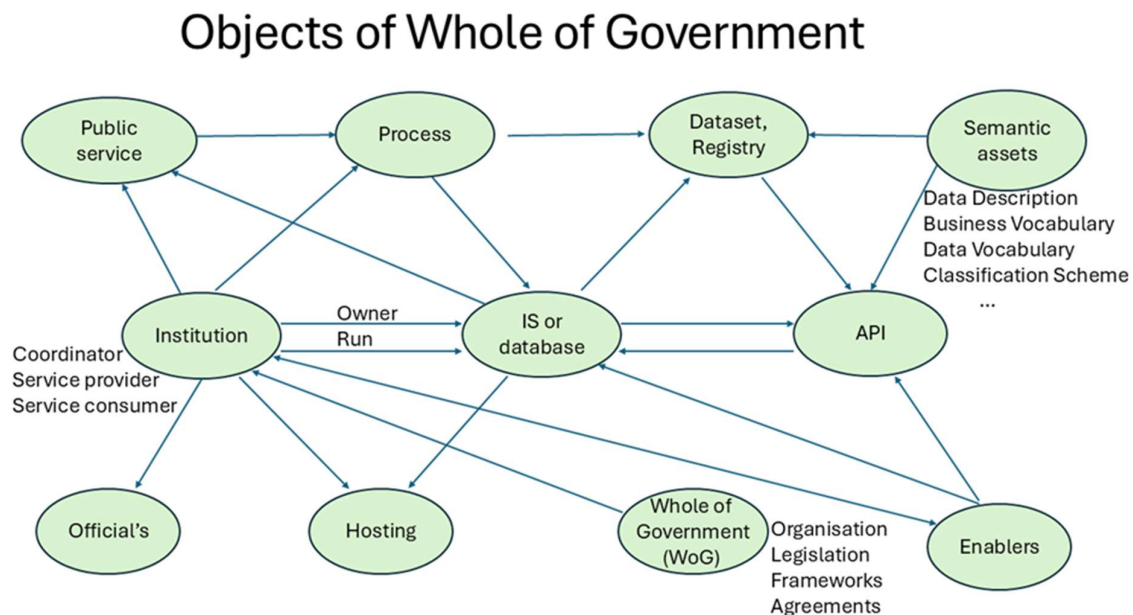


Figure 1 WoG objects.

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.

3.4. Uganda SHOULD establish Catalogue System (registry) as mandatory instrument for Interoperability Governance

3.5. Definitions

3.5.1. Interoperability

Interoperability is the ability of making systems and organisations operate together (inter-operate). In the following document the term "interoperability" is used in a broad way. It considers not only technical but also social, political, and organisational factors. We are following the definition of the European Commission¹⁵, which has been accepted in governmental context internationally:

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

3.5.2. Data Space

Data Space is a secure, decentralized ecosystem that allows different government agencies, public institutions, and trusted private partners to share and access data without losing sovereignty over it. Data Space relies on four specific elements:

- **Data Sovereignty:** The administration that collects the data decides exactly who can see it and for how long. They don't "give it up"; they "grant access."
- **Interoperability:** It forces different administrations to speak the same digital language.
- **Trust Framework:** A common set of legal, technical, and ethical rules. If Agency A shares data with Agency B, they both operate under the same privacy and security standards.
- **Decentralization:** Data stays at the source. When a service needs information, it "calls" for it in real-time rather than storing a stale copy in a central silo.

¹⁵ https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

3.5.3. Public Service

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

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

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

3.5.4. Dataset

Dataset: an identifiable collection of data, controlled or managed by a government authority, representing a specific administrative, legal, or functional domain. Architecturally, the dataset is the primary object of governance; the law applies to its content and legal basis regardless of the storage medium.

3.5.5. Information System

Information System: A set of technical components, including software, hardware, and network infrastructure, organized to perform specific functions of collecting, processing, storing, and distributing information designed to collect, process, store, and distribute information. In a WoG context, the system acts as the host for one or more Data Services.

3.5.6. Registry

Registry (including Base Registry): A trusted and authoritative dataset managed by a government authority that serves as the primary legal "source of truth" for a specific administrative domain, such as persons, land, businesses, or vehicles. Each Registry SHALL be managed within a designated Information System and MUST be described in the Catalogues System. List of most prominent registries are described in section 5.5.4.

3.5.7. API

An **application programming interface (API) (or data service)** is a connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software. It is recommended to set up official API catalogue in Uganda. It can be one component of a Governmental Digital Registry (GDR).

3.5.8. Enabler

Enablers support interoperability by offering services, data structures, standards, or guidelines that can be reused across many solutions. They enable the functioning of digital public services.

3.5.9. Shared services

Shared services are Services provided centrally by one or several public administrations that can be reused by others to support the delivery of digital public services. They typically cover common functions needed by many government services.

3.5.10. Data Space Model

A **data space** is a distributed, interoperable data-sharing environment where multiple participants retain control over their own data while using common standards, trust frameworks, and governance rules to exchange data securely and fairly. It enables sovereign, federated data sharing across organizations, sectors, or countries without centralizing the data.

3.5.11. GoU Interoperability Framework

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

3.6. Stakeholders of digital Uganda ecosystem

3.6.1. Principal stakeholders

The principal stakeholders of the e-GIF can be grouped into three broad categories as the main beneficiaries of Ugandan interoperable public services: A (administrations), B (businesses) and C (citizens). This framing is also consistent with international practice, as reflected in the work of the EU, the OECD, the World Bank, and the United Nations on digital public infrastructure, public services, and interoperability.¹⁶ These organisations highlight how interoperable systems strengthen administrative efficiency and enhance accessibility and service quality for citizens and businesses. The three categories can be described as follows:

A - Administrations include all public sector bodies, governments on national, sectoral, regional and local levels, public organisations, and public sector-owned service organisations.

B - Businesses include privately controlled companies (large, small and medium sized, or very small) with activities on international, African, national and/or local level, and their supporting associations.

¹⁶ OECD (2024). Digital Public Infrastructure for Digital Governments; World Bank.2022. Interoperability: Towards a Data-Driven Public Sector; UN, Universal DPI Safeguards Framework; The UN DPI framework refers to individuals, civic and public authorities, and private entities; The EU EIF and EIRA initiatives.

C - Citizens are physical persons residing in Uganda, their supporting associations, NGOs and the civic society in general. The term also includes all individuals in general with fundamental rights.

3.6.2. Stakeholder roles

The effective implementation of the e-GIF relies not only on identifying who the stakeholder groups are, but also on understanding the **distinct roles** each actor may play within the interoperability ecosystem. Each role contributes to shaping, operating, or sustaining interoperable digital public services.¹⁷

Clarifying these roles helps define responsibilities, **dependencies, and collaboration pathways** across governance levels. It also ensures that interoperability is addressed consistently throughout the policy, design, and delivery of digital public services.

By mapping these roles, the e-GIF provides an operational perspective on where coordination, capacity building, and common specifications are most needed to achieve a connected and effective Ugandan digital administration.

3.6.2.1. Public Service Consumers.

Every citizen, business and even administrations are consumers of digital public services. Service consumers are the direct and most important beneficiaries of a higher degree of interoperability. From an inner-market perspective, users that are consuming services across borders are of special interest. Service consumers receive help from interoperable services, by reduced perceived complexity, effective use of devices and data across services, and indirectly through lower cost of providing public services.

3.6.2.2. Legislators

Legislators create binding legal requirements through parliamentary or equivalent processes. They define laws that shape the operation of public services, whether targeting specific services, sectors, digital technology use, or the general functioning of public administrations, based on societal needs. Their role is primarily normative and formal, providing the rules governing public services.

3.6.2.3. Policymakers

Policymakers set strategic directions and priorities that guide how organisations operate within the legal framework. They operationalise rules and drive the development and improvement of public services, coordinating initiatives both within individual organisations and across the broader system. Policymakers also identify gaps or emerging needs that can inform the evolution of legislation over time. Unlike legislators, they do not create binding laws but contribute to how rules are applied, interpreted, and adapted. Citizens, including civil society,

¹⁷ This section is inspired from discussions and draft materials of EU member states about New Generation of EIF

influence policy through advocacy or political engagement, helping to inform and steer these strategic decisions.

3.6.2.4. Service Designers

Public and private services are the results of deliberate design processes. Often with a strong focus on ease of use, efficiency and overall value proposition for both providers, consumers and society in general. Designers form different communities of practices across administrations, business and citizens, provide formal education and set up research disciplines. A service design results in requirements for its various users, and most follow a growing number of horizontal regulations both within a sector and across them. Service designers benefit from interoperability through reuse of existing solutions for common problems (patterns).

3.6.2.5. Public Service Providers

Administrations on every level provide some form of public service. With the growing degree of digitalisation of society in general, most, if not all, services will involve some kind of direct or indirect digital interaction. Providers of public services rely on private services to operate, and private services often rely on some public services or are required by law to interact directly with public services. Service providers benefit from interoperability when building service with a high degree of reuse of existing services, data and products and cheaper private digital products through market mechanisms.

