Tonga Interoperability Framework (TIF)

Project: Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure

Version 1.0
11 January 2022

Table of Contents

1. Executive Summary

Interoperability is the ability of making systems and organizations operate together (inter-operate). The objective of the Tongan Interoperability Framework, hereinafter: **TIF**, is to outline the main principles and general guidelines enabling the development and implementation of electronic services for citizens, businesses, and public administrations in the Government of Tonga.

TIF reuses the terminology and paradigms of TOGAF®[1] (The Open Group Architecture Framework) and the generic European Interoperability Framework (EIF)[2]. It uses the approach of terminology and structure of the EIF, but the content is adjusted to the Tongan national policies, strategies, and guidelines.

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

- cooperation between public administrations aiming at the establishment of public services,
- information exchange between public administrations to fulfil legal requirements or political commitments,
- sharing and reusing information among public administrations to increase administrative efficiency and reduce administrative burden on citizens and businesses.

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

To achieve the **interoperability by design** paradigm, TIF implements a model that includes:

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

Public administrations need to agree on a common approach to interconnect information systems and services. TIF proposes a conceptual model that must be used as the baseline for that common approach that comprises loosely coupled components that are interconnected through shared infrastructure.

To ensure interoperability of public sector information systems, several common infrastructure components with very clear ownership and leadership must be established in the public sector.

[1] http://www.opengroup.org/subjectareas/enterprise/togaf

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

2. Introduction

The Tonga Interoperability Framework (TIF) supports the vision "A more progressive Tonga supporting higher quality of life for all" and the goals the Government of Tonga fixed in the Tongan Strategic Development Framework 2015-2025 (TSDF):[3]

- A more inclusive, sustainable, and dynamic knowledge-based economy
- A more inclusive, sustainable, and balanced urban and rural development across island groups
- A more inclusive, sustainable, and empowering human development with gender equality
- A more inclusive, sustainable, and responsive good governance with law and order
- A more inclusive, sustainable, and successful provision and maintenance of infrastructure and technology
- A more inclusive, sustainable, and effective land administration, environment management, and resilience to climate and risk
- A more inclusive, sustainable, and consistent advancement of our external interests, security, and sovereignty

One of the five pillars of the TSDF is dedicated to the use of reliable, safe, and affordable information and communication technology.

The first Tonga Digital Government Strategic Framework (TDGSF) promotes the use of ICT within government ministries and agencies. This promotion includes an aggressive transition from paper-based transactions to digital government. TDGSF sets the following objectives:

- Strengthen and build governance through change management
- Implement digital government across all government agencies and activities
- Advance digital inclusion for all
- Promote data sharing and a service-oriented information systems architecture
- Enhance public engagement

TDGSF includes the following inter-connected and mutually re-enforcing basic principles that each information technology (IT) infrastructure project or information systems (IS) project should consider prior to procurement: security, connectivity, interoperability, portability, innovation, accessibility, customer focus, standardization, redundancy, holistic (whole-of-government) approach.

TSDF and TDGSF serve as starting points for developing the Tongan Enterprise Architecture Framework (TEAF) including the Tonga Interoperability Framework (TIF).

[3] Tonga Strategic Development Framework (TSDF II), 2015-2025
http://extwprlegs1.fao.org/docs/pdf/ton168846.pdf

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

TIF uses the terminology and structure of EIF, the content is adjusted to Tongan national policies, strategies, and guidelines.

2.1. Context

TIF is an important part of activities for building the Tonga Enterprise Architecture Framework (TEAF). By TEAF 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 TEAF lifecycle:

- **Strategy of building an information society**. The strategy is fixed in vision papers of the government (such as TSDF and TDGSF), and in legislation.
- **TIF**. TIF provides an implementation strategy for the TEAF. It defines basic interoperability guidelines in the form of common principles, models, and recommendations for interactions between public institutions.
- **Tonga Enterprise Reference Architecture Framework**. 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 Ministries, Departments, and Agencies (MDAs).
- **Implementation of TEAF.** This phase provides an implementation plan and a roadmap highlighting the required activities, resources, and timelines as well as cross-government governance structures to ensure compliance and uptake of the developed TEAF.
- **Governance of TEAF.** Building, monitoring, managing, and steering of the implemented TEAF. Building the TEAF is an iterative process. Some components need to be renewed; sometimes some components need to be added. Sometimes it is reasonable to start a new lifecycle from the beginning.

2.2. Definitions

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. The definition of the European Commission[4] is followed, which has been internationally accepted in governmental context:

> *"Interoperability is the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between the organisations,*

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

> *through the business processes they support, by means of the exchange of data between their ICT systems."*

Public service. In this document, we follow the service-oriented principle. It means all the activities of any organisation are considered as services. A 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 a specific functionality in response to requests from actors or other services.

A Tongan public service comprises any public sector services supplied by MDAs, either to one another or to businesses or citizens of Tonga.

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

2.3. Purpose

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

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

The TIF is oriented to:

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

The objective of the TIF 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.

TIF is a set of agreements and guidelines aimed at ensuring the provision of services for institutions, enterprises, and citizens. TIF serves as:

- guidance for elaborating concepts for country-wide information systems – interoperability enablers

- guidance for IT project managers at the MDAs for elaborating concepts for the information systems of their institutions
- a list of requirements for public procurements.

