Contribution ID: b8ef97d5-e115-4b0a-8710-d8b133a20a51
Date: 07/05/2024 16:20:50

# CAMSS Assessment EIF Scenario v6.0.0

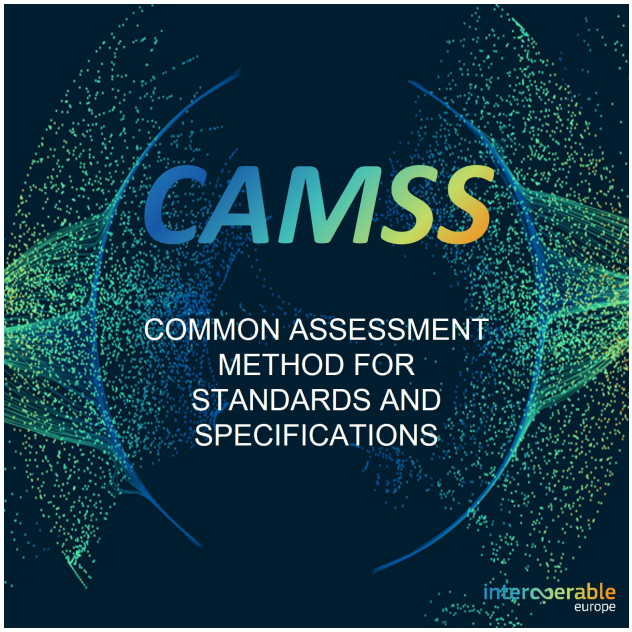
Fields marked with * are mandatory.

# CAMSS Assessment EIF Scenario v6.0.0


**Release Date:** 14/04/2023

**Scenario Version:** 6.0.0

## INTRODUCTION




## EIF Scenario

The European Interoperability Framework (EIF) provides guidance to public administrations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that existing and new legislation do not compromise interoperability efforts.

This CAMSS Scenario allows to assess 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.

## Background

CAMSS is the European guide for assessing and selecting standards and specifications for an eGovernment project, 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.
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 will be compliant with Regulation 1025/2012 on European Standardisation.
While ICT solutions have specific characteristics at the political, legal, and organisational levels; semantic and technical interoperability are based mostly on technical specifications or standards. Within the context of the elaboration of their National Interoperability Frameworks, Member States organise the assessment of technical specifications or standards, in order to establish their national recommendations. Deciding on the recommended technical specifications or standards often calls for a resource-intensive and time-consuming assessment. In order to tackle this, the Digital Europe Programme (DEP) defines an action focused on the development of a common assessment method for standards and specifications (CAMSS).

**The purpose of CAMSS is:**

- to ensure that assessments of technical ICT specifications or standards and interoperability profiles are performed according to high and consistent standards;
- to ensure that assessments will contribute significantly to the confidence in the interoperability of systems implementing these specifications and profiles;
- to enable the reuse, in whole or in part, of such assessments;
- to continuously improve the efficiency and effectiveness of the assessment process for ICT technical specifications, standards, and interoperability profiles.

**The expected benefits of the CAMSS are:**

- Ensuring greater transparency throughout the selection of standards in the context of ICT strategies, architectures, and interoperability frameworks. This will be achieved through the establishment of a commonly agreed assessment method, assessment process, and a list of assessment attributes.
- Reducing resource and time requirements and avoiding duplication of efforts. (Partial) sharing of finalised assessments of standards and specifications.
- Allowing easier and faster assessments, and reusing the ones already performed through the creation and maintenance of a library of standards.

Your compliance level of the specification assessed depends on the scores you achieved in each section of the survey. Please see below the survey score conversion table below for guidance.

| | | | Compliance Level | | |
|---|---|---|---|---|---|
| **Section** | **Ad-hoc** | **Opportunistic** | **Essential** | **Sustainable** | **Seamless** |
| **Principles setting the context for EU Actions on Interoperability** | 20 | 40 | 60 | 80 | 100 |
| **EIF Core Interoperability Principles** | 0 to 340 | 341 to 680 | 681 to 1020 | 1021 to 1360 | 1361 to 1700 |
| **EIF Principles Related to generic user needs and expectations** | 0 to 240 | 241 to 480 | 481 to 720 | 721 to 960 | 961 to 1200 |

| | | | | | |
|---|---|---|---|---|---|
| **EIF Foundation principles for cooperation among public administrations** | 0 to 100 | 101 to 200 | 201 to 300 | 301 to 400 | 401 to 500 |
| **EIF Interoperability Layers** | 0 to 200 | 201 to 400 | 401 to 600 | 601 to 800 | 801 to 1000 |

The following table shows the 'compliance levels' that a specification can reach depending on the assessment score.

| Compliance Level | Description |
|---|---|
| **Ad-hoc** | Poor level of conformance with the EIF - The specification does not cover the requirements and recommendations set out by the EIF in this area. |
| **Opportunistic** | Fair level of conformance with the EIF - The specification barely covers the requirements and recommendations set out by the European Interoperability Framework in this area. |
| **Essential** | Essential level of conformance with the EIF - The specification covers the basic aspects set out in the requirements and recommendations from the European Interoperability Framework. |
| **Sustainable** | Good level of conformance with the EIF scenario - The specification covers all the requirements and recommendations set out by the European Interoperability Framework in this area. |
| **Seamless** | Leading practice of conformance level with the EIF - The specification fully covers the requirements and recommendations set out by the European Interoperability Framework in this area. |

**Contact:** For any general or technical questions, please send an email to DIGIT-CAMSS@ec.europa.eu. Follow all activities related to the CAMSS on our CAMSS community page.

## USER CONSENT

***Disclaimer:***
*By no means will the Interoperability Specification assessment imply any endorsement of the EC to the assessed specification. Likewise, the use of CAMSS Assessment EIF Scenario implies that the user accepts that the EC is not liable on the assessment nor on any direct or indirect consequence/decision of such assesment.*

The CAMSS Assessment EIF Scenario is based on EU Survey, by accepting the CAMSS Privacy Statement the user also accepts EU Survey Privacy Statement and the Terms of use.

* Please, fill in the mandatory* information to start the assessment

- [x] *I have read and agreed to the following CAMSS Privacy Statement: here
- [ ] I agree to be contacted for evaluation purposes, namely to share my feedback on specific DEP solutions and actions and on the DEP programme and the European Interoperability Framework in general.



# IDENTIFICATION

## Information on the information provider

Your Last name

Your First Name

CAMSS Team

Your Position / Role

* Your Organisation

European Commision DG - DIGIT

Your Contact phone number

* Would you like to be contacted for evaluation purposes in the context of your assessment? To see how your data is handled, please check again the Privacy statement here

In case you would like to be contacted, please select "yes" and provide your email.

- ( ) Yes
- (•) No

* Where did you learn about CAMSS?

- ( ) DEP Programme (DEP website, DEP social media)
- ( ) Joinup (e.g., CAMSS Collection, Joinup social media)
- (•) European Commission
- ( ) Public Administrations at national, regional or local level
- ( ) Standards Developing Organizations (SDOs)
- ( ) Other

If you answered "Other" in the previous question, please specify how:

## Information on the specification

* Specification type

**Specification**: Set of agreed, descriptive, and normative statements about how a specification should be designed or made.
**Standard**: Specification that is largely adopted and possibly endorsed.
**Application Profile**: An application profile "customises one or more existing specifications potentially for a given use case or a policy domain adding an end to end narrative describing and ensuring the interoperability of its underlying specification(s)".
**Family**: A family is a collection of interrelated and/or complementary specifications, standards, or application profiles and the explanation of how they are combined, used, or both.

- (●) Specification
- ( ) Standard
- ( ) Application Profile
- ( ) Family of Specification

* Title of the specification

Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation (ETSI TS 119 432)

* Version of the specification

1.2.1

* Description of the specification

ETSI TS 119 432 specifies protocols and interfaces for components providing specific functionalities as part of a process for remote digital signatures creation and construction of AdES formats. It aims at supporting electronic signatures and electronic seals, including qualified electronic signatures and qualified electronic seals according to the current EU regulation.

* URL from where the specification is distributed

https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* Name and website of the standard developing/setting organisation (SDO/SSO) of the specification

- ( ) W3C (https://www.w3.org)
- ( ) OASIS (https://www.oasis-open.org/)
- ( ) IEEE (https://standards.ieee.org/)
- (●) ETSI (https://www.etsi.org/)
- ( ) GS1 (https://www.gs1.fr/)
- ( ) openEHR (https://www.openehr.org/)

- ○ IETF (https://www.ietf.org/)
- ○ Other (SDO/SSO)

Contact information/contact person of the SDO
a) for the organisation
b) for the specification submitted

## Information on the assessment of the specification

Reason for the submission, the need and intended use for the specification.

If any other evaluation of this specification is known, e.g. by Member States or European Commission projects, provide a link to this evaluation.

## Considerations

Is the functional area of application for the formal specification addressing interoperability and eGovernment?

- ◉ YES
- ○ NO

Additional Information

Standards for digital signatures have generally been developed for a long time. Given developments in distributed systems, cloud computing, mobile equipment and related technologies, solutions have been emerging in the last few years where the process of digital signature creation and construction of AdES format is done in a distributed way with different steps of the process carried out by different systems /services that may be controlled by different actors. Considering these circumstances, this specification offers a EU-aligned standard for the digital signature creation.

# EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

This category is related to the first underlying principle (UP) 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.

***Please note that some of the questions have a prefilled answer depending on the SDO. To ensure it, please see that these questions include a help message that remarks it.***

## Subsidiarity and Proportionality

---

* **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?**

**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

- ○ Not Answered
- ○ Not Applicable
- ◉ The specification has not been included within the catalogue of any Member State.
- ○ The specification has been included within the catalogue of a Member State with a lower performance than stated in the Digital Public Administration Factsheets from the NIFO.
- ○ The specification has been included within the catalogue of a Member State with a middle-lower performance than stated in the Digital Public Administration Factsheets from the NIFO.
- ○ The specification has been included within the catalogue of a Member State with a middle-upper performance than stated in the Digital Public Administration Factsheets from the NIFO.
- ○ The specification has been included within the catalogue of a Member State with a higher performance than stated in the Digital Public Administration Factsheets from the NIFO.

* Justification

ETSI TS 119 432 is not included in any national catalogue of recommended specifications whose Member State NIF has a high performance on interoperability according to NIFO factsheets.

CAMSS List of Standards:
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards

2023 NIFO factsheets:
https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-publicadministration-factsheets-2023

# EIF CORE INTEROPERABILITY PRINCIPLES

In this category, elements related to the core interoperability principles (UP) are encompassed, which are: openness (UP 2), transparency (UP3), reusability (UP4), technological neutrality and data portability (UP5).

## Openness

* **A2 - Does the specification facilitate the publication of data on the web?**

**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.

- ( ) Not Answered
- ( ) Not Applicable
- ( ) The specification does not support the publication of data on the web.
- ( ) The specification supports the publication of data on the web but under a non-open license.
- ( ) The specification supports the publication of data on the web with an open license, but in an unstructured format.
- ( ) The specification supports publication of data on the web with an open license and in a structured, machine-readable format.
- (•) In addition to the previous question, the specification does not require proprietary software for the processing of its related data.
- ( ) In addition to the previous question, the specification is or incorporates open standards (e.g. W3C).

* Justification

ETSI TS 119 432 specifies the protocols semantics for requesting the digital signatures creation to a remote server and for receiving the related response. For the semantics mentioned, the specification has two bindings, each one in a different format (XML and JSON). Both XML and JSON can be easily parsed and manipulated by programming languages and tools, making them machine-readable and ideal for exchanging data between different systems and platforms.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* **A3 - To what extent do stakeholders have the opportunity to contribute to the development 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.

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

- ( ) Not Answered
- ( ) Not Applicable
- ( ) There is no information on the working group of the specification.

- (●) The working group is open to participation by any stakeholder but requires registration, fees, and membership approval.
- ( ) The working group is open to participation by any stakeholder but requires fees and membership approval.
- ( ) The working group is open to participation following a registration process.
- ( ) The working group is open to all without specific fees, registration, or other conditions.

* Justification

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI). There are two paths to get involved in ETSI's Industry Specification Groups (ISG): as an ETSI member, or as a direct participant. The participation in the technical group is reserved to ETSI members, who require registration, fees, and membership approval. Organisations who are not members of ETSI may still participate in the ISG, attend meetings, subscribe to the e-mail lists and help build the specifications by making technical contributions. They do not have voting rights and must pay a participation fee per person per meeting day to attend ISG meetings.

ETSI Technical Committee ESI: https://www.etsi.org/committee/esi

*** A4 - To what extent is a public review part of the release lifecycle?**

**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.

- ( ) Not Answered
- ( ) Not Applicable
- ( ) Specification releases do not foresee public reviews.
- ( ) Public review is applied to certain releases depending on the involved changes.
- ( ) All major releases foresee a public review.
- ( ) All major and minor releases foresee a public review but, during which, collected feedback is not publicly visible.
- (●) All major and minor releases foresee a public review during which collected feedback is publicly visible.

* Justification

TC ESI has a policy of openly publishing intermediate material (as soon as consensus is reached) to enhance feedback. The working group publishes an activity report anually where they indicate what they have done and future plans. Furthermore, there is a further overview of the committee’s activities – including all published standards and reports available.

TC ESI Activity Report 2022 https://www.etsi.org/committee-activity/activity-report-esi

Electronic Signatures and Trust Infrastructures Activities: https://portal.etsi.org/TB-SiteMap/esi/esi-activities

*** A5 - To what extent do restrictions and royalties apply to the specification's use?**

**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)

- ○ Not Answered
- ○ Not Applicable
- ○ The specification has no public definition of its Intellectual Property Right (IPR) policy or licence.
- ○ Use of the specification is restricted and requires the payment of royalty fees.
- ○ Use of the specification is royalty-free but imposes an Intellectual Property Right (IPR) policy or licence that goes against Fair, Reasonable and Non-Discriminatory (F/RAND) principles.
- ◉ Use of the specification is royalty-free and its Intellectual Property Right (IPR) policy or licence is aligned with Fair, Reasonable and Non-Discriminatory (F/RAND) principles.

* Justification

ETSI (European Telecommunications Standards Institute) typically follows a policy of providing fair, reasonable and non-discriminatory (FRAND) licensing for its standards. This means that ETSI aims to make its standards accessible to the broadest possible audience by offering licenses on fair and reasonable terms.

ETSI IPR Policy: https://www.etsi.org/intellectual-property-rights

Justification:
The ETSI IPR Policy which is part of the ETSI directives seeks to reduce the risk that our standards-making efforts might be wasted if SEPs are unavailable under Fair, Reasonable and Non-Discriminatory (FRAND) terms and conditions.
The main objective of the ETSI IPR Policy is to balance the rights and interests of IPR holders to be fairly and adequately rewarded for the use of their SEPs in the implementation of ETSI standards and the need for implementers to get access to the technology defined in ETSI standards under FRAND terms and conditions.

ETSI's intellectual property rights policy:
https://www.etsi.org/intellectual-property-rights

Additional information

In case you need to add further justification.

* **A6 - To what extent is the specification sufficiently mature for its use in the development of digital solutions/services?**

**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.)

- ○ Not Answered
- ○ Not Applicable
- ○ The specification has no published releases and no publicly accessible information on its development state.
- ○ The specification is under development without published releases.
- ○ The specification is under development with published preview releases.

- ○ The specification has published major releases but without public documentation on its supporting processes (e.g. change management and release management).
- ◉ The specification, in addition to having major releases available, has published documentation on its supporting processes (e.g. change management and release management).

* Justification

ETSI TS 119 432 is currently in its 1.2.1 version thus, major releases have been published. In addition, public documentation inside the specification has been published about its supporting process, specifically related to change history and issues regarding every version. Annex D of the specification is dedicated to change history while any release related to ETSI TS 119 432 has been published in the TC ESI domain.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

ETSI Technical Committee ESI: https://www.etsi.org/committee/esi

* **A7 - To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?**

**EIF Recommendation 4:** Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support, and innovation.

Relates to how the specification is supported by the market, taking as a reference whether or not the specifications are widely used or implemented. There is an exception, and it is when the specification is used to implement innovative solutions, then, the specification should not be considered as failing to meet the requirements of the criterion.

- ○ Not Answered
- ○ Not Applicable
- ○ There is no information about the specification's market uptake.
- ○ The specification has known implementations but not enough to indicate market acceptance.
- ○ The specification has widespread use indicating market acceptance.
- ○ The specification has widespread use and relevant independent reports proving its market acceptance.
- ◉ The specification does not have market acceptance because it is directly used to create innovative solutions.

* Justification

ETSI TS 119 432 was created as a support for electronic signatures and electronic seals according to the trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation). The eIDAS Regulation provides for the interoperability of national eID schemes among EU member states. This requires the development of a technology-neutral framework that does not favour any particular technical solution for eID implementation.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

eIDAS Regulation: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

* **A8 - To what extent has the specification support from at least one community?**

**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.

Related to whether or not communities exist around the specification at any level legal, organisational, semantic, or technical contributions to its enhancement and development.

- ○ Not Answered
- ○ Not Applicable
- ○ There is no community linked to the specification.
- ○ Specification support is available but as part of a closed community requiring registration and possibly fees.
- ○ There is no specific community to support the specification but there are public channels for the exchange of help and knowledge among its users.
- ○ There is a community providing public support linked to the specification but in a best-effort manner.
- ◉ There is a community tasked to provide public support linked to the specification and manage its maintenance.

* Justification

ETSI TS 119 432 is developed and maintained by the European Telecommunications Standards Institute (ETSI). Its development involves contributions from industry experts and collaboration within ETSI working groups, particularly ETSI Technical Committee ESI. This standardisation body covers the format of digital signatures, as well as procedures and policies for creation and validation. ETSI takes into account the impact of users as they improve their standards and their relevancy.

ETSI Technical Committee ESI: https://www.etsi.org/committee/esi

## Transparency

* **A9 - To what extent does the specification enable the visibility of administrative procedures, rules data, and services?**

**EIF Recommendation 5:** Ensure internal visibility and provide external interfaces for European public services.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification hinders visibility.
- ○ The specification neither promotes nor hinders visibility.
- ○ The specification can contribute and promote the visibility of administrations, but it is not its main purpose.
- ○ The specification can enable the visibility of administrations if combined with other specifications.
- ◉ The specification actively promotes and supports visibility.

* Justification

Protocols for remote digital signature creation can indeed enable visibility into administrative procedures, rules data, and services, but the extent of this visibility depends on the specific protocol and its implementation. Remote digital signature protocols often involve interactions between a client (the party requesting the signature) and a server (where the signature is generated). The protocol may include mechanisms for users, verifying the integrity of documents, and ensuring the security of the signature generation process.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* **A10 - To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification hinders comprehensibility.
- ○ The specification neither promotes nor hinders comprehensibility.
- ○ The specification can contribute and promote the comprehensibility of administrations, but it is not its main purpose.
- ○ The specification can scope the comprehensibility of administrations if combined with other specifications.
- ◉ The specification actively promotes and supports comprehensibility.

* Justification

The protocol for remote digital signature creation aims to scope comprehensibly administrative procedures, rules data, and services as it can help define the services required for remote digital signature creation, such as signature generation, key management, and timestamping. In addition, it may define the administrative procedures involved in remote digital signature creation, such as user authentication, authorization, and key management.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* **A11 - To what extent does the specification enable the exposure of interfaces to access the public administration's services?**

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.*

- ○ Not Answered
- ○ Not Applicable
- ○ The specification prevents the exposure of such interfaces.
- ○ The specification neither promotes nor hinders the exposure of such interfaces.
- ○ The specification can contribute to the exposure of interfaces, but it is not its main purpose.

- The specification can enable the exposure of interfaces if combined with other specifications.
- (selected) The specification enables exposure of such interfaces.

* Justification

The specification actively promotes and supports exposure of interfaces to access the public administration's services as it is completely aligned with eIDAS, a project that allows the European recognition of electronic identities, specifically, the acceptance of the electronic IDs in services of other European administrations as well as the identification of European citizens outside their home country. In addition, it also facilitates the connection of interfaces for trust service providers and to access digital services through authentication and authorisation mechanisms.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

eIDAS Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

## Reusability

* **A12 - To what extent is the specification usable beyond the business-specific domain, allowing its usage across business domains?**

**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.

- Not Answered
- Not Applicable
- The specification is tied to a specific domain and is restricted from being implemented or used in other domains.
- The specification is associated with a specific domain but its implementation and/or use in other domains is difficult.
- The specification is associated with a specific domain but could be partially implemented and/or used in other domains.
- The specification is associated with a specific domain but could be implemented and/or used 'as-is' to other domains.
- (selected) The specification is domain-agnostic, designed to be implemented and/or used in any domain.

* Justification

The protocol for remote digital signature creation can be domain-agnostic as it can be applicable across various industries and use cases. Standards for digital signatures have generally been developed for a long time considering solutions tailored to the characteristics of devices, therefore they could be implemented and /or used in any domain.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Technological Neutrality and Data Portability

*** A13 - Is the specification technology agnostic?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

The specification itself is designed to be technology-agnostic as it aims to represent and exchange context information about entities in a machine-readable way, without being tied to specific implementation technologies or platforms.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

*** A14 - Is the specification platform agnostic?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

This specification has two bindings regarding the protocol components, each one in a different format (XML and JSON). XML is a markup language that uses tags to structure and describe data. It is widely used in various applications and industries for representing structured data. JSON, on the other hand, is a lightweight data interchange format that uses key-value pairs to represent data. It is commonly used in web development for transmitting data between a server and a web application.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

*** A15 - To what extent does the specification allow for 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.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification is only meant to be used as a whole.
- ○ The specification could be partially implemented but does not make specific provisions towards this.
- ◉ The specification could be partially implemented but includes only guidelines towards this rather than sets of requirements.
- ○ The specification explicitly foresees sets of requirements that can be implemented incrementally.
- ○ The specification explicitly foresees sets of requirements that can be implemented incrementally or separately.

* Justification

ETSI TS 119 432 specifies generally applicable policy and security requirements for Trust Service Providers (TSPs) implementing a service component operating a remote signature creation device. While it does not explicitly address partial implementations, the document defines two different implementations for remote digital signature creation: A JSON-based Implementation based on the Cloud Signature Consortium specification and an XML-based Implementation that follows the OASIS DSS-X standard2. Overall, the specification allows partial implementations but there are essential componenets that ensure alignment with security requirements.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

Architectures and protocols for remote signature applications: https://cloudsignatureconsortium.org/wp-content/uploads/2020/01/CSC_API_V1_1.0.4.0.pdf

Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0: https://docs.oasis-open.org/dss-x/dss-core/v2.0/dss-core-v2.0.pdf

*** A16 - Does the specification allow customisation?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

ETSI TS 119 432 allows customisations to a certain extent. It does allow customisations in the sense that it can be implemented within different IT infrastructures, which allows the specification to be adapted based on integration with existing systems. It is also extensible to the parameters of the protocols it defines.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* **A17 - Does the specification allow extension?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

Although ETSI TS 119 432 does not explicitly allow extensions, it is safe to assume that extensions are possible as new features such as additional cryptographic protocols can always be added. Even if it does not detail the process regarding the addition of extensions, it is something that can be inferred from the specification itself.
ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* **A18 - To what extent does the specification enable data portability between systems/applications supporting the implementation or evolution of European public services?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification prevents or does not support data portability.

- The specification neither addresses data portability nor prevents it.
- The specification addresses data portability but without specific provisions to enable it.
- (●) The specification introduces certain aspects that can contribute to enabling data portability.
- The specification explicitly addresses and enables data portability.

* Justification

> The protocol for remote digital signature creation itself may not directly address data portability, as its primary focus is on defining the technical procedures for creating digital signatures remotely. However, data portability can still be facilitated as part of the broader digital signature workflow that involves the use of such a protocol. Implementations of the protocol aims for interoperability, allowing digital signatures created using one system to be verified by another. This interoperability helps ensure that signed documents remain portable across different platforms and environments.
>
> ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## 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

* **A19 - To what extent does the specification allow relevant information to be reused when needed?**

**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

- Not Answered
- (●) Not Applicable
- Information needs to be provided whenever this is needed.
- There is limited reuse of provided information.
- Provided information is reused, but this is not consistently done.
- Provided information is reused, but not in all scenarios.
- Information is provided once-only and reused as needed.

* Justification

ETSI TS 119 432 does not mention any specific action to support the reuse of relevant information when needed. Therefore, this criterion is considered not applicable to this specification.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Inclusion and Accessibility

* **A20 - To what extent does the specification enable the e-accessibility?**

**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/).

- ○ Not Answered
- ○ Not Applicable
- ○ The specification prevents or does not support e-accessibility.
- ○ The specification neither addresses e-accessibility nor prevents it.
- ◉ The specification can contribute and promote e-accessibility, but it is not its main purpose.
- ○ The specification can enable e-accessibility if combined with other specifications.
- ○ The specification explicitly addresses and enables e-accessibility.

* Justification

ETSI TS 119 432 is not related to enabling e-accessibility. Therefore, this criterion is considered not applicable to this specification.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Privacy

* **A21 - To what extent does the specification ensure the protection of personal data managed by Public Administrations?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification hinders the protection of personal data.
- ○ The specification does not address the protection of personal data but neither prevents it.
- ○ The specification includes certain data protection considerations but without being exhaustive.
- ○ The specification explicitly addresses data protection but without referring to relevant regulations.
- ◉ The specification explicitly addresses data protection and its alignment to relevant regulations.

* Justification

The protocol aims at supporting electronic signatures and electronic seals, including qualified electronic signatures and qualified electronic seals according to the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation).

Regulation (EU) No 910/2014: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0910

Directive 1999/93/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

*** A22 - Does the specification provide means for restriction of access to information/data?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification prevents or does not support the implementation of confidentiality mechanisms/features.
- ○ The specification neither addresses confidentiality nor prevents it.
- ○ The specification addresses confidentiality but without specific provisions to enable it.
- ◉ The specification introduces certain aspects that can contribute to enabling confidentiality.
- ○ The specification explicitly addresses and enables the implementation of features to guarantee confidentiality.

* Justification

Section 5 of the specification about confidentiality, security and integrity expresses that the SCASC shall guarantee the integrity and confidentiality of the received information. For instance, in remote signing services with SCAL1 (Section 5.3), the signing key's confidentiality and integrity are ensured by the SCDev that can be activated by the SSASC. Such activation can remain for a given period and/or for a given number of signatures.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* **A23 - Is the specification included in any initiative at European or National level covering privacy aspects?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ Yes, but at national or regional level.
- ◉ Yes, at European level.

* Justification

ETSI TS 119 432 was part of ENISA's 2018 Trust Services Forum. The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow.

ENISA ETSI ESI and Signature Validation Services: https://www.enisa.europa.eu/events/tsforum-caday-2018/presentations/C03_Rock.pdf

## Security

### Data processing and exchange

* **A24 - To what extent does the specification enable the secure exchange of data?**

**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.

- Not Answered
- Not Applicable
- The specification prevents or does not support the secure and trustworthy exchange of data.
- The specification introduces certain aspects that can contribute to enabling the secure exchange of data.
- The specification addresses data security and trustworthy data exchange but does not foresee specific provisions to enable them.
- The specification addresses data security and trustworthy data exchange but specific provisions to enable them are limited.
- (●) The specification explicitly addresses and enables the secure and trustworthy exchange of data.

* Justification

The main purpose of ETSI TS 119 432 is to provide the means for a secure and trustworthy exchange of data through digital signatures. Digital Signature Values (DSV) are created using a signing key held within a cryptographic security module named Signature Creation Device (SCDev) operated by a Signature Creation Service Provider (SCSP).

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

*** A25 - To what extent does the specification enable the secure processing of data?**

**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.

- Not Answered
- Not Applicable
- The specification prevents or does not support the secure and trustworthy processing of data.
- The specification introduces certain aspects that can contribute to enabling the secure processing of data.
- The specification addresses data security and trustworthy data processing but does not foresee specific provisions to enable them.
- The specification addresses data security and trustworthy data processing but specific provisions to enable them are limited.
- (●) The specification explicitly addresses and enables the secure and trustworthy processing of data.

* Justification

ETSI TS 119 432 provides a variety of processing models for the correct implementation of the protocol. For instance, the purpose of the signature creation process is to take the Data To Be Signed Representation (DTBSR) and create a digital signature value under the control of the signer. The creation of the digital signature value is managed by an Server Signing Application Service Component (SSASC) that uses a signing key, held within a cryptographic security module (SCDev), that the signers can activate by means of a secure authorisation and activation process.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

**Data authenticity**

* **A26 - To what extent the specification guarantees the authenticity and authentication of the roles agents involved in the data transactions?**

**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.”

- ○ Not Answered
- ○ Not Applicable
- ○ The specification prevents or does not support the implementation of authentication features.
- ○ The specification neither addresses authenticity nor prevents it.
- ○ The specification addresses the implementation of authenticity features but without specific provisions to enable it.
- ○ The specification introduces certain aspects that can contribute to enabling authenticity features.
- ◉ The specification explicitly addresses and enables the implementation of authenticity features.

* Justification

Section 7.7 of ETSI TS 119 432 is dedicated to the component for the client application authentication. This component shall contain information to authenticate the client application to access to the SCASC or the SSASC. However, the way a client application authenticates to the SCASC or SSASC is out of scope of the protocol.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

**Data integrity**

* **A27 - To what extent information is protected against unauthorised changes?**

**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.

- Not Answered
- Not Applicable
- The specification prevents or does not support the implementation of data integrity mechanisms /features.
- The specification neither addresses data integrity nor prevents it.
- The specification addresses data integrity but without specific provisions to enable it.
- The specification introduces certain aspects that can contribute to enabling data integrity.
- The specification explicitly addresses and enables the implementation of features to guarantee data integrity.

* Justification

The specification explicitly addresses and enables data integrity with the implementation of digital signatures. A digital signature is data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. As a result, the value of a digital signature is the result of the cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

**Data accuracy**

*** A28 - To what extent does the specification ensure and enable data processing accuracy?**

**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.

- Not Answered
- Not Applicable
- The specification prevents or does not support the implementation of data accuracy mechanisms/features.
- The specification neither addresses data accuracy nor prevents it.
- The specification addresses data accuracy but without specific provisions to enable it.
- The specification introduces certain aspects that can contribute to enabling data accuracy.
- The specification explicitly addresses and enables the implementation of features to guarantee data accuracy.

* Justification

ETSI TS 119 432 addresses and enables the implementation of features to guarantee data accuracy. For instance, it guarantees data accuracy by providing a interface capable of warning if it cannot accurately present all parts of the SD according to the data content type when the SCASC presents the document to the signer.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

**Access Control**

* **A29 - To what extent does the specification provide an access control mechanism?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification does not provide access control mechanisms.
- ○ The specification neither addresses nor prevents access control mechanisms.
- ○ The specification addresses access control mechanisms but without specific provisions to enable them.
- ○ The specification introduces certain aspects that can contribute to enabling access control mechanisms.
- ◉ The specification explicitly foresees a set of requirements for the enabling of access control mechanisms.

* Justification

ETSI TS 119 432 foresees enabling access control mechanisms. Digital signatures can work as access control mechanisms to private data. The authorised signer's use of its key for signing requires users to provide multiple proofs of their claimed identity before being granted access to the needed set of resources. Nevertheless, the way in which the user identity verification process is carried out by the service provider or any suggestion concerning the usage of multi-factor authentication mechanisms is out of the scope of the present document.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Multilingualism

* **A30 - To what extent could the specification be used in a multilingual context?**

**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.

- Not Answered
- Not Applicable
- The specification cannot be used in a multilingual context.
- The specification could be used in a multilingual context but has no specific provisions to facilitate this.
- The specification foresees limited support for multilingualism.
- The specification foresees support for multilingualism but this is not complete.
- (●) The specification is designed to fully support multilingualism.

* Justification

Section 7.9 of the specification focuses on the component for language selection. This component shall be used to request a preferred language of the response and shall be specified according to IETF RFC 5646. The service should provide language-specific responses using the requested language. In the case the requested language is not supported then no error shall be raised and the responses shall be produced in the SCS default language.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

IETF RFC 5646: https://datatracker.ietf.org/doc/rfc5646/

## 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

* **A31 - Does the specification simplify the delivery of European public services?**

**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 administratice simplification by for example helping an Identification service access a Digital Portfolo with citizens information.

- Not Answered
- Not Applicable
- NO
- (●) YES

* Justification

ETSI TS 119 432 can simplify the delivery of European public services as the EU has made various efforts related to the implementation of digital signatures across all Europe. For instance, eSignature is a set of free standards, tools and services that help public administrations and businesses accelerate the creation and verification of electronic signatures that are legally valid in all European Member States.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

eSignature: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature

* **A32 - Does the specification enable digital service delivery channels?**

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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

ETSI TS 119 432 enables digital service delivery channels as it can improve the delivery of information including data and content across multiple platforms and devices like web or mobile. Thanks to an standardised method of creating digital signatures, transactional services such as submitting forms for processing and receiving benefits can be easier to carry out.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Preservation of Information

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

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.

- ○ Not Answered
- ◉ Not Applicable
- ○ The specification prevents or does not support long-term preservation.
- ○ The specification neither addresses the long-term preservation nor prevents it.
- ○

The specification addresses the long-term preservation of electronic resources (information, data, etc) in a limited manner.

- The specification addresses long-term preservation of electronic resources (information, data, etc), but not in a complete manner.
- The specification explicitly addresses and enables long-term preservation.

* Justification

ETSI TS 119 432 is not related to enabling the long-term preservation of data (electronic records included). Therefore, this criterion is considered not applicable to this specification

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Assessment of Effectiveness and Efficiency

* **A34 - To what extent are there assessments of the specification's effectiveness?**

**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.*

- Not Answered
- Not Applicable
- There are no such assessments.
- There are such assessments that indirectly address the specification.
- There are such assessments evaluating digital solutions' effectiveness that involve the specification.
- There are such assessments addressing the specification and its effectiveness together with other specifications.
- (●) There are such assessments directly addressing the specification.

* Justification

The effectiveness of ETSI TS 119 432 is often evaluated through various means, including practical implementations and pilot projects. For instance, a 2020-paper about learned lessons from implementing an android client for the Cloud Signature Consortium API highlights the ETSI protocol as the one to be respected for communication between SCA/SIC and SSA/SAM.

Learned Lessons from Implementing an Android Client for the Cloud Signature Consortium API: https://link.springer.com/chapter/10.1007/978-3-030-41025-4_15

* **A35 - To what extent are there assessments of the specification's efficiency?**

**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.

- ( ) Not Answered
- ( ) Not Applicable
- ( ) There are no such assessments.
- ( ) There are such assessments that indirectly address the specification.
- ( ) There are assessments evaluating digital solutions' efficiency that involve the specification.
- ( ) There are such assessments addressing the specification and its efficiency together with other specifications.
- (•) There are such assessments directly addressing the specification.

* Justification

Assessments of the efficiency of ETSI TS 119 432 primarily involves evaluating the performance, scalability, and practicality of implementations. A 2022-paper about digital signatures offers an overview on the regulation and standards perspective and present a comparison of several implementations of long-term preservation solutions that are available on the market. ETSI TS 119 432 is mentioned as one of the main components that sustain recent digitisation efforts made by public and private institutions, expressing its efficiency.

Long-term Preservation of Digital Signatures: a Need-to-have or a Nice-to-have?
https://jmiltechnol.mta.ro/9/6_ARSENI,%20BUREAC%C4%82,%20TOGAN-min.pdf

## 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

* **A36 - Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

ETSI TS 119 432 is associated with EIRA ABB's in the EIRA Library of Interoperability Specifications (ELIS). More specifically, it is associated with the "Data Persistence", "Data Space", "e-Seal Creation", "e-Seal Verification and Validation", "e-Signature Creation" and "e-Signature Verification and Creation" ABBs from the "Technical-Application" View of the current European Library Of Specifications (ELIS).

EIRA Library of Interoperability Specifications (ELIS):
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis

* **A37 - To what extent can the conformance of the specification's implementations be assessed?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification does not include a definition of conformance.
- ○ The specification defines conformance but not as a set of measurable requirements.
- ○ The specification defines conformance as requirements that can be measured manually.
- ○ The specification defines conformance as requirements with resources to enable automated measurement.
- ◉ The specification is complemented by a conformance testing platform to allow testing of implementations.

* Justification

ETSI, the SDO/SSO that created and currently maintains the specification, explains that most ETSI test specifications are developed according to the well-proven methodology defined in ISO/IEC 9646. This standard, which covers the entire test development process, provides an excellent basis for the production of high-quality test frameworks and specifications.

ETSI Conformance Testing:
https://portal.etsi.org/Services/Centre-for-Testing-Interoperability/ETSI-Approach/Conformance

ISO/IEC 9646: https://www.iso.org/standard/17473.html

* **A38 - Is the specification recommended by a European Member State?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

This specification has been recommended by the Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS), a public administration under the authority of the Minister of the Economy.

ILNAS: https://ilnas.gouvernement.lu/en/service.html

*** A39 - Is the specification selected for its use in a European Cross-border project/initiative?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

The first version of ETSI TS 119 432 (“Protocols for remote digital signature creation”) was published thanks to the effort of experts from ETSI ESI, OASIS DSS-X, Cloud Signature Consortium (CSC) and go.eIDAS. This protocol may play a crucial role within the practical implementation of the forthcoming Art. 6a (4) (ec) eIDAS2, which stipulates that the European Digitial Identity Wallet (EUDIW) shall offer the ability to create qualified electronic signatures free of charge for non-professional purposes.

EUDIW: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/

*** A40 - Is the specification included in an open repository/catalogue of standards at national level?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ◉ NO
- ○ YES

* Justification

There are no Member States recommending ETSI TS 119 432 in their ICT National Catalogues.

CAMSS List of Standards:
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards

* **A41 - Is the specification included in an open repository/catalogue of standards at European level?**

**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.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ◉ YES

* Justification

Besides being part of ETSI's repository, ETSI TS 119 432 is also part of ENISA's catalogue related to digital identity. This report gives an overview of the most important standards and standardisation organisations in this area. It also provides an analysis of standards related to different means supporting digital identity. This covers means created and managed by trust services, electronic identification means and the EU Digital Identity Wallet.

ENISA Digital Identity Standards 2023: https://www.enisa.europa.eu/publications/digital-identity-standards

Justification:
ETSI is a European standards development organisation, and as such, all the specifications developed within the organisation are available and can be accessed through its website repository.

ETSI standards repository:
https://www.etsi.org/standards#page=1&search=ETSI%20TS%20319%20422&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2022-07-25&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

Additional information:

In case ypu need to add further clarifications.

## Legal Interoperability

* **A42 - Is the specification a European Standard?**

**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/

- ( ) Not Answered
- ( ) Not Applicable
- ( ) NO
- (•) YES

* Justification

ETSI is a European standards development organisation, and as such, all the specifications developed within the organisation are available and can be accessed through its website repository. Therefore, ETSI TS 119 432 is a European Standard.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Organisational Interoperability

* **A43 - Does the specification facilitate the modelling of business processes?**

**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.

- ( ) Not Answered
- ( ) Not Applicable
- ( ) NO
- (•) YES

* Justification

While ETSI TS 119 432 may not explicitly facilitate the modeling of business processes, the protocol can still play a role within the broader context of modeling business processes that involve digital signature workflows. Within a business process model, organisations can define specific steps or activities that involve digital signature creation using the protocol. This helps document and visualise the flow of documents and

information requiring signatures within the context of broader business processes.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

* **A44 - To what extent does the specification facilitate organisational 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).

- Not Answered
- Not Applicable
- The specification's definition hinders the drafting of such agreements.
- The specification makes no provisions that would facilitate the drafting of such agreements.
- The specification defines certain elements to facilitate such agreements.
- The specification defines most elements to facilitate such agreements.
- (●) The specification explicitly identifies all elements to be used in drafting such agreements.

* Justification

ETSI TS 119 432 can facilitate interoperability between organisations by providing a common framework for signature creation and verification. Standards such as XAdES (XML Advanced Electronic Signatures) and PAdES (PDF Advanced Electronic Signatures) define interoperable formats and procedures that enable signatures to be exchanged and verified across different systems and platforms. Furthermore, an open and accessible protocol encourages widespread adoption and interoperability by minimising barriers to entry for organizations wishing to implement digital signature capabilities.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Semantic Interoperability

* **A45 - Does the specification encourage the creation of communities along with the sharing of their data and results in national and/or European platforms?**

**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.

- Not Answered
- Not Applicable
- Yes, but at national or regional level.

Yes, at European platforms.

* Justification

ETSI TS 119 432 is maintained by the European Telecommunications Standards Institute (ETSI), a European Standards Organization (ESO) that is recognised as the regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services.

ETSI TS 119 432: https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.02.01_60/ts_119432v010201p.pdf

## Useful links

CAMSS Joinup Page (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss)

CAMSS Library of Assessments (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-assessments-library)

CAMSS Assessment EIF Scenario - User Guide (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/camss-assessment-eif-scenario-quick-user-guide)

## Contact

CAMSS@everis.com

# CAMSS Assessment EIF Scenario v6.0.0 - Results

# CAMSS Assessment Result

Thank you for your contribution.

The score of the specification related to the scenario under which it is being evaluated depends on the scores achieved in each section of the survey. Please see the example below for guidance.

The following table shows the 'compliance levels' that a specification can reach depending on the assessment score.

**EIF Scenario Compliance Level Conversion Table**

| Section | Compliance Level | | | | |
|---|---|---|---|---|---|
| | Ad-hoc | Opportunistic | Essential | Sustainable | Seamless |
| **Principles setting the context for EU Actions on Interoperability** | 20 | 40 | 50 | 80 | 90 |
| **EIF Core Interoperability Principles** | 0 to 340 | 341 to 681 | 681 to 1020 | 1021 to 1360 | 1361 to 1700 |
| **EIF Principles Related to generic user needs and expectations** | 0 to 240 | 241 to 480 | 481 to 720 | 721 to 960 | 961 to 1200 |

| | | | | | |
|---|---|---|---|---|---|
| **EIF Foundation principles for cooperation among public administrations** | 0 to 100 | 101 to 200 | 201 to 300 | 301 to 400 | 401 to 500 |
| **EIF Interoperability Layers** | 0 to 200 | 201 to 400 | 401 to 600 | 601 to 800 | 801 to 1000 |

The table below expresses the range of the score per section. When used in combination with the table above, the total score can be interpreted. See the example below for guidance.

**Section Compliance Conversion Table**

| Compliance Level | Description |
|---|---|
| **Ad-hoc** | Poor level of conformance with the EIF - The specification does not cover the requirements and recommendations set out by the EIF in this area. |
| **Opportunistic** | Fair level of conformance with the EIF - The specification barely covers the requirements and recommendations set out by the European Interoperability Framework in this area. |
| **Essential** | Essential level of conformance with the EIF - The specification covers the basic aspects set out in the requirement and recommendations from the European Interoperability Framework. |
| **Sustainable** | Good level of conformance with the EIF scenario - The specification covers all the requirements and recommendations set out by the European Interoperability Framework in this area. |
| **Seamless** | Leading practice of conformance level with the EIF - The specification fully covers the requirements and recommendations set out by the European Interoperability Framework in this area. |

**Example – How to find the final Compliance Level**

Using the score reached after the initial assessment, the interpretation can be made as follows.

1. In the summary table, observe the score for each section, e.g. EIF Core Interoperability Principles has 1800 points.

2. In the middle table – the Section Compliance Conversion Table – see that this number correlates to a column. In our example, the 1800 points of Core Interoperability Principles fall in the EIF Core Interoperability Principles row, and ‘1441 to 1800’ point range, placing it in the column 'Compliance **Seamless**'.

3. Next, in the top table – the EIF Scenario Compliance Level Conversion Table – we see Compliance Level "**Seamless**", and from its description that the specification for the EIF Core Interoperability Principles 'fully covers the requirements and recommendations set out by the European Interoperability Framework in this area.'.

For additional calculation of the assessment strength, please follow the instruction provided in the User Guide, found here.

## Summary

**Your Score** 4140

**Maximum Score** 4502

| Section | Score for this Section | |
|---|---|---|
| EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY | 20/100 |  |
| EIF CORE INTEROPERABILITY PRINCIPLES | 1560 /1701 |  |
| EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS | 1140 /1200 |  |
| EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS | 500 /500 |  |
| EIF INTEROPERABILITY LAYERS | 920 /1001 |  |

## Scores by Question

## EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

Score for this Section: 20/100

**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?**

| | | |
|---|---|---|
| Your answer | ✖ The specification has not been included within the catalogue of any Member State. | 20 out of 100 points |

## EIF CORE INTEROPERABILITY PRINCIPLES

Score for this Section: 1560/1701

**A2 - Does the specification facilitate the publication of data on the web?**

| | | |
|---|---|---|
| Your answer | ✔ In addition to the previous question, the specification does not require proprietary software for the processing of its related data. | 80 out of 100 points |

**A3 - To what extent do stakeholders have the opportunity to contribute to the development of the specification?**

| | | |
|---|---|---|
| Your answer | ✔ The working group is open to participation by any stakeholder but requires registration, fees, and membership approval. | 40 out of 100 points |

**A4 - To what extent is a public review part of the release lifecycle?**

| | | |
|---|---|---|
| Your answer | ✔ All major and minor releases foresee a public review during which collected feedback is publicly visible. | 100 out of 100 points |

**A5 - To what extent do restrictions and royalties apply to the specification's use?**

| | | |
|---|---|---|
| Your answer | ✔ Use of the specification is royalty-free and its Intellectual Property Right (IPR) policy or licence is aligned with Fair, Reasonable and Non-Discriminatory (F/RAND) principles. | 100 out of 100 points |

**Additional information**

| | | |
|---|---|---|
| Your answer | | 0 out of 1 points |

**A6 - To what extent is the specification sufficiently mature for its use in the development of digital solutions/services?**

| | | |
|---|---|---|
| Your answer | ✔ The specification, in addition to having major releases available, has published documentation on its supporting processes (e.g. change management and release management). | 100 out of 100 points |

**A7 - To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?**

| | | |
|---|---|---|
| Your answer | ✔ The specification does not have market acceptance because it is directly used to create innovative solutions. | 100 out of 100 points |

**A8 - To what extent has the specification support from at least one community?**

| | | |
|---|---|---|
| Your answer | ✔ There is a community tasked to provide public support linked to the specification and manage its maintenance. | 100 out of 100 points |

**A9 - To what extent does the specification enable the visibility of administrative procedures, rules data, and services?**

| | | |
|---|---|---|
| Your answer | ✔ The specification actively promotes and supports visibility. | 100 out of 100 points |

**A10 - To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?**

| | | |
|---|---|---|
| Your answer | ✔ The specification actively promotes and supports comprehensibility. | 100 out of 100 points |

**A11 - To what extent does the specification enable the exposure of interfaces to access the public administration's services?**

| | | |
|---|---|---|
| Your answer | ✔ The specification enables exposure of such interfaces. | 100 out of 100 points |

**A12 - To what extent is the specification usable beyond the business-specific domain, allowing its usage across business domains?**

| | | |
|---|---|---|
| Your answer | ✔ The specification is domain-agnostic, designed to be implemented and/or used in any domain. | 100 out of 100 points |

**A13 - Is the specification technology agnostic?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A14 - Is the specification platform agnostic?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A15 - To what extent does the specification allow for partial implementations?**

| | | |
|---|---|---|
| Your answer | ✔ The specification could be partially implemented but includes only guidelines towards this rather than sets of requirements. | 60 out of 100 points |

**A16 - Does the specification allow customisation?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A17 - Does the specification allow extension?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A18 - To what extent does the specification enable data portability between systems/applications supporting the implementation or evolution of European public services?**

| | | |
|---|---|---|
| Your answer | ✔ The specification introduces certain aspects that can contribute to enabling data portability. | 80 out of 100 points |

## EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

Score for this Section: 1140/1200

**A19 - To what extent does the specification allow relevant information to be reused when needed?**

| | | |
|---|---|---|
| Your answer | ✔ Not Applicable | 100 out of 100 points |

**A20 - To what extent does the specification enable the e-accessibility?**

| | | |
|---|---|---|
| Your answer | ✔ The specification can contribute and promote e-accessibility, but it is not its main purpose. | 60 out of 100 points |

**A21 - To what extent does the specification ensure the protection of personal data managed by Public Administrations?**

| | | |
|---|---|---|
| Your answer | ✔ The specification explicitly addresses data protection and its alignment to relevant regulations. | 100 out of 100 points |

**A22 - Does the specification provide means for restriction of access to information/data?**

| | | |
|---|---|---|
| Your answer | ✔ The specification introduces certain aspects that can contribute to enabling confidentiality. | 80 out of 100 points |

**A23 - Is the specification included in any initiative at European or National level covering privacy aspects?**

| | | |
|---|---|---|
| Your answer | ✔ Yes, at European level. | 100 out of 100 points |

**A24 - To what extent does the specification enable the secure exchange of data?**

| | | | |
|---|---|---|---|
| Your answer | ✔ The specification explicitly addresses and enables the secure and trustworthy exchange of data. | 100 out of 100 points |  |

**A25 - To what extent does the specification enable the secure processing of data?**

| | | | |
|---|---|---|---|
| Your answer | ✔ The specification explicitly addresses and enables the secure and trustworthy processing of data. | 100 out of 100 points |  |

**A26 - To what extent the specification guarantees the authenticity and authentication of the roles agents involved in the data transactions?**

| | | | |
|---|---|---|---|
| Your answer | ✔ The specification explicitly addresses and enables the implementation of authenticity features. | 100 out of 100 points |  |

**A27 - To what extent information is protected against unauthorised changes?**

| | | | |
|---|---|---|---|
| Your answer | ✔ The specification explicitly addresses and enables the implementation of features to guarantee data integrity. | 100 out of 100 points |  |

**A28 - To what extent does the specification ensure and enable data processing accuracy?**

| | | | |
|---|---|---|---|
| Your answer | ✔ The specification explicitly addresses and enables the implementation of features to guarantee data accuracy. | 100 out of 100 points |  |

**A29 - To what extent does the specification provide an access control mechanism?**

| | | | |
|---|---|---|---|
| Your answer | ✔ The specification explicitly foresees a set of requirements for the enabling of access control mechanisms. | 100 out of 100 points |  |

**A30 - To what extent could the specification be used in a multilingual context?**

| | | | |
|---|---|---|---|
| Your answer | ✔ The specification is designed to fully support multilingualism. | 100 out of 100 points |  |

## EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS

Score for this Section: 500/500

**A31 - Does the specification simplify the delivery of European public services?**

Your answer: ✔ YES — 100 out of 100 points

**A32 - Does the specification enable digital service delivery channels?**

Your answer: ✔ YES — 100 out of 100 points

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

Your answer: ✔ Not Applicable — 100 out of 100 points

**A34 - To what extent are there assessments of the specification's effectiveness?**

Your answer: ✔ There are such assessments directly addressing the specification. — 100 out of 100 points

**A35 - To what extent are there assessments of the specification's efficiency?**

Your answer: ✔ There are such assessments directly addressing the specification. — 100 out of 100 points

## EIF INTEROPERABILITY LAYERS

Score for this Section: 920/1001

**A36 - Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A37 - To what extent can the conformance of the specification's implementations be assessed?**

| | | |
|---|---|---|
| Your answer | ✔ The specification is complemented by a conformance testing platform to allow testing of implementations. | 100 out of 100 points |

**A38 - Is the specification recommended by a European Member State?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A39 - Is the specification selected for its use in a European Cross-border project/initiative?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A40 - Is the specification included in an open repository/catalogue of standards at national level?**

| | | |
|---|---|---|
| Your answer | ✖ NO | 20 out of 100 points |

**A41 - Is the specification included in an open repository/catalogue of standards at European level?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**Additional information:**

| | | |
|---|---|---|
| Your answer | | 0 out of 1 points |

**A42 - Is the specification a European Standard?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A43 - Does the specification facilitate the modelling of business processes?**

| | | |
|---|---|---|
| Your answer | ✔ YES | 100 out of 100 points |

**A44 - To what extent does the specification facilitate organisational interoperability agreements?**

| | | |
|---|---|---|
| Your answer | ✔ The specification explicitly identifies all elements to be used in drafting such agreements. | 100 out of 100 points |

**A45 - Does the specification encourage the creation of communities along with the sharing of their data and results in national and/or European platforms?**

| | | |
|---|---|---|
| Your answer | ✔ Yes, at European platforms. | 100 out of 100 points |

| | |
|---|---|
| Contact | CAMSS@everis.com |
| Useful links | CAMSS Joinup Page |
| | CAMSS Library of Assessments |
| | CAMSS Assessment EIF Scenario - User Guide |
| Contribution ID | b8ef97d5-e115-4b0a-8710-d8b133a20a51 |
| Completed at | 07/05/2024 16:20:50 |
| Completion time | - |