ΚΥΠΡΙΑΚΗ  ΔΗΜΟΚΡΑΤΙΑ

CYPRUS

NATIONAL INTEROPERABILITY FRAMEWORK

(eGIF)

Version 2.0

DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES

13 July 2017

REVISION HISTORY

Date	Version	AuthorS	Description / Changes
18/12/2013	0.1	Contractor's Project Team	Final version for informal review by DITS Project Team
24/12/2013	0.2	Contractor's Project Team	Integration of DITS Project Team comments Initial version for Quality Review
29/01/2014	1.0	Contractor's Project Team	Integration of QRB comments Final version
13/7/2016	0.1	Contractor's Project Team	UPDATE - Initial version for informal review by DITS Project Team
15/7/2016	0.2	Contractor's Project Team	UPDATE - Integration of DITS Project Team comments Initial version for Quality Review
1/8/2016	1.0	Contractor's Project Team	UPDATE - Integration of QRB comments Final version
18/8/2016	1.1	DITS Project Manager	Cyprus eGIF
8/6/2017	0.1	Contractor's Project Team	UPDATE – Based on new EIF - Initial version for informal review by DITS Project Team
15/6/2017	0.2	Contractor's Project Team	UPDATE – Based on new EIF - Integration of DITS Project Team comments Initial version for Quality Review

Date	Version	AuthorS	Description / Changes
30/6/2017	1.0	Contractor's Project Team	UPDATE – Based on new EIF - Integration of QRB comments Final version
13/7/2017	2.0	DITS Project Manager	Cyprus eGIF

DISTRIBUTION

Name	Role	Organisation
DITS Project Team Members	DITS Project Team	DITS
Contractor's Project Team Members	Contractor's Project Team	PLANET
All DITS Officers	DITS Officers	DITS
Any other interested individuals or organisations		

ΕΛΕΓΧΟΣ ΕΓΓΡΑΦΟΥ

Name	Role	Date
Christos Tsiakaliaris	Contractor's Project Coordinator	28/01/2014
Christos Tsiakaliaris	Contractor's Activity Coordinator	28/01/2014
Demos Kontoravdis	Contractor's Project Manager	1/8/2016
Demos Kontoravdis	Contractor's Project Manager	30/6/2017

ACRONYMS – ABBREVIATIONS

Acronym	Description
DAE	Digital Agenda for Europe
DCMI	Dublin Core Metadata Initiative
DITS	Department of Information Technology Services
eGIF	eGovernment Interoperability Framework
EIF	European Interoperability Framework
EIS	European Interoperability Strategy
ETSI	European Telecommunications Standards Institute
EU	European Union
ICT	Information and Communication Technology
IDABC	Interoperable Delivery of European e-Government Services to public Administrations, Business and Citizens
IETF	Internet Engineering Task Force
ISA	Interoperability Solutions for European Public Administrations
ISO	International Organisation for Standardisation
IT	Information Technology
N/A	Not Applicable
NIF	National Interoperability Framework
NIFO	National Interoperability Framework Observatory
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Open Geospatial Consortium
OMG	Object Management Group

Acronym	Description
SEMIC	Semantic Interoperability Community
W3C	World Wide Web Consortium
WfMC	Workflow Management Coalition

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 EXECUTIVE SUMMARY

1.1 Purpose and Objectives

The National eGovernment Interoperability Framework of the Republic of Cyprus describes the principles, recommendations and technical standards that shall be taken into account by government organisations when designing, developing or operating information systems that support the provision of eServices to citizens and businesses both at the national and international level.

The National eGovernment Interoperability Framework aims to assist government organisations to conform to the minimum set of principles, rules, guidelines and standards, necessary to achieve interoperability with other government organisations and enable the exchange of information between them. Ultimate goal of the Cyprus eGIF is the provision of eServices to citizens and businesses in a uniform and co-ordinated way.

1.2 Target audiences

The principles, recommendations and standards of the eGovernment Interoperability Framework of the Republic of Cyprus **apply to all Ministries, Departments and Independent Offices of the Cyprus Government** and shall be taken into consideration during planning, designing, implementing or upgrading Government information systems. More specifically, the following government officers' groups are targeted:

- **Government organisations' management**, who may be primarily interested in the general principles of the eGIF and the recommendations at the integrated public service governance component, and the legal and organisational interoperability levels.
- **Government organisations' business officers** as well as government services/departments undertaking business process re-engineering/ simplification initiatives, who may be primarily interested in the general principles of the eGIF and the recommendations regarding achieving interoperability at the legal and organisational level.
- **DITS officers appointed either at the central office or decentralised at Ministries IT Units**, who may be primarily interested in the semantic and technical aspects of interoperability.

The eGIF also applies to:

- **other public sector organisations**, when interoperability with government organisations is required for the exchange of information or the development and provision of services;
- **private sector ICT companies**, when they provide ICT services to government organisations (e.g. applications' development/upgrade);
- **any other interested party** (natural or legal person, domestic or not) may have access to the eGIF for information purposes.

1.3 Benefits

The Government of the Republic of Cyprus anticipates several important benefits from the adoption of the eGIF, including:

- Transformation of the government service model from government-centric to user-centric;
- Design and development of information systems based on the same principles and common technical standards, thus setting the foundations for achieving interoperability from the very early stages of software development;
- Better coordination between government organisations for the provision of interoperable eServices;
- Cost and time reduction for information systems development by reusing existing functionality blocks available within the Government;
- Realisation of significant cost savings from transferring service requestors (i.e. citizens and businesses) from traditional service channels to electronic ones;
- General improvement of the image and the credibility of government organisations.

Private ICT companies which are contracted by the Government for the development of information systems as well as ICT service providers are also benefited from the adoption of the eGIF, since they are able to:

- develop products based on specifications that are known beforehand and do not change significantly in each information system development project,
- achieve economies of scale, and
- reduce time-to-market for their solutions.

1.4 eGIF structure

At first, the eGIF introduces the key concepts used throughout the framework, as well as the classification scheme and lifecycle of standards, followed by the introduction of the interoperability levels of the Cyprus eGIF, namely:

- Legal interoperability,
- Organisational interoperability,
- Semantic interoperability,
- Technical interoperability.

The recommendations at the legal, organisational and semantic level are then presented followed by an introduction to the reference architecture for developing interoperable information systems and applications, and a description of the technical standards, which are classified in the present version of the eGIF. The technical standards that shall be used by government organisations when designing and developing information systems and eServices are classified in three (3) levels, based on their conformance requirements; mandatory, recommended, and under observation. Technical standards have been defined in several categories and sub-categories as follows:

- eGovernment Applications Documentation & Development: Modelling Standards, Process Models Exchange Schemas.
- Service Modelling: Process Modelling Methods, Process Execution Languages.
- Data Modelling: Modelling Methods, Data Models Exchange Schema, Data Exchange Formats, Data Transformation, Metadata Schema, Metadata description, Semantic Information representation languages.
- Application Development Frameworks and Programming Languages.
- Information Presentation and Processing: Accessibility, Hypertext Exchange Schemes, Stylesheets, Character Encoding, Date & Time Representation, File Formats Recognition, Document formats for Information Exchange, Documents formats for Information Processing, Graphics Exchange Formats, Sound, Video and Video Streaming file formats, Data Compression.
- Communication and Interoperability: Interoperability with Third-Party Systems, Discovery of Resources, Locating of Resources, Network Protocols, Application Layer Protocols, IP Telephony, Content Delivery.
- Security and Authentication: Web Services Security, Data Transmission Security, Encryption, Authentication, Identification and Authorization.

- Standards for specific Business Sectors: Medical images exchange, Medical data exchange, Geographical data representation and exchange, e-Learning content, Election data exchange, Virtualization.

1.5 General principles

In the process of planning, designing, implementing and delivering eGovernment services, government organisations shall ensure that the following general principles are considered:

1. Subsidiarity and proportionality
2. Proximity to citizens
3. Administrative simplification
4. Accessibility
5. Transparency
6. Trust and security
7. Preservation of information
8. Reusability
9. Multilingualism
10. Open standards and technologies
11. Once-only registration of data
12. Assessment of effectiveness and efficiency

The above mentioned general principles are further detailed in section 3.1.

1.6 eGIF Governance

The responsible body for the management of the National eGovernment Interoperability Framework of the Republic of Cyprus is the Department of Information Technology Services (DITS) of the Ministry of Finance. DITS's responsibilities as regards the eGIF and interoperability in general include inter alia:

- Definition of the interoperability strategy of the Cyprus Government.
- Formulation, maintenance and update of the eGIF.
- Planning and execution of dissemination and awareness activities regarding the eGIF.
- Monitoring of the adoption of the eGIF.

- Gathering and evaluation of suggestions for updates and changes to the eGIF.
- Monitoring of and participation in EU interoperability initiatives and events.

1.7 Submission of comments and suggestions

The National eGovernment Interoperability Framework of the Republic of Cyprus is available at the website of the Department of Information Technology Services (DITS) of the Ministry of Finance[1]. The eGIF is a live framework that is under a constant review process. All interested parties are invited to submit comments and suggestions for updates and changes to the eGIF through either the DITS website or to the e-mail address egif@dits.mof.gov.cy. DITS accumulates the comments and suggestions received by all interested parties, evaluates them, integrates the accepted modifications to the eGIF and publishes a new version of the framework.

1.8 Amendments to previous version of the framework

This is the third version of the National eGovernment Interoperability Framework of the Republic of Cyprus. The preparation of this version followed the announcement of an updated version of the European Interoperability Framework in March 2017[2]. Main changes from the previous version, performed in order to align the Cyprus eGIF to the new EIF, include:

- Update of the general principles of the eGIF in order to fully comply the new or amended principles of the new version of EIF
- Adjustments to the interoperability levels, where the “Political context” layer of the interoperability stack was replaced by the “integrated public service governance” component, following the relevant amendment of the new version of EIF
- Addition of a small number of new recommendations and adjustment/ enrichment of the content of others
- Enhancement of the relationship between the eGIF and the eGovernment Strategy as well as the Government Security Policy, by adding specific references, where appropriate
- Upgrade of the significance of the role of information sources and services for achieving interoperability

1 https://goo.gl/w5m7QD

2 Annex 2 of the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “European Interoperability Framework - Implementation Strategy”, COM(2017) 134 final, Brussels, 23.3.2017

2 INTRODUCTION

2.1 Scope

The principles, recommendations and standards of the eGovernment Interoperability Framework of the Republic of Cyprus apply to all Ministries, Departments and Independent Offices of the Cyprus Government and shall be taken into consideration during planning, designing, implementing or upgrading Government information systems.

The eGIF also applies to other public sector organisations, when interoperability with government organisations is required for the exchange of information or the development and provision of services.

Furthermore, the eGIF applies to private sector ICT companies, when they provide ICT services to government organisations (e.g. applications' development/upgrade).

Last but not least, any other interested party (natural or legal person, domestic or not) may have access to the eGIF for information purposes.

2.2 Key concepts

The main concepts used in the Cyprus eGIF are the following:

- Interoperability level: The term refers to one of the four interoperability levels of the Cyprus eGIF as also described in the European Interoperability Framework; legal, organisational, semantic and technical.
- Classification level: The term refers to one of the three levels used for the classification of the eGIF standards; Mandatory, Recommended, Under Observation.
- Standards lifecycle: It describes how technical standards are included into the eGIF, evolved within the eGIF (upgraded/downgraded) and, finally, discarded from the eGIF.
- Standards maturity lists: Maturity lists are complementary to classification levels and are used for keeping information about standards that are currently not included in the eGIF. Three lists are defined; white, grey, black.
- Guidelines: Apart from technical standards, the eGIF also includes a number of guidelines aiming to support government organisations to achieve interoperability at the legal, organisational and semantic level.

2.3 Classification scheme and lifecycle of standards

2.3.1 Classification of standards

The Cyprus eGIF employs three (3) levels for the classification of its standards and guidelines as depicted in the following figure:

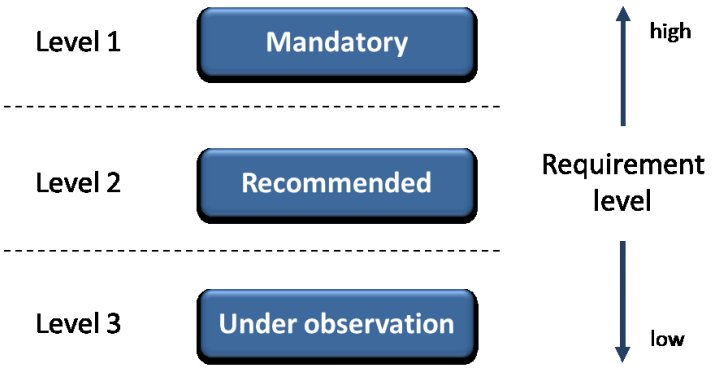

Figure 1: Classification of standards in the Cyprus eGIF

Level 1: Mandatory

A technical standard is characterised as "Mandatory" and indicated by the letter "M" followed by a reference number when it fully conforms to the principles of the eGIF, has been used extensively by the ICT sector in real world information systems, and is supported and maintained by organisations, consortia, groups or similar entities with worldwide recognition. Mandatory standards comprise the primary category to search when there is a need to find a standard in a specific application area.

If a specific category hosts both Mandatory and lower level standards (Recommended or Under Observation), Mandatory standards shall be applied by priority. Recommended standards or standards Under Observation shall be used only in exceptional cases with proper justification.

More than one standard may be classified as Mandatory in a specific application area, in case they are considered as equivalent from the eGIF's perspective.

Level 2: Recommended

A technical standard is characterised as "Recommended" and indicated by the letter "R" followed by a reference number when it has been used in numerous real world information systems by the ICT sector, and is supported and maintained by organisations, consortia, groups or similar entities with worldwide recognition. On the other hand, it does not entirely conform to the principles of the eGIF or a more suitable Mandatory standard may exist in the same application area.

In case no Mandatory standards exist in the same application area of the Recommended standard, the latter shall be applied by priority. Lower level standards (i.e. Under Observation) shall be used only in exceptional cases with proper justification.

More than one standard may be classified as Recommended in a specific application area, in case they are considered as equivalent from the eGIF's perspective.

Level 3: Under Observation

A technical standard is characterised as "Under Observation" and indicated by the letter "U" followed by a reference number when it is "open", its adoption is continuously increasing and significant benefits from its use are expected. On the other hand, low level of conformance to the principles of the eGIF may be currently depicted and limited applications in real world information systems may be encountered.

"Under Observation" standards are the first to be examined in every eGIF revision for upgrade to a higher level (e.g. Mandatory, Recommended) or abandonment.

A standard that is Under Observation may only be used, in case no higher level standard exists in the same application area or in exceptional cases with proper justification.

2.3.2 Keywords & phrases used to denote requirement levels

The keywords or phrases "MUST", "REQUIRED", "SHALL", "MUST NOT", "SHALL NOT", "SHOULD", "SHOULD NOT", "NOT RECOMMENDED" and "MAY" in this document are to be interpreted as described in RFC 2119[3]:

- The keywords "MUST", "REQUIRED" and "SHALL" are used in mandatory standards and mean that the specification is an absolute requirement of the eGIF.
- The phrases "MUST NOT" and "SHALL NOT" are used in mandatory standards and mean that the specification is an absolute prohibition of the eGIF.
- The keyword "SHOULD" is used in recommended standards and means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

[3] Internet Engineering Task Force (IETF) Request For Comments (RFC) 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997, http://www.ietf.org/rfc/rfc2119.txt

- The phrases “SHOULD NOT” and "NOT RECOMMENDED" are used in recommended standards and mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- The keyword “MAY” is used in standards that are currently under observation since they do not fully adhere to the principles of the eGIF, but have the potential to be upgraded to mandatory or recommended classification level in the future.

2.3.3 Standards maturity lists

Apart from the three (3) levels used for the classification of the standards, the Cyprus eGIF also employs three (3) lists for keeping information about former eGIF standards, new standards suggested for inclusion to the eGIF or even abandoned standards and standards that do not conform to the eGIF’s principles.

White List

The White List hosts candidate standards to be included in the eGIF. These standards are evaluated in every eGIF review for inclusion to the eGIF.

Grey List

The Grey List hosts standards that were part of the eGIF as mandatory or recommended standards in the past. These standards may still be used by legacy government information systems but they cannot be used for the implementation of new information systems.

Black List

The Black List hosts standards that cannot be used or included in the eGIF.

2.3.4 Lifecycle of standards

The evolution of the technical standards within the Cyprus eGIF may follow several different paths as depicted in the following figure:

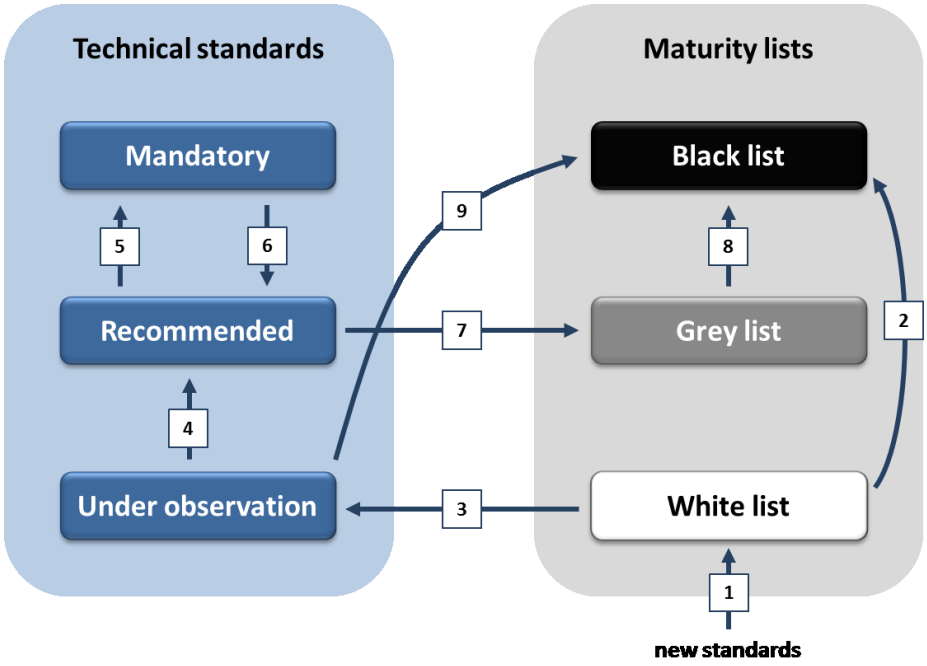

Figure 2: Lifecycle of standards in the Cyprus eGIF

The transitions of a standard in the Cyprus eGIF, as graphically presented in the above picture, are explained below:

1. When a new standard is suggested for inclusion to the eGIF according to the eGIF's review procedures, it is registered into the White List of the eGIF. This List is being continuously populated with suggested standards until a new version of the eGIF is decided to be elaborated. At that point, the standards of the White List are thoroughly evaluated, and the following transitions are possible:
   a. Transition 1-2: A standard does not conform to the principles of the eGIF so as to be included in it, thus it is moved to the Black List.
   b. Transition 1-3: The inclusion of a suggested standard to the eGIF has been approved. The standard is classified as "Under Observation" in the respective application area of the eGIF.
   c. No transition: In this case, a suggested standard remains in the White List and its inclusion into the eGIF will be re-evaluated in the next review of the eGIF.
2. A standard of the White List, which does not conform to the principles of the eGIF so as to be included in it, is moved to the Black List.
3. A standard of the White List, which shows conformance to the principles of the eGIF, is classified as a standard "Under Observation" in the respective application area of the eGIF. In case the standard satisfies the requirements of higher classification levels of the eGIF (i.e. Recommended, Mandatory), a direct

transition of the standard from the White List to the appropriate classification level is allowed, following the transitions:

a. Transition 3-4: A standard of the White List is classified as a Recommended standard of the Cyprus eGIF in the respective application area.

b. Transition 3-4-5: A standard of the White List is classified as a Mandatory standard of the Cyprus eGIF in the respective application area.

4. A standard that has been attributed the “Under Observation” classification may be upgraded to the “Recommended” status in the next review of the eGIF or follow one of the transitions below:

   a. Transition 4-5: The standard is directly classified as a Mandatory standard of the Cyprus eGIF in the respective application area in case it satisfies the requirements of the specific classification level.

   b. Transition 9: In case the standard “Under Observation” fails to conform to the principles of the eGIF, it is moved to the Black List, thus discarded from the eGIF.

   c. No transition: In this case, the standard preserves the “Under Observation” classification and will be re-evaluated for upgrade in the next review of the eGIF.

5. A standard that has been attributed the “Recommended” classification may be upgraded to the “Mandatory” status in the next review of the eGIF in case it satisfies the requirements of the specific classification level. Other possible transitions of a “Recommended” standard include:

   a. Transition 7: In case the standard is no longer used in the development of new information systems, it is moved to the Grey List of the eGIF.

   b. No transition: In this case, the standard preserves the “Recommended” classification and will be re-evaluated for upgrade in the next review of the eGIF.

6. A standard that has been attributed the “Mandatory” classification may be downgraded to the “Recommended” status in the next review of the eGIF in case a more suitable standard appears. Other possible transitions of a “Mandatory” standard include:

   a. Transition 6-7: In case the standard is no longer used in the development of new information systems, it may be moved directly to the Grey List of the eGIF.

   b. No transition: In this case, the standard preserves the “Mandatory” classification and will be re-evaluated for upgrade in the next review of the eGIF.

7. A “Recommended” standard that is no longer used in the development of new information systems is moved to the Grey List of the eGIF.
8. The standards registered in the Grey List of the eGIF are also evaluated in every review of the eGIF and either remain in the Grey List or are moved to the Black List.
9. In case a standard with the “Under Observation” classification fails to conform to the principles of the eGIF, it is moved to the Black List, thus discarded from the eGIF.

2.4 Relationship with other National and European initiatives

The Cyprus eGovernment Interoperability Framework is fully aligned with the eGovernment Strategy of Cyprus as well as with other strategic initiatives at the national level, such as the National Digital Strategy and the National Reform Programme of the Republic of Cyprus.

It is also fully aligned with the European Interoperability Strategy and the European Interoperability Framework, thus serving the relative objectives of the Digital Agenda for Europe and the European Commission’s eGovernment Action Plan.

The overall objectives of the ISA programme (Interoperability Solutions for European Public Administrations), which succeeded the former IDABC programme (Interoperable Delivery of pan-European Services to Public Administrations, Businesses and Citizens) were also considered during the elaboration of the National eGovernment Interoperability Framework of the Republic of Cyprus.

Furthermore, the eGIF builds upon the experience gained at EU level regarding interoperability also capitalising on the results of the NIFO and the SEMIC project as well as on good practices realised by other EU Member States from the elaboration of their National Interoperability Frameworks.

3 eGOVERNMENT INTEROPERABILITY FRAMEWORK

3.1 General principles

In the process of planning, designing, implementing and delivering eGovernment services, government organisations shall ensure that the following general principles are considered:

1. Subsidiarity and proportionality

The Cyprus eGovernment Interoperability Framework **is fully aligned with the European Interoperability Strategy and the European Interoperability Framework, adjusting and extending their provisions and recommendations to the national context and needs**, where necessary. It is also fully aligned with the eGovernment Strategy of Cyprus as well as with other strategic initiatives at the national level, such as the National Digital Strategy and the National Reform Programme of the Republic of Cyprus, thus forming altogether a coherent base set of strategic documents that guide the development of interoperable electronic public services with a pan-European dimension by design.

At the same time, **Government decisions** regarding eGovernment services and interoperability **shall be taken as close as possible to the citizen**. The decision making responsibilities of local and regional authorities shall be enriched since they are in direct contact with citizens. **Central Government** shall not take action unless this is more effective than action taken at regional or local level, and this action **shall enable the achievement of agreed policy objectives**. Local and regional authorities shall be in close cooperation among themselves to exchange information and coordinate the delivery of joint electronic services, conforming, where applicable, to policy actions taken by the Government.

2. Proximity to citizens

Government should be at the disposal of the people and not the other way around. The target for future services should be the provision of **personalised** eServices at the maximum possible **sophistication level**, that will allow service users, i.e. citizens and businesses, to be able to interact with public administrations any time, as easily as possible. In order to gain acceptance and approval from end users, electronic environments shall have a consistent design and shall be **friendly** and **understandable**, which means they shall be readable, predictable and interactive.

3. Administrative simplification

Aiming to achieve the objectives of the Cyprus eGovernment Strategy, government organisations shall focus, inter alia, on enhancing their capacity, reduce operational costs, design and deliver additional eGovernment services, and facilitate cross-border collaboration at European level. Prior to their automation, the **simplification of government services** shall be investigated, so as to avoid transferring inefficiencies of the physical to the digital channels, ensure that the outcome of services is the same irrespectively of the delivery channel, and reduce the administrative burden on public administrations, businesses and citizens.

4. Accessibility

eGovernment services shall be **accessible to everyone without discrimination**. Solutions developed as well as the web sites themselves must be barrier-free and accessible to all. In this direction, efforts shall be made to allow web content and eServices to be accessible to a wider range of people regardless of their computer literacy, including people with disabilities or cognitive limitations.

5. Transparency

Openness and **improved transparency** are two of the cornerstones of eGovernment. Any government transformation will only be accepted if all those affected by it, from government organisations employees to those in business, are involved in the process, and developments are carried out in a transparent way. Citizens and businesses should be able to **understand administrative processes**, **track administrative procedures** that involve them, and have insight into the rationale behind decisions that could affect them. End users (citizens or businesses) **feedback about the quality of the public services provided shall be sought** so that existing services are improved or new ones are developed based on this contribution. The concept is the use of ICT to make public sector decisions and actions more open to scrutiny.

Extending transparency to also cover system-to-system communications, government organisations, through their information systems, shall **enable visibility into their internal IT environment**; applications, services and data. This visibility may be achieved by the adoption of the reference architecture for interoperability and the use of technical standards of the eGIF, thus facilitating the development and availability of external interfaces to internal services and data of a government organisation.

On the other hand, following the mandates of the Cyprus eGovernment Strategy, government organisations shall **become more "open"**, and **share data and services** within Government and with the public. Opening up of government registries (e.g. civil and alien registry, businesses registry, cadastre and town planning and housing registries) and giving access to public sector information to

citizens and businesses (where possible, and/or no restrictions apply) are two areas to be addressed by government organisations.

6. Trust and security

Citizens have to be able to trust the electronic service channels as much as they do the traditional ones, having no doubt about the **integrity of information** sent or received or about the **identity** of the government organisation's website with which they transact. Citizens also put a high value on the protection of their **privacy**. The citizens' confidence in the public administration with regard to sensitive data protection must be gained. This means that public administrations must guarantee the privacy of citizens and the confidentiality of information provided by businesses. To this end, **government organisations**, when designing or delivering electronic services to citizens and businesses, or exchanging data with other organisations, **shall investigate the related information security implications following a systematic risk management approach and the guidelines of the Cyprus Government Security Policy**.

7. Preservation of information

Evidence on the delivery of a service was always of paramount importance in the traditional paper-based public administration. This is even more important in the modern electronic public administration since services have become more accessible, thus easier to use, to citizens and business, and their results (e.g. certificates, statements) are acceptable even at court procedures, if properly secured (e.g. with electronic signatures, timestamps, etc.). **Government organisations shall keep records of transactions** with citizens and businesses in their information systems, **retain their legibility, reliability and integrity, and ensure their accessibility** as long as needed, taking into account security and privacy. Records shall be kept at least for as long is foreseen by the applicable European and national legal framework. Standards and technologies included in the eGovernment Interoperability Framework shall be preferred for assuring the long-term preservation of information.

8. Reusability

The **reuse of existing functionality components**, which a) conform to the eGIF's principles and standards, and b) are available for reuse at least within the Cyprus Government, **shall be examined by priority** when developing eGovernment information systems and services. This way, development time and cost may be reduced and conformance of the new system/service to the eGIF may be easier to be achieved. Additionally, in cases where **open source software** is used, government organisations should share any important experiences gathered with the pertinent developer communities, thus **contributing to the further evolution of the**

solutions. Last but not least, since data rather than software or hardware components bear the actual value for an organisation, **data portability**, i.e. the ability to move and reuse data easily among different applications and systems (where legally allowed), is of paramount importance for government organisations, which shall pay special attention to this during their eGovernment initiatives.

9. Multilingualism

In the case of eGovernment services targeted to non-Greek speakers, **the provision of the services in other languages** shall be foreseen in order to raise their adoption level and usability. Support for multilingual features is also important when a public service requires **exchanges between information systems across language boundaries**, so as to preserve the meaning of the information exchanged. To this end, technical architectures and standards employed for the development of the information systems and services shall not raise any obstacles for the provision of government content and services in multiple languages.

10. Open standards and technologies

Open standards and **technological neutrality** offer opportunities for more cost-effective use of resources and delivery of services, while promoting interoperability. The use of common standards can make ICT solutions fully interoperable, in turn facilitating reuse, sharing and scalability across organisational and national boundaries. Moreover, **open source software** is now considered to be a reasonable alternative to commercial-off-the-shelf products, where strong developer communities exist and actively support the available solutions. eGovernment must avoid becoming dependent upon a specific software or hardware monopoly or being locked on one particular technology. Furthermore, **commoditized design** enables flexibility and agility of supply. Through opening up the market, costs (i.e. total costs of ownership) will come down, innovation will increase and services will improve.

11. Once-only registration of data

Citizens' information **shall be collected once**, e.g. during registration or at the first time a service is used, and reused by different government organisations, provided that data and privacy protection are ensured.

12. Assessment of effectiveness and efficiency

Pursuing interoperability for interoperability is not a target for eGovernment initiatives. Where different interoperability solutions are available, government organisations shall **put them under evaluation** so as to ensure that the options selected serve businesses and citizens **in the most effective and efficient way** and **provide the best value for money**.

3.2 Interoperability levels

The Cyprus eGIF adopts the four interoperability levels proposed by the European Interoperability Framework as depicted in the following figure:

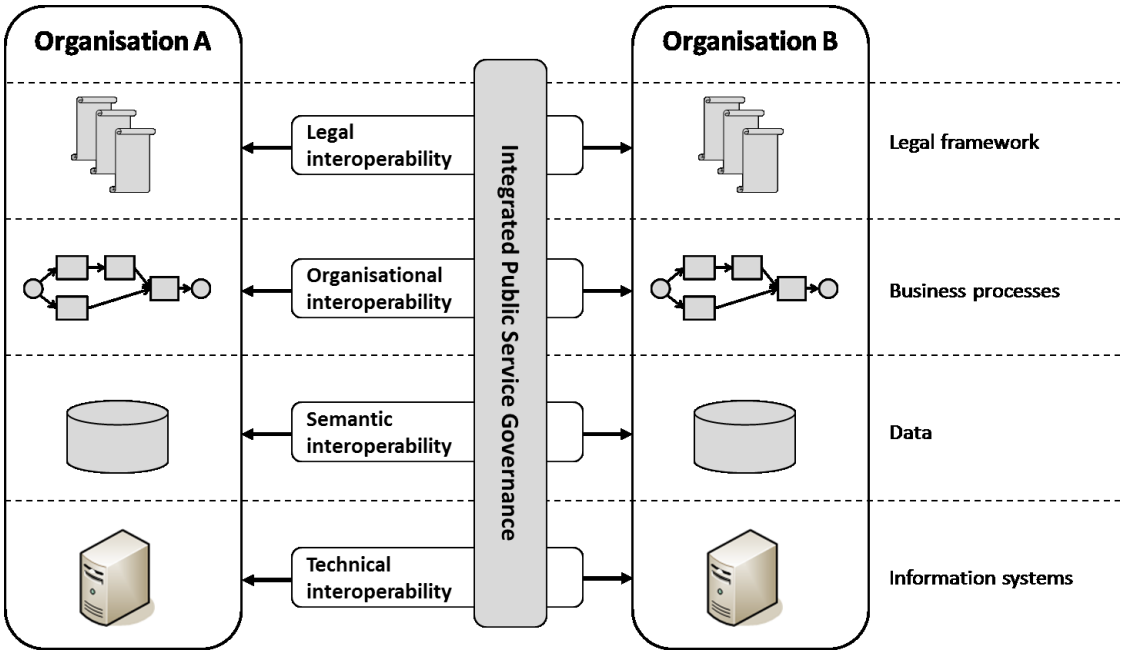

Figure 3: Interoperability levels

Legal interoperability: When two or more organisations wish to exchange information or collaborate for the provision of interoperable eServices, the legal framework that regulates their operation must be investigated in order to see whether they have the right to be involved is such endeavours. Possible modifications to the legal framework may also be identified. Legal interoperability also addresses the legal validity of the actions of the collaborating organisations, the legal validity of the eServices provided as well as the protection of data exchanged.

Organisational interoperability refers to the definition of mutually agreed goals and the alignment of the internal business processes of the organisations that wish to collaborate for the exchange of information or the provision of interoperable eServices. Organisational interoperability is commonly ensured via legal provisions or bilateral agreements between organisations.

Semantic interoperability ensures that exchanged data have the same meaning and are understood in the same way by involved organisations. Vocabularies, data elements sets, codelists and other semantic models are most commonly used for ensuring interoperability at the semantic model.

Technical interoperability refers to the interoperability between information systems at a technical level. Technical interoperability is ensured via the use of common technical standards and specifications.

It shall be noted that interoperability at a certain level cannot be achieved prior to establishing interoperability at all higher interoperability levels, e.g. technical interoperability may be achieved only if interoperability at legal, organisational and semantic level is achieved.

The Cyprus eGIF, similarly to the EIF, introduces an additional cross-cutting component of the four layers, the "**integrated public service governance**" component, which indicates that the collaboration and the exchange of information between two or more organisations shall have the support of the management of the organisations (i.e. management commitment) and be conducted under the auspices and the coordination of the appropriate governance structure.

Last but not least, the overall promotion and monitoring of interoperability at the national level and the coordination of national interoperability initiatives with relevant ones at the EU level require an **eGIF governance function**, performed by the Department of Information Technology Services of the Ministry of Finance of the Republic of Cyprus.

4 INTEGRATED PUBLIC SERVICE GOVERNANCE

Before any interoperability initiative is to be implemented, the need for such an initiative and the will to implement it shall be verified. This is something that has to be done by all parties who wish to collaborate and exchange information.

Key roles involved in this task are usually the business managers of the organisational entities (e.g. directorates, departments) that wish to exchange information and the management of the organisations at a political level; business managers are describing and analysing the business case, while the management ensures the political support and sponsorship of the interoperability initiatives.

Of course, the interoperability mandate may be initiated the other way around, i.e. from the management of the organisations, in case, for example, the need for interoperability is identified so as to conform to a specific legislative act. In this case, the management authorises the business managers to analyse the business case and, after examining and refining it, provides its support and commits the necessary resources to its implementation.

Recommendation 01.
Government organisations that wish to exchange information or collaborate for the provision of interoperable eServices shall agree, at the political/ management level, on the terms of this collaboration, prior to committing resources to its realisation. Specific agreements (e.g. Memoranda of Understanding) that define the high level terms of the collaboration may be signed for this purpose.

The support of the interoperability initiatives from the political leadership of the collaborating organisations should be regularly verified, at least until interoperability is achieved and fine-tuned.

Recommendation 02.
Interoperable eServices shall be monitored and fine-tuned over time under the responsibility of the appropriate governance structures and according to the terms included in the respective collaboration agreements.

5 LEGAL INTEROPERABILITY

5.1 Context and scope

The organisational structure, the responsibilities, the services provided and, in general, the operation of a government organisation is defined by legal acts. So, when an organisation wishes to automate some of its business processes, deliver a new eService to citizens or businesses, or exchange information with another organisation, the corresponding legal framework shall be investigated first. The following issues shall be addressed:

- Identification of the legal acts that regulate the business processes or the services to be automated.
- Adjustment of the legal acts, if necessary, so as the automation of a business process or a service is allowed.
- Assurance of the legal validity of the results of the business processes or the services to be automated.
- Protection of the data involved in the execution of the business processes or the delivery of the services.
- Protection of users' data.

When two or more organisations wish to exchange information or collaborate for the provision of interoperable eServices, the alignment of the legal framework that regulates their operation is additionally required.

The timely and proper resolution of the above issues is a prerequisite for achieving interoperability at the legal level. Furthermore, since interoperability levels are examined top-down, if legal interoperability is not ensured, it is very difficult, if not impossible, to achieve interoperability at any other level.

5.2 Adjustments to the legal framework for the automation of business processes

As mentioned before, the legal framework that regulates a business process or a service of a government organisation shall be investigated and probably modified prior to the automation of the process.

Recommendation 03.

The legal framework that regulates a business process or a service of a government organisation shall be clearly indicated in the documentation of the process/service.

Recommendation 04.

The legal framework shall be properly adjusted, removing any unnecessary barriers (e.g. clauses applicable only to the physical world, over-restrictive rules on the use and/or storage of data), so as to reflect the automation of a business process or a service of a government organisation, prior to the automation of the process/service.

The legal validity of the results of the business processes or the services to be automated shall also be ensured.

Recommendation 05.

Government organisations shall make all appropriate modifications or additions to the legal framework in order to ensure the legal validity of the results of the business processes or the services they provide via electronic means.

The protection of the data involved in the execution of a business process or the delivery of a service via electronic means (including user's information) is one of the main issues to be addressed during any automation endeavour.

Recommendation 06.

The sensitivity of the data involved in electronic transactions with government organisations shall be taken into consideration during the automation of a business process or service. The provisions of the data protection act and other relevant legal framework shall be ensured.

5.3 Legal framework alignment

In case the business process automation goes beyond the boundaries of a single government organisation or the delivery of an eService to citizens/businesses requires the collaboration of more than one organisations, performing uncoordinated adjustments to the legal framework of each organisation separately does not ensure the success of the overall effort.

Recommendation 07.

Government organisations that exchange information or collaborate for the provision of interoperable eServices shall ensure that proper modifications have been performed to their legal frameworks in a coordinated way.

6 ORGANIZATIONAL INTEROPERABILITY

6.1 Context and scope

From an organisational point of view, interoperability focuses on the alignment of business processes of government organisations that collaborate for the exchange of information or the provision of eServices. Therefore, key issues to be addressed in the effort of two or more government organisations to achieve organizational interoperability include:

- Service modelling.
- Assignment of service custodians.
- Business process alignment.
- Bilateral/Multilateral agreements.
- Transparent one-stop service provision.
- Reuse of existing functionality modules and base registries.

The achievement of organisational interoperability is very important since it is a prerequisite for the investigation of interoperability at lower levels (i.e. semantic and technical).

6.2 Service modelling

Until recently, it was very common for government organisations to focus on their internal business automation rather than pay attention to the needs of the citizens and businesses that were the primary consumers of their services. This often resulted in the automation of bureaucratic, old, if not obsolete, and in any case not optimised business processes. Furthermore, the documentation of the services provided is in most of the cases limited. In the digital era, government organisations shall adjust their operational model to the needs of the consumers of their services.

Recommendation 08.
Government organisations shall have detailed documentation of the services they provide to citizens, businesses and other organisations. The documentation shall include graphical representation of the services as well as descriptions of the organisational entities and documents involved in the service provision. Metadata shall also be kept for each service.

6.3 Service custodians

Another issue to be addressed is the identification of the roles that are responsible or involved in the service provision and their assignment to the personnel of the government organisation. A key role that shall always be present is the role of the "service custodian", i.e. the responsible role for the provision of a service, from a business perspective.

Recommendation 09.

Government organisations shall assign custodians to the services they provide to citizens, businesses and other organisations.

It is strongly recommended that this role is assigned to the head of the department of the government organisation that has the responsibility for the delivery of the service to the end users.

The typical responsibilities of the service custodian may include:

- Keeping and updating the documentation of the service.
- Assigning duties to people involved in the service delivery.
- Monitoring and evaluating the service efficiency and effectiveness, including measuring user satisfaction.
- Looking for improvement opportunities.

Apart from the role of the service custodian, other lower level roles (e.g. process custodians) may also be created, depending on the complexity of a service and the availability of personnel.

6.4 Business process alignment

In order for two or more government organisations to be able to collaborate and provide an end service to citizens or businesses, the objectives of this collaboration, the information to be exchanged and the "business interoperability interfaces" from all sides shall be defined first.

Recommendation 10.

In case government organisations work together for the provision of a service, they shall be aware of the objectives of this collaboration and the information to be exchanged. Appropriate "business interoperability interfaces" shall be defined by all parties involved in order to facilitate the collaboration.

It is strongly recommended that the role of business interoperability interface is assigned to the organisational units (e.g. departments/services) of a government organisation and not at the level of a person.

After the establishment of business interoperability interfaces, focus shall be given to the alignment of the business processes of the government organisations.

Recommendation 11.

The business interoperability interfaces of the collaborating organisations shall work together to identify and perform the necessary changes to the business processes that support the delivery of services in order to make them interoperable and improve the experience of the service consumers (i.e. citizens, businesses).

The documentation of the business processes is the starting point for their streamlining.

6.5 Bilateral/Multilateral agreements

Similarly to the Service Level Agreements that define the terms and conditions for the delivery of ICT services from one organization to another, government organisations may sign business agreements that regulate their collaboration.

Recommendation 12.

In case government organisations work together for the provision of a service, they may sign agreements (e.g. Memoranda of Understanding) that define the terms and conditions of their collaboration.

These agreements may indicatively include:

- The objectives of the collaboration.
- The business interoperability interfaces defined by all parties.
- The information to be exchanged.
- The response times of a party to the requests of the other party.
- The measures that ensure the quality of service from all parties.
- The measures that ensure the protection of information exchanged.
- The services to be provided by each party (e.g. building blocks, access to base registries) and the service levels expected.
- The change management processes that ensure continuous service delivery, and allow the assessment and application of changes to be done in a controlled way.

- Business continuity/ disaster recovery policies and plans to be initiated when severe abnormal events occur, so as to ensure the security and the continuity of the service.

The agreements mentioned here may elaborate on the high-level terms of the collaboration agreements signed by the political leadership of the organisations, if such exist. Furthermore, they may be complemented, at lower interoperability levels (i.e. semantic and technical), with other types of agreements focusing on more technical or operational matters (e.g. SLAs, support/ maintenance agreements, etc.).

Recommendation 13.

Where interoperability (or similar) agreements exist at the management/ organisational level, government organisations may benefit from complementing them with agreements focusing on technical or operational matters.

6.6 Transparent one-stop service provision

The final goal of government organisations in the effort of providing better services to citizens and businesses is to deliver truly interoperable electronic services, thus removing bureaucratic barriers from their business processes and looking for information in other organisations instead of requesting it from citizens and business. This way, the need for citizens and businesses to provide information that is already available in other government organisations is significantly decreased.

Recommendation 14.

Government organisations shall work towards the end-to-end automation of a service and remove the obligation of citizens and businesses to supply information that is already available within the government.

6.7 Reuse of existing functionality modules and base registries

Several government organisations may wish to develop and deliver electronic services to citizens and businesses but not have the necessary ICT infrastructure or financial resources to do so. In these cases, the reuse of existing functionality modules, e.g. for users authentication and electronic payments, may provide a satisfactory and cost-effective solution.

Recommendation 15.

Government organisations shall investigate the possibility of reusing existing government-wide services instead of developing the same services in their own ICT infrastructure. Primary functional areas to be examined in terms of reusability potential include user identity management, electronic payments, electronic signatures and data warehousing.

Examples of Cyprus government information systems that support the above mentioned functional areas are the Government Gateway “ARIADNI” (providing Single-Sign-On services and supporting the once-only principle) and the Government Data Warehouse (GDW).

Another key concept involved in the effort of achieving interoperability, both at organizational and semantic level, is this of “base registries”. Base registries are these government registries that provide timely and reliable information on several items, such as persons, companies, buildings, vehicles, categories of professionals, forests, water resources, road network, etc. Today, these registries are in most cases not available to government organisations that need to use this kind of data. Instead, their use is generally limited to the government organization that is authorized to maintain them. According to the eGovernment Strategy of the Republic of Cyprus, base registries shall be made accessible at least by government organisations with proper authorization.

Recommendation 16.

Government organisations shall open up the registries they are responsible for, and allow other properly authorised government organisations to have access to them.

7 SEMANTIC INTEROPERABILITY

7.1 Context and scope

According to the European Interoperability Framework, "*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*."

Similarly to achieving interoperability at legal or organisational level, where the challenges refer to bridging the differences on the legal framework that regulates the operation of the interoperating organisations, and identifying the organisational entities that will be communicating and defining the corresponding procedures, interoperability at a semantic level refers to the identification of a common communication code in terms of the data exchanged, their structure and their exact meaning for all parties involved.

Therefore, key issues to be addressed in the effort of two or more government organisations to achieve semantic interoperability include:

- Semantic models development approach
- Semantic models custodians
- Data schemas and ontologies
- Semantic-based definition languages

The achievement of semantic interoperability is a prerequisite for the investigation of interoperability at the technical level.

7.2 Semantic models development approach

There are several approaches that may be employed for the development of semantic models:

- Global model approach: a global semantic model (vocabulary) is developed in order to define the meaning of the concepts in a specific business area. All organisations that use these data make also use of this global model. This is the most appropriate approach when well-known or de facto standards exist in a specific area, based on which semantic models are built. However, since a global semantic model shall be general by nature in order to accommodate several different requirements in a particular business area, specific needs of the organisations in the area may be partially met.

- Multiple models approach: a different semantic model is developed by each organisation in order to define the meaning of the concepts in a specific business area. This approach serves the needs of each organisation in the best possible way, but, on the other hand, may raise significant problems when different organisations need to communicate and exchange data, due to the need of correlating the different semantic models employed.
- Hybrid approach: this approach, as expected, is a combination of the two previous approaches. Based on the hybrid approach, each organisation in a specific business area develops its own semantic model thus accommodating its particular needs. However, this semantic model is compliant with a global semantic model used for the communication of different organisations in a business area.

Recommendation 17.

Government organisations shall use the hybrid approach for the development of semantic models.

According to this approach, it is recommended that government organisations first investigate whether a global semantic model exists in the business area of interest and, if yes, whether it meets their own specific needs. Based on the results of this investigation, government organisations should:

- In case a global semantic model exists and meets, at least partially, the needs, extend this global semantic model for internal use purposes
- In case a global semantic model does not exist or does not meet the needs, create their own semantic model for the specific business area

In both cases, it is recommended that the semantic models (either new or derived from global models) are published, e.g. to the web portal of government organisations, other government portals or a government repository of reusable semantic models.

7.3 Semantic models custodians

In order for the hybrid approach for the development of semantic models to be effective, the organisation responsible for the design, development and maintenance of the global semantic model in a specific business area shall be identified.

Recommendation 18.

In every business area of interest, a government organisation shall be assigned the

responsibility of designing, developing and maintaining the global semantic model for the representation of data in the specific business area. This organization shall act as "custodian" for the specific semantic model, putting in place and systematically following a specific quality assurance plan for the model itself and its contents.

For example, the Ministry of Health may be responsible for the design, development and maintenance of the global semantic model for the representation of diseases and related health problems, probably by adopting and extending a suitable international standard.

In order to enhance the reusability potential of a semantic model, it is recommended that it is complemented by suitable descriptions and/ or documentation.

Recommendation 19.

Semantic model custodians shall provide adequate information about the model to increase its reusability potential, including, inter alia, the description of its content, the type of data it keeps, conditions of access and the relevant licenses, terminology, a glossary, and information about its relationships with other models, if any. The details of the custodian and the plans ensuring the quality of the model and its contents shall also be clearly presented.

7.4 Data schemas and ontologies

Semantic interoperability addresses both the semantic aspect of data exchanged, i.e. their exact meaning, and their syntax, i.e. their exact structure. In the eGovernment context, semantic models may indicatively include:

- Code Lists, which are lists of commonly used concepts in the area of eGovernment e.g. government organisations, information systems, eServices, Cyprus cities and villages, countries, etc.
- Core Data Components, which are combinations of basic (elementary) data components commonly used in information systems and eServices; e.g. the core data component "Address" is a combination of "country", "region", "municipality", "street", "street number" and "postal code" basic data components.
- XML Schemas, representing the data exchanged.
- Metadata, which is "data about the data", thus facilitating the retrieval and understanding of the meaning of the data.
- Ontologies, which allow the representation of the correlation of entities involved in eGovernment, their relationships and their metadata in a global, strongly typed and formally described way.

Recommendation 20.

Government organisations shall use XML-based data schemas for the representation of data.

In case Core Data Components are officially defined and standardised in the Cyprus government, government organisations shall try to reuse them in the data schemas to be developed.

Recommendation 21.

Ontologies may be used for the representation of data, in case this is justified by the complexity of the environment (entities, relationships, metadata) to be represented.

7.5 Semantic-based definition languages

Recommendation 22.

Government organisations shall use standardized definition languages for the representation of data, as defined in the eGovernment Interoperability Framework.

Without the use of standardized definition languages, data may probably not be adequately understood by all parties involved in a communication.

8 REFERENCE ARCHITECTURE FOR INTEROPERABILITY

The Cyprus Government has established a reference architecture to be used for the development of government information systems and applications that interoperate, share functionality components and exchange data.

The reference architecture, which adopts the conceptual model for public services introduced by the European Interoperability Framework[4] and is based on Service Oriented Architecture (SOA), is depicted in the following figure:

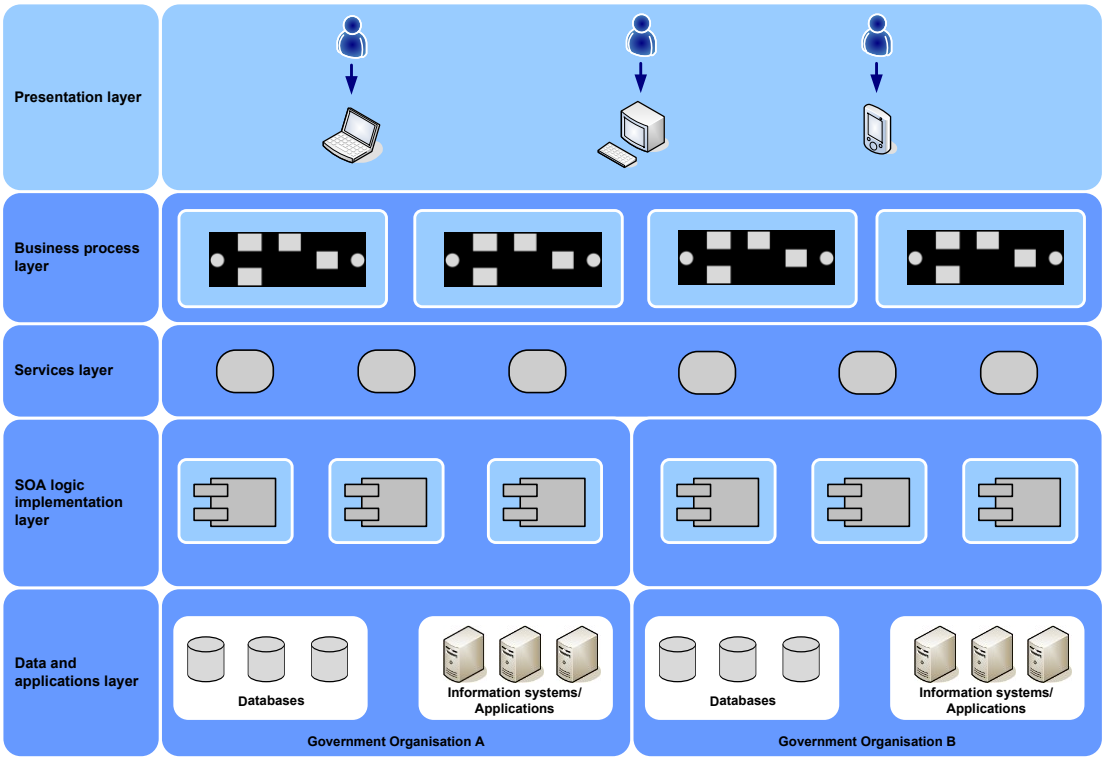

Figure 4: Cyprus Government SOA Architecture

The architecture comprises the following layers:

[4] "European Interoperability Framework - Implementation Strategy", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2017) 134 final, Brussels, 23.3.2017

- The **presentation layer**, which is responsible for the presentation and the delivery of eGovernment services to users (i.e. citizens and businesses) through available channels (web, mobile web).
- The **business process layer**, where the business process workflow is designed and executed. Business processes may be simple, i.e. only one organisation is responsible for them, or complex, i.e. they span across two or more organisations. Orchestration of the business processes is also performed in this layer of the SOA architecture.
- The **services layer**, which is responsible for the publication and registration of all available services implemented at the SOA logic implementation layer to an appropriate services registry so as to facilitate their discovery.
- The **SOA logic implementation layer**, which comprises the components/ services/functions that are used in order to retrieve data from the databases of government information systems for the purposes of the execution of specific government business processes at the higher levels of the architecture. The entire coordination of information sources (i.e. data) and services (provided by information systems and applications) that facilitates the delivery of integrated services to their intended recipients is done at this layer. Web services are most commonly used for this purpose.
- The **data and applications layer**, which consists of the government information systems that support the business processes and the databases that keep the data required for their execution. Base registries, i.e. "*registries that provide reliable sources of basic information on items such as persons, companies, vehicles, licences, buildings, locations and roads*", according to the European Interoperability Framework's definition, are among the databases found at this layer.

Two of the main foundation elements for the realization of the reference architecture and the delivery of integrated electronic services are information sources and services. For the Cyprus eGIF, information sources are considered as the 'providers' of data required for the delivery of an electronic service. On the other hand, information services are those 'basic' services, which, combined with other services, may be used for the development and delivery of an integrated service to citizens, businesses, and other organisations.

Information sources and services reside at the **data and applications layer** of the Reference Architecture and may be 'internal' (i.e. within the government organization that provides the electronic service or within another government organization), or 'external' (i.e. provided by private sector organisations, e.g. EU-level organisations, banks, telecom providers).

Given the commitment of the Cyprus Government to ensure the sustainability of interoperability initiatives[5], the development of a central repository of reusable government artefacts, such as “prototype” process models, web services, XML schemas, code lists, etc. is within its plans. Using this repository, appropriately authorised organisations will be able to search, locate, retrieve, and reuse data and services. Initial proof-of-concept of this repository is the Government Gateway “ARIADNI”, which provides reusable components such as Single-Sign-On services, communication protocol, application submission interface and access to a number of public services provided by other government organisations. Other examples, with focus on open data, are the National Open Data portal (http://www.data.gov.cy), and the Geospatial Information Portal (http://www.geoportal.gov.cy), which supports the implementation the INSPIRE Directive. More information about Cyprus Government IT systems that adhere to the principles of eGIF and materialize its provisions can be found in Appendix D.

As far as external information sources are concerned, open data published by international or private sector organisations may prove to be useful in interoperability initiatives, especially those with a pan-European or international dimension. The same applies to external services, e.g. e-payments, mobile payments, e-invoicing, which have become a commodity in the private sector, thus giving the opportunity to government organisations to capitalize on this experience and achieve significant gains in a relatively short period of time.

[5] Action 3.4.2 of the Cyprus eGovernment Strategy 2014-2020

9 TECHNICAL INTEROPERABILITY

9.1 Introduction

This chapter presents the technical standards of the eGIF grouped in the following categories:

- eGovernment Applications Documentation & Development.
- Service Modelling.
- Data Modelling.
- Application Development Frameworks and Programming Languages.
- Information Presentation and Processing.
- Communication and Interoperability.
- Security and Authentication.
- Standards for specific Business Sectors.

Each of the above categories may include several sub-categories.

Technical standards are classified in three (3) levels according to the definitions presented in section 2.3.1 “Classification of standards”; “Mandatory” (indicated by the letter “M”), “Recommended” (indicated by the letter “R”) and “Under Observation” (indicated by the letter “U”).

9.2 eGovernment Applications Documentation & Development

9.2.1 Modelling Methods

[R01]. Unified Modelling Language			
Abbreviation	**UML**	Custodian	Object Management Group (OMG)
Version	v2.4.1	Announcement date	06.08.2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.omg.org/spec/UML/2.4.1/		

The UML is an Object Management Group (OMG) (http://www.omg.org/) standard which SHOULD BE used for visualizing, specifying, modelling and documenting the components of software systems as well as for modelling business and similar processes, during the design of large scale information systems. The current version of UML, v2.4.1, has been formally published by ISO as the 2012 edition standard: ISO/IEC 19505-1 and 19505-2.

UML is utilized for modelling a system using the UML model and a set of diagrams. A UML model consists of elements such as packages, classes, and associations. The corresponding UML diagrams are graphical representations of parts of the UML model. UML diagrams contain graphical elements (nodes connected by paths) that represent elements in the UML model.

UML diagrams represent two different views of a system model:

- Static (or structural) view: emphasizes the static structure of the system using objects, attributes, operations and relationships. The structural view includes class diagrams and composite structure diagrams.
- Dynamic (or behavioural) view: emphasizes the dynamic behaviour of the system by showing collaborations among objects and changes to the internal states of objects. This view includes sequence diagrams, activity diagrams and state machine diagrams.

In total, there are thirteen (13) types of diagrams grouped in three (3) categories: a) Structure Diagrams, containing six (6) types of diagrams that represent the static structure of the objects in a system, b) Behavioural Diagrams containing three (3) types of diagrams, which illustrate the dynamic behaviour of the objects in a system, and c) Interaction Diagrams containing four (4) types of diagrams, which are a subset of behavioural diagrams and represent the flow of control and data among the objects in the system being modelled.

During object-oriented modelling of large scale information systems, the following four (4) types of UML diagrams SHOULD BE used:

- Component Diagrams, which represent a set of components and their relationships. These components consist of classes, interfaces or collaborations. As such, component diagrams represent the implementation view of a system.
- Use Case Diagrams, which are a set of use cases, actors and their relationships. They represent the use case view of a system, where a use case represents a particular functionality of a system.
- Activity Diagrams, which describe the flow of control in a system using activities and links. The flow can be sequential, concurrent or branched. Activities are nothing but the functions of a system. Numbers of activity diagrams are prepared

to capture the entire flow in a system.

- Sequence Diagrams are interaction diagrams dealing with some sequences, which are the sequence of messages flowing from one object to another. Sequence diagrams are used to visualize the sequence of calls in a system to perform a specific functionality.

[U01]. Unified Modelling Language			
Abbreviation	**UML**	Custodian	Object Management Group (OMG)
Version	v2.5	Announcement date	June 2015
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/UML/2.5/		

Version 2.5 is formally a minor revision to the UML 2.4.1 specification, having been substantially rewritten as solicited by the UML Specification Simplification RFP ad/09-12-10. It supersedes formal/2011-08-05 (Infrastructure) and formal/2011-08-06 (Superstructure). UML 2.5 MAY BE used in the future for visualizing, specifying, modelling and documenting the components of software systems, as well as for modelling business and similar processes, if version v2.4.1 gets superseded or its use is reduced significantly.

9.2.2 Process Models Exchange Schemas

[R02]. XML Process Definition Language			
Abbreviation	**XPDL**	Custodian	Workflow Management Coalition (WfMC)
Version	v2.2	Announcement date	30.08.2012
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.xpdl.org/		

XPDL is an XML-based language, created as a standard from the Workflow Management Coalition (http://bpmexcellence.com/) that SHOULD BE used for the definition and storing of a process diagram in a way that can be exchanged between different process modelling and/or execution tools. This way, a process diagram that

is modelled in a software tool can be captured and imported to another tool with the ability to edit the diagram or "run" the process model on an XPDL-compliant Business Process Management (BPM) engine. Thus, XPDL facilitates the interoperability between BPM software.

XPDL SHOULD BE used to store a one-to-one representation of a BPMN process diagram in case there is a need to exchange BPMN process diagrams. Version 2.2 of XPDL allows existing XPDL users and supporters to continue to exploit their investment in XPDL, whilst extending BPMN support to encompass the new process modeling constructs of BPMN 2.0. XPDL version 2.2 is backward compatible with prior versions of XPDL and can be used as a file format for BPMN 2.0 and BPMN 1.x.

[R03]. XML Metadata Interchange			
Abbreviation	**XMI**	Custodian	Object Management Group (OMG)
Version	v2.4.2	Announcement date	04.04.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/XMI/2.4.2/		

XMI is an Object Management Group (OMG) (http://www.omg.org/) specification which SHOULD BE used for exchanging metadata information via Extensible Markup Language (XML) between models based on the MetaObject Facility (MOF) (http://www.omg.org/mof/) by OMG. UML is a model based on the MOF, which is the foundation technology for describing metamodels. With XMI, model details can be exchanged between different UML tools and other tools that are capable of using XMI, e.g. UML v2.0 – v2.3 model specifications can be imported/ exported from/to XMI v2.1.

XMI is an open, vendor independent, schema standard for model exchange. Version 2.4.2 of XMI has been formally published by ISO as the 2014 edition standard: ISO/IEC 19509:2014.

[U02]. XML Metadata Interchange			
Abbreviation	**XMI**	Custodian	Object Management Group (OMG)
Version	v2.5.1	Announcement date	07.06.2015

Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/XMI/2.5.1/PDF		

XMI v2.5.1 is an updated version of the XMI specification that MAY BE used for exchanging metadata information via Extensible Markup Language (XML) between models based on the MetaObject Facility (MOF) (http://www.omg.org/mof/) by OMG.

[U03]. Canonical XML Metadata Interchange			
Abbreviation	**Canonical XMI**	Custodian	Object Management Group (OMG)
Version	Beta 2	Announcement date	28.08.2013
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/XMI/CanonicalXMI/Beta2/PDF		

Canonical XMI is a specific constrained format of XMI that minimizes variability and provides predictable identification and ordering. Use of Canonical XMI is not mandatory; however it is noted that in general it will be easier, especially for import, for tools to conform to Canonical XMI compared to 'full' XMI – since there is significantly less variation that needs to be handled.

A Canonical XMI file is itself a valid XMI file that MAY BE used for exchanging metadata information in future implementations.

9.3 Service Modelling

9.3.1 Process Modelling Methods

[M01]. Business Process Modelling Notation			
Abbreviation	**BPMN**	Custodian	Object Management Group (OMG)
Version	v2.0.2	Announcement date	December 2013
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.omg.org/spec/BPMN/2.0.2/PDF		

BPMN is a standard developed by the Business Process Management Initiative (BPMI) (http://www.bpmi.org/) and maintained by the Object Management Group (OMG) (http://www.omg.org/). The primary goal of BPMN is to provide a notation that is readily understandable by all business users, from the business analysts that create the initial drafts of the processes, to the technical developers responsible for implementing the technology that will perform those processes, and finally, to the business people who will manage and monitor those processes. Thus, BPMN creates a standardized bridge for the gap between the business process design and process implementation. This is achieved through mapping the appropriate visualization of the business processes (a notation) to the appropriate execution format (a BPM execution language) for these business processes. To this end, another goal of BPMN is to ensure that XML languages designed for the execution of business processes, such as BPEL4WS can be visualized with a business-oriented notation.

BPMN v2.0.2 is an enhanced version of BPMN which introduces new concepts and constructs, such as the Collaboration and Choreography diagrams, the scope of which is to model interactions in a process. Compared to previous version (v1.2) there have been several notational and technical changes to the BPMN Standard.

In addition, part of BPMN v2.0.2 specification is the BPMN DI (Diagram Interchange) meta-model, which is defined as a MOF-based meta-model. The BPMN DI is meant to facilitate interchange of BPMN diagrams between tools. Being a MOF-based meta-model, its instances can be serialized and interchanged using XMI. BPMN DI is also defined by an XML schema. Thus its instances can also be serialized and interchanged using XML.

BPMN v2.0.2 SHALL BE used for the end-to-end representation, definition and documentation of government business processes, especially for those processes related to the provision of eServices to citizens and businesses. The ISO organisation has formally published BPMN version 2.0.2 as an international standard (ISO/IEC

19510:2013), under the general title "*Information technology – Open distributed processing – Business Process Model and Notation (BPMN) specification*".

[R04]. Unified Modelling Language, Activity Diagrams			
Abbreviation	**UML**	Custodian	Object Management Group (OMG)
Version	v2.4.1	Announcement date	06.08.2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.omg.org/spec/UML/2.4.1/		

In accordance to section 9.2.1, Activity Diagrams, which are part of the UML Behavioural Diagrams category, describe the flow of control in a process using activities and links and SHOULD BE used for process modelling in case the BPMN standard cannot be used.

[U04]. Unified Modelling Language			
Abbreviation	**UML**	Custodian	Object Management Group (OMG)
Version	v2.5	Announcement date	June 2015
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/UML/2.5/		

UML 2.5 MAY BE used for process modelling in case the BPMN standard cannot be used and UML v2.4.1 gets superseded or its use is reduced significantly.

9.3.2 Process Execution Languages

[R05]. Web Services Business Process Execution Language			
Abbreviation	**WS-BPEL**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v2.0	Announcement date	11.04.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.pdf		

WS-BPEL is an OASIS (https://www.oasis-open.org/) standard that provides a language for formally describing business processes and business interaction protocols. WS-BPEL was designed to extend the Web Services interaction model to support business transactions. It defines a model and a grammar for describing the behaviour of a business process based on interactions between the process and its partners. The interaction with each partner occurs through Web services interfaces. The WS-BPEL process defines how multiple service interactions with these partners are coordinated to achieve a business goal, as well as the state and the logic necessary for this coordination.

WS-BPEL leverages other Web services standards such as SOAP and WSDL for communication and interface description. By describing the inbound and outbound process interfaces in WSDL, BPEL enables them to be easily integrated into other processes or applications. In turn, this allows consumers of a process to inspect and invoke a BPEL process just like any other Web service, thereby inheriting all other aspects of a Web service such as quality of service policies.

WS-BPEL v2.0 SHOULD BE used for the execution of government business processes.

9.4 Data Modelling

9.4.1 Modelling Methods

[M02]. Entity-Relationship Diagram			
Abbreviation	ERD	Custodian	N/A
Version	N/A	Announcement date	N/A
Registration date	02.12.2013	Revision date	N/A
Reference URL	N/A		

Entity-Relationship diagrams are used to design the entities and relationships of an E-R model, which is a data model utilised for describing a database in an abstract way. ERD SHALL BE used in developing Relational Database schemas during e.g. the stage of database design. ERDs use a notation to represent three (3) different types of information: (i) entity sets (ii) relationships between entity sets and (iii) attributes of entity sets.

[R06]. Unified Modelling Language			
Abbreviation	**UML**	Custodian	Object Management Group (OMG)
Version	v2.4.1	Announcement date	06.08.2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.omg.org/spec/UML/2.4.1/		

UML SHOULD BE used for data modelling in object-oriented software development. In accordance to section 9.2.1, UML Class Diagrams, which are part of the Structured Diagrams category and represent the object oriented view of a system which is static in nature, SHOULD BE used for data modelling when developing object-oriented software.

A Class Diagram shows a collection of static model elements such as classes and types, their contents, and their relationships. More specific, UML Class Diagrams show the classes of the system, their interrelationships (including inheritance, aggregation, and association) and the operations and attributes of the classes. Class Diagrams of an application can also be used by other applications, while relevant XML data structures can be immediately created from relative specifications.

[U05]. Unified Modelling Language			
Abbreviation	**UML**	Custodian	Object Management Group (OMG)
Version	v2.5	Announcement date	June 2015
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/UML/2.5/		

Version 2.5 is formally a minor revision to the UML 2.4.1 specification, having been substantially rewritten as solicited by the UML Specification Simplification RFP ad/09-12-10. UML 2.5 MAY BE used in the future for data modelling in object-oriented software development, if version v2.4.1 gets superseded or its use is reduced significantly.

9.4.2 Data Models Exchange Schemas

[M03]. XML Schema Definition			
Abbreviation	**XSD**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	05.04.2012
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.w3.org/standards/techs/xmlschema		

XML Schemas SHALL BE used for data structure description. XML Schemas SHALL conform to XSD v1.1 specification, as published by W3C (www.w3.org). W3C XSD Specification consists of three parts, of which the first part, numbered zero, is an introductory document. The second part, called Structures, specifies the XML Schema Definition Language, which offers features for describing the structure and constraining the contents of XML documents, including those which exploit the XML Namespace facility. The last part, called Datatypes, defines the features for defining datatypes to be used in XML Schemas as well as other XML specifications. The datatype language, which is itself represented in XML, provides a superset of the capabilities found in XML document type definitions (DTDs) for specifying datatypes on elements and attributes.

[R07]. XML Schema Definition			
Abbreviation	**XSD**	Custodian	World Wide Web Consortium (W3C)
Version	v1.0	Announcement date	28.10.2004
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.w3.org/standards/xml/schema		
XSD version 1.0 SHOULD BE used for data structure description, when XSD version 1.1 cannot be used due to incompatibilities with other pieces of software, or due to other reasons.			

[R08]. XML Metadata Interchange			
Abbreviation	**XMI**	Custodian	Object Management Group (OMG)
Version	v2.4.2	Announcement date	04.04.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/XMI/2.4.2/		
See section 9.2.2.			

[U06]. XML Metadata Interchange			
Abbreviation	**XMI**	Custodian	Object Management Group (OMG)
Version	v2.5.1	Announcement date	07.06.2015
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/XMI/2.5.1/PDF		
See section 9.2.2.			

[U07]. Canonical XML Metadata Interchange			
Abbreviation	**Canonical XMI**	Custodian	Object Management Group (OMG)
Version	Beta 2	Announcement date	28.08.2013
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.omg.org/spec/XMI/CanonicalXMI/Beta2/PDF		
See section 9.2.2.			

9.4.3 Data Exchange Formats

[M04]. Extensible Markup Language			
Abbreviation	**XML**	Custodian	World Wide Web Consortium (W3C)
Version	v1.0 (Fifth edition)	Announcement date	26.11.2008
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2008/REC-xml-20081126/		
XML is a standard language developed by the World Wide Web Consortium (www.w3.org) that SHALL BE used for the structured description of data. Actually, XML is a subset of SGML (http://validator.w3.org/docs/sgml.html) and its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML. The fifth edition incorporates the changes dictated by the accumulated errata (http://www.w3.org/XML/xml-V10-4e-errata) to the Fourth Edition of XML 1.0, dated 16 August 2006.			

[R09]. JavaScript Object Notation			
Abbreviation	**JSON**	Custodian	Internet Engineering Task Force (IETF), ECMA International
Version	N/A	Announcement date	October 2013 (ECMA 404) March 2014 (RFC 7159)
Registration date	13.07.2016	Revision date	N/A
Reference URL	https://tools.ietf.org/html/rfc7159 http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf		

JavaScript Object Notation (JSON) is a lightweight, text-based, language-independent data interchange format that facilitates structured data interchange between all programming languages. It was derived from the object literals of JavaScript a.k.a. ECMAScript Programming Language Standard. JSON format SHOULD BE used for data exchange between different Governmental information systems, especially for the provision of interoperable eGovernment services, as long as the systems are able to support JSON adequately.

[U08]. Extensible Markup Language			
Abbreviation	**XML**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1 (Second edition)	Announcement date	16.08.2006
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2006/REC-xml11-20060816/		

XML v1.1 is not a new version of XML, but rather a parallel version which MAY BE used for the structured description of data. In particular, XML v1.1 was created due to changes in the Unicode Standard (from version 2.0 to version 4.0 and beyond), on which XML v1.0 relies for character specifications. Characters not present in Unicode

2.0 may already be used in XML 1.0 character data. However, they are not allowed in XML names such as element type names, attribute names, enumerated attribute values, processing instruction targets, and so on. In addition, some characters that should have been permitted in XML names were not, due to oversights and inconsistencies in Unicode 2.0.

For that reason, the overall philosophy of names has changed since XML 1.0. Whereas XML 1.0 provided a rigid definition of names, wherein everything that was not permitted was forbidden, XML 1.1 names are designed so that everything that is not forbidden (for a specific reason) is permitted. Since Unicode will continue to grow past version 4.0, further changes to XML can be avoided by allowing almost any character, including those not yet assigned, in names.

The distinction between XML 1.0 and XML 1.1 documents is indicated by the version number information in the XML declaration at the start of each document.

9.4.4 Data Transformation

[M05]. Extensible Stylesheet Language Transformation			
Abbreviation	**XSLT**	Custodian	World Wide Web Consortium (W3C)
Version	v2.0	Announcement date	23.01.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2007/REC-xslt20-20070123/		

XSLT is a W3C (www.w3.org) standard that SHALL BE used in case there is a need to transform an XML schema used by a system, in order to interoperate with another system that uses a different XML schema. XSLT is designed for use as part of XSL, which is a stylesheet language for XML, presented in section 9.6.3. In addition to XSLT, XSL includes an XML vocabulary for specifying formatting. XSL specifies the styling of an XML document by using XSLT to describe how the document is transformed into another XML document that uses the formatting vocabulary.

XSLT is also designed to be used independently of XSL. However, XSLT is not intended as a completely general-purpose XML transformation language. Rather it is designed primarily for the kinds of transformations that are needed when XSLT is used as part of XSL.

XSLT v2.0 is a revised version of the XSLT 1.0 Recommendation published on 16 November 1999. Many new features have been added to the language with this new

version, while retaining a high level of backwards compatibility.

9.4.5 Metadata Schema

[M06]. Dublin Core Metadata Element Set			
Abbreviation	**Dublin Core**	Custodian	Dublin Core Metadata Initiative (DCMI)
Version	v1.1	Announcement date	14.06.2012
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://dublincore.org/documents/dces/		

The Dublin Core Metadata Element Set is a Dublin Core Metadata Initiative (DCMI, dublincore.org) recommendation that SHALL BE used for the description of metadata of services, documents and/or web pages. The Dublin Core Metadata standard contains a vocabulary of fifteen properties for use in resource description. The fifteen element "Dublin Core" described in this standard is part of a larger set of metadata vocabularies and technical specifications maintained by the DCMI. The Dublin Core Metadata Element Set has been formally endorsed in the following standards:

- ISO Standard 15836:2009 of February 2009 (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52142).
- ANSI/NISO Standard Z39.85-2007 of May 2007 (http://www.niso.org/apps/group_public/project/details.php?project_id=57).
- IETF RFC 5013 of August 2007 (http://www.ietf.org/rfc/rfc5013.txt).

Each of the fifteen Dublin Core elements corresponds to an attribute of the resource being described, where this attribute is assigned a specific value. Dublin Core elements can be used in HTML/XHTML documents, as well as in RDF/XML documents. The fifteen elements are the following: (1) Title, (2) Creator, (3) Subject, (4) Description, (5) Publisher, (6) Contributor, (7) Date, (8) Type, (9) Format, (10) Identifier, (11) Source, (12) Language, (13) Relation, (14) Coverage and (15) Rights.

9.4.6 Metadata Description

[M07]. Resource Description Framework			
Abbreviation	**RDF**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	25.02.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	https://www.w3.org/TR/2014/REC-rdf-schema-20140225/		

The Resource Description Framework (RDF) is a language created by the W3 Consortium (www.w3.org) that SHALL BE used for representing information about resources in the World Wide Web. The RDF recommendation consists of a set of six documents (Primer, Concepts, Syntax, Semantics, Vocabulary, and Test Cases) intended to jointly replace the original Resource Description Framework specifications, RDF Model and Syntax (1999 Recommendation) and RDF Schema (2000 Candidate Recommendation). It has been developed by the RDF Core Working Group as part of the W3C Semantic Web Activity. Changes compared to previous version (v1.0) are limited to errata, revised references, terminology updates, and adaptations to the introduction. The technical content of the standard's document is unchanged.

RDF is particularly intended for representing metadata about Web resources, such as the title, author, and modification date of a Web page, copyright and licensing information of a Web document, or the availability schedule for some shared resources. RDF can also be used to represent information about things that can be identified on the Web, even when they cannot be directly retrieved on the Web (e.g., information about specifications, prices, and availability of products in an online shop). RDF provides a common framework for expressing the information mentioned above so it can be exchanged between applications without loss of meaning.

9.4.7 Semantic Information Representation Languages

[M08]. Extensible Markup Language			
Abbreviation	**XML**	Custodian	World Wide Web Consortium (W3C)
Version	v1.0 (Fifth edition)	Announcement date	26.11.2008
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2008/REC-xml-20081126/		

See section 9.4.3.

[R10]. Web Ontology Language			
Abbreviation	**OWL**	Custodian	World Wide Web Consortium (W3C)
Version	v2.0	Announcement date	11.12.2012
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.w3.org/TR/2012/REC-owl2-overview-20121211/		

The OWL Web Ontology Language is designed for use by applications that need to process the content of information instead of just presenting information to humans. OWL facilitates greater machine interpretability of Web content than that supported by XML and RDF by providing additional vocabulary along with formal semantics. OWL can be used to explicitly represent the meaning of terms in vocabularies and the relationships between those terms. This representation of terms and their interrelationships is called ontology. OWL is a revision of the DAML+OIL web ontology language incorporating lessons learned from the design and application of DAML+OIL.

OWL v2.0 SHOULD BE used for the description of semantic data models. The OWL v2.0 is an extension and revision of the OWL v1.0 published in 2004. OWL v2.0 ontologies provide classes, properties, individuals, and data values and are stored as Semantic Web documents. OWL v2.0 ontologies can be used along with information written in RDF, and OWL v2.0 ontologies themselves are primarily exchanged as RDF documents.

[U09]. Extensible Markup Language			
Abbreviation	**XML**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1 (Second edition)	Announcement date	16.08.2006
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2006/REC-xml11-20060816/		
See section 9.4.3.			

[U10]. Core Components Technical Specification			
Abbreviation	**CCTS**	Custodian	UN Centre for Trade Facilitation and e-Business (UN/CEFACT)
Version	v3.0	Announcement date	29.09.2009
Registration date	27.07.2016	Revision date	N/A
Reference URL	http://www.unece.org/fileadmin/DAM/cefact/codesfortrade/CCTS/CCTS-Version3.pdf		

The Core Components Technical Specification (CCTS) defines a meta model and rules that MAY BE used for describing the structure and contents of conceptual and logical data models and information exchange models. The CCTS is described using the Unified Modeling Language (UML), however UML is not required in CCTS implementation. CCTS can be employed wherever data is being defined, stored, used, shared or exchanged. It is especially well suited for defining data models and for creating data exchange standards for information flows amongst and between enterprises, governmental agencies, and/ or other organizations in an open, global environment. The CCTS specification describes an approach for developing a common set of semantic building blocks that represent the general types of business data in use today. This approach provides for the creation of new business vocabularies as well as restructuring of existing business vocabularies to achieve semantic interoperability of data. CCTS complements traditional data modelling techniques.

9.5 Application Development Frameworks & Programming Languages

[M09]. Java Platform, Standard Edition (Java SE)			
Abbreviation	Java SE	Custodian	Oracle Corporation
Version	v8 (update 92)	Announcement date	18.03.2014 (initial release) 19.04.2016 (update 92 release)
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.oracle.com/technetwork/java/javase/overview/index.html		

Java Platform, Standard Edition (Java SE) is a platform specification that SHALL BE used for development and deployment of portable applications for desktop and server environments. The Java Platform SE has two components: (a) The Java Virtual Machine and (b) The Java Application Programming Interface (API). The API is a large collection of ready-made software components that provide many useful capabilities. It is grouped into libraries of related classes and interfaces, known as packages. The Java platform is a platform-independent environment, being a software-only platform that runs on top of other hardware-based platforms. One of the most well-known implementations of Java SE is Oracle Corporation's Java Development Kit (JDK).

The Java Development Kit (JDK) is an implementation of either one of the Java SE, Java EE or Java ME platforms released by Oracle Corporation in the form of a binary product aimed at Java developers on Solaris, Linux, Mac OS X or Windows. Since its introduction, the Java platform has been by far the most widely used Software Development Kit (SDK). It includes tools for developing, debugging, and monitoring Java applications. JDK became in large part free software on 8 May 2007, when Sun contributed the source code to the OpenJDK.

[M10]. Java Platform, Enterprise Edition (Java EE)			
Abbreviation	Java EE	Custodian	Oracle Corporation
Version	v7	Announcement date	28.05.2013
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.oracle.com/technetwork/java/javaee/overview/index.html		

Java Platform, Enterprise Edition (Java EE) is developed using the Java Community Process, with contributions from industry experts, commercial and open source organizations, Java User Groups, and countless individuals. Java EE offers an enterprise software platform which provides an API and runtime environment for developing and running enterprise software, including network and web services, and other large-scale, multi-tiered network applications.

The platform incorporates a design based largely on modular components running on an application server. The Java EE application model begins with the Java programming language and the Java virtual machine. Java EE is designed to support applications that implement enterprise services for customers, employees, suppliers, partners, and others who make demands on or contributions to the enterprise. Such applications are inherently complex, potentially accessing data from a variety of sources and distributing applications to a variety of clients. Java EE SHALL BE used in software development for multi-tiered applications, where the business functions that support the various users of the applications are executed in the middle tier.

Java EE includes several API specifications, such as JDBC, RMI, e-mail, JMS, web services, XML, etc., and defines how to coordinate them. Java EE also features some specifications unique to Java EE for components. These include Enterprise JavaBeans, Connectors, servlets, JavaServer Pages and several web service technologies. This allows developers to create enterprise applications that are portable and scalable, and that integrate with legacy technologies. The Java EE APIs includes several technologies that extend the functionality of the base Java SE APIs, such as Java Message Service (JMS), J2EE Connector Architecture (JCA), Java Transaction API (JTA), JavaMail API, Java API for XML Registries (JAXR), Java Management Extensions (JMX), Enterprise JavaBeans (EJB), Web Services, Java Server Pages (JSP) and Servlet API.

[R11]. .NET Framework			
Abbreviation	.NET	Custodian	Microsoft Corporation
Version	v4.6.1	Announcement date	17.11.2015
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.microsoft.com/net		

.NET Framework is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It is used for building applications for Windows, Windows Phone, Windows Server, and Windows Azure. It consists of the common language runtime (CLR) and the .NET Framework class library, which is a collection of reusable types (classes, interfaces, and value types) that tightly integrate with the common language runtime and support an extensive range of technologies. .NET Framework contains a Base Class Library that provides user interface, data access, database connectivity, cryptography, web application development, numeric algorithms, and network communications. The framework provides language interoperability (each language can use code written in other languages) across several programming languages. Programmers produce software by combining their own source code with .NET Framework and other libraries. .NET Framework SHOULD BE used for developing web applications, service-oriented applications and/or workflow-enabled applications.

[R12]. JavaScript			
Abbreviation	N/A	Custodian	ECMA International, Mozilla Foundation, Netscape Communications Corporation
Version	1.8.5	Announcement date	27.07.2010
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-262.pdf		

JavaScript is an object-oriented programming language, based on the ECMAScript Language Specification (ECMA-262), for performing computations and manipulating computational objects within a host environment. ECMAScript was originally designed

to be a Web scripting language, providing a mechanism to enliven Web pages in browsers and to perform server computation as part of a Web-based client-server architecture. However, ECMAScript usage has moved beyond simple scripting and it is now used for the full spectrum of programming tasks in many different environments and scales. JavaScript, being based on ECMAScript, has become one of the most popular programming languages on the Web, supported by all modern Web browsers without plug-ins. Alongside HTML and CSS, it is one of the three core technologies of World Wide Web content production. JavaScript SHOULD BE used for web scripting when developing portals, sites and/ or information systems in a web-based environment, mostly for the client-side but also for server-side programming, if feasible.

[U11]. Java Platform, Mobile Edition (Java ME)			
Abbreviation	Java ME	Custodian	Oracle Corporation
Version	v8	Announcement date	30.04.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.oracle.com/technetwork/java/javame/index.html		

Java Platform, Mobile Edition (Java ME) is a platform specification that MAY BE used for development and deployment of applications for mobile devices. Java ME provides a robust, flexible environment for applications running on embedded and mobile devices: microcontrollers, sensors, gateways, mobile phones, personal digital assistants (PDAs), TV set-top boxes, printers and more. Java ME platform is a collection of technologies and specifications that can be combined to construct a complete Java runtime environment specifically to fit the requirements of a particular device or market. With Java ME technology it is possible to create Java applications running on small devices with limited memory, display and power capacity. The Java ME technology is based on three elements:

- A configuration provides the most basic set of libraries and virtual machine capabilities for a broad range of devices,
- A profile is a set of APIs that support a narrower range of devices, and
- An optional package is a set of technology-specific APIs.

Over time the Java ME platform has been split into two base configurations; one to fit small mobile devices and one to be targeted towards more powerful devices like smart-phones and set top boxes. The configuration for small devices is called the Connected Limited Device Configuration (CLDC) and the more capable configuration

is called the Connected Device Configuration (CDC). As of 22 December 2006, the Java ME source code is licensed under the GNU General Public License.

9.6 Information Presentation and Processing

9.6.1 Accessibility

[M11]. Web Content Accessibility Guidelines			
Abbreviation	**WCAG**	Custodian	World Wide Web Consortium (W3C)
Version	v2.0	Announcement date	11.12.2008
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/WCAG20/		

Web Content Accessibility Guidelines (WCAG) is a technical standard developed by Web Accessibility Initiative (WAI), which is part of W3C, through the W3C process (http://www.w3.org/WAI/intro/w3c-process.php) in cooperation with individuals and organizations around the world, with a goal of proving a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally. The guidelines set by WCAG v2.0, at least at the AA level, SHALL BE followed during design and implementation of web-based applications, in order for the web content managed by those applications to be more accessible by people with disabilities.

WCAG 2.0 has been approved as an ISO standard, ISO/IEC 40500:2012.

[R13]. Mobile Web Best Practices			
Abbreviation	N/A	Custodian	World Wide Web Consortium (W3C)
Version	v1.0	Announcement date	29.07.2008
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2008/REC-mobile-bp-20080729/		

Mobile Web Best Practices are a series of recommendations designed to improve the user experience of Web browsing on mobile devices that SHOULD BE used when

designing and implementing applications for mobile devices. The Best Practice recommendations refer to delivered content. While they are clearly relevant to the processes of content creation and rendering on devices, they are not intended to be Best Practices for those activities. The recommendations are in part derived from the Web Content Accessibility Guidelines (WCAG), with their scope limited to matters that have a specific mobile relevance.

9.6.2 Hypertext Exchange Schemas

[M12]. Hyper Text Markup Language			
Abbreviation	**HTML**	Custodian	World Wide Web Consortium (W3C)
Version	v4.01	Announcement date	24.12.1999
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/html4		

HTML SHALL BE used for publishing information in the form of hypertext to the World Wide Web. HTML is a universally understood language that serves as the publishing language used by the World Wide Web. HTML gives authors the means to:

- Publish online documents with headings, text, tables, lists, photos, etc.
- Retrieve online information via hypertext links, at the click of a button.
- Design forms for conducting transactions with remote services, for use in searching for information, making reservations, ordering products, etc.
- Include spread-sheets, video clips, sound clips, and other applications directly in their documents.

[R14]. Hyper Text Markup Language			
Abbreviation	**HTML**	Custodian	World Wide Web Consortium (W3C)
Version	v5	Announcement date	28.10.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	https://www.w3.org/TR/2014/REC-html5-20141028/		

HTML 5 specification defines the 5th major revision of the Hypertext Markup Language (HTML). In this version, new features are introduced to help Web application authors, new elements are introduced based on research into prevailing authoring practices, and special attention has been given to defining clear conformance criteria for user agents in an effort to improve interoperability.

HTML 5 SHOULD BE used for publishing information in the form of hypertext to the World Wide Web.

[R15].	**Extensible Hyper Text Markup Language**		
Abbreviation	**XHTML**	Custodian	World Wide Web Consortium (W3C)
Version	v1.0	Announcement date	01.08.2002
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/xhtml1		

XHTML is a family of current and future document types and modules that reproduce, subset, and extend HTML 4. It is a reformulation of the three HTML 4 document types as applications of XML 1.0. It is intended to be used as a language for content that is both XML-conforming and, if some simple guidelines are followed, operates in HTML 4 conforming user agents. XTHML v1.0 SHOULD BE used for publishing information in the form of hypertext.

[R16].	**Extensible HyperText Markup Language Basic**		
Abbreviation	**XHTML Basic**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	23.11.2010
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.w3.org/TR/2010/REC-xhtml-basic-20101123/		

The XHTML Basic document type includes the minimal set of modules required to be an XHTML host language document type, and in addition it includes images, forms, basic tables, and object support. It is designed for Web clients that do not support the full set of XHTML features; for example, Web clients such as mobile phones, PDAs,

pagers, and set top boxes. The document type is rich enough for content authoring.

XTHML Basic v1.1 SHOULD BE used for publishing information in the form of hypertext in mobile devices.

9.6.3 Stylesheets

[M13]. Cascading Style Sheets			
Abbreviation	**CSS**	Custodian	World Wide Web Consortium (W3C)
Version	v2.1	Announcement date	07.06.2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2011/REC-CSS2-20110607/		

CSS is a style sheet language that allows authors and users to attach style (e.g., fonts and spacing) to structured documents (e.g., HTML documents and XML applications). By separating the presentation style of documents from the content of documents, CSS simplifies Web authoring and site maintenance. CSS v2.1 SHALL BE used for manipulating the presentation style (the look and formatting) of markup language documents. CSS includes elements such as the layout, colours and fonts. CSS can also allow the same markup page to be presented in different styles for different rendering methods, such as on-screen, in print, by voice (when read out by a speech-based browser or screen reader) and on Braille-based, tactile devices. It can also be used to allow the web page to display differently depending on the screen size or device on which it is being viewed. CSS v2.1 is revision of CSS v2.0 that fixes errors, removed poorly supported or not fully interoperable features and added already-implemented browser extensions to the specification.

[M14]. Extensible Stylesheet Language			
Abbreviation	**XSL**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	05.12.2006
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/xsl/		

XSL is a language for expressing stylesheets that SHALL BE used for specifying the presentation of XML documents. XSL consists of two parts:

- a language for transforming XML documents (XSLT);
- an XML vocabulary for specifying formatting semantics.

XSL stylesheet is used by designers to express their intentions about how the content of arbitrarily structured XML documents or data files should be presented; that is, how the source content should be styled, laid out, and paginated onto some presentation media, such as a window in a Web browser or a hand-held device, or a set of physical pages in a catalogue, report or book.

9.6.4 Character Sets Encoding

[M15]. Unicode UTF-8			
Abbreviation	UTF-8	Custodian	Unicode Consortium
Version	v6.2	Announcement date	26.09.2012
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.unicode.org/		

The Unicode Standard is a character coding system designed to support the worldwide interchange, processing, and display of the written texts of the diverse languages and technical disciplines of the modern world. In addition, it supports classical and historical texts of many written languages. The standard consists of a set of code charts for visual reference, an encoding method and set of standard character encodings, a set of reference data computer files, and a number of related items, such as character properties, rules for normalization, decomposition, collation, rendering, and bidirectional display order (for the correct display of text containing both right-to-left scripts, such as Arabic and Hebrew, and left-to-right scripts). UTF-8 character encoding of Unicode standard SHALL BE used for the encoding of characters in markup language documents. Version 6.2 of the standard is standardised from ISO organisation in ISO/IEC 10646:2012 standard.

9.6.5 Date & Time Representation

[M16]. ISO 8601			
Abbreviation	ISO 8601	Custodian	International Organization for Standardization (ISO)
Version	8601:2004	Announcement date	01.12.2004
Registration date	27.07.2016	Revision date	N/A
Reference URL	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40874		

ISO 8601 is an international standard that SHALL BE used for the exchange of date and time-related data. Its purpose is to provide an unambiguous and well-defined method of representing dates and times, in order to avoid misinterpretation of numeric representations of dates and times, particularly when data are transferred between countries with different conventions for writing numeric dates and times. The standard uses the Gregorian calendar, which serves as an international standard for civil use. The ISO 8601 standard includes also representation formats for time zone designators, durations, time intervals etc.

9.6.6 File Formats Recognition

[M17]. Multipurpose Internet Mail Extensions			
Abbreviation	**MIME**	Custodian	The Internet Engineering Task Force (IETF)
Version	v1.0 (RFC 2045 – RFC 2049)	Announcement date	November 1996
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.ietf.org/rfc/rfc2045.txt		

Multipurpose Internet Mail Extensions (MIME) is an Internet standard developed and maintained by IETF (www.ietf.org) working groups that describes the content type in general including the web, and as storage for rich content in some commercial

products. MIME SHALL BE used for the standardised definition of file format types or a part of them. MIME facilitates an e-mail client or a web browser to identify the type of a file format. MIME is specified in six linked RFC memoranda: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2049, which together define the specifications.

9.6.7 Document Formats for Information Exchange

[M18]. Portable Document Format			
Abbreviation	**PDF**	Custodian	Adobe Systems
Version	v1.7 (Sixth edition)	Announcement date	01.07.2008
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.adobe.com/devnet/pdf/pdf_reference.html http://www.iso.org/iso/catalogue_detail.htm?csnumber=51502		

PDF is a standard for electronic information exchange via documents that SHALL BE used as the standard text document format, in case there isn't the need for further editing and/or changing the document. The initial scope of PDF documents was to enable users to exchange and view electronic documents easily and reliably, independently of the environment in which they were created. PDF relies on the same imaging model as the Postscript page description language to describe text and graphics in a device-independent and resolution-independent manner. To improve performance for interactive viewing, PDF defines a more structured format than that used by most Postscript language programs. The MIME identifier for PDF files is "application/pdf".

In January 2007, Adobe announced its intention to release the full Portable Document Format (PDF) 1.7 specification to AIIM, the Enterprise Content Management Association, for the purpose of publication by the International Organization for Standardization (ISO). During July 2008 this was completed, with ISO publishing the approved ISO 32000-1 standard, which was based upon the sixth edition of PDF v1.7 specification. The ISO standard ISO 32000-1:2008 and Adobe PDF 1.7 are technically consistent and after that Adobe announced that it will not produce a PDF 1.8 Reference. Future versions of the PDF Specification will be produced by ISO technical committees. However, Adobe published documents specifying what extended features for PDF, beyond ISO 32000-1 (PDF 1.7), are supported in its newly released products. This makes use of the extensibility features of PDF as documented in ISO

32000-1 in Annex E.

[M19]. Hyper Text Markup Language			
Abbreviation	**HTML**	Custodian	World Wide Web Consortium (W3C)
Version	v4.01	Announcement date	24.12.1999
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/html4		
Hypertext documents that are used during information exchange (e.g. newsletters) SHALL BE represented in HTML format (See section 9.6.2).			

[R17]. Hyper Text Markup Language			
Abbreviation	**HTML**	Custodian	World Wide Web Consortium (W3C)
Version	v5	Announcement date	28.10.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	https://www.w3.org/TR/2014/REC-html5-20141028/		
See section 9.6.2.			

9.6.8 Document Formats for Information Processing

[M20]. Text			
Abbreviation	**TXT**	Custodian	N/A
Version	N/A	Announcement date	N/A
Registration date	02.12.2013	Revision date	N/A
Reference URL	N/A		
Simple text files for which there is a need for editing and commenting SHALL BE transferred using the widely known plain text (.txt) file format, in order to ensure the			

accessibility and readability of the document. The character set that SHALL BE used in these text files is defined in section 9.6.4. The MIME identifier for TXT files is "text/plain".

[M21]. Open Document Format			
Abbreviation	**ODF**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.2	Announcement date	29.09.2011
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://docs.oasis-open.org/office/v1.2/os/OpenDocument-v1.2-os.zip		

The OpenDocument Format (ODF) is an open XML-based document file format for office applications, developed and maintained from OASIS (https://www.oasis-open.org/) technical committees that SHALL BE used for documents containing text, spreadsheets, charts, and graphical elements like drawings or presentations. The file format makes transformations to other formats simple by leveraging and reusing existing standards wherever possible. The aim is to provide an open, XML-based file format specification for office applications. ODF benefits from separation of concerns by separating the content, styles, metadata, and application settings into four separate XML files.

The most common filename extensions used for OpenDocument documents are:

- .odt and .fodt for word processing (text) documents
- .ods and .fods for spreadsheets
- .odp and .fodp for presentations
- .odb for databases
- .odg and .fodg for graphics
- .odf for formulas, mathematical equations

ODF is used in free software and in proprietary software. This includes office suites (both stand-alone and web-based) and individual applications such as word-processors, spreadsheets, presentation, and data management applications.

ODF version 1.2 is published as an ISO/IEC international family of standards, namely

the ISO/IEC 26300-1:200615, ISO/IEC 26300-2:200615 and ISO/IEC 26300-3:200615 — Open Document Format for Office Applications (OpenDocument) v1.2. Some governments around the world have come to view open formats like ODF as a public policy issue, since their main objective is to guarantee long-term access to data without legal or technical barriers. As a result, several governments around the world have introduced policies of partial or complete adoption.

[M22]. Office Open XML			
Abbreviation	**OOXML**	Custodian	Microsoft Corporation, ECMA, ISO/IEC
Version	ISO/IEC 29500:2012 ECMA-376:2012	Announcement date	22.08.2012 (ISO) December 2012 (ECMA)
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61750 http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-376,%20Fourth%20Edition,%20Part%201%20-%20Fundamentals%20And%20Markup%20Language%20Reference.zip		

OOXML is an XML-based file format initially developed by Microsoft Corporation that SHALL BE used for representing spreadsheets, charts, presentations and word documents. Actually, OOXML is a set of XML schemas that define the XML vocabularies for word documents, spreadsheets and presentations, as well as the packaging of documents that conform to these schemas. The goal is to enable the implementation of the Office Open XML formats by the widest set of tools and platforms, fostering interoperability across office productivity applications and line-of-business systems, as well as to support and strengthen document archival and preservation, all in a way that is fully compatible with the existing corpus of Microsoft Office documents.

OOXML was initially standardised by ECMA (http://www.ecma-international.org/default.htm) as ECMA-376 (1st edition in December 2006), where the standardisation was co-sponsored by Microsoft. Later, in April 2008, ISO/IEC concluded in turn the standardisation of OOXML as the ISO/IEC 29500:2008 standard. Following, a technically equivalent set of texts was published by ECMA as

ECMA-376 Office Open XML File Formats - 2nd edition (December 2008). Since then, the two international organisations retain their own standards that are technically aligned. The OOXML format became the default file format in Microsoft Office application suite as of version 2007.

9.6.9 Graphics Exchange Formats

[M23]. Graphics Interchange Format			
Abbreviation	**GIF**	Custodian	CompuServe Incorporated
Version	v89a	Announcement date	31.07.1990
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/Graphics/GIF/spec-gif89a.txt		

The GIF graphics and images file formation standard, which was developed by CompuServe Incorporated (www.compuserve.com), SHALL BE used for the exchange of graphic and diagram files. GIF standard compresses the graphic files with a colour depth of 256 colours (8 bit per pixel). GIF is well-suited for simpler images such as graphics or logos with solid areas of colour but unsuitable for reproducing colour photographs and other images with continuous colour due to palette limitations.

GIF is the copyright property of CompuServe Incorporated, which is the sole authorized to define, redefine, enhance, alter, modify or change in any way the definition of the format. However, GIF is an open format, since CompuServe Incorporated has granted a limited, non-exclusive, royalty-free license for the use of GIF in computer software.

[M24]. Joint Photographic Experts Group			
Abbreviation	**JPEG**	Custodian	Independent JPEG Group/JPEG Committee
Version	v1.02	Announcement date	18.09.1992
Registration date	02.12.2013	Revision date	N/A

Reference URL	https://jpeg.org/jpeg/index.html

JPEG is a file format standard, initially developed by the Independent JPEG Group (www.ijg.org) and maintained by the JPEG Committee (www.jpeg.org) that SHALL BE used for image and picture files exchange. The format uses lossy compression in image files, where the compression level can be adjusted, allowing a trade-off between storage size and image quality based on user's choices. JPEG typically achieves 10:1 compression with little perceptible loss in image quality, and is the file type most often produced in digital photography. JPEG standard supports 17,7 million colours (24-bit per pixel). JPEG/JFIF is the most common format for storing and transmitting photographic images on the World Wide Web.

JPEG standard has been initially standardised from ISO/IEC as the ISO/IEC 10918-1:1994 standard; followed by ISO/IEC 10918-2:1995, ISO/IEC 10918-3:1997 and ISO/IEC 10918-4:1999. Also, JPEG standard has been standardised by ITU-T (www.itu.int) as Recommendation T.81.

The MIME identifier for JPEG is "image/jpeg", except in Internet Explorer, which provides a MIME identifier of "image/pjpeg" when uploading JPEG images. The most common filename extensions for files employing JPEG compression are .jpg and .jpeg, though .jpe, .jfif and .jif are also used.

[R18]. Portable Network Graphics			
Abbreviation	**PNG**	Custodian	World Wide Web Consortium (W3C)
Version	Second edition	Announcement date	10.11.2003
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2003/REC-PNG-20031110		

Portable Network Graphics (PNG) is an extensible file format for the portable, well-compressed storage of raster images that supports lossless data compression. PNG format SHOULD BE used for publishing and/or transferring image files on the Internet, through online applications such as a web browser.

PNG format supports indexed-colour, grayscale and true-colour images, plus an optional alpha channel. Sample depths range from 1 to 16 bits. PNG is robust, providing both full file integrity checking and simple detection of common transmission errors. Also, PNG can store gamma and chromaticity data for improved colour matching on heterogeneous platforms. PNG was not designed for professional-quality

print graphics, and therefore does not support non-RGB colour spaces such as CMYK.

The MIME identifier for PNG is “image/png”. PNG became the ISO/IEC 15948:2004 international standard, which was published in March 2004 (http://www.iso.org/iso/catalogue_detail?csnumber=29581).

[R19].	**Tagged Image File Format**		
Abbreviation	**TIFF**	Custodian	Adobe Systems
Version	v6.0	Announcement date	03.06.1992
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf		

TIFF file format, initially developed by Aldus Corporation and maintained by Adobe Systems (www.adobe.com), SHOULD BE used to store binary graphic and image files (bitmaps). TIFF describes image data that typically comes from scanners, frame grabbers and paint- and photo-retouching programs. TIFF is supported by all major graphic and photo application viewers.

The MIME identifier for TIFF is “image/tiff” and “image/tiff-fx”.

[R20].	**Scalable Vector Graphics**		
Abbreviation	**SVG**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1 (Second edition)	Announcement date	16.08.2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2011/REC-SVG11-20110816/		

SVG format is a modularized language for describing two-dimensional vector and mixed vector/raster graphics in XML that SHOULD BE used for exchanging vector graphic file types. SVG allows for three types of graphic objects: vector graphic shapes (e.g. paths consisting of straight lines and curves), images and text. Graphical objects can be grouped, styled, transformed and composited into previously rendered objects. The feature set includes nested transformations, clipping paths, alpha masks,

filter effects and template objects.

SVG drawings can be interactive and dynamic. Animations can be defined and triggered either declaratively (i.e. by embedding SVG animation elements in SVG content) or via scripting. The MIME identifier for SVG is "image/svg+xml".

[U12]. Joint Photographic Experts Group			
Abbreviation	**JPEG**	Custodian	Independent JPEG Group/JPEG Committee
Version	2000	Announcement date	December 2000
Registration date	24.01.2014	Revision date	N/A
Reference URL	https://jpeg.org/jpeg2000/index.html		

JPEG 2000 is a new image coding system that uses state-of-the-art compression techniques based on wavelet technology. Its architecture should lend itself to a wide range of uses from portable digital cameras through to advanced pre-press, medical imaging and other key sectors. JPEG 2000 MAY BE used for image and picture files exchange.

9.6.10 Sound, Video and Video Streaming Formats

[M25]. Moving Picture Expert Group-4 Part 14			
Abbreviation	**MPEG-4**	Custodian	Moving Picture Experts Group (MPEG)
Version	v2	Announcement date	31.03.2009
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://mpeg.chiariglione.org/standards/mpeg-4		

MPEG is a method of defining compression of audio and visual (AV) digital data that SHALL BE used for the compression and transmission of audio and video data in web (streaming media) and CD distribution, as well as for voice (telephone, videophone). The standard has been developed by the Moving Picture Experts Group (http://mpeg.chiariglione.org/), a working group of experts that was formed by ISO and IEC, designated as ISO/IEC JTC1/SC29 WG11 – Coding of moving pictures and

audio.

MPEG has been standardised from ISO in 1998 as the ISO/IEC 14496 standard. The standard has 30 parts, where part 14 defines the MPEG-4 file format which SHALL BE used for the exchange of multimedia video files and for video streaming over the internet. The second version of MPEG-4 file format has been standardised as ISO/IEC 14496-14:2003. MPEG-4 is an open standard, supported by numerous tools and applications in the field of multimedia management, for different platforms.

[M26]. OGG Vorbis			
Abbreviation	**OGG**	Custodian	Xiph.Org Foundation
Version	Vorbis I	Announcement date	03.02.2012
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.xiph.org/vorbis/doc/Vorbis_I_spec.html		

Ogg Vorbis is a completely open, patent-free, audio encoding and streaming technology that SHALL BE used to compress audio files for exchange and/or playback over the internet. Vorbis is the file format, created in the scope of a free and open-source software project headed by the Xiph.Org Foundation (formerly Xiphophorus company – www.xiph.org). The project produces an audio format specification and software implementation (codec) for lossy audio compression. Ogg is the container format mostly used for Vorbis format files.

The MIME identifiers (see section 9.6.6) for OGG Vorbis used are “application/ogg”, “audio/ogg”, “audio/vorbis” and “audio/vorbis-config”.

[R21]. QuickTime			
Abbreviation	QuickTime	Custodian	Apple Inc.
Version	v7.7.x	Announcement date	23.08.2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.apple.com/quicktime/		

QuickTime is an extensible multimedia framework developed by Apple Inc., capable of handling various formats of digital video, picture, sound, panoramic images, and interactivity. QuickTime File Format (QTFF) SHOULD BE used for video sequences exchange. The QuickTime framework provides encoding and transcoding video and

audio from one format to another, decoding video and audio and a "component" plug-in architecture for supporting additional 3rd-party codecs (such as DivX).

QuickTime is bundled with OS X and is available as a downloadable, standalone installation for Microsoft Windows, free of charge only for basic playback operations. For additional features, such as editing clips, saving and exporting to other coding formats, saving existing QuickTime movies from the web directly to a hard disk drive etc., a professional license must be purchased by Apple.

The ISO/IEC 14496-12 standard (MPEG-4 part 12) was created on the basis of the QuickTime format specification.

[U13]. WebM			
Abbreviation	**WebM**	Custodian	Google Inc.
Version	N/A	Announcement date	19.05.2010
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.webmproject.org/docs/container/		

WebM is a digital multimedia container format for audio and video data that MAY BE used for serving video over the internet. It is an open source, royalty-free format. WebM files consist of video streams compressed with the VP8 video codec and audio streams compressed with the Vorbis audio codec. The WebM file structure is based on the Matroska container.

WebM is natively supported by Mozilla Firefox, Opera and Google Chrome web browsers. Internet Explorer 9 requires third-party WebM software. Similarly, the Safari web browser relies on QuickTime to play web media, which does not support WebM unless a third-party plug-in is installed. Also, Adobe Systems announced that its Flash Player will be updated to support WebM, though the exact date is not known. Google has announced that the WebM Project Team will release plugins for Internet Explorer and Safari to allow playback of WebM files through the standard HTML5 <video> tag.

The MIME identifiers (see section 9.6.6) for WebM are “video/webm” and “audio/webm”.

9.6.11 Data Compression

[M27]. ZIP			
Abbreviation	**ZIP**	Custodian	N/A
Version	v6.3.4	Announcement date	01.10.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	N/A		

ZIP is an archive format which supports lossless data compression and SHALL BE used to exchange data in compressed format. .ZIP files generally use the file extensions ".zip".

The MIME identifier for ZIP is “application/zip”.

9.7 Communication and Interoperability

9.7.1 Interoperability with Third-Party Systems

[M28]. Simple Object Access Protocol			
Abbreviation	**SOAP**	Custodian	World Wide Web Consortium (W3C)
Version	v1.2 (Second edition)	Announcement date	27.04.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2007/REC-soap12-part0-20070427/		

SOAP is a protocol specification that SHALL BE used for the exchange of structured data through Web Services technologies in Service Oriented Architecture (SOA) implementations. Moreover, SOAP SHALL BE used for message exchange in the form of XML information set, negotiated and transmitted with the use of other application layer protocols, such as HyperText Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP). A SOAP message is an ordinary XML document containing the following elements:

- Envelope: Identifies the XML document as a SOAP message.

- Header: Contains header information.
- Body: Contains call and response information.
- Fault: Provides information about errors that occurred while processing the message.

[M29]. Web Services Description Language			
Abbreviation	**WSDL**	Custodian	World Wide Web Consortium (W3C)
Version	v2.0	Announcement date	26.07.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2007/REC-wsdl20-primer-20070626/		

WSDL is an XML-based interface description language that SHALL BE used for the description and definition of standard functionality offered by Web Services. A WSDL description of a web service (also referred to as a WSDL file) provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns. The description of a Web Service is done with WSDL in such a way that the Web Services can be utilised from third-party application software, without having the knowledge of technical details and the programming language used to develop the services. Specifically, the description is based on collections of ports, where a port is defined by associating a network address with a reusable binding, and a collection of ports defines a service. WSDL is often used in combination with SOAP and an XML Schema to provide Web services over the Internet.

[R22]. Web Services Description Language			
Abbreviation	**WSDL**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	15.03.2001
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/wsdl		

The older version of WSDL SHOULD BE used only where the newer version is not

feasible to be applied.

[R23]. Universal Description, Discovery and Integration			
Abbreviation	**UDDI**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v2	Announcement date	19.07.2002
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://uddi.org/pubs/ProgrammersAPI-V2.04-Published-20020719.pdf		

Universal Description Discovery & Integration (UDDI) is the name of a group of XML-based registries that expose information about a business or other entity and its technical interfaces (or API's). These registries are run by multiple Operator Sites, and can be used by anyone who wants to make information available about one or more businesses or entities, as well as anyone that wants to find that information. UDDI provides a mechanism to register and locate web service applications. UDDI is an open, platform-independent standard supported by OASIS (www.oasis-open.org), which aims in enabling businesses to publish service listings and discover each other, and to define how the services or software applications interact over the Internet.

The focus of UDDI is the definition of a set of services supporting the description and discovery of (1) businesses, organizations, and other Web services providers, (2) the Web services they make available, and (3) the technical interfaces which may be used to access those services. Based on a common set of industry standards, including HTTP, XML, XML Schema, and SOAP, UDDI provides an interoperable, foundational infrastructure for a Web services-based software environment for both publicly available services and services only exposed internally within an organization.

The UDDI standard SHOULD BE used for the design and development of a standardised interoperability platform, which will allow the simple, fast and dynamic registration, search and retrieval of Web Services. UDDI v2 SHOULD BE used in combination with the compatible versions of XML, SOAP and WSDL standards.

[R24]. Universal Description, Discovery and Integration			
Abbreviation	**UDDI**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v3	Announcement date	19.10.2004
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://uddi.org/pubs/uddi-v3.0.2-20041019.htm		

The newer version of UDDI SHOULD BE used for the design and development of a centralised interoperability platform for the registration, search and retrieval of Web Services, whenever the previous version cannot be used due to incompatibility issues with other standards or technologies. The version 3 of UDDI specification is actually a parallel version that is compatible with newer versions of the basic standards (XML, WSDL, SOAP etc.) that works together with in a Service Oriented Architecture (SOA) environment. Also, version 3 provides some extra functionality compared to previous version such as support for registry affiliation, information model improvements, support for digital signatures, extended discovery features etc. As such, UDDI v3 SHOULD BE used in case it is needed to implement some functionalities that are not supported by UDDI v2.

UDDI v3 SHOULD BE used in combination with compatible versions of XML, SOAP and WSDL standards.

[R25]. Web Services Interoperability Basic Profile			
Abbreviation	**WS-I BP**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.2	Announcement date	09.11.2010
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html		

The WS-I Basic Profile is a specification developed by the Web Services Interoperability industry consortium (WS-I – http://www.ws-i.org/), which is now a

Member Section of OASIS. The WS-I Basic Profile consists of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications that promote interoperability. It also contains a set of executable test assertions for assessing the conformance to the profile.

WS-I Basic Profile v1.2 interoperability guidelines SHOULD BE followed when applying core Web Services standards such as SOAP, WSDL and UDDI.

[R26]. Web Services Interoperability Basic Profile			
Abbreviation	**WS-I BP**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v2.0	Announcement date	09.11.2010
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html		

The interoperability guidelines of the newer version of WS-I Basic Profile SHOULD BE followed when applying core Web Services standards such as SOAP, WSDL and UDDI. WS-I BP v2.0 SHOULD BE used whenever the previous version (1.2) is incompatible with other interoperability standards that work together with in a specific implementation.

[R27]. Simple Object Access Protocol			
Abbreviation	**SOAP**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	08.05.2000
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/soap11/		

The older version of SOAP protocol SHOULD BE used only where the newer version is not feasible to be applied.

[R28]. XML Query Language			
Abbreviation	**XQuery**	Custodian	World Wide Web Consortium (W3C)
Version	v1.0 (Second edition)	Announcement date	14.12.2010
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2010/REC-xquery-20101214/		

XQuery is a standardized language for combining documents, databases, Web pages and almost anything else, with the scope to intelligently query XML data sources. XQuery v1.0 SHOULD BE used for retrieving and interpreting information from diverse XML data sources. It is designed to be a language in which queries are concise and easily understood. It is also flexible enough to query a broad spectrum of XML information sources, including both databases and documents.

[U14]. XML Query Language			
Abbreviation	**XQuery**	Custodian	World Wide Web Consortium (W3C)
Version	v3.0	Announcement date	08.04.2014
Registration date	13.07.2016	Revision date	N/A
Reference URL	https://www.w3.org/TR/xquery-30/		

XQuery 3.0 is an extended version of the XQuery 1.0 Recommendation published initially on 23 January 2007. This version provides some new features including, indicatively, the following:

- Dynamic function call;
- Private functions;
- Switch expressions;
- Output declarations;
- Annotations.

XQuery v3.0 MAY BE used for retrieving and interpreting information from diverse XML data sources, in case XQuery v1.0 cannot be used due to features needed but

not supported, due to compatibility issues etc.

9.7.2 Discovery of Resources

[M30]. Domain Name System			
Abbreviation	**DNS**	Custodian	Internet Engineering Task Force (IETF)
Version	N/A	Announcement date	November 1987
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.ietf.org/rfc/rfc1034.txt		

DNS is a hierarchical naming system for computers, services or other devices and resources connected to a network, either the internet or a private network. DNS is defined in RFC 1034 and RFC 1035 of the IETF (www.ietf.org). Its goal is to map easily memorised domain names to numerical IP addresses, which are used to locate a computer or any other device in a network.

DNS SHALL BE applied for every internet service, web-based application and/or web portal owned or operated by a government organisation.

[R29]. Universal Description, Discovery and Integration			
Abbreviation	**UDDI**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v2	Announcement date	19.07.2002
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://uddi.org/pubs/ProgrammersAPI-V2.04-Published-20020719.pdf		

See section 9.7.1.

[R30]. Universal Description, Discovery and Integration			
Abbreviation	**UDDI**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v3	Announcement date	19.10.2004
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://uddi.org/pubs/uddi-v3.0.2-20041019.htm		
See section 9.7.1.			

[R31]. Lightweight Directory Access Protocol			
Abbreviation	**LDAP**	Custodian	Internet Engineering Task Force (IETF)
Version	v3	Announcement date	June 2006
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc4511		

LDAP is a protocol that provides access to distributed directory services. Directory services may consist of any organised set of records, mainly in a hierarchical structure, such as a corporate email directory.

LDAP SHOULD BE used for accessing directory services either on a government intranet or in the context of e-services provision to citizens and businesses.

9.7.3 Locating of Resources

[M31]. Uniform Resource Identifier			
Abbreviation	**URI**	Custodian	Internet Engineering Task Force (IETF)
Version	N/A	Announcement date	January 2005
Registration date	02.12.2013	Revision date	N/A

Reference URL	http://www.ietf.org/rfc/rfc3986.txt

A Uniform Resource Identifier (URI) is a compact sequence of characters that identifies an abstract or physical resource that SHALL BE used for the identification of web resources. A URI consists of a Uniform Resource Locator (URL) and a Uniform Resource Name (URN), where the URN is used to identify the name of a resource and the URL to identify the location of the same resource. Additionally, a URI includes information about protocols used for the identification of a resource over a network (such as the internet). Each URI is defined by schemes which specify a concrete syntax and associated protocols. The first RFC that described URLs and URNs and defined a formal syntax for URIs was the RFC 1630, created by Tim Berners-Lee (the founder of World Wide Web) and published in June 1994 by IETF, while the most recent RFC for URIs is the RFC 3986.

[M32]. Uniform Resource Locator			
Abbreviation	**URL**	Custodian	Internet Engineering Task Force (IETF)
Version	N/A	Announcement date	December 1994
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.ietf.org/rfc/rfc1738.txt		

URL, often called as web address, is a compact string of characters that identify a resource available on a network, such as the internet. URL is the major part of a URI and SHALL BE used for the identification of a network resource's location. URL was standardised in 1994 by Tim Berners-Lee and the IETF (www.ietf.org) in the RFC 1738. Although URL and URI are quite similar, URL is commonly used instead of URI or both terms are used to define the same string.

9.7.4 Network Protocols

[M33]. Internet Protocol			
Abbreviation	**IP**	Custodian	Internet Engineering Task Force (IETF)
Version	v4	Announcement date	September 1981

Registration date	02.12.2013	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc791		

The Internet Protocol (IP) is the most known and widely used protocol in the internet and in computer networks in general. Its purpose is to interconnect systems of packet-switched computer communication networks. IP is used for transmitting blocks of data, called datagrams, from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. For this purpose, IP defines the format of packets and provides an addressing system that has two functions: identifying hosts and providing a logical location service. IPv4 uses addresses that have a length of 32 bit, allowing approximately 4 billion different addresses.

IPv4 SHALL BE used for the communication of network resources and devices in every governmental computer communications network, in conjunction with TCP protocol (Transmission Control Protocol, RFC 793) or UDP protocol (User Datagram Protocol, RFC 768).

[M34]. Internet Control Message Protocol			
Abbreviation	**ICMP**	Custodian	Internet Engineering Task Force (IETF)
Version	v4	Announcement date	September 1981
Registration date	24.01.2014	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc792		

The Internet Control Message Protocol (ICMP) SHALL BE used for diagnostic or control purposes by network devices, or even for reporting errors in IP packets processing, with ICMP errors directed to the source IP address of the originating packet. An error example is that a requested service is not available or that a router could not be reached. ICMP can also be used to relay query messages. Many popular networking utilities use the ICMP protocol, such as traceroute and ping command.

Although ICMP messages are contained within standard IP packets, ICMP messages are usually processed as a special case, distinguished from normal IP processing, rather than processed as a normal sub-protocol of IP. In many cases, it is necessary to inspect the contents of the ICMP message and deliver the appropriate error message to the application that generated the original IP packet.

[M35]. Simple Network Management Protocol			
Abbreviation	**SNMP**	Custodian	Internet Engineering Task Force (IETF)
Version	v3	Announcement date	December 2002
Registration date	24.01.2014	Revision date	N/A
Reference URL	http://tools.ietf.org/search/rfc3412 http://tools.ietf.org/search/rfc3414 http://tools.ietf.org/search/rfc3417		

SNMP is a protocol maintained by the Internet Engineering Task Force (IETF – www.ietf.org) that SHALL BE used for monitoring and/or managing devices attached in an IP network. SNMP v3 is an extensible SNMP Framework which supplements the SNMPv2 Framework, by supporting the following:

- a new SNMP message format;
- advanced security for messages;
- access control and
- remote configuration of SNMP parameters.

The SNMP protocol is part of the SNMP Management Framework, which consists of five major components:

1. An overall architecture, described in RFC 3411 (http://tools.ietf.org/search/rfc3411).
2. Mechanisms for describing and naming objects and events for the purpose of management.
3. Message protocols for transferring management information.
4. Protocol operations for accessing management information.
5. A set of fundamental applications described in RFC 3413 (http://tools.ietf.org/search/rfc3413) and the view-based access control mechanism described in RFC 3415 (http://tools.ietf.org/search/rfc3415).

[R32]. Simple Network Management Protocol			
Abbreviation	**SNMP**	Custodian	Internet Engineering Task Force (IETF)
Version	v2	Announcement date	April 1999
Registration date	24.01.2014	Revision date	N/A
Reference URL	http://tools.ietf.org/search/rfc1901 http://tools.ietf.org/search/rfc2578 http://tools.ietf.org/search/rfc2579 http://tools.ietf.org/search/rfc2580		
SNMP v2 SHOULD BE used for monitoring and/or managing network devices in an IP network, in case these devices do not support the latest version (SNMP v3).			

[R33]. Secure Shell			
Abbreviation	**SSH**	Custodian	Internet Engineering Task Force (IETF)
Version	v2	Announcement date	January 2006
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	https://www.rfc-editor.org/rfc/rfc6668.txt http://tools.ietf.org/html/rfc4251		

SSH is a transport layer protocol for secure remote login and other secure network services over an insecure network. However, due to the fact that it has some uses at the application layer as well, such as X11 connections forwarding, TCP ports forwarding, SSH file transfers etc., it is sometimes considered as an application layer protocol. SSH provides strong encryption, server authentication and integrity protection, while it may also provide compression. The protocol has been designed to be simple and flexible to allow parameter negotiation and to minimize the number of round-trips.

SSH is organized as three components that typically run on top of a TCP/IP connection, but might also be used on top of any other reliable data stream:

- The Transport Layer Protocol [SSH-TRANS] provides server authentication,

confidentiality, and integrity. It may optionally also provide compression.

- The User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

The original document that describes the SSH standard, RFC 4253, has been updated by RFC 6668 IETF standard as of July 2012. This update defines algorithm names and parameters for use in some of the SHA-2 family of secure hash algorithms for data integrity verification in the Secure Shell (SSH) protocol. It also updates RFC 4253 by specifying a new recommended data integrity algorithm.

SSH SHOULD BE used for secure remote connections to servers from clients machines over an insecure network, such as the internet, in order to remotely execute commands, securely transfer files (using SSH-FTP) or to implement tunnelling.

[R34]. Border Gateway Protocol			
Abbreviation	**BGP**	Custodian	Internet Engineering Task Force (IETF)
Version	v4	Announcement date	January 2006
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://tools.ietf.org/html/rfc4271		

BGP is an inter-Autonomous System routing protocol, utilised for the exchange of routing information between autonomous systems in order to be able to communicate with each other.

BGP is one of the most critical protocols used in the internet since 1994, being an IETF standard (RFC 4271) since 2006. Until 2015, RFC 4271 has been updated by the following IETF standards: RFC 6286, RFC 6608, RFC 6793, RFC 7606, RFC 7607 and RFC 7705.

BGP SHOULD BE applied for the communication between different autonomous systems or inside the same autonomous system.

[R35]. Routing Information Protocol			
Abbreviation	**RIP**	Custodian	Internet Engineering Task Force (IETF)
Version	v2	Announcement date	November 1998
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://tools.ietf.org/html/rfc2453 https://www.rfc-editor.org/rfc/rfc4822.txt		

RIP v2 is a routing protocol that uses the distance vector algorithm, initially developed in 1993 (RFC 1388) and standardised in 1998 (RFC 2453) by IETF (www.ietf.org). RIP uses the hop count as a routing metric, with a limit of 15 hops allowed in a path between the source and the destination, in order to avoid routing loops. This limitation however imposes a restriction for the RIP protocol to not be suitable for large scale networks.

The original specification of RIPv2 (RFC 2453) was updated on February 2007 by RFC 4822, which describes a revision to the RIPv2 Cryptographic Authentication mechanism. This update adds details of how the SHA family of hash algorithms can be used with RIPv2 Cryptographic Authentication, whereas the original document only specified the use of Keyed-MD5. Also, this document clarifies a potential issue with an active attack on this mechanism and adds significant text to the Security Considerations section.

RIP SHOULD BE deployed as a routing protocol in small networks, due to the fact that RIP has very little overhead in terms of bandwidth used. Also, RIP requires a small amount of time for configuration and management. RIP is also very easy to implement, especially in relation to the newer Interior Gateway Protocols.

[R36]. Encapsulating Security Payload			
Abbreviation	**ESP**	Custodian	Internet Engineering Task Force (IETF)
Version	N/A	Announcement date	December 2005
Registration date	24.01.2014	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc4303		

Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite, which SHOULD BE used to provide confidentiality, data origin authentication, and connectionless integrity for IP packets. ESP also provides an anti-replay service (a form of partial sequence integrity) and limited traffic flow confidentiality. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange. ESP operates directly on top of IP, using IP protocol number 50.

[R37]. Open Shortest Path First			
Abbreviation	**OSPF**	Custodian	Internet Engineering Task Force (IETF)
Version	v2	Announcement date	April 1998
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc2328#page-185		

OSPF is a routing protocol that uses a link state routing algorithm, initially defined in December 1999 (RFC 2740), that falls in the class of Interior Gateway Protocols (IGPs). OSPF uses path cost as its basic routing metric and leverages the shortest path first algorithm to map the network, with the ability to detect network topology changes and converge within seconds. It supports variable-length subnet masking (VLSM) and Classless Inter-Domain Routing (CIDR) addressing models. OSPF does not use a TCP/IP transport protocol (UDP, TCP), but is encapsulated directly in IP datagrams, in contrast with other routing protocols such as RIP and BGP.

OSPF v2 SHOULD BE used for IP packet routing for large scale networks within a single autonomous system (routing domain).

[U15]. Open Shortest Path First			
Abbreviation	**OSPF**	Custodian	Internet Engineering Task Force (IETF)
Version	v3	Announcement date	July 2008
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc5340#page-57		

OSPF v3 is a modified version of OSPF v2, initially aiming at supporting the routing of IPv6 packets. In particular, the fundamental mechanisms of OSPF (flooding,

Designated Router (DR) election, Short Path First calculations etc.) remain unchanged. However, some changes have been necessary, either due to changes in protocol semantics between IPv4 and IPv6, or simply to handle the increased address size of IPv6. Additionally, due to several inefficiencies and weaknesses identified over the years in OSPF v2, OSPF v3 constitutes an improved version of the protocol. It is noted that OSPFv3 is not backward-compatible with OSPFv2, so if both IPv4 and IPv6 must be routed with OSPF, then both OSPFv2 and OSPFv3 must be used.

OSPF v3 MAY BE used in the future when IPv6 is deployed widely or it MAY BE used in case there is a need to route both IPv4 and IPv6 packets in an autonomous system.

[U16]. Internet Protocol			
Abbreviation	**IP**	Custodian	Internet Engineering Task Force (IETF)
Version	v6	Announcement date	December 1998
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc2460		

IPv6 is the successor of IPv4, which mainly addresses the problem of IPv4 address depletion, caused by the limited number of different addresses combined with the exponential and continuous growth of resources connecting to the internet. IPv6 uses addresses of 128-bit length, providing a total number of approximately 3.4×10^{38} different addresses to be assigned to devices. The two versions of IP are not designed to be interoperable, thus making the transition from IPv4 to IPv6 quite hard. However, since it is expected that in a few years all IPv4 addresses will be exhausted (already a top-level exhaustion has occurred in early 2011 and some parts of the world have already exhausted their IPv4 allocations), IPv6 MAY BE deployed at least in governmental local area networks (LANs). Also government organisations should require both IPv4 and IPv6 support during procurement of computers, servers or other ICT equipment in order to facilitate a possible future transition from IPv4 to IPv6.

[U17]. Internet Control Message Protocol			
Abbreviation	**ICMP**	Custodian	Internet Engineering Task Force (IETF)
Version	v6	Announcement date	March 2006

Registration date	24.01.2014	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc4443		

ICMPv6 is the implementation of the ICMP protocol for the IPv6 protocol. ICMPv6 MAY BE used for diagnostic and control purposes or for reporting errors in IP packets processing, for network devices operating in an IPv6 based network.

[U18].	**Routing Information Protocol Next Generation**		
Abbreviation	**RIPng**	Custodian	Internet Engineering Task Force (IETF)
Version	N/A	Announcement date	January 1997
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc2080		

RIP next generation (RIPng) is a modified version of the RIP routing protocol that contains enhancements which aim at supporting the routing of IPv6 packets. RIPng MAY BE used in the future when IPv6 is deployed widely for IP packet routing within a small scale network.

9.7.5 Application Layer Protocols

[M36].	**File Transfer Protocol**		
Abbreviation	**FTP**	Custodian	Internet Engineering Task Force (IETF)
Version	N/A	Announcement date	October 1985
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.ietf.org/rfc/rfc959.txt		

The FTP is a widely used protocol that SHALL BE used for transferring files between computers over a TCP-based network, such as the internet. The original specification was published as RFC 114 in April 1971, which defined its operation over the NCP protocol. Later it was substituted by a TCP/IP version (RFC 765 and RFC 959 – the latter became the formal specification of FTP). Several amendments have been published for RFC 959, in order to deal with various subjects such as security

extensions, support for IPv6 etc. FTP has proved to be faster than HTTP in transferring large files and is preferred in such cases.

In case encryption needs to be applied when transferring files using the FTP protocol, FTPS (FTP Secure or FTP-SSL) SHOULD BE used. FTPS is an extension to FTP that adds support for the TLS and SSL cryptographic protocols, including the use of server-side public key authentication certificates and client-side authorization certificates. Using FTPS, the FTP session can be encrypted either entirely or partly (depending on the mode used). FTPS supports compatible ciphers including AES, RC4, RC2, and Triple DES.

[M37]. HyperText Transfer Protocol			
Abbreviation	**HTTP**	Custodian	Internet Engineering Task Force (IETF)
Version	v1.1	Announcement date	June 1999 (updated June 2014)
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	https://www.rfc-editor.org/rfc/rfc7230.txt https://www.rfc-editor.org/rfc/rfc7231.txt https://www.rfc-editor.org/rfc/rfc7232.txt https://www.rfc-editor.org/rfc/rfc7233.txt https://www.rfc-editor.org/rfc/rfc7234.txt https://www.rfc-editor.org/rfc/rfc7235.txt		

HTTP is a protocol for distributed, collaborative, hypermedia information systems, being the foundation of data communication for the World Wide Web since 1990. It builds on the discipline of reference provided by the URI, as a location (URL) or name (URN), for indicating the resource to which a method is to be applied. HTTP follows a client-server computing model and SHALL BE used for the exchange of hypertext information over a TCP/IP based network between a client and a server.

[M38]. Simple Mail Transport Protocol			
Abbreviation	**SMTP**	Custodian	Internet Engineering Task Force (IETF)

Version	N/A	Announcement date	October 2008
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://tools.ietf.org/html/rfc5321 https://www.rfc-editor.org/rfc/rfc7504.txt		

SMTP is an internet standard that SHALL BE used for transferring electronic mail (e-mail) over an IP-based network, in a reliable and efficient manner. An important feature of SMTP is its capability to transport mail across multiple networks, usually referred to as "SMTP mail relaying". The original SMTP specification was published in RFC 821, while further enhancements were made over the time, with the most recent version of the specification published in RFC 5321, which replaces RFC 821, RFC 974, RFC 1869 and RFC 2821. RFC 5321 was updated by RFC 7504 in June 2015.

Files attached to e-mails SHALL use the file formats specified in sections 9.6.7 and 9.6.8.

[M39]. Post Office Protocol			
Abbreviation	**POP**	Custodian	Internet Engineering Task Force (IETF)
Version	v3	Announcement date	May 1996
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://tools.ietf.org/html/rfc1939		

POP3 is an internet standard that SHALL BE used by e-mail client applications to retrieve e-mail from a remote server over a TCP/IP based network. POP3 is not intended to provide extensive manipulation operations of mail on the server; normally, mail is downloaded and then deleted.

[M40]. Internet Message Access Protocol			
Abbreviation	**IMAP**	Custodian	Internet Engineering Task Force (IETF)
Version	v4 (Revision 1)	Announcement date	March 2003
Registration date	02.12.2013	Revision date	13.07.2016

Reference URL	http://tools.ietf.org/html/rfc3501

IMAP is a protocol that SHALL BE used for accessing and/or manipulating e-mail messages on a remote server by a mail client application. In contrast to the POP3 protocol, IMAP supports advanced operations such as creating, deleting, and renaming mailboxes (remote message folders), permanently removing messages, setting and clearing flags, searching and selective fetching of message attributes, texts, and portions thereof. IMAP also provides the capability for an offline client to resynchronize with the server.

The original document that defines the IMAP standard was updated by subsequent IETF documents, namely the: RFC 4466, RFC 4469, RFC 4551, RFC 5032, RFC 5182, RFC 5738, RFC 6186, RFC 6858 and RFC 7817.

9.7.6 IP Telephony

[R38]. H.323			
Abbreviation	**H.323**	Custodian	International Telecommunication Union (ITU)
Version	v7.1	Announcement date	16.03.2013
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.itu.int/rec/T-REC-H.323-201303-I!Amd1/en		

H.323 is an ITU (www.itu.int) recommendation for transmitting multimedia content over packet-based networks. H.323 entities may provide real-time audio, video and/or data communications, where support for audio is mandatory. The packet-based network over which H.323 entities communicate may be a point-to-point connection, a single network segment, or an internetwork having multiple segments with complex topologies.

H.323 is widely deployed worldwide by service providers and enterprises for both voice and video services over IP networks. Additionally, H.323 was the first VoIP standard to adopt the IETF standard Real-time Transport Protocol (RTP) to transport audio and video over IP networks.

Version 7.1 comprises an amendment to v7 of the standard. It formalizes the widely implemented call transfer mechanism in ITU-T H.323 that relies upon the FACILITY message with a reason of "callForwarded".

Government organisations SHOULD use H.323 for providing voice and video services over IP networks.

[R39]. Session Initiation Protocol			
Abbreviation	**SIP**	Custodian	Internet Engineering Task Force (IETF)
Version	v2.0	Announcement date	June 2002
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://tools.ietf.org/html/rfc3261		

SIP is a communications control protocol that can establish, modify and terminate multimedia communication sessions such as Internet telephony calls. The protocol defines the messages sent between peers which control the establishment, termination and other essential elements of a call. SIP works with both IPv4 and IPv6.

RFC 3261, the IETF document that defines the Session Initiation Protocol (SIP), has been updated in terms of additional functionalities (alerts, notifications, transaction and request handling etc.) by the following RFC documents: 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630, 5922, 5954, 6026, 6141, 6665, 6878, 7462 and 7463.

Government organisations SHOULD use SIP v2.0 for the control of communication sessions in VoIP and/or teleconference applications.

9.7.7 Content Delivery

[M41]. Real Simple Syndication			
Abbreviation	**RSS**	Custodian	Harvard University
Version	v2.0	Announcement date	15.07.2003
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://cyber.law.harvard.edu/rss/rss.html		

RSS is an XML-based Web content syndication format that SHALL BE used to deliver Web content that frequently changes to users, such as blog entries, news headlines, audio and video. An RSS document (called "feed" or "channel") includes full or summarized text and metadata, like publishing date and author's name. Internet users

often use software applications called “RSS readers” to receive updated information from a website or to aggregate data from many sites. Web sites of government organisations SHALL provide their content to users through RSS feeds, where applicable.

[M42]. Atom Format			
Abbreviation	**Atom**	Custodian	Internet Engineering Task Force (IETF)
Version	v1.0	Announcement date	December 2005
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://tools.ietf.org/html/rfc4287		

Atom is an XML-based document format that describes lists of related information known as "feeds". Feeds are composed of a number of items, known as "entries", each with an extensible set of attached metadata. For example, each entry has a title. The original document of the standard, RFC 4287, has been updated by RFC 5988 which specifies relation types for Web links, and defines a registry for them. It also defines the use of such links in HTTP headers with the Link header field.

Atom format SHALL BE used for the syndication of Web content such as weblogs and news headlines to Web sites, as well as directly to user agents. Atom also provides a standard way to export an entire blog, or parts of it, for backup or for importing into other blogging systems.

9.8 Security and Authentication

9.8.1 Web Services Security

[M43]. Web Services Security			
Abbreviation	**WS-Security**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.1.1	Announcement date	18.05.2012
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.pdf		

The WS-Security specification SHALL BE used when building Web Services in order to ensure quality, integrity, confidentiality and validation of Web Services provided by government organisations. WS-Security provides support for multiple security token formats, multiple trust domains, multiple signature formats and multiple encryption technologies. Also, WS-Security provides three main mechanisms: ability to send security tokens as part of a message, message integrity and message confidentiality. These mechanisms by themselves do not provide a complete security solution for Web services. Instead, this specification is a building block that SHALL BE used in conjunction with other Web service extensions and higher-level application-specific protocols to accommodate a wide variety of security models and security technologies.

The WS-Security v1.1.1 is the result of significant new work by the WSS Technical Committee of OASIS and SHALL BE used for the secure implementation of Web Services from government organisations.

[R40]. Web Services SecurityPolicy			
Abbreviation	**WS-SecurityPolicy**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.3	Announcement date	02.02.2009

Registration date	02.12.2013	Revision date	N/A
Reference URL	http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.pdf		

WS-SecurityPolicy defines a framework for allowing web services to express their constraints and requirements as policy assertions. A policy assertion represents a requirement, capability, or other property of a behaviour. The framework defines a set of security policy assertions for use with the WS-Policy framework with respect to security features provided in WS-Security, WS-Trust and WS-SecureConversation. WS-SecurityPolicy v1.3 SHOULD BE used to describe how messages are to be secured when implementing Web services.

[R41]. Web Services Policy			
Abbreviation	**WS-Policy**	Custodian	World Wide Web Consortium (W3C)
Version	v1.5	Announcement date	04.09.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2007/REC-ws-policy-20070904/		

The WS-Policy Framework provides a general purpose model and corresponding syntax to advertise the policies of entities (for example, required security tokens, supported encryption algorithms, and privacy rules) in a Web Services-based system. Also, it defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements and capabilities. WS-Policy SHOULD BE used to describe the capabilities and constraints of the security policies on intermediaries and end points of Web Services and how to associate policies with services and end points.

[R42]. Web Services SecureConversation			
Abbreviation	**WS-SecureConversation**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.4	Announcement date	02.02.2009

Registration date	02.12.2013	Revision date	N/A
Reference URL	http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.pdf		

The WS-SecureConversation specification provides extensions to WS-Security mechanisms to allow security context establishment and sharing, as well as session key derivation. It works in conjunction with WS-Security, WS-Trust and WS-Policy to allow the creation and sharing of security contexts. Its scope is to allow contexts to be established and potentially more efficient keys or new key material to be exchanged, thereby increasing the overall performance and security of the subsequent exchanges. WS-SecureConversation SHOULD BE used together with WS-Policy and WS-Security frameworks when designing and implementing the security aspects of Web Services in government organisations.

9.8.2 Data Transmission Security

[M44]. Transport Layer Security			
Abbreviation	**TLS**	Custodian	Internet Engineering Task Force (IETF)
Version	v1.2	Announcement date	August 2008
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://tools.ietf.org/html/rfc5246		

TLS is a protocol designed to prevent eavesdropping and tampering during a communication session over a network between client-server applications. TLS uses X.509 certificates to assure the counterparty whom they are talking with and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. TLS is widely used in applications such as web browsing, electronic mail, instant messaging and VoIP. TLS v1.2 SHALL BE used during the exchange and transmission of data in a computer communications network.

TLS v1.2 is a revision of the TLS v1.1 protocol which was developed aiming in improved flexibility, particularly for negotiation of cryptographic algorithms. TLS v1.2 is the recommended version of the TLS standard to be used according to the latest version (v3.1) of the international security standard PCI DSS. In addition, IETF's standard RFC 7525 mandates to not use TLS v1.1 among others, due to security vulnerabilities that have weakened the effectiveness of the algorithms used and

consequently this version of the standard cannot ensure at the greatest level, preservation of data confidentiality during a communication session over a network.

[M45]. HyperText Transfer Protocol Secure			
Abbreviation	**HTTPS**	Custodian	Internet Engineering Task Force (IETF)
Version	N/A	Announcement date	May 2000
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.ietf.org/rfc/rfc2818.txt		

HTTPS derives from the combination of HTTP protocol and the SSL/TLS protocols in order to provide HTTP data transfers with the security capabilities of SSL/TLS protocols, making the communication between networked devices more secure. It is widely applied in the World Wide Web, initially for payment and other sensitive transactions but later on its use spread in protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private. HTTPS SHALL BE used for securing the channels and protecting the privacy of communications based on the HTTP protocol.

[R43]. X.509			
Abbreviation	**X.509**	Custodian	International Telecommunication Union (ITU)
Version	v3 (7th edition)	Announcement date	14.10.2012
Registration date	13.07.2016	Revision date	N/A
Reference URL	http://www.itu.int/rec/T-REC-X.509-200811-I/en		

X.509 is an ITU-T Recommendation (www.itu.int) and an international standard (ISO/IEC 9594-8) that defines a framework for public-key certificates and attribute certificates, as well as for the provision of authentication services by Directory to its users. X.509 recommendation SHOULD BE applied to Public Key Infrastructures (PKI) implementations.

X.509 describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials

formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication SHOULD BE used as the basis for providing secure services.

X.509 v3 certificate format is also profiled for use in the Internet by IETF in its RFC 5280 document standard, updated by RFC 6818. In addition, these documents provide the Certificate Revocation List (CRL) Profile. The CRL format is described in detail along with standard and Internet-specific extensions. Also, the 7th edition of X.509 v3 is identical with the ISO/IEC 9594-8:2014 international standard.

9.8.3 Encryption

[M46]. Advanced Encryption Standard			
Abbreviation	**AES**	Custodian	National Institute of Standards and Technology (NIST)
Version	N/A	Announcement date	26.11.2001
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf		

AES is a standard published by Federal Information Processing Standards Publications (FIPS PUB) of NIST organisation that specifies an encryption algorithm for the protection of electronic data's privacy. AES is also included in the ISO/IEC 18033-3 international standard. AES algorithm is a symmetric block cipher that can encrypt and decrypt information and is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. AES is the successor of the Data Encryption Standard (DES), which has been withdrawn as a standard from NIST.

AES SHALL BE used by government organisations during electronic data transmission and/or exchange, in case an organisation determines that sensitive (unclassified) information requires cryptographic protection.

[M47]. Secure Hash Algorithm			
Abbreviation	**SHA**	Custodian	National Institute of Standards and Technology (NIST)

Version	v2	Announcement date	March 2012
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf		

Secure Hash Algorithm v2 (referred to as SHA-2) is a set of secure hash algorithms (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256) which SHALL BE used to manage the integrity of exchanged electronic data. SHA-2 is published by Federal Information Processing Standards Publications (FIPS PUB) of NIST organisation. SHA-2 currently consists of a set of six hash functions with digests that are 224, 256, 384 or 512 bits. Each one is a variant of SHA-2 algorithm, named after the bit length, i.e. SHA-224, SHA-256, SHA-384 and SHA-512.

SHA-2 SHALL BE used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

[M48]. Extensible Markup Language Encryption			
Abbreviation	**XML-Enc**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	11.04.2013
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/		

The XML Encryption v1.1 is a W3C recommendation that SHALL BE used for encrypting data and representing the result in XML format in a Web Services environment. The data to be encrypted may be arbitrary data (including an XML document), an XML element, or XML element content. The result of encrypting data is an XML Encryption *EncryptedData* element that contains (via one of its children's content) or identifies (via a URI reference) the cipher data.

The previous version of the standard, XML Encryption v1.0, was found in 2011 by German researchers to have a significant security flaw (CBC Block Encryption vulnerability), which in turn led to the modification of the standard, resulting in v1.1. The new version dealt with several security considerations, which led to additions and changes of cryptographic algorithms and changes in keys management.

[R44]. Extensible Markup Language Key Management Specification			
Abbreviation	**XKMS**	Custodian	World Wide Web Consortium (W3C)
Version	v2.0	Announcement date	28.06.2005
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2005/REC-xkms2-20050628/		

The XKMS is a W3C standard that specifies protocols for the distribution and registration of public keys that SHOULD BE used for public keys management together with the XML Signature and XML Encryption standards.

[R45]. Triple Data Encryption Standard			
Abbreviation	**TDES or 3DES**	Custodian	National Institute of Standards and Technology (NIST)
Version	N/A	Announcement date	25.10.1999
Registration date	24.01.2014	Revision date	13.07.2016
Reference URL	http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf		

The TDES is a cryptographic algorithm, which is actually the 3-times application of the DES cryptographic algorithm to each data block. The DES cryptographic engine is permitted to be used only as a component of the TDES algorithm. TDES is a symmetric-key block cipher algorithm, created in order to deal easily with brute-force attacks, which can be used to intercept data encrypted with DES algorithm, without having to develop a new cipher algorithm. The DES cryptographic engine is used by TDES to encrypt blocks of data consisting of 64 bits under the control of a 64-bit key.

As of December 2015, NIST has declared the use for encryption of Two-key TDEA (Triple DES Encryption Algorithm) as disallowed (it was already in a restricted mode throughout 2015). Decryption using Two-key TDEA is allowed for legacy-use only. Instead, Three-key TDEA is allowed to be used for encryption/ decryption functions.

TDES SHOULD BE used by government organisations during electronic data transmission and/or exchange, in case an organisation determines that sensitive (unclassified) information requires cryptographic protection and the AES encryption standard cannot be applied.

9.8.4 Authentication, Identification and Authorisation

[M49]. Extensible Markup Language Signature			
Abbreviation	**XML-Sig or XML-DSig**	Custodian	World Wide Web Consortium (W3C)
Version	v1.1	Announcement date	11.04.2013
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.w3.org/TR/2013/REC-xmldsig-core1-20130411		

XML Signature is a W3C recommendation that provides integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere. Version 1.1 of XML-Sig constitutes a revision of the previous version published in June 2008 and incorporates several additions and changes related to cryptographic algorithms, element changes as well as other security considerations changes (e.g. the use of SHA-256 is strongly recommended in preference to SHA-1). XML-Sig v1.1 SHALL BE used for digitally signing XML documents.

[M50]. Web Services Trust			
Abbreviation	WS-Trust	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.3	Announcement date	19.03.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf		

WS-Trust is an OASIS standard that defines additional primitives and extensions for security token exchange to the base mechanisms of WS-Security standard, in order to enable the issuance and dissemination of credentials within different trust domains.

In order to secure a communication between two parties, the two parties must exchange security credentials (either directly or indirectly). WS-Trust SHALL BE used when each party needs to determine if it can "trust" the asserted credentials of the

other party. In general, WS-Trust SHALL BE used together with the general Web services framework, including WSDL service descriptions, UDDI and SOAP messages.

[R46]. Web Services Trust			
Abbreviation	WS-Trust	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.4	Announcement date	02.02.2009
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf		

WS-Trust v1.4 SHOULD BE used when it is more widely supported or in cases that previous version v1.3 cannot be applied.

[R47]. Web Services Federation			
Abbreviation	WS-Federation	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.2	Announcement date	22.05.2009
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf		

WS-Federation is an OASIS standard developed by several enterprises such as Novell, Microsoft, BMC software, VeriSign etc. related to identity federation. Specifically, the standard defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities are managed in other realms. The federation framework defined in WS-Federation builds on WS-Security, WS-Trust and the WS-* family of specifications providing a rich extensible mechanism for federation.

WS-Federation SHOULD BE used for federation of identities in Web Services environment. A federated identity related example is a Single-Sign-On (SSO) implementation for different IT systems, e.g. a Google user account that can be used to access all of Google's digital services.

[R48]. Web Services Addressing			
Abbreviation	WS-Addressing	Custodian	World Wide Web Consortium (W3C)
Version	v1.0	Announcement date	09.05.2006
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/		

Web Services Addressing is a W3C recommendation that SHOULD BE used to provide transport-neutral mechanisms to address Web services and messages. Web Services Addressing 1.0 defines a set of abstract properties and an XML Infoset (XML Information Set) representation thereof, to reference Web services and to facilitate end-to-end addressing of endpoints in messages. The specification enables messaging systems to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner.

[R49]. Security Assertion Markup Language			
Abbreviation	SAML	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v1.1	Announcement date	02.09.2003
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.oasis-open.org/committees/download.php/3400/oasis-sstc-saml-1.1-pdf-xsd.zip		

SAML is an XML-based data format that SHOULD BE used for exchanging authentication and authorization data between an identity provider and a service provider. This security information (authentication and authorization data) is

expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. The SAML specification defines the syntax and semantics of XML-encoded assertions, protocol requests and protocol responses.

[R50]. Security Assertion Markup Language			
Abbreviation	**SAML**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v2.0	Announcement date	15.03.2005
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip		

SAML v2.0 assertions and protocol messages are incompatible with SAML v1.1 processors. Thus, SAML v2.0 SHOULD BE used for exchanging authentication and authorization data between an identity provider and a service provider provided no incompatibilities exist regarding the previous version of SAML or other Web Services standards.

[R51]. Extensible Access Control Markup Language			
Abbreviation	**XACML**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v2.0	Announcement date	01.02.2005
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf		

XACML is an XML-based, OASIS language that SHOULD BE used for the definition of an access control policy in a uniform and consistent way throughout an organisation. The standard also defines a processing model, which describes how to evaluate access requests and make relative decisions according to the rules defined

in policies. The ultimate goal of XACML is to promote common terminology and interoperability between access control implementations by multiple vendors.

Regarding authorisation decisions for every access request, XACML supports both Attribute Based Access Control (ABAC) and Role Based Access Control (RBAC) systems.

[R52]. Extensible Access Control Markup Language			
Abbreviation	**XACML**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v3.0	Announcement date	22.01.2013
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf		

The newest version of XACML standard is version 3.0, which SHOULD BE used for the definition of an access control policy, when it is more widely supported or in cases that previous version v2.0 cannot be applied.

[R53]. XML Advanced Electronic Signatures			
Abbreviation	**XAdES**	Custodian	European Telecommunications Standards Institute (ETSI)
Version	v1.4.1	Announcement date	June 2009
Registration date	02.12.2013	Revision date	13.07.2016
Reference URL	http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.01_60/ts_101903v010401p.pdf		

XAdES is an ETSI standard (www.etsi.org) that provides extensions to the XML-Sig standard and specifies precise profiles of XML-Sig for use with advanced electronic signature in the meaning of eIDAS Regulation (EU) No 910/2014 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN).

XAdES SHOULD BE used from a government organisation when needed to implement advanced electronic signatures that remain valid over long periods and are compliant with eIDAS Regulation (EU) No 910/2014, effective to all EU Member States as of 01.07.2014 (eIDAS Regulation repeals EU Directive 1999/93/EC).

XAdES defines six profiles (XAdES, XAdES-T, XAdES-C, XAdES-X, XAdES-X-L and XAdES-A) differing in protection level offered. Each profile includes and extends the previous one. Government organisations SHOULD at least apply the XAdES-T profile in advanced electronic signatures, which adds timestamp field to protect against repudiation. XAdES can be applied to any environment e.g. smart cards, GSM SIM cards, special programs for electronic signatures, etc.

[R54]. CMS Advanced Electronic Signatures			
Abbreviation	**CAdES**	Custodian	European Telecommunications Standards Institute (ETSI)
Version	v1.8.3	Announcement date	06.01.2011
Registration date	24.01.2014	Revision date	13.07.2016
Reference URL	http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/01.08.03_60/ts_101733v010803p.pdf		

CAdES is an ETSI standard (www.etsi.org) that provides extensions to the Cryptographic Message Syntax (CMS) standard and specifies precise profiles of CMS signed data for use with advanced electronic signature in the meaning of eIDAS Regulation (EU) No 910/2014 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN). CAdES SHOULD BE used from a government organisation when needed to implement advanced electronic signatures that remain valid over long periods and are compliant with Regulation (EU) No 910/2014.

CAdES defines six profiles (CAdES, CAdES-T, CAdES-C, CAdES-X, CAdES-X-L and CAdES-A) differing in protection level offered. Each profile includes and extends the previous one. Government organisations SHOULD at least apply the CAdES-T profile in advanced electronic signatures, which adds timestamp field to protect against repudiation.

[R55]. PDF Advanced Electronic Signatures			
Abbreviation	**PAdES**	Custodian	European Telecommunications Standards Institute (ETSI)
Version	v1.1.1 (Part 1) v1.2.1 (Part 2) v1.2.1 (Part 3) v1.1.2 (Part 4) v1.1.2 (Part 5)	Announcement date	31.07.2009 (Part 1) 31.07.2009 (Part 2) 13.07.2010 (Part 3) 18.12.2009 (Part 4) 18.12.2009 (Part 5)
Registration date	24.01.2014	Revision date	13.07.2016
Reference URL	http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf (Part 1) http://www.etsi.org/deliver/etsi_ts/102700_102799/10277802/01.02.01_60/ts_10277802v010201p.pdf (Part 2) http://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/ts_10277803v010201p.pdf (Part 3) http://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/01.01.02_60/ts_10277804v010102p.pdf (Part 4) http://www.etsi.org/deliver/etsi_ts/102700_102799/10277805/01.01.02_60/ts_10277805v010102p.pdf (Part 5)		

PAdES is an ETSI standard (www.etsi.org) that provides extensions to PDF and the ISO 32000-1 standards and specifies precise profiles for use with advanced electronic signature in the meaning of eIDAS Regulation (EU) No 910/2014 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN).
PAdES SHOULD BE used from a government organisation when needed to implement advanced electronic signatures that remain valid over long periods and are compliant with Regulation (EU) No 910/2014.

The PAdES technical specification contains the following 5 parts:

- Part 1: PAdES Overview – a framework document for PAdES
- Part 2: PAdES Basic – Profile based on ISO 32000-1
- Part 3: PAdES Enhanced – PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles

- Part 4: PAdES Long Term – PAdES-Long Term Validation Profile
- Part 5: PAdES for XML Content – Profiles for XAdES signatures of XML content in PDF files.

[U19]. openID			
Abbreviation	**openID**	Custodian	OpenID Foundation (OIDF)
Version	v2.0	Announcement date	05.12.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://openid.net/specs/openid-authentication-2_0.html		

openID is an open standard, developed and maintained by the OIDF (http://openid.net) that MAY BE used for user authentication in a website or a web application using a third party service, where the organisation does not need to use its own infrastructure. Users have the ability to create an account with an openID identity provider (such as Google, Yahoo!, PayPal, BBC, AOL, MySpace, IBM, Steam, Orange and VeriSign) and use it to authenticate themselves in a website or a web application which accepts OpenID authentication.

9.9 Standards for Specific Business Sectors

9.9.1 Medical Images Exchange

[M51]. Digital Imaging and Communications in Medicine			
Abbreviation	**DICOM**	Custodian	National Electrical Manufacturers Association (NEMA)
Version	2011	Announcement date	2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://medical.nema.org/standard.html		

DICOM is a standard developed by NEMA, the Association of Electrical Equipment and Digital Imaging Manufacturers, that facilitates interoperability of medical imaging equipment.

DICOM SHALL BE used for exchanging, handling, storing and printing medical imaging information using equipment from different manufacturers that conforms to the standard. DICOM has also been standardised as the ISO12052:2006 international standard (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43218).

9.9.2 Medical Data Exchange

[M52]. Health Level 7			
Abbreviation	**HL7**	Custodian	Health Level Seven (HL7)
Version	v2.x	Announcement date	2011 (v2.7)
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.hl7.org/implement/standards/product_brief.cfm?product_id=185		

HL7 v2.x set of specifications is a widely implemented standard for healthcare in the world that SHALL BE used for the exchange, integration and retrieval of medical and other healthcare electronic data between various healthcare systems, such as Patient Administration Systems (PAS), Laboratory Information Systems (LIS), Electronic Medical Record (EMR) and Electronic Health Record (EHR) systems, etc. The standard is developed and maintained by the Health Level Seven (HL7) organisation, initially released in October 1987.

As of March 2013, the HL7 organisation has announced its decision to make its standards freely available under licensing terms.

[U20]. Health Level 7			
Abbreviation	**HL7**	Custodian	Health Level Seven (HL7)
Version	v3	Announcement date	2005
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.hl7.org/implement/standards/product_brief.cfm?product_id=186		

HL7 v3 is not a new version of the standard following v2, rather a restructured standard aiming to support all healthcare workflows. HL7 v3 suite of specifications is based on the Reference Information Model (RIM) and defines a model-driven methodology for the exchange of clinical information, where messages and electronic documents are structured in an XML format. HL7 v3 includes standards for communications that document and manage the care and treatment of patients in a wide variety of healthcare settings. HL7 v3 MAY BE used for the exchange, integration and retrieval of medical and other healthcare electronic data, as well as for the design and/or implementation of relative healthcare workflows.

9.9.3 Geographical Data Representation and Exchange

[M53]. Geography Markup Language			
Abbreviation	**GML**	Custodian	Open Geospatial Consortium (OGC)
Version	v3.2.1	Announcement date	27.08.2007
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://portal.opengeospatial.org/files/?artifact_id=20509		

Geography Markup Language is an XML-based standard that SHALL BE used for geographic data representation, as well as the transport and storage of geographic information. GML consists of a language for modelling geographic systems and an open interchange format for geographic transactions on the Internet.

GML is standardised as the ISO 19136:2007 international standard (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=32554). The MIME identifier for GML is “application/gml+xml”.

[R56]. GeoTIFF			
Abbreviation	**GeoTIFF**	Custodian	N/A
Version	v1.8.2	Announcement date	28.12.2000
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.remotesensing.org/geotiff/spec/geotiff1.html		

GeoTIFF v1.8.2 is a standard initially developed by Dr. Niles Ritter, a former member

of NASA Jet Propulsion Labs that can be used to embed geographical information within a TIFF file. This information originates from satellite imaging systems, scanned aerial photography, scanned maps, digital elevation models or as a result of geographic analyses. GeoTIFF v1.8.2 SHOULD BE used to exchange geographical information within a TIFF file, in case of incompatibility issues with software that cannot read specialized metadata but is able to read standard TIFF files.

The GeoTIFF Working Group was responsible for the development of the current version, which derived from many discussions between an international body of TIFF users and developers. GeoTIFF is fully compatible with the TIFF 6.0 specifications.

[R57]. Keyhole Markup Language			
Abbreviation	**KML**	Custodian	Open Geospatial Consortium (OGC)
Version	v2.2	Announcement date	14.04.2008
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://portal.opengeospatial.org/files/?artifact_id=27810		

KML is an XML language focused on geographic visualization, including annotation of maps and images within two-dimensional maps and three-dimensional Earth browsers. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look. KML SHOULD BE used as a complimentary standard to GML for geographic information representation and/or exchange of geographic data.

Initially KML was developed by Keyhole Inc., which was acquired by Google Inc. in 2004. KML became an OGC standard in 2008. Since then, OGC and Google have agreed that there can be additional harmonization of KML with GML (e.g. to use the same geometry representation) in the future, in order to avoid duplications and leverage the work done, improving interoperability in the geographical information domain.

The MIME identifier for KML is “application/vnd.google-earth.kml+xml” or “application/vnd.google-earth.kmz”.

[U21]. Geography Markup Language			
Abbreviation	**GML**	Custodian	Open Geospatial Consortium (OGC)
Version	v3.3	Announcement date	07.02.2012
Registration date	02.12.2013	Revision date	N/A
Reference URL	https://portal.opengeospatial.org/files/?artifact_id=46568		
GML v3.3 provides extended schemas and encoding rules compared to version 3.2.1. This version of GML is backwards compatible with the previous version GML 3.2. GML v3.3 MAY BE used in case a geographical feature cannot be modelled with schemas defined in version 3.2.1.			

9.9.4 e-Learning Content

[M54]. Shareable Content Object Reference Model			
Abbreviation	**SCORM**	Custodian	Advanced Distributed Learning (ADL) Initiative
Version	2004 4th edition	Announcement date	14.08.2009
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://www.adlnet.gov/wp-content/uploads/2011/07/SCORM_2004_4ED_v1_1_Doc_Suite.zip		
SCORM is a standard that SHALL BE used for the creation of online learning content, which is used in a web based e-learning platform as well as for the definition of communication principles between e-learning platforms.			

9.9.5 Election Data Exchange

[R58]. Election Markup Language			
Abbreviation	**EML**	Custodian	Organization for the Advancement of Structured Information Standards (OASIS)
Version	v7.0	Announcement date	27.10.2011
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://docs.oasis-open.org/election/eml/v7.0/cs01/eml-v7.0-cs01.pdf		

EML is an OASIS (https://www.oasis-open.org/) standard that SHOULD BE used for the structured data interchange in the specific environment of election or voter services provision to public or private organizations. The objective is to introduce a uniform and reliable way to allow systems involved in the election process to interact. EML contains a set of data and message definitions described as XML schemas. EML is flexible enough to be used for elections and referendums that are primarily paper-based or that are fully e-enabled.

9.9.6 Virtualisation

[M55]. Open Virtualization Format			
Abbreviation	**OVF**	Custodian	Distributed Management Task Force (DMTF)
Version	v1.1	Announcement date	12.01.2010
Registration date	02.12.2013	Revision date	N/A
Reference URL	http://dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf		

OVF is an open, portable virtualization format maintained by DMTF, a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability. OVF SHALL BE used for the packaging and

distribution of software to be run in virtual machines. The current version has been developed as a result of joint work with many individuals and teams, including corporate representative staff from IBM, Oracle, VMware, Symantec, Intel, NEC, Microsoft, Dell etc.

The OVF standard is independent from the hypervisor or process architecture used, supported by all major virtualization platforms (VirtualBox, VMware ESXi, Red Hat Enterprise Virtualization, Oracle VM, IBM SmartCloud, SUSE Studio etc.). As of November 2011, OVF has been adopted by the ISO organisation as the ISO/IEC 17203:2011 international standard (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59388).

10 IMPLEMENTATION GUIDELINES

10.1 For government organisations

Government organisations planning to develop information systems for the provision of eServices to citizens and businesses shall specify the necessary interoperability requirements and specifications to be followed as well as the technical standards to be used in the appropriate document (e.g. requirements document, design document, specifications document). A list of preferred technologies may complement the technical standards to be used, in case this is in line with public procurement legislation and procedures. For information systems that will be developed through public procurement contracts, the elaboration of an interoperability study should be included in the obligations of the Contractor described in the tender documents of the competition. At least the following topics must be adequately covered by the interoperability study:

- Description of the business processes to be supported by the information system:
  - Process title,
  - Process description (start event, steps, end event), including graphical representation,
  - Roles responsible for each step of the process,
  - Information exchanged during the execution of the process,
  - Information exchange requirements with other organisations or entities.
- Description of the technical environment and the technical standards to be used for the interconnection and exchange of information with third party information systems:
  - Logical and technical architecture of the system,
  - Schemas for the representation of the information and metadata,
  - XML schemas and web services.

Similar topics shall be also addressed for all interoperability interfaces (processes and information systems) of the information system to be developed.

Government organizations shall ensure the results of the interoperability study comply with the principles, recommendations and standards of the eGIF.

It should be noted that the interoperability study may be part of another project deliverable or document.

10.2 For businesses

The role of businesses in the context of the eGIF is three-fold:

- Businesses that use eServices to interact with government organisations. In this case, the eGIF does not impose any requirements regarding the use of eServices by businesses, apart from the use of 'standard' ICT infrastructure, i.e. a web browser and an Internet connection. Of course, depending on the nature and the implementation of the eServices, additional features that conform to the appropriate eGIF standards may be required, such as digital certificates.
- ICT companies, contracted by the Government for the development of information systems. In this case, government contractors shall ensure that the information systems and services they develop are based on the eGIF standards, except otherwise required by the responsible government organisation (Contracting Authority).
- ICT companies and related associations, acting as 'reviewers' of the eGIF, which, based on their practical experiences from eGIF's implementation in ICT projects, submit comments or suggestions for changes to the eGIF.

10.3 For citizens

In the eGIF context, citizens are perceived as eGovernment services users. Similarly to businesses, the eGIF does not impose any requirements regarding the use of eServices by citizens, apart from the use of 'standard' ICT infrastructure, i.e. a web browser and an Internet connection. Of course, depending on the nature and the implementation of the eServices, additional features that conform to the appropriate eGIF standards may be required, such as digital certificates.

11 CONFORMANCE & AUDIT REQUIREMENTS

11.1 Conformance requirements

The adoption of eGIF's principles, recommendations and standards is mandatory for all government organisations. This obligation refers to the development of new information systems and eServices for the Government as well as to the upgrade/enhancement of existing ones. Current government information systems may continue to operate in the same way as now, but, in case they are upgraded, they must conform to eGIF's standards.

The mandatory nature of the conformance to eGIF is preferable to the voluntary conformance of government information systems to the framework, due to the following reasons:

- The existence of a central ICT unit (DITS) for the entire Government favours the mandatory enforcement of ICT standards.
- Other IT standards are of mandatory application as well (i.e. DITS IT standards).
- Faster adoption of the eGIF, leading to a uniform ICT landscape in the Cyprus Government.

On the other hand, the following problems may be raised:

- IT projects currently in implementation stage may not be fully compliant with the eGIF, thus conforming to the eGIF may require changes and probably additional cost (e.g. in case a system is developed under a contract).
- IT projects currently in a design stage (e.g. tender documents elaboration) may require additional time to integrate the changes to the specifications that derive from the eGIF, thus causing delays to their procurement/development.
- Private sector ICT companies that undertake contracts for the government may raise significant disagreements to the eGIF specifications, in case their software development methods or products do not conform to eGIF.

Based on the above, **it is suggested that the eGIF becomes mandatory after a short trial period of time**, e.g. 6 months after its initial announcement. However, during this period, the design of new IT projects (e.g. requirements elicitation, tender documents preparation) shall take into account the eGIF standards.

11.2 Audit requirements

The conformance of an information system must be checked in several stages of the software development lifecycle:

- **During the design stage**. In this stage the requirements of the system are elaborated and probably the tender documents for the procurement of the system are prepared. Therefore the entities responsible to carry out this task (government officers or private sector contractors) shall:
  - take into account the eGIF,
  - integrate several of its provisions to the requirements of the system, and
  - include a generic obligation that "the information system to be developed must conform to the eGIF".

    The obligation for the elaboration of a specific interoperability study is also strongly suggested to be included.
- **During the implementation stage**. In this stage, both the entity developing the system (most probably a private sector contractor) and the government officers who are responsible to monitor and support the system implementation shall ensure that the system conforms to the eGIF. Again, this can be checked is several points of the system implementation:
  - During the finalisation of the system's requirements, by reviewing the requirements document, design document, implementation/interoperability study or a similar project deliverable and ensuring that the eGIF provisions have properly and adequately been considered.
  - During the acceptance tests of the system or specific modules, when the interoperability requirements of the system are thoroughly checked against the document that describes them.
- **During the final acceptance of the system**, when the overall conformance of the system and its documentation to the eGIF is checked. In reality, during this stage, the results of the conformance checks performed in previous stages are again verified.

It shall be noted that a new government information system must not be put into real operation mode unless its conformance to the eGIF is adequately proved.

12 APPENDICES

12.1 Appendix A: Overview of eGIF Technical Standards

The technical standards of the National eGovernment Interoperability Framework of Cyprus are summarized in the following table.

Table 1: Overview of eGIF Technical Standards

Category	Sub-Category	Mandatory	Recommended	Under Observation
eGovernment Applications Documentation & Development	**Modelling Methods**		UML v2.4.1	UML v2.5
	Process Models Exchange Schemas		XMI v2.4.2 XPDL v2.2	XMI 2.5.1 Canonical XMI Beta 2
Service Modelling	**Process Modelling Methods**	BPMN v2.0	UML v2.4.1 (Activity Diagrams)	UML v2.5
	Process Execution Languages		WS-BPEL v2.0	
Data Modelling	**Modelling Methods**	E-R Diagram (ERD)	UML v2.4.1	UML v2.5
	Data Models Exchange Schema	XSD v1.1	XMI v2.4.2 XSD v1.0	XMI v2.5.1 Canonical XMI Beta 2
	Data Exchange Formats	XML v1.0 (Fifth edition)	JSON	XML v1.1 (Second edition)
	Data Transformation	XSLT v2.0		
	Metadata Schema	Dublin Core v1.1		
	Metadata description	RDF v1.1		
	Semantic Information representation languages	XML v1.0 (Fifth edition)	OWL v2.0	XML v1.1 (Second edition) CCTS v3.0

Category	Sub-Category	Mandatory	Recommended	Under Observation
Application Development Frameworks and Programming Languages		Java SE v8 Java EE v7	.NET Framework v4.6.x JavaScript	Java ME v8
Information Presentation and Processing	**Accessibility**	WCAG v2.0	Mobile Web Best Practices v1.0	
	Hypertext Exchange Schemas	HTML v4.01	XHTML v1.0 HTML v5 XHTML Basic v1.1	
	Stylesheets	CSS v 2.1 XSL v1.1		
	Character Sets Encoding	UTF-8 v6.2		
	Date & Time Representation	ISO 8601		
	File Formats Recognition	MIME v1.0 (RFC 2045 – RFC 2049)		
	Document formats for Information Exchange	HTML v4.01 PDF v1.7 (Sixth edition)	HTML v5	
	Document formats for Information Processing	TXT ODF v1.2 OOXML (ISO/IEC 29500:2012, ECMA-376:2012)		
	Graphics Exchange Formats	GIF v89a JPEG v1.02	PNG (Second edition) TIFF v6.0 SVG v1.1 (Second edition)	JPEG 2000

Category	Sub-Category	Mandatory	Recommended	Under Observation
	Sound, Video and Video Streaming file formats	MPEG-4 v2 OGG (Vorbis I)	QuickTime v7.7.x	WebM
	Data Compression	ZIP v6.3.4		
Communication and Interoperability	**Interoperability with Third-Party Systems**	SOAP v1.2 (Second edition) WSDL v2.0	UDDI v2 UDDI v3 WS-I BP v1.2 WS-I BP v2.0 WSDL v1.1 SOAP v1.1 XQuery 1.0 (Second edition)	XQuery 3.0
	Discovery of Resources	DNS	LDAP v3 UDDI v2 UDDI v3	
	Locating of Resources	URI URL		
	Network Protocols	IP v4 ICMP v4 SNMP v3	SSH v2 BGP v4 RIP v2 OSPF v2 ESP SNMP v2	IP v6 OSPF v3 ICMP v6 RIPng
	Application Layer Protocols	FTP HTTP v1.1 SMTP POP v3 IMAP v4 (Revision 1)		
	IP Telephony		H.323 v7.1	

Category	Sub-Category	Mandatory	Recommended	Under Observation
			SIP v2.0	
	Content Delivery	RSS v2.0 Atom v1.0		
Security and Authentication	**Web Services Security**	WS-Security v1.1.1	WS-SecurityPolicy v1.3 WS-Policy v1.5 WS-SecureConversation v1.4	
	Data Transmission Security	TLS v1.2 HTTPS	X.509 v3 (7th edition)	
	Encryption	AES SHA v2 XML-Enc v1.1	XKMS v2.0 TDES or 3DES	
	Authentication, Identification and Authorisation	XML Signature v1.1 WS-Trust v1.3	WS-Trust v1.4 WS-Federation v1.2 WS-Addressing v1.0 SAML v1.1 SAML v2.0 XACML v2.0 XACML v3.0 XAdES v1.4.1 CAdES v1.8.3 PAdES [v1.1.1 (Part 1), v1.2.1 (Part 2), v1.2.1 (Part 3), v1.1.2 (Part 4), v1.1.2 (Part 5)]	openID v2.0
Standards for specific Business Sectors	**Medical images exchange**	DICOM 2011		
	Medical data	HL7 v2.x		HL7 v3

Category	Sub-Category	Mandatory	Recommended	Under Observation
	exchange			
	Geographical data representation and exchange	GML v3.2.1	GeoTIFF v1.8.2 KML v2.2	GML v3.3
	e-Learning content	SCORM 2004 4th edition		
	Election data exchange		EML v7.0	
	Virtualization	OVF v1.1		

12.2 Appendix B: References

[1] "A Digital Agenda for Europe", Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 245 final/2, 26.8.2010

[2] "The European eGovernment Action Plan 2011-2015, Harnessing ICT to promote smart, sustainable & innovative Government", Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 743 final, 15.12.2010

[3] "Towards interoperability for European public services", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 744 final, 16.12.2010

[4] "European Interoperability Framework - Implementation Strategy", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2017) 134 final, Brussels, 23.3.2017

[5] Lampathaki, F., Tsiakaliaris, C., Stassis, A., Charalabidis, Y. (2009), "National Interoperability Frameworks: The Way Forward", in Charalabidis Y. (Ed.): "Interoperability in Digital Public Services and Administration: Bridging E-Government and E-Business", IGI Global book, ISBN: 978-1-61520-887-6, 2011

[6] Greek eGovernment Interoperability Framework, www.e-gif.gov.gr (retrieved: September 2013)

[7] SAGA 5 for the federal Government, IT Council, http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/saga_node.html (retrieved: September 2013)

[8] "Confederations-wide IT Control (IT-Steuerung Bund)," http://www.cio.bund.de/SharedDocs/Publikationen/DE/Bundesbeauftragte-fuer-Informationstechnik/konzept_it_steuerung_bund_download.pdf?__blob=publicationFile. (retrieved: September 2013)

[9] SAGA 5.0, http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/SAGA%205-aktuelle%20Version/saga_5_aktuelle_version_node.html. (retrieved: September 2013)

[10] "Rahmenarchitektur IT-Steuerung Bund," http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/rahmenarchitektur_itsteuerung_bund_grundlagen_download.pdf?__blob=publicationFile. (retrieved: September 2013)

[11] An overview of the eGovernment and eInclusion situation in Europe, http://www.epractice.eu/en/factsheets/, Germany – Denmark – Estonia – United Kingdom. (retrieved: October 2013)

[12] Transforming government services to make them more efficient and effective for users, Policy, https://www.gov.uk/government/policies/transforming-government-services-to-make-them-more-efficient-and-effective-for-users. (retrieved: September 2013)

[13] Digital by Default Service Standard, Government Service Design Manual, https://www.gov.uk/service-manual/digital-by-default. (retrieved: September 2013)

[14] e-Government Interoperability Framework, Cabinet Office, Version 6.1, 18 March 2005.

[15] Government Digital Service, http://digital.cabinetoffice.gov.uk/about/ (retrieved: September 2013)

[16] "Open Standards Principles: For software interoperability, data and document formats in government IT specifications", HM Government, Crown Copyright 2012.

[17] Introduction til national enterprise architecture in Denmark - http://arkitekturguiden.digitaliser.dk/introduction-til-national-enterprise-architecture-denmark. (retrieved: October 2013)

[18] OIO Catalog, Danish Interoperability Framework portal, http://digitaliser.dk/katalog/2. (retrieved: October 2013)

[19] Danish Interoperability Framework technical standards list, http://digitaliser.dk/katalog/2/alle. (retrieved: October 2013)

[20] "Brugervejledning for OIO-katalog over offentlige it-standarder (User Guide for OIO catalog of public IT standards)", Version 2.0, April, 2008, http://arkitekturguiden.digitaliser.dk/oio-ea-20-beta-0.

[21] "Denmark – Efficient e-Government for Smarter Public Service Delivery", OECD e-Government Studies, Preliminary Copy, 3 June 2010.

[22] The EA Pad – Enterprise Architecture in Denmark, http://eapad.dk/gov/dk/. (retrieved: October 2013)

[23] "Interoperability Framework", Interoperability of the State Information System, Ministry of Economic Affairs and Communications, version 3.0, 2011.

[24] "Harmonization of the Estonian framework with the European framework," in Interoperability Framework of the State Information System, 3rd ed., Talin, Ministry of Economic Affairs and Communications, 2011, pp. 40-42.

[25] "Administration system for the state information system RIHA", Estonian Information System's Authority, https://www.ria.ee/administration-system-of-the-state-information-system/. (retrieved: October 2013)

[26] "Information security interoperability framework", Interoperability of the State Information System, Ministry of Economic Affairs and Communications, version 2, 2011.

[27] "Software Framework", Interoperability of the State Information System, Ministry of Economic Affairs and Communications, version 2, 2012.

[28] "Framework of Websites", Interoperability of the State Information System, Ministry of Economic Affairs and Communications, version 1.0, 2012.

12.3 Appendix C: eGIF Governance - OMITTED

12.4 Appendix D: Examples of SOA implementations in Cyprus Government