The specific objectives of the Tongan Interoperability Framework are the following:

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

The report contains:

- the list of underlying principles for achieving interoperability
- the principles for achieving interoperability at the legal, organisational, semantic, and technical levels
- the public service conceptual model

The primary target groups of the interoperability framework are public sector officials with the following roles:

- Permanent Secretaries
- Chief Executive Officers (CEO)
- Chief Financial Officers (CFO)
- Chief Information Security Officers (CISO)
- Chief Information Officers (CIO)
- Chief Technical Officers (CTO)

TIF is also a guideline for private sector managers and project leaders who offer development and administrative services to the public sector. The government encourages the private sector to follow the TIF and use the government’s shared interoperable solutions.

The Ministry of Finance (MOF) and the Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Climate Change and Communications (MEIDECC), responsible for planning and development of the state information systems, are also in charge of designing the Interoperability Framework and the related documents.

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

2.4. Scope and Structure

TIF and TEAF are applicable for all information systems in Tonga. They lay 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 Tonga.

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

TIF is oriented to the development of a Tongan public services ecosystem in which owners and designers of systems and public services become aware of interoperability requirements, MDAs are ready to collaborate with each other and with businesses and citizens, and information flows seamlessly across Tonga.

TIF's scope covers three types of interactions:

- G2G (MDA to MDA), which refers to interactions between MDAs
- G2B (MDA to business), which refers to interactions between MDAs and businesses
- G2C (MDA to citizen), which refers to interactions between MDAs and citizens.

TIF's content and structure is presented below:

- Chapter 3 presents a set of 12 **principles** that are intended to establish the general behaviour towards interoperability. This chapter provides 28 requirements/ recommendations for MDAs.
- Chapter 4 presents a layered **interoperability model**, which presents the different layers of interoperability aspects to be addressed when designing public services. This chapter provides 29 requirements/recommendations for MDAs.
- Chapter 5 outlines a **conceptual model** for interoperable public services. The model is aligned with the interoperability principles and promotes the idea of 'interoperability by design' as a standard approach for the design and operation of public services. This chapter provides 16 requirements/recommendations for MDAs.
- Chapter 6 stipulates the rules of **TIF governance**. TIF handles information systems from the point of view of the state as a whole. The maintenance of the TIF document will be handled by the strategic and coordination bodies[5]. This chapter provides 5 requirements/recommendations for TIF governance.

[5] Currently MOF and MEIDECC

- Chapter 7: Abbreviations
- Chapter 8: Glossary

The requirements and recommendations are numbered across the chapters and highlighted in green boxes.

> The most important conclusions and requirements have been provided in green text boxes. They are numbered within the chapters throughout the document.

The keywords 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)[6]. To highlight the relevance of these words, they have been provided in block capitals and their meaning is as follows:

Keywords expressing the meaning	**Meaning**
MUST, REQUIRED, SHALL	Required/obligatory. Absolute requirement.
SHOULD, RECOMMENDED	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.
MAY, OPTIONAL	Acceptable/allowed.
SHOULD NOT, NOT RECOMMENDED	Not recommended. Acceptable only under reasons or circumstances.
MUST NOT, SHALL NOT	Prohibited. Absolute prohibition.

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

3. Underlying Principles

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

The TDGSF gives ten basics architecture principles that IT project should consider prior of procurement: security, connectivity, interoperability, portability, innovation, accessibility, customer focus, standardization, redundancy, holistic (whole-of-government) approach. TIF principles are more specific and oriented to the achieving interoperability. There is a strong overlap between these two sets of principles: most TDGSF principles are important for interoperability as well.

The twelve underlying principles of the TIF are grouped into four categories:

- Principles setting the context for Tongan Government 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 MDAs (principles 10 to 12).

TIF is based on the following principles:

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

3.1. Principle 1: Subsidiarity and Proportionality

Subsidiarity. The subsidiarity principle implies that Tongan Government 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 a lower level (e.g. ministry level). Application of subsidiarity principles means that centralized solutions are used as little as possible. At the same time, the subsidiarity principle does not restrict public sector institutions cooperation on working out joint standard solutions.

Proportionality. By using a central solution, public bodies MUST NOT lose control of own business processes and data.

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

3.2. MDAs MUST align their frameworks and strategies with the TIF.

3.3. Decisions related to information technology SHOULD be taken at the political level only if this is more efficient than doing it at the level of public sector institutions.

We distinguish between three types of activities: centralized, standard solutions, and decentralized.

Centralized. Tonga has decided to centralise:

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

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

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

Decentralized solutions should focus on functional role of each ministry. Each Ministries have their own network segment assigned to each ministry in which they have the freedom to develop on it, but they are still part of the whole Government secured backbone network that is centralized managed. Each ministry should be the own custodian of their own website contents, datasets etc.

3.2. Principle 2: Openness

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

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

3.4. MDAs MUST publish the data they own as open data unless certain restrictions apply.

The positive effect of open specifications is demonstrated by the internet ecosystem. However, MDAs 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.

