Tonga Enterprise Architecture Framework (TEAF)

Project: Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure

Version 1.0
28 April 2022

Change history

Version	Date	Summary of changes
1.0	28 April 2022	First version for approval

Document status

Draft	
For approval	
Approved	X

Authors

Name	Role
Dr Uuno Vallner	Enterprise architect

Table of Contents

Abbreviations

Abbreviation	Meaning
ABB	Architecture Building Block
ADM	Architecture Development Method
CR	Civil Registry
eID	Electronic Identification
G2G	Administration to administration
G2B	Administration to business
G2C	Administration to Citizen
GoT	Government of Tonga
TIF	Tongan e-Government Interoperability Framework
EIRA	European Interoperability Reference Architecture
ICT	Information and communication technology
IT	Information Technology
MDA	Ministries, Departments, and Agencies
MOF	Ministry of Finance
MoU	Memorandum of Understanding
NCRO	National Civil Registry Office
NICO	National Identity Card Office
NID	National ID
PKI	Public Key Infrastructure
PMO	Prime Minister Office
PSC	Point of Single Contact
RGO	Registrar-General's Office
SDE	Secure Data Exchange
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

1. Introduction

1.1. Background

The Tonga Enterprise Architecture Framework (TEAF) supports the vision "A more progressive Tonga supporting higher quality of life for all" and the goals of the Government of Tonga (GoT) as fixed in the Tongan Strategic Development Framework 2015-2025 (TSDF).[1] 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, and holistic (whole-of-government) approach.

The Tonga Interoperability Framework (TIF)[2] 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.

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

This document is a reference architecture, focused on the design of end-to-end interoperable digital public services. The TEAF is composed of the salient Architecture Building Blocks (ABBs) needed to promote cross-sector interactions between the Tongan Ministries, Departments, and Agencies (MDAs). The document provides the necessary policy and technical recommendations for its sustainable and systematic implementation.

The TEAF provides a **common terminology** that can be used by people working for public administrations in various architecture and system development tasks.

---

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

[2] Tonga Interoperability Framework (TIF).

Alignment with TIF and TOGAF. TEAF is aligned with the Tonga Interoperability Framework (TIF) The views of TEAF correspond to the interoperability levels in the TIF: legal, organisational, semantic, and technical. TEAF reuses terminology and paradigms from TOGAF® such as architecture building blocks and views. This not only assures a high level of quality but also allows architects to easily understand the TEAF and relate it to existing work.

The reference architecture targets the following users within the MDAs:

- **Architects**, Enterprise Architects as well as Solution Architects who are responsible for the design of solution architectures,
- **Business analysts** responsible for assessing and studying the impact of changes in the (external) environment on IT systems,
- **Portfolio managers** responsible for maintaining of assets related to the design and implementation of e-government solutions and for making investment decisions on these assets.

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

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

1.2. Methodology: frameworks, standards, tools

In this section we list and shortly describe the main frameworks, standards and tools that have been applied to build TEAF:

- Tonga Interoperability Framework (TIF),
- Open Group Architecture Framework (TOGAF©),
- Architecture Development Method (ADM),
- Enterprise Architecture Modelling Language ArchiMate®,
- Archi®, a modelling toolkit for creating ArchiMate models and sketches,
- European Interoperability Reference Architecture (EIRA©)

TIF.[3] The Tonga Interoperability Framework (TIF) is the agreed approach to the delivery of the Government of Tonga public services in an interoperable manner. It defines the basic interoperability guidelines in the form of common principles, models, and recommendations. TEAF is aligned with TIF.

[3] Ibid, 2

TOGAF®.[4] The Enterprise Architecture framework TOGAF® is used by the Government of Tonga for developing the Tonga Enterprise Architecture Framework (TEAF). TOGAF is a generic framework. The TOGAF standard considers an "enterprise" to be any collection of organizations that have common goals.

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

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

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

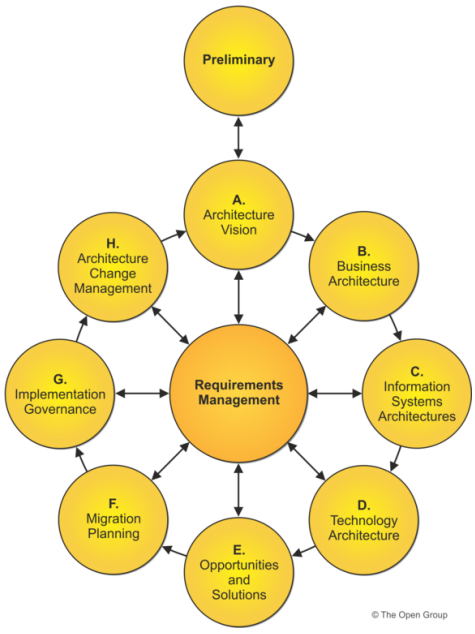

Figure 1 Basic structure of the ADM

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

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

The basic structure of the TOGAF ADM is shown in Figure 1. Throughout the TOGAF ADM cycle, there needs to be frequent validation of outputs against original expectations, both those from the whole TOGAF ADM cycle, and those from the particular phases of the method.

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

[4] https://pubs.opengroup.org/architecture/togaf9-doc/arch/

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

ArchiMate®.[5] The ArchiMate® modelling language is an open and independent Enterprise Architecture standard that supports the description, analysis, and visualisation of architecture within and across business domains. ArchiMate is one of the open standards hosted by The Open Group® and is fully aligned with TOGAF®. ArchiMate® aids stakeholders in assessing the impact of design choices and changes. All views and viewpoints of TEAF are visualised by using the ArchiMate® language.

ArchiMate 3.1 Notation Overview is presented in Figure 2.

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

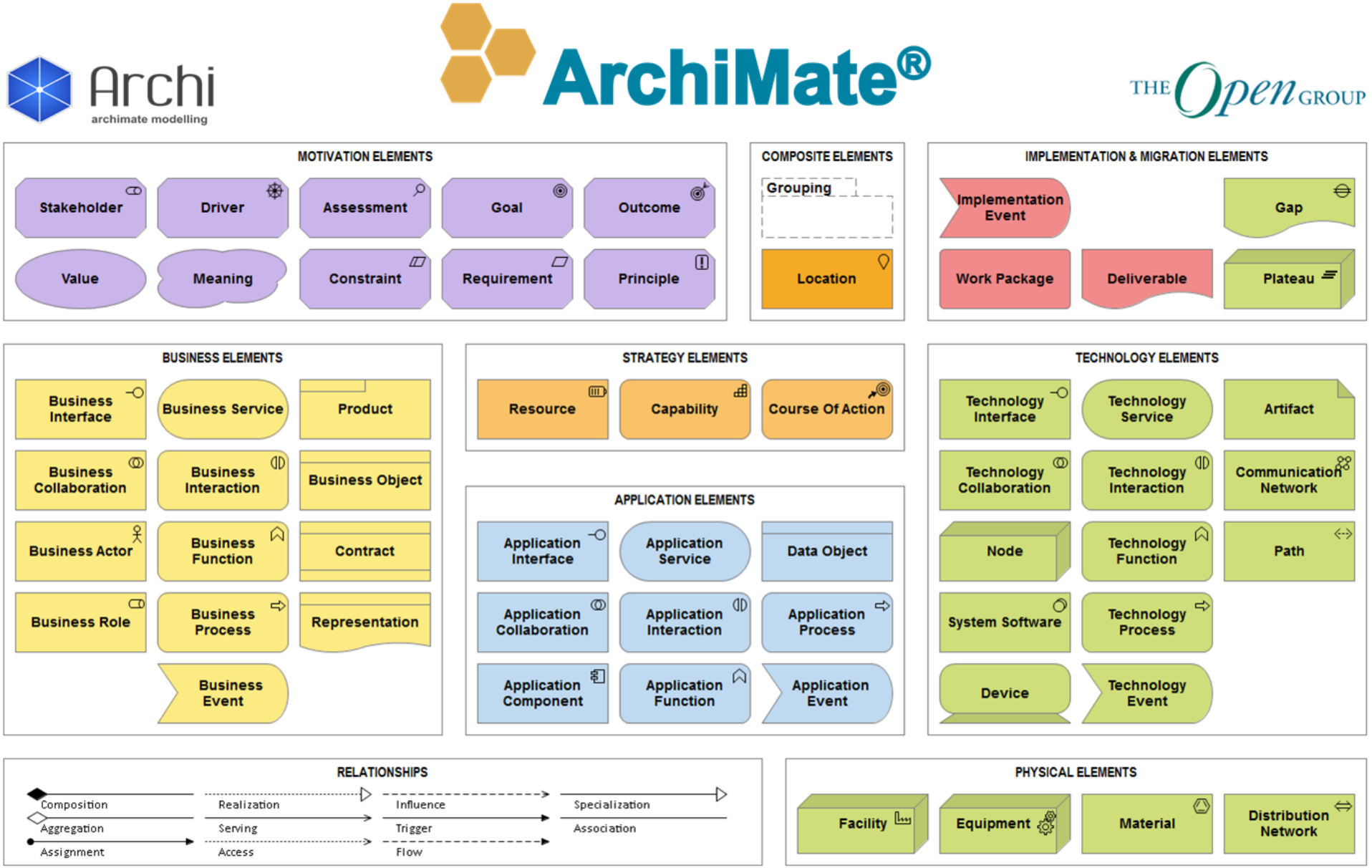

Figure 2 ArchiMate notation

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

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

1.3. Context

Tonga Enterprise Architecture Framework (TEAF) describes 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 (Figure 3):

1. **Strategy of building an information society**. The strategy is fixed in vision papers.
2. **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.
3. **Tonga Enterprise 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 the MDAs.

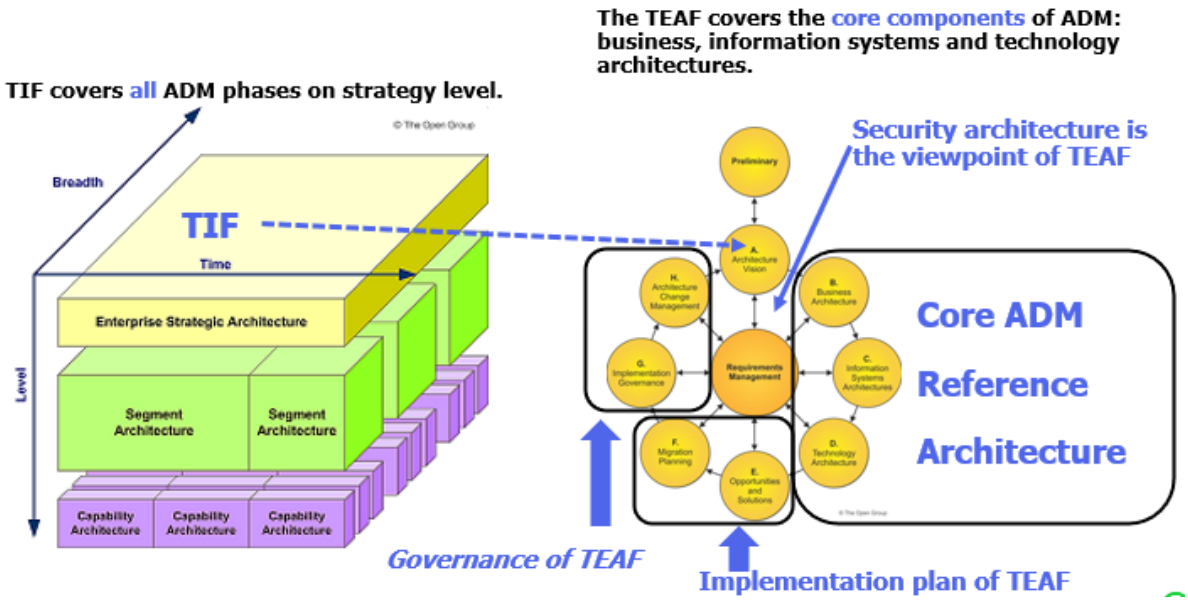

Figure 3 TIF covers all ADM phases on strategy level. The TEAF covers the core components of ADM: business, information systems and technology architectures.