3.6.2.6. Data Providers

Digital public services consume data which is processed (especially registered, stored and exchanged) in a variety of contexts within these services. Administrations maintain base registries, statistics, records of individual decisions and historical data – business records of product properties, transactions from providing services and other customer interactions – citizens record of their transactions with services and private records of everyday life events.

3.6.2.7. ICT Providers

Digital Public services are implemented using technology provided by an ecosystem of products and services from the private sector. Service consumers access digital public services through products and custom-built ICT systems. Administrations procure products and services implementing technical specifications and harmonised standards. ICT providers work together to establish and maintain technical interoperability between products.

3.6.2.8. Mapping of e-GIF stakeholder roles

Stakeholder role	Contribution	Benefits
Public Service Consumers (ABC)	• Feedback on existing services. • Demand for new and better services.	• Access (easier) to cross-border services. • Better user experience.

	• Influence through civic organisations.	• Stronger security, privacy and trustfulness. • More control over data (re)-use • Indirect savings through efficiency.
Public Service Providers (A)	• Authority of data Regulatory enforcement. • Investments in ICT solutions and digital infrastructure. • Investments in standardisation.	• Reuse of existing data and solutions. • Lower ICT cost through market mechanisms. • Efficient service delivery. • Support for ICT procurement
Service Designers (ABC)	• Expertise in user experience. • Design methodologies. • Service innovation	• Access to interoperability solutions. • Efficient assessments through alignment. • Faster design cycles and improved service quality
Legislators (A)	• Translating strategy and policy into law. • Consistency of legislation. • High-level legal frameworks	• Improved regulatory coherence. • Feedback from implementation of law.
Data Providers (ABC)	• Support of data communities. • Technical support for data reuse.	• Broader use and recognition of their datasets. • Value generated from data reuse and linkage. • Overview of existing solutions for reuse.
Policymakers (AB)	• Strategic direction. • Reporting on uptake. • Collaboration agreements.	• Access to interoperability solutions. • Policies and measures that promote sustainable digital transformation of the public sector
ICT Providers (B)	• Existing and new solutions. • Existing technical interoperability. • Competition on quality and cost.	• Market alignment of industry and public-sector. • Common requirements from customers

4. Underlying Principles

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

e-GIF-2026 retains the structure of e-GIF-2021, which is built on 12 core interoperability principles. These principles remain the backbone of the framework. However, because the 2026 revision aims to “integrate new developments in digital technology” and “address practical needs in the implementation of interoperable digital public services”, several principles are expected to be updated, expanded, or strengthened. Updates reflect:

- New digital technologies (AI, cloud/edge, data spaces)
- Practical implementation aspects
- Cross-border service needs
- Stronger governance and monitoring

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

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

The e-GIF is based on the following principles:

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

4.1. Principle 1: Subsidiarity and Proportionality

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

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

4.1. Data sovereignty: MDA/LGs SHOULD have ability to make decisions and act independently in the own digital domain.

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

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

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

Centralised. GoU has decided to centralise:

- Coordination activities (ICT policy and legislation, standardisation, interoperability framework, security framework, reference architecture).
- eID and PKI ecosystem.
- Orchestration of Services. UGHub is used for orchestration of services, and it also partially performs functions of secure data exchange: data between institutions are exchanged through a central solution UGHub.
- Catalogues of interoperability governance (institutions, datasets, systems, public services, APIs, assets).
- Citizen portal.
- Secure and centralised government authentication gateway for services requiring user authentication and authorisation.
- Centralised payment system.
- Open data portal.

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

- Document management systems.
- Public Financial Management & Accounting.

- Human resources systems.
- Systems for implementation functions of municipalities.
- E-mail and notification services.
- Collaboration services.

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

4.2. Principle 2: Openness

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

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

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

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

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

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

- ❖ all stakeholders could contribute to the development of the specification, and a public review is part of the decision-making process.
- ❖ the specification is available for everyone to study.

- ❖ intellectual property rights to the specification are licensed on FRAND¹⁸ terms, in a way that allows implementation in both proprietary and open-source software,¹⁹ and preferably on a royalty-free basis.

The positive effect of open specifications is proved by the internet ecosystem. However, MDA/LGs MAY decide to use fewer open specifications if open ones do not exist or do not meet functional needs. In all cases, specifications MUST be mature and sufficiently supported by the market, unless they are being used to create innovative solutions. From implementation viewpoint is increasing need to the API standards, AI model transparency, and data space participation.

4.6. The MDA/LGs MUST give preference to open specifications, API standards, AI model transparency, and data space participation taking due account of the coverage of functional needs, maturity and market support and innovation.

4.3. Principle 3: Transparency

Transparency in the e-GIF context refers to:

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

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

4.4. Principle 4: Reusability

Reuse means that MDA/LGs confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevance to the problem at hand, and where appropriate, adopting solutions that have proven their value elsewhere.

¹⁸ FRAND: fair, reasonable, and non-discriminatory.

¹⁹ This fosters competition since providers working under various business models may compete to deliver products, technologies and services based on such specifications.

This requires the MDA/LG to be open to sharing its interoperability solutions, concepts, frameworks, specifications, tools, and components with others.

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

4.8. MDA/LGs SHOULD reuse and share solutions and cooperate in the development of joint solutions including AI building blocks, event-driven services, and cross-sectorial and cross-border API components.

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

4.5. Principle 5: Technological Neutrality and Data Portability

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

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

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

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

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

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

4.14. Service components SHOULD be remained portable across jurisdictions, platforms, cloud/edge solutions, AI systems.

4.6. Principle 6: User-Centricity

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

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

- A **multi-channel** service delivery approach, meaning the availability of alternative channels, physical and digital, to access a service, is an important part of public service design, as users may prefer different channels depending on the circumstances and their needs.
- ❖ A **single point** of contact with AI assistance and multilingual support SHOULD be made available to users, to hide internal administrative complexity and facilitate access to public services, e.g. when multiple bodies must work together to provide a public service.
- ❖ **Users' feedback** SHOULD be systematically collected, assessed and used to design new public services and to further improve existing ones. Feedback tools should be easy to identify and utilise. User feedback should be regarded as a priority for continuous service quality improvement.
- ❖ As far as possible, under the legislation in force, users should be able to provide data **once only**, and MDA/LGs SHOULD be able to retrieve and share this data to serve the user, in accordance with data protection rules.
 - Users SHOULD be asked to provide only the **information that is necessary** to obtain a given public service.

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

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

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

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

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

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

4.7. Principle 7: Inclusion and Accessibility

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

- AI model fairness.
- Accessible machine generated summaries.
- Cross language support in automated processing.

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

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

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

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

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

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

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

4.8. Principle 8: Security and Privacy

Citizens, administrations 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.²⁰ MDA/LGs must guarantee the citizens' privacy, and the confidentiality, authenticity, integrity and non-repudiation of information provided by citizens and businesses.

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

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

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

²⁰ The Data Protection and Privacy Act

4.25. GoU information systems MUST guarantee confidentiality, integrity, authenticity, availability and provability of data and services. MDA/LGs MUST implement zero-trust and security-by-design architecture approach.

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

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

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

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

4.9. 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. Whenever possible, information SHOULD be transferred in a language independent format, agreed between all parties involved.

4.28. Interfaces of services SHOULD be provided in English and in any other languages relevant for the users, including Ugandan local languages.

4.29. The multilingual AI tools and multilingual data-exchange layers SHOULD be considered in service interfaces.

4.10. Principle 10: Administrative Simplification

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

Simplification SHOULD be supported by:

- Automation where appropriate
- Once-only processes
- Standardized API-based data flows

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

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

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

4.11. Principle 11: Preservation of Information

Legislation should require that decisions and data are stored and can be accessed for a specified time²¹. This means that records and information in electronic form held by MDA/LGs for the purpose of documenting procedures and decisions must be preserved and be converted, where necessary, to new media when old media become obsolete. The goal is to ensure that records and other forms of information keep their legibility, reliability and integrity and can be accessed as long as needed, subject to legal, security and privacy provisions.

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

4.31. Digital continuity SHOULD be considered also in cloud/edge pipelines and for AI reproducibility^{3.28}. Uganda MUST formulate a long-term preservation policy for information in electronic form.

4.12. Principle 12: Assessment of Effectiveness and Efficiency

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

- return on investment,
- total cost of ownership,
- level of flexibility and adaptability,
- reduced administrative burden,
- efficiency,
- reduced risk,
- transparency,

²¹ National Records and Archives Act, 2001. <http://library.health.go.ug/publications/local-government/national-records-and-archives-act2001>

- simplification,
- improved working methods,
- and level of user satisfaction.

