national ICT interoperability framework
Table Of Contents

Executive Summary ........................................................................................................................................................................... 4

1 Introduction To The NIF ........................................................................................................................................................................... 6

    1.1 Purpose ............................................................................................................................................................................................................ 7

    1.2 Challenges And Opportunities ........................................................................................................................................................................... 7

    1.3 Objectives And Key Principles ........................................................................................................................................................................... 8

    1.4 Scope And Applicability ........................................................................................................................................................................... 8

        1.4.1 Information Systems Framework (ISF) ........................................................................................................................................................................... 9

        1.4.2 Information Technology Strategic Plan (ITSP) ........................................................................................................................................................................... 9

        1.4.3 Ict Governance Framework ........................................................................................................................................................................... 9

        1.4.4 Compliance Management Framework ........................................................................................................................................................................... 9

    1.5 Main Definitions ........................................................................................................................................................................... 9

        1.5.1 Public Services ........................................................................................................................................................................... 9

        1.5.2 Interoperability ........................................................................................................................................................................... 10

        1.5.3 Interoperability Agreements ........................................................................................................................................................................... 11

    1.6 European Interoperability Framework Overview ........................................................................................................................................................................... 11

    1.7 Based On Best Practice ........................................................................................................................................................................... 11

    1.8 NIF Structure ........................................................................................................................................................................... 12

2 Interoperability Architecture ........................................................................................................................................................................... 13

    2.1 Introduction ........................................................................................................................................................................... 13

        2.1.1 Visualising The Public Service Architecture ........................................................................................................................................................................... 13

        2.1.2 European Interoperability Architecture ........................................................................................................................................................................... 14

    2.2 Multilateral Agreements And How They Help To Improve Interoperability ........................................................................................................................................................................... 15

        2.3 Share, Discover And Reuse ........................................................................................................................................................................... 16

        2.4 Standardisation ........................................................................................................................................................................... 16

        2.5 Trusted Exchange Of Information ........................................................................................................................................................................... 17

    2.6 Presenting The Interoperability Architecture ........................................................................................................................................................................... 18

        2.6.1 Describing The Building Blocks ........................................................................................................................................................................... 19

        2.6.2 Governance ........................................................................................................................................................................... 20

3 Organisational Interoperability ........................................................................................................................................................................... 21

    3.1 Introduction ........................................................................................................................................................................... 21

    3.2 Business Process Interoperability Principles ........................................................................................................................................................................... 22

    3.3 Service Attributes ........................................................................................................................................................................... 22

        3.3.1 Start By Identifying Contact Points ........................................................................................................................................................................... 23

4 Semantic Interoperability ........................................................................................................................................................................... 24

    4.1 Introduction ........................................................................................................................................................................... 24

    4.2 Key Drivers For Semantic Interoperability ........................................................................................................................................................................... 25

        4.2.1 Data Provisioning Principles ........................................................................................................................................................................... 25

        4.2.2 Accredited Data Services ........................................................................................................................................................................... 25

    4.3 Semantic Interoperability Assets ........................................................................................................................................................................... 26
4.3.1 What Are Data Standards? .........................................................................................................................................27
4.4 Organisational Support ........................................................................................................................................................27
4.5 The International Dimension .............................................................................................................................................. 28
4.5.1 Semantic Initiatives Promoted Through The Joinup Platform ................................................................................28
5 Technical Interoperability .............................................................................................................................................................29
5.1 Introduction .......................................................................................................................................................................... 29
5.2 Qualities Of A Technical Standard ......................................................................................................................................29
5.2.1 Openness In Standardisation.....................................................................................................................................30
5.2.2 Selection Criteria ..........................................................................................................................................................31
5.3 Adopted Specifications Catalogue ...................................................................................................................................... 31
5.3.1 How Are Adopted Specifications Classified? .............................................................................................................32
5.3.2 Contextualising Specifications Using Interoperability Profiles ................................................................................32

Appendix A Different Types Of Common Infrastructure Services .............................................................................................. 34

LIST OF FIGURES
Figure 1 NIF key principles.............................................................................................................................................................8
Figure 2 Service Types....................................................................................................................................................................9
Figure 3 Interoperability Levels...................................................................................................................................................10
Figure 4 The 12 EIF Principles .....................................................................................................................................................11
Figure 5 Public Service Architecture Domains...........................................................................................................................14
Figure 6 Bilateral vs. Multilateral Agreements ...........................................................................................................................15
Figure 7 Interoperability Architecture .....................................................................................................................................19
Figure 8 Organisational Interoperability........................................................................................................................................22
Figure 9 Syntax versus Semantics..............................................................................................................................................24
Figure 10 Infrastructure Services Categories...............................................................................................................................32

LIST OF TABLES
Table 1: Interoperability Agreements ............................................................................................................................................18
Executive Summary

Over the past two decades, technological progress has accelerated at an unprecedented rate introducing newer opportunities for citizens to interact with Governments. Mobility is now a reality; the use of social networks has become part and parcel of our daily chores, and for professionals from different walks of life to exchange their accumulated knowledge.

Concepts like the one-stop shop, eGovernment and Gov 2.0 are seen as transformative catalysts that enable collaboration, innovation and participation; bridging the interaction of public officers and citizens alike.

On the other hand, information systems tend to reflect the technologies, ideas and contexts that were key influencers during their respective establishment. Whilst a degree of evolution is common, ensuring that information systems are up to date is not a trivial task. Perhaps more importantly, the ability to integrate the various information systems which can exhibit varying degrees of isolation is considered even more challenging.

In fact, from a number of initial observations, the majority of public sector organisations will either need to introduce necessary enablers within respective information systems or create additional external layer(s) of intelligence intended to expose their business services and/or base data registers via a more approachable web oriented or service oriented means.

To this extent, one of the primary objectives of the National ICT Interoperability Framework (NIF) is to facilitate a strong vision of a connected Government through the alignment of departmental business processes, the standardisation, discovery and reuse of ICT assets and a continuous rigour in improving the level of trust in the services provided by the public sector.

During the articulation of this NIF, the European context was duly considered by incorporating the principles and recommendations of initiatives such as the European Interoperability Framework, European Interoperability Strategy and the Semantic initiatives promoted through the European Commission’s Joinup platform. The building blocks that are proposed are based on international best practices and experience acquired from 20 years of continuous ICT investment.

The NIF relates to other complimentary initiatives developed by the Malta Information Technology Agency (MITA) that specifically deal with the development and support of public services including, but not limited to, the Information Systems Framework, the Information Technology Strategic Plan, the ICT Governance Framework and the Compliance Management Framework.
The NIF also provides a series of tools and guidelines to support public sector organisations in undertaking interoperability initiatives as follows:

- **Chapter 1**: Introduces the purpose, objectives and key principles for the NIF, and defines the main definitions used throughout;

- **Chapter 2**: Draws a conceptual model of an Interoperability Architecture that identifies key interoperability agreements across the public sector to reduce the interoperability gap in a connected Government paradigm. This chapter sets the scene for more in depth organisational (business processes), data (semantic) and technical discussions in the next chapters;

- **Chapter 3**: Presents a number of organisational interoperability principles and recommends service attributes which contribute in designing interoperable business processes;

- **Chapter 4**: Introduces concepts of semantic interoperability and identifies steps towards the standardisation of Government’s data assets in this context. This includes the relevant consideration for evolving data into meaningful and reusable information;
1. Introduction to the National ICT interoperability framework

1.1 Purpose
MITA assists the Maltese Government in its vision towards evolving Malta into a world class information society and economy, nurturing the growth of a strong knowledge workforce and transforming public services through innovation with a continued drive towards excellence.