4. **Implementation plan 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.
5. **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.

1.4. Key concepts and key enablers of TEAF

The Key Interoperability Enablers viewpoint in Figure 4 models the key interoperability enablers. Government of Tonga (GoT) public service provision often requires different MDAs to work together to meet end users' needs and provide public services in an integrated way. When multiple organizations are involved, there is a need for coordination and governance by the authorities with a mandate for planning, implementing and operating public services. Services should be governed to ensure:

- collaboration
- seamless execution
- reuse of services and data
- and development of new services and building blocks.

The Key Interoperability Enablers viewpoint covers all TIF interoperability aspects: legal, organizational, semantic, and technical. Ensuring interoperability when preparing legal instruments, organization's business processes, data/information/knowledge exchange, services and components that support GoT interoperable digital public services is a continuous task, as interoperability is regularly disrupted by changes to the environment, i.e. in legislation, the needs of businesses or citizens, the organizational structure of public administrations, the business processes, and by the emergence of new technologies.

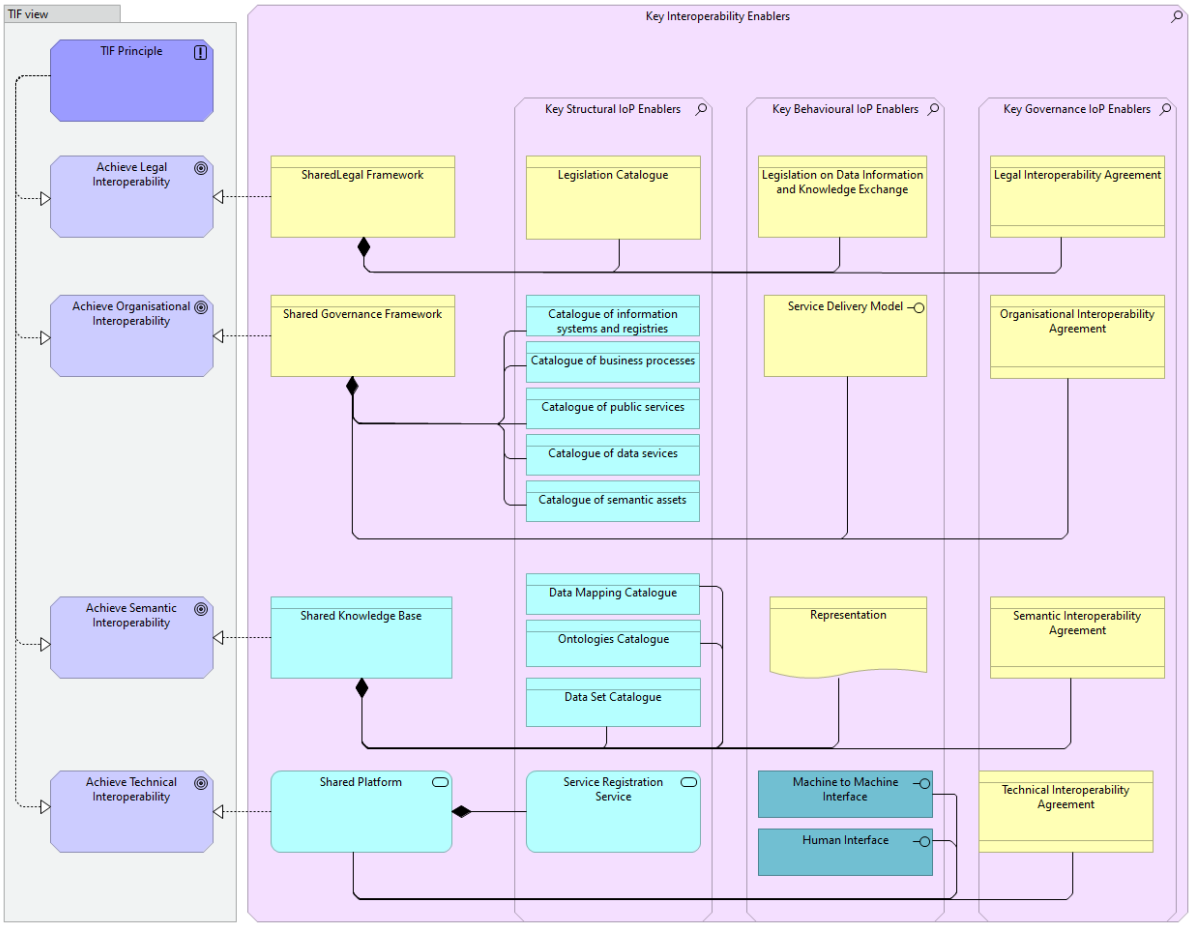

Figure 4 Key enablers of TEAF

The key concepts of TEAF are defined as follows:

TIF interoperability level. TIF is a set of guidelines for developing public services. Figure 4 depicts the interoperability levels of TIF. They cover legal, organizational, semantic, and technical interoperability. Each level deserves special attention when a new GoT public service is established.

TIF principle. TIF outlines 12 underlying principles of GoT public services. These general principles of good administration are relevant to the process of establishing GoT public services. They describe the context in which GoT public services are decided and implemented. They complement one another regardless of their different natures, e.g. legal or technical. More information on the TIF interoperability levels and principles can be found in the GoT Interoperability Framework (TIF).

TEAF view. TEAF consists of several views, including one view for each of the TIF interoperability levels. TEAF views contain a graphical notation of the TEAF ontology.

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

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

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

Reference Architecture. Architecture is the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. A reference architecture is a generalized architecture of a solution, based on best practices, domain neutral and, occasionally, with a focus on a particular aspect. The goal of a reference architecture is reusability; it reduces the amount of work, reduces errors and accelerates the development of solutions. A reference architecture is based in a reference model and in a style. The model covers the ontology of the components and their interrelationships and in the case of TEAF it is ArchiMate®. The architecture style covers the architecture design principles and patterns and in the case of the TEAF it is "Service Oriented Architecture" (SOA). The focus of the TEAF is interoperability in GoT institutions. This definition of "reference architecture" needs to be complemented with the notion of Enterprise Architecture, which is an end-to-end generic domain neutral approach to design the architecture of an enterprise or a solution. The goal of an enterprise architecture is to align IT-related activities with the overall goal of the enterprise.

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

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

1.5. TEAF Ontology viewpoint

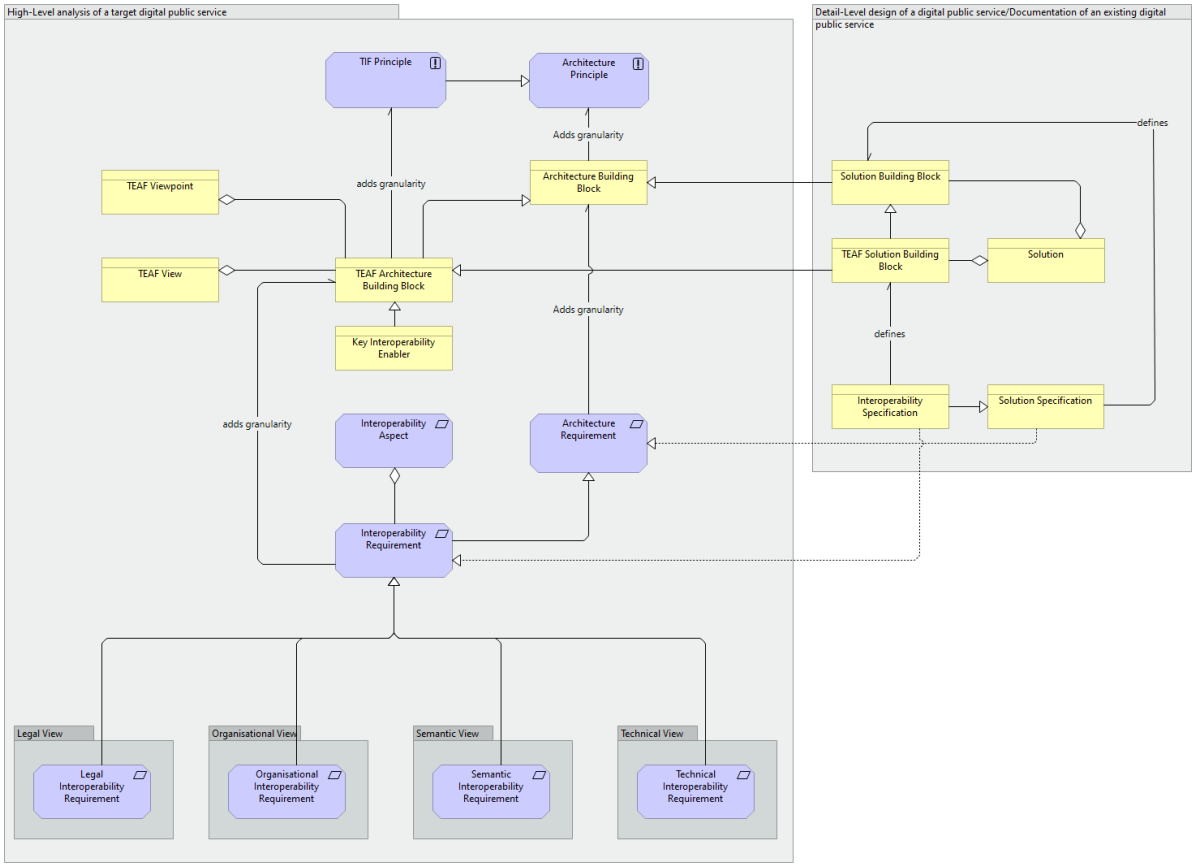

Figure 5 Ontology viewpoint of TEAF

The following list explains the different relationships between the key concepts of TEAF depicted in Figure 5:

- The TEAF has TEAF views, each TEAF view aligns with one or more TIF Interoperability Levels
- Each TEAF view has TEAF Architecture Building Blocks
- The TEAF has TEAF Viewpoints that conform to TEAF Views
- A TEAF Architecture Building Block is modelled as a specialisation of a TOGAF® Architecture Building Block
- A Key Interoperability Enabler is a TEAF Architecture Building Block, which is necessary to enable the efficient and effective delivery of public services across MDAs.
- A TEAF Architecture Building Block has interoperability requirements. An Interoperability Requirement is a statement of an interoperable need that must be realised by a system. Interoperability Requirements can be formulated for all the TIF interoperability levels:
    - Legal Interoperability Requirements,
    - Organisational Interoperability Requirements,
    - Semantic Interoperability Requirements, and
    - Technical Interoperability Requirements.
- Interoperability requirements are grouped in Interoperability Aspects. An Interoperability Aspect is an externally observable characteristic or a set of

characteristics to be provided/supported by the solution that partially or entirely fulfils a stakeholder's interoperability need.
- An Interoperability Specification is a document containing agreed normative statements for solution building blocks used in an information exchange context. It can refer to existing standards or specifications. An Interoperability Specification realises an Interoperability Requirement.
- A TEAF Solution Building Block is a realisation of an EIRA© Architecture Building Block and a specialization of a TOGAF® Solution Building Block.
- A Solution consists of TEAF Solution Building Blocks and TOGAF® Solution Building Blocks.

1.6. Benefits

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

- Providing a controlled vocabulary
- Decoupling functionalities in Architectural Building Blocks
- Facilitating the identification of Interoperability Specifications
- Providing the key interoperability enabler Architectural Building Blocks
- Accelerating the development cycle
- Supporting portfolio management decision making
- Supporting public policy formulation

1.6.1. Providing a controlled vocabulary

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

1.6.2. Decoupling functionalities in Architectural Building Blocks

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

1.6.3. Facilitating the identification of Interoperability Specifications

TEAF allows stakeholders/MDAs to effectively communicate with other MDAs when systems across organizational borders must interoperate. TEAF facilitates the identification of interoperability specifications and promotes the use of common interoperability specifications based on open standards.

Architects and system owners can then rely on these interoperability specifications to ensure:

- stable interfaces between their systems/services and others inside and outside their own organizations, and
- interfaces towards users that consider non-technical interoperability aspects like usability, inclusiveness, and multilingualism.

