

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.

Section	Compliance Level				
	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

- ☒ *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 is licensed under the [European Union Public License \(EUPL\)](#)

IDENTIFICATION

Information on the information provider

Your Last name

Your First Name

Your Position / Role

* Your Organisation

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

Advanced Encryption Standard (AES)

* Version of the specification

1.0.0

* Description of the specification

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data.

* URL from where the specification is distributed

<https://csrc.nist.gov/pubs/fips/197/final>

* 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)

* In case of Other SDO, please, provide its name:

National Institute of Standards and Technology (NIST)

* and, provide its URL:

<https://www.nist.gov/>

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

The Advanced Encryption Standard (AES) enhances interoperability by providing a secure, standardised encryption method that various organisations can use to communicate effectively. Its widespread acceptance ensures compatibility across different systems, improving secure communications.

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

The Advanced Encryption Standard is included in 4 national catalogues of recommended specifications. They belong to Cyprus, Germany, Malta and The Netherlands. The National Interoperability Framework (NIF) of The Netherlands is aligned with at least 3 out of 4 scoreboards of the EIF Monitoring according to the National Interoperability Framework Observatory (NIFO) factsheets.

NIFO Factsheets:

<https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2024>

National Catalogue of Cyprus:

[https://dits.dmr.gov.cy/dmr/dits/dits.nsf/all/B83AA8E4EB4EFD19C225855800288B10/\\$file/Cyprus%20eGovernment%20Interoperability%20Framework_new%20EIF_v2.0-To%20Publish.pdf](https://dits.dmr.gov.cy/dmr/dits/dits.nsf/all/B83AA8E4EB4EFD19C225855800288B10/$file/Cyprus%20eGovernment%20Interoperability%20Framework_new%20EIF_v2.0-To%20Publish.pdf)

National Catalogue of Germany:

https://www.cio.bund.de/Web/DE/Architekturen-und-Standards/SAGA/SAGA%205-aktuelle%20Version/saga_5_aktuelle_version_node.html

National Catalogue of Malta:

<https://mccaa.org.mt/Section/Content?contentId=1243>

National Catalogue of The Netherlands:

<https://www.forumstandaardisatie.nl/open-standaarden/lijt>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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**

The purpose of Advanced Encryption Standard is not related to the publication of public data as open data. Therefore this criterion is not applicable to the specification.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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 NIST organisation offers a guide on how to contribute to the development of new solutions. Tools and use cases can be contributed via GitHub pull requests, while feedback can be provided via GitHub issues. Contributed tools and use cases can be hosted directly in the NIST repository, or they can be hosted elsewhere online and linked to from the NIST repository.

NIST collaboration space:

<https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

As can be seen in the Crypto Publication Review Board, the NIST organisation establishes periods for initial comments, and then, they make a decision proposal, taking into account all the comments. In addition, all the comments collected in the "call for comments" period can be found in each specification section in the Crypto Publication Review Board. This process for the crypto standards, can be extended to other type of solutions.

NIST crypto standards release lifecycle:

<https://csrc.nist.gov/projects/crypto-publication-review-project>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

NIST asserts rights outside of the United States. The public is granted the non-exclusive, perpetual, paid-up, royalty-free, worldwide right to reprint works in all formats, including print, electronically, and online, and in all subsequent editions and derivative works.

NIST IRP and F/RAND principles:

<https://www.nist.gov/open/copyright-fair-use-and-licensing-statements-srd-data-software-and-technical-series-publications#:~:text=To%20the%20extent%20NIST%20may%20assert%20rights%20outside,and%20in%20all%20subsequent%20editions%2C%20and%20derivative%20works.>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

The Advanced Encryption Standard (AES) was established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The Rijndael submission by Daemen and Rijmen won an open competition organized by NIST in 2000. Then, in 2001, the submission was standardised as AES. However, the first version of the standard began to be discussed in 1997, although its original name was not AES. Since then, all releases have been published. And since its first version, one minor release addressing some formal aspects of the standard document has been launched.

NIST AES Reference:

<https://www.nist.gov/publications/review-advanced-encryption-standard>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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

The Advanced Encryption Standard (AES) is a solution used to encrypt data, making it more secure against attacks or attempts to access data in an unauthorised way. In this context, the standard not only addresses data protection but also interoperability and collaboration. Moreover, AES has been assessed in many papers and discussed in terms of how it can be implemented in different contexts. Finally, it has been integrated into solutions such as VeraCrypt.