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

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

5. Interoperability Layers

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

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

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

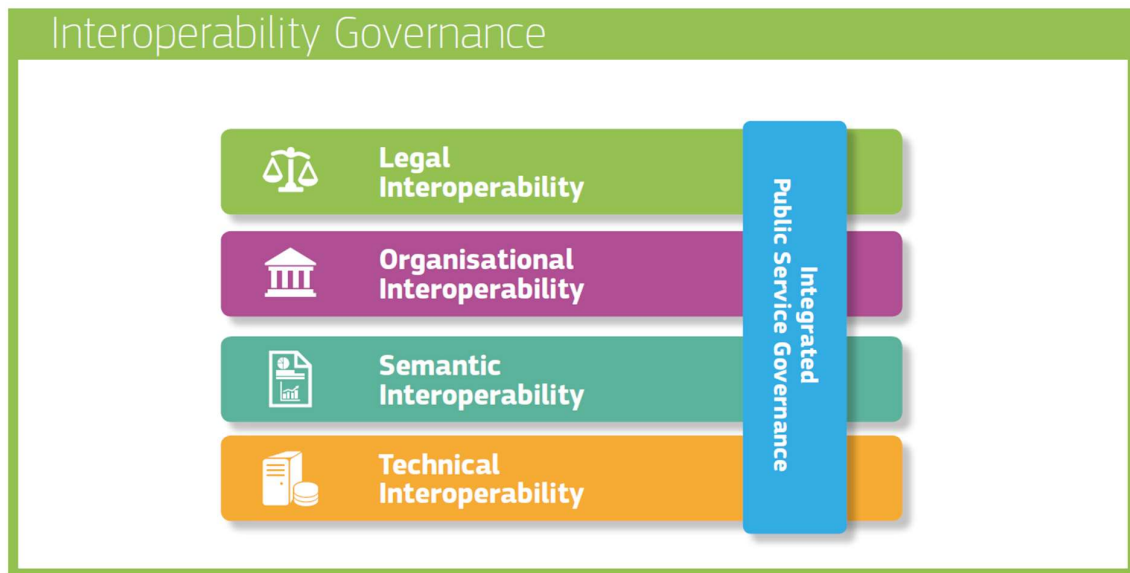


Figure 2. Interoperability model (picture is taken from the EIF)

5.1. Interoperability Governance

5.1.1. Barriers of Interoperability Governance

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

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

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

The implementation of information systems and services often relies on components that are common to many GoU information system owners. The sustainability of these components SHOULD be guaranteed over time. **Interoperability should be guaranteed in a sustainable way** and not as a one-off target or project. As common components and interoperability agreements are the results of work done by MDA/LGs at diverse levels (local, regional, national), coordination and monitoring require a holistic approach. Successful and sustainable implementation of interoperability related principles and rules can be achieved by sustainable planning of actions. It means that planning of state budget for digital transformation is coordinated and implementation of most important developments is supervised. For that ICT expenses must be clearly defined in state budget level.

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

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

5.1.2. Governance on the Interagency Level

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 formation of information society in Uganda. In addition, the Ministry is responsible for supervising its agencies on the implementation and reporting on progress to Cabinet for all ICT interventions including the e-GIF.

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

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

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

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

5.3. It is RECOMMENDED for GoU to centralise development of the policies and decentralise the implementation.

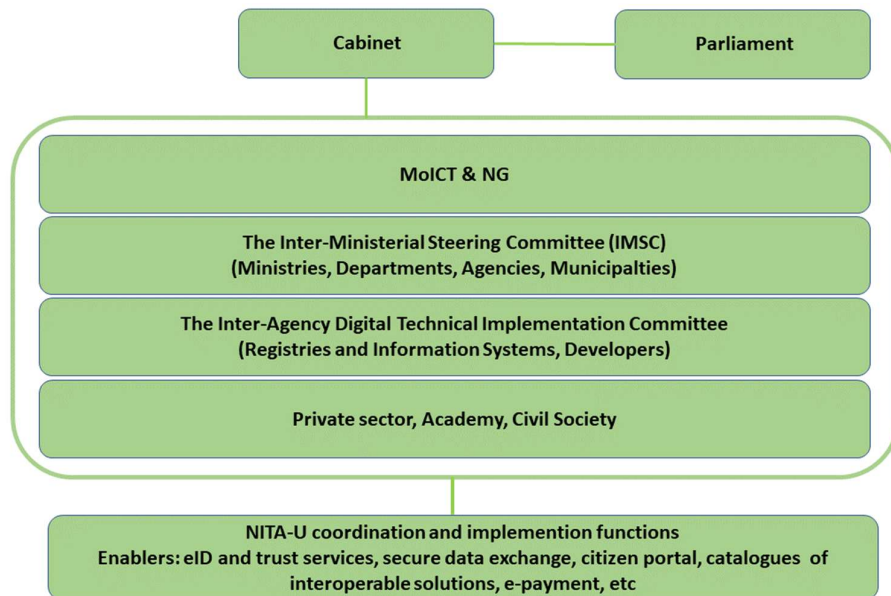


Figure 3. Institutional Framework. NITA-U supports preparing and implementation of strategic and political decisions. MDA/LGs, registries and information systems, developers, private sector, Academy, etc are involved.

Other important stakeholders:

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

Other community organisations

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

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

- Collecting and analysing data about ICT systems in the government
- e-Government budget planning with the Ministry of Finance and donors
- Developing and approving legal acts related to e-Government
- Preparing e-Government strategies and action plans
- Monitoring Action Plan development
- Cooperation with CIOs, training courses for CIOs
- Planning and coordinating international cooperation on e-Government

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

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

5.1.3. Financing

For a e-government development and operation, sustainable financing must be secured. Ugandan e-Government will be financed mainly by the State budget. It will guarantee stability and sustainability of development and maintenance of eGovernment projects and systems. The financing will be provided through annual budgeting. Development of e-government is partially dependent on international donor funding but, this funding should follow rules and principles defined by e-GIF and GEA. The main donor organisations supporting digital transformation in Uganda include UNDP, World Bank and USAID. The Ministry of Finance, Planning and Economic Development (MOFPED) and Ministry of ICT and National Guidance are s coordinating activities with donor.

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

E-government financing can be broadly described as follows:

- Government (or donors) cover investment budget of cross government and sectoral IT systems (hardware, software). Cross-government IT systems budgets are centralized. Sectoral budgets (including MDA ones) are presented in budgets of Ministries.
- Operational costs (maintenance, support, further developments, etc.) are covered from the Ministries (MDA/LG) budgets.

The Government of Uganda charges state levy for public services (including e-services). For example, there are state levy to Motor-Vehicle Registration, transfer; business registration; land search; land transfer, certification services etc.

5.1.4. Monitoring, Conformance, and Enforcement

Interoperability governance shifts from mere alignment to active execution through measurable performance tracking and financial enforcement

- **The Observatory Model:** Uganda uses an Observatory Tool to measure implementation maturity (levels 0–4) for each of the 76 recommendations organised across the three pillars: principles, layers, and the conceptual model.
- **Financial Enforcement (NITA-U N7 Procedures):** Compliance with the e-GIF is a mandatory prerequisite for IT project funding. Any IT project that fails to pass "digital checks" or refuses to use shared national enablers will be denied funding by the Ministry of Finance, Planning and Economic Development (MoFPED).
- **Statutory Status of Solutions:** If an information system is not registered in the central catalogue, it officially "does not exist" in the legal domain and is ineligible for state budget allocation or maintenance funding.

5.4. GoU SHOULD establish procedures for observatory, compliance checking and statutory status

5.1.5. Standards and specifications

The government adopts and draws up standards and specifications for government data and technology processes. The seven principles²² that will be used for adopting and drawing standards by the Uganda government:

- **Standards must meet user needs** - Government IT specifications are based on user needs, expressed in terms of capabilities with associated open standards for software interoperability, data, and document format. Security, risk and privacy aspect MUST be considered.
- **Standards must give suppliers equal access to government contracts** - Standards can be implemented by a diverse range of suppliers. In selecting open standards for government IT specifications, the government removes barriers to competition, such as lock-in.
- **Standards should support flexibility and change** - The government's IT and data and the standards upon which they are built, are enablers for change, giving services the freedom to evolve according to changing user needs, expectations, and technology innovation.
- **Standards must support sustainable cost** - Decisions are based on the most economical solution for the public sector as a whole and costs are sustainable.

²² These principles are adopted from UK open standards policy: <https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles>

- **Decisions on standards selection are well informed** - Effective selection of standards for government IT specifications is a result of pragmatic and informed decision making, taking the consequences for citizens, users, and government finances into account.
- **Select standards using fair and transparent processes** - The selection and adoption process for open standards and open standards-based profiles in government IT is transparent, allowing engagement with the public and subject matter experts.
- **Specify and implement standards using fair and transparent processes**- Government IT procurement, specifications, implementation plans and agreed exemptions from the open standards policy are open and transparent.

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

NITA-U is charged to:

- set, monitor and regulate standards for information technology planning, acquisition, implementation, delivery, support, organisation, sustenance, disposal, risk management, data protection, security and contingency planning
- regulate and enforce standards for information technology hardware and software equipment procurement in all government ministries, departments, agencies and parastatals; and
- protect and promote the interests of consumers or users of information technology services or solutions.

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

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

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

5.2. Integrated Public Service Governance

GoU service provision often requires different MDA/LGs to work together to meet end users' needs and provide **public services in an integrated way**. When multiple organisations are involved, there is a need for coordination and governance by the authorities (NITA-U) with a mandate for planning, implementing and operating GoU shared services. Services SHOULD be

governed to ensure integration, seamless execution, reuse of services and data, and development of new services and **'building blocks'**.²³

5.2.1. Governance on the Administration Level

Ensuring interoperability when preparing legal instruments, organizational processes, and technical components is a continuous task. Administrations must transition to a "Whole-of-Government" (WoG) model where every agency creates sectoral increments to the Ugandan GEA.

Accountability: Each administration must appoint an accountable interoperability leader (typically a CIO or designated coordinator) empowered to enforce e-GIF principles and ensure that internal frameworks are harmonized with national standards

Service Lifecycle Management: Every service must have a defined lifecycle from design to decommissioning. This includes mandatory **"interoperability checks"** and **"digital checks"** during the legislative drafting and policy formulation phases to identify and remove barriers to digital exchange.

Mandatory Use of Shared Enablers: Administration-level governance must mandate the use of centralized national enablers—such as UgHub (with added secure data exchange layer), UgPass (digital identity), and the National Data Centre—to eliminate "ICT islands" and redundant infrastructure spending.

Service Level Objectives (SLOs): Technical components should be managed as reusable products exposed as versioned, contracted microservices with defined Service Level Objectives (SLOs) and clear incident escalation models.

5.7. MDA/LGs MUST transition to a "Whole-of-Government" (WoG) model where every agency creates own sectoral increments to the national GEA

5.2.2. Interoperability Agreements

Organizations involved in integrated service provision must make formal, binding arrangements for cooperation to define responsibilities and ensure service continuity:

- **Layered Agreements:** Formal agreements must cover all four interoperability layers—legal, organizational, semantic, and technical—to clarify data ownership, usage control policies, and custodial roles.
- **Shared SLAs and OLAs:** These agreements should include shared **Service Level Agreements** (SLAs) and Operational Level Agreements (OLAs) that are detailed enough to achieve service aims while preserving each organization's feasible internal autonomy.
- **Change Management:** Robust change management procedures must be established to ensure that updates to one system (especially a **Base Registry**) do not disrupt the

²³ A 'building block' is a self-contained, interoperable, and replaceable unit encapsulating an internal structure.

accuracy, reliability, or security of integrated services relied upon by other public administrations, businesses, or citizens.

- **Registration as a Prerequisite:** No WoG object (dataset, service, ...) is eligible for inter-agency exchange unless it is registered in the legally binding **Catalogues**, which serves as the national "Source of Truth" for metadata, technical specifications, and legal bases.

5.8. MDA/LGs involved in integrated service provision **MUST** make formal, binding arrangements for cooperation to define responsibilities and ensure service continuity.

5.3. Legal Interoperability

Legal interoperability ensures that public administrations—which often operate under distinct sectoral laws, internal policies, and strategic mandates—can interact without legal friction. It provides the "legal glue" that allows a health registry to share data with a social services system, even if they were established by separate Acts of Parliament with differing mandates. Ugandan e-GIF-2026 shifts from a passive legal compliance model to a proactive, "Whole-of-Government" (WoG) alignment strategy. In the e-GIF-2026 framework, legal interoperability is not merely about ensuring systems follow the law; it is about ensuring that the laws themselves are drafted to support a seamless digital society.

5.3.1. Interoperability and Digital Checks

To prevent digital fragmentation and the creation of "ICT islands," all proposed and existing legislation must undergo rigorous screening:

Interoperability Checks: Administrations **MUST** ensure that legislation is screened to identify barriers to interoperability, such as sectoral restrictions on data reuse, contradictory requirements for business processes, or outdated data protection needs.

Digital Checks: When drafting legislation to establish a public service, MDA/LGs **MUST** perform a "digital check" as early as possible in the law-making process. This ensures the law suits the digital world, identifies barriers to digital exchange, and assesses the ICT impact on stakeholders.

Mandatory Catalogue System Approval: All IT-related legislation **MUST** pass through an approval process in the Catalogue System to ensure technical feasibility and alignment with the national architecture.

5.9. Law-making process **MUST** pass the interoperability check, digital check and Catalogues based approval.

5.3.2. Data-Centric Legal Definitions

The e-GIF-2026 framework shifts from a "system-centric" to a "**data-centric**" approach in the law to resolve the "Silo Problem". This involves several key legal principles:

- **Principle of Decoupling:** The legal obligation of a **Dataset** (the information asset) persists independently of the Data Service or technical system used to host it.

- **Statutory Status of Solutions:** If an information system or dataset is not registered in the central catalogue, it officially "does not exist" in the legal domain and is ineligible for state budget allocation.
- **The "Once-Only" Clause:** Legislation should explicitly state that Government Authorities **SHALL NOT** ask data from citizens that is already available as a verified dataset in the national catalogue.

5.3.3. Legal Framework for AI and Automated Decisions

The rapid integration of Artificial Intelligence requires new legal safeguards and enablers:

- **Algorithmic Transparency:** Legal bases must be clarified for **automated/AI-assisted** decisions, ensuring that they are explainable and auditable.
- **AI for Legal Drafting:** AI tools should be used during law-making to suggest harmonized language, detect inconsistencies, and ensure **multilingual semantic alignment** across different jurisdictions.
- **AI-Driven Conformity Checking:** AI systems should be implemented to perform automated checking between legal provisions and actual service implementation rules.

5.3.4. Recommended Framework Legislation

To provide a unified legal foundation for digital governance, the following is recommended:

- 5.10. **Framework Law on Digital Government:** GoU SHOULD consider a framework law defining general rules for the creation and governance of WoG objects, enablers, and information systems
- 5.11. **Regulation of Interoperability Governance:** GoU SHOULD create specific regulations for the governance of the State Information System and the mandatory management of the Catalogue of Interoperability Governance
- 5.12. **Renewal of Secure Data Exchange Legislation:** GoU SHOULD Update the 2019 National Databank Regulations to comprehensively cover secure data exchange aspects and provide stronger legal grounding for the UgHub ecosystem

5.3.5. Compliance with Key National Acts

Legal interoperability actions must remain aligned with Uganda's core digital laws:

- **Data Protection and Privacy Act (2019):** Regulating the processing of personal data.
- **Electronic Transactions and Signatures Acts (2011):** Removing barriers to electronic interaction.
- **Access to Information Act (2005):** Promoting transparency and the right to information in electronic formats.
- **Registration of Persons Act (2015):** Establishing the national identification register as the platform for digital identity.
- **Data Protection and Privacy Act 2019:** This Act protects the constitutional right to privacy by regulating the collection and processing of personal information.

5.4. Organisational Interoperability

Organisational interoperability refers to the way in which public administrations align their business processes, responsibilities, and expectations to achieve commonly agreed and mutually beneficial goals. In the e-GIF-2026 framework, this moves beyond simple documentation to active **WoG** coordination, multi-level governance, and the use of AI to optimize administrative interactions.

5.4.1. Business Process Alignment and Optimization

To provide integrated public services, MDA/LGs must align their existing business processes or define new ones that support seamless data flows.

- **Modelling Standards:** Administrations **SHOULD** document business processes using commonly accepted modelling techniques (e.g., BPMN, UML, ArchiMate) so that all contributing agencies understand the end-to-end process and their specific roles.
- **Proactive and Event-Based Services:** Processes **SHOULD** be re-engineered to be proactive and event-based, moving away from manual application-driven cycles to automated transactions based on digital life-events.
- **AI-Driven Process Mining:** Public administrations **SHOULD** apply AI-driven workflow mining to discover and optimize interoperability-relevant interactions and identify redundant processes or overlapping mandates across agencies.

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

5.4.2. Multi-Level Governance and Relationships

The e-GIF-2026 renewal emphasizes a shift from siloed operations to a unified digital ecosystem that includes international, national, regional, and local government levels.

- **Formal Agreements:** Organisational relationships **MUST** be clarified and formalized through **Memoranda of Understanding (MoUs)** and **Service Level Agreements (SLAs)**. For integrated services, these agreements must define a clear "Chain of Responsibility" for data assets.
- **Multi-Level Seats:** Coordinating an operating body **SHOULD** embed **regional and local actors** in their decision-making processes to ensure that frameworks are practical for LGs implementation.
- **Cross-Sector Interoperability Boards:** Permanent boards should be institutionalized to coordinate across critical economic and social sectors (e.g., Health, Education, Agriculture) to harmonize data-sharing practices

5.4.3. Service Lifecycle and Change Management

Sustainable interoperability requires a structured approach to how services are managed over time.

- **Service Lifecycle Management:** Every digital service **MUST** have a defined lifecycle from design to decommissioning, including regular updates and quality monitoring measured through shared performance dashboards.
- **Mandatory Catalogue Registration:** No organisational process or information system is legally recognized or eligible for state funding unless it is registered in the Catalogues of Interoperability Governance

5.4.4. Capacity Building and Communities of Practice

To sustain organisational interoperability, the government must invest in the people managing these systems.