Public procurers benefit from an easy way to discover relevant specifications for specific types of solutions, and avoid vendor lock-in.

1.6.4. Accelerating the development cycle

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

1.6.5. Supporting portfolio management decision making

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

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

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

1.6.6. Supporting public policy formulation

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

- legislative proposals,
- non-legislative proposals such as financial plans and recommendations for the negotiations of agreements),
- implementing and delegating acts.

1.7. Scope and structure

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

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

- Permanent Secretaries
- Chief Executive Officers (CEO)
- Chief Financial Officers (CFO)
- Chief Information Security Officers (CISO)
- Chief Information Officers (CIO)
- Chief Technology Officer (CTO)
- Chief Operations Officers (COO).

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

- **Architects**. Both enterprise architects as well as solution architects who are responsible for the design of solution architectures
- **Business analysts** responsible for assessing and studying the impact of changes in the (external) environment on IT systems
- **Portfolio managers** responsible for maintaining of assets related to the design and implementation of e-government solutions and for making investment decisions on these assets.

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

TEAF is oriented to the development of a GoT 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.

The TEAF 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.

It must be noted that TEAF can also be used for B2B (business to business) and B2C (business to citizens) interactions.

The TEAF content and structure is presented below:

Chapter 1 provides an overview of TEAF. It includes background information, methodology, context in building TEAF, key concept, ontology, and benefits.

Chapter 2 provides a vision for the GoT enterprise architecture development lifecycle.

Chapter 3 provides the legal reference architecture. It includes a description of crucial components for the implementation of the legal view.

Chapter 4 provides the business reference architecture. It includes the description of crucial components for the implementation of the organisational view.

Chapter 5 provides data reference architecture. It includes description of crucial components for the implementation of the data view.

Chapter 6 provides application and technical reference architecture. It includes description of crucial components for the application and technical view.

Chapter 7 gives viewpoint to the security architecture.

Chapter 8 describes the governance of TEAF.

Chapter 9 lists and describes the TEAF architecture building blocks.

2. The Architecture Vision

2.1. Architecture Principles View

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

TEAF is aligned with the GoT Interoperability Framework (TIF). The views of TEAF correspond to the interoperability levels in TIF: legal, organisational, semantic, and technical interoperability. TEAF reuses terminology and paradigms from TOGAF®, such as architecture patterns, building blocks, and views.

Five types of architecture principles are distinguished:

- TIF underlying principles
- Digital Public Service Strategy
- Digital Public Service Design
- Digital Public Service Operations
- Improvement

The architecture principles view is depicted in Figure 6.

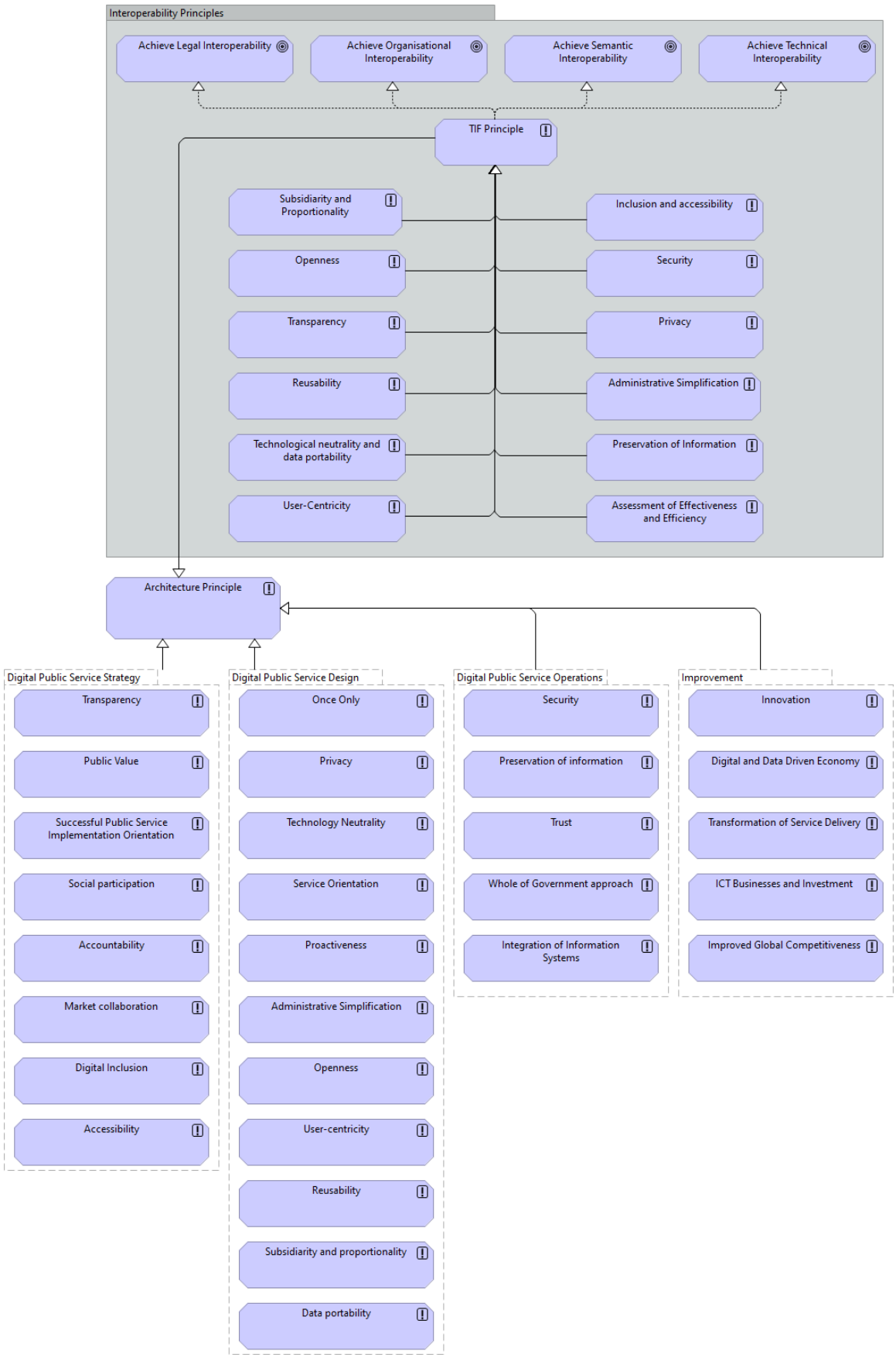

Figure 6 Architecture principles view

2.2. Conceptual model viewpoint

The GoT TIF 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. TEAF is aligned with the TIF conceptual model. This model in terms of ArchiMate is depicted in.

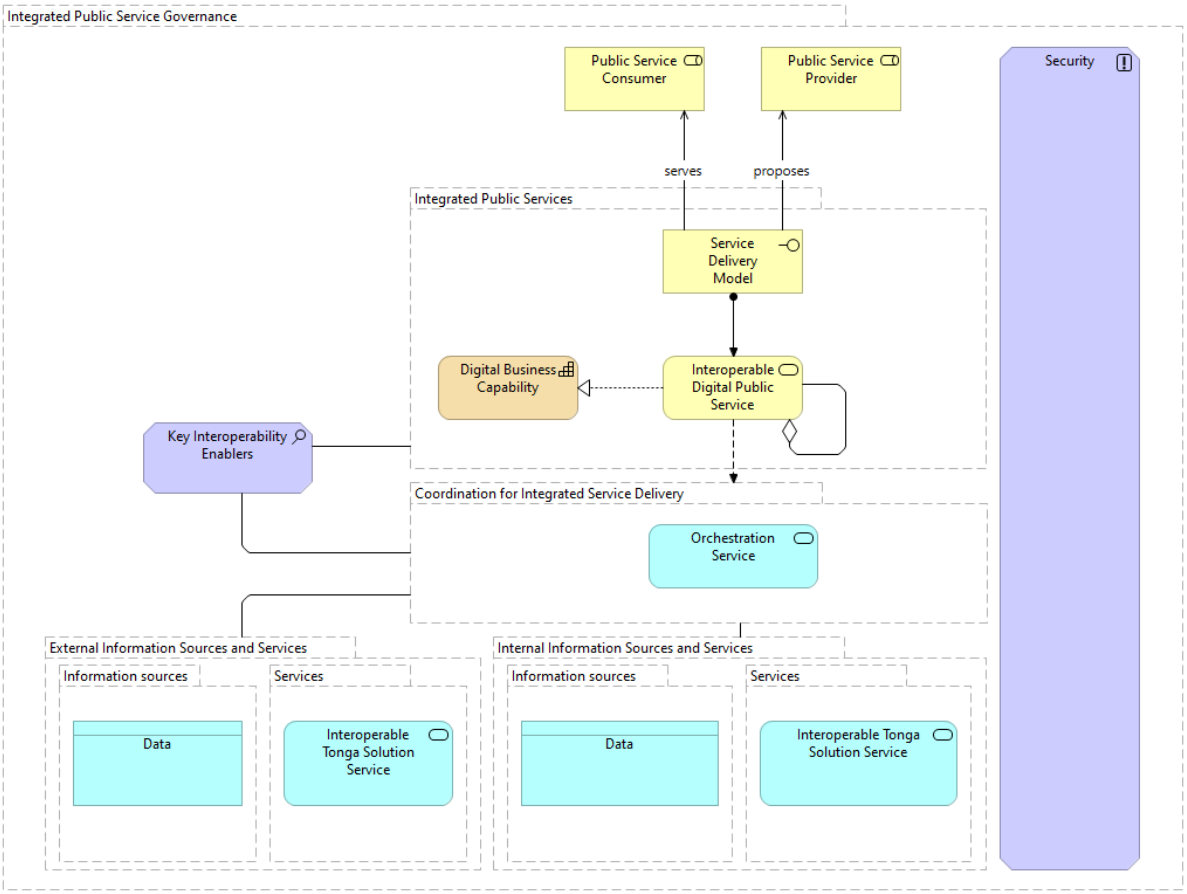

Figure 7 Conceptual model for integrated public services

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

2.3. High level viewpoint

The high-level viewpoint of Tonga interoperability architecture is depicted in Figure 8. TEAF provides a set of Architecture Building Blocks, important to facilitate the interoperability of any

GoT solution. Each view is represented by the Architecture Building Blocks needed to deliver an interoperable solution.