3.5. MDAs MUST give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation.

3.3. Principle 3: Transparency

Transparency in the TIF context refers to:

- Enabling **visibility** inside the administrative environment of an MDA. This is about allowing other MDAs, citizens, and businesses to view and understand administrative rules, processes, data, services, and decision-making.
- Ensuring **availability of interfaces** with internal information systems. MDAs operate many often heterogeneous and disparate information systems to support their internal processes. Interoperability depends on ensuring the availability of interfaces to these systems and the data they handle. In turn, interoperability facilitates the 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 MDAs.

3.6. MDAs SHOULD ensure internal visibility and provide external interfaces for Tonga public services.

3.4. Principle 4: Reusability

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

3.7. MDAs SHOULD reuse and share solutions and cooperate in the development of joint solutions.

3.8. MDAs MUST reuse and share information and data unless certain privacy or confidentiality restrictions apply.

3.5. Principle 5: Technological Neutrality and Data Portability

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

3.9. MDAs SHALL NOT impose any specific disproportionate technological solutions for citizens, businesses and other MDAs when establishing information systems and services.

3.10. 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. Data portability is a concept to protect users from having their data stored in "silos" or "walled gardens" that are incompatible with one another.[7] The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

3.11. MDAs MUST ensure that data is easily transferable between systems and applications.

[7] https://en.wikipedia.org/wiki/Data_portability

3.12. Information systems interfaces MUST be API-centric and created in a technology neutral way, using open standards and specifications (XML, WSDL, SOAP, REST, etc.). A Technical Interoperability Agreement[8] MUST be set up where the acceptable formats are specified.

3.6. Principle 6: User-Centricity

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

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

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

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

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

3.15. Citizen portal MUST act as single point of contact for public services. It is RECOMMENDED that multiple MDAs work together to provide aggregated services via the citizen portal. MDAs are encouraged to create their own portals.

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

3.16. User 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 Tongan public services SHOULD be put in place.

3.17. Data MUST be provided by users only once, and MDAs SHOULD be able to retrieve and share this data considering data protection rules and legislation.

3.18. An institution-based approach MUST be replaced with a user-based approach. Institutions MUST provide information at their own initiative.

3.7. Principle 7: Inclusion and Accessibility

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

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

Inclusion and accessibility MUST be part of the whole development lifecycle of Tongan public services in terms of design, information content and delivery. This should comply with e-accessibility specifications widely recognized 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 authorise another person to represent them. In this case representative can act on behalf of citizens who are unable, either permanently or temporarily, to use public services.

3.19. MDAs SHALL ensure that all public sector websites and public services are accessible to all citizens, including persons with disabilities and special needs.

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

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

3.8. Principle 8: Security

Citizens and businesses must be confident that when they interact with public authorities they are doing so in a secure and trustworthy environment and in full compliance with relevant regulations. MDAs 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 MDAs and other entities exchange official information, the information should be transferred, depending on security requirements, via a secure, harmonized, managed, and controlled network. Transfer mechanisms should facilitate information exchanges between MDAs, businesses, and citizens. Appropriate mechanisms should allow secure exchange of electronically verified messages, records, forms, and other kinds of information between the different systems; should handle specific security requirements and electronic identification and trust services such as electronic signatures/seals creation and verification; and should monitor traffic to detect intrusions, changes of data and other type of attacks.

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

3.22. Tonga SHOULD define a common security framework, adopt data protection legislation, and establish processes for public services to ensure secure and trustworthy data exchange between MDAs and in interactions with citizens and businesses.

3.23. Tongan information systems MUST guarantee confidentiality, integrity, authenticity, availability and provability of data and services.

3.9. Principle 9: Privacy

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

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

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

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

3.10. Principle 10: Administrative Simplification

Where possible, MDAs 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, MDAs should introduce services supported by electronic means, including their interactions with other MDAs, citizens, and businesses.

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

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

3.26. MDAs MUST simplify processes and use digital channels whenever appropriate for the delivery of public services, to respond promptly and with high quality to user requests and reduce the administrative burden on MDAs, businesses, and citizens.

