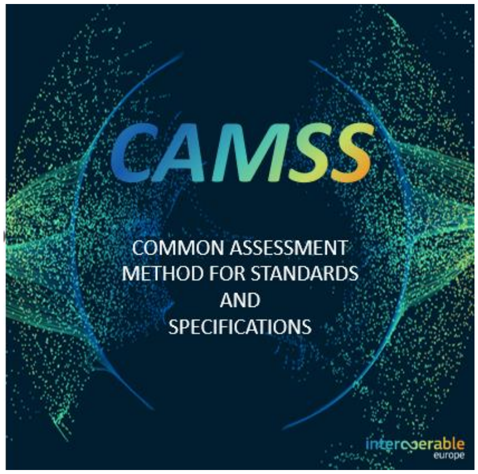
European
Commission



ASSESSMENT SUMMARY v1.0.0

Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation (ETSI TS 119 432)[1]

European Telecommunications Standards Institute (ETSI)[2]

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

[2] ETSI: https://www.etsi.org/

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. Introduction

The present document is a summary of the assessment of **ETSI TS 119 432** carried out by CAMSS using the CAMSS EIF assessment scenario. The purpose of this scenario is assessing the compliance of a standard orspecification with the European Interoperability Framework (EIF)[3].

2. Assessment Summary

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

ETSI is a European Standards Organization (ESO). They are the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. They have a special role in Europe. This includes supporting European regulations and legislation through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

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 specifically addresses interoperability in cloud computing, which can be extremely useful in eGovernment by enhancing data portability, increased efficiency, and integrity.

***The specification does not support the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**

  ETSI TS 119 432 is not included within the catalogue of any Member State.

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

- **Openness**

  ETSI TS 119 432 has two bindings, each one in a different format (XML and JSON). Both of them are machine-readable and ideal for exchanging data between different systems and platforms. This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI)[4]. The participation in the technical group is reserved to ETSI members, who require membership approval. TC ESI has a policy of openly publishing intermediate material (as soon as consensus is reached) to enhance feedback and they typically follow a policy of providing fair, reasonable and non-discriminatory licensing for its standards.

[3] European Interoperability Framework (EIF): https://ec.europa.eu/isa2/eif_en

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

ETSI TS 119 432 is currently in its 1.2.1 version thus, major releases have been published. Annex D of the specification is dedicated to change history while any release related to ETSI TS 119 432 has been published in the TC ESI domain. Furthermore, ETSI TS 119 432 was created as a support for electronic signatures and electronic seals according to the trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation)[5]. Finally, Its development involves contributions from industry experts and collaboration within ETSI working groups. This standardisation body covers the format of digital signatures, as well as procedures and policies for creation and validation. ETSI takes into account the impact of users as they improve their standards and their relevancy.

- **Transparency**

  Remote digital signature protocols often involve interactions between a client and a server. The protocol may include mechanisms for users, verifying the integrity of documents, and ensuring the security of the signature generation process. The protocol for remote digital signature creation aims to scope comprehensibly administrative procedures such as user authentication, authorisation, and key management. Furthermore, the specification actively promotes and supports exposure of interfaces to access the public administration's services as it is completely aligned with eIDAS, a project that allows the European recognition of electronic identities.

- **Reusability**

  The protocol for remote digital signature creation can be domain-agnostic as it can be applicable across various industries and use cases. ETSI TS 119 432 allows customisations to a certain extent. It does allow customisations in the sense that it can be implemented within different IT infrastructures, which allows the specification to be adapted based on integration with existing systems. It is also extensible to the parameters of the protocols it defines. Standards for digital signatures have generally been developed for a long time considering solutions tailored to the characteristics of devices, therefore they could be implemented and/or used in any domain.

- **Technological neutrality and data portability**

  The specification itself is designed to be technology and platform-agnostic as it aims to represent and exchange context information about entities in a machine-readable way. ETSI TS 119 432 specifies generally applicable policy and security requirements for Trust Service Providers (TSPs) implementing a service component operating a remote signature creation device.

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

On the other hand, the protocol for remote digital signature creation itself may not directly address data portability, as its primary focus is on defining the technical procedures for creating digital signatures remotely. However, data portability can still be facilitated as part of the broader digital signature workflow that involves the use of such a protocol. Implementations of the protocol aims for interoperability, allowing digital signatures created using one system to be verified by another. This interoperability helps ensure that signed documents remain portable across different platforms and environments.

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

- **User-centricity**

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

- **Inclusion and accessibility**

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

- **Privacy**

  The protocol aims at supporting electronic signatures and electronic seals, including qualified electronic signatures and qualified electronic seals according to the Regulation (EU) No 910/2014[6]. In addition, section 5 of the specification about confidentiality, security and integrity expresses that the SCASC shall guarantee the integrity and confidentiality of the received information. Furthermore, ETSI TS 119 432 was part of ENISA's 2018 Trust Services Forum[7]. The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.

- **Security**

  The main purpose of ETSI TS 119 432 is to provide the means for a secure and trustworthy exchange of data through digital signatures. It provides a variety of processing models for the correct implementation of the protocol. Specifically, section 7.7 of ETSI TS 119 432 is dedicated to the component for the client application authentication. The specification explicitly addresses and enables data integrity and accuracy with the implementation of digital signatures. In addition, ETSI TS 119 432 foresees enabling access control mechanisms as digital signatures can work as access control mechanisms to private data. The authorised signer's use of its key for signing requires users to provide multiple proofs of their claimed identity before being granted access to the needed set of resources.

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

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

- **Multilingualism**
  Section 7.9 of the specification focuses on the component for language selection. This component shall be used to request a preferred language of the response and shall be specified according to IETF RFC 5646[8]. The service should provide language-specific responses using the requested language. In the case the requested language is not supported then no error shall be raised and the responses shall be produced in the SCS default language.

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

- **Administrative Simplification**
  ETSI TS 119 432 can simplify the delivery of European public services as the EU has made various efforts related to the implementation of digital signatures across all Europe. For instance, eSignature is a set of free standards, tools and services that help public administrations and businesses accelerate the creation and verification of electronic signatures that are legally valid in all European Member States. Besides, it enables digital service delivery channels as an standardised method of creating digital signatures, transactional services such as submitting forms for processing and receiving benefits can be easier to carry out.

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

- **Assessment of effectiveness and efficiency**
  The effectiveness and efficiency of ETSI TS 119 432 is often evaluated through various means, including practical implementation and scalability. For instance, a 2020-paper[9] about learned lessons from implementing an android client for the Cloud Signature Consortium API highlights the ETSI protocol as the one to be respected for communication between SCA/SIC and SSA/SAM. On the other hand, another 2022-paper[10] mentions ETSI TS 119 432 as one of the main components that sustain recent digitisation efforts made by public and private institutions regarding digital signatures.

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.

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

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

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

- 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**

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

  ETSI TS 119 432 is relevant in both national and European scenarios. This specification has been recommended by the Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS)[11]. Furthermore, this protocol may play a crucial role within the practical implementation of the forthcoming Art. 6a (4) (ec) eIDAS2, which stipulates that the European Digitial Identity Wallet (EUDIW)[12] shall offer the ability to create qualified electronic signatures free of charge for non-professional purposes.

- **Legal interoperability**

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

- **Organisational interoperability**

  While ETSI TS 119 432 may not explicitly facilitate the modelling of business processes, the protocol can still play a role within the broader context of it. The protocol can help visualise the flow of documents and information requiring signatures within the context of broader business processes. In addition, ETSI TS 119 432 can facilitate interoperability between organisations by providing a common framework for signature creation and verification. Standards such as XAdES (XML Advanced Electronic Signatures) and PAdES (PDF Advanced Electronic Signatures) define interoperable formats and procedures that enable signatures to be exchanged and verified across different systems and platforms.

- **Semantic Interoperability**

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

[11] ILNAS: https://ilnas.gouvernement.lu/en/service.html

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

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for the **ETSI TS 119 432.** 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
Principles setting the context for EU actions on interoperability	20/100 (20%)	100%	Ad-hoc
Core interoperability principles	1560/1700 (92%)	100%	Seamless
Principles related to generic user needs and expectations	1140/1200 (95%)	92%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	920/1000 (92%)	100%	Seamless
Overall Score	3940/4300 (92%)[13]	96%	

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

With an 96% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 92% (3940/4300) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[13] 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