- **Interoperability Competence Network:** Uganda will build a skilled community of practitioners ensuring officials have the skills in legal, organisational, semantic, and technical areas.
- **Community of Practice:** MDA/LGs **SHOULD** participate in sectoral, national and regional (EAC/COMESA) communities of practice to co-create assets, share lessons learned, and ensure the e-GIF remains a living, evolving framework.

5.4.5. AI-Enhanced Coordination

AI tools should be utilized to improve cooperation and reduce administrative friction:

- **Digital Assistants:** Deploy AI chatbots as digital assistants for cross-department coordination and to interpret complex digital legislation in plain language for public sector employees.
- **Network Mapping:** Use AI-based network mapping to analyse organisational structures and detect collaboration gaps or interoperability bottlenecks in multi-agency workflows.

5.5. Semantic Interoperability

Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties. In the e-GIF-2026 framework, this moves beyond manual data mapping to a data-centric model supported by linked-data standards, automated AI-driven alignment, and a Catalogues System for interoperability governance.

5.5.1. Data as a Strategic Public Asset

Uganda perceives data and information as a valuable public asset that must be generated, collected, managed, and shared as a strategic resource for the nation.

- **The Data-Centric Shift:** MDAs **MUST** transition from a "system-centric" to a "**data-centric**" approach. This regulates the **Dataset** (the information asset) as the primary object of governance, ensuring its legal obligations persist independently of the technical system or database used to host it.

- **Information Management Strategy:** An overarching strategy **MUST** be coordinated at the WoG level to prioritise the management of metadata, master data, and reference data to avoid duplication and fragmentation.

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

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

5.5.2. Metadata Standards and Findability

To ensure consistency across the public sector and enable "findability," Uganda aligns its semantic terminology with international standards.

Mandatory Metadata: Every dataset **MUST** be registered in the Catalogues system with metadata conforming to the W3C DCAT-3 standard.

Single Identifiers for Objects: Information about core objects—such as persons, addresses, and land properties—**MUST** use the same specified single identifier across all Ugandan information systems to ensure cross-sector traceability.

Standard Classifications: MDAs **MUST** use common codes and names (e.g., city codes, currency codes, bank codes) published in the Catalogue of Semantic Assets to ensure data can be compared and analysed across the government.

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

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

5.5.3. Base Registries as the Semantic "Source of Truth"

Base registries are the cornerstone of the "once-only" principle and serve as the authoritative source for semantic standards.

Syntax and Semantic Authority: Owners of base registries (e.g., NIRA for persons, Ministry of Lands for titles) **SHALL** establish the syntax and semantics for their respective data domains.

Mandatory Adherence: All secondary registries and information systems **SHALL** follow the semantic standards established by base registries to ensure data remains consistent as it flows through the Integration/Orchestration processes.

Uniform Addressing: All address objects **MUST** be described by a uniform and unambiguous set of data to support infrastructure planning and service delivery.

5.18. Data standards **SHALL** be established and maintained by owners of base registries and **SHALL** be published in the catalogue of information systems. Other MDA/LGs **SHALL** follow these standards.

5.5.4. Base registries

Base registries provide basic information used across nearly all government sectors. Most important base registries:

- **National Identification Register.** Managed by National Identification & Registration Authority (NIRA),²⁴ 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.**²⁵ 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)**²⁶ includes Uganda's central land registry, covering:
 - Land titles (freehold, leasehold, mailo²⁷)
 - Parcel information
 - Land records digitization
 - Land transactions and cadastral information
- **Government Land Registry:** Registry is managed by the Uganda Land Commission (ULC)²⁸ 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)²⁹ managed registry through periodic censuses that provide:
 - Population data

²⁴ <https://www.nira.go.ug/home>

²⁵ <https://www.registrall.com/company-registries/uganda>

²⁶ <https://mlhud.go.ug/ugnlis/>

²⁷ <https://en.wikipedia.org/wiki/Mailo>

²⁸ <https://ulc.go.ug/>

²⁹ <https://www.ubos.org/>

- 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.**³⁰ 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

5.5.5. AI-Driven Semantic Alignment

Uganda will leverage Artificial Intelligence to automate the alignment of heterogeneous data models and languages.

- **Automated Mapping:** Public administrations **SHOULD** utilize AI models to map equivalent concepts between heterogeneous data schemas and detect hierarchies in taxonomies and ontologies.
- **Multilingual Semantic Equivalence:** AI-based translation tools **SHOULD** be used to ensure that data meanings and metadata remain equivalent across English and relevant Ugandan local languages in digital service interfaces.
- **Semantic Version Tracking:** Use AI agents to validate semantic consistency during real-time data exchange and to automatically track changes in data meaning over time to prevent "semantic drift".

5.5.6. Semantic Readiness for Data Spaces

As Uganda moves toward a federated architecture, semantic assets must be designed for broader integration.

- **Linked Data Vocabularies:** Administrations **SHOULD** institutionalize linked-data vocabularies and ontologies to support machine-to-machine reasoning and data-driven decision-making.

³⁰ <https://nhfr.health.go.ug/>

- **Regional Alignment:** Semantic assets **MUST** be designed for compatibility with EAC and COMESA digital protocols to facilitate secure, interoperable cross-border data exchange.

5.6. Technical Interoperability

Technical interoperability covers the applications and infrastructure linking systems and services, including interface specifications, interconnection services, and secure communication protocols. Technical interoperability architecture will be created through “building blocks”. Building blocks can be layered into 6 layers as depicted in Figure 1.³¹

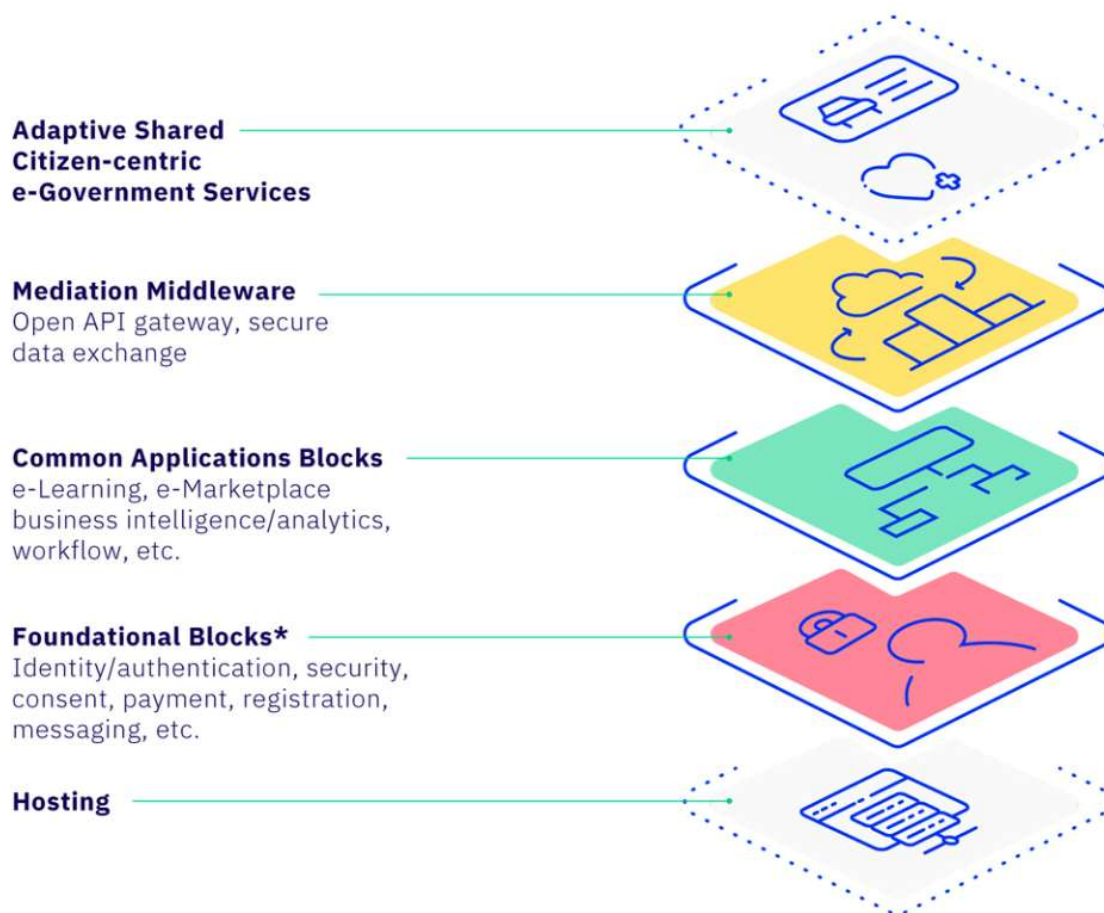


Figure 4 Layers of technical architecture

In the e-GIF-2026 framework, Uganda transitions from legacy "hub-and-spoke" models to a **Federated Data Space** architecture, making **API-first** and **event-driven** patterns the mandatory default for all new government IT investments.

