Tongan Data Exchange Policy and Framework

Project: Tonga Enterprise Architect for Developing and Supporting ICT Infrastructure

15 November 2021, version 0.9

Change history

Version	Date	Summary of changes
0.8	03.09.2021	Draft. Uuno Vallner
0.9	15.11.2021	Updated draft. Marit Lani, Uuno Vallner

Document status

Draft	
For approval	
Approved	X

Authors

Name	Role
Dr Uuno Vallner	Enterprise architect
Marit Lani	Project manager

Table of Contents

1. Introduction

One of the five pillars of the Tongan Strategic Development Framework 2015-2025 (TSDF)[1] was dedicated to the use of reliable, safe, and affordable information and communication technology. The Tonga Digital Government Strategic Framework (TDGSF)[2] 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

TSDF and TDGSF serve as starting points for developing the Tongan Enterprise Architecture Framework (TEAF), including the Tonga Interoperability Framework (TIF)[3], and this Data Exchange Policy/framework.

The Data Exchange Policy and Framework is applicable to all public bodies in Tonga. It lays out the basic conditions for building a Secure Data Exchange (SDE) ecosystem at all levels of the public bodies. This document is addressed to all those involved in defining, designing, developing, and delivering public services in Tonga.

Data exchange content and structure:

- Chapter 2 presents the model for Secure Data Exchange based on the Conceptual Model for Integrated Public Services Provision described in TIF. The TIF provides the main principles and requirements for building an SDE ecosystem. The conceptual model for integrated public services is relevant to all public bodies. The Secure Data Exchange ecosystem and its technical platform support public sector bodies to resolve data exchange tasks in a more efficient and secure way. Public bodies will use a standardized approach for providing and consuming all services.
- Chapter 3 provides an overview of the main criteria to be considered when selecting or developing a secure data exchange platform. These include message transfer, trust, performance, availability, flexibility, architecture, operations, scalability, resilience, security, support, total cost of ownership, and cross-border data exchange.
- Chapter 4 presents the Reference Architecture of SDE. 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, which is based on best practices, is domain

[1] Tonga Strategic Development Framework (TSDF II), 2015-2025
http://extwprlegs1.fao.org/docs/pdf/ton168846.pdf
[2] Digital Government Strategic Framework 2019-2024. Kingdom of Tonga, 2019, p 50
[3] Tonga Interoperability Framework (TIF). Version 0.8, 2021

neutral and, occasionally, has a focus on a particular aspect.[4]. According to TIF interoperability model, four layers of interoperability: legal, organizational, semantic, and technical are distinguished. The key architectural building blocks (ABB) needed for these layers are presented. Key stakeholders of the SDE ecosystem are the SDE Operator, SDE Members, and Trust Service Providers.

SDE Operator is responsible for all the aspects of the operations in the SDE ecosystem. The responsibilities include defining regulations and practices, accepting new members, providing support to Members, and operating the central components of the SDE software.

SDE Members are organizations that have joined the ecosystem and produce and/or consume services with other Members. A Member organization can be a service provider, a service consumer, or both.

Trust Service Provider(s). A functioning SDE ecosystem requires two types of trust services: 1) time-stamping authority (TSA) and 2) certification authority (CA).

- Chapter 5 presents the key aspects of the open data policy. To exchange open data, the SDE MAY not be needed. 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. The focus of open data policy is on releasing machine-readable data for use by others to stimulate transparency, fair competition, innovation, and a data-driven economy. To ensure a level playing field, the opening and reuse of data MUST be non-discriminatory, meaning that data must be interoperable so that can be found, discovered, and processed.
- Chapter 6: Abbreviations
- Chapter 7: Glossary

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

The most important conclusions and requirements are provided in text boxes.

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

[4] https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/chapter-2-key-concepts-and-archimater-notation

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

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

2. Secure data exchange ecosystem

2.1. Why?

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) authorities 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

If there are N bodies in Tonga, we will need to create up to N(N-1) solutions for data exchange. Each solution must take all of the 6 above-listed aspects into account. *Ad hoc* approach has used in several countries[6]. It is quite expensive and requires high level skills in all MDAs.

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 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 in a more efficient and secure way. Public bodies will use a standardized approach for providing and consuming all services. After the implementation of this policy, only up to N-1 data exchange solutions will be needed.

1. A Secure Data Exchange ecosystem SHOULD be developed for improving efficiency, increasing security, and achieving interoperability.