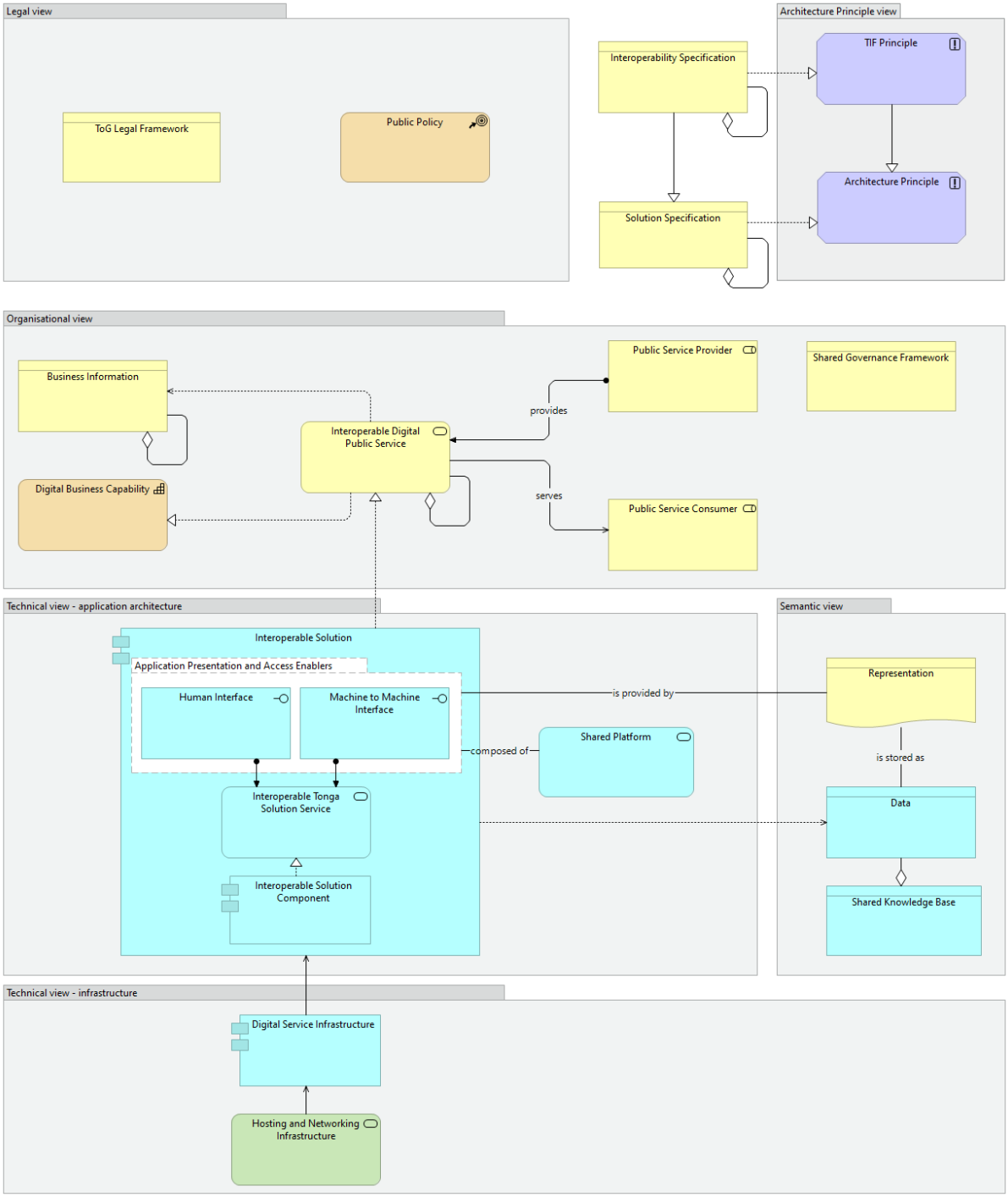

Figure 8 High level viewpoint

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

- **The Architecture Principle view.** The Architecture Principle view shows that Interoperability Specifications realize ABB Interoperability Principles. The Interoperability Specifications can be used to define the interoperability aspects for any other of the Architecture Building Blocks.

- **The Legal view.** The Legal view models the most salient public policy development enablers and implementation instruments that shall be considered to support the End-to-End design of interoperable digital public services.
- **The Organisational view**. A Public Service can be an aggregation of other Public Services serving Consumers and is provided by a Service Provider. The Public Service is realized by a Business Capability, which can be an aggregation of other Business Capabilities.
- **The Semantic view**. The Semantic view models the most salient Architecture Building Blocks that should be considered to support semantic aspects for the End-to-End design of interoperable digital public services.
- **The Technical - Application view.** The application view contains the most salient application Architecture Building Blocks that need to be considered to support technical aspects for the end-to-end design of Interoperable GoT Solutions.
- **The Technical -Infrastructure view.** The Technical -Infrastructure view provides an architecture content metamodel for the most salient cross-sectorial infrastructure services, along with the supporting hosting and networking facilities, which shall be considered in order to support technical aspects for the end-to-end design of interoperable GoT solutions. The difference with the application part of the technical view is that the Architecture Building Blocks in the infrastructure view are considered to be relevant to solutions in any sector of the government.

3. Legal interoperability architecture

3.1. Current view

The Legal view models the most salient public policy development enablers and implementation instruments that shall be considered to support the end-to-end design of interoperable digital public services.

Each MDA contributing to the provision of a Tongan 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 Tongan 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.

MDAs shall fulfil requirements of existing e-government related legal acts. Important legal acts related to interoperability currently 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

3.2. Crucial components of the target legal interoperability architecture

Tonga has a legal framework for e-governance in place, but continuous improving and amendment of it is needed. The TEAF implementation strategy for achieving legal interoperability is formulated by the TIF. The most crucial components are explained below.

3.2.1. Review of legislation processes

All new legislation should be reviewed/checked before approval looking at the following aspects:

- Digitalization
- Data protection
- Interoperability

The review should be carried out by MDAs and by a Coordination body as depicted in Figure 9.

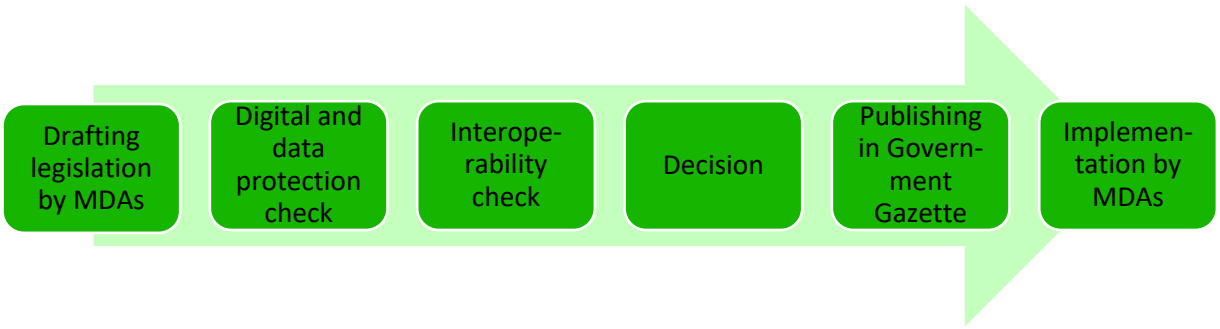

Figure 9 Legislation review process

3.2.1.1. Digital check

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

Bearing in mind that Tongan public services are clearly meant to be provided also via digital channels, ICT must be considered as early as possible in the law-making process.

The 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 also facilitate interoperability between public services at lower levels (semantic and technical) and increase the potential for reusing existing ICT solutions, thereby reducing cost and implementation time.

3.2.1.2. Interoperability check

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

Coherence between legislation, in view of ensuring interoperability, should be assessed before adoption. The performance of legislation should be audited once it is applied.

3.2.2. Catalogue of legislation

The catalogue of legislation should be redesigned adding a machine readable form (XML) for legal acts, improving/creating metadata for legal acts, improving search and navigation, etc.

3.2.3. Improvement of 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

4. Organisational interoperability architecture

4.1. Current view

Organisational Architecture 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.

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.

Governance allows following the principles of separation of powers: decision-making (strategic), coordination (supervision), and implementation may be allocated to different institutions.[6]

The proposed organisational structure is illustrated below in Figure 10 Strategic, coordinating and implementation bodies are depicted in different shades.

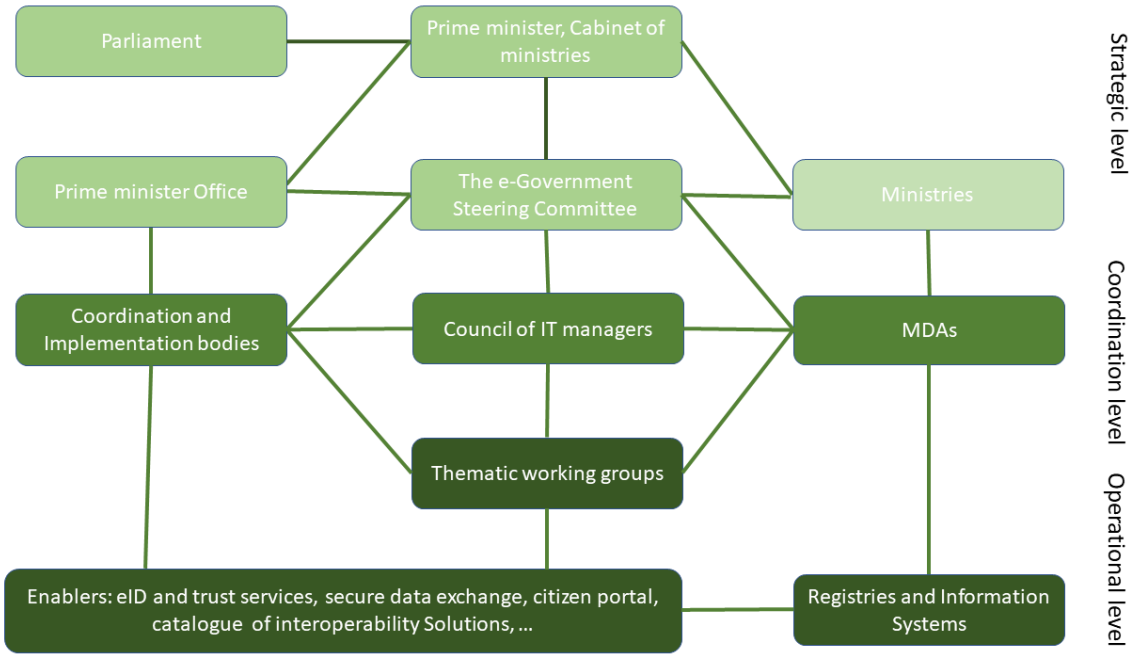

Figure 10 Proposed governance model

[6] Currently the PMO performs strategic functions and the Digital Transformation Department at the PMO performs both coordination and implementation functions.

4.2. TEAF Organisational View

The GoT 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 government gives enough priority and assigns resources to their respective interoperability efforts.

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

Figure 11illustrates the most important ABBs of organisational architecture.

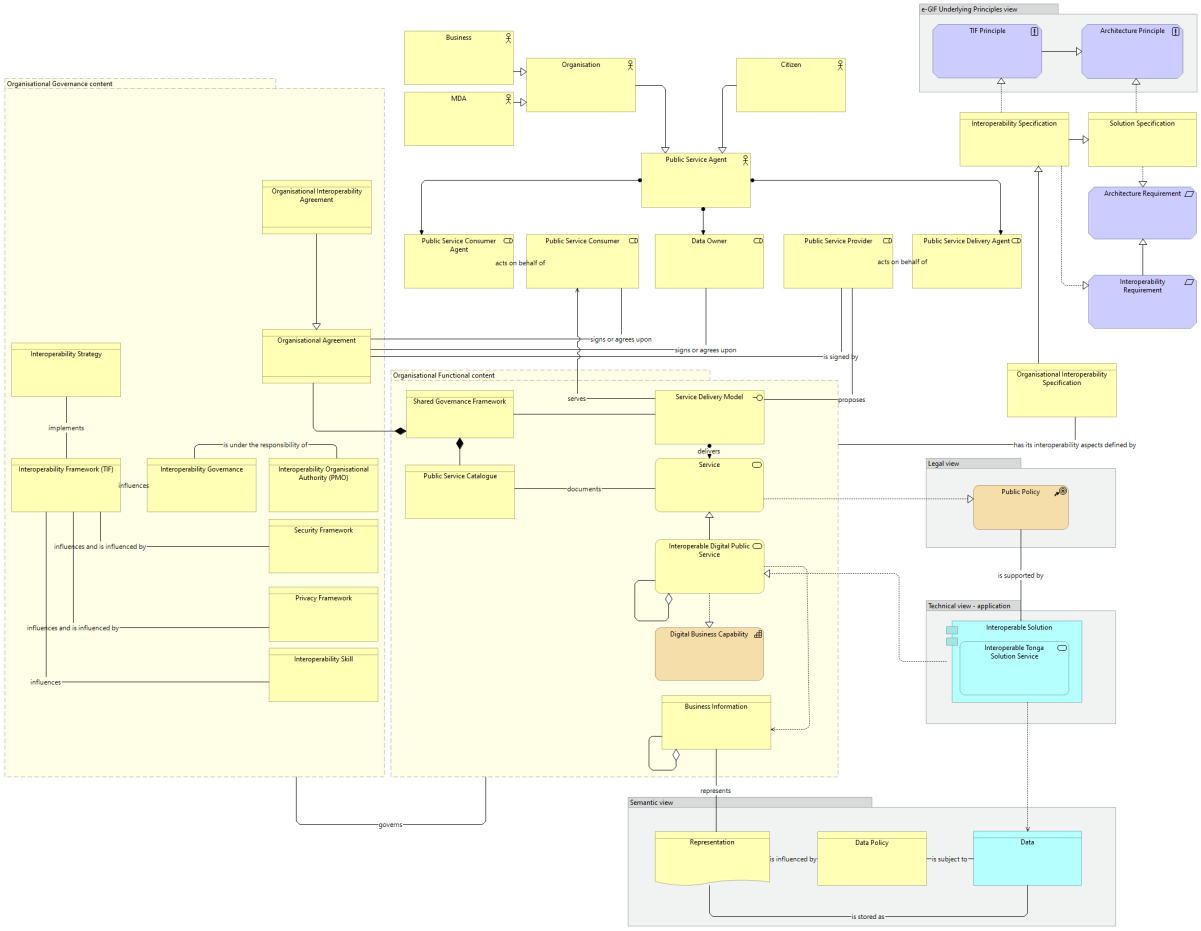

Figure 11 TEAF organizational view

4.3. Crucial Components of the Target Organisational Interoperability Architecture

4.3.1. 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.