³¹ <https://specs.govstack.global/>

5.6.1. Service-oriented architecture

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

5.20. Service-oriented architecture MUST be followed by MDA/LGs.

5.6.2. API-First and Event-Driven Architecture

To eliminate "ICT islands" and support real-time public services, MDAs **MUST** adopt modern architectural patterns:

- **API-First Mandatory Default:** All new information systems **MUST** expose their functionality via secure, versioned, and well-documented APIs (e.g., REST, WSDL, GraphQL).
- **Event-Driven Patterns:** For proactive and real-time services, MDA/LGs **SHOULD** utilise event buses and message brokers to enable systems to react to digital life-events (e.g., automated notification of birth to health and identity registries).
- **AI-Based Discovery:** Uganda will utilise AI-based API discovery and matching tools within the Catalogues to facilitate faster system integration and detect interface incompatibilities.

5.21. MDAs SHOULD adopt API-First and Event-Driven Architecture

5.6.3. Federated Data Space and Decentralization

Uganda is shifting away from centralized traffic controllers toward a Federated Data Space model to ensure scalability and data ownership.

- **Sovereign Connectors:** Integration **SHALL** be achieved through distributed sovereign connectors rather than a single central message bus, eliminating "Single Points of Failure" (SPOF).
- **Data Stays at Source:** Data **MUST** remain with the custodial MDA. Consumers access data through the Integration/Orchestration processes, ensuring MDAs maintain absolute control over their primary registries.
- **Cryptographic Non-Repudiation:** All technical exchanges **MUST** implement "Evidence of Exchange" receipts signed via the Ugandan PKI system to provide undeniable proof of origin and receipt.

5.22. To ensure scalability, data ownership and Non-Repudiation GoU SHOULD shift to the Data Space Architecture.

5.6.4. Cloud-Native and Zero-Trust Security

Technical interoperability must be resilient against modern cybersecurity threats and portable across infrastructure providers.

- **Zero-Trust Model:** MDA/LGs **MUST** implement a zero-trust security architecture, where no device or user is trusted by default, regardless of their location on the government network.
- **Cloud-Native Patterns:** Information systems **SHOULD** be designed using cloud-native patterns (e.g., containerisation, microservices) to ensure portability across the Secure Data Exchange System and edge solutions.
- **AI-Enhanced Monitoring:** Deploy AI-enhanced cybersecurity monitoring to identify anomalies in cross-border and cross-sector data exchanges in real-time.

5.23. To achieve resiliency against cybersecurity threats Administrations **MUST** implement Zero-Trust Security architecture.

Administrations **SHOULD** design their information systems using Cloud Native patterns.

5.6.5. Technical Conformance and Observability

To ensure sustained interoperability, technical components must be measurable and auditable.

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

Observability Baseline: Every operational component **MUST** include built-in metrics for reliability, performance, and latency, feeding into Ugandan Observability Dashboards.

AI Auto-Documentation: MDAs **SHOULD** use AI auto-documentation tools to maintain up-to-date technical specifications and API documentation in the Catalogues of Interoperability Governance.

5.6.6. Legacy System Transition

Acknowledge that legacy systems are a major obstacle to technical interoperability.

- **Modernization Wrappers:** For critical legacy systems unable to natively support APIs, MDA/LGs **MUST** implement API wrappers or middleware to expose data to the Ugandan Secure Data ecosystem.
- **Exception Handling:** Any project seeking funding for legacy system maintenance must pass an "interoperability check" to define a clear transition plan toward e-GIF-2026 standards.

6.The Conceptual Model for Integrated Public Services Provision

6.1. Introduction

The conceptual model for integrated public services proposes a blueprint for the “interoperability by design” paradigm. It is relevant to all governmental levels – regional, ministerial, sectorial, national – and promotes a modular approach where loosely coupled service components are interconnected through a shared infrastructure. The e-GIF-2026 model shifts from legacy static architectures to a Federated Data Space model, emphasizing the reuse of existing information and services across organisational boundaries. Conceptual model by using ArchiMate notation is depicted in Figure 5.

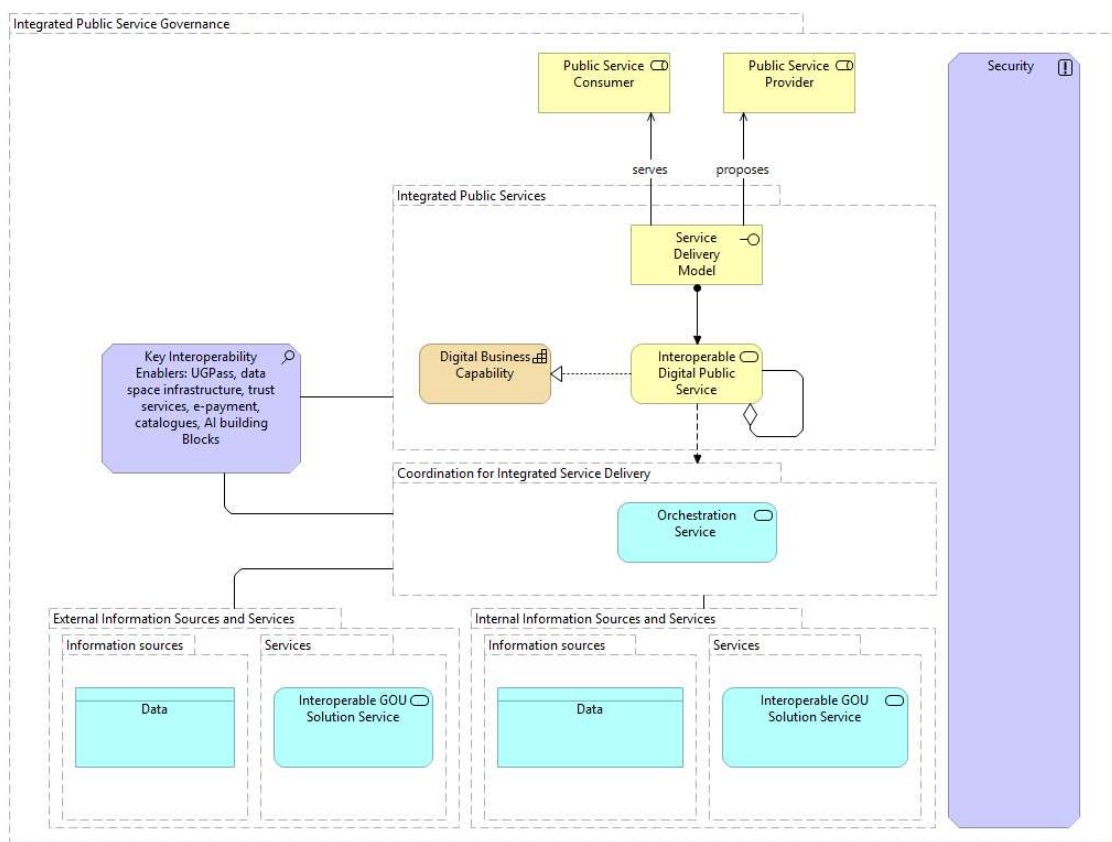


Figure 5 Conceptual model

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

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

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

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

6.2. Model overview

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

The basic components of the conceptual model are presented below.

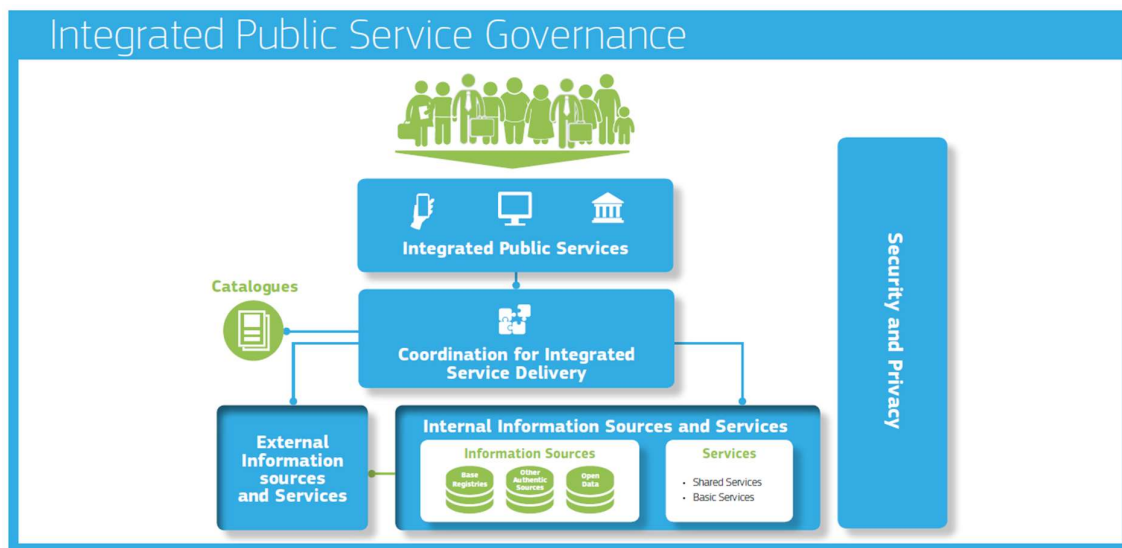


Figure 6. Conceptual model for integrated public services (taken from EIF)

The e-GIF-2026 conceptual model promotes the idea that public services should be designed with reusability as the primary driver for interoperability.

