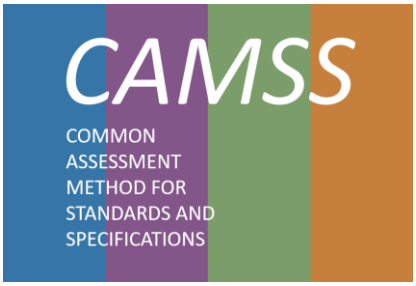

ASSESSMENT SUMMARY v1.0.0

X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP[1]

Internet Engineering Task Force (IETF)[2]

[1] https://datatracker.ietf.org/doc/html/rfc2560

[2] https://www.ietf.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 the **Online Certificate Status Protocol - OCSP** carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is assessing the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. ASSESSMENT SUMMARY

The **Online Certificate Status Protocol (OCSP)** defines a protocol useful in determining the current status of a digital certificate without requiring CRLs (certificate revocation list).

OCSP may be used to meet some of the operational requirements of providing more timely revocation information than is possible with the usual CRL mechanism and may also be used to obtain additional status information. Two examples are high value funds transfers or large stock trades.

The specification has been developed by Internet Engineering Task Force (IETF), which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

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

- **Subsidiarity and proportionality**
  OCSP is included in 1 national catalogue of recommended specifications. It belongs to Spain.
  The National Interoperability Framework (NIF) of this Member States is almost fully aligned with the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO) [5] factsheets.

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

- **Openness**
  OCSP describes the data to be used between an application that checks the status of one or more certificates and the server that provides the corresponding status. Consequently, this specification supports the publication of data as open data. Moreover, OCSP generally uses open-source protocol syntax when determining the status of a digital certificate, such as HTTP and SMTP. The development process has been developed by IETF[6] to make it accessible to the different stakeholders and it also includes a public review. IETF has a formal review and approval

[3] https://ec.europa.eu/eusurvey/runner/EIFScenario_v500

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

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

[6] https://www.w3.org/2018/Process-20180201/#Policie

so that all the relevant stakeholders can formally appeal or raise objections to the development and approval of specifications.

Each distinct version of an Internet standards-related specification is published as part of the RFC (Request for Comments) 2560[7] document series. This archival series is the official publication channel for Internet standards documents and other publications. During the development of a specification, the specification is subjected to several iterations of review by the Internet community and revision based upon experience. These reviews foresee quality, consensus and acceptance, which is a sign of an open and transparent process.

In terms of availability, OCSP is publicly available for free and is licensed under the royalty-free basis for its implementation or study.

- **Transparency**
  OCSP is a protocol useful in determining the current status of a digital certificate without requiring Certificate Revocation Lists (CRLs). The specification addresses data protection but does not make any reference to any transparency process nor relevant regulations at a European level.

- **Reusability**
  The OCSP is publicly available for its use for free at IETF's website. Additionally, even though it was not developed under the scope of the eGovernment System Development, OCSP is meant to serve in the Internet of Things domain and is available for its use within any public administration service, for example in certification processes (e.g., PDF signatures).

- **Technological neutrality and data portability**
  OCSP can be used for large amounts of data without too much risk of hampering the interoperability of systems nor the scalability. This specification specifies the data to be exchanged between an application that checks the status of one or more certificates and the server that provides the corresponding status. This creates a risk of hampering interoperability as OCSP may depend on different transport mechanism, such as HTTP, SMTP or LDAP, when sending an OCSP request in specific rollout scenarios. No evidence was found supporting the evolution of European public services.

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

- **User-centricity**
  The specification is focused on the revocation status of an online certificate, and therefore its purpose does not relate to enhancing the discoverability and reuse by administrations across borders. Moreover, it is not focused on the implementation of the OOP.

- **Inclusion and accessibility**

[7] https://datatracker.ietf.org/doc/html/rfc2560

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

- **Security and privacy**
  OCSP supports trustworthy data exchange by suspending acceptance of the concerned certificates until the responder provides a response. The use of precomputed responses allows replay attacks in which an old (good) response is replayed prior to its expiration date but after the certificate has been revoked. Deployments of OCSP should carefully evaluate the benefit of precomputed responses against the probability of a replay attack and the costs associated with its successful execution.

- **Multilingualism**
  The purpose of OCSP 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**
  OCSP defines a protocol useful in determining the current status of a digital certificate without requiring CRLs (certificate revocation list). Therefore, it can simplify the delivery of any European public service and implicitly reduce the administrative burden.

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

- **Assessment of effectiveness and efficiency**
  After researched whether exist studies or documentation assessing the efficiency and effectiveness, any study or documentation has been found assessing the specification in terms of effectiveness. In terms of efficiency, all the certificate validation services from the Spanish Certification Authorities are using OCSP[8].

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'.

[8] https://www.cert.fnmt.es/en/catalogo-de-servicios/validacion-de-certificados/ocsp (text in Spanish)

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

- **Interoperability governance**
  OCSP can be mapped with EIRA. More specifically, OCSP can define the interoperability aspects of the Trust Registry Component, Trust Registry Service and Trust Registry Provisioning Component ABBs of the EIRA Technical View. Moreover, the specification is recommended and included in the Spanish catalogue[9]. Despite having been included in MS's catalogues, it is not included in any catalogue at European Level. In terms of implementation conformity, there is no available validation tool provided by the IETF, but the specification defines conformance as requirements that can be measured manually.

- **Legal Interoperability**
  The specification does not make any reference to relevant regulations at a European level.

- **Organisational interoperability**
  OCSP helps easing the formalisation of Interoperability agreements. E.g., the Digital Signature Service[10].

- **Semantic Interoperability**
  The purpose of OCSP is not related to defining organisational interoperability aspects.

[9] https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#CATALOGOESTANDARES

[10] https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **OCSP**. 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
Principle setting the context for EU actions on interoperability	100/100	100%	Seamless
Core interoperability principles	2040/2200	82%	Seamless
Principles related to generic user needs and expectations	480/500	40%	Seamless
Foundation principles for cooperation among public administrations	420/500	80%	Seamless
Interoperability layers*	860/1100	73%	Sustainable
Overall Score	3900/4400	75%	

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

With a 75% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 88,63% (3900/4400) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.