The current MITA Strategic Plan\(^1\) addresses this mission by establishing five Strategic Priorities (SPs):

**SP 1** To lead ICT strategy development and drive the deployment of an ICT Governance Framework within public sector

**SP 2** To deliver and sustain a robust, resilient and secure ICT infrastructure and IT services to Government

**SP 3** To transform public service delivery through the application of ICTs

**SP 4** To enable the growth of the knowledge economy through the engendering of a life-long ICT learning framework

**SP 5** To deliver quality of life improvements through innovative citizen-centric application of ICTs.

Within the scope of the second Strategic Priority (SP2), MITA has identified the need to establish a rigorous interoperability framework to be adopted across all systems deployment in Government.

It is the intention of this first iteration of the National ICT Interoperability Framework to guide the public sector in maximising the benefits and reducing the cost burden derived from all technology investments by introducing ICT resources that are flexible, reusable and interoperable.

\(^1\) MITA Strategic plan 2009-2012 can be found at: http://bit.ly/IKCBMT
MITA provisions and manages a variety of over 400 live information systems for the Government of Malta. The architecture that these information systems are modelled upon vary considerably and include traditional terminal based approaches, client/server applications and web based implementations; reflecting the technology trends and business needs of over 20 years of continuous ICT investment. MITA also provides dedicated Government owned Data Centres and networking infrastructures to connect the various ministries and departments.

A number of these information systems and their underlying infrastructures are already sharable, to varying degrees. A number of others were not designed with interoperability in mind, reducing their potential effectiveness.

When one takes into perspective how public services have been linked across relevant boundaries, it becomes evident that a considerable number exhibit technology and business process dependencies which are, today, not considered the most effective, introducing a number of limitations within the established relationship. This architecture brittleness is commonly associated with the interoperability schemes in place that are being employed to integrate these information systems together. Other than the technical inter-operation requirements, new and innovative public services increasingly require information or services that span multiple domains. Furthermore, basic service discovery opportunities as well as the approaches associated with effectively making use of them are also required. Once more, this is considered as a key perspective of interoperability – another reason why at a pan-European level interoperability continues to garner increased attention and effort.

From this specific perspective, EU wide public services are a clear indication that public sector organisations will soon need to expose base data registers and services to each other and to EU administrations. Initial observations show that the majority of organisations will either need to introduce the necessary enablers within their information systems or create additional external layer(s) of intelligence intended to expose their business services and / or base registers.

The National ICT Interoperability Framework (NIF) is driven by the following objectives depicting the desired state of play of interoperable public services:

1. Shared and reusable ICT assets owned by the public sector are discoverable and can be used by public services with minimal effort;
2. Public services are deployed on a flexible architecture centred on business needs and provided through standardised approaches and capabilities so as to reduce dependencies on specific vendors, technologies and practices. In turn this promotes:
   a. a level playing field so that multiple vendors can fairly compete on the feature set and performance levels of their products;
   b. a wider selection during the acquisition process which may allow for improved business continuity and exit strategy scenarios whilst keeping in view of the required performance levels and functional capabilities;
   c. the ability to take advantage of pre-established international best practices that have already been applied by other EU Member States;
3. Public services mediate business processes by offering user-centric and one-stop shop services;
4. Inter-connectivity and information sharing between solution constituents, public services and EU-wide implementations is transparent, secure and trustworthy;
5. Citizens can, at any point in time, request and make use of public information.
Interoperability objectives can be summarised using four principles which are at the heart of this first iteration of this initiative. Represented pictorially in Figure 1, these principles are described in Chapter 2.

Figure 1 - NIF key principles

1.4 Scope and Applicability

This document is mostly applicable to public officers involved in defining:
- ICT strategy for the public sector;
- Citizen facing public services together with their respective back office processes and ICT constituents.

The NIF offers guiding principles that contribute in taking the public sector a step further in increasing interoperability among public services. It should be taken into account when making decisions on public services that support a connected Government.

This version of the NIF will mostly focus on the identification of technical enablers for the exchange of meaningful information and the ability to reuse existing ICT resources. It considers organisational challenges, but does not directly take into consideration the legal perspective of public services.

The NIF also takes into account the European context by adopting the definitions and introducing the principles and recommendations issued by the European Interoperability Framework (EIF) as directed by the European Interoperability Strategy (EIS).²

The NIF also serves as a complimentary document to initiatives developed by MITA that specifically deal with the development and support of public services including, but not limited to, the Information Systems Framework and the Information Technology Strategic Plan.

This document does not present policy, regulation and/or compliance perspectives as these fall directly within the ICT Governance and the Compliance Management Frameworks respectively. Related policy documentation is issued separately on the GMICT Policy portal³ to compliment the framework’s guidance.

² Both these activities fall under the EU’s Interoperability solutions for European public administrations (ISA) programme which can be found at: http://ec.europa.eu/isa

³ Policy documents are published online through the GMICT Policies section of the MITA web portal
The primary objective of this framework is to describe the information system landscape of Government. It provides a basic set of indicators which specify best practices and patterns that can be applied to ensure smooth integration between the various horizontal and vertical solutions. This should enable quicker and additional service orchestrations which introduce the additional value added services from current investments. In this context, it is important that the necessary governance parameters, roles and responsibilities are clearly articulated. The Information Systems Framework provides a set of key guidelines to this extent as well.

The ITSP identifies the main technology challenges faced by the public sector, discusses the most relevant technology trends, and presents a high-level information technology strategy and explains how that strategy will drive specific activities.

This document focuses on a set of principles, processes and stakeholders related to the ICT Policy Management Lifecycle for the Government of Malta, that is the compilation, authorisation, publication, ongoing monitoring and review of GMICT Policy. The framework establishes proactive and reactive measures to verify the controls defined within established GMICT Policies. It mainly relates to high level areas of applications, people, infrastructure and information assets.

In this context, public services refer to “Services supplied by the public sector to Maltese and European businesses and citizens.”

A public service delivers ‘business functionality’, provided by an ICT system to support one or more business processes, which is tangible from an end-user perspective. As seen in Figure 2, any given public service is supported by infrastructure services.

An infrastructure service is a generic ‘technical feature’ of a system that supports the delivery of one or multiple business services and which is not normally directly accessible by end-users.

A service (business or infrastructure), has one or more service features. A feature is a distinctive characteristic of a service.

A system has one or more components that implement the features required from a public or infrastructure service.

---

1.4.1 Information Systems Framework (ISF)

1.4.2 Information Technology Strategic Plan (ITSP)

1.4.3 ICT Governance Framework

1.4.4 Compliance Management Framework

1.5 Main Definitions

1.5.1 Public services

4 Many of these definitions can be found in the GMICT Vocabulary (GMICT X 0003:2011) which serves as a common resource for ICT policy documents published by MITA
1.5.2 Interoperability

The NIF approaches interoperability within the context of public services delivery. In doing so, it acknowledges that interoperability touches on a number of viewpoints and levels of detail which are relevant to different people in different ways.

From a wider perspective, Interoperability can be defined as follows:

"Interoperability, within the context of public services delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems."

The EIF describes four key levels of interoperability, i.e. legal, organisational, semantic and technical.

The Political context is considered as a necessary backdrop to the more detailed levels of interoperability. Political support and sponsorship is required when cross-sectoral visions and strategies need to be harmonised for the elaboration of new public services.