MDAs should document business processes using commonly accepted modelling techniques (such as BPMN, UML, ArchiMate, Gantt charts, LEAN, etc.) and agree on how these processes should be aligned to deliver a Tonga public service as proposed by the Business Process Management report[7].

4.3.2. Interoperability Skills

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

4.3.3. Supervision of Information Systems

Create capability for supervision of information systems. Establish the supporting instruments (described in 6.3.1) for describing information systems, public services, data services and semantic assets. Improve the interoperability of new IT projects through coordinated use of centrally developed common infrastructure services and open standards. improve the coordination and management of state information systems and to accelerate the development of IT solutions.

4.3.4. Modernisation of PSC

Point of Single Contact (PSC) is an e-government portal that allows service consumers to get the information they need and complete administrative procedures online. The Tongan PSC is a one-stop online centre for government online services. Its main objective is to enhance government service delivery to citizens, non-citizens, businesses and to Government Ministries, Departments and Agencies (MDAs). The benefits include making government services more accessible, reducing access cost and queueing at Government offices, transparency, timeliness and increasing convenience of transaction with the Government of Tonga anytime and from anywhere.

ABBs for the PSC are described in detail in section 6.3.2.

---

[7] Report: Business Process Management. Contract number: TO-MFNP-128799-CS-CQS

4.3.5. Creating organisational capacity for building and management eID and PKI ecosystem

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

ABBs for eID and PKI are described in section 6.3.4.

4.3.6. Creating organisational capacity for building and managing the secure data ecosystem

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

The architecture of the secure data exchange ecosystem is described in the Tongan Data Exchange Policy and Framework[8] and in section 6.3.5.

4.3.7. Creating Organisational Capacity for Building and Managing the Data Centre and Government Cloud

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

The architecture of these components is described in a dedicated report[9] and in section 6.3.6.

4.3.8. Modernisation of Open Data Ecosystem

Public bodies should publish open data in machine-readable, non-proprietary formats. They should ensure that open data is accompanied by high quality, machine-readable metadata in non-proprietary formats, including a description of their content, the way data is collected and its level of quality and the license terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.

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

---

[8] Tongan Data Exchange Policy and Framework. Project: Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure. Contract number: TO-MFNP-128799-CS-CQS

[9] Tonga Cloud First Policy. Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure. Contract number: TO-MFNP-128799-CS-CQS

5. Data architecture

5.1. Current view

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

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

The main characteristics of baseline data architecture:

1. A significant number of Government registries and services are not digitalised.
2. Semantic interoperability requirements formulated in the TIF await implementation.
3. A catalogue of registries does not exist.
4. A catalogue of public services does not exist.
5. A catalogue of data services does not exist.
6. Data sharing is organised in an *ad hoc* manner.
7. Data policy, base registry policy, reference data policy formulated in the TIF await implementation

5.2. Crucial components of the target data interoperability architecture

5.2.1. Digitisation, digitalisation, digital government

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

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

Digital government refers to the use of digital technologies, as an integrated part of governments' modernisation strategies, to create public value. It relies on a digital government ecosystem comprised of government actors, non-governmental organisations, businesses, citizens' associations, and individuals, which supports the production of and access

to data, services, and content through interactions with the government.[10] Implementation of TEAF supports creating a digital government.

5.2.2. Catalogues

Data about data (metadata) must be properly managed and made publicly available. Catalogues help others to find reusable resources (e.g. services, data, software, data models). Various types of catalogues exist, e.g. directories of services, libraries of software components, open data portals, registries of base registries, metadata catalogues, catalogues of standards, specifications and guidelines.

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

5.2.3. Once-only principle

The once-only principle ensures that users should be able to provide data once only, and MDAs should be able to retrieve and share this data to serve the user. 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 copying of the data, but in this case, it must be considered that data may be outdated.

5.2.4. The single identifier of objects

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

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

5.2.5. Classifications

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.

---

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

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

5.2.6. Uniform addresses

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

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

5.2.7. 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 use the same syntax and semantics.

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

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

6. Technical architecture

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

6.1. Application architecture view

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

The view depicts the application architecture of any MDA solution. The view does not reflect the use of infrastructure services in detail. Infrastructure view, supporting ABB **Digital Service Infrastructure** is described in granularity in section 6.2.

Application Interoperability view in Figure 12 illustrates the most important ABBs of application architecture.

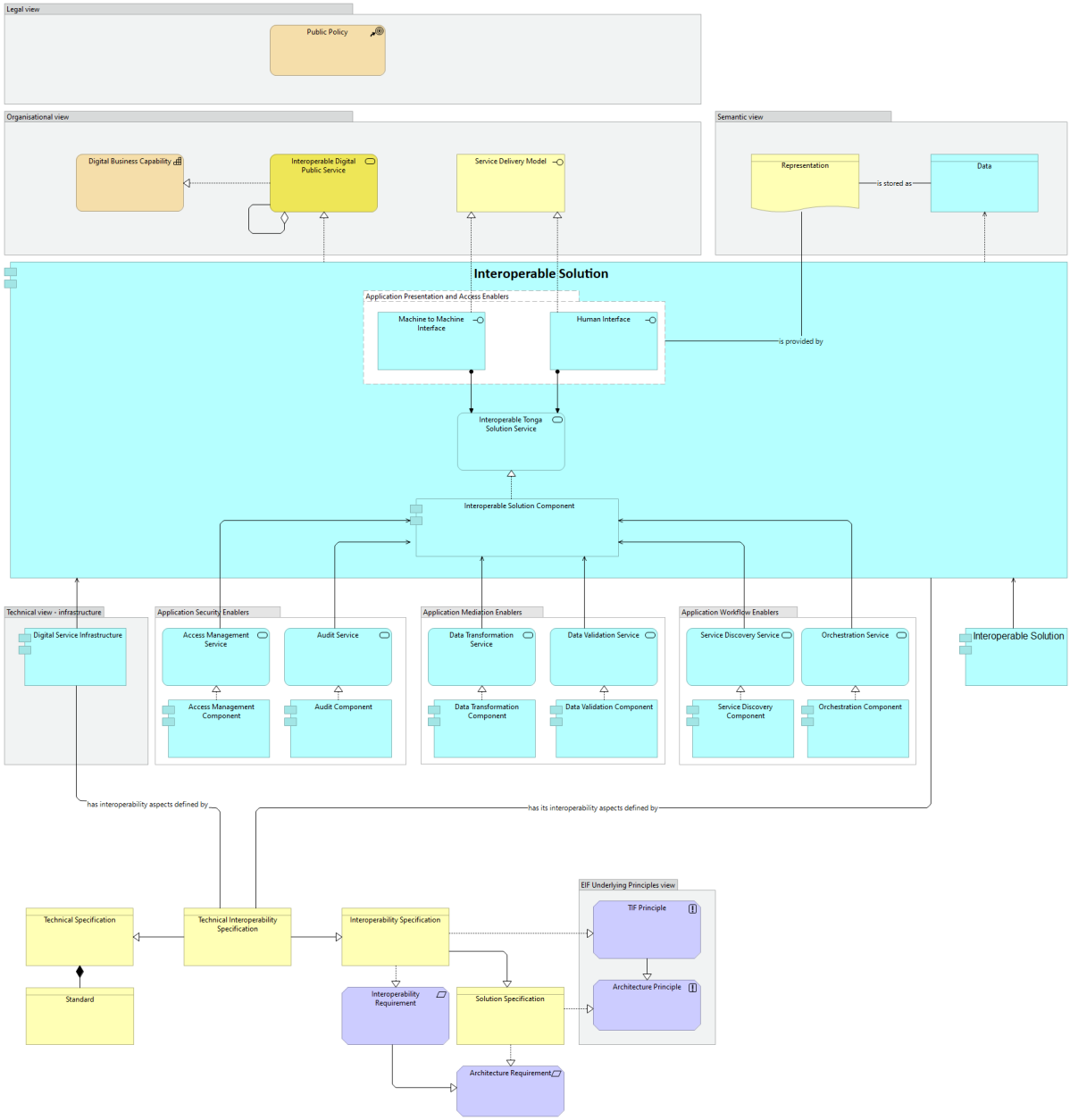

Figure 12 Application Architecture view

6.2. Infrastructure architecture view

The TEAF Infrastructure view depicted in Figure 13 provides an architecture content metamodel for the most salient cross-sectorial infrastructure services, along with the supporting hosting and networking facilities, which shall be considered to support technical aspects for the end-to-end design of interoperable solutions. The difference with the application part of the Application view is that the Architecture Building Blocks in the infrastructure view are relevant to solutions in any sector of government.

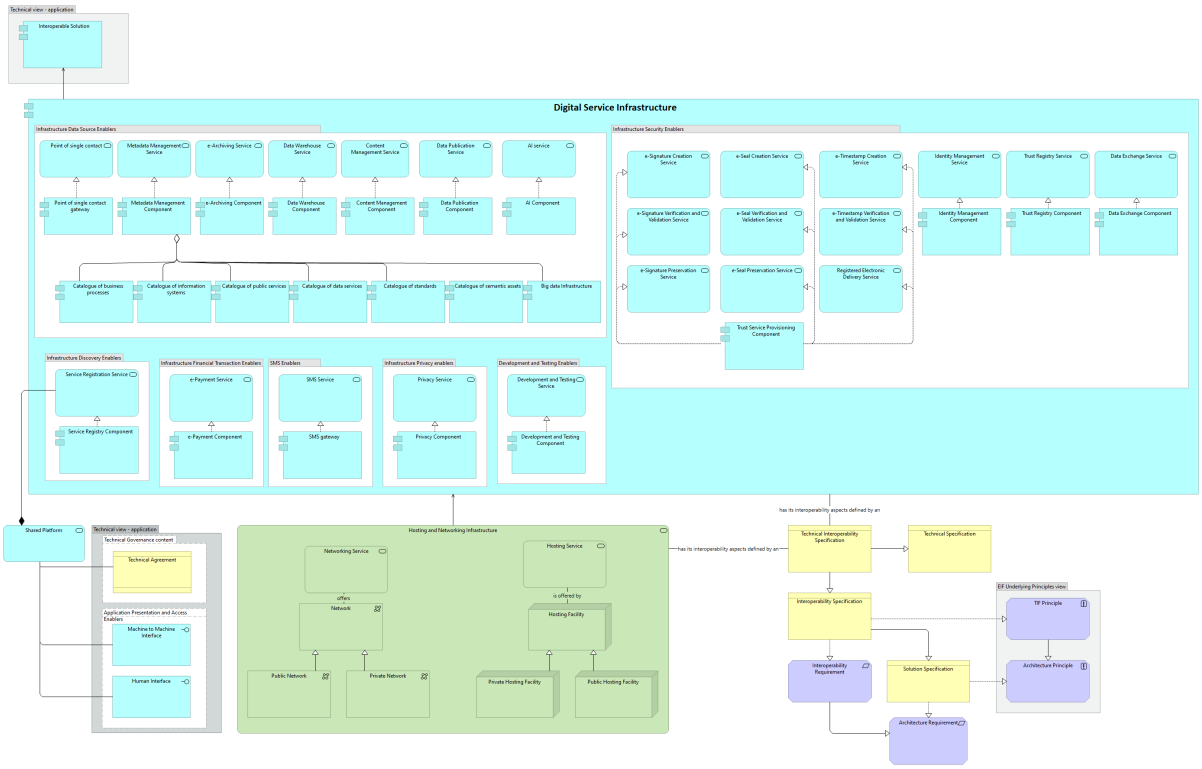

Figure 13 TEAF Infrastructure view

6.3. Crucial components of application and technical interoperability architecture

6.3.1. Catalogues

Catalogues describe reusable services and other assets to increase their findability and usage. This component allows publishers to document and make available resources with the potential to be reused by others. Various types of catalogues exist, for example directories of services, libraries of software components, open data portals, registers of registers, metadata catalogues and catalogues of standards. This ABB is described on the basis of eGA experience in several countries.

