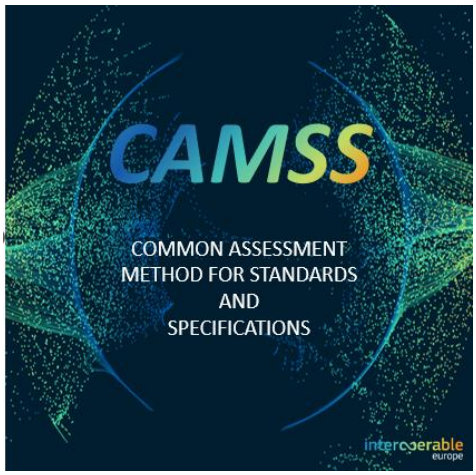

ASSESSMENT SUMMARY v1.0.0

Decentralized Identifiers (DIDs)[1]

World Wide Web Consortium (W3C) [2]

[1] DIDs specification: https://www.w3.org/TR/did-core/

[2] World Wide Web Consortium (W3C): https://www.w3.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 DIDs carried out by the CAMSS Team 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

Decentralized identifiers (DIDs)[4] are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities.

Implementers can create Decentralized Identifiers based on identifiers registered in federated or centralized identity management systems. Indeed, almost all types of identifier systems can add support for DIDs. This creates an interoperability bridge between the worlds of centralized, federated, and decentralized identifiers.

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**

  Decentralized Identifiers (DIDs) is not included in any national catalogue of recommended specifications whose Member State NIF has a high performance on interoperability according to the NIFO factsheets[5]. Despite this, it is recommended by Spain and it is included in the Action plan for the deployment of data spaces[6].

[1] European Interoperability Framework: https://ec.europa.eu/isa2/eif_en

[4] DIDs specification: https://www.w3.org/TR/did-core/

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

[6] Action plan for the deployment of data spaces: https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2024/OdD-Plan_actuaciones_despliegue_espacios_datos_v1-0.pdf

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

- **Openness**
  Decentralized Identifiers (DIDs) is an open specification publicly available for anyone to study or implement, supported by the World Wide Web Consortium (W3C[7]). The W3C has established a transparent process for the development and approval of this specification as a recommended standard. DIDs are licensed on a royalty-free and (F)RAND (Fair, Reasonable, and Non-Discriminatory) basis. The W3C published the first public working draft of DIDs in 2019. Since then, updates have been made, which are accessible on the W3C website. Additional documentation on the supporting processes has also been published to ensure proper change management and release of the content. DIDs are used in Self-Sovereign Identity (SSI) within the eIDAS project[8] and are being implemented in Dataspaces initiatives[9], demonstrating their application in innovative solutions.

- **Transparency**

  Through the use of identifiers, a decentralized and verifiable method for monitoring and managing administrative processes is provided. By associating each step in the administrative process with a DID, these processes can be verified, made more transparent, and become more reliable. Additionally, DIDs are designed to allow individuals and organizations to generate their own identifiers using trusted systems. These new identifiers enable entities to prove control over them by authenticating with cryptographic proofs such as digital signatures, addressing data immutability. Furthermore, public services can offer authentication APIs that accept DIDs and verifiable credentials (VCs) to verify user identities.

- **Reusability**
  The DID specification is highly usable beyond business-specific domains due to its standardized, interoperable, and decentralized nature. Its applications span government, healthcare, education, finance, IoT, and more, providing secure, verifiable, and user-controlled identity management.

- **Technological neutrality and data portability**
  DIDs can be implemented in any platform and it is independent of any technology.
  DIDs allow for extension and partial implementations using optional properties found in DID documents properties. Regarding extensions, the data model supports two tpes of extensibility. Moreover, the creation of a DID is a process that is defined by each DID Method, so DIDs also allow customisation. Furthermore, DIDs enhance data portability, allowing users to seamlessly transfer their identifiers and related data between different platforms.

[7] W3C: https://www.w3.org/

[8] Self-sovereign identity (SSI) in eIDAS project: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge

[9] Dataspaces initiatives: https://www.linkedin.com/pulse/what-data-space-dr-antonio-j-jara-sztrf

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

- **User-centricity**
  DIDs are persistent and can be updated and reusable in many situations. In this way, if the controller of a web page or any other web resource wants to assign it a persistent, cryptographically verifiable identifier, the controller can create a DID. Moreover, in the DIDs document, the author can include the "alsoKnownAs" property pointing to the current URL of the blog, and make DID upgradable.

- **Inclusion and accessibility**
  The purpose of DIDs is not related to e-accessibility. Therefore, this criterion is considered not applicable to this specification.

- **Privacy**
  This privacy architecture prioritizes the protection of personal data. It enables data exchange on a secure, peer-to-peer basis using communication channels identified and secured by verification methods within DID documents. However, for publicly available DID documents, it's crucial to exclude personal data. These documents should focus on non-personal information. For secure transmission of personal data, alternative methods like Verifiable Credentials [VC-DATA-MODEL][10], or service endpoints controlled by the DID subject or controller are recommended.
  Furthermore, the DID Rotation project[11] demonstrates a practical application of this privacy focus. It outlines a process for updating DIDs while ensuring the continuity and integrity of the associated digital identity.