2.2. Data exchange framework as part of the interoperability framework

The Conceptual Model for Integrated Public Services Provision described in the Tonga Interoperability Framework (TIF)[7] includes the main principles and requirements for building a secure data exchange (SDE) platform. The conceptual model for integrated public services

[6] For example in New Zealand: https://ndhadeliver.natlib.govt.nz/webarchive/wayback/20171203200520/https://ict.cwp.govt.nz/guidance-and-resources/standards-compliance/new-zealand-secure-web-services-standard/

[7] Tonga Interoperability Framework. eGA report, 19 August 2021, p 52

is relevant to all governmental levels: local, government bodies, ministerial, national. The modular model comprises loosely coupled service components. Components are interconnected through shared infrastructure. This model according to the notation of ArchiMate is depicted in Figure 1.

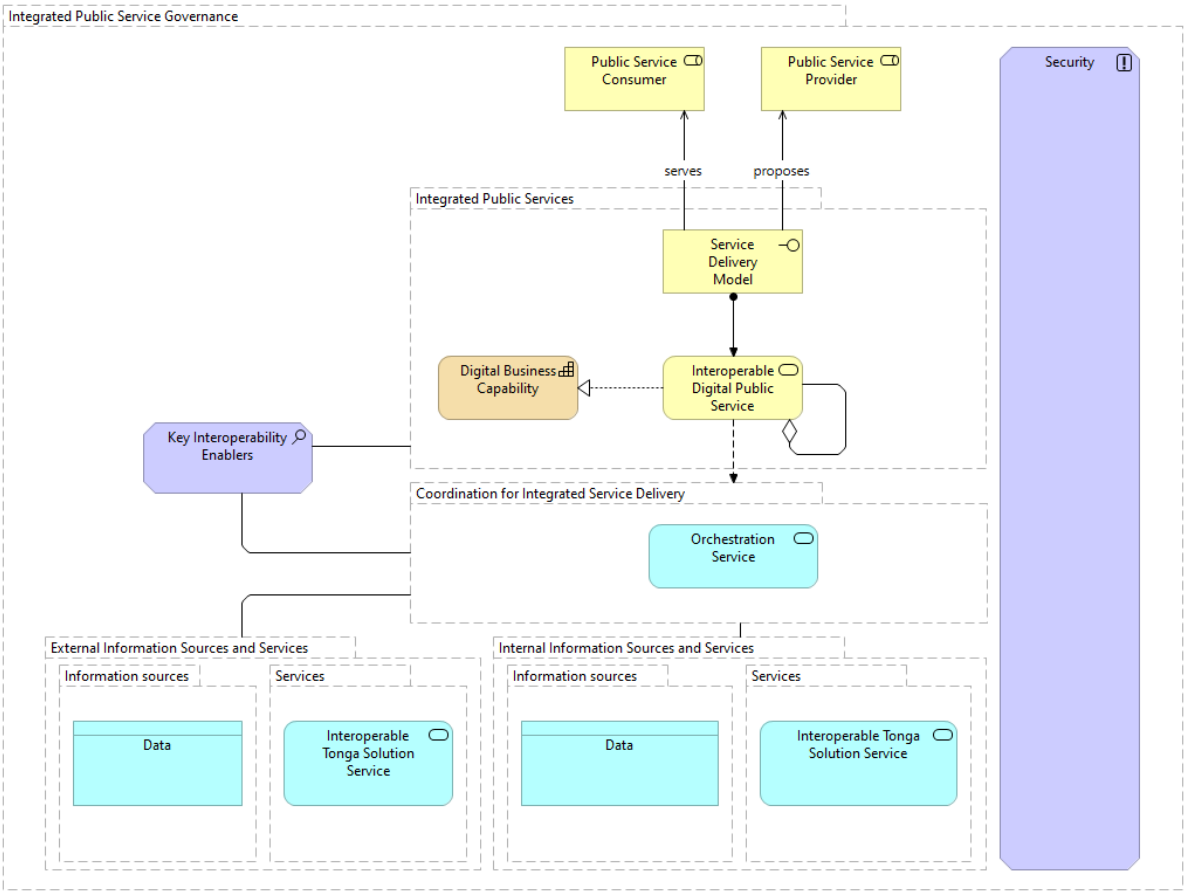

Figure 1 Conceptual model for integrated public services

The Conceptual Model promotes reusability as a driver for interoperability (interoperability by design), recognising that Tongan public services should reuse information and services that already exist and may be available from various sources inside or beyond the organizational boundaries of the public bodies. 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. The Tongan Data Exchange Framework MUST be aligned to the requirements and recommendations of the Tongan Interoperability Framework.