VeraCrypt AES project:
<https://veracrypt.eu/en/AES.html>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

* **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

The Advanced Encryption Standard has been published and is maintained by the National Institute of Standards and Technology (NIST). Moreover, there are specifications that extend AES in Internet Engineering Task Force (IETF).

IETF AES Reference:
<https://mailarchive.ietf.org/arch/browse/smime/?q=Advanced%20Encryption%20Standard>

National Institute of Standards and Technology (NIST):
<https://www.nist.gov/>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

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**

The purpose of Advanced Encryption Standard is not related to enabling the visibility of administrative procedures, rules data, and services. Therefore this criterion is not applicable to the specification.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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 purpose of Advanced Encryption Standard is not related to scope comprehensibly administrative procedures, rules data, and services. Therefore this criterion is not applicable to the specification.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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

*** Justification**

The purpose of Advanced Encryption Standard is not related to enabling the exposure of interfaces to access the public administration's services. Therefore this criterion is not applicable to the specification.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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.
- ☒ The specification is domain-agnostic, designed to be implemented and/or used in any domain.

*** Justification**

The Advanced Encryption Standard is designed to be implemented and used in any domain, allowing its usability in different sectors and applications. In this context, AES is designed to protect data; thus, the standard can be implemented to protect data of any type.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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 Advanced Encryption Standard can be implemented in any software, firmware, hardware or any combination of them. Therefore, the standard is technology agnostic.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

* 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

The Advanced Encryption Standard can be implemented in any software, firmware, hardware or any combination of them. Therefore, the standard is platform agnostic.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

* 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**

The Advanced Encryption Standard allows implementations to support at least one of the three key lengths, established by the standard guide. A "key length" refers to the size of the cryptographic key used to encrypt and decrypt data, measured in bits. In this context, the standard allows optional support for two or three key lengths, but it's not required to support all three.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

The Advanced Encryption Standard does not allow the customisation of its core components when is implemented.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

The AES specification is designed to be adaptable and extended in the future. This means that future versions of the official AES standard could introduce changes or additions to the allowed values for some of its key parameters. For example, they might permit modify technical settings. However, at this moment the specification cannot be extended, and if it is modified, it can cause a loose of security capabilities.

Computer Security Objects Register (CSOR) reference:
<https://csrc.nist.gov/projects/computer-security-objects-register>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

If different systems or apps, even those made by different groups in different European countries, use AES following the technical guide of the standard, they will be able to encrypt data so that other systems using the same guide can decrypt it correctly, and the other way around.

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

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

The Advanced Encryption Standard (AES) allows information protected by AES in one system to be used and understood by any other system that also correctly implements the standard and possesses the appropriate key.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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**

The purpose of Advanced Encryption Standard is not related to e-accessibility. Therefore this criterion is considered not applicable to the specification.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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 Advanced Encryption Standard is a fundamental tool that allows public administrations to protect the confidentiality of personal data through the use of a strong and standardised encryption algorithm. By adhering to this specification, public entities can ensure that sensitive information remains secure and is only accessible to authorised parties.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

By encrypting information, access is effectively restricted to those who do not possess the decryption key. In this sense, encryption serves as a powerful form of de facto access control. This means that even if someone gains access to the encrypted data, they cannot read or use it without the correct key. This ensures that sensitive information remains confidential and secure, providing a robust layer of protection against unauthorised access.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

The Advanced Encryption Standard can be found in the VeraCrypt project. VeraCrypt encrypts partitions or storage devices, including those where Windows is installed. In this sense, encryption is automatic and fast,

with hidden volumes for plausible deniability.

VeraCrypt AES project:
<https://veracrypt.eu/en/Home.html>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

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 Advanced Encryption Standard, which defines the Advanced Encryption Standard (AES), significantly enables the secure exchange of data by providing a robust and widely trusted encryption algorithm. By converting data into an unreadable format without the appropriate key, AES ensures that transmitted information remains incomprehensible to any unauthorised person who might intercept it.

Geeksforgeeks AES reference:
<https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

* 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**

Although the Advanced Encryption Standard focuses on confidentiality, encryption significantly hinders unauthorised modification of data without detection upon decryption. This means that while AES primarily ensures that data remains private, it also makes it much harder for anyone to alter the data without being noticed, adding an extra layer of security.

Geeksforgeeks AES reference:

<https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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

The purpose of Advanced Encryption Standard is not related to guarantee the authenticity and authentication of the roles agents involved in the data transactions. Therefore, this criterion is not applicable to the specification.

Geeksforgeeks AES reference:

<https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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

AES encryption can indirectly contribute to protecting information against such alterations. However, protection against unauthorised changes is significantly enhanced when AES is used in conjunction with dedicated integrity verification mechanisms like MACs (Message Authentication Codes). This combination ensures both the confidentiality and integrity of the data, making it more secure against tampering and unauthorised modifications.

Message Authentication Codes (MAC) specification reference:

<https://csrc.nist.gov/projects/message-authentication-codes>

Geeksforgeeks AES reference:

<https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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**

The Advanced Encryption Standard includes mechanisms that help guarantee data accuracy, such as data encryption. By encrypting information, it can help ensure that data has not been altered by an unauthorised user since it was sent.

Geeksforgeeks AES reference:

<https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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

The Advanced Encryption Standard itself does not define a formal access control system with explicit roles and permissions. However, the encryption it provides acts as an effective access control by restricting data access to those who possess the decryption key.

Geeksforgeeks AES reference:

<https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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

The purpose of Advanced Encryption Standard is not related to the delivery of multilingual services. Therefore this criterion is not applicable to this specification.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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 administrative simplification by for example helping an Identification service access a Digital Portfolio with citizens information.

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

*** Justification**

The Advanced Encryption Standard provides a standardised method for protecting data by encrypting it in a common format. This standard facilitates collaboration by ensuring data is encrypted and decrypted uniformly. An example can be found looking at VeraCrypt project. The aim of this initiative is to encrypt partitions or storage devices, in an automatic and fast manner.

VeraCrypt AES project:

<https://veracrypt.eu/en/Home.html>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

The purpose of Advanced Encryption Standard is not related to enable digital service delivery channels. Therefore this criterion is not applicable to this specification.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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

Although the Advanced Encryption Standard is designed to encrypt and securely store data, it is not related to the long-term preservation of electronic resources.

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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 the Advanced Encryption Standard has been assessed by the Institute of Electrical and Electronics Engineers (IEEE), dedicated to standardisation and development in technical areas. In the study "Advanced Encryption Standard (AES) Security Enhancement Using Hybrid Approach," a mechanism is proposed to enhance security in message transmission. This involves using the AES algorithm combined with Dynamic Key Generation and Dynamic S-box Generation.

"Advanced encryption standard (AES) security enhancement using hybrid approach" study:
<https://ieeexplore.ieee.org/abstract/document/8229881>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

* **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

The efficiency of the Advanced Encryption Standard specification has been assessed by the Institute of Electrical and Electronics Engineers (IEEE), dedicated to standardisation and development in technical areas. In the "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter" study, a method for integrating the AES encrypter and the AES decrypter into a full functional AES crypto-engine is proposed.

"Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter" study:
<https://ieeexplore.ieee.org/abstract/document/1030726>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

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

Advanced Encryption Standard is already associated to EIRA ABBs in the EIRA Library of Interoperability Specifications (ELIS). More specifically, Advanced Encryption Standard can define the interoperability aspects of the "Integrity Verification" ABB of the EIRA Technical View.

EIRA Library of Interoperability Specifications (ELIS):

<https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v610>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

* 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**

The "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)" document offers a guide on how to test the Advanced Encryption Standard. In this sense, it specifies the procedures involved in validating implementations of the Advanced Encryption Standard (AES) algorithm in FIPS 197 : Advanced Encryption Standard. The AESAVS is designed to perform automated testing on Implementations Under Test (IUTs). In addition, NIST has developed a validation program to test implementations for conformance to the algorithms in this standard.

AESAVS Test guidelines:

<https://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf>

Cryptographic Module Validation Program (CMVP) Reference:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

4 Member States are recommending Advanced Encryption Standard in their ICT National Catalogues. These Member States are Cyprus, Germany, Malta and The Netherlands.

CAMSS List of Standards:

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

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

*** 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 Advanced Encryption Standard (AES) is used in the VeraCrypt project as an encryption algorithm to protect data from unauthorised access.

VeraCrypt AES project:
<https://veracrypt.eu/en/AES.html>

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

The Advanced Encryption Standard is included in 4 Member States catalogues of recommended specifications. These Member States are Cyprus, Germany, Malta and The Netherlands.

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

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

*** 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**

Although the Advanced Encryption Standard cannot be found in any repository of standards at European level, the standard is mentioned in the "Cryptographic security: Critical to Europe's digital sovereignty" document, from the European Parliament, as a main cryptographic algorithm. In addition, the Advanced Encryption Standard can also be found in the eDelivery specification.

"Cryptographic security: Critical to Europe's digital sovereignty" document:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI\(2024\)766237_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766237/EPRS_BRI(2024)766237_EN.pdf)

eDelivery specification encryption:

<https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=866025549>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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.cenelec.eu/>

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

*** Justification**

The Advanced Encryption Standard is developed by a non-European organisation. Therefore, the specification cannot be considered a European standard.

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

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

The purpose of Advanced Encryption Standard is not related to facilitate the modelling of business processes. Therefore this criterion is not applicable to this specification.

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

* 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

The Advanced Encryption Standard facilitates organisational interoperability agreements by offering a widely adopted, open, and technically detailed encryption standard. This allows organisations to have a common basis for data security in their interactions, and to facilitate the exchange of data.

AES Standard Reference:
<https://csrc.nist.gov/pubs/fips/197/final>

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

The Advanced Encryption Standard is assessed and discussed in various forums and across the Internet. For example, in the Autoit Web can be found some forums that discuss the Advanced Encryption Standard, and its implementation in different contexts.

Autoit Advanced Encryption Standard:

<https://www.autoitscript.com/forum/topic/78745-advanced-encryption-standard-aesrijndael-udf/>

AES Standard Reference:

<https://csrc.nist.gov/pubs/fips/197/final>

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 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 4160

Maximum Score 4500




Section	Score for this Section	
EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY	100 /100	<div><div></div></div>
EIF CORE INTEROPERABILITY PRINCIPLES	1540 /1700	<div><div></div></div>
EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS	1160 /1200	<div><div></div></div>
EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS	480 /500	<div><div></div></div>
EIF INTEROPERABILITY LAYERS	880 /1000	<div><div></div></div>

Scores by Question:

EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

Score for this Section: 100/100

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 been included within the catalogue of a Member State with a higher performance than stated in the Digital Public Administration Factsheets from the NIFO.

100
out of
100
points



EIF CORE INTEROPERABILITY PRINCIPLES

Score for this Section: 1540/1700


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

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 all without specific fees, registration, or other conditions.

100
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



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	<div></div>
-------------	---	--------------------------------	-------------

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	<div></div>
-------------	---	--------------------------------	-------------

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	<div></div>
-------------	---	--------------------------------	-------------

A9 - 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	<div></div>
-------------	------------------	--------------------------------	-------------


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

Your answer	✔ Not Applicable	100 out of 100 points	<div></div>
-------------	------------------	--------------------------------	-------------

A11 - 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	<div></div>
-------------	------------------	--------------------------------	-------------

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 explicitly foresees sets of requirements that can be implemented incrementally or separately.

100
out of
100
points



A16 - Does the specification allow customisation?

Your answer  NO

20
out of
100
points




A17 - Does the specification allow extension?

Your answer  NO

20
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 explicitly addresses and enables data portability.

100
out of
100
points



EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

Score for this Section: 1160/1200

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

✔ Not Applicable

100
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 explicitly addresses and enables the implementation of features to guarantee confidentiality.

100
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  Not Applicable

100
out of
100
points




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

Your answer  The specification introduces certain aspects that can contribute to enabling data integrity.

80
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 introduces certain aspects that can contribute to enabling access control mechanisms.

80
out of
100
points



A30 - 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: 480/500


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  Not Applicable

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 addressing the specification and its effectiveness together with other specifications.

80
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: 880/1000


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 defines conformance as requirements with resources to enable automated measurement.

80
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  YES
answer

100
out of
100
points



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

Your  YES
answer

100
out of
100
points



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

Your  YES
answer

100
out of
100
points




A42 - Is the specification a European Standard?

Your  NO
answer

20
out of
100
points



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

Your  Not Applicable
answer

100
out of
100
points




A44 - 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



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  Yes, at European platforms.
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	92174c66-12b1-4c03-a440-bf0a3980c5c2
Completed at	05/06/2025 13:20:34
Completion time	-