- **Security**
  This specification proposes a privacy-focused architecture that facilitates secure data exchange and processing. Personal data can be exchanged privately on a peer-to-peer basis using secure communication channels identified and verified by methods within DID documents. DID documents play a crucial role in authentication as well. They specify how the DID subject (the entity the DID represents) is expected to be authenticated, for instance, when logging into a website. A particular DID method might determine that authentication as a DID controller (entity managing the DID) is sufficient for actions like updating or deleting the DID document.

  To further enhance security, the architecture incorporates mechanisms to prevent unauthorized DID document changes. One approach involves monitoring and notifying the DID subject of any modifications. Additionally, DID documents can express verification methods, such as cryptographic keys, used to authenticate or authorize interactions with the DID subject or related parties, improving access control.

[10] Verifiable Credentials specification: https://www.w3.org/TR/vc-data-model/

[11] DID Rotation project: https://www.ownyourdata.eu/en/did-rotation/

- **Multilingualism**
  DIDs are globally unique and language-neutral, consisting of an alphanumeric string that remains consistent across different languages. This consistency ensures seamless interoperability, regardless of the user's preferred language.

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

- **Administrative Simplification**
  DIDs empower individuals to control their digital identities, streamlining administrative processes. This eliminates dependence on centralized authorities for identity management and authentication. Citizens can manage their data, selectively share it with different entities, and authenticate themselves using DIDs. This fosters the principle of "digital-first" by placing control directly in the hands of individuals.

- **Preservation of information**
  The purpose of DIDs is not related to long term preservation of electronic records. Therefore this criterion is considered not applicable to this specification.

- **Assessment of effectiveness and efficiency**
  There are existing studies that assess and document the features of DIDs, offering potential improvements in performance and other aspects. The study "A Survey on Decentralized Identifiers and Verifiable Credentials[12]" provides background information on DIDs and VCs, analyzes available implementations, and offers an in-depth review of how these technologies have been employed across different use-case scenarios. Additionally, it presents challenges that hinder their adoption in real-world scenarios and suggests future research directions. The paper "Methods for Decentralized Identities: Evaluation and Insights[13]" evaluates a selection of distributed identity methods, analyzing their properties based on the categorization specified in the W3C recommendation rubric.

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

[12] "A Survey on Decentralized Identifiers and Verifiable Credentials": https://arxiv.org/pdf/2402.02455

[13] “Methods for Decentralized Identities: Evaluation and Insights”: https://eprint.iacr.org/2021/1087.pdf

- **Interoperability governance**

  The W3C Decentralized Identifier (DID) specification demonstrates growing recognition. It's recommended by the Spanish Data Office's Action Plan for data spaces deployment and is associated with the European Interoperability Reference Architecture (EIRA) within the European Library of Specifications (ELIS)[14]. More specifically, DIDs can define the interoperability aspect of the "Blockchain Ledger" ABB of the EIRA Technical View.

  Beyond technical specifications, DIDs are finding practical applications. They are used in Self-Sovereign Identity (SSI) within the eIDAS project, which represents a significant step towards user-centric identity management. Both DIDs and SSI empower users to control their digital identities, fostering autonomy and enabling them to use their identities across various contexts.

  To ensure interoperability, the W3C DID Working Group maintains the DID Test Suite[15], a collection of tests that verify the specification's implementation.

- **Legal interoperability**

  The specification has been developed by W3C, which is a non-European international SDO. Therefore, it can not be considered as an European Standard.

- **Organisational interoperability**

  DIDs address a critical need: enabling individuals and organizations to generate their own identifiers using trusted systems. This foundation of trust empowers cooperation and interoperability between different organizational systems and domains. DIDs achieve this by leveraging their capabilities, such as guaranteeing reliable data exchanges and ensuring compliance with privacy regulations.

- **Semantic interoperability**

  Joinup offers several services that aim to help e-Government professionals share their experience with each other. Joinup supports them to find, choose, re-use, develop and implement interoperability solutions. DIDs appears in many Joinup entries[16] as a discussion topic.

[14] EIRA Library of Interoperability Specifications (ELIS): https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss /solution/elis/release/600

[15] DID Test Suite: https://github.com/w3c/did-test-suite

[16] Joinup DIDs: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for DIDs. 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	Compliance Level
EIF Principle setting the context for EU actions on interoperability	100/100 (100%)	100%	Seamless
Core interoperability principles	1640/1700 (96%)	94%	Seamless
Principles related to generic user needs and expectations	1160/1200 (97%)	92%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	840/1000 (84%)	100%	Seamless
Overall Score	3940/4200 (94%)	93%	

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

With 93% of assessment strength, this assessment can be considered representative of the high specification compliance with the EIF principles and recommendations. The Overall Automated Score of 94% demonstrates that DIDs highly supports the European Interoperability Framework in the domains where it applies.