We follow the **service-oriented** principle. It means all the activities of any organization are services. A service can be:

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

Interoperability infrastructure represents a set of IT systems that support the delivery of Tongan public services to administration bodies, citizens, and businesses. There are two types of services - business services and infrastructure services. An infrastructure service is a generic technical functionality of a system that supports the delivery of one or multiple business services. Infrastructure services are hidden for end users.

To ensure interoperability of public sector information systems, the public sector will develop and implement several common infrastructure components. The most important components/enablers of Tongan e-Government infrastructure are:

- Secure data exchange ecosystem
- eID and trust services ecosystem
- Catalogue of interoperability solutions
- Open Data infrastructure
- Single point of services

The first three enablers are highly interdependent. It is recommended to create them according to each other's needs.

3. SDE ecosystem and other infrastructure services MUST be available for all public sector bodies, business, and citizens free of charge.

2.3. The secure data exchange model

The establishment of a secure data exchange solution/platform is one of the key elements of Tongan e-Government. The key properties for SDE ecosystem are:

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

4. All data exchange MUST be done in a secure and controlled way. The secure data exchange building block is the most crucial factor for the implementation of the model.

5. Data transferred over the SDE MUST preserve their legal status. The official decisions made on basis these data are binding.

The concept of separate front-end and back-end systems should be supported by the Secure Data Ecosystem. The task of back-end systems is data management and provision of network services. Machine-to-machine services of back-end systems are made available for the end user only through service intermediaries (front-end systems).

Front-end systems are divided into internal (e.g. Intranet) and public systems. Internal front-end systems are responsible for administering the employees' access rights to any service having evidential value in the country. Service usage rights are personal and restrictions can be added to them (e.g. time limit with regard to using a service). Front-end systems should not grant rights to employees of other institutions. Qualified certificates are used for authorization of services with evidential value.

6. Back-end and front-end systems SHOULD be architecturally separated.

7. Back-end systems SHOULD NOT be engaged in end users' authentication and authorization.

8. Services of back-end systems SHOULD be available for an end user only through front-end systems.

Security is a primary concern for data sharing and for the provision of public services. Public administration bodies providing public services should ensure:

- that the complete infrastructure and building blocks are secure by complying with the principles of a privacy-by-design approach
- that the services are not vulnerable to attacks, which might interrupt their operation, cause data theft or data damage
- and that they are compliant with the legal requirements and obligations regarding data protection and privacy.

Data sharing mechanisms should facilitate information exchange between administration bodies, businesses and citizens that are:

- registered and verified: both sender and receiver have been identified and authenticated through agreed procedures and mechanisms
- encrypted: confidentiality of the exchanged data is ensured
- timestamped: maintain accurate time
- logged: electronic records are logged and archived to ensure a legal audit trail.

The logical view of the secure service infrastructure components of the government data sharing platform and their interconnection is illustrated below in Figure 2Figure 1.

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 own 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 2.

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.