3.11. Principle 11: Preservation of Information

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

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

3.27. Tonga MUST formulate a long-term preservation policy (digital archiving) for information in electronic form.

3.12. Principle 12: Assessment of Effectiveness and Efficiency

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

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

3.28. MDAs MUST evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits.

4. Interoperability Layers

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

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

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

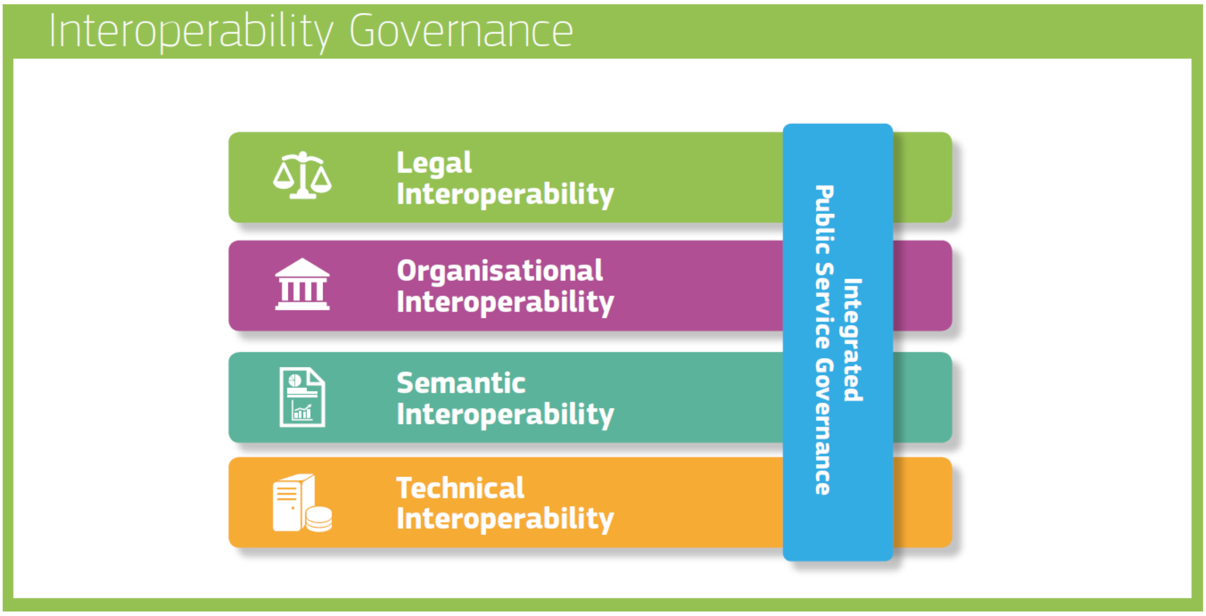
Interoperability Governance
Legal Interoperability
Organisational Interoperability
Semantic Interoperability
Technical Interoperability
Integrated Public Service Governance

Figure 1. Interoperability model (picture taken from EIF)

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.[9]

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

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

Barriers of interoperability governance. As information systems are constantly changing, it is necessary continuously improve the skills of IT personnel. The possible **lack of necessary in-house skill sets** is another barrier when implementing interoperability policies. Tonga 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 Tonga 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 MDAs at different levels (local, regional, national), coordination and monitoring require a holistic approach.

4.1. Interoperability Governance

4.1.1. Governance at the Interagency Level

Without interagency level intervention, systems do not become interoperable. To enable interoperability, technical requirements, standards, baseline solutions and tools must be implemented by a central competent authority. These artefacts must then be introduced to all existing and new projects to enable string interoperability between solutions.

By governance is appropriate to follow the principles of separation of powers: decisions (strategic), coordination (supervision), and implementation may be distributed into different institutions.[10]

Ministries, departments, other agencies and public bodies are responsible for business processes. They may choose and implement technologies by themselves, with respect to commonly agreed principles. Principles of information policies must be agreed and secured at higher level.

It is recommended to centralise development of policy and to decentralise its implementation. In the centralized level, the principles of information policies and supportive legislation will be developed, and the management and financing decisions will be made.

There is a need for **high level coordination of the e-government activities** between the various units of the government. Strategic and coordination bodies SHOULD have the legal rights and competence to take binding decisions.

All government institutions like to modernise their processes by using modern technology. The idea of the coordination is not to centralise all decision making and technical capacities.

[10] Ministry of MEIDECC currently performs both coordination and implementation functions.

On the contrary, the idea is to support innovation and service delivery modernisation in every government institution.

Coordination tools include policies, legislation and regulations, budgeting, monitoring, common standards, allowing nation-wide re-use of data, data exchange, re-use of software solutions and rapid development of online services.

Coordination of the planning process as well as using investments to ICT infrastructure and to avoid duplication and overinvestment.

Monitoring of the progress allows to understand the general advancement and benchmark it.

4.1. According to good governance principles it MAY be reasonable to separate the levels of decision making at the interagency level.

Example of organisational structure illustrated below Figure 2. Strategic, coordinating and implementation bodies are depicted in different shades.

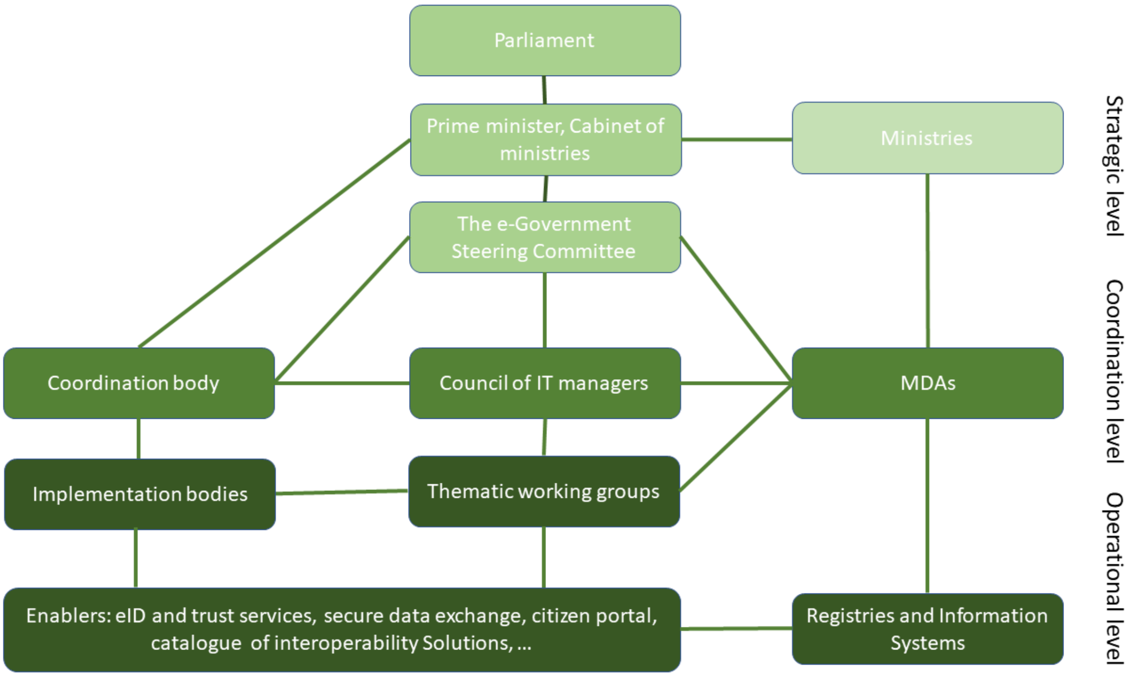
Parliament
Prime minister, Cabinet of ministries
Ministries
The e-Government Steering Committee
Coordination body
Council of IT managers
MDAs
Implementation bodies
Thematic working groups
Enablers: eID and trust services, secure data exchange, citizen portal, catalogue of interoperability Solutions, ...
Registries and Information Systems
Strategic level
Coordination level
Operational level