The catalogues of interoperability solutions are a supplementary instrument for the coordination of state information systems, a tool for development and administration of cross-domain systems and a support system for the maintenance of base registers and master data.

The goal of the catalogues is to guarantee transparent, optimally balanced, and efficient management of public sector information systems. Catalogues support the interoperability of databases, the life-cycle management of information systems and re-use of data by providing complete and up-to-date metadata of public sector information systems.

Recommended catalogues are:

- **Database of institutions**. Provides data about owners, administrators, developers and consumers of registers and information systems. It includes data about important

events: registration of institutions, joining institutions to the secure data exchange system, etc.

- **Public service repository.** The repository describes human interfaces of public services. This information can be used for building citizen portals.
- **Database of databases and information systems.** This component provides metadata about government registers (DB) and information systems (IS): the name of DB/IS; owner; type of DB/IS; list of services; information about registration and approval; technical architecture; legal acts; service-level agreements; security parameters; logical structure of data (data objects, data fields, parameters of fields).
- **Data service repository.** Repository ensures the interoperability of public sector information systems and the reuse of technical, organisational, and semantic resources. The service repository is an addition to the metadata kept in the database of databases and includes specifications for all web services and a detailed description of government services (incl. business process descriptions).
- **Repository of semantic assets.** This repository provides information about reusable components: semantic assets, guidelines, etc.

Catalogues guarantee the transparency of the state's information system's administration and helps to plan the state's information management. Catalogues provide information on the following subjects:

- Which information systems and databases are implemented in the public sector?
- Which data is collected and processed in which information systems?
- Which services are provided and who uses them?
- Who the responsible and authorised processors of the information systems and databases are, and who the contact persons are.
- What legal basis the databases are operated on, and the data is processed on.
- Which reusable components ensure the interoperability of information systems (XML assets, classifications, dictionaries, and ontologies)?

Catalogues serve as the procedural and administrative environment for the following actions:

- Registration and approval of information systems and databases
- Registration of services
- Registration of connections to the secure data exchange (SDE) platform
- Administration of reusable components (XML assets, classifications, dictionaries, ontologies).

Catalogues provide trustworthy assistance and are a great tool for developers, administrators and users of the state's information system. Catalogues offer tools for coordinated activities of several bodies. The main stakeholders of catalogues are depicted in Figure 14.

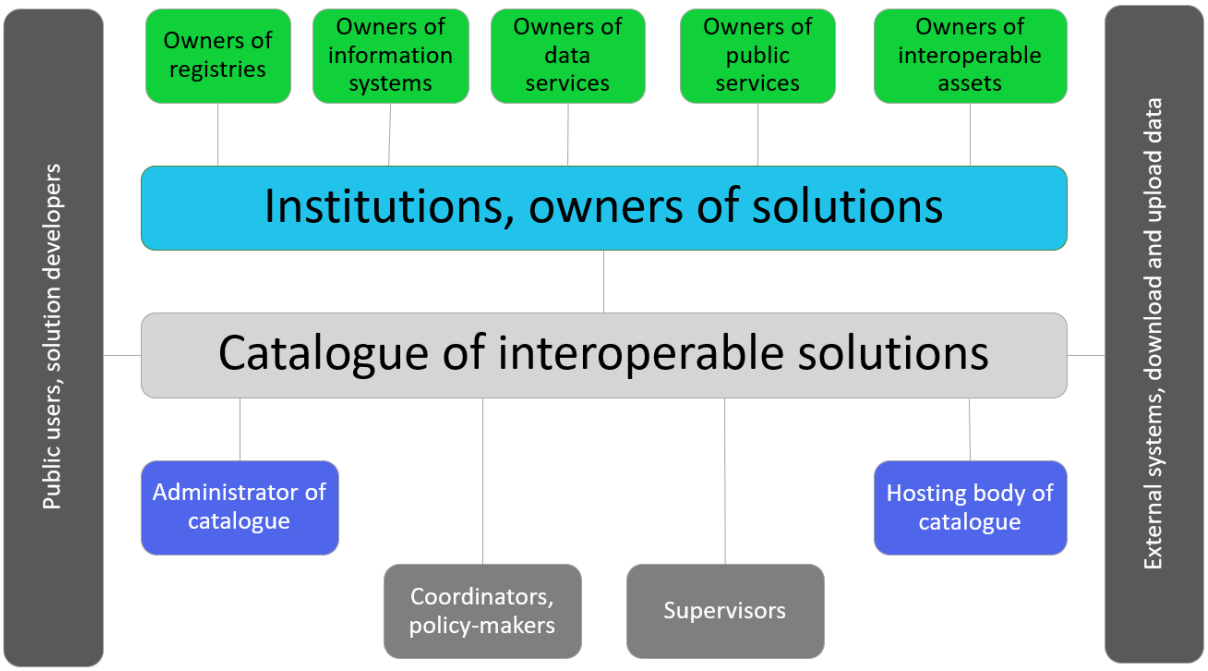

Figure 14 Main stakeholders of catalogues

Stakeholders co-create the content of the catalogue. Experts of institutions submit data about their institutions, owners of registers provide data about their registers, owners of consumer organisations about their information systems, owners of services about their services, owners of interoperability assets about their assets. Coordinators and supervisors use the catalogue and will register their decisions there.

All administration bodies should register their information systems, services and interoperability assets in the catalogue of interoperability solutions.

6.3.2. Point of single contact

Point of Single Contact (PSC) is an e-government portal that allows service providers to get the information they need and complete administrative procedures online. PSC enables users to get access to multiple information systems and portals without the need to log in multiple times. The portal enables access to a number of e-services. The access to the system is possible with or without eID and depending on the access method the number of available services may vary. Citizen portal is the official website for the Government. The functions of PSC are performed by the state portal at https://www.gov.to/

Ideally, the PSC should take data about public services from the Catalogues.

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

- **Lifecycle area** containing articles on how to resolve important or frequently occurring issues (such as applying for family benefits) and advice on what to do in certain

situations. The e-services, articles and contact details in the portal should be linked to make it easy for people to find information related to certain topics.

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

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

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

6.3.3. e-Payment

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

6.3.4. eID and PKI ecosystem

Current situation:[11]

[11] Inception report. Technical Advisor on Civil Registration and National

- Different online service providers currently have their own authentication systems and solutions. Primarily username and password pairs are used that is nowadays considered unsecure. Those can be used only for accessing the services of a specific online service provider. It makes access to services cumbersome and non-feasible both for the users and service providers.
- No nationally recognized e-ID tool/solution exists.
- There is a small number of computer, internet and smartphone users that make the spread of online services and possible e-ID tools complicated.
- State-controlled identity management is not established.

Before starting the PKI project, the Civil Registry (CR) system and the National ID (NID) system will be upgraded.

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

By building eID and PKI infrastructure Tonga will follow the conceptual model of eIDAS[12]. A high-level view of eIDAS is illustrated in Figure 15. The view includes following ABBs:

Electronic identification (eID) is the process of using a person's identification data in electronic form, uniquely representing either a natural or legal person or a natural person representing a legal person.

Trust service is an electronic service normally provided for remuneration, which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

eID-Service. The "eID-Service" provides services for the secure electronic identification and authentication of users and legal persons.

Certification Authority (CA). A Certification Authority generates electronic certificates and issues them to users or other entities, commonly called the subject of a certificate.

Time Stamping Authority (TSA). Proving the existence of a given set of digital data at a given time is a fundamental requirement in many electronic transactions. For this purpose, a Time Stamping Authority receives the data, which need to be time stamped, or a hash thereof, and returns a time stamp token, which is signed by the TSA.

Signature Generation & Sealing Service (SigS). The Signature Generation & Sealing Service allows to generate (qualified) electronic signatures.

[12] eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation on electronic identification and trust services for electronic transactions

Validation Service (ValS). The (qualified) electronic signatures and seals generated with the SigS above can be validated with the Validation Service.

Preservation Service (PresS). The long-term retention of signed documents requires a form of safekeeping that ensures the legibility and conclusiveness regardless of the storage medium.

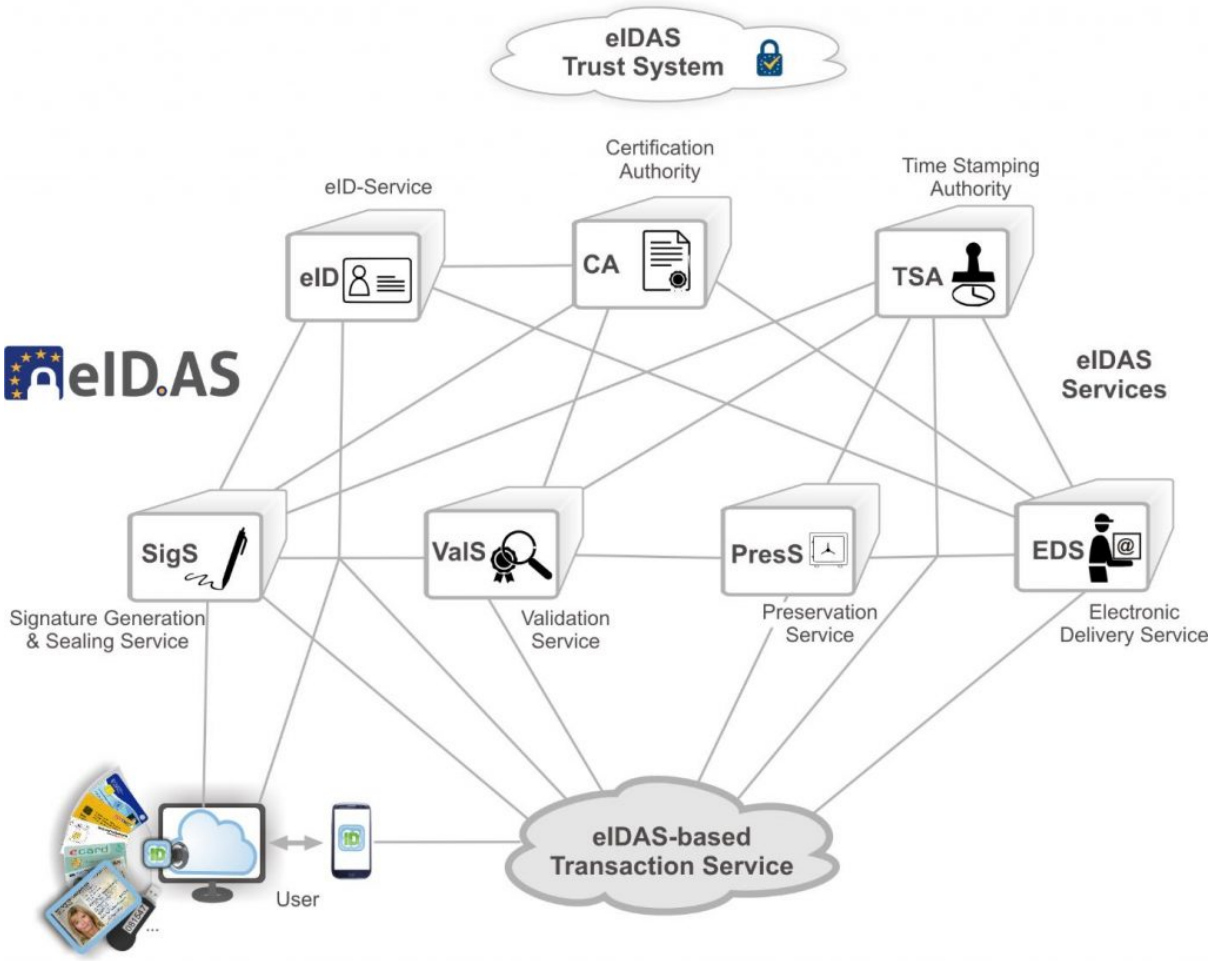

Figure 15 General model of eID and trust service infrastructure by https://blog.eid.as/

Electronic Delivery Service (EDS). Electronic services delivery or ESD refers to providing government services through the Internet or other electronic means.

Tonga eID and PKI infrastructure is recommended to be built in partnership with private entities (banks, telecom, certification authorities, etc.) and public institutions:

- National Civil Registry Office (NCRO) with National Identity Card Office (NICO) are responsible for personal identity management and for electronic/digital identity management.
- Digital Transformation Department at the PMO is responsible for certification management and for management of the provision of trust services.
- Other stakeholders: banks, Registrar-General's Office (RGO), MDAs, etc.

6.3.5. Secure data exchange ecosystem

Tonga is currently using an *ad hoc* approach to data exchange. When the need for data exchange arises, the two public bodies agree on the rules and tools for it. This approach is flexible and reasonable if a small number (less than four) of authorities or when low density of connections are involved. In any case, there is a need to:

- make certain changes in legislation
- create organizational agreements and procedures
- agree on the meaning and structure of data
- create separate procedures and tools for achieving security and privacy
- create separate technical interfaces
- chose channels for data transmission

There is a growing trend to use appropriate technical platforms for information exchange to ensure security and reduce overhead costs. We recommend for secure data exchange to use a technical platform, which will encapsulate technical and security details from MDAs.

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

The architecture of the secure data exchange ecosystem is described in Tongan Data Exchange Policy and Framework.[13]

The logical view of the secure service infrastructure components of the government data sharing platform and their interconnection is illustrated below in Figure 16.

The secure data exchange is based on TCP/IP networks. There are two types of members of information systems: service providers (publishers, back-end) and consumers (subscribers, front-end). An information system can act in both roles at the same time – publish its data and at the same time consume data published by someone else. The number of members is unlimited. The components of the platform are displayed below in Figure 16.

The most important component of the platform is the gateway. The gateway encapsulates all the security complexity for the members of the data sharing system. Gateways standardize the processes of message transfer between the members of the data sharing system. Only the sender and the receiver can see the structure and the content of the messages.

The model implies only a minimal number of central services:

- registry of information systems and services

[13] Tongan Data Exchange Policy and Framework. Project: Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure. Contract number: TO-MFNP-128799-CS-CQS

- services health monitoring
- and PKI functionality
- third party identification and authentication.

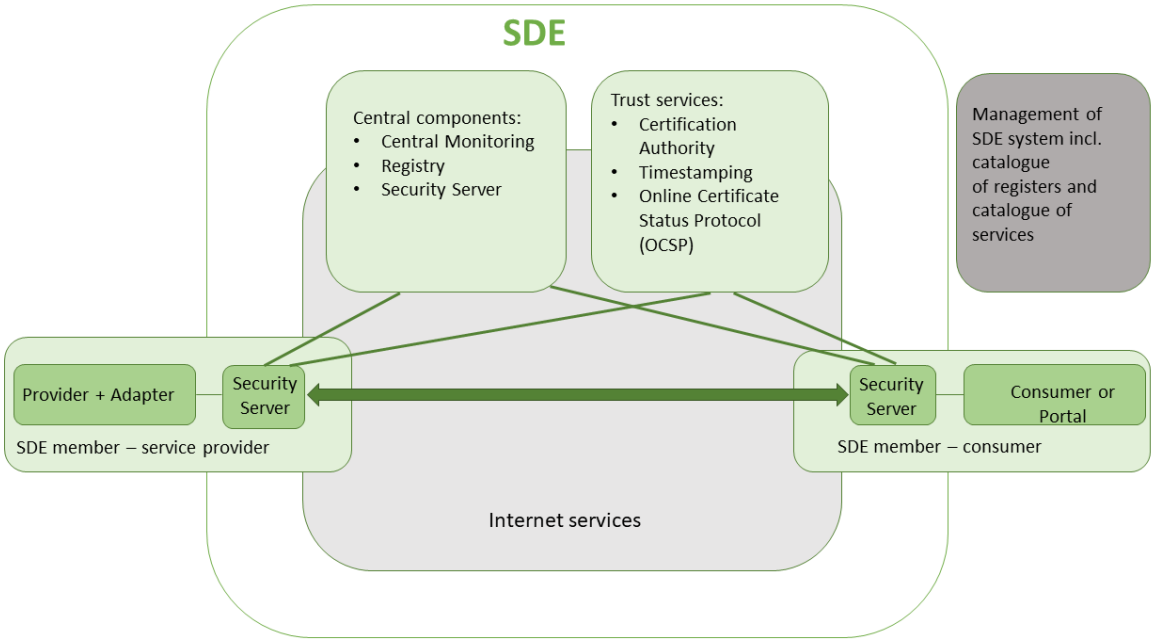

Figure 16 Secure data exchange infrastructure components

Central components provide information to proxy servers about the data exchange participants. These kinds of mechanisms allow for the secure exchange of electronically verified messages, records, forms, and other kinds of information between the different systems. In addition to transporting data, this layer should also handle specific security requirements such as the creation and verification of electronic signatures, encryption, and timestamping. Furthermore, there should be monitoring of traffic to detect intrusions, changes of data and other types of attacks.

The provision of secure (i.e. signed, verified, encrypted, and logged) data exchange via the data exchange platform 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 exchange is logged for future evidence and archived when necessary.

As this secure data exchange model is based on the principle that data is exchanged directly between the data supplier and the recipient without a central intermediator, it does not have a single point of failure. This means there is no single point of risk for a cyber-attack or system

malfunction. In case of failure of one component, other parties can continue to operate. Also, participants can build their systems at their own pace without waiting for central development.

6.3.6. Data Centre and Government Cloud

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

Potential government investments in cloud computing for the public sector should be evaluated on a case-by-case basis. Each case should be assessed from 1) a cybersecurity perspective to make sure it satisfies the national cyber security requirements, 2) a technical perspective to ensure its technical viability and 3) a commercial perspective to ensure it represents the most cost-efficient solution available.[14]

6.3.7. Open Data ecosystem

Open data is digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere. Tongan public bodies agree to follow a globally agreed set of principles, formulated by the International Open Data Charter[15]. These principles will form the foundation for access to data and for the release and use of data:

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

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

Public bodies shall publish open data in machine-readable, non-proprietary formats. They shall ensure that open data is accompanied by high quality, machine-readable metadata in non-proprietary formats, including a description of their content, the way data is collected and its level of quality and the license terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.

---

[14] Tonga Cloud First Policy. Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure. Contract number: TO-MFNP-128799-CS-CQS

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

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

7.Security Viewpoint

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

The Security Architecture viewpoint models the most salient Architecture Building Blocks related to security. Citizens and businesses must be confident that when they interact with public authorities they are doing so in a secure and trustworthy environment and in full compliance with relevant regulations, e.g. the Regulation on electronic identification and trust services. The SA viewpoint of TEAF is illustrated in Figure 17.

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

Security Framework is an agreed governance approach focusing on the protection aspects related to data, information and knowledge assets and organisational resources handling them.

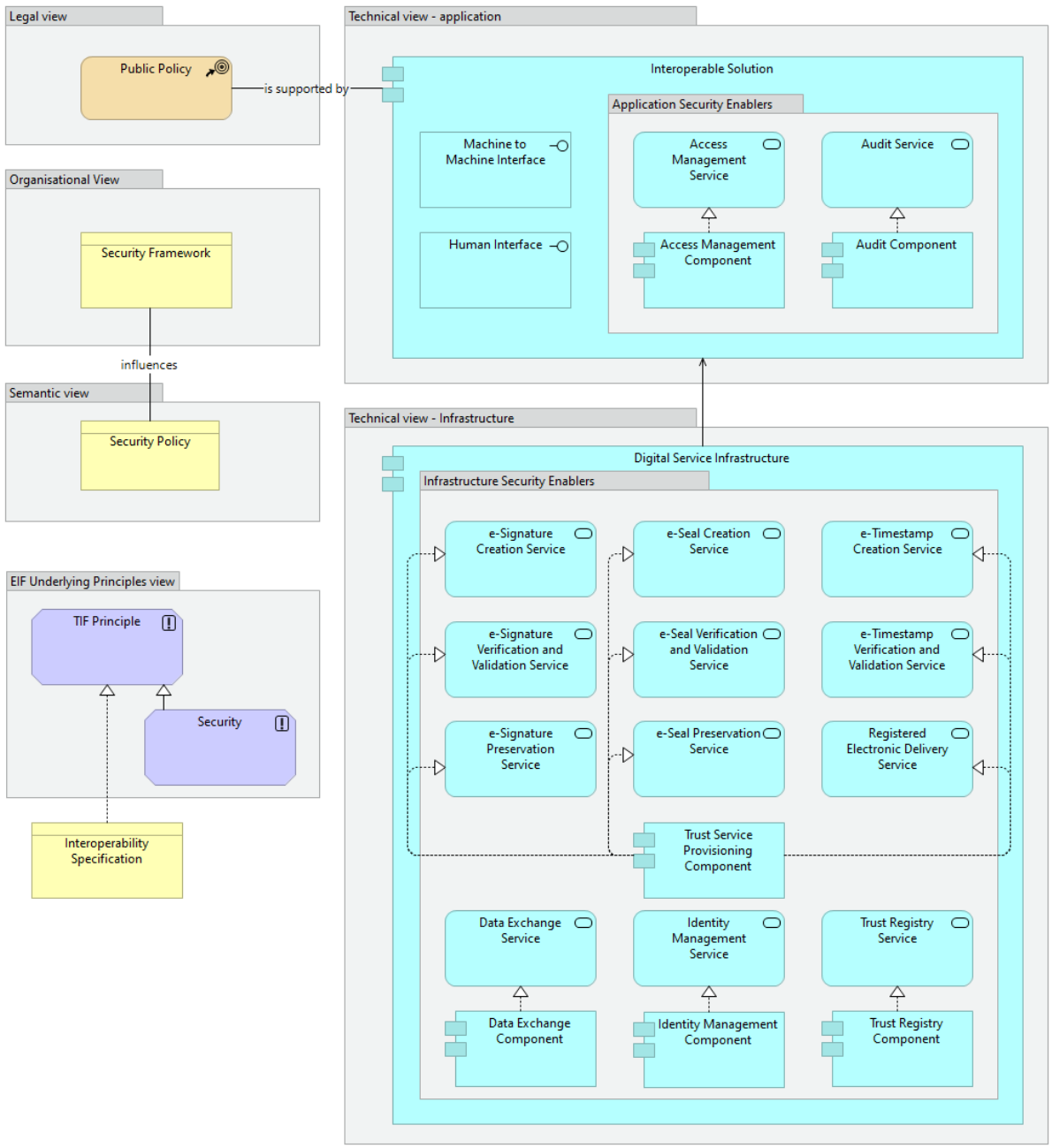

Figure 17 TEAF Security viewpoint

8.Governance of implementing TEAF

There is a need for high level coordination of the e-government activities between the various units of the government. PMO 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 coordination is not to centralise all decision making and technical capacities. Vice versa, the idea is to support innovation and service delivery modernisation in every government institution.

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

TEAF handles information systems from the point of view of the state as a whole. The maintenance and implementation of TEAF will be done by the e-Government Steering Committee with the leadership of the Coordination Body. Compliance to the TIF and TEAF 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 and TEAF standards shall neither receive funding nor be sanctioned to proceed.