The Federated Data Space Paradigm: Uganda is transitioning from a centralized "Hub-and-Spoke" model to a Federated Data Space. In this model, data remains at its source with the custodial MDA, and integration is achieved through distributed Sovereign Connectors.

The Distributed Integration/Orchestration layer. Rather than a central facility, the Integration/Orchestration layer is a decentralized technical layer that coordinates secure, peer-to-peer data exchange without compromising participant sovereignty. It consists of distributed API gateways, an event bus for real-time orchestration.

Service Delivery Principles: The model enforces a “No Wrong Door” policy, ensuring citizens can access assistance through any channel (service bureaus, digital portals, or post) while requests are routed seamlessly to the correct authority.

6.3. Shared Enablers and Reusable Building Blocks

To ensure consistency and efficiency, MDAs SHALL utilize centralized national enablers rather than developing redundant institutional solutions.

- **Core Shared Enablers:** Mandatory building blocks include Digital Identity (UgPass), Secure Data Exchange (renewed UgHub), the National Payment Switch, PKI ecosystem, and the Catalogues system for interoperability governance.
- **AI-Enabled Components:** The model explicitly incorporates AI building blocks, such as document intelligence, multilingual assistance, and decision support systems with a mandatory human-in-the-loop (HITL) requirement.
- **Standardized Connector Stacks:** MDAs utilize Data-Space Adapters to participate in the federated ecosystem with minimal custom development, ensuring technical and semantic compatibility across sectors.

6.4. Internal information sources and services

Uganda adopts a "Data-Centric" approach, treating data as the primary object of governance independent of the systems hosting it.

- **Decoupling Principle:** The legal obligation of a Dataset (the information asset) persists independently of the Data Service (the API) or Information System used to host it.
- **The "Once-Only" Principle:** The architecture is designed to ensure citizens and businesses provide information to the state only once, with that data being reused securely across the entire federated ecosystem.
- **Proactive and Event-Based Services:** Processes are re-engineered to react in real-time to digital life-events (e.g., birth or business registration) instead of relying on manual application cycles.

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

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

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

aggregation is relevant to information, services, and other interoperability solutions (e.g. software).

6.5. Base registries

Base registries are trusted, authoritative datasets that serve as the primary legal source of truth for specific domains.

6.4. **Mandatory Adherence:** Owners of base registries SHALL set up the syntax and semantics for their respective data domains, which all secondary systems MUST follow.

6.5. **Service Level Obligations (SLO):** Data Providers are legally RESPONSIBLE for the availability and integrity of the data services connected to base registries.

6.6. **Quality and Transparency:** Base registries SHALL implement data quality assurance plans and allow citizens to verify the accuracy of their data in line with the Data Protection and Privacy Act.

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

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

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

6.6. Open data

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

GoU SHALL establish Open Data policy/framework³² and update it regularly. Open data working group with the participation of the private sector, academy and SCO SHOULD be established.

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

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

³² <https://www.ict.go.ug/wp-content/uploads/2018/06/Open-Data-Policy-First-Draft-vX.pdf>

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

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

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

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

6.7. Interoperability Governance Catalogues

Catalogues help others to find reusable resources (e.g. services, data, software, data models). Several 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.

Uganda utilizes a legally binding system of catalogues as the primary instrument for digital coordination which includes catalogues of administrations, public services, datasets, information systems, data services (APIs), enablers, semantic assets. System of catalogues acts as:

- **Mandatory Registration:** Any information system, registry, or dataset not registered in the central catalogue officially “does not exist” in the legal domain and is ineligible for state budget allocation.
- **Approval Platform:** The catalogue acts as the platform for conducting mandatory “digital checks” and “interoperability checks” during the legislative drafting and project planning phases.

6.13. GoU SHALL utilise a legally binding system of catalogues as the primary instrument for digital coordination.

6.8. External information sources and services

MDA/LGs need to exploit services delivered outside their organisational boundaries by third parties, such as payment services provided by financial institutions or connectivity services provided by telecommunications providers. They need also to exploit external information sources such as open data and data from international organisations, chambers of commerce,

etc. Moreover, useful data can be collected through the Internet of Things (e.g. sensors) and social web applications.

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

The model is cross-border ready, ensuring compatibility with East African Community (EAC), COMESA, and AfCFTA digital protocols.

6.15. MDAs SHOULD consider regional interoperability needs when designing new services to facilitate secure cross-border data exchange.

6.9. Security and privacy

The model mandates a Zero-Trust and security-by-design architecture across all layers.

6.16. **Cryptographic Non-Repudiation:** Technical exchanges MUST implement “Evidence of Exchange” receipts signed via the National PKI to provide undeniable proof of origin and receipt.

6.17. **Data Sovereignty and Usage Control:** MDAs SHOULD maintain sovereignty over their data using machine-readable Usage Control Policies (ODRL) to dictate exactly who can access data and for what purpose.

6.18. **Personal Data Protection:** Citizens SHALL be supplied with services to check their data and find out who has accessed it, in full compliance with the Data Protection and Privacy Act (2019).

6.19. **Algorithmic Transparency:** For any service utilizing AI for decision support, the integration/orchestration service SHOULD ensure citizens can understand and audit automated outcomes.

6.20. Administrations MUST follow the rules and procedures of National Information Security Framework (NISF) 2026 and National Cybersecurity Strategy (2022-2026)

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

- they follow the **privacy-by-design** and **security-by-design** approach to secure their complete processes (including supply chain), infrastructure and building blocks.
- public sector organisations **manage information security** systematically and methodically.
- services **are not exposed to threats** which might interrupt their operation and cause data leakage or data damage.

- they are compliant with the legal requirements and obligations regarding **data protection and privacy**³³ acknowledging the risks to privacy from advanced data processing and analytics.
- they are compliant with the legal requirements and obligations regarding the **use of electronic communications and transactions**.³⁴
- they are compliant with the legal requirements and obligations regarding the use of **electronic signatures** and **public key infrastructure** for authenticity and security.³⁵

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

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

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

³³ Data Protection and Privacy Act 2019.

<https://www.nita.go.ug/sites/default/files/publications/Draft%20Data%20Protection%20and%20Privacy%20Regulations%202019.pdf>

³⁴ Electronic Transactions Act 2011 (Act No. 8 of 2011) <https://www.nita.go.ug/publication/electronic-transactions-act-2011-act-no-8-2011>

³⁵ Electronic Signatures Act 2011 (Act No. 7 of 2011)

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

7. Governance of Interoperability Framework

The governance of the e-GIF 2026 ensures that digital transformation and interoperability is coordinated as a WoG effort.

7.1. Institutional Roles

Political Leadership: The Ministry of ICT and National Guidance (MoICT&NG) coordinates national interoperability initiatives and ensures the framework remains modern.

Implementation Agency: NITA-U serves as the autonomous statutory body responsible for building and maintaining interoperability enablers, including the PKI ecosystem, secure data exchange

Sectoral Accountability: Each sector and MDA/LG is responsible for building its own internal architecture increments, provided they are harmonized with the national e-GIF standards.

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

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

7.2. Assessment and Approval Procedures

All assessment and approval procedures, including N7 procedures, SHOULD will be carried out through Catalogues System.

Any information system, registry, or dataset not registered in the Catalogues System is legally deemed non-existent and is ineligible for state budget allocation.

7.3. All digital government assessment and approval processes SHALL be compliant with the e-GIF and GIRA.

7.3. Monitoring and the Observatory

GoU regularly assess the implementation level of every recommendation. The observatory process provides dashboards for decision-makers to identify bottlenecks in legal, organizational, semantic, or technical layers across the public sector.

7.4. Incremental Architecture Methodology

The implementation of the GEA and e-GIF follows an Incremental Architecture Methodology. Rather than a "big-bang" rollout, the framework is delivered through prioritized architecture packages (e.g., identity, payments, or sectoral increments), allowing the government to deliver early wins while continuously maturing the national architecture.

7.5. Role of sectors and administrations

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

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

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

7.4. Sectoral Accountability: Each sector and MDA/LG is responsible for building its own internal architecture increments, provided they are harmonized with the national e-GIF standards and GEA

8.Abbreviations

Abbreviation	Meaning
A2A	Administration to administration
A2B	Administration to business
A2C	Administration to Citizen
AI	Artificial Intelligence
AfCFTA	African Continental Free Trade Area
Africa CDC HIE	African Union Health Information Exchange
BpMN	Business Process Modelling Notation
CI/CD	Continuous Integration/Continuous Delivery/Deployment
COMESA	Common Market for Eastern and Southern Africa
DCAT	Data Catalogue Vocabulary
DUV	Digital Uganda Vision
EAC	East African Community
e-GIF	e-Government Interoperability Framework
eID	Electronic Identity
EIF	European interoperability framework
EU	European Union
FRAND	Fair, Reasonable, and Non-Discriminatory
GEA	e-Government Enterprise Architecture
GESA	e-Government Enterprise Security Architecture
GIRA	e-Government Interoperability Reference Architecture
GoU	Government of Uganda
GraphOL	A Graphical Language for Ontology Modelling
HITL	Human-in-the-Loop
ICT	Information and communication technology
IMSC	The Inter-Ministerial Steering Committee
IOT	Internet of things
ISMS	Information Security Management System
LLMs	Large Language Models
MDA/LG	Ministries Departments, Agencies and Local governments
MoICT&NG	The Ministry of Information and Communications Technology and National Guidance
MoU	Memorandum of Understanding
NCIP	Northern Corridor Integration Projects
NITA-U	National Information Technology Authority
NIRA	National Identification & Registration Authority
NISF	National Information Security Framework
NISP	National Information Security Policy
NTR	Non-Tax Revenue
ODRL	Open Digital Rights Language
OLA	Operational Level Agreements
PCC	Policy Coordination Committee
PKI	Public Key Infrastructure
PPP	Public-Private-Partnership
SLA	Service Level Agreement

SLO	Service Level Objectives/Obligations
SOA	Service-oriented architecture
SPOF	Single Points of Failure
UgHub	Ugandan Data integration Platform
UML	Unified Modelling Language
UNBS	Uganda National Bureau of Standards
UNDP	United Nations Development Programme
USAID	U.S. Agency for International Development
WSDL	Web Services Description Language

9. Glossary

Term / acronym	Definition
Aggregate Public Services	A generic term used in the conceptual model for public services to refer to a set of basic public services accessed in a secure and controlled way before being combined and then delivered as a whole to end users.
Artificial Intelligence (AI)	AI acts as a driver for interoperability by improving the capacity of systems to exchange, interpret, and reuse information across legal, organisational, semantic, or technical boundaries. Conversely, interoperability for AI requires that these systems are designed to natively interoperate, adhering to common standards, transparent data structures, and explainable algorithms to prevent the creation of new digital silos
Authentic Source	An authentic source is information that is stored only once and which is believed to be correct, so can serve as a basis for reuse.
Base registry	A base registry is a trusted and authoritative source of information, which CAN and SHOULD be digitally reused by others, where one organisation is responsible and accountable for the collection, use, updating and preservation of information.
Building block approach	An approach to building information systems from architecture to implementation in which the information system is designed as an assembly or aggregation of components that encapsulate data and functionalities in groups that can also be reused as 'building blocks' to build other public services or information systems.
Business Process	A business process is a sequence of linked activities that creates value by turning inputs into a more valuable output. This can be performed by human participants or ICT systems, or both.
Catalogues	Catalogues is a metadata repository of WoG objects and mandatory instrument for interoperability governance.
Data Controller	Person, who alone, jointly with other persons or in common with other persons or as statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.
Data Processor	Data processor in relation to personal data, means a person other than employee of the data controller who processes the data on behalf of the data controller.
Data Repository	Any collection of data meant for use (processing, storage, querying, etc.) by an information system. Typically, a data repository contains additional structural and semantic information about the data in question, designed to aid the use of the data (data model, relationships between data elements, metadata, etc.). It may provide specific functionalities closely tied to the data stored in the repository (searching, indexing, etc.).
Dataset	An identifiable collection of data, controlled or managed by a government authority, representing a specific administrative, legal, or functional domain.
Data Space	Data Space is a secure, decentralized ecosystem that allows different government agencies, public institutions, and trusted

	private partners to share and access data without losing sovereignty over it.
eGovernment	eGovernment is about using the tools and systems made possible by information and communication technologies (ICTs) to provide better public services to citizens and businesses.
Electronic Certification	Electronic certification is the application of an electronic signature, by a specifically authorised person or entity, in a specific context for a specific purpose. It is mostly used to indicate that a certain validation process has been executed and that a given result is being attested by the signer.
Electronic Signature	An electronic signature, or e-signature, refers to data in electronic form, which is logically associated with other data in electronic form, and which is used by the signatory to sign. This type of signature provides the same legal standing as a handwritten signature as long as it adheres to the requirements of the specific regulation under which it was created
Enabler	Enablers support interoperability by offering services, data structures, standards, or guidelines that can be reused across many solutions. They enable the functioning of digital public services.
Formalised Specifications	Formalised specifications are either standards or specifications established by ICT industry fora or consortia.
Government Enterprise Architecture (GEA)	The structure of e-Government components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.
Information	Information is semantically enriched data, i.e. collections of data that have been given relevance and purpose.
Information System	A set of technical components, including software, hardware, and network infrastructure, organized to perform specific functions of collecting, processing, storing, and distributing information designed to collect, process, store, and distribute information.
Interface	An interface is a conceptual or physical boundary where two (or more) independent legal systems, organisations, processes, communicators, IT systems, or any variation/combination thereof interact.
Interoperability	The ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their ICT systems.
Interoperability Agreements	Written interoperability agreements are concrete and binding documents which set out the precise obligations of two parties cooperating across an 'interface' to achieve interoperability.
Interoperability Framework	An interoperability framework is an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.

Interoperability Governance	Interoperability governance covers the ownership, definition, development, maintenance, monitoring, promoting and implementing of interoperability frameworks in the context of multiple organisations working together to provide (public) services. It is a high-level function providing leadership, organisational structures and processes to ensure that the interoperability frameworks sustain and extend the organisations' strategies and objectives
Interoperability Levels	The interoperability levels classify interoperability concerns according to who/what is concerned and cover, within a given political context, legal, organisational, semantic and technical interoperability.
Legal interoperability	Ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together
Memorandum of Understanding	A bilateral or multilateral written agreement between two organisations which sets out a number of areas and means by which they will cooperate, collaborate or otherwise assist one another. The exact nature of these activities depends on the nature of the two organisations, the domain of activity in question, and the scope of the cooperation envisaged.
Orchestration	The aggregation and sequenced execution of sets of transactions involving use of other services and functionalities, according to business rules embodied in one or more documented business processes, with the ultimate goal of performing or providing some other value-added function or service. Orchestration is closely related to the concept of workflow. Usually, orchestration involves executing a set of processes, described in a standard language, by an 'orchestration engine', which is configurable and capable of executing all the requisite service calls and routing the inputs and outputs of processes according to rules described in that language.
Organisational Interoperability	Ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together
Open Data	Open data is information that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.
Public Service	Service can be: A repeatable activity: a discrete behaviour that a component of organisation may be requested or otherwise triggered to perform. An element of behaviour that provides specific functionality in response to requests from actors or other services.
Reusability	The degree to which a software module or other work product can be used in contexts other than its original, intended or main purpose.
Shared services	Shared services are Services provided centrally by one or several public administrations that can be reused by others to support the delivery of digital public services. They typically cover common functions needed by many government services.

Secure Data Exchange	This is a component of the conceptual model for public services. Its aim is to ensure that all data exchanges are done in a secure and controlled way.
Semantic interoperability	Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'.
Semantic Interoperability Assets	Semantic interoperability assets are a subset of interoperability assets and include any element of the semantic layer, such as nomenclatures, thesauri, dictionaries, ontologies, mapping-tables, mapping-rules, service descriptions, categories, and web services.
Service Agreement Level	A formalised agreement between two cooperating entities; typically, a service provider and a user. The agreement is expressed in the form of a written, negotiated contract. Typically, such agreements define specific metrics (Key Performance Indicators — KPIs) for measuring the performance of the service provider (which in total define the 'service level'), and document binding commitments defined as the attainment of specific targets for certain KPIs, plus associated actions such as corrective measures. SLAs can also cover commitments by the user, for example to meet certain notification deadlines, provide facilities or other resources needed by the service provider in the course of service provision, problem solving, or to process inputs given by the service provider to the user.
Service Orientation	Service orientation means creating and using business processes packaged as services.
Service-oriented architecture (SOA)	Service-oriented architecture is a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations
Standard	A standard is a technical specification approved by a recognised standardization body for repeated or continuous application, with which compliance is not compulsory
Taxonomy	A taxonomy represents a classification of the standardised terminology for all terms used within a knowledge domain. In a taxonomy, all elements are grouped and categorised in a strict hierarchical way and are usually represented by a tree structure. In a taxonomy, the individual elements are required to reside in the same semantic scope, so all elements are semantically related with one another to one degree or another.
Technical interoperability	Technical interoperability covers the applications and infrastructure linking systems and services
GoU Interoperability Framework (e-GIF)	The agreed approach to the delivery of GoU public services in an interoperable manner. It defines basic interoperability guidelines in the form of common principles, models, and recommendations.

Vocabulary	A vocabulary is a set of terms (words or phrases) that describe information in a particular domain.
Workflow	The organisation of a process into a sequence of tasks that are performed by duly designated sets of actors fulfilling given roles in order to complete the process.