



ASSESSMENT SUMMARY v1.0.0

Advanced Encryption Standard (AES)¹

National Institute of Standards and Technology (NIST)²

¹ AES Standard Reference: <https://csrc.nist.gov/pubs/fips/197/final>

² NIST organisation: <https://www.nist.gov/>

Change Control

Modification		Details	
Version 1.0.0			
Initial version			

TABLE OF CONTENT

1. INTRODUCTION..... 4

2. ASSESSMENT SUMMARY 4

2.1. EIF Interoperability Principles.....4

2.2. EIF Interoperability Layers7

3. ASSESSMENT RESULTS 9

1. INTRODUCTION

The present document is a summary of the assessment of the **AES** carried out by CAMSS using the CAMSS Assessment EIF scenario³. The purpose of this scenario is to assess the compliance of a standard or specification with the European Interoperability Framework (EIF)⁴.

2. ASSESSMENT SUMMARY

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES specification is essential to protect data by encrypting it, 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 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. In this context, the AES specification can be seen included in some European initiatives, such as the VeraCrypt project and eDelivey specification.

Finally, AES was announced by the NIST organisation as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardisation process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable.

2.1. EIF Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

The specification supports the principles setting context for EU actions on interoperability:

- **Subsidiarity and proportionality**

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) factsheets⁵.

³ CAMSS Assessment EIF Scenario: <https://ec.europa.eu/eusurvey/runner/CAMSSAssessmentEIFScenario6>

⁴ ISA2 programme website: https://ec.europa.eu/isa2/eif_en

⁵ NIFO Factsheets: <https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2024>

The specification supports the principles setting context for EU actions on interoperability:

- **Openness**

NIST encourages public contributions for new solutions via GitHub⁶. They follow a process, where feedback is gathered and considered before decisions. This open approach applies to various technologies, and NIST grants broad usage rights.

AES, a well-known encryption standard developed by NIST, exemplifies this process. The AES process started in 1997 and finalised in 2001 with a minor release. However the standard has been updated in 2023, demonstrating how NIST creates impactful and widely adopted standards that enhance security and interoperability, as seen in its integration with tools like VeraCrypt⁷.

- **Transparency**

The purpose of AES is not related to enabling the visibility of administrative procedures, to scope comprehensibly administrative procedures nor to enabling the exposure of interfaces. These criteria are not applicable to the specification.

- **Reusability**

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.

- **Technological neutrality and data portability**

The Advanced Encryption Standard (AES) is a flexible encryption method that can be used in software, firmware, hardware, or any combination of these, making it adaptable to different technologies and platforms. It supports various key lengths, which are the sizes of the keys used to encrypt and decrypt data. The standard requires support for at least one key length but allows for optional support for two or three key lengths.

However, although AES is designed to be updated in the future, at this moment the specification cannot be extended, and if it is modified, it can cause a loss of security capabilities.

The specification supports the principles related to generic user needs and expectations:

- **User-centricity**

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.

⁶ GitHub Collaboration Space: <https://github.com/usnistgov/PrivacyEngCollabSpace>

⁷ VeraCrypt AES project: <https://veracrypt.eu/en/AES.html>

- **Inclusion and accessibility**

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

- **Privacy**

Advanced Encryption Standard enhances data protection through a standardised encryption algorithm. In this sense, AES uses symmetric key encryption to encrypt large amounts of data efficiently. Specifically, the keys used by AES can be three different lengths: 128, 192, or 256 bits. This allow public administrations to ensure the confidentiality of data. Moreover, this standard allow public entities to ensure that sensitive information remains secure, providing a robust layer of protection against unauthorised access.

In addition, the Advanced Encryption Standard can be found in the VeraCrypt project. This project allows to encrypt partitions or storage devices, including those where Windows is installed⁸.

- **Security**

The Advanced Encryption Standard (AES) is a widely trusted encryption algorithm that secures data by making it unreadable without the correct key. This ensures data privacy and helps prevent unauthorised modifications. For enhanced security, AES can be combined with Message Authentication Codes (MACs)⁹ to ensure both confidentiality and integrity of the data. Although AES doesn't define access control roles, it effectively restricts data access to those who possess the decryption key.

- **Multilingualism**

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

The specification supports the foundation principles for cooperation among public administrations:

- **Administrative Simplification**

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. However, the specification is not related to enable digital service delivery channels.

- **Preservation of information**

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.

⁸ VeraCrypt Windows: <https://veracrypt.eu/en/Downloads.html>

⁹ Message Authentication Codes (MAC) specification reference: <https://csrc.nist.gov/projects/message-authentication-codes>

- **Assessment of effectiveness and efficiency**

The effectiveness and efficiency of the Advanced Encryption Security specification has been assessed by the Institute of Electrical and Electronics Engineers, dedicated to standardisation and development in technical areas. In the "Advanced encryption standard (AES) security enhancement using hybrid approach"¹⁰ study, 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. In addition, in the "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter"¹¹ study, a method for integrating the AES encrypter and the AES decrypter into a full functional AES crypto-engine is proposed.

2.2. EIF Interoperability Layers

The interoperability model which is applicable to all digital public services includes:

- Four layers of interoperability: legal, organisational, semantic and technical;
- A cross-cutting component of the four layers, 'integrated public service governance';
- A background layer, 'interoperability governance'.

The Specification supports the implementation of digital public services complying with the EIF interoperability model:

- **Interoperability governance**

Advanced Encryption Standard is linked to EIRA ABBs in the EIRA Library of Interoperability Specifications (ELIS)¹², defining interoperability aspects of the "Integrity Verification" ABB in the EIRA Technical View. Moreover, it can be found a platform developed by the NIST organisation to test the standard implementations¹³. Additionally, the specification is important in both, national and European level, and can be found in some projects, such as Veracrypt and eDelivery specification in encryption functions.

- **Legal Interoperability**

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

¹⁰ "Advanced encryption standard (AES) security enhancement using hybrid approach" study: <https://ieeexplore.ieee.org/abstract/document/8229881>

¹¹ "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter" study: <https://ieeexplore.ieee.org/abstract/document/1030726>

¹² EIRA Library of Interoperability Specifications (ELIS): <https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v610>

¹³ Cryptographic Module Validation Program (CMVP) Reference: <https://csrc.nist.gov/projects/cryptographic-module-validation-program>

- **Organisational interoperability**

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.

- **Semantic Interoperability**

The Advanced Encryption Standard is assessed and discussed in various forums and across the Internet. For example, in the Autoit Web¹⁴ can be found some forums that discusses the Advanced Encryption Standard, and its implementation in different contexts.

¹⁴ Autoit Advanced Encryption Standard: <https://www.autoitscript.com/forum/topic/78745-advanced-encryption-standard-aesrijndael-udf/>

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **AES**. The CAMSS “Strength” indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones is used to calculate the “Automated Score” per category and an “Overall Score”.

Category	Automated Score	Assessment Strength	Compliance Level
EIF Principle setting the context for EU actions on interoperability	100/100 (100%)	100%	Seamless
Core interoperability principles	1540/1700 (91%)	100%	Seamless
Principles related to generic user needs and expectations	1160/1200 (97%)	100%	Seamless
Foundation principles for cooperation among public administrations	480/500 (96%)	100%	Seamless
Interoperability layers*	880/1000 (88%)	100%	Seamless
Overall Score	3060/3400 (90%) ¹⁵	100%	

**The technical interoperability layer is covered by the criteria corresponding to the core interoperability principle "Openness".*

With an 100% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 90% (3060/3400) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

¹⁵ See the “results interpretation” section of the 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/results-visualisation-and-interpretation>