Figure 2 Recommended governance model

4.2. Interoperability MUST be maintained by the Coordination Body. Existing and planned registries must be designed to be interoperable with other solutions and registers.

The coordination body must collect and maintain information about existing and planned solutions and data services. Dedicated catalogue-type tools are recommended for implementing such capabilities. Such tools will define an authentic source for each dataset – the organisation primarily responsible for gathering, maintaining, and sharing (on a valid legal basis) data to other organisations. They will also define the status and importance of different registers as well as the dependency between those registers. Furthermore, the tools will allow aligning metadata with existing and upcoming legislation.

4.3. An overview of existing and planned solutions MUST be maintained by the Coordination Body.

Implementation of this requirement will have two outputs:

- Government knows its resources and has input to its management decisions.

- Metadata is published to ensure all organisations have the knowledge of what data structure is maintained in other organisations and which organisations are the authentic sources for specific data elements.

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

4.4. The Coordination Body SHALL ensure holistic governance of interoperability activities across administrative levels and sectors.

There should be clear roles, mandates, and responsibilities between the institutions.

The main Tongan e-Government actors are described below.

The Parliament and the Prime Minister are responsible for the approval of the principles, reflected in the document defining information policy. Only those institutions can secure the support for changes at the highest possible level with strategic decisions and monitor the implementation progress.

The e-Governance Steering Committee[11] shall be responsible for formulating strategic directions of e-government and ensuring effective implementation of decisions made by the Cabinet.

The Ministry of Finance (MOF) shall provide strategic support to MDAs and other stakeholders in the implementation of e-government policies.

The Ministry of MEIDECC shall coordinate, implement, and operate IT infrastructure services in Tonga. The Ministry of MEIDECC is responsible for building e-government enablers, such as the data centre, secure data exchange ecosystem, citizen portal, metadata management and other cross-government systems and services.

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

[11] Currently in the form of the Tonga Digital Government Support Project Steering Committee

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

4.5. It MAY be reasonable to centralise development of the policies and decentralise the implementation.

Other important external stakeholders:

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

Other community organisations and donors:

- International activities, stakeholders, donors, partners
- ADB
- World Bank
- Government of Australia
- Governments of Japan and China

4.1.2. Financing

For e-government development and operation, sustainable financing must be secured. The financing of Tongan e-government will be mainly organized by the government. The financing will be provided through annual budgeting within five-year budget cycles. Development of e-government is partially dependent on international donor funding. The main donor organisations supporting digital transformation in Tonga include World Bank, ADB, and the governments of Australia, Japan, and China. The MOF is responsible for coordinating activities with donors.

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) covers the development of cross-government IT systems from their investment budget (hardware, software).

- Operational costs (maintenance, support, further developments, etc.) are covered from the MDA budgets.

The Government of Tonga charges fees for some government services and business.

4.1.3. Standards and Specifications

The government adopts and draws up standards and specifications for government data and technology processes. The seven principles[12] that will be used for adopting and drawing standards by the Government of Tonga:

1. **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 aspects MUST be considered.
2. **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.
3. **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.
4. **Standards must support sustainable cost** - Decisions are based on the most economical solution for the public sector as a whole and costs are sustainable.
5. **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.
6. **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.
7. **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.

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

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

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

4.2. Governance at the Level of Public Bodies

Tonga service provision often requires different MDAs 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 with a mandate for planning, implementing and operating Tonga shared services. Services SHOULD be governed to ensure integration, seamless execution, reuse of services and data, and development of new services and **'building blocks'**.[13]

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

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

- the definition of organisational structures, roles and responsibilities, and the decision-making process for the stakeholders involved
- the imposition of requirements for:
    - aspects of interoperability including quality, scalability and availability of reusable building blocks including information sources (base registries, open data portals, etc.) and other interconnected services
    - external information/services, translated into clear service level agreements (including on interoperability)

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

- a change management plan, to define the procedures and processes needed to deal with and control changes
- a business continuity/disaster recovery plan to ensure that digital public services and their building blocks continue to work in a range of situations, e.g. cyberattacks or the failure of building blocks.

