



ASSESSMENT SUMMARY v1.0.0

Decentralized Identifiers (DIDs)

World Wide Web Consortium (W3C)

Change Control

Modification		Details	
Version 1.0.0			
Initial version			

TABLE OF CONTENT

1. INTRODUCTION..... 4

2. ASSESSMENT SUMMARY 4

2.1. EIF Interoperability Principles.....4

2.2. EIF Interoperability Layers7

3. ASSESSMENT RESULTS 8

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)¹.

2. ASSESSMENT SUMMARY

Decentralized identifiers (DIDs)² 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. Moreover, 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 factsheets³. Despite this, it is recommended by Spain and it is included in the Action plan for the deployment of data spaces⁴.

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

- **Openness**

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

² DIDs specification: <https://www.w3.org/TR/did-core/>

³ NIFO factsheets: <https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory-nifo/nifo-factsheets>

⁴ 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

DIDs is an open specification that is publicly available for everyone to study or implementation, and it is supported by W3C⁵. W3C has a defined and publicly available Process for the Development and approval process of the specification as a recommended standard. DIDs it's also lincensed on a Royalty-free and (F)RAND basis.

W3C DIDs first public working draft was published in 2019. Since then, changes have been made and are available in the W3C web. In addition, different documentation on its supporting processes has been published to ensure the correct change and release of its content.

On the other hand, DIDs is also used in Self-sovereign identity (SSI) in eIDAS project⁶. And it is impelmenting in dataspace initiatives⁷, which evidences its use in innovative solutions.

- **Transparency**

Through identifiers, a decentralised and verifiable way of monitoring and managing administrative processes is provided. If each step in the administrative process can be associated with a did, the processes can be verified and made more visible and reliable. Moreover, DIDs are designed to enable individuals and organizations to generate their own identifiers using systems they trust. These new identifiers enable entities to prove control over them by authenticating using cryptographic proofs such as digital signatures. And it also adresses to immutability of data. Furthermore, public services can offer authentication APIs that accept DIDs and verifiable credentials (VCs) to verify user identity.

- **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 and platform. DIDs allow for extension and partial implementations using optional properties of DID documents properties. For extension, 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 portability, allowing users to seamlessly transfer their identifiers and related data between different platforms.

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

- **User-centricity**

⁵ W3C: <https://www.w3.org/>

⁶ Self-sovereign identity (SSI) in eIDAS project: <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge>

⁷ Dataspace initiatives: <https://www.linkedin.com/pulse/what-data-space-dr-antonio-j-jara-sztrf>

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 give it a DID. Moreover, in the DID 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**

With the privacy architecture suggested by this specification, personal data can be exchanged on a private, peer-to-peer basis using communication channels identified and secured by verification methods in DID documents. Moreover, if a DID method specification is written for a public-facing verifiable data registry where corresponding DIDs and DID documents might be made publicly available, it is critical that those DID documents contain no personal data. Personal data can instead be transmitted through other means such as Verifiable Credentials [VC-DATA-MODEL]⁸, or service endpoints under control of the DID subject or DID controller.

Moreover, it has been found a project covering privacy. The DID Rotation project refers to the process of updating or changing a Decentralized Identifier (DID) while maintaining the continuity and integrity of the digital identity it signifies.

- **Security**

With the privacy architecture suggested by this specification, personal data can be exchanged on a private, peer-to-peer basis using communication channels identified and secured by verification methods in DID documents, improving the secure exchange of data and the secure processing of data. Moreover, the authentication verification relationship is used to specify how the DID subject is expected to be authenticated, for purposes such as logging into a website or engaging in any sort of challenge-response protocol. A particular DID method could decide that authenticating as a DID controller is sufficient to, for example, update or delete the DID document.

On the other hand, one mitigation against unauthorized changes to a DID document is monitoring and actively notifying the DID subject when there are changes. And also for improve the access control, a DID document can express verification methods, such as cryptographic public keys, which can be used to authenticate or authorize interactions with the DID subject or associated parties.

- **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.

⁸ Verifiable Credentials specification: <https://www.w3.org/TR/vc-data-model/>

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

- **Administrative Simplification**

By allowing individuals to control their own digital identities, DIDs can help avoid administrative burden. With DIDs, citizens can manage their own data, share it selectively, and authenticate their identities without dependence on centralized authorities. Moreover, DIDs allows to control digital identities, as well as authenticate identities without dependence on centralized authorities. Therefore, DIDs provides administrative simplification allowing people to manage their digital identities, and also supporting the principle of digital-first.

- **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 already existing studies and documents assessing and documenting DIDs features and providing possible improvements of its performance among other aspects. In "A Survey on Decentralized Identifiers and Verifiable Credentials"⁹ it is provided the background on DIDs and VCs. Moreover, it is analyzed available implementations and offer an in-depth review of how these technologies have been employed across different use-case scenarios. In addition, there are presented some challenges that hinder their adoption in real-world scenarios and future research directions. And in "Methods for Decentralized Identities: Evaluation and Insights"¹⁰ it is provided an evaluation of a selection of distributed identity methods, and it is analyzed 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:

- **Interoperability governance**

The specification is recommended by the Data Office of Spain. Specifically, it is mentioned in the Action plan for the deployment of data spaces. Additionally, the specification is already associated with the European Interoperability Reference Architecture (EIRA) ABBs in the European Library of

⁹ "A Survey on Decentralized Identifiers and Verifiable Credentials": <https://arxiv.org/pdf/2402.02455>

¹⁰ "Methods for Decentralized Identities: Evaluation and Insights": <https://eprint.iacr.org/2021/1087.pdf>

Specifications (ELIS)¹¹. More specifically, DIDs can define the interoperability aspect of the "Blockchain Ledger" ABB of the EIRA Technical View.

Moreover, DIDs is used in Self-sovereign identity (SSI) in eIDAS project. This, is the next step beyond user-centric identity. Both concepts are based on the idea that a user must be central to the administration of his/her digital identity, which requires not only a user's ability to use an identity across multiple locations but also true control over that digital identity, creating user autonomy.

On the other hand, the DID Test Suite¹² performs interoperability tests on the W3C Decentralized Identifier specification and is maintained by the W3C DID Working Group.

- **Legal interoperability**

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

- **Organisational interoperability**

DIDs can be useful for modeling business processes in public administrations. DIDs addresses the need of enable individuals and organizations to generate their own identifiers using systems they trust. Moreover, the specification improves the co-operation and interoperability of different organizational systems and domains taking advantage of the capabilities of dids such as the guarantee of reliable data exchanges or 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 entries¹³ as a discussion topic.

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".

¹¹ EIRA Library of Interoperability Specifications (ELIS): <https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/600>

¹² DID Test Suite: <https://github.com/w3c/did-test-suite>

¹³ Joinup DIDs: <https://joinup.ec.europa.eu/collection/ssi-eidas-bridge>

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 (96%)	92%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	840/1000 (84%)	100%	Seamless
Overall Score	4240/4500 (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.