

CAMSS ASSESSMENT EIF SCENARIO v6.0.0



METHODOLOGY

Disclaimer

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this document. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

© European Union, 2023

European Commission

Directorate-General for Informatics
Directorate D – Digital Public Services, Unit B2 – Interoperability Unit
Contact: Raul-Mario Abril-Jimenez – Project Officer for the CAMSS action
E-mail: Raul-Mario.ABRIL-JIMENEZ@ec.europa.eu
European Commission
B-1049 Brussels

Luxembourg: Publications Office of the European Union, 2023

© European Union, 2022

Reuse is authorised provided the source is acknowledged.

The reuse policy of European Commission documents is regulated by Decision 2011/833/EU (OJ L 330, 14.12.2011, p. 39).

Table of content

Table of content	3
1. Introduction	5
1.1 What is the purpose of this document?	5
1.2 Who is this document meant for?	5
1.3 What is the value of CAMSS?	6
2. Use cases	7
2.1 Solution Architect	7
2.2 Government Official	7
2.3 Public Procurer	8
2.4 Consideration on assessing families of specifications.....	8
3. EIF Scenario	9
3.1 Description	9
3.2 Categories and Criteria	9
3.1.2.1 PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY.....	9
3.1.2.2 EIF CORE INTEROPERABILITY PRINCIPLES	10
3.1.2.3 EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS.....	16
3.1.2.4 EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS	21
3.1.2.5 EIF INTEROPERABILITY LAYERS	23
4. Glossary	27

Table of figures

Figure 1: Diagram of possible users that are involved in the use cases	7
---	---

1. Introduction

1.1 What is the purpose of this document?

The purpose of this document is to provide guidance for assessing standards and specifications using the Common Assessment Method for Standards and Specifications (CAMSS)¹. The main objective of CAMSS is achieving interoperability and avoiding vendor lock-in by establishing a neutral and unbiased method for the assessment of technical specifications and standards in the field of ICT. This method is compliant with the Regulation 1025/2012 on European Standardisation.

Note that CAMSS is the European guide for assessing and selecting standards and specifications for eGovernment projects, a reference when building an architecture, and an enabler for justifying the choice of standards and specifications in terms of interoperability needs and requirements. It is fully aligned with the European Standardisation Regulation 1025/2012.

Reviewing this document will lead the reader to the following.

- Understand what the CAMSS Assessment EIF scenario is and how an assessment can be carried out using it.
- Know which inputs are expected per scenario to properly assess the standard or specification.
- Understand the relevance of criteria established by the scenario and its scope.

The CAMSS Assessment EIF Scenario – which this document supports – can be found [here](#) together with the different release components for each release.

1.2 Who is this document meant for?

This document applies to different user profiles with the need to analyse and assess a standard or a specification. This is possible as the document provides different elements for the development and understanding of assessments and their insights.

Examples of these profiles are as follows.

- **Solution Architect** is the person in charge of leading the practice, and introducing the overall technical vision for a particular solution.
- **Government Official** is an official who works for a government department.
- **Policymaker** is a member of a government department who is responsible for making new rules and laws.
- **Public Procurer** is a person who is involved in procurement processes.

¹CAMSS Collection Homepage: <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/about>

You will find more information about how these profiles can leverage this document later on in the “Use cases” Section.

Moreover, it is worth mentioning that all users doing assessments by themselves can afterwards use the CAMSS as a Service (CAMSSaaS²) to ensure the assessment is compliant with the different requirements. For more information about the service, [here](#) is the Joinup space for the solution and service.

1.3 What is the value of CAMSS?

CAMSS is an established European guide for assessing and selecting standards and specifications for eGovernment projects. It can be used as a reference when building an ICT architecture, and for justifying the selection of standards and specifications.

The use of CAMSS allows for the following.

- Improvement of quality by increasing transparency, efficiency, and accountability in public administrations.
- Increase reusability by reusing existing assessments or specifications already recommended by EU Member States.
- Saving time by reducing administrative burden, speeding up assessment processes.
- Being compliant by assessing the compliance of cutting-edge specifications with reference frameworks.

The CAMSS method provides a comprehensive method and guidance for the assessment and selection of standards and specifications. It is focused on fostering interoperability and avoiding the vendor lock-in within the context of European Interoperability.

Moreover, the CAMSS Assessment EIF Scenario is available for use on self-assessments and can be accessed via Joinup. The CAMSS Team uses the CAMSS Assessment EIF Scenario on a regular basis to produce assessments using this scenario. The use by CAMSS Team allows for the detection and improvement of the scenario as well as the current document.

² CAMSSaaS access point: <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-service-camssaaS>

2. Use cases

This methodology can be applied to different use cases. The following diagram presents three main profiles that can use the CAMSS Tools.

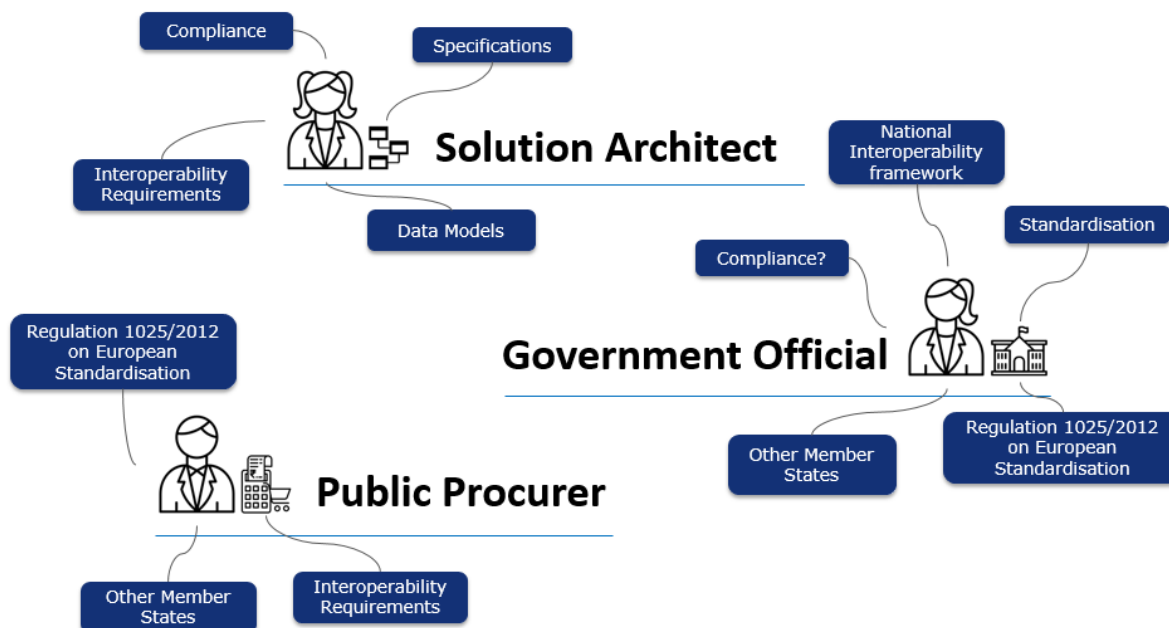


Figure 1: Diagram of possible users that are involved in the use cases

- **Solution Architect** is the person in charge of leading the practice and introducing the overall technical vision for a particular solution.
- **Government Official** is an official who works for a government department.
- **Public Procurer** is a person who is involved in procurement processes.

2.1 Solution Architect

As a Solution Architect, I want to assess a technical specification so I can determine its suitability as an interoperability enabler by evaluating it against the requirements of the European Interoperability Framework.

2.2 Government Official

As a Government Official in a Member State, in charge of developing the national catalogue of standards, I want to assess a technical specification so I can collect the evidence that it complies with the principles of the European Interoperability Framework (EIF) ³.

³ European Interoperability framework: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

As a Government Official in a Member State, I want to assess a (national) technical specification in an effort to support its developmental improvement towards their recognition as EU or at least cross-border standards.

2.3 Public Procurer

As a Public Procurer, I want to assess the compliance of a specification with the requirements laid out in the standardisation regulation 1025/2012⁴ to determine if I can reference it in my public procurement documents (e.g. Terms of Reference).

As a Public Procurer, I want to provide clear technical requirements in the procurement requests I issue in terms of specifications for a solution's building blocks.

2.4 Consideration on assessing families of specifications

Specifications belonging to a family of specifications often depend on their companion documents to be fully implemented. This fact may influence the overall assessment performance, the score of which may be reduced.

To prevent this from happening, when evaluating a specification belonging to a specification family, it is important that, instead of considering the specification in isolation, consider the feature that can achieve by leveraging other specifications from the family. For this reason, whenever possible, it is important to mention the specification together with the accompanying documents, to emphasize their complementarity and positively justify the assessment criteria.

The same reasoning applies to individual specifications whose functionalities can be enhanced with extensions and/or complementary specifications, such as DNS and DNSSec or HTTP and HTTPS. In these cases, the approach should be the same as the one used to evaluate families of specifications.

Another case that can lead to misunderstanding and answering negatively harming the score of the specification is when a specification has been built over another defacto standard or relevant specifications. To illustrate, a simple case that brings light to the situation is the extension of Core Vocabularies. Some vocabularies are used as the basis, or directly extended. In those cases, the specification cannot be hampered by depending on external specifications. A case where it happens is in both CAMSS Vocabularies, the CSSV and the CAV, which reuse DCAT or the CCCEV in the case of the CAV.

⁴ Regulation (EU) No 1025/2012 Standardisation Regulation <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R1025>

3. EIF Scenario

The EIF Scenario contains different sections according to the insights and recommendations of the European Interoperability Framework (EIF).

The different sections of the scenario are organised according to criteria, which are declared as Criterion 1 (A1), Criterion 2 (A2), and so on. For every criterion, there is an instruction or guidance on how to answer, as detailed below.

The current document is targeting the latest version of the CAMSS Assessment EIF Scenario, which is 6.0.0. Even though the methodology can be used amongst versions as some criteria remain the same, this document is specific to version 6.0.0 of the scenario. If the user is using a previous version, use the methodology included as a release component for the scenario.

3.1 Description

The European Interoperability Framework (EIF) provides guidance to public administrations on how to improve the governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that existing and new legislation does not compromise interoperability efforts. This CAMSS Scenario allows for the assessment of the compliance of interoperability specifications with the EIF. The objective of the obtained assessment is to determine the suitability of the assessed interoperability specification for the delivery of interoperable European public services.

3.2 Categories and Criteria

The different criteria in the EIF scenario are divided considering the recommendations of the European Interoperability Framework (EIF).

3.1.2.1 PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

This category is related to the first underlying principle (UP)⁵ of the EIF Subsidiarity and Proportionality (UP1). The basis of this principle is to ensure that the EU Actions are taken or stated to improve national actions or decisions. Specifically, it aims to know if National Interoperability Frameworks are aligned with the EIF.

SUBSIDIARITY AND PROPORTIONALITY

Criterion 1 (A1) – To what extent has the specification been included in a national catalogue from a Member State whose National Interoperability Framework has a high performance on interoperability according to National Interoperability Framework Observatory factsheets?

⁵ EIF Underlying Principles: <https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/2-underlying-principles-european-public-services>

Search for the specification in the National catalogue of Member States. Only Member States with aligned NIFO factsheets are considered for this criterion.

NIFO factsheets can be found in the following link:

<https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets>

EIF Recommendation 1: Ensure that national interoperability frameworks and interoperability strategies are aligned with the EIF and, if needed, tailor and extend them to address the national context and needs.

This criterion assesses if the specifications have been included within the National Catalogues of Specifications of the Member States that are highly aligned with the higher level of performance in terms of interoperability.

The Digital Public Administration Factsheets use three categories to evaluate the level of National Interoperability frameworks in accordance with the EIF. The three categories are 1. CONCEPTUAL MODEL FOR INTEGRATED PUBLIC SERVICES PROVISION; 2 INTEROPERABILITY LAYERS, and 3. INTEROPERABILITY PRINCIPLES. National Interoperability Frameworks reports can be found here:
<https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2021>

3.1.2.2 EIF CORE INTEROPERABILITY PRINCIPLES

In this category, elements related to the core interoperability principles (UP) are encompassed, which are: openness (UP2), transparency (UP3), reusability (UP4), technological neutrality and data portability (UP5).

OPENESS

Criterion 2 (A2) – Does the specification facilitate the publication of data on the web?

The evidence used to justify this criterion will typically come from the function of the specification or a specific implementation of it. The specification must meet at least one level of the Tim Berners-Lee 5-star to be positive.

The 5-star of Tim Berners-Lee can be found in the following link:

<https://5stardata.info/en/>

EIF Recommendation 2:

Publish the data you own as open data unless certain restrictions apply.

Relates to the ability of the specification to publish data as open data or not.

Criterion 3 (A3) – To what extent do stakeholders have the opportunity to contribute to the development of the specification?

The evidence to justify this criterion can typically be found on the webpage of the SDO that developed the standard or specification. The SDO must confirm that all stakeholders can contribute to developing their solutions.

EIF Recommendation 3:

Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Relates to in which measure the different stakeholders that a specification can benefit can participate in the working groups focused on the development of certain specifications.

Criterion 4 (A4) – To what extent is a public review part of the release lifecycle?

The evidence to justify this criterion will typically be found on the webpage of the SDO that developed and/or maintains the standard or specification. The SDO must confirm that a public review is part of the development and approval of the specification.

EIF Recommendation 3:

Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

A public review consists of the public availability of the specification's draft for stakeholders to provide inputs for the improvement and fix of possible bugs.

Criterion 5 (A5) – To what extent do restrictions and royalties apply to the specification's use?

The evidence to justify this criterion will typically be available on the webpage of the SDO developing and/or maintaining the standard or specification. FRAND shall be understood according to the description provided in the Communication from the Commission to the European Parliament, the Council and the European Economic, and Social Committee setting out the EU approach to Standard Essential Patents.

For more information:

<https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/fair-reasonable-and-non-discriminatory-frand-licensing-terms-research-analysis-controversial>

EIF Recommendation 3:

Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Additionally to the EIF's recommendation that refers to open-source software it applies to a specification in itself at any interoperability level (legal, organisational, semantic, or technical)

Criterion 6 (A6) – To what extent is the specification sufficiently mature for its use in the development of digital solutions/services?

The evidence to justify this criterion will typically consist of providing implementations of the specification or providing information about the creation date and the updates of the specification.

EIF Recommendation 4:

Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support, and innovation.

Maturity related to the stability of the specification, meaning that it has been evolved enough and mechanisms for its development have been put in place (Change Management processes, monitoring, etc.)

Criterion 7 (A7) – To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?

The evidence to justify this criterion will typically consist of providing implementations of the specification or providing information about the creation date and the updates of the specification.

EIF Recommendation 4:

Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support, and innovation.

Maturity related to the stability of the specification, meaning that it has been evolved enough and mechanisms for its development have been put in place (Change Management processes, monitoring, etc.)

Criterion 8 (A8) – To what extent has the specification support from at least one community?

The evidence to justify this criterion will typically consist of checking if any work or development has been carried out by any developer community regarding the standard or specification.

EIF Recommendation 3:

Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Relates to whether communities exist around the specification at any level legal, organisational, semantic, or technical contributions to its enhancement and development.

TRANSPARENCY

Criterion 9 (A9) – To what extent does the specification enable the visibility of administrative procedures, rules data, and services?

The evidence to justify this criterion will typically consist of providing examples of implementations or plans for the inclusion of the standard or specification in any process related to public administration. A common use case is the digitalisation of public services.

EIF Recommendation 5:

Ensure internal visibility and provide external interfaces for European public services.

Criterion 10 (A10) – To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?

The evidence to justify this criterion will typically consist of providing implementations or plans for the inclusion of the standard or specification in any process related to a public administration. A common use case is the digitalisation of public services.

EIF Recommendation 5:

Ensure internal visibility and provide external interfaces for European public services.

Criterion 11 (A11) – To what extent does the specification enable the exposure of interfaces to access the public administration's services?

The evidence to justify this criterion will typically consist of providing evidence of services that implemented the specification to exchange and make use of information more efficiently and overcome interoperability barriers.

EIF Recommendation 5:

Ensure internal visibility and provide external interfaces for European public services.

Relates to ensuring availability of interfaces with internal information systems. As the EIF defines: *Public administrations operate a large number of what are often heterogeneous and disparate information systems in support of their internal processes. Interoperability depends on ensuring the availability of interfaces to these systems and the data they handle. In turn, interoperability facilitates the reuse of systems and data and enables these to be integrated into larger systems.*

REUSABILITY

Criterion 12 (A12) – To what extent is the specification usable beyond the business-specific domain, allowing its usage and implementation across business domains?

The evidence to justify this criterion will typically consist of providing examples of usage of the standard or technical specifications in domains different from the one for which it was originally developed. For example, DCAT-AP – which was developed under a specific purpose and domain – describes public sector datasets for open data portals. However, it has been commonly reused for the creation of other specifications and solutions rather than data portals in Europe.

EIF Recommendation 6:

Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

Relates to the use of the specification beyond a specific business domain. E.g. a specification developed under the eHealth domain that can be used in other domains or not.

TECHNOLOGICAL NEUTRALITY AND DATA PORTABILITY

Criterion 13 (A13) – Is the specification technology agnostic?

The evidence to justify this criterion will typically consist of checking that the implementation of the standard or specification does not rely on/depend on any other standard or specification mainly focused on proprietary technologies or vendors. However, it should be considered whether the specification is dependent on other specifications, even if they are open source. Meaning that the specification requires other specifications/platform to run.

EIF Recommendation 8:

Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

Technology-neutrality relates to not being dependent on any other ("sister") specifications, and platform-neutrality, not being dependent on any specific environment, web platform, operating system.

Criterion 14 (A14) – Is the specification platform agnostic?

The evidence to justify this criterion will typically consist of checking that the implementation of the standard or specification does not rely/depend on any other standard or specification mainly focused on proprietary technologies or vendors. However, it should be considered whether the specification is dependent on other specifications, even if they are open source. Meaning that the specification requires another specification/platform to run.

EIF Recommendation 8:

Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

Technology-neutrality relates to not being dependent on any other ("sister") specifications, and platform-neutrality, not being dependent on any specific environment, web platform, operating system.

Criterion 15 (A15) – To what extent does the specification allow for partial implementations?

The evidence to justify this criterion will typically consist of checking that the specification documentation includes considerations concerning partial implementations.

EIF Recommendation 8:

Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

Partial implementations refer to the application of specifications, not in their whole, but part of the requirements or features defined in the documentation.

It can also be understood as the implementation of different profiles, which is also related to a certain set of requirements depending on the context of implementation.

Criterion 16 (A16) – Does the specification allow customisation?

The evidence to justify this criterion will typically consist of checking that the specification documentation supports partial implementations.

EIF Recommendation 8:

Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

A clear example of customizations is Core Vocabularies, which define a set of general requirements that could fit in any context and allow for the customization to fit specific business requirements in the implementation.

Criterion 17 (A17) – Does the specification allow extension?

The evidence to justify this criterion will typically consist of checking that the specification documentation allows the extension of the specification.

EIF Recommendation 8:

Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

A clear example of extension is Core Vocabularies, which are a set of general requirements fitting in different contexts that can complement each other in a sort of extensibility practice to fit specific business requirements in any implementation.

Criterion 18 (A18) – To what extent does the specification enable data portability between systems / applications supporting the implementation or evolution of European public services?

The evidence to justify this criterion will typically consist of documentation about the characteristics of the specification which proves that it positively impacts interoperability.

EIF Recommendation 9:

Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.

3.1.2.3 EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

This category includes all underlying principles from the EIF which are related to user needs. Principles included here are user-centricity (UP6), inclusion and accessibility (UP7), security and privacy (UP8), and multilingualism (UP9).

USER-CENTRICITY

Criterion 19 (A19) – To what extent does the specification allow relevant information to be reused when needed?

This criterion shall be interpreted within the context of European solutions that help to implement the Once-Only Principle (OOP) (i.e. CEF). For this reason, the evidence to justify this criterion will typically consist of implementations or mentions to the specification in these solutions.

EIF Recommendation 13:

As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.

The Once-Only Principle is related to making the operations or transactions between administrations and stakeholders more efficient. It implies avoiding the provision of certain data or information twice or more when this information is already available for public administrations.

First European Data Space, Once Only Technical System (OOTS):

<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Once+Only+Technical+System>

Additional and relevant information can be found here:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle>

INCLUSION AND ACCESSIBILITY

Criterion 20 (A20) – To what extent does the specification enable the e-accessibility?

The evidence to justify this criterion will typically consist of documentation proving that the standard or specification fosters e-accessibility. Moreover, it can be positively justified if the specification document deals with e-accessibility, at some point. The specification shall foster the creation of digital services accessible to all citizens, including people with disabilities, the elderly, and other disadvantaged groups.

An example of specification can be considered WCAG: <https://www.w3.org/TR/WCAG20/>

EIF Recommendation 14:

Ensure that all European public services are accessible to all citizens, including persons with disabilities, the elderly, and other disadvantaged groups. For digital public services, public administrations should comply with e-accessibility specifications that are widely recognised at the European or international level.

Examples of specifications addressing e-accessibility are, for instance, WAI-ARIA (<https://www.w3.org/WAI/standards-guidelines/aria/>) included within Web Content Accessibility Guidelines (WCAG) Overview (<https://www.w3.org/WAI/standards-guidelines/wcag/>).

PRIVACY

Criterion 21 (A21) – To what extent does the specification ensure the protection of personal data managed by Public Administrations?

The evidence to justify this criterion will typically consist of supporting the data management according to Data Protection directives.

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

Securing the right to the protection of personal data, by respecting the applicable legal framework for the large volumes of personal data of citizens, held and managed by Public administrations.

Criterion 22 (A22) - Does the specification provide means for restriction to access to information/data

The evidence to justify this criterion will typically consist of proving the specification gives some provisions for restriction to access to information/data. Moreover, cases where extensions for the specification or when the specification enables data processing accuracy by means of another specification should also be considered.

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

The principle of confidentiality defines that only the sender and the intended recipient(s) must be able to create the content of a message. Confidentiality have compromised if an unauthorized person is able to create a message.

Criterion 23 (A23) - Is the specification included in any initiative at European or National level covering privacy aspects?

The evidence to justify this criterion will typically consist on finding if the specification is being implemented or used as the basis for the design and implementation of any initiative (digital public service when possible).

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Securing the right to the protection of personal data, by respecting the applicable legal framework for the large volumes of personal data of citizens, held and managed by Public administrations.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

For example, the ETSI (Electronic Signatures and Infrastructures) family of specifications are part of the trust establishment of the eDelivery solution, ensuring that its implementation is salient to guarantee security and privacy.

SECURITY

DATA EXCHANGE AND PROCESSING

Criterion 24 (A24) – To what extent does the specification enable the secure exchange of data?

For the provision of evidence to justify this criterion, data exchange can be understood as publication by the administration of data for its later consumption by citizens. The specification must ensure that the data exchange is completely secure and that the data has not been altered.

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

This relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

Criterion 25 (A25) – To what extent does the specification enable the secure processing of data?

For the provision of evidence to justify this criterion, data exchange can be understood as publication by the administration of data for its later consumption by citizens. The specification must ensure that the data processing is completely secure, and that the data has not been altered.

EIF Recommendation 15:

Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

DATA AUTHENTICITY

Criterion 26 (A26) – To what extent the specification guarantees the authenticity and authentication of the agents involved in data transactions?

The evidence to justify this criterion will typically consist of documentation proving the specification guarantees the authenticity and authentication of the agents involved in data transactions. Moreover, cases where extensions for the specification or when the specification enables data processing accuracy by means of another specification should also be considered.

EIF Recommendation 15:

Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Authentication defines that users are who they request to be. Availability defines that resources are available by authorized parties; “denial of service” attacks, which are the subject matter of national news, are attacks against availability. The concerns of information security professionals are access control and Nonrepudiation. Authorization defines the power that it can have over distinguishing authorized users from unauthorized users, and levels of access in-between. Authenticity defines the constant checks that it can have to run on the system to make sure sensitive places are protected and working perfectly.”

DATA INTEGRITY

Criterion 27 (A27) – To what extent is information protected against unauthorised changes?

The evidence to justify this criterion will typically consist of documentation proving the specification features mechanisms to provide the integrity of data. Moreover, cases where extensions for the

specification or when the specification enables data processing accuracy by means of another specification should also be considered.

EIF Recommendation 15:

Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Integrity defines that information is protected against unauthorized changes that are not perceptible to authorized users; some incidents of hacking compromise the integrity of databases and multiple resources.

DATA ACCURACY

Criterion 28 (A28) – To what extent does the specification ensures and enables data processing accuracy?

The evidence to justify this criterion will typically consist of documentation proving that the specification enables data processing. Moreover, cases where extensions for the specification or when the specification enables data processing accuracy by means of another specification should also be considered.

EIF Recommendation 15:

Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

The accuracy and completeness of information systems and the data supported within the systems should be an administration concern. The information which has been inappropriately changed or destroyed (by external or employees) can impact the organization. Each organization should make controls to provide that data entered into and saved in its automated files and databases are complete and accurate and provide the accuracy of disseminated data.

ACCESS CONTROL

Criterion 29 (A29) – To what extent does the specification provide an access control mechanism?

The evidence to justify this criterion will typically consist of documentation of a mechanism provided by the specification or by an extension that guarantees access control. Moreover, the cases where specification can be used in conjunction with the one being assessed to provide access control mechanisms can also be mentioned.

EIF Recommendation 15:

Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

The principle of access control decides who must be able to access what. For example, it must be able to define that user A can view the data in a database, but cannot refresh them. User A can be allowed to create updates as well. An access-control mechanism can be installed to provide this. Access control is associated with two areas including role management and rule management. Role management applies on the user side, whereas rule management targets the resources side.

MULTILINGUALISM

Criterion 30 (A30) – To what extent could the specification be used in a multilingual context?

The evidence to justify this criterion will typically consist of documentation proving that the standard or specification fosters multilingualism in public services. Moreover, the specification can contribute to the European public service by enabling a development in different languages, for example HTML can be configured to make a website information in many languages.

EIF Recommendation 16:

Use information systems and technical architectures that cater to multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.

3.1.2.4 EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS

This category includes the criteria aiming to evaluate principles related to collaboration amongst public organisations, business, and citizens. This is related to the underlying principles of administrative simplification (UP10), preservation of information (UP11), and assessment of effectiveness and efficiency (UP12).

ADMINISTRATIVE SIMPLIFICATION

Criterion 31 (A31) – Does the specification simplify the delivery of European public services?

The evidence to justify this criterion will typically consist of documentation proving that the standard or specification streamlines administrative processes. Specifications easing and fostering digital exchanges while avoiding the non-digital exchange of information can be considered as part of the reduction of administrative burden. For instance, the implementation of HTML as part of the information exchange fosters the creation of digital services allowing digital data exchange and consumption, while avoiding the non-digital processes.

EIF Recommendation 17:

Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.

A positive answer would cover every specification easing digitalisation and administrative simplification by for example helping an Identification service access a Digital Portfolio with citizens information.

Criterion 32 (A32) – Does the specification enable digital service delivery channels?

The evidence to justify this criterion will typically consist of documentation proving that the standard or specification streamlines administrative processes. Specifications easing and fostering digital exchanges while avoiding the non-digital exchange of information can be considered as part of the reduction of administrative burden. For instance, the implementation of HTML as part of the information exchange fosters the creation of digital services allowing digital data exchange and consumption, while avoiding the non-digital processes.

EIF Recommendation 17:

Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.

A positive answer would cover that a specification eases or provides better means of delivering public services as a good asset for digitalisation and administrative simplification. For instance, a specification directly related to API performance easing and improving the delivery of a Digital Public Service through an API.

PRESERVATION OF INFORMATION**Criterion 33 (A33) – To what extent does the specification enable the long-term preservation of data/information/knowledge (electronic records included)?**

In order to provide evidence to justify this criterion, the documentation of the specification must emphasise the long-term preservation of information and ensure its preservation.

EIF Recommendation 18:

Formulate a long-term preservation policy for information related to European public services and especially for information that is exchanged across borders.

Relates to the capacity of the specification to contribute to the long-term preservation of information.

ASSESSMENT OF EFFECTIVENESS AND EFFICIENCY**Criterion 34 (A34) – To what extent are there assessments of the specification's effectiveness?**

The evidence to justify this criterion will typically consist of already performed assessments of the standard or technical specification considering its effectiveness. Commonly, these can be studies that compare the effectiveness with other specifications. An example of studies or documentation could be articles in research journals (e.g., Researchgate, amongst others) or posts in specialised forums.

EIF Recommendation 19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality, and balance between costs and benefits.

Related to the degree to which the specification is effective while using it. There are indirect methods to determine that the specification is effective, for instance when a solution that has an effective performance and uses the specification to deliver the expected service.

Effectiveness: the extent to which the specifications reach the expected action according to its purpose.

Criterion 35 (A35) – To what extent are there assessments of the specification's efficiency?

The evidence to justify this criterion will typically consist of already performed assessments of the standard or technical specification considering its efficiency. Commonly, these can be studies that compare the efficiency with other specifications. An example of studies or documentation could be articles in research journals (e.g., Researchgate, amongst others) or posts in specialised forums.

EIF Recommendation 19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality, and balance between costs and benefits.

Related to the good use of time and resources not wasted unnecessarily by a specification being used. There are indirect methods to determine that the specification is efficient, for instance, a solution delivering a service with an efficient performance that uses the specification.

Efficiency: times and means needed to achieve the results using the specification.

3.1.2.5 EIF INTEROPERABILITY LAYERS

This category is aligned with the related interoperability models described in the EIF and apply to all the public services. It includes six layers: interoperability governance, integrated public service governance, legal interoperability, organisational interoperability, semantic interoperability, and technical interoperability covered by criteria A2 to A10 under the Openness category.

INTEROPERABILITY GOVERNANCE

Criterion 36 (A36) – Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?

The evidence to justify this criterion will typically consist of a narrative sustaining the possibility for the association of the standard or specification to an EIRA ABB.

EIF Recommendation 20:

Ensure holistic governance of interoperability activities across administrative levels and sectors.

The EIRA defines the required capabilities for promoting interoperability as a set of Architecture Building Blocks (ABBs). The association of specification to these ABBs means the capacity to enable Legal, Organisational, Semantic, or Technical aspects needed for the development of interoperable public services. This association can be taken from ELIS the EIRA Library of Interoperability Specifications (ELIS) but also can be established ad-hoc.

Criterion 37 (A37) – To what extent can the conformance of the specification's implementations be assessed?

The evidence to justify this criterion will typically consist of free existing testing tools or certifications that assess the standard or specification.

EIF Recommendation 21:

Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability.

Relates to the implementation of the specification being conformant with the requirements established in the text of the specification. There are different methods to ensure the conformance of an implementation: check manually if the implementation meets the requirements in the specification text (if any), use additional methods or resources provided to this purpose or use specific tools provided by the SDO developing the specification.

Criterion 38 (A38) – Is the specification recommended by an European Member State?

The evidence to justify this criterion will typically consist of a recommendation by a Member State for the implementation of the standard or specification. This recommendation can come from the administration of the Member State or from the entity in charge of standardization in that particular Member State (e.g. Difi in Norway as could be the following assessment of standard and specifications for the secure exchange of data, <https://www.digdir.no/digitalisering-og-samordning/standarder-sikker-informasjonsutveksling-pa-internett/1406>, or this catalogue of recommended specifications: <https://www.digdir.no/digitale-felleslosninger/arkivstandarder/1482>).

EIF Recommendation 23:

Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

Recommended specifications are these specifications that the Member States provide as examples for the implementation of certain digital public services or for being used when procuring these digital public services or solutions.

Criterion 39 (A39) – Is the specification selected for its use in an European Cross-border project/initiative?

The evidence to justify this criterion will typically consist of documentation of an implementation of the standard or specification in the context of a cross-border project or initiative (e.g., look through CEF Digital, CEF Building Blocks, TESTA, etc.).

EIF Recommendation 23:

Consult relevant catalogues of standards, specifications, and guidelines at national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

The European Commission set up a process for the identification and assessment of specifications for its use in the development of IT solutions and also when procuring them. Find here the commission implementing decisions that include the specifications identified by the European

Commission: https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation/ict-technical-specifications_en

Additionally, there could be other situations where a specification can be selected for European projects or initiatives out of the scope of the above-mentioned context. These specifications can be considered positively in this assessment.

Criterion 40 (A40) – Is the specification included in an open repository/catalogue of standards at national level?

The evidence to justify this criterion will typically consist of evidence of the standard or specification being included in a national catalogue of standards. It can be checked in the CAMSS List of Standards: <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards>

EIF Recommendation 23:

Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

EIF Recommendation 6:

Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

Criterion 41 (A41) – Is the specification included in an open repository/catalogue of standards at European level?

The evidence to justify this criterion will typically consist of evidence of the standard or specification being included in a supra-national catalogue of standards. The specification can be searched in European platforms, for example in CEN, CENELEC or ETSI.

EIF Recommendation 23:

Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

EIF Recommendation 6:

Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

LEGAL INTEROPERABILITY

Criterion 42 (A39) – Is the specification a European Standard?

The evidence to justify this criterion will typically consist of an assessment of the standard or specification in regards to Regulation 1025/2012.

EIF Recommendation 27:

Ensure that legislation is screened by means of ‘interoperability checks’, to identify any barriers to interoperability. When drafting legislation to establish a European public service, seek to make it consistent with relevant legislation, perform a ‘digital check’, and consider data protection requirements.

European Standards are those standards developed by certain organisations dedicated to this purpose. CEN, CENELEC, and ETSI are the principal organisations and all of them are developing their standards under the basis of meeting the requirements established within the European Standardisation Regulation. CEN-CENELEC homepage: <https://www.cencenelec.eu/>

ORGANISATIONAL INTEROPERABILITY

Criterion 43 (A43) – Does the specification facilitate the modelling of business processes?

The evidence to justify this criterion will typically consist of evidence of the standard or specification supporting a common way of modelling business processes – meaning that the specification is involved or commonly used for the design of instances of flowcharts, etc. An example of this could be UML, or ITIL, which are specifications used for the definition of different steps or moments related to the business development.

EIF Recommendation 28:

Document your business processes using commonly accepted modelling techniques and agree on how these processes should be aligned to deliver a European public service.

Criterion 44 (A44) – To what extent does the specification facilitate organisational interoperability agreements?

The evidence to justify this criterion will typically consists of checking whether the specification impacts positively in the creation or adoption of organisation interoperability agreements.

EIF Recommendation 29:

Clarify and formalise your organisational relationships for establishing and operating European public services.

Relates to specifications' capacities to help and ease the creation and formalisation of Interoperability agreements. E.g. Memorandums of Understanding (MoUs), Services Level Agreements (SLAs).

SEMANTIC INTEROPERABILITY

Criterion 45 (A45) – Does the specification encourage the creation of communities along with the sharing of their data and results in national and/or European platforms?

The evidence to justify this criterion will typically consists of checking whether the specification supports the creation of European platforms/communities to share and include the findings and results of extending and implementing digital solutions/services.

EIF Recommendation 32:

Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.

Relates to specifications that are narrowly related to the data/information being exchanged, its format, and structure. It would allow a common method/mechanism to improve its reuse and exchange removing possible limitations. An example of it could be RDF, which is used to describe information and its metadata using specific syntax and serialisation.

4. Glossary

The following table list acronyms mentioned in the current document.

Acronym	Definition
ABB	Architecture Building Blocks
CAMSS	Common Assessment Method for Standards and Specifications

CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
ETSI	European Telecommunications Standards Institute
EU	European Union
FRAND	Fair, Reasonable And Non-Discriminatory
ISA	Interoperability Solutions for public Administrations
IPR	Intellectual Property Rights
MS	Member State
NIF	National Interoperability Framework
NIFO	National Interoperability Framework Observatory
OOP	Once-Only Principle
SDO	Standards Developing Organisation

Table 1: Acronyms and Terms used in the document