4.8. MDAs SHOULD ensure interoperability and coordination over time when operating and delivering integrated public services by putting the necessary governance structure in place.

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

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

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

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

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

4.9. MDAs SHOULD establish interoperability agreements at all layers, complemented by operational agreements and change management procedures.

4.3. Legal Interoperability

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

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

Coherence between legislation, in view of ensuring interoperability, SHOULD be assessed before adoption. The performance of legislation SHOULD be audited once they are put into application.

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

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

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

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

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

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

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

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

- Interoperability
- Electronic identification and electronic signature
- Databases/registries
- Archiving
- Access to information
- Information and Communications Technology (ICT)
- Public procurement and Public-Private-Partnership (PPP)
- Intellectual property
- Incentives for use of e-services
- Security and privacy

MDAs SHALL fulfil requirements existing e-government related legal acts. Important acts (as of 2020) related to interoperability include:

- Freedom of Information Act
- Tonga Telecommunications Commission Act. http://www.paclii.org/to/legis/consol_act/ttca385/
- Draft Electronic Transactions Act
- Communication Act. http://www.paclii.org/cgi-bin/sinodisp/to/legis/num_act/ca2015176/index.html?stem=&synonyms=&query=Electronic
- National Identity Card Act. http://www.paclii.org/cgi-bin/sinodisp/to/legis/num_act/nica2010219/nica2010219.html?stem=&synonyms=&query=identity%20card

4.4. Organisational Interoperability

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

Business Process Alignment

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

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

4.13. MDAs 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 Tonga public service.

Organisational Relationships

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

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

4.14. MDAs SHOULD clarify and formalize organisational relationships for establishing and operating public services.

4.5. Semantic Interoperability

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

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

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

4.15. MDAs SHOULD perceive data and information as a public asset that SHOULD be appropriately generated, collected, managed, shared, protected, and preserved.

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

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

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

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

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

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

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

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

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

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

4.20. Data standards SHALL be established and maintenance by owners of base registries and SHALL be published in the catalogue of information systems. Other MDAs SHALL follow these standards.

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

4.6. Technical Interoperability

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

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

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

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

4.21. MDAs SHOULD use open specifications, where available, to ensure technical interoperability when establishing public services.

Once-only principle. The proposed model[14] ensures the principle that information is supplied to information consumers only once from the authentic source responsible for handling the information and there is no other information source for the same information. According to the "once-only" principle, public bodies SHOULD take action to share data with each other, respecting privacy and data protection rules. This calls for a generic and scalable solution to interconnect different systems. Data is kept only in a database, where it serves as master data. Availability requirements MAY lead to the copying of data, but in this case, it must be considered that data MAY be outdated.

4.22. MDAs MUST use data from authentic sources and open their authentic data to others.

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

4.23. Technical solutions MUST support service-centred approach.

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

4.24. MDAs SHOULD separate front-end and back-end systems.

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

To help build a software solution, the Coordination Body SHALL develop common usable infrastructure services. MDAs SHALL use these instead of developing their own solutions.

4.25. MDAs SHALL use common infrastructure services established and administrated by the Coordination Body.

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

[14] The model is described in chapter 5.

without the need for the service-using system to “know” anything about the internal architecture, platform, etc. of the service-providing system. In case of SOA, the service publisher and the actual service provider do not necessarily have to be the same, while from the point of view of the service user, this does not make any difference. There are no restrictions as to technologies to be used for the application of SOA.

4.26. Data MUST be made accessible to registries through a security-enhanced service-oriented approach.

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

4.27. MDAs SHALL be able to aggregate data services.

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

4.28. Critical solutions SHOULD be hosted in a centralized cloud data centre.

The need to make data usable for several participants is common for most registers in a transforming society. The establishment of a secure data exchange solution/platform is one of the key elements to speed up successful digital transformation. While the finer details of such a platform must be locally identified and resolved, there are some properties of data exchange solution that are generic:

- Data must be exchanged between registered participants.
- Structure, semantics and authorizations must be controlled by the original data owner.
- Information security (availability, integrity, and confidentiality) must be ensured by the platform.

4.29. MDAs must use the Secure Data Exchange enabler maintained by the Coordination Body.

5. Conceptual Model for Integrated Public Service Provision

5.1. Introduction

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

5.1. MDAs 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.

MDAs need to identify, negotiate, and agree on a common approach to interconnecting service components. This will be done at different administrative levels according to the 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 MDAs, including common or compatible models, standards, and agreements on common infrastructure.

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

5.2. Model overview

The conceptual model promotes the idea of **interoperability by design**. It means that for Tonga 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 Tonga public services should reuse information and services that already exist and may be available from various sources inside or beyond the organisational boundaries of MDAs. Information and services should be retrievable and be made available in interoperable formats.

The basic components of the conceptual model are presented below.

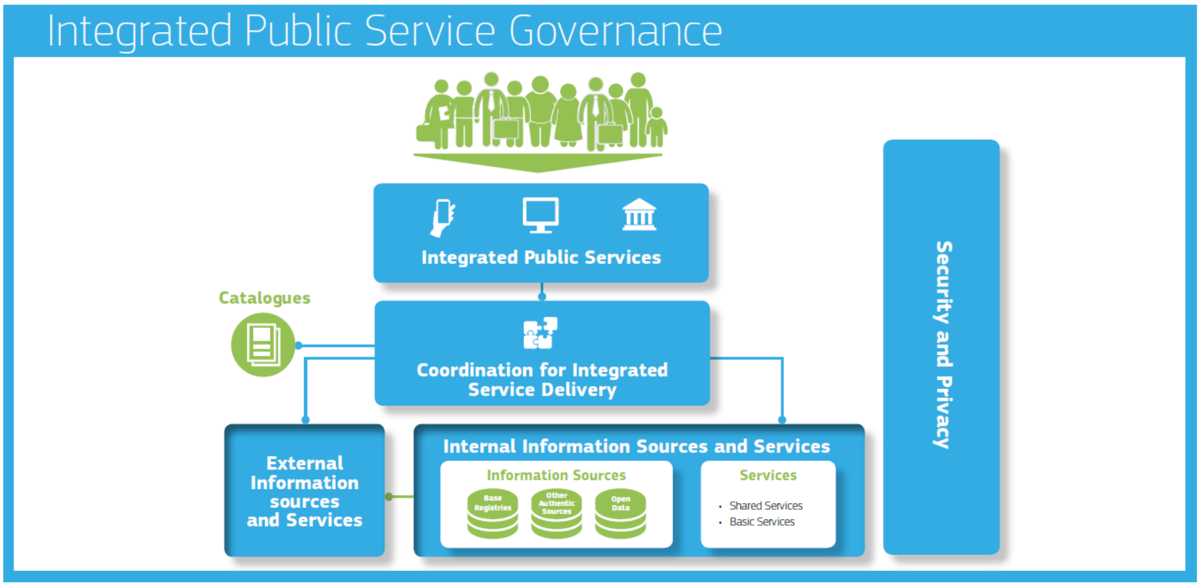
Integrated Public Service Governance
Integrated Public Services
Catalogues
Coordination for Integrated Service Delivery
External Information sources and Services
Internal Information Sources and Services
Information Sources
Base Registries
Other Authentic Sources
Open Data
Services
• Shared Services
• Basic Services
Security and Privacy

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

The model's structure comprises:

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

5.3. Coordination function

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

Process phases of integrated public service provision

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

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

5.4. Internal information sources and services

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

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

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

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

MDAs 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). For example, for the calculation of TAX data from different sources a set of services needed to get data from different sources. Results of these services are combined and then delivered as a whole to end users.

The reusable **building block** approach finds a suitable application by mapping solutions against the conceptual building blocks of a **reference architecture**[15] that allows reusable components to be detected, which also promotes rationalisation. The result of this mapping is a **cartography**[16] of solutions, including their building blocks that CAN be reused to serve common business needs and ensure interoperability.

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

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

5.5. Base Registries

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

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

[15] It is RECOMMENDED to develop interoperability architecture document for Tonga
[16] Ideas of the European cartography MAY be used: https://ec.europa.eu/isa2/solutions/eira_en

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

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

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

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

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

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

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

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

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

5.7. MDAs SHALL create and follow data quality assurance plans for base registries and related master data.

5.6. Open data

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

Tonga SHALL establish an Open Data policy/framework and update it regularly. Open data working group with the participation of the private sector, academy and civil society organisations SHOULD be established.

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

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

5.9. MDAs 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 standardized.

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

MDAs MAY use existing tools and frameworks such as the UNESCO "E-government toolkit for developing countries[17], ITU E-government framework[18] and European Union "Open Data Goldbook[19]" for open data activities.

5.7. Catalogues

Catalogues help others to find reusable resources (e.g. services, data, software, data models). Various types of catalogues exist, e.g. directories of services, libraries of software

[17] http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/e-government-toolkit-for-developing-countries/

[18] https://www.itu.int/ITU-D/cyb/app/docs/eGovernment%20toolkitFINAL.pdf

[19] https://data.europa.eu/sites/default/files/european_data_portal_-_open_data_goldbook.pdf

components, open data portals, registries of base registries, metadata catalogues, catalogues of standards, specifications, and guidelines. Commonly agreed descriptions of the services, data, registries, and interoperable solutions published in catalogues are needed to enable interoperability between catalogues.

5.11. The Coordination Body SHOULD put in place catalogues of public services, public data, and interoperability solutions and use common models for describing them.

5.8. External information sources and services

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

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

5.9. Security and privacy

Security and privacy are the primary concerns in the provision of public services. MDAs 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** 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**
- they are compliant with the legal requirements and obligations regarding the use of **electronic signatures** and **public key infrastructure** for authenticity and security

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. Unauthorized 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 MDAs data. This plan can mitigate threats against MDA, 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.

5.13. MDAs SHOULD consider the specific security and privacy requirements and identify measures foreseen by the National Information Security Framework (NISF) for the provision of each public service.

NISF MUST follow the ISO/IEC 27000 family security standards, and Tonga Enterprise Architecture Framework (TEAF) requirements.

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

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

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

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

- defining and applying security policies
- security training and awareness
- physical security (including access control)
- security in development

- security in operations (including security monitoring, incident handling, vulnerability management, cryptographic controls)
- security reviews (including audits, technical checks, and security testing).