Legal interoperability deals with the legal validity of exchanged information across the public sector and the EU.

Organisational interoperability aligns the goals and objectives of the business processes that support public services delivery.

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. Semantic interoperability encompasses the following aspects:

- 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;
- describing the exact format of the information to be exchanged in terms of grammar, format and schemas.

Technical interoperability covers the technological aspects of linking information systems. It includes aspects such as interface specifications, interconnection services, data integration services, data presentation and exchange, etc.
As defined by the EIF, “interoperability agreements are concrete and binding documents which set out the precise obligations of different parties cooperating across an ‘interface’ to achieve interoperability.”

Interoperability agreements can be present at all levels of interoperability, and thus are used as the basis for the conceptualisation of interoperability architecture (discussed in Chapter 2).

The EIF addresses a number of key issues for the efficient and effective delivery of European public services. It does so by providing:

- 12 underlying principles of good administration that are relevant to the process of establishing European public services (see Figure 4);
- 25 recommendations that address specific interoperability requirements;
- A conceptual model for public services that establishes the practice to reuse basic services to build aggregated services;
- A description of the interoperability levels described in Figure 3;
- The concept of interoperability agreements, formalised specifications and open specifications;
- Governance measures and coordination activities.

The 12 principles of the EIF can be broken down into three categories:

- The first principle sets the context for EU action on European public services;
- The next group reflect generic user needs and expectations (2–8);
- The last group provides a foundation for cooperation among public administrations (9–12).

Public officers are invited to familiarise themselves with the EIF’s principles and recommendations to ensure a more harmonised approach in developing cross-border public services7.

Current research trends establish that many interoperability frameworks developed within the EU specifically deal with standards and specifications that address a number of technical challenges.

These frameworks also consider the promotion of semantic efforts to identify and understand the meaning of Government’s data as crucial.

7The EIF can be found on: http://ec.europa.eu/isa/
The following best practices have been identified and considered as a baseline for the articulation of this NIF (the list does not depict any particular order of preference):

- A catalogue that lists technical specifications that are adopted by their respective Government (such as the UK e-GiF\(^8\) and the Australian Technical Interoperability Framework\(^9\)),
- The processes that govern how these specifications are adopted (such as the selection process for the open standards list in the Netherlands\(^10\)),
- The documentation of scenarios in which these specifications should be used by solution providers (such as the Danish Security Assertion Markup Language (SAML) 2.0 Interoperability Profiles\(^11\)),
- The governance context surrounding the use of a given specification or service (such as the Danish classification of standards within a specific area of applicability\(^12\)),
- Products or Services accredited for use in defining solution architectures (such as The Open Group Architecture Framework (TOGAF)’s Standards Information Base\(^13\)),
- A catalogue that lists reusable data assets and their formal structure / schema and ontologies (such as the UK Data Standards Catalogue \(^14\) and the Estonian Instructions for the Semantic Description of Databases and Operations Performed by Databases\(^15\)),
- The European Interoperability Infrastructure Services study\(^16\) (used for the determination of the infrastructure services most valuable for reuse across the EU);
- The development of a European Interoperability Architecture, Trusted Information exchange platform and the Semantic initiatives promoted through the Joinup platform\(^17\) (discussed at the ISA\(^18\) working groups).

While this first chapter gave an introduction to the NIF initiative, the next will approach the highlighted objectives as follows:

- Chapter 2: Draws a conceptual model of an Interoperability Architecture that identifies key Interoperability Agreements across the public sector to reduce the interoperability gap in a connected Government paradigm. This chapter sets the scene for more in depth organisational (includes business processes), data (semantic) and technical;
- Chapter 3: Presents organisational interoperability principles and recommends service attributes which contribute towards the design of interoperable business processes;
- Chapter 4: Introduces the concept of semantic interoperability and identifies steps to discover and standardise Government’s data assets. This chapter contributes in evolving data into meaningful and reusable information introducing, among other things, data provisioning principles, typical characteristics of reusable data and potential sources for reuse;
- Chapter 5: Defines a standardisation approach to technical interoperability, including contextualisation through Interoperability Profiles.

---

**1.8 NIF Structure**


\(^11\) Denmark’s SAML 2.0 profile, http://digitaliser.dk/resource/355488

\(^12\) Denmark’s Catalogues and NIF, http://digitaliser.dk/kataloger

\(^13\) Open Group’s Standard Information Base, http://www.opengroup.org/sib.htm

\(^14\) UK’s Data Standards http://bit.ly/mPxoQa


\(^17\) http://joinup.ec.europa.eu/

\(^18\) Interoperability Solutions for European public administrations (ISA), http://ec.europa.eu/isa
2. Interoperability Architecture

2.1 Introduction

This chapter proposes the first iteration of an Interoperability Architecture that will contribute towards achieving the objectives highlighted in Chapter one.

To start with, formal architectural terminology is used to determine the main constituents of a public service; this is the same language used to position public services in relation to Government’s overall Enterprise Architecture.19

Subsequently, the key interoperability principles are explored in more detail, leading to the identification of the Interoperability Agreements most relevant for the public sector. The agreements are implemented through supporting services, among which, are a series of shared infrastructure and data services that are common for public services. The overall depiction of the agreements into the relevant actions is what constitutes the Interoperability Architecture.

The implications of the identified services highlighted in this section are explored in greater detail in the following three chapters.

2.1.1 Visualising the public service architecture

The public service architecture (the major consumer of interoperability initiatives) can be visualised using TOGAF’s20 widely accepted architecture domains for enterprise architecture, namely Business, Data, Application, and Technology Architecture.

---

19 More information can be found in the Enterprise Architecture section of the MITA web portal

20 TOGAF is a framework - a detailed method and a set of supporting tools - for developing an enterprise architecture. It may be used freely by any organisation wishing to develop an enterprise architecture for use within that organisation. It is found at http://www.opengroup.org/togaf
The intention of the enterprise architecture is to:

- drive the continuous alignment of the adoption and use of technology with the Government’s business objectives and strategic direction;
- describe the current and future state of an Government’s business processes and technology implementations;
- provide an overall plan for designing, implementing and maintaining the underlying infrastructure to support the transition from the current to the future state.

While the enterprise architecture depicts the whole Government, in this context, a public service architecture represents a “solution-specific” architecture that deals with the necessary building blocks required to offer the service in question. Apart from incorporating the various public services and their underlying ICT constituents, the enterprise architecture identifies common and shared solutions that can be used by the various public services.

In order to facilitate the transformation to a connected Government, it is useful to determine the key responsible owner or custodian for each aspect of a public service and as much as possible to harmonise the decisions made for each domain.

The four architectural domains are being used to link, the interoperability requirements and expectations of public services, with the most appropriate interoperability agreements that are available across the public sector.

The European Commission (EC), through the Interoperability Solutions for European Public Administrations program (ISA)\(^2\) is prioritising a number of common interoperability agreements required for the realisation of a European Interoperability Architecture (EIA). While the focus of this exercise is for cross-border European public services, the rational for identifying and prioritising interoperability agreements are still very relevant for local use.

---

2\(^{2}\) ISA is located at http://ec.europa.eu/isa
The analysis takes a bottom-up approach by studying “real life” solutions, together with a top-down approach that conceptualises the findings in a reusable model using formal paradigms (such as the TOGAF’s architectural domains) to classify the agreements.

Eventually these agreements will be used by the EC to create common frameworks, generic tools and common services that can be used to reduce cost associated with European public services through reuse and more effective inter-operation.

Complimentary to the interoperability agreements are a set of “common infrastructure services” which have been identified in most European public services. Annex A provides a description of the common infrastructure services identified by this study, i.e. audit trail and log, service registry, identity and access control, data certification, data transport, data translation, workflow management, document storage, and structured data storage.

From this list, the vision for an EIA prioritises the ones with the highest relevance at a European level. The two services which garnered most attention are identity and access control and data certification, two services required for the trusted exchange of cross-border information. While the latter will most likely be implemented centrally by the EC, other services being closer to the specific needs of public services (such as data translation), seem to prefer a more localised implementation.

Knowing which infrastructure services are always present in public services helps in prioritising which standards the public sector needs to develop and adopt.

More information on how infrastructure services are relevant to technical standardisation can be found in Chapter 5.

2.2 Multilateral agreements and how they help to improve interoperability

Within any singular instance of a public service, interoperability is not a major concern especially when the solution deployed is developed and maintained by the same team of people. However when a public service spreads across organisational and/or sectoral boundaries, agreements usually need to be established to formalise the obligations and expectations of the parties involved. In turn, these have a cascading effect on the underlying process workflows, application interfaces, data packaging requirements and communication protocols that need to be established to satisfy the interoperability needs of the respective layers.

In a multi-actor environment, one way to achieve this type of interoperability is to establish separate bi-lateral agreements and solutions for each exchanging partner. The net effect (and disadvantage) of such an approach is that it potentially requires as many communications/links as there are external partners, resulting in reduced efficiency and higher costs.

Figure 6 - Bilateral vs. Multilateral agreements

---

22Identified through the European Interoperability Infrastructure Services study
If each of the interoperating partners adopts the same set of agreements for interoperating solutions, each can reap the benefits of a single solution that is developed once and fits the needs of all with minor amendments if any.

ICT solutions based on multilateral agreements can be viewed as shared or common services of a generic nature which meet common user requirements across multiple sectors and policy areas. It is a consumable service that can be used without modification, in support of the implementation of the Public service being offered.

An example of a common service (from a technology perspective), provided and managed by MITA, is MAGNET; the Government’s own private IP-based network. MAGNET offers a telecommunications interconnection platform that responds to the growing need for secure information exchange between public sector organisations.

On the other hand, a reusable generic tool is a component that can be used to produce a system or part thereof. Normally, it needs customisation to meet specific needs. It is reusable across multiple sectors and it is usually not a service.

An example of a platform promoting generic tools is the European repository for open source software and best practices within the Joinup platform (previously known as OSOR23). Some of these components are licensed under the European Union Public Licence (EUPL). Joinup and EUPL assist, among others, public administrations to share and reuse software components or to collaborate on the development of such components.

Both types of reuse can facilitate all the layers and dimensions of Government’s architecture. They can help reduce the cost of public services and are therefore acknowledged and promoted as vital considerations for interoperability agreements.

To be effective such services and tools need to be:

1. Created with reusability in mind and are shared by their owners;
2. Discoverable by and meaningful to their consumers.

There are also plenty of opportunities for reuse beyond our borders. International best practice, data schemas and even entire software solutions can be found from reputable sources and adopted as-is or with minor modifications.

While ICT solutions derived from shared services and generic tools help reduce the cost of public services, from a technical perspective, standardisation is acknowledged as a key contributor to the realisation of a truly sharable and connected Government.

Standardisation helps to create common baselines and understandings by referring to accredited specifications created by field experts for challenges which are common among a particular sector or technical area.

Semantic awareness and technical standardisation are discussed in more detail in chapter 4 and 5 respectively. Suffice to say that the discovery of which standards could (or even should in certain cases) be used in specific scenarios can add a lot of value when defining public services.
Trust is considered as one of the key elements that enable effective, governed and sound inter-operation; it is however not an implicit quality. Trust management addresses relationships between entities within organisations, security domains, and systems amongst others. These relationships can be system-to-system, business-to-business, and so on. In the context of the NIF, trust management mostly deals with three aspects: organisational (includes business process), data and technology.

The organisational aspect deals with the scenario where entities agree upon a set of rules to conduct business. These rules include relationship management, liability management, and other legal and contractual aspects. Relevant business processes and policies are necessary for establishing trusted relationships. These processes might include choosing a legal procedure to follow and the process used for evaluating liability. This process might also include the policies specific to resource access. These policies often already exist as part of the business arrangement between a public sector organisation and its business partner.

The Data aspect deals with agreements on the terms and conditions for collectors, custodians and consumers of data. Data quality metrics include accessibility (the extent to which data is available or retrievable), credibility (the extent to which data is regarded as true and credible), completeness (the extent to which data is not missing and is of sufficient detail for the required task), relevancy (the extent to which the data is applicable for the required task), etc.

The technology aspect of trust management deals with managing the infrastructure that supports the capability for establishing trust by, among other things, utilising cryptographic methods. These include key management (strength, key validation, and so on) protocols, attributes, and other technical considerations for establishing trust.

Ultimately, as a multi-faceted characteristic, trust is earned by providing a desired level of assurance to collaborating parties that instil a sense of reliability and security. The following technical features exemplify such expectations:

- Any sensitive information (whether it is personal or technical/internal data) is protected against eavesdropping;
- Data cannot be modified during transmission;
- Any interacting entity (citizen, system, machine, etc.) is authenticated;
- Any information transmitted or presented is valid at the time it is transmitted or presented;
- Users are able to see the exact information that will be transmitted, the exact origin and destination of this information;
- Personal information revealed should be the minimal needed for the purpose of the service provided;
- It is possible to identify uniquely each entity (citizen, system, machine, etc);
- It is possible to trace actions performed on the system.

While trust features are required in all data exchange scenarios, the level of assurance is dependent on factors that can be determined by participating parties. Common services implementing trust features should therefore be designed to accept multiple levels of exchange scenarios that provide practical implementations without jeopardising the quality and performance of the involved services.

To mitigate this potential risk, trust features which are common to the majority of the parties involved are more often then not delegated to trusted parties as centralised infrastructure services. Similarly to the findings of the EIA (discussed in Section 2.1.2), identity and access control and data certification are perceived as ideal candidates for centralised common services.
The following Interoperability Agreements represent the constituting building blocks of the first iteration of an Interoperability Architecture.

<table>
<thead>
<tr>
<th>Architecture Domain</th>
<th>Interoperability Agreement</th>
<th>Description</th>
<th>Identified Building Blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>Agreement on the establishment of contact points to govern the technical access</td>
<td>Contact points are representatives of organisations within the public sector that act as mediators between the organisation’s data and services and its other consumers within the public sector. While this falls into the business domain, Contact points should also be aware of the legal frameworks relevant to the Public service in question.</td>
<td>Contact Points</td>
</tr>
<tr>
<td>Application</td>
<td>Agreement on list of solutions and solution components to be reused</td>
<td>A catalogue, or federation of catalogues, for standard software solutions and components which can be reused or shared by multiple public sector organisations for the creation of public services. Reusing components by different parties improves interoperability by harmonizing the differences between components, resulting in a more similar IT Architecture.</td>
<td>Reusable solutions</td>
</tr>
<tr>
<td>Data</td>
<td>Agreement on common semantic schemas at the public sector level</td>
<td>A semantic schema is a model with entities and the relations between these entities. As such, semantic schemas define business objects at the public sector level. To understand the meaning of data, it is important to harmonise the identification of business objects across the public sector.</td>
<td>Schemas Catologue</td>
</tr>
<tr>
<td></td>
<td>Agreement on establishment of catalogue of accredited datasets available for the public sector</td>
<td>Commonly used and reusable data sets can be endorsed by a central clearing house to support the delivery of public services by providing consistent data.</td>
<td>Accredited Data services</td>
</tr>
<tr>
<td>Technology</td>
<td>Agreement for requirements of the trusted exchange of information</td>
<td>Providing the required shared infrastructure services to support the trusted exchange of information between public sector organisations. In order to exchange information, the security aspects such as identification, authentication and authorisation should be aligned between partner organisations.</td>
<td>Sharable Infrastructure services</td>
</tr>
<tr>
<td></td>
<td>Agreement on a common set of formalised specifications for technical connectivity</td>
<td>Formalised specifications which can impact the way public services interoperate can be endorsed by a central body and contextualised for effective use in the public sector. Adopted specifications can also be used in acquisition scenarios as technical requirements.</td>
<td>Adopted Specifications Catalogue Interoperability Profiles Adopted Standards &amp; Services</td>
</tr>
</tbody>
</table>

Based on the identified agreements, Figure 7 presents the key Interoperability building blocks required for an Interoperability Architecture and their relationship with relevant governance functions and external resources.
The next section discusses the overall structure of the Interoperability Architecture.

2.6.1 Describing the building blocks

The Interoperability Architecture identifies centralised, sharable and reusable building blocks classified as Supporting Services, Data Standards and Technical Standards.

Supporting services includes:

- Sharable infrastructure services which benefit from a centralised implementation;
- Solutions which can be reused in part or in full; and
- Accredited data sets that are endorsed for use by the public sector.

Data Standards deal with the semantic rules and guidelines which determine and regulate the meaning of data (more details in Chapter 4).

Technical Standards deal with the adoption and contextualisation of formalised specifications within the public sector (more details in Chapter 5).

For these services and standards to be effective, they need to adopt, or be based on, international best practices from reputable sources. To this extent, the External Resources block represents the various resources that the public sector adopted or intends to adopt in the implementation of the various NIF building blocks. Some of these resources (such as EU Directives) have a legal basis which mandates their use across the EU, while others are best practices which have high reusability value, such as readily available Open Source Software (OSS).
It is important to note that services originating from the public sector should follow the direction and guidance given by the respective Standards catalogue and take the opportunity to use existing solutions and services.

The Public Service Architecture also includes a Contact Points and Adopted Standards & Services block. While Contact Points (more information in Chapter 3) deal with people and their various roles within the organisation, the Adopted Standards & Services block is intended to record information about the centralised building blocks adopted for the solution architecture.

### 2.6.2 Governance

The **GMICT Policy Suite**[^24] is a collection of policies, directives, procedures and standards, managed centrally by MITA, governing the adoption and use of technology within the Government of Malta.

More specifically, an **Interoperability Policy** is used to regulate the building blocks identified by the NIF. In addition, formalised specifications adopted by MITA are also coordinated and governed by GMICT Policies.

The **Architecture Assessment**[^25] process governed by the Enterprise Architecture Policy, among other things, is intended to verify that the Interoperability related building blocks are being used by public services as intended and that the envisaged benefits are in fact being fulfilled.

Public services adopting building blocks as defined by the NIF will only need to describe their use within their solution without the need to explain their technical validity as this analysis would have already been done. For instance a solution proposing the use of SAML 2.0 (a formalised specification already adopted and endorsed by MITA) to request an authentication claim from the Government’s identity repository of public officers can do so immediately.

An added benefit here is that the overall assessment time can be **drastically reduced** if solutions are **standardised** and use **pre-established services**.

The Adopted Standards & Services block can capture where and how the adopted building blocks are used within the public service. Any specialised building blocks (such as formalised specifications which are only relevant to the solution), and international best practices can also be described and linked to the relevant functional component. This mapping gives a deeper understanding on the effectiveness of the chosen building blocks across the Enterprise Architecture and can be used to prioritise actions for the next NIF iteration and for other technical strategies.

[^24]: Policy documents are published online through the GMICT Policies section of the MITA web portal
[^25]: More information about the Architecture Assessment process can be found through the Enterprise Architecture section of the MITA web portal
3. Organisational Interoperability

3.1 Introduction

In an era dominated by web applications, mobile devices and social networks, citizens expect service providers to give them what they want, when they want it, using technologies and form factors they choose. It is seldom important for end users to know that the service they expect is an aggregation of business processes provided from various internal departments; each potentially having different service level agreements and expected outcomes.

The concept of a “one-stop” shop has been discussed on numerous occasions, and through initiatives such as eGovernment, the public sector is opening its doors to the public over the web. Similarly, concepts like Gov 2.0 conceptualises Government as a transformative platform that is collaborative, innovative and participative, bridging the interaction of public officers and citizens alike.

The main challenge that persists in offering new cross-departmental services is that certain technological solutions are based on organisational- (or silo-) based business processes. A silo in this context supports and preserves processes within a rigid structure and organisational controls which are usually not interoperable by nature.

While organisational borders are there for a reason, the underlying processes can still be constructed or extended to allow increasingly seamless dynamic aggregation.

As portrayed in Figure 8, a solution to this challenge is to start treating business processes as “basic services”. Services are created to be used by consumers and are therefore accompanied with service-oriented qualities or attributes (such as service contract and location) which facilitate their consumption. Basic services can then be combined to create “aggregated services” which offer services for cross-boundary processes.

For this to be possible, organisations need to start aligning their business processes, starting with those that can be mapped to cross-boundary life events.
This chapter provides a set of principles intended to improve business process interoperability and recommends a set of potential attributes that could accompany services that are meant to be used by multiple actors.

### 3.2 Business Process Interoperability Principles

The following principles can be helpful for public sector organisations during their planning exercises and when collaborating on processes that cut across organisational and sectoral boundaries:

- Focus on tangible and measurable outcomes by asking questions about “why” and “what” needs to be achieved before thinking about the “how”.
- Consider similar, interrelated and government wide initiatives when planning public services and ensure that the pre-defined outcomes are linked to the organisation’s strategy;
- Always take into consideration the end-user experience when defining services and their underlying ICT solutions;
- Use a common and standardised approach for documenting and communicating business processes with collaborating organisations (facilitators for this principle are the taxonomies and dictionaries discussed in chapter 4);
- When sharing business processes across public sector boundaries, such as between departments, aim to establish trust and confidence by applying pre-determined controls and measures;
- Cross-sector or cross-departmental agreements should be standards based but also practical;
- Introduce awareness and further promote the key importance of public officers for the success of cross-boundary services;
- Prefer multilateral solutions when establishing agreements;
- Introduce “Interoperability capability” and “maturity” as quality criteria for public services and the underlying ICT solutions.

### 3.3 Service Attributes

Service attributes are compiled by service providers and should contain enough information to be usable by multiple actors.

The following descriptive information is a typical set of high-level attributes:

- Identification details (for more information refer to Section 3.3.1);
- Service provisioning policy describing the underlying principles for providing this service, to whom it applies, and for which purposes it is being provided;
- Service quality indicators to describe functional indicators (such as an appreciation of the expected preconditions and envisaged outcomes), and qualitative indicators (such as service level agreements).

When transitioning from a business process approach to a service-oriented model, it
is sometimes preferred to document and preserve service descriptions and attributes in both human and machine readable formats. Models such as W3C’s Web Service Modelling Ontology and Dublin Core Meta Data Element Set are such examples.\textsuperscript{26}

It is important that a step-by-step approach is taken when such a transition is being employed by public sector organisations.

### 3.3.1 Start By Identifying Contact Points

As discussed in Chapter 2, the Interoperability Architecture identifies a vital organisational building block within the public service architecture, i.e. “Contact Points”.

The intention of Contact Points is to identify the public officers who are close to the organisation’s business processes and data assets (more of this in the next chapter), with the intention to establish communication channels among relevant public sector organisations.

This in turn creates a network of “business experts” who can directly contribute towards the creation of cross-boundary services, and eventually opening the door to collaboration opportunities with Maltese citizens, the EU community and the industry.

To start with, organisations are invited to start using a minimal set of attributes to identify business processes across the public sector, such as the following:

- Identifier: An unambiguous reference to the business process or basic service within a given context;
- Publisher (can be referred as Custodian): An entity responsible for making the resource available;
- Providing public body (can be referred as Owner): the public sector organisation that is responsible for the service;
- Contact: the actual Public Officer that should be contacted for a given context, for example technical support;
- Contact email, telephone number or other communication channel: The means with which the Public Officer can be contacted.

Whichever attributes are chosen, it is important that this information is published in a way that is discoverable and searchable by its intended user base.

---

\textsuperscript{26}Existing service attribute definitions for technical services include W3C’s Web Service Modelling Ontology located at http://www.w3.org/Submission/WSMO/ and Dublin Core Meta Data Element Set located at http://dublincore.org/documents/dces/
4. Semantic Interoperability

4.1 Introduction

While organisational interoperability facilitates the interoperable execution of administrative operations and procedures, semantic interoperability is the ability of organisations to understand the exchanged data in a similar way.

Figure 9 illustrates how a syntactically understandable word <plant> can still be misinterpreted due to multiple possible meanings.

For two or more systems to understand and interpret data in a similar way, that data needs to be formally described in terms of an expected structure and a set of common terms and definitions that reduce contextual discrepancies.

Data tends to have a longer lifetime than the software components of a typical information system. Technically speaking, data can be consumed through numerous ways including pre-established application interfaces, directly at source (e.g. relational database), or exported from system to system.

Data has also a deep affiliation with the business process, life-events and legal frameworks that surround its lifecycle. It is this deep connection with what the public sector wants to achieve that data should be treated like an important resource, avoiding situations where its integrity and usability is jeopardised.

It is therefore quite clear that data has to play a central role in creating innovative public services, even more so when data is transformed into a semantic asset which can be made available to the public sector, EU community, citizens and the industry.
This chapter discusses some of the drivers and principles required for the continuous transitioning of traditional data management practices to semantic interoperability approaches. It also explains the rationale for creating the data relating building blocks identified in Chapter 2, i.e. Schemas, Data Standards Catalogue and Accredited Data Services.

4.2 Key drivers for Semantic Interoperability

The main drivers for the transition to semantic interoperability are as follows:

- Decision making is based on data that is increasingly more accurate;
- Improved data reuse;
- Improved integration opportunities;
- Increased sustainability of the consuming application or information system.

As a first step to reach these objectives, the public sector is invited to consider the Data provisioning principles and Accredited Data Services provided in the following sections.

The more long term transition to semantic interoperability is facilitated by the approaches discussed in section 4.3.

4.2.1 Data provisioning principles

The effective management and distribution of data across government can result in information being used more efficiently and effectively. The following data provisioning principles have been identified as key considerations that can lead to an effective information sharing lifecycle contributing to a better quality and accuracy of information:

- Data is made available and maintained by the respective legal owner and/or authorised custodian. As much as possible, this should be done directly at source;
- Data operations are mapped to real life event driven processes;
- Citizens, commercial / non-commercial organisations and the European Community are provided with consistent, reliable, secure, trustworthy and reusable data;
- The originally intended data context is applied at the time of provisioning to safeguard the data authenticity and integrity;
- Where Open Specifications that define data persistence, interchange and presentation exist, these must be used;
- Attention is given to European wide activities and directives for relevant principles, methodologies, approaches and guidelines;
- Data services promote automated means for consumption using Service Oriented Architecture principles;
- Data objects (wrapped through services, interfaces or otherwise) have an externally unique object identifier. The scope of uniqueness is defined by the target audience and usage.

4.2.2 Accredited Data Services

Accredited Data Services are commonly used official data sets which have been endorsed for use across the public sector. A list of datasets has already been identified and an exercise is currently ongoing to align and assign each dataset to at least one government function. The next step will be to find the legal and administrative owner/custodian for each dataset.

In 2010, the Data Governance Council was instituted within MITA to serve as a "forum for all data governance related issues, recommendations and decisions".

27 Service Oriented Architectures are architectural styles that package discrete functions as a set of de-coupled, atomic, reusable and shareable services.
One of the first decisions taken by the Data Governance Council was on the definition and scope of the data governance function:

- **Definition** - “The people, processes and technologies, together with the legal instruments and organisational structures required to ensure the availability, accessibility, quality, consistency, auditability and security of the data utilised by the Government of Malta.”

- **Scope** - “All the official records together with the supporting data, structured, semi-structured and unstructured, created or used by the internal or external processes as employed by the applicable administrative functions in line with the relevant Government information systems strategy.”

It is important to highlight that the scope is limited to administrative functions and thus exempts all the data and processes that can be traced to the security forces including police and the military. The same applies to data and records governed under the official secrets act, including cabinet papers.

**4.3 Semantic Interoperability Assets**

As described in section 1.5.2, Semantic interoperability is made up of syntactic interoperability which deals with the structure of data, and semantic interoperability which explains how data should be interpreted.

While the two activities are complimentary, they create different kind of interoperability related assets that the public sector can make use of:

- **Syntactic assets** relate to the Schemas building block (refer to Interoperability Architecture in Section 2.6) and their main role is to define data structures in a formal fashion. This includes schemas (today usually in an XML compatible format) and metadata schemas that determine the data attributes for “core” data assets such as a “person” or a “vehicle”. The syntactic level of interoperability is the first stage in achieving semantic interoperability because it provides a level of formalisation around known data subjects. This is usually achieved by creating asset repositories for common schemas and establishing a public sector wide policy for their use.

- **Semantic assets** relate to the Data Standards Catalogue building block (refer to Interoperability Architecture in section 2.6) and their main role is to provide a central terminology to ensure that data elements are interpreted in the same way by communicating parties. These assets denote information resources that have been created in order to ensure the interoperability of information systems. Semantic assets for semantic interoperability are divided as follows (the division is based on the IDABC working paper IDABC Content Interoperability Strategy[^28]):
  - dictionaries
  - thesauri
  - nomenclatures
  - taxonomies
  - mapping tables
  - ontologies
  - service registers.

Syntactic asset example: Many information systems in the public sector need some basic information about the citizens they are dealing with. A common model can be created to identify those elements that are always present when dealing with personal data. In this way, there is increased opportunity that all participating information systems are referring to the same element.

Semantic asset example: When dealing with business processes or services, it is common that specific functions within a public sector organisation are responsible for the process. To assist in the identification of cross-boundary recognition of roles and responsibility, ontology can be used to describe a common organisational structure for Government.

Data Standards are a formal collection of syntactic and semantic assets that have been officially endorsed by the relevant authority. Once these assets go through a clearing process\(^\text{29}\) that verifies their integrity, maturity and reusability they are ready to be published and made available to the public sector.

Data Standards embed the following characteristics:

- Reuse one data element or operation should be described only once and in any other use the initial description should be referred to;
- Simple and standard\(^\text{30}\) compilation, management and search of the descriptions of data elements and operations;
- Preferably written in both human and machine readable formats.

The technical implementation of syntactic and semantic assets requires the adoption of technical standards such as XML, XSD, WSDL, SA–WSDL, RDF and OWL from the W3C\(^\text{31}\) recommendations, and UML2 and XMI from OMG\(^\text{32}\).

In this case, the Interoperability Profiles (discussed in Chapter 5) would be provided through the Data Standards Catalogue and Schemas.

Semantic interoperability depends primarily on high-quality documentation of repositories (registries / databases), services, applications and ultimately business domains. To reach a mature and stable semantic state, collaborative agreements should be established across the public sector to establish a realistic version of the asset descriptions.

Policies, standards and procedures can be created to centrally coordinate and guide these efforts. An elaboration of dictionaries, thesauri and nomenclatures can be centrally established as a reference point. If necessary references to these semantic assets can also be made in the legislation; making their use mandatory.

\(^{29}\) A clearing process guides the evolution of an interoperability asset along different stages of development. For an example refer to the European Commission's semantic clearing process found at: http://joinup.ec.europa.eu/

\(^{30}\) Compliance with W3C standards and recommendations ensures semantic interoperability at international level, including with regard to relevant EU programmes. See Interoperability between national administrations for pan-European eGovernment services (IP/06/216, 2006-02-23).


\(^{32}\) http://www.w3.org/TR/
The following actions can create an organisational support framework to drive semantic interoperability:

- In all major business domains, expert groups are formed with the task of creating and maintaining the respective business domain’s semantic assets;
- Semantic assets spanning or interacting among multiple domains might require cross-sectoral / cross-domain expert discussions. So while a multilateral agreement can eventually be reached, working groups represented by the relevant ministries / departments can create and maintain instructions on the translation/modification of data objects of one area into those of another area.
- On an international level, the participation in semantic interoperability fora can influence the elaboration of mutual agreements and semantic gateways for the semantic interoperability between information systems of different countries.

Together with the Data Governance Council, public sector organisations are invited to incorporate semantic considerations when developing public services. This will facilitate the gradual transformation of data to value added information.

4.5 The International Dimension

4.5.1 Semantic initiatives promoted through the Joinup platform

The foundations for semantic interoperability at a national level compliment European interoperability initiatives. As a starting point for semantic interoperability with European initiatives, Joinup’s semantic initiatives have been identified as a key horizontal activity that is backed up by the European community at large.

The Joinup platform consolidates the previously known Open Source Observatory and Repository for European public administrations (OSOR.EU) and the Semantic Interoperability Centre Europe (SEMIC.EU) into one consolidated presence. The content of the platform reflects the efforts carried out in the various ISA working groups and activities, which Member States have the opportunity to collaborate in.

Within this platform, a number of semantic related services and guidelines (including coaching) are being provided by the European Commission to enable seamless data exchange across Europe, particularly between public administrations. This is mostly because it is understood and acknowledged that EU Member States have different administrative, technical and linguistic backgrounds and realities.

This particular source provides an open repository of interoperability assets. Following the principle of harmonisation through standardisation, Joinup promotes the reuse of syntactic and semantic assets needed to ensure cross-border semantic interoperability. They are collected, quality checked and made available for download in the Joinup asset repository.

The assets undergo a collaborative clearing process so that other projects and organisations may reuse them. The term “interoperability asset” in the European context describes a resource that supports the exchange of data in distributed information systems, basically data models that help overcome differences in the systems involved in the exchange of certain data.

Data modelling and semantic experts across the Public Sector are invited to:
 a) consider the adoption of interoperability assets from the Joinup platform;
 b) collaborate in identifying and publishing interoperability assets in the Joinup’s asset repository.
5. Technical Interoperability

Technical Interoperability delves into the technological aspects of linking information systems. It includes aspects such as interface specifications, interconnection services, data integration services, data presentation and exchange, etc.

It is becoming increasingly evident that the speedy evolution of technology is influencing the way business is expected to be handled in government. Doing more with less is a continuous axiom from a technology perspective.

To harness this continued evolution and maximise its usefulness, technical interoperability employs tried and tested technical standards (identified by the Interoperability Architecture in Chapter 2) which have the support of the marketplace.

At the same time, technical interoperability is mostly effective when technological objectives are derived from organisational and semantic requirements. Expected business outcomes can be mapped with the most effective interoperability enablers, profiling pre-established scenarios to describe when and how technical standards are useful.

It is the intention of this chapter to discuss the qualities accompanying technical standards (also referred to as formalised specifications\(^{34}\)), with a note on “openness”, and introduce the concept of interoperability profiles to contextualise the use of adopted standards.

5.2 Qualities of a technical standard

Technical standards are particularly important in the IT industry, as they allow products, services, hardware and software to interoperate and work together even though they may be coming from different parties or vendors. Consequently without these standards, users may be forced to use a vendor specific hardware, software or services.

Eventually in the industry, standards increase the levels of quality, safety, reliability, efficiency and interoperability, and provide such benefits at an economical cost.

The Internet which is accessible from almost any type of computing platform and device would not achieve its current ubiquitous presence, if it did not use widely accepted and freely available (as in freedom to use) technical specifications in its networking infrastructure and supported services.

\(^{34}\)The EIF defines formalised specifications as either a standard pursuant to EU Directive 98/34 or a specification established by ICT industry fora or consortia.
While many definitions exist, calling a standard or specification "open" makes a clear distinction against so-called "closed" or "proprietary" standards and specifications which may favour a single vendor or a small group of vendors only. More often then not, Open Standards (as they are usually referred to) are subject to full public assessment and can be used without constraints in a manner equally available to all parties.

Open standards are most of the time intended to be platform independent and / or vendor neutral. This gives implementers and end-users the ability to use the product of choice without impeding on their business needs.

This freedom of choice can still be jeopardised because openness without context can still create unrealistic objectives. For instance, it is not the first time that a technically inferior specification (not necessarily only in ICT) has overshadowed others purely due to reachability. To avoid this, Open Standards must be workable and implementable specifications which are also supported by governments and industry players.

On the other hand, when a standard is critical for the operation of any given process, the level of openness versus the level of capabilities provided by the underlying specification must be considered according to the context in question.

The market is not only made up of completely ‘open’ or ‘closed’ standards; some standards, for example, may require purchase of the specification, restriction to certain fields of use and royalty payments to intellectual property owners. Common types of intellectual property include patents, copyrights and trademarks and may apply differently according to the relevant legal jurisdiction.

Because of this, many countries and organisations have different interpretations, definitions and characteristics to determine the “openness” of Standards and formalised specifications, i.e. there is no single definition since interpretations may vary with usage.
Technical standards need to be evaluated against a number of criteria mostly falling within the following categories:

- **Level of Openness** - gauging the formalised specification’s conformity with “open” characteristics including:
  - All stakeholders have the same possibility of contributing to the development of the specification and public review is part of the decision-making process;
  - The specification is available for everybody to study;
  - Intellectual property rights related to the specification are licensed on FRAND terms or a royalty-free basis in a way that allows implementation in both proprietary and open source software.
- **Relevance to the business context** - gauging the applicability of the technical standard’s features to its scope of use;
- **Market support** - gauging the more practical side of the technical standard by looking at the quality of its implementations, commercially or otherwise, that are readily available for use;
- **Impact assessment** - gauging the extent to which the technical standard is envisaged to be used within Government and therefore what potential benefits and risks it might introduce.

While the consideration to the criteria mentioned above is vital for an effective selection process, the public sector should opt for the use of technical standards which embed “openness” characteristics in their development, implementation and use.

### 5.3 Adopted Specifications Catalogue

The Adopted Specifications Catalogue building block, lists the formalised specifications that the public sector has adopted, or is intending to adopt, in the provision of ICT Solutions. The list is published online through the GMICT Policy Framework. The catalogue is accompanied by a procedure describing the adoption process. An adoption template is available for the public sector, citizens and the industry to be able to request the consideration for the adoption of a formalised specification. All forms are evaluated and endorsed centrally by MITA.

Within this initiative, the Adopted Specifications Catalogue facilitates the adoption of formalised specifications which can drastically improve interoperability within the public sector (see following section for more details). The public sector is therefore invited to take advantage of adopted specifications as defined in the catalogue.

One of the benefits of using this list is to take advantage of previous studies and results that verify the specification’s usefulness in a given scenario. In addition, Adopted specifications can also be useful as technical requirements when writing procurement documents.
5.3.1 How are adopted specifications classified?

Classification helps to identify the most relevant formalised specification through a pre-established set of technical categories which are relevant to Government’s Enterprise Architecture.

As described in Chapter 2, the Interoperability Architecture identifies a series of infrastructure services which should be always present (to varying degrees) when implementing an ICT solution for the public sector.

The identified infrastructure services are shown in Figure 11. A description is provided in Annex A. Some of these services are so common that they are good candidates for a sharable implementation. Others might require more personalised approaches and therefore should be more flexible.

Irrespective of their deployment approach, their commonality makes them the ideal candidate for this type of classification.

While each infrastructure service category can span a number of technical solutions, at the very least, each category should at least be associated with one formalised specification.

The Adopted Specifications Catalogue should also give the facility to determine the scope and applicability for each formalised specification; in certain cases allowing for multiple contexts.

When public officers encounter scenarios not yet covered by this catalogue, it is recommended that they instigate the adoption process mentioned above.

5.3.2 Contextualising specifications using Interoperability Profiles

Applying standards in ICT solutions is the starting point to facilitate technical interoperability. However formalised specifications can be very versatile, at times requiring practical scenarios to explain their use within the public sector. This is because if a standard is used differently among collaborating parties, interoperability can still be jeopardised.

As an example, consider the usefulness of recipes that a head chef adopts to deliver menu items for a restaurant. First and foremost, a recipe is required so items described in the menu can be delivered as expected by the customer; this expectation is either based on a previous experience which establishes a baseline, or by the overall perception of the restaurant. If the kitchen has multiple personnel, a common recipe written in understandable nomenclature facilitates predictability by assuring that the food looks and tastes the same on every occasion.
For ICT solutions and services, Interoperability Profiles (the recipes) have been identified as a standardisation building block for the conceptual aggregation of guidelines, templates, patterns, profiles and other forms of reference material that contextualises the use of formal specifications within the public sector.

Highly flexible and configurable formalised specifications that are applicable across the public sector should have at least one documented interoperability profile which is relevant and reusable by the public sector clearly describing “when” and “how” to use the specification:

- “When” describes the relevant use cases and dependencies, providing enough information to solution architects so they can determine the most applicable scenario;

- “How” provides sound technical documentation to guide solution implementers in their local instantiation of the standard.

An interoperability profile can also package and describe complimentary technical standards required by an infrastructure service to present a more concrete explanation.

Going back to the recipe example, the end-user (customer) is usually not interested in the cooking process, but the kitchen personnel need to at least know how the ingredients are being measured, especially if the process is split between multiple cooks. It is also important for cooks to know the intended usage of all the ingredients. If for instance, a meal is based on red meat, changing this to poultry will change its expected outcome in ways which will most likely offend the customer. However, innovating on the herbs used or type of sauce, can improve the overall experience, leaving way for creativity.

While it is usually the case that for a given interoperability scenario only one standard is promoted, there are situations which demand the exact contrary. It is therefore important to appreciate that technical standards can and will be used differently in different scenarios. If the benefits of including an alternative standard outweigh the costs it introduces, then it should probably be considered as a plausible solution.

Ultimately the technical benefits should always be based on or at least consider the required business outcomes.
Appendix A. Different types of common Infrastructure Services

The following definitions have been adopted from the Common Vision for an EIA (ISA/2011/SN22.5) developed by the European Commission.

Audit trail and log chronologically records information about the usage of European public services. It collects data to examine how and when events occurred, who accessed a system and what actions he or she performed during a given period of time. The logged information can be the exchanged information between the system and the users of the system (incoming and outgoing messages), the log-on data, the transaction content and properties—time, checks and other actions performed by the users as well as actions performed by system administrators, or automated action initiated by the system. Audit trail and log records data generated by system processes and which do not correspond to specific user actions, and actions taken by identifiable and authenticated users.

Service registries are central registries that provide a description of available services. The registry presents, for each service how to use them, their current status, and their physical locations. A service registry maintains the catalogue of available services in a service-oriented context. Service producers publish services and register them into the registry such that consumers are able to find them. An enterprise may have one or more service registries that can be merged to one enterprise service registry, which is called a federated service registry.

Identity and access management encapsulates all the processes, policies, and technology solutions that manage digital identities and specifies how digital identities are used to access resources. This infrastructure service includes entity authentication (the mechanism needed to manage controlled access of entities to applications) and authorisation (the mechanism to define what access privileges an entity has within the application by defining roles and groups). Note that data authentication, which verifies origin and integrity of data, is not part of this “identity and access management” infrastructure service, as this is treated in the “data certification” infrastructure service.

Data certification is defined as the process of signing an electronic information (which could also be an e-mail, a file or a data source), and of verifying whether the origin and integrity of information are what they are expected to be based on certificates issued by different Certification Authorities (CA). This infrastructure service includes the creation, validation, and extension of advanced electronic signatures as front-end services in conformity with the requirements of the EC Directive. Validation of certificates and time stamping are back-end services to provide these front-end services, and may optionally offer also a direct client interface.

Data transport is the exchange of data in a reliable way by providing standardised transport capabilities. This service facilitates communication between systems for collecting and delivering EC ISA European Interoperability Architecture (EIA) 97 / 132 data, and does not store the data centrally. Each system independently handles its own data and, when required, draws data from the database and sends it to another system.

Data translation facilitates data transfers between systems (using their own data format, data model and data encoding) and includes semantic translation, syntax translation and multilingualism capabilities.

Workflow management orchestrates interactions between workflow participants (human and systems) and provides each participant with the information that is necessary to complete his or her task.

Document storage is used to store and to manage documents, providing features at each stage of the document life cycle: creation, retrieving, reviewing, versioning, distribution, publishing, archiving and eventual destruction. This service facilitates collaboration between different contributors to the document life cycle.
Structured data storage facilitates the exchange of data by providing a simple and structured interface to access data stored in large and complex databases. This service acts as an abstraction layer between the technical data structure of a database and the functional point of view of a standard user. The structured data service removes the need to maintain a schema, while your attributes are automatically indexed to provide fast real-time lookup and querying capabilities. This flexibility minimises the performance tuning required as the demands for your data increase.