European Commission

CAMSS

COMMON ASSESSMENT METHOD FOR STANDARDS AND SPECIFICATIONS

ASSESSMENT SUMMARY v1.0.0

CMS Advanced Electronic Signatures (CAdES)[1]

International Organization for Standardization (ISO)[2]

[1] https://www.iso.org/standard/64756.html

[2] https://www.iso.org/home.html

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

TABLE OF FIGURES

1. INTRODUCTION

The present document is a summary of the assessment of CAdES carried out by CAMSS using the CAMSS EIF assessment scenario. The purpose of this scenario is assessing the compliance of a standard or specification with the European Interoperability Framework (EIF)[3].

2. ASSESSMENT SUMMARY

CAdES is a group of extensions to Cryptographic Message Syntax (CMS) signed data which purpose is to make advanced electronic signatures. It was first introduced in 2005 as CMS Advanced Electronic Signatures (CAdES) on ETSI Technical specifications. In 2008 was introduced in IETF webpage as a copy of the ETSI specification.

2.1. 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 fully supports the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**
  There is no Member State that includes CAdES in their national catalogue with The National Interoperability Framework (NIF) aligned with at least 4 out of 5 sections of the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO)[4] factsheets.

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

- **Openness**
  ISO has defined a clear procedure to develop its standards and all stakeholders have the opportunity to contribute to the development of the CAdES. As defined on the TC standardisation, only ISO members are involved in the development of ISO standards. A review is carried out to arrange the consensus firstly within the TC members and subsequently is reviewed by the different ISO member bodies. Moreover, the specification is not available for free for everyone to study, payment is needed to reach access to the standard. Also, CAdES is not licensed in any (F)RAND or royalty-free basis.
  CAdES has a significant market acceptance which demonstrates that it is mature enough for its use. Moreover, it can be considered an asset to build innovative solutions. The specification has the ISO community that supports the development of: International standards, Technical Specifications, Technical Report and Publicly Available Specification. However, it is not related to the publication of open data.

[3] https://ec.europa.eu/isa2/eif_en

[4] https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets

- **Transparency**

  The purpose of CAdES is not related to the visibility of administrative information, data or services. It is not related to the comprehensibility of administrative information, data or services. Moreover, CAdES is not related to the availability of interfaces with internal information systems.

- **Reusability**

  CAdES is a business domain agnostic specification that can be reused in a cross-domain way. It can apply to any type of transaction. However, it is an ISO standard and as all ISO standards, they have to be paid to access its content. Moreover, there is no national or European platform with the specification CAdES available for free.

- **Technological neutrality and data portability**

  CAdES it is independent of any technology or platform. Moreover, it is independent of any environment so it can be applied to any environment, for example, smart cards, GSM SIM cards or special programs for electronic signatures. The adoption of CAdES as electronic signature for signing online documents does not hamper the scalability of systems. However, the purpose of CAdES is not related to the availability of interfaces with internal information systems.

***The specification does not support the principles related to generic user needs and expectations*:**

- **User-centricity**

  The purpose of CAdES is not related to the implementation of the once-only principle. Therefore, this criterion is considered not applicable to this specification.

- **Inclusion and accessibility**

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

- **Security and privacy**

  CAdES as an electronic signature will proportianate a secure and trustworthy eSignature for the data exchange between citizens and administrations.

- **Multilingualism**

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

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

- **Administrative Simplification**

  The purpose of CAdES is to foster the use of electronic signature. Therefore, it is clear that it reduces the administrative burden by making signing possible electronically.

- **Preservation of information**

  CAdES fosters the long-term preservation of electronic records by allowing electronic signatures remain valid for long period of time.

- **Assessment of effectiveness and efficiency**

  After carrying out information retrieval, no document or study has been found assessing the CAdES in terms of efficiency or effectiveness.

2.2. 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**

  CAdES is already associated with EIRA ABBs in the European Library Of Specifications (ELIS). More specifically, CAdES can define the interoperability aspects of the "e-Seal Preservation Service" and "e-Signature Preservation Service" ABBs of the EIRA Technical View. Moreover, there are many free online tools that performs numerous checking in order to verify the conformity of the ETSI Advanced Electronic Signatures which includes CAdES.

  There are no Member States recommending CAdES in their ICT National Catalogues. CAdES is not included in any catalogue of standards at national level nor at EU level. After searching in the different official European websites, there is no evidence of any cross-border project that use CAdES nor explicit agreements involving the usage of the specification.

- **Integrated public service governance & Legal Interoperability**

  No evidences have been found of the specification being included in a formal interoperability agreement between organisations involved in the European public services provision. Moreover, no assessment verifying the compliance of CAdES with the European standardisation regulation has been found.

- **Organisational interoperability**

  CAdES is not a business process modelling standard or specification and it does not define organisational interoperability aspect. The purpose of the specification is not related to organisational Interoperability.

- **Semantic Interoperability**

  CAdES does not define a cross-sector reusable data model, but defines an electronic signature format. Moreover, it is not related to the publication of public data as linked open data.

- **Technical interoperability**
  This technical interoperability layer is covered by the core interoperability principle ''Openness''.

3. Assessment Results

This section presents an overview of the results of the CAMSS assessments for **CAdES**. 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 are used to calculate the "Automated Score" per category and an "Overall Score".

Category	Automated Score	Assessment Strength	# Favourable	# Unfavourable	# Not Applicable
Principle setting the context for EU actions on interoperability	0%	100%	0	1	0
Core interoperability principles	57%	74%	8	6	5
Principles related to generic user needs and expectations	100%	25%	1	0	3
Foundation principles for cooperation among public administrations	67%	100%	2	1	0
Interoperability layers*	39%	82%	7	11	4
Overall Score	46%	72%	13	15	11

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

With a 72% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 46% demonstrates that the specification barely supports the European Interoperability Framework in the domains where it applies.

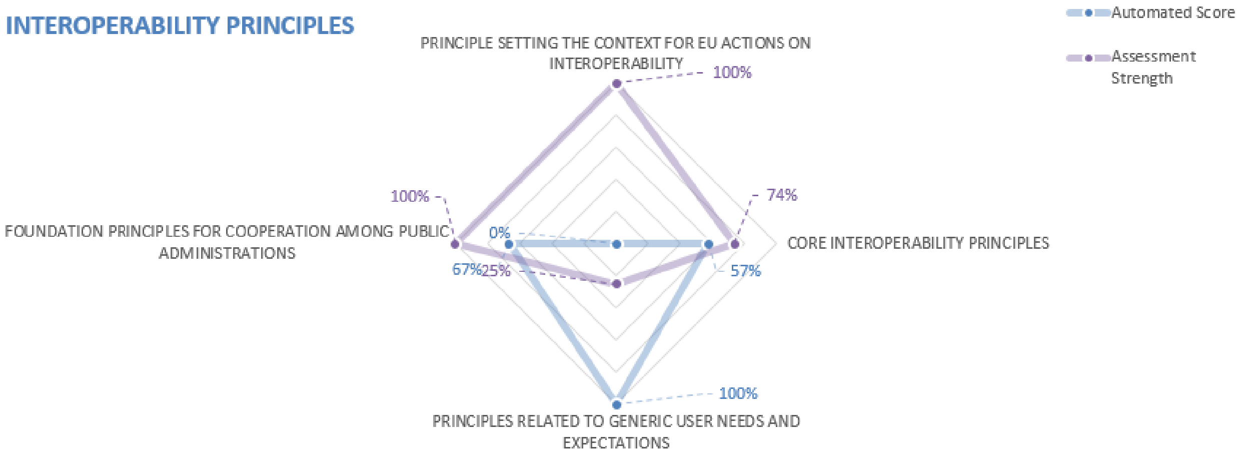

Figure 1. Interoperability principles Results

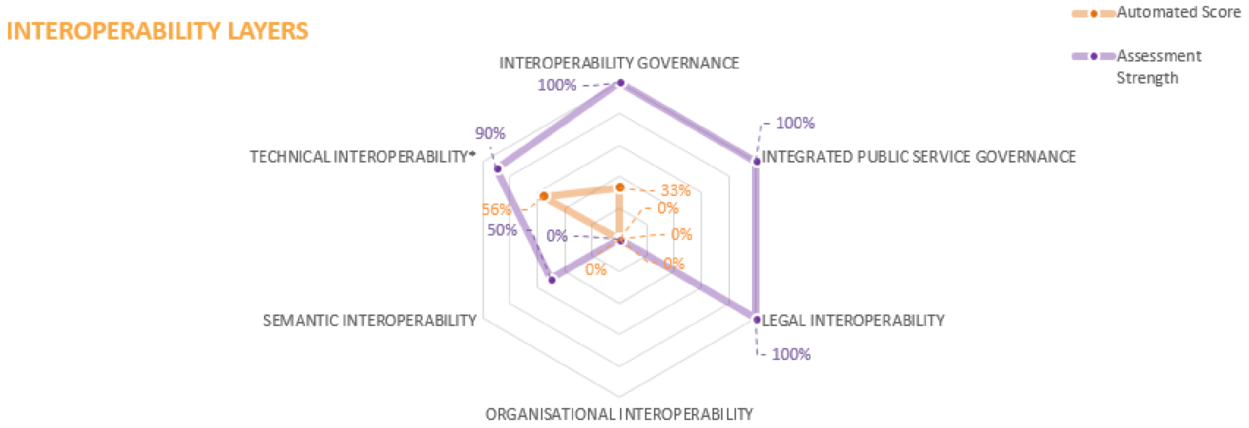

Figure 2. Interoperability layers Results