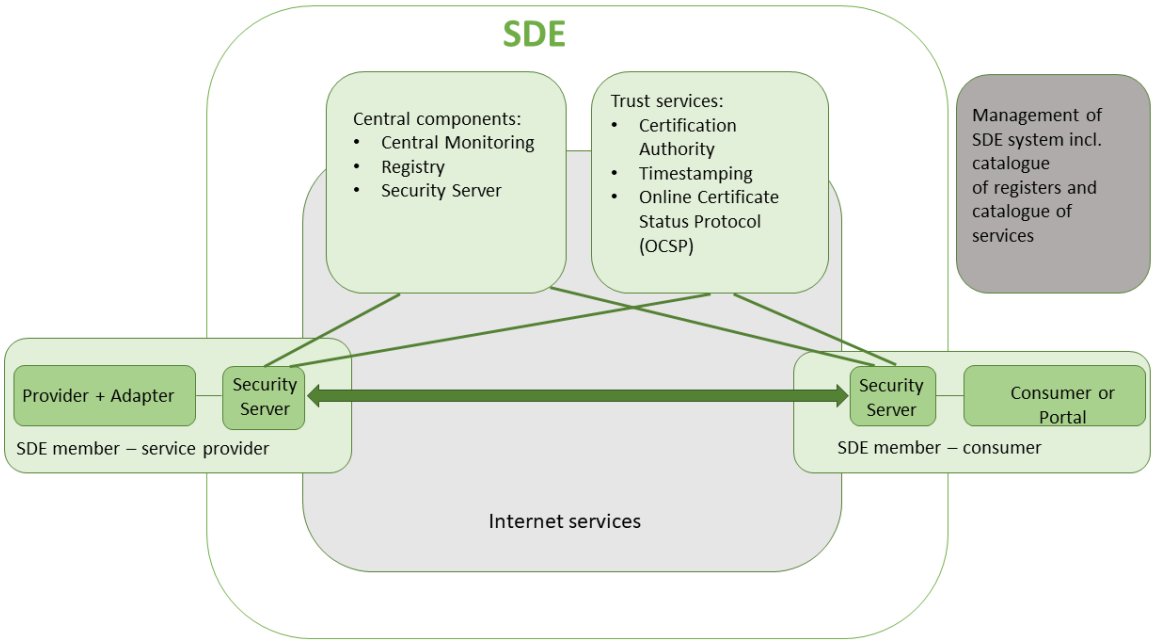

Figure 2 Secure data exchange infrastructure components

The model implies only a minimal number of central services:

- registry of information systems and services,
- third party identification and authentication,
- transaction log,
- services health monitoring
- and PKI functionality.

Central components provide information to proxy servers about the data exchange participants. These kinds of mechanisms should 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 of other type 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 still continue to operate. Also, participants can build their systems at their own pace without waiting for central development.

9. For the management of SDE, a catalogue of interoperable solutions (catalogues of members, information systems, services, assets) SHOULD be used.

10. Trust Service Providers MAY be commercial third parties, or the services MAY be provided and maintained by the operator of central components.

11. Public sector bodies MUST use the secure data exchange ecosystem when exchanging legally binding data.

3. Criteria for SDE platform

In this chapter we will provide an overview of the main criteria to be considered when selecting or developing a solution for secure data exchange.

3.1. Message transfer

Message transfer is about how the exchange of messages between connecting ministries, agencies and other organizations is enabled. Message transfer concerns security and non-repudiation (certified dispatch and certified receipt), not the content of the message.

It is possible to have a solution where all messages are sent from the provider platform to a central portal, which transfers the message to the consumer platform. However, this causes the central portal to become a single point of failure and a performance bottleneck (all the messages exchanged MUST pass through this portal, therefore this portal must accommodate increasing traffic as the data exchange platform gains more ground). In this case, the system administrator of the central platform can read the message transfer log, which contains real data, and which means that the administrator can see the exact information exchanged between any two parties.

"Agnostic message transfer" should be preferred, where the interoperability solution transfers the bits/bytes of the message without any knowledge of the structure and/or content of the message.

3.2. Trust

Trust is essential between different organizations that may not even know each other. Trust is established by the following security facilities:

- Identification – to identify an entity (a person or a system) sending and/or receiving messages
- Authentication – to ascertain that an entity really is who it claims to be
- Certification – to certify (sign) a message sent, or a message received
- Encryption – to ensure that nobody can read or modify messages during transfer
- Non-repudiation – to ensure that an entity cannot deny the authenticity of their signature on a document, or the sending of a message that they initiated
- Logging – to store legal proof of a message transfer. This could be the message itself, or a hash of the message. A message hash has four main properties: 1) easy to compute the hash value for any given message, 2) infeasible to generate a message from its hash, 3) infeasible to modify a message without changing the hash, 4) infeasible to find two different messages with the same hash.

It is important to include certification and non-repudiation concepts in the secure data exchange solution. Logging is recommended to be implemented in the central part (service providers are not logging by default what data is requested from them). It is better if logging

is done in the publisher and subscriber environments, while the central component would only store a hash of the logs.

3.3. Performance

Time delays when transferring a message between organizations should be as short as possible. Performance is affected by the resource use (i.e. demand) of the message transfer software, by the resource capacity of the platform, and by the volume of message transfers at any specific moment.

In a centralized solution, message transfer is initiated by the sender by sending the message to the portal. This implies that centralized infrastructure is a performance bottleneck and decentralized infrastructure should be preferred.

3.4. Availability

Availability is dependent on many factors, including architecture (distributed or centralized), software distribution, resilience of operations, and resilience against malware attacks. For a national secure message transfer infrastructure, 24/7 availability is mandatory.

3.5. Flexibility

Optimal flexibility is needed to connect organizations. For a national secure interoperability solution for agnostic message transfer, flexibility in message structures, message transformation and/or message processing is a non-issue. This is because the data sharing only requires transferring bit/byte streams. It is strongly advisable for the data sharing platform to limit itself to agnostic (without any knowledge of structure and content) message transfer only. Any message structure, transformation and/or processing is done at application levels by the systems of the interoperating organizations.