MDAs shall have the following roles to play:

- Contribute to the continuous development and improvement of TEAF.
- Ensure that TEAF compliance is a fundamental part of their organisational e-business and IT strategies
- Prepare a 'roadmap' for implementing the conformity with TEAF.
- 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 and enterprise architecture in their organisations and are encouraged to compile their own enterprise architecture (or similar) where principles and requirements are specified. These frameworks must be harmonized with the Tonga TEAF.

Working groups should be established for more salient ABBs: Catalogues, PSC, eID and PKI, SDE, open data.

It is not possible give the TEAF for all e-government components in detail. According to TOGAF®, the building of big systems is an iterative process. It is reasonable that every MDA will build their own architecture independently, considering the requirements of the TIF and

TEAF. This document focuses on the components important for achieving interoperability. The document is the first iteration of TEAF. The document points out the most critical segments of TEAF important for achieving interoperability in the Tongan e-Government. For implementing those segments, new ADM cycles need to be initiated.

The division of the TEAF into segments and initiating new ADM cycles for each component is illustrated in Figure 18. For several segments, their division into subsegments and initiating the next level of ADM cycles may be reasonable. Figure 18 does not reflect all components of the Tongan TEAF: only very few segments and subsegments are outlined. For each subsegment and sub subsegment, a new iteration needs to be initiated.

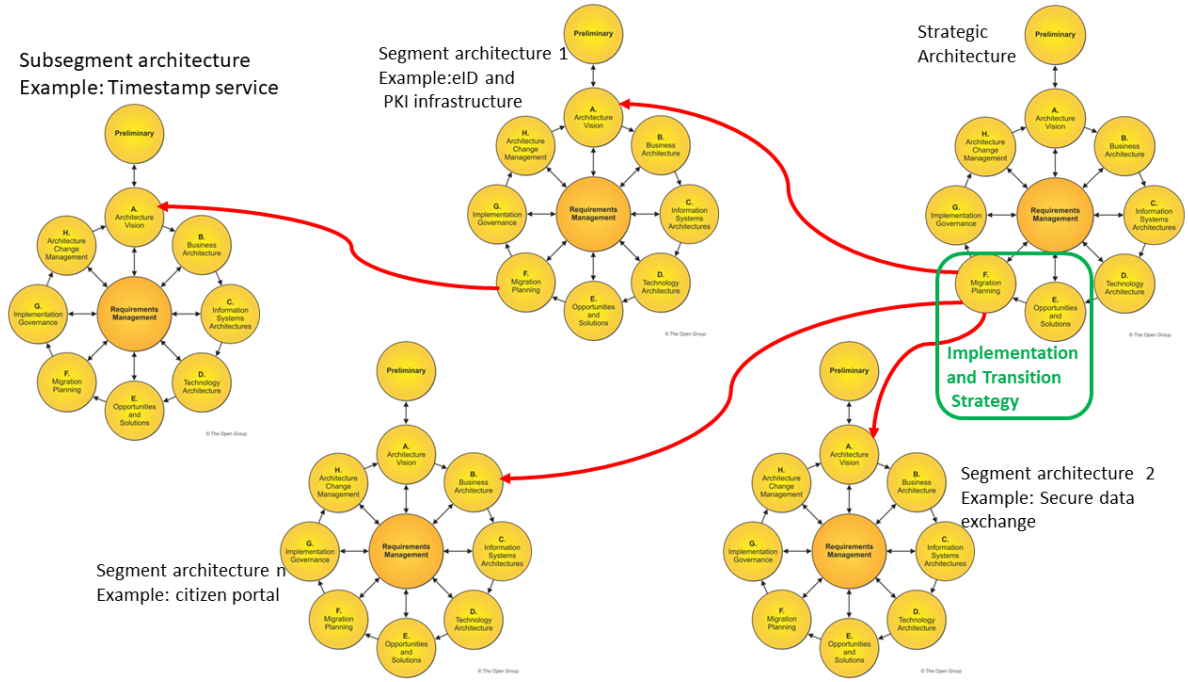

Figure 18 Segmentation needed for building e-Government Architecture (example)

9.Architecture Building Blocks

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

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

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

Architecture Building Block. An Architecture Building Block (ABB) is a constituent of the architecture model that describes a single aspect of the overall model. An Architecture Building Block describes generic characteristics and functionalities.

Architecture Building Blocks are used to describe reference architectures, solution architecture templates or solution architectures of specific solutions. Source TOGAF®: https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_8.

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

Architecture Requirement is a requirement of the highest possible level of granularity for an Architectural Building Block, formulated as an agreed normative statement of a to-be GoT Public Service.

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

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

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

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

Base registries are reliable sources of basic information on items such as persons, companies, vehicles, licenses, buildings, locations, and roads and are authentic and authoritative and form, separately or in combination, the cornerstone of public services.

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

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

Binding Instrument. The Binding Instrument ABB is relevant to interoperability as, by being a specialization of the legal act, it makes mandatory the implementation of the policy (and therefore the underlying interoperability implications).

Business. Economic operator with a legal entity entitled to perform a private activity for a profit. The Business ABB is salient for organization interoperability because organizations can play the role of consumers of public services.

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

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

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

Catalogue of information systems and registries. This component provides metadata about government registries and information systems: the name of; owner; type; list of services; information about registration and approval; technical architecture; legal acts; SLA; security parameters; logical structure of data (data objects, data fields, parameters of fields).

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

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

Catalogue of standards. Standards have been developed through consensus by industry, consumers, government departments, research organizations, universities and private institutions.

Citizen. An individual is a principal that provides and/or consumes public services. A citizen has rights because of having been born in Tonga or because of having been given rights. The Citizen ABB is salient for organisation interoperability because citizens can play the role of consumers of public services.

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

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

The Content Management Service ABB is salient for technical interoperability because it provides and shares the functionalities of dynamic creation, distribution, and analysis of contents (images, videos, etc.). Catalogues help others to find reusable resources (e.g. services, data, software, data models). Various types of catalogues exist, e.g. directories of services, libraries of software components, open data portals, registries of base registries, metadata catalogues, catalogues of standards, specifications and guidelines. Commonly agreed descriptions of the services, data, registries, and interoperable solutions published in catalogues are needed to enable interoperability between catalogues.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The right to data portability applies:

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

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

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

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

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

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

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

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

Data Transformation Service. Shares the functionality of conversion of one data representation to another. The Data Transformation Service ABB is salient for technical

interoperability because it provides the functionalities to transform internal data structures to common and agreed interoperable formats.

Data Validation Component. Implements the functionality of referring to any activity aimed at verifying that the value of a data item comes from a given set of acceptable values. Data validation may be followed by corrective actions, such as data editing or data imputation. In statistics, imputation is the process of replacing missing data with substituted values. The Data Validation Component ABB is salient for technical interoperability because it allows the implementation of the functionality to validate if data received (or to be sent) is compliant with common and agreed interoperable formats.

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

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

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

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

The Descriptive Metadata Policy ABB is salient for semantic interoperability because metadata facilitates opening and sharing data by providing the appropriate format, description of the content, high level of quality in order to achieve interoperability. Ensure that open data is accompanied by high quality, machine-readable metadata in non-proprietary formats, including a description of their content, the way data is collected and its level of quality and the license terms under which it is made available. The use of common vocabularies for expressing metadata is recommended.

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

Digital Business Capability. A particular digital ability or capacity that an organisation may possess or exchange to achieve a specific purpose or outcome.

Digital Service Infrastructure. Infrastructure which enables networked services to be delivered electronically, typically over the internet, providing Tongan interoperable services of common interest for citizens, businesses and/or public authorities, and which are composed

of core service platforms and generic services. The Digital Infrastructure Service ABB is salient for technical interoperability because it a central element through which interoperability is ensured.

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

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

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

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

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

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

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

e-Seal Creation Service. Shares the functionality of signing data in electronic forms on behalf of a legal person. **An 'electronic seal'** means data in electronic form, which is

attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. The 'creator of a seal' is a legal person who creates an electronic seal.

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

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

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

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

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

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

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

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

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

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

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

Interoperability Organisational Authority. An organisation having the powers to govern the interoperability of public administration. The Interoperability Organisational Authority ABB is an interoperability enabler because it helps achieve organisational interoperability by

ensuring political and/or administrative governance of the interoperability capabilities of an organisation.

Interoperability Requirement. An Interoperability Requirement is a requirement of the highest possible level of granularity for a TEAF ABB, formulated as an agreed normative statement in functional terms on a legal, organisational, semantic, or technical attribute of a to-be GoT public service.

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

Interoperable Solution. A solution developed by MDAs that facilitate the delivery of electronic Public Services between MDAs (or Citizens and Businesses) in support to the implementation and advancement of public policies.

Interoperable Solution Component. Interoperable GoT Solution component represents the encapsulation of a functionality provided by an Interoperable GoT Solution. The Interoperable GoT Solution Component ABB is salient for technical interoperability because it is a central element of the TIF conceptual model for integrated public services. It represents all the functionalities provided by interoperable solutions.

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

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

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

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

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

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

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

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

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

Identity Management Service. Shares the functionality of user authentication.

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

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

Interoperable Solution Component. Interoperable Tongan Solution Component represents the encapsulation of a functionality provided by an Interoperable GoT Solution.

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

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

Legal Act. Formalised set of rules on a subject potentially including requirements concerning digital public services. The granularity of the requirements might be of high level or detail level. Requirements of high-level granularity contain generic/abstract functional requirements like principles and/or recommendations with considerable degrees for transposition/execution and of not binding nature. On the other side, requirements of detail-level granularity imply a limited degree for transposition/execution, and they contain specific/concrete functionalities, solution components, data, procedures, and/or technical specifications or standards to be used.

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

Legal agreements/ International treaties. Under international law, a treaty is any legally binding agreement between states (countries). A treaty can be called a Convention, a Protocol,

a Pact, an Accord, etc.; it is the content of the agreement, not its name, which makes it a treaty.

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

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

Legal Interoperability Agreement. A legal interoperability agreement is a legal resource formalising governance rules enabling collaboration between digital public services.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Open Data Policy. The rules and practice of publishing (raw) data in a way that is accessible, reusable, machine readable and licensed permissively. It can be generated by a wide range of parties, including public authorities, the semi-public sector, businesses and the public. In the case of MDA, making their data available for public reuse supports economic development, openness, and transparency.

The Open Data Policy ABB is salient for semantic interoperability because Open Data is a part of the basic components of the TIF conceptual model for integrated public services.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A private network is a computer network that uses a private address space of IP addresses. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments, and are not accessible from outside of organisation.

Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Service Delivery Model. The way of delivering to public service consumers, or otherwise interacting with them, for the purpose of supplying specific public services with accessibility value. This involves a number of management practices to ensure that the public services are provided as agreed between the public service provider and the consumer.

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

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

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

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

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

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

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

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

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

Solution Building Block (SBB) is a candidate solution which conforms to the specification of an Architecture Building Block[16] (ABB).

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

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

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

TEAF View. The TEAF consists of several architecture views, including one view for each of the TIF interoperability levels. The TEAF views contain a graphical notation of the TEAF ontology. TOGAF®: An architecture view is a representation of a system from the perspective of a related set of concerns[17].

TEAF Viewpoint. The TEAF provides several viewpoints that conform to TEAF views. The viewpoints provide a perspective with specific stakeholder's concern in mind. TOGAF®: A specification of the conventions for a particular kind of architecture view[18].

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

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

---

[16] https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_70
[17] https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_17
[18] https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap03.html#tag_03_18

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

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

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

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

- Note 1 to entry: A technical specification should indicate, whenever appropriate, the procedure(s) by means of which it may be determined whether the requirements given are fulfilled.
- Note 2 to entry: A technical specification may be a standard, a part of a standard or independent of a standard.

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

TIF Principle. Underlying principle stipulated by the Tonga Interoperability Framework.

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

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

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

1. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
2. the creation, verification and validation of certificates for website authentication; or

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