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

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

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

5.15. MDAs SHOULD use trust services foreseen by the Coordination Body as mechanisms that ensure secure and protected data exchange in public services.

5.10. Government Cloud

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

5.16. MDAs SHOULD follow the requirements provided by the Coordination Body cloud policy.

6. Governance of the Interoperability Framework

TIF handles information systems from the point of view of the state as a whole. The maintenance of the TIF document will be done by the e-Government Steering Committee with the leadership of the Coordination Body.

6.1. The Strategic and Coordination bodies coordinate the initiatives relating to the interoperability of the state information system and MUST ensure the modern nature of the TIF. An interoperability architecture workgroup SHOULD be established.

Preparation of the interoperability framework and the related documents is supported by the Coordination Body in cooperation with the Strategic Bodies.

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

Compliance to the TIF will be an integral part of IT project funding reviews by the Coordination and strategic bodies. Any IT project by government organisations that is non-compliant with the TIF standards shall neither receive funding nor be sanctioned to proceed.

6.3. All IT projects SHALL be compliant with the TIF.

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

- Contribute to the continuous development and improvement of the TIF.
- Ensure that TIF compliance is a fundamental part of their organisational e-business and IT strategies
- Prepare a 'roadmap' for implementing the conformity with the TIF.
- 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 behind interoperability and can quickly respond to interoperability concerns in the respective government organisations.
- 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.

MDAs MUST analyse all the issues of interoperability in their organisations and are encouraged to compile their own interoperability framework (or similar) where principles and requirements are specified. These frameworks MUST be harmonized with the Tonga TIF.

6.4. MDAs are encouraged to set up their own frameworks that are harmonized with TONGA TIF.

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

7. Abbreviations

Abbreviation	Meaning
G2G	Administration to administration
G2B	Administration to business
G2C	Administration to Citizen
TIF	Tongan e-Government Interoperability Framework
EIF	European Interoperability Framework
ICT	Information and communication technology
IT	Information Technology
MDA	Ministries, Departments, and Agencies
MEIDECC	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Climate Change and Communications
MOF	Ministry of Finance
MoU	Memorandum of Understanding
SLA	Service Level Agreement
SOA	Service Oriented Architecture
TDGSF	Tonga Digital Government Strategic Framework
TEAF	The Enterprise Architecture Framework Tonga (TEAF)
TIF	Tonga Interoperability Framework
TOGAF	The Open Group Architecture Framework
TSDF	Tongan Strategic Development Framework 2015-2025

8. Glossary

Term	Definition
Aggregated Public Services	A generic term used in the conceptual model for public services to refer to a set of basic public services accessed in a secure and controlled way before being combined and then delivered as a whole to end users.
Authentic (or Authoritative) Source	An authentic source is information that is stored only once and which is believed to be correct, so can serve as a basis for reuse.
Base registry	A base registry is a trusted and authoritative source of information, which CAN and SHOULD be digitally reused by others, where one organisation is responsible and accountable for the collection, use, updating and preservation of information.
Building block approach	An approach to building information systems from architecture to implementation in which the information system is designed as an assembly or aggregation of components that encapsulate data and functionalities in groups that can also be reused as 'building blocks' to build other public services or information systems.
Business Process	A business process is a sequence of linked activities that creates value by turning inputs into a more valuable output. This can be performed by human participants or ICT systems, or both.
Data Controller	Person, who alone, jointly with other persons or in common with other persons or as statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.
Data Processor	Data processor in relation to personal data, means a person other than employee of the data controller who processes the data on behalf of the data controller.
Data Repository	Any collection of data meant for use (processing, storage, querying, etc.) by an information system. Typically, a data repository contains additional structural and semantic information about the data in question, designed to aid the use of the data (data model, relationships between data elements, metadata, etc.). It may provide specific functionalities closely tied to the data stored in the repository (searching, indexing, etc.).
E-government	E-government 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 authorized 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

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

	some other value-added function or service. Orchestration is closely related to the concept of workflow. Usually, orchestration involves executing a set of processes, described in a standard language, by an 'orchestration engine', which is configurable and capable of executing all the requisite service calls and routing the inputs and outputs of processes according to rules described in that language.
Organisational Interoperability	Ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together
Public Data	Public data is information that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.
Public Service	Service can be: A repeatable activity: a discrete behaviour that a component of organisation may be requested or otherwise triggered to perform. An element of behaviour that provides specific functionality in response to requests from actors or other services.
Reusability	The degree to which a software module or other work product can be used in contexts other than its original, intended or main purpose.
Secure Data Exchange	This is a component of the conceptual model for public services. Its aim is to ensure that all data exchanges are done in a secure and controlled way.
Semantic interoperability	Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'.
Semantic Interoperability Assets	Semantic interoperability assets are a subset of interoperability assets and include any element of the semantic layer, such as nomenclatures, thesauri, dictionaries, ontologies, mapping-tables, mapping-rules, service descriptions, categories, and web services.
Service Level Agreement	A formalized 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 recognized standardization body for repeated or continuous application, with which compliance is not compulsory
Taxonomy	A taxonomy represents a classification of the standardized terminology for all terms used within a knowledge domain. In a taxonomy, all elements are grouped and categorized 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
Tonga Interoperability Framework (TIF)	The agreed approach to the delivery of Tonga 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.