3.6. Architecture

As architecture determines facilities such as security, performance, and resilience, it is one of the most important criteria for the data sharing platform.

In case of a decentralized architecture (right-hand side on Figure 3 below), messages are transferred directly between proxy software created *ad hoc* at all the interoperating organizations. The proxies are asynchronously managed and monitored by central components. Because the central components can also be replicated, the overall architecture of the data sharing platform proves resilient to errors and attacks.

In case of a centralized architecture (left-hand side in Figure 3 below), messages are transferred by the interoperating organizations to/from the central infrastructure. The advantage is that message transformation and business process management are easy to manage centrally. However, this is a capability that is explicitly NOT wanted for an inter-organization facility, because the connecting organizations will not defer their unique responsibilities to a central organization. However, for the e-government, the missing security features (certification and non-repudiation) are mandatory. A centralized architecture is also

more vulnerable to internal (maintenance and updates) and external (hacking, DoS) disruptions.

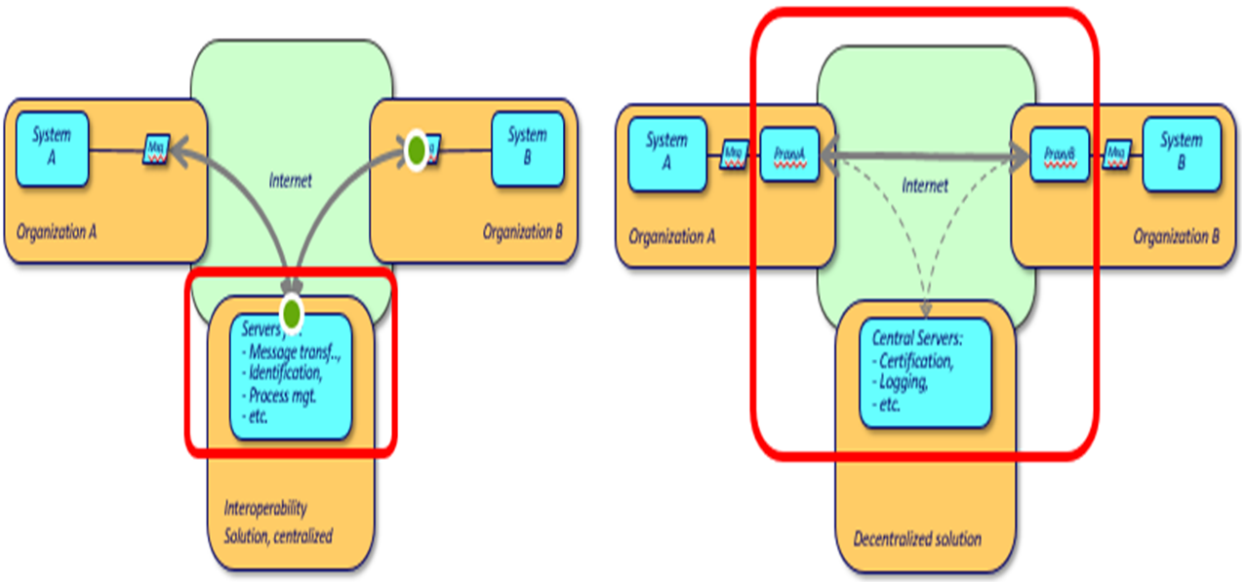

Figure 3 Centralized and decentralized data sharing platform architecture

3.7. Operations

Operations, oversight, management, and maintenance of the infrastructure must be made easy. For the governance agency, as well as for the connecting organizations, smooth operations, monitoring, management, backup/restore, maintenance, upgrades, etc. are mandatory for a 24/7 facility.

3.8. Scalability

Scalability is the capability that allows retaining low transfer times (response times) also when the number of message transfers increases. Scalability can be achieved by replicating the components of the data sharing platform.

Central servers may become a scalability bottleneck. The platform should be scalable without stopping data sharing functionalities.

3.9. Resilience

Resilience is the capability of an infrastructure to retain operations, irrespective of hardware, software or operator faults, or external threats. For a national infrastructure, resilience is one of the key attributes, since any failure to provide 24/7 availability may have large economic impacts. It is unacceptable to have a downtime of the platform for even one minute.

Centralized platforms are more vulnerable, due to their centralized infrastructure, both to internal and to external threats. Message transfers stop when one of the central servers fails, or if taken offline for maintenance or upgrades.

3.10. Security

Security supports identification, authentication, certification, encryption, nonrepudiation, and logging of all message transfers. The presence of end-to-end security properties such as non-repudiation is highly important.

3.11. Support

Optimal internal and external support must be available during the lifetime of the infrastructure.

3.12. Total Cost of Ownership

Cost is always a factor to be considered. However, because the economic value of the interoperability infrastructure is orders of magnitude greater, in this case, cost is less important. It is possible to use established enterprise-oriented solutions that need to be adapted, products from international software companies, or obtain open-source solutions.

3.13. Cross-border data exchange

Secure data exchange between countries is a relatively new challenge, but this criterion could be considered to have a future-proof solutions.

12. The choice of the SDE platform MUST be based on clear criteria.

4. 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, which is based on best practices, is domain neutral and, occasionally, has a focus on a particular aspect.[8]

According to the TIF interoperability model we distinguish four layers of interoperability: legal, organizational, semantic, and technical. In sections below we describe the key architectural building blocks (ABB) needed for these layers.

4.1. Legal view

Listed below are the IT areas where new legislation needs to be created and existing legislation needs to be supplemented/improved:

(1) Freedom of Information Policy

(2) Electronic Transactions Act

(3) Electronic identification (eID) and ecosystem of Public Key Infrastructure (PKI): similar act to the eIDAS regulation on electronic identification and trust services for electronic transactions in the European Union

(4) Regulation about registries (rules for management registries, registry of registries)

(5) Secure data exchange regulation

(6) Legislation on data protection

(7) Regulation about information security

(8) Tonga Interoperability Framework

13. New legislation MUST be created for SDE implementation, and existing relevant legislation MUST be reviewed.

4.2. Organizational view

The SDE ecosystem consists of a SDE Operator, member organizations, and trust service providers as depicted in Figure 4.

SDE operator. The operator is responsible for all the aspects of the operations. The responsibilities include defining regulations and practices, accepting new members, providing support for members, and operating the central components of the SDE software.

14. The Ministry of MEIDECC MUST create a team capable of creating and operating the SDE.

[8] https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/chapter-2-key-concepts-and-archimater-notation

SDE members are organizations that have joined the ecosystem and produce and/or consume services with other members. A member organization can be a service provider, a service consumer, or both. Organizations can become members of an ecosystem by completing the onboarding process defined by the operator. Also, members need to have access to the technical component that is required for exchanging messages via the SDE, the Security Server/Gateway.

15. Public bodies responsible for providing and/or consuming e-services MUST be capable to connect their information systems with the SDE ecosystem. Service providers MUST be capable to open their e-services to the other members. Service consumers MUST be capable to consume the e-services of the other members.

Trust Service Provider(s). A functioning SDE ecosystem requires two types of trust services: 1) a time-stamping authority (TSA) and 2) a certification authority (CA). Trust Service Providers are organizations providing these services. Trust Service Providers may be commercial third parties, or the services can be provided and maintained by the SDE Operator.

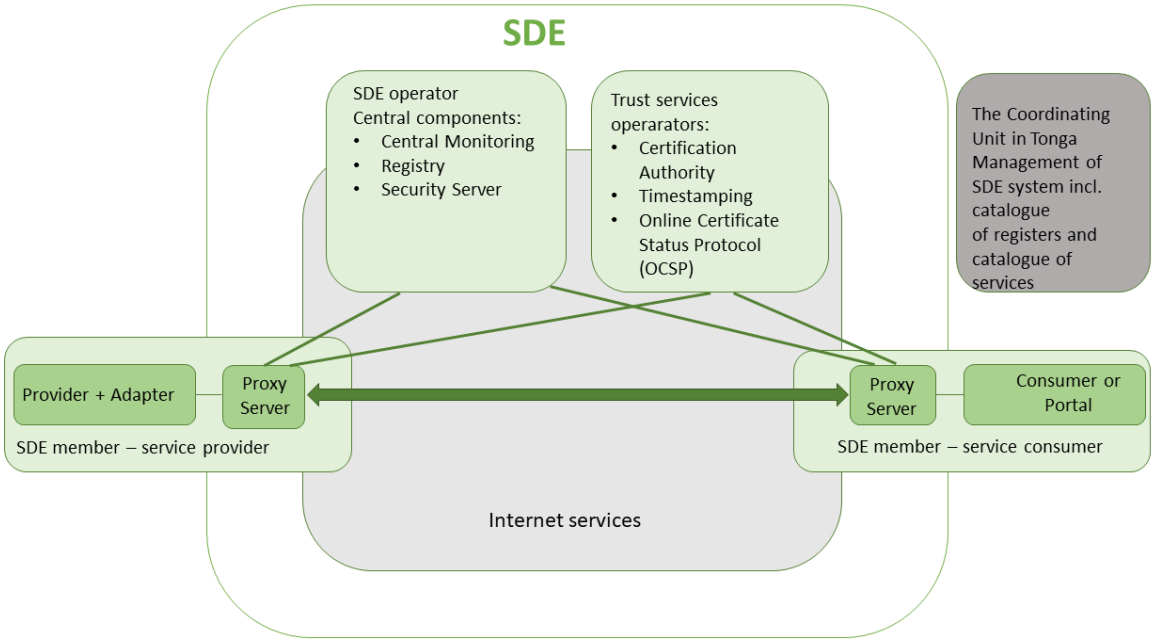

Figure 4 Organizational model of SDE ecosystem

16. The Ministry of MEIDECC MUST create the capacity of the SDE ecosystem to use the services of an existing certification authority or provide and maintain CA services itself.

17. The Ministry of MEIDECC MUST create the capacity of the SDE ecosystem to use the services of an existing time-stamping services or provide and maintain time-stamping services itself.

Organizational activities:

1. Achieve political approval and financing for building the SDE.
2. Clarify organizational relationships for establishing and operating the SDE.
3. Create skills/expertise in organising, implementing, and managing the SDE

4. Create skills in providing and consuming services by MDAs
5. Supervision of information systems/registries over compliance with legislation and the TIF
6. Implementation of the SDE. Setting up the organization (Ministry of MEIDECC) and infrastructure for building and maintaining the SDE platform. Setting up MDAs to join the SDE ecosystem as members of the SDE. Political will, additional financing, increased capability of public bodies, skilled staff, and supervision of information systems MUST be achieved for building SDE.

4.3. Semantic view

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

20. A significant number of government registries and services MUST be digitized.

21. Data policy, base registry policy, reference data policy formulated in the TIF MUST be implemented.

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

23. Public bodies MUST describe their interoperable solutions (information systems/registries, public services, machine services, semantic assets) in a catalogue of interoperable solutions. The Ministry of MEIDECC MUST supervise these processes. The catalogue is used for the management of SDE members and their services.

4.4. Technical view

24. The PKI ecosystem (eID, certification authority, authentication service, signing services, timestamp services, validation services) MUST be developed or made available through third parties.

25. An SDE management and coordination system/tool (including a catalogue of registries/information systems, catalogue of data services, catalogue of public services, catalogue of business processes, catalogue of reference data and semantic assets) SHOULD be established.

26. The Ministry of MEIDECC MUST choose an SDE platform and implement central services.

27. Service providers MUST implement REST and/or SOAP services and make these available in the SDE ecosystem.

28. Service consumers MUST be capable to consume machine-to-machine services provided by the SDE ecosystem.

5. Open Data Policy

The Freedom of Information (FOI)[9] policy provides public access to information held by public authorities. It does this in two ways: public authorities are obliged to publish certain information about their activities; and members of the public are entitled to request information from public authorities. The FOI Steering committee is responsible for the FOI Policy. A specialized FOI Unit functions as the central government unit for implementing the policy. Tonga SHALL update an Open Data policy regularly. Each public body MUST implement the FOI policy within their organization and nominate an Information Officer responsible for processing information requests and liaising with the FOI Unit.

29. Public bodies MUST implement the FOI policy.

The FOI policy is mainly oriented towards traditional procedures. Below we include some recommendations that are related to digital transformation and digital data.

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[10]. These principles will form the foundation for access to data and for the release and use of data:

1. Open by default
2. Timely and comprehensive
3. Accessible and usable
4. Comparable and interoperable
5. For improved governance and citizen engagement
6. For inclusive development and innovation

30. Public bodies SHOULD follow the principles of the Open Data Charter.

To exchange open data, the SDE MAY not be needed. The focus of the open data policy is on releasing machine-readable data for the use by others to stimulate transparency, fair competition, innovation, and a data-driven economy. To ensure a level playing field, the opening and reuse of data MUST be non-discriminatory, meaning that the data must be interoperable so that it can be found, discovered, and processed.

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

[9] Freedom of Information Policy. Kingdom of Tonga, 2012, 44p

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

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.

32. 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.

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

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

33. 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.

6. Abbreviations

Abbreviation	Meaning
ABB	Architectural Building Block
CA	Certification Authority
xGEA	The e-Government Enterprise Architecture
eID	Electronic Identity
EU	European Union
FOI	Freedom of Information
GSN	Government Secure Telecommunications Network
IETF	Internet Engineering Task Force
ICT	Information and communication technology
IP	Internet Protocol
IS	Information System
IT	Information Technology
MDA	Ministries, Departments, Agencies
MEIDECC	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Climate Change and Communications
PKI	Public Key Infrastructure
SDE	Secure Data Exchange
SOA	Service Oriented Architecture
TCP	Transmission Control Protocol
TDGSF	Tonga Digital Government Strategic Framework
TEAF	Tonga Enterprise Architecture Framework
TIF	Tongan e-Government Interoperability Framework
TOGAF	The Open Group Architecture Framework
TSA	Time-stamping authority
TSDF	Tongan Strategic Development Framework 2015-2025
WSO2	Web Services oxygenated. Enterprise integration platform

7. Glossary

Term / acronym	Definition
Aggregate Public Services	A generic term used in the conceptual model for public services to refer to a set of basic public services accessed in a secure and controlled way before being combined and then delivered to end users.
ArchiMate®	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®.
e-Government	e-Government is about using the tools and systems made possible by information and communication technologies (ICTs) to provide better public services to citizens and businesses.
Government Enterprise Architecture (GEA)	The structure of e-Government components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.
Information	Information is semantically enriched data, i.e. collections of data that have been given relevance and purpose.
Interface	An interface is a conceptual or physical boundary where two (or more) independent legal systems, organizations, processes, communicators, IT systems, or any variation/combination thereof interact.
Interoperability	The ability of organizations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between the organizations, through the business processes they support, by means of the exchange of data between their ICT systems.
Interoperability Agreements	Written interoperability agreements are concrete and binding documents which set out the precise obligations of two parties cooperating across an 'interface' to achieve interoperability.
Interoperability Framework	An interoperability framework is an agreed approach to interoperability for organizations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications, and practices.
Interoperability Governance	Interoperability governance covers the ownership, definition, development, maintenance, monitoring, promoting, and implementing of interoperability frameworks in the context of multiple organizations working together to provide (public) services. It is a high-level function providing leadership, organizational structures, and processes to ensure that the interoperability frameworks sustain and extend the organizations' strategies and objectives
Interoperability Levels	The interoperability levels classify interoperability concerns according to who/what is concerned and cover, within a given political context, legal, organizational, semantic, and technical interoperability.

Legal interoperability	Ensuring that organizations operating under different legal frameworks, policies and strategies are able to work together
Open Data	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
Orchestration	The aggregation and sequenced execution of sets of transactions involving use of other services and functionalities, according to business rules embodied in one or more documented business processes, with the ultimate goal of performing or providing some other value-added function or service. Orchestration is closely related to the concept of workflow. Usually, orchestration involves executing a set of processes, described in a standard language, by an 'orchestration engine', which is configurable and capable of executing all the requisite service calls and routing the inputs and outputs of processes according to rules described in that language.
Organizational Interoperability	Ensuring that organizations operating under different legal frameworks, policies and strategies are able to work together
Public Data	Public data is information that can be freely used, reused, and redistributed by anyone with no existing local, national, or international legal restrictions on access or usage.
Public Service	Service can be: A repeatable activity: a discrete behaviour that a component of organization may be requested or otherwise triggered to perform. An element of behaviour that provides specific functionality in response to requests from actors or other services.
Reusability	The degree to which a software module or other work product can be used in contexts other than its original, intended, or main purpose.
SDE Member	SDE Members are organizations that have joined the ecosystem and produce and/or consume services with other Members.
SDE Operator	SDE Operator is responsible for all the aspects of the operations in the SDE ecosystem.
Secure Data Exchange	This is a component of the conceptual model for public services. Its aim is to ensure that all data exchanges are done in a secure and controlled way.
Semantic interoperability	Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'.
Service Orientation	Service orientation means creating and using business processes packaged as services.
Service Oriented Architecture (SOA)	Service oriented architecture is a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects consistent with measurable preconditions and expectations

Standard	A standard is a technical specification approved by a recognized standardization body for repeated or continuous application, with which compliance is not compulsory
TCP/IP	The Internet protocol suite, commonly known as TCP/IP, is the set of communications protocols used on the Internet and similar computer networks.
Technical interoperability	Technical interoperability covers the applications and infrastructure linking systems and services
Tonga Interoperability Framework (TIF)	The agreed approach to the delivery of Tonga public services in an interoperable manner. It defines basic interoperability guidelines in the form of common principles, models, and recommendations.
Trust Service Providers	A functioning SDE ecosystem requires two types of trust services: 1) time-stamping authority (TSA) and 2) certification authority (CA).