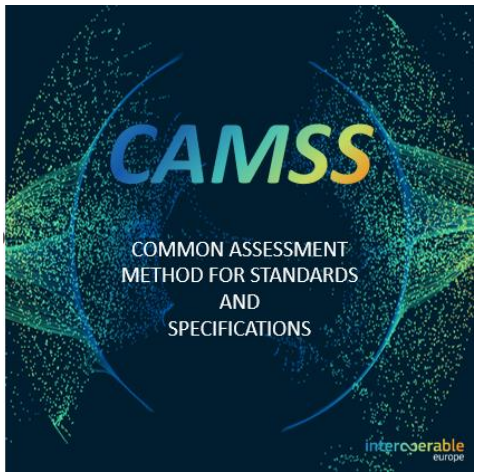

ASSESSMENT SUMMARY v1.0.0

Verifiable Credentials[1]

World Wide Web Consortium[2]

[1]Verifiable Credentials: https://www.w3.org/TR/vc-data-model/
[2] World Wide Web Consortium (W3C): https://www.w3.org/

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 the **Verifiable Credentials** carried out by CAMSS using the CAMSS Assessment EIF Scenario 6.0.0[3]. The purpose of this scenario is assessing the compliance of a standard orspecification with the European Interoperability Framework (EIF)[4].

2. ASSESSMENT SUMMARY

Verifiable Credentials is a specification that provides a mechanism to express credentials (e.g., driver's license or government-issued passports) on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.

Verifiable Credentials are designed to enable the issuance of digital credentials in a way that allows individuals to own and control their credentials, and share them selectively with different entities or parties, like employers, service providers, or institutions.

Verifiable Credentials was developed for the first time in 2017 by the W3C Verifiable Credentials Working Group, and has been evolving until where it is now, in its 1.1 version.

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 Does not support the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**

  Verifiable Credentials is not included in any national catalogue of recommended specifications whose Member State NIF has a high performance on interoperability according to NIFO factsheets.

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

- **Openness**

  Verifiable Credentials help solve problems related to integrity and privacy of personal information on the Web, while incorporating W3C standards. With that in mind, to contribute to the maintenance of the specification a user needs to follow a registration process. The specification is

[3]CAMSS Assessment EIF Scenario 6.0.0: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/release/600
[4] European Interoperability Framework (EIF): https://ec.europa.eu/isa2/eif_en

licensed on a (F)RAND basis and all major and minor releases foresee a public review during which collected feedback is publicly visible. Also, Verifiable Credentials has reached a certain maturity given the number of releases and documentation on its supporting processes.

Thanks to the specification, issuing organizations can generate fraud-proof digital credentials and verifying organizations can instantly check the authenticity of those credentials hence, the specification is being directly used to create innovative solutions in different areas. Furthermore, Verifiable Credentials has the support of the Credentials Community Group, whose mission is to explore the creation, storage, presentation, verification, and user control of credentials.

- **Transparency**

  Verifiable Credentials defines the standard way to present credentials/certificates on the internet in a common digital way therefore, the specification is involved in fostering the comprehensibility, visibility, and exposure of interfaces of Public Administrations data.

- **Reusability**

  This specification refers to the W3C Verifiable Credentials Data Model thus, it is inherently abstract and can be implemented and/or used in any domain as long as it fulfills the requirements. Therefore, its use goes beyond a specific business domain.

- **Technological neutrality and data portability**

  The specification is independent from any software, hardware, or operating system. Therefore, it can be said that Verifiable Credentials is technology and platform agnostic. Verifiable Credentials is designed to be modular and flexible, allowing for partial implementations based on specific use cases and requirements. Furthermore, it also allows customization so that users can tailor the structure of the credentials to their specific needs. One of the goals of the Verifiable Credentials Data Model is to enable permissionless innovation. To achieve this, the data model needs to be extensible in several different ways. For instance, it enables data portability by providing them with the means to issue, manage and verify fraud-proof credentials securely and for users to maintain privacy and control over their personal data.

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

- **User-centricity**

  The specification provides mechanisms that support the selective sharing and reuse of relevant information, contributing to more efficient and privacy-preserving interactions in various scenarios.

- **Inclusion and accessibility**

  Verifiable Credentials mentions that it is important to follow accessibility guidelines and

standards, such as WCAG21[5], to ensure that all people, regardless of ability, can make use of this data.

- **Privacy**

  There are details available about the general privacy considerations and specific privacy implications of deploying the Verifiable Credentials Data Model into production environments. Because a verifiable credential often contains personally identifiable information (PII), implementers are strongly advised to use mechanisms while storing and transporting verifiable credentials that protect the data from those who should not access it.

- **Security**

  Given the purpose of this specification, which is to enable organizations and individuals to create and share verified data, the secure exchange of data is explicitly addressed. There is a specific section in the specification that attempts to highlight a broad set of security considerations. The specification guarantees the authenticity and authentication of the role agents involved in the data transactions (issuer and holder) with a verifier. Also, Verifiable Credentials describes mechanisms for ensuring integrity of Verifiable Credentials and similar types of constrained digital documents using cryptography, especially using digital signatures and related mathematical proofs. As a specification created to provide a standard-way to express credentials on the Web, there are several features that ensure the alignment with this definition. Furthermore, the specification does provide an access control mechanism for the credentials.

- **Multilingualism**

  The specification strongly encourages data publishers to read the section on Cross-Syntax Expression in the Strings on the Web: Language and Direction Metadata document to ensure that the expression of language and base direction information is possible across multiple expression syntaxes.

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

- **Administrative Simplification**

  Thanks to this specification, digital documents related to European public services containing information about a person or entity that can be easily shared and automatically verified. Therefore, Verifiable Credentials enable digital service delivery channels as a good asset for digitalisation and administrative simplification.

- **Preservation of information**

  While Verifiable Credentials themselves do not guarantee long-term preservation of

[5] Web Content Accessibility Guidelines 2.1 (WCAG21): https://www.w3.org/TR/WCAG21/

information, their use within a broader framework of standards and data archiving best practices can contribute to the sustainability and preservation of electronic records and information.

- **Assessment of effectiveness and efficiency**

  The effectiveness and efficiency of Verifiable Credentials is often evaluated through various means, including practical implementations, pilot projects, and community feedback. For example, the effectiveness and efficiency of Verifiable Credentials is often evaluated based on its adoption in various use cases and the W3C Working Group has published a collection.[6]

2.1. 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**

  Currently, this specification is not included in the current version of the EIRA Library of Interoperability Specifications (ELIS). Nevertheless, Verifiable Credentials include evaluations of verifiable credentials through a verifiable data registry. This role an entity may perform is the evaluation of whether a verifiable credential or verifiable presentation is an authentic and timely statement of the issuer or presenter.

  Even though only Spain recommends Verifiable Credentials as a specification, it is included in the Rolling Plan for ICT standardisation regarding electronic identification and trust services including e-signatures. In fact, Verifiable Credentials was selected for its use in the European Blockchain Services Infrastructure (EBSI)[7], the first pan-European, public-driven blockchain initiative of its kind where verifiable credentials and verifiable presentations play a major role within the EBSI ecosystem. EBSI VC/VP data models build upon the W3C Verifiable Credentials, which defines the standard way to present credentials/certificates on the internet in a common digital way.

- **Legal interoperability**

  Verifiable Credentials specification does not appear in any of the main European standard

[6] Verifiable Credentials Use Cases: https://www.w3.org/TR/vc-use-cases/

[7] EBSI: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

development bodies. Therefore, the specification is not a European standard.

- **Organisational interoperability**
  Verifiable Credentials' purpose is the secure and privacy-preserving credential exchange therefore, they can play a role in supporting and enhancing the modeling of certain business processes. Verifiable Credentials can play a role in facilitating organizational interoperability agreements, particularly in the context of identity management and secure exchange of private personal data.

- **Semantic Interoperability**
  Verifiable Credentials is developed by W3C, a standard development organisation based in the US, thus, sharing of their data and results in national and/or European platforms is out of their scope. Nevertheless, the specification can contribute to the creation of communities and the sharing of data and results, particularly in the context of digital identity, credentialing, and related applications as they offer a standard for credentials being exchanged, its format, and structure.

3. *ASSESSMENT RESULTS*

This section presents an overview of the results of the CAMSS assessments for **Verifiable Credentials**. 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	1680/1700 (99%)	100%	Seamless
Principles related to generic user needs and expectations	1140/1200 (95%)	100%	Seamless
Foundation principles for cooperation among public administrations	460/500 (92%)	100%	Seamless
Interoperability layers*	780/1000 (78%)	100%	Sustainable
Overall Score	4080/4500 (91%)[8]	100%	

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

With a 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 91% (4080/4500) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[8] 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