I-DELTA

Interoperable Distributed Ledger Technology

Deliverable 6.3

Standardization

Deliverable type:	**Document**
Deliverable reference number:	**ITEA| D6.3**
Related Work Package:	**WP6**
Due date:	**31.03.2023**
Actual submission date:	**24.03.2024**
Responsible organisation:	**Mavennet**
Editor:	**Mohamad Jawhar**
Dissemination level:	**Public**

Abstract:	**This deliverable explores the utilization of existing and emerging W3C standards, such as Verifiable Credentials, Decentralized Identifiers (DIDs), and Verifiable Credential API, to achieve interoperability across different systems and platforms. These technologies facilitate secure, privacy-preserving, and decentralized data sharing, ultimately reducing the risk of data breaches and fostering trust. The deliverable also discusses the role of Traceability Interoperability and Vocabulary, which are crucial for establishing standardized ways to track and share information about digital assets' provenance, lineage, and authenticity. The I-Delