

CAMSS Assessment EIF Scenario v5.0.0

Fields marked with * are mandatory.

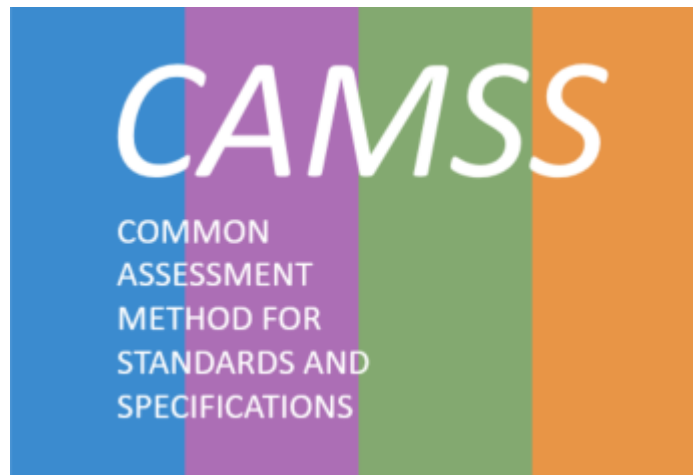
CAMSS Assessment EIF Scenario v5.0.0



Release Date: 31/01/2022

Scenario Version: 5.0.0

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.

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 440	441 to 880	881 to 1320	1321 to 1760	1761 to 2200
EIF Principles Related to generic user needs and expectations	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500
EIF Foundation principles for cooperation among public	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500

administrations

EIF

Interoperability Layers

0 to 220

221 to 440

441 to 660

661 to 880

881 to 1100

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 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.

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 Tool 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.

CAMSS Tools are based on EU Survey, by accepting the CAMSS Privacy Statment the user also accepts EU Survey [Privacy Statement](#) and the [Terms of use](#).

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

- ☒ *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.

This assessment tool is licensed under the [European Union Public License \(EUPL\)](#)

IDENTIFICATION

Information on the information provider

Your Last name

CAMSS Team

Your First Name

Your Position / Role

* Your Organisation

European Commission 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

Contact Email

DIGIT-CAMSS@eu.europa.eu

* 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

* Specifacaton type

- ☒ Specification
- ☐ Standard
- ☐ Application Profile
- ☐ Family of Specification

* Title of the specification

Cyber Security for Consumer Internet of Things Baseline Requirements (EN 303 645)

* Version of the specification

2.1.1

* Description of the specification

EN 303 645 is a standard for cybersecurity on the Internet of Things and is considered as a security baseline for Internet-connected consumer products.

* URL from where the specification is distributed

<https://www.etsi.org/technologies/consumer-iot-security>

* 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 Info

There is no reference to any functional area of application of the specification addressing interoperability and eGovernment.

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 uses 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-2020>

- ☐ 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**

There is no Member State that includes the EN 303 645 specification in their national catalogue with The National Interoperability Framework (NIF) in alignment with the three categories: 1. Conceptual model for integrated public services provision, 2. interoperability layers, and 3. interoperability principles.

CAMSS List of Standards:

<https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards>

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 open data?**

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
- ☐ NO
- ☐ YES

*** Justification**

The purpose of the EN 303 645 is not related to the publication of open data. Therefore, this criterion is not applicable to this specification.

EN 303 645 homepage reference:

<https://www.etsi.org/technologies/consumer-iot-security>

*** 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**

The Technical Committee (TC) CYBER (Cybersecurity) is encharged of the development and maintenance of the EN 303 645 specification. As other ETSI technical committes, the TC CYBER contributes to the report writing. Participation is open prior a registration process and a financial contribution (see ETSI Directives' Rules of Procedure).

ETSI Directives, Rules of Procedure:

<https://portal.etsi.org/Resources/ETSI-Directives>

ETSI TC CYBER press release reference:

<https://www.etsi.org/committee/1393-cyber>

*** 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

The Technical Committee (TC) CYBER (Cybersecurity) collaborates with stakeholders (primarily, National Standards Organizations -NSOs, academics and governmental bodies) to develop standards that improve the privacy and security of organizations and citizens in Europe and all over the world (see ETSI Directives, Rules of Procedure section, and EN 303 645 homepage reference). As the EN 303 645 is a European Standard (EN), the specification has gone through (national) public enquiry and voting (see NSOs ETSI-partnerships, EN 303 645 Public enquiry, and ETSI TC CYBER Contribution references). However, public consultations on major and minor releases are not publicly visible.

ETSI Directives, Rules of Procedure section:

<https://portal.etsi.org/Resources/ETSI-Directives>

EN 303 645 homepage reference:

<https://www.etsi.org/technologies/consumer-iot-security>

EN 303 645 Public Enquiry reference:

<https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard>

NSOs ETSI-partnerships reference:

<https://www.etsi.org/about/our-partnerships>

ETSI TC CYBER, Contribution reference:

<https://portal.etsi.org/tb.aspx?tbid=824#/50610-contributions>

* **A5 - Is the specification available with any restrictions related to Fair, Reasonable, and Non-Discriminatory ((F)RAND)?**

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.

The FRAND basis relates to fair, reasonable, and non-discriminatory IPR disclosures.

- ☐ Not Answered
- ☐ Not Applicable
- ☐ NO
- ☒ YES

* Justification

The ETSI and any of its committees, in charge of the development of EN 303 645, operates under the ETSI Intellectual Property Rights (IPRs) and IPR Policy. The specification is licensed on a (F)RAND basis.

Intellectual Property Rights Policy, ETSI ownership of IPRs section:
<https://www.etsi.org/intellectual-property-rights>

* **A6 - Is the specification licensed on a royalty-free basis?**

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
- ☐ NO
- ☒ YES

* Justification

The ETSI and any of its committees, in charge of the development of EN 303 645, operates under the ETSI Intellectual Property Rights (IPRs) and IPR Policy. The specification is licensed on a Royalty-free.

IPR Policy, ETSI ownership of IPRs section:
<https://www.etsi.org/intellectual-property-rights>

* **A7 - 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

The first version of the EN 303 645 specification was published in 2019 and up to date has reached version 2.1.1. The specification's predecessor was TS 103 645, prior to its designation as a European Standard (EN)

(see EN 303 645 homepage reference, OUR ROLE & ACTIVITIES section). All the specification releases can be found in the TC CYBER website or at the EN 303 645 homepage.

EN 303 645 homepage reference:

<https://www.etsi.org/technologies/consumer-iot-security>

*** A8 - 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 being used to create innovative solutions.

- ☐ Not Answered
- ☐ Not Applicable - The specification does not have market acceptance because it is directly used to create innovative solutions.
- ☐ 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 has widespread use, indicating market acceptance.

*** Justification**

The first version of the EN 303 645 specification was published in 2019 and superseded the ETSI TS 103 645 specification for consumer Internet of Things (CIoT); the latter was the first standard for cybersecurity in the Internet of Things, which was considered as a security baseline for Internet-connected consumer products and a basis for future IoT certification schemes. As a proof of market acceptance, at present EN 103 701 is meant to serve as an input to a forthcoming EU cybersecurity certification system, as proposed in the Cybersecurity Act (see ETSI Work Programme reference).

EN 303 645 homepage reference:

<https://www.etsi.org/technologies/consumer-iot-security>

TS 103 645 reference:

<https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security>

TS 103 701 reference:

https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

ETSI Work Programme reference:

[https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434&curlItemNr=39&totalNrItems=296&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%25)

[WKI_ID=58434&curlItemNr=39&totalNrItems=296&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434&curlItemNr=39&totalNrItems=296&optDisplay=100000&qSORT=TB&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%25)

3BM58&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qCLUSTER=19&qFREQUENCIES_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=

*** A9 - 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 are surrounding 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**

The Technical Committee (TC) CYBER (Cybersecurity) provides public support to members and non-members alike, with different conditions depending on ETSI membership status. Besides, it dedicates a wiki page to disseminate the Global cybersecurity Ecosystem (constituted in a specification itself, TR 103 306) to help stakeholders, and anyone, discover and identify the components of global cybersecurity.

ETSI TC CYBER reference:

<https://portal.etsi.org/tb.aspx?tbid=824#/5068-home>

ETSI TC CYBER wiki:

<https://cyberpublicwiki.etsi.org/index.php?title=ETSI>

ETSI TR 103 306 reference:

https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/

Transparency

*** A10 - 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**

The purpose of the EN 303 645 specification is not related to the visibility of administrative procedures, rules data, and services.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

*** A11 - 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 purpose of the EN 303 645 specification is not related to the comprehensibility of administrative procedures, rules data, and services.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

*** A12 - 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.
- ☐ The specification enables exposure of such interfaces.

* Justification

The purpose of the EN 303 645 specification is not related to enabling the exposure of interfaces of public administration's services.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

* **A13 - To what extent does the specification ensure the protection of personal data managed by Public Administrations?**

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

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 EN 303 645 specification ensures the protection of personal data according to the sixth clause of the specification documentation (see EN 303 645 reference, section 6 'Data protection provisions for consumer IoT'). Moreover, as an ETSI specification, EN 303 645 is compliant with all the European Regulations and Policies (see ETSI Role in Europe reference).

EN 303 645 reference, section 6:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

ETSI Role in Europe reference:

[https://www.etsi.org/about/etsi-in-europe?](https://www.etsi.org/about/etsi-in-europe?highlight=WyJldXJvcGVhbiIsIldldXJvcGVhbiIsImV1cm9wZWFuJ3MiLCJyZWd1bGF0aW9ucyIsImV1cm9wZWFuIHJIZ3VsYXRpb25zIl0=)

[highlight=WyJldXJvcGVhbiIsIldldXJvcGVhbiIsImV1cm9wZWFuJ3MiLCJyZWd1bGF0aW9ucyIsImV1cm9wZWFuIHJIZ3VsYXRpb25zIl0=](https://www.etsi.org/about/etsi-in-europe?highlight=WyJldXJvcGVhbiIsIldldXJvcGVhbiIsImV1cm9wZWFuJ3MiLCJyZWd1bGF0aW9ucyIsImV1cm9wZWFuIHJIZ3VsYXRpb25zIl0=)

Reusability

* **A14 - 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 used in other domains.
- ☐ The specification is associated with a specific domain but its use in other domains is difficult.
- ☐ The specification is associated with a specific domain but could be partially used in other domains.
- ☐ The specification is associated with a specific domain but could be used 'as-is' to other domains.
- ☐ The specification is domain-agnostic, designed to be used in any domain.

*** Justification**

EN 303 645 is associated to the consumer IoT device and the data security domain. EN 303 645 is a comprehensive, single-purpose specification that manufacturers and IoT stakeholders need in order to meet basic security requirements (see EN 303 645 homepage, 'International alignment and adoption' section). European directives are currently making an effort to verticalise the consumer IoT industry (see EN 303 645 homepage reference, about the vertical standard concept), opening up new possibilities to other domains (see Europe Plans on IoT reference). However, there is no evidence of the use of the specification in other domains, nor in the public sector.

EN 303 645 homepage, 'International alignment and adoption' section:

<https://www.etsi.org/technologies/consumer-iot-security>

EN 303 645 homepage, 'Vertical Standard' section:

<https://www.etsi.org/technologies/consumer-iot-security>

Europe Plans on IoT reference:

<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/internet-things>

*** A15 - To what extent is the specification usable beyond the business-specific domain, allowing its implementation 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 in other domains.
- ☐ The specification is associated with a specific domain but its implementation in other domains is difficult.
- ☐ The specification is associated with a specific domain but could be partially implemented in other domains.
- ☐ The specification is associated with a specific domain but could be implemented 'as-is' to other domains.
- ☐ The specification is domain-agnostic, designed to be implemented in any domain.

*** Justification**

EN 303 645 is associated to the consumer IoT device and the data security domain. EN 303 645 is a comprehensive, single-purpose specification that manufacturers and IoT stakeholders need in order to meet basic security requirements (see EN 303 645 homepage, 'International alignment and adoption' section). There is no evidence of the use of the specification in the public sector.

Technological Neutrality and Data Portability

* A16 - 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

Relates to the dependency of the specification to be implemented without relying on specific technologies or platforms.

- ☐ Not Answered
- ☐ Not Applicable
- ☒ NO
- ☐ YES

* Justification

EN 303 645 is a set of security best practices for Internet-connected consumer devices and is intended to support all parties involved in the development and manufacture of consumer IoT devices. The specification's recommendations (provisions) are intended to depend on any product from the IoT domain, and therefore the specification cannot be considered technology-agnostic.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

* A17 - 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

Relates to the dependency of the specification to be implemented without relying on specific technologies or platforms.

- ☐ Not Answered
- ☐ Not Applicable
- ☐ NO
- ☒ YES

* Justification

EN 303 645 is a set of security best practices for Internet-connected consumer devices and is intended to support all parties involved in the development and manufacture of consumer IoT devices. The specification is not intended to depend on any particular specification, and therefore is platform-agnostic.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

*** A18 - 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 it defines in the text.

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**

The EN 303 645 specification addresses the most significant and widespread security weaknesses. Due to the large consumer IoT landscape, it is inevitable that the applicability of the provisions (recommendations) will depend on the device, which gives the specification a degree of flexibility (see 'Reporting implementation' section). In this sense, the specification allow for partial implementation.

EN 303 645 reference, 'Reporting implementation' section:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

*** A19 - 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**

EN 303 645 is associated to the consumer IoT devices domain and is not intended to be used in other domains. Therefore, the specification does not allow customisation.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

*** A20 - 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 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**

EN 303 645 is associated to the consumer IoT devices domain. Prior to some adaptations, the specification could be extended and broaden to specific subsectors. As they state in their official website, CYBER is providing an EN 303 645 template that sets the principles for the specification to be extended. For example, the smart door locks extension is under development and is based on the EN 303 645 specification.

EN 303 645, 'Vertical Standard' section:
<https://www.etsi.org/technologies/consumer-iot-security>

*** A21 - To what extent does the specification enable data portability between systems/applications supporting the implementation 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 purpose of the EN 303 645 specification is not related to data portability. Therefore, this criterion does not apply to this specification.

EN 303 645 reference:
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

*** A22 - To what extent does the specification enable data portability between systems/applications supporting the 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 purpose of the EN 303 645 specification is not related to data portability. Therefore, this criterion does not apply to this specification.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.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

*** A23 - 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.

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**

The purpose of En 303 645 specification is not related to the implementation of the once-only principle. Therefore, this criterion does not apply to this specification.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Inclusion and Accessibility

* A24 - 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

The purpose of EN 303 645 is not related to e-accessibility. Therefore, this criterion is considered not applicable to this specification.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Security and Privacy

* A25 - 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.

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**

Nowadays people entrust their personal data to an increasing number of services, which are connected to their devices and homes. In this sense, the specification explicitly addresses and enables the secure and trustworthy data exchange (see EN 303 645 reference, provision 5.8).

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

*** A26 - 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**

Nowadays people entrust their personal data to an increasing number of services, which are connected to their devices and homes. In this sense, the specification explicitly addresses and enables the secure and trustworthy data processing (see EN 303 645 reference, provisions 5.4, 5.10 and 5.11).

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Multilingualism

*** A27 - 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**

The purpose of EN 303 645 is not related to the delivery of multilingual public services. Therefore, this criterion is not applicable to this specification.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

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

*** A28 - 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.

- ☐ Not Answered
- ☐ Not Applicable
- ☒ NO
- ☐ YES

*** Justification**

The EN 303 645 specification does not simplify the delivery of European public services, but can indirectly facilitate their delivery. The specification has been included in several initiatives supported by the EU cybersecurity certification framework for ICT products (see J. Pandza's presentation on the ENISA Cybersecurity Standardisation Event, and see EU cybersecurity certification framework reference). For example, there is the Eurosmart IoT Certification Scheme, which relies on the EN 303 645 specification,

setting the first common certification scheme for IoT devices in Europe and facilitating the delivery of European public services.

ENISA Cybersecurity Standardisation Event 2021, Jasper Pandza presentation:

https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/std-2021-presentations

EU cybersecurity framework reference:

<https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>

Eurosmart IoT Certification Scheme reference:

<https://www.eurosmart.com/eurosmart-iot-certification-scheme/>

*** A29 - 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.

- ☐ Not Answered
- ☐ Not Applicable
- ☒ NO
- ☐ YES

*** Justification**

Up to date, the EN 303 645 specification does not enable digital service delivery channels. Nonetheless, the specification could enable new channels once the EU cybersecurity certification framework for ICT products is consolidated.

EU cybersecurity framework reference:

<https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>

Preservation of Information

*** A30 - 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

The purpose of EN 303 645 is not related to the long-term preservation of data/information/knowledge. Therefore, this criterion is considered not applicable to this specification.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Assessment of Effectiveness and Efficiency

* **A31 - 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 then 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

There is no evidence of any study directly assessing the effectiveness of the EN 303 645 specification. However, there are some organisations from the private sector, offering solutions based on the specification's performance with respect to the market, that indirectly assess the specification's effectiveness. It is the case of TÜV SÜD, which offers testing against the EN 303 645 specification.

TÜV SÜD-EN 303 645 reference:

<https://www.tuvsud.com/en-us/industries/consumer-products-and-retail/iot-cybersecurity/>

* **A32 - 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

There is no evidence of any study directly assessing the efficiency of the EN 303 645 specification. However, there are some organisations from the private sector, offering solutions based on the specification's performance with respect to the market, that indirectly assess the specification's efficiency. It is the case of TÜV SÜD, which offers testing against the EN 303 645 specification.

TÜV SÜD-EN 303 645 reference:

<https://www.tuvsud.com/en-us/industries/consumer-products-and-retail/iot-cybersecurity/>

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

* **A33 - 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

This specification is not currently included in the EIRA Library of Interoperability Specifications (ELIS), but will be included in the next release of the ELIS. The response to this criterion is positive because EN 303 645 is mappable to the European Interoperability Reference Architecture (EIRA).

EIRA Library of Interoperability Specifications (ELIS):

<https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v110>

*** A34 - 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**

EN 303 645 does not define any specific methodology for testing its provisions' conformance, but it provides for each each of the implemented features a recording template that eases conformity testing in a structured way (see the Implementation Conformance Statement proforma in Annex B of the EN 303 645 specification). On the other hand, there is the ETSI TS 103 701 conformance assessment methodology for consumer IoT devices, which is intended to set a provisions conformance testing with respect to ETSI EN 303 645, giving test cases and assessment criteria for each provision.

EN 303 645 reference, Annex B:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

TS 103 701 reference:

https://etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

*** A35 - Is the specification recommended by an 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

The EN 303 645 specification is not included in any national catalogue. However, the specification has been recommended by some European national agencies like the Federal Office for Information Security (BSI) in Germany, or has been integrated in a public service like the Cybersecurity label in Finland to certify safe smart devices and assist consumers in buying safer products.

CAMSS List of Standards:

<https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards>

Finnish Transport and Communications Agency Traficom reference:

<https://www.kyberturvallisuuskeskus.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label>

German BSI reference:

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/SmartHome_130720.html

* A36 - Is the specification selected for its use in an 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 EN 303 645 specification, through ETSI, participates in cooperative projects at the European level. In particular, the EU Agency for Cybersecurity (ENISA), together with ETSI and the CEN and CENELEC "Cybersecurity and Data Protection" technical committee (see J. Pandza's presentation on the ENISA Cybersecurity Standardisation Event, and CEN-CLC/JTC 13 reference), are part of several European initiatives (see Official Journal of the European Union reference) to develop "home-grown" European standards in the field of cybersecurity. For example, the specification has direct implications in the context of European certification systems.

ENISA Cybersecurity Standardisation Event 2021, Jasper Pandza presentation:

https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/std-2021-presentations

CEN-CLC/JTC 13 reference:

<https://www.cencenelec.eu/areas-of-work/cenelec-sectors/digital-society-cenelec/cybersecurity-and-data-protection/>

Official Journal of the European Union reference:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XG1210%2801%29>

*** A37 - 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**

EN 303 645 is not included in any Member States' catalogues of recommended specifications.

CAMSS List of Standards:

<https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards>

*** A38 - 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**

There is no evidence of the inclusion of EN 303 645 in an open repository/catalogue of standards at European level.

EUOS repository of standards:

<https://www.standict.eu/standards-repository>

CENELEC and CEN search tool catalogue:

<https://standards.cencenelec.eu/dyn/www/f?p=CEN:105::RESET:::>

Legal Interoperability

* A39 - 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

Although the EN 303 645 specification is not a Harmonised European Standard (HEN) following Radio Equipment Directive (RED) specification (see J. Pandza's presentation on the ENISA Cybersecurity Standardisation Event, and HEN reference), the specification is a European Standard (see EN 303 645 reference).

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

ENISA Cybersecurity Standardisation Event 2021, Jasper Pandza presentation:

https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/std-2021-presentations

HEN reference:

https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en#:~:text=A%20harmonised%20standard%20is%20a%20European%20standard%20developed,the%20European%20Commission%20to%20one%20of%20these%20organisations.

Organisational Interoperability

* A40 - 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

The EN 303 645 specification facilitates business modeling, as the specification can be deployed into any architecture for consumer IoT in a home environment. The evidence for this is that consumer IoT devices are collections of hardware and software components, with physical or network interfaces, typically connected to online or local services.

EN 303 645 reference, Annex A Basic concepts and models:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

* **A41 - 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

Although organisational interoperability agreements on the cybersecurity domain are not formalised (see Cybersecurity Act reference), the EN 303 645 specification establishes a cybersecurity baseline for connected consumer products and is intended to set the basis for future IoT certification systems in Europe (see IoT Policy and Legislation reference). This baseline comprises the set of provisions defined in the specification documentation, but is not specifically designed for establishing these agreements.

EN 303 645 reference:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Cybersecurity Act reference:

<https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act#:~:text=The%20EU%20Cybersecurity%20Act%20introduces%20an%20EU-wide%20cybersecurity,see%20their%20certificates%20recognised%20across%20the%20European%20Union.>

IoT Policy and Legislation reference:

<https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/internet-things>

Semantic Interoperability

* **A42 - Does the specification encourage the creation of communities along with the sharing of their data and results on national 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
- ☒ NO
- ☐ YES

*** Justification**

The Technical Committee (TC) CYBER (Cybersecurity) provides feature requests to open source projects and results of implementation experience to open source communities; however, not in national platforms.

TC CYBER reference:

<https://www.etsi.org/cyber-security/tc-cyber-roadmap>

*** A43 - Does the specification encourage the creation of communities along with the sharing of their data and results on 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
- ☐ NO
- ☒ YES

*** Justification**

The Technical Committee (TC) CYBER (Cybersecurity) provides feature requests to open source projects and results of implementation experience to open source communities. ETSI, as an acknowledged European standardisation, offers different channels for the creation of communities and the sharing of data and results in European platforms.

TC CYBER reference:

<https://www.etsi.org/cyber-security/tc-cyber-roadmap>

Useful links

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

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

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

DIGIT-CAMSS@ec.europa.eu



CAMSS Assessment EIF Scenario v5.0.0 - 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 440	441 to 880	881 to 1320	1321 to 1760	1761 to 2200
EIF Principles Related to generic user needs and expectations	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500

**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 220

221 to 440

441 to 660

661 to 880

881 to 1100

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 2200 points.
2. In the middle table – the Section Compliance Conversion Table – see that this number correlates to a column. In our example, the 2200 points of Core Interoperability Principles fall in the EIF Core Interoperability Principles row, and '1761 to 2200' 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 3200

Maximum Score 4300




Section	Score for this Section	
EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY	20/100	<div><div></div></div>
EIF CORE INTEROPERABILITY PRINCIPLES	1660 /2100	<div><div></div></div>
EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS	500 /500	<div><div></div></div>
EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS	220 /500	<div><div></div></div>
EIF INTEROPERABILITY LAYERS	800 /1100	<div><div></div></div>

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: 1660/2100


A2 - Does the specification facilitate the publication of open data?

Your answer  Not Applicable

100
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 fees and membership approval.

60
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 but, during which, collected feedback is not publicly visible.

80
out of
100
points



A5 - Is the specification available with any restrictions related to Fair, Reasonable, and Non-Discriminatory ((F)RAND)?

Your answer  YES

100
out of
100
points




A6 - Is the specification licensed on a royalty-free basis?

Your answer  YES

100
out of
100
points




A7 - 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




A8 - To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?

Your answer  The specification has widespread use, indicating market acceptance.

100
out of
100
points




A9 - To what extent has the specification support from at least one community?

Your answer  There is a community providing public support linked to the specification but in a best-effort manner.

80
out of
100
points




A10 - To what extent does the specification enable the visibility of administrative procedures, rules data, and services?

Your answer  Not Applicable

100
out of
100
points




A11 - To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?

Your answer  Not Applicable

100
out of
100
points




A12 - To what extent does the specification enable the exposure of interfaces to access the public administration's services?

Your answer  Not Applicable

100
out of
100
points




A13 - 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




A14 - To what extent is the specification usable beyond the business-specific domain, allowing its usage across business domains?

Your answer  The specification is associated with a specific domain but its use in other domains is difficult.

40
out of
100
points



A15 - To what extent is the specification usable beyond the business-specific domain, allowing its implementation across business domains?

Your answer  The specification is tied to a specific domain and is restricted from being implemented in other domains.

20
out of
100
points



A16 - Is the specification technology agnostic?

Your answer  NO

20
out of
100
points




A17 - Is the specification platform agnostic?

Your answer  YES

100
out of
100
points



A18 - To what extent does the specification allow for partial implementations?

Your answer  The specification could be partially implemented but does not make specific provisions towards this.

40
out of
100
points




A19 - Does the specification allow customisation?

Your  NO
answer

20
out of
100
points




A20 - Does the specification allow extension?

Your  YES
answer

100
out of
100
points




A21 - To what extent does the specification enable data portability between systems/applications supporting the implementation of European public services?

Your  Not Applicable
answer

100
out of
100
points



A22 - To what extent does the specification enable data portability between systems/applications supporting the evolution of European public services?

Your  Not Applicable
answer


100
out of
100
points



EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

Score for this Section: 500/500


A23 - To what extent does the specification allow relevant information to be reused when needed?

Your  Not Applicable
answer

100
out of
100
points




A24 - To what extent does the specification enable the e-accessibility?

Your  Not Applicable
answer



100
out of
100
points



A25 - 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 

A26 - 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 


A27 - To what extent could the specification be used in a multilingual context?

Your answer  Not Applicable 100 out of 100 points 

EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS

Score for this Section: 220/500


A28 - Does the specification simplify the delivery of European public services?

Your answer  NO 20 out of 100 points 


A29 - Does the specification enable digital service delivery channels?

Your answer  NO 20 out of 100 points 


A30 - 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 


A31 - To what extent are there assessments of the specification's effectiveness?

Your answer  There are such assessments that indirectly address the specification.


40
out of
100
points



A32 - To what extent are there assessments of the specification's efficiency?

Your answer  There are such assessments that indirectly address the specification.

40
out of
100
points



EIF INTEROPERABILITY LAYERS

Score for this Section: 800/1100


A33 - Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?

Your answer  YES


100
out of
100
points



A34 - To what extent can the conformance of the specification's implementations be assessed?

Your answer  The specification defines conformance as requirements that can be measured manually.

60
out of
100
points



A35 - Is the specification recommended by an European Member State?

Your answer  YES

100
out of
100
points



A36 - Is the specification selected for its use in an European Cross-border project/initiative?

Your answer  YES

100
out of
100
points



A37 - Is the specification included in an open repository/catalogue of standards at national level?

Your answer  NO

20
out of
100
points



A38 - Is the specification included in an open repository/catalogue of standards at European level?

Your  NO
answer

20
out of
100
points



A39 - Is the specification a European Standard?

Your  YES
answer

100
out of
100
points




A40 - Does the specification facilitate the modelling of business processes?

Your  YES
answer

100
out of
100
points



A41 - To what extent does the specification facilitate organisational interoperability agreements?

Your  The specification defines most elements to
answer facilitate such agreements.

80
out of
100
points



A42 - Does the specification encourage the creation of communities along with the sharing of their data and results on national platforms?

Your  NO
answer

20
out of
100
points



A43 - Does the specification encourage the creation of communities along with the sharing of their data and results on European platforms?

Your  YES
answer

100
out of
100
points



Contact DIGIT-CAMSS@ec.europa.eu

[CAMSS Joinup Page](#)

Useful links [CAMSS Library of Assessments](#)

[CAMSS Assessment EIF Scenario - User Guide](#)

Contribution ID 94327cfb-087f-4e7d-9d7f-03bdc71964d5

Completed at 28/03/2022 10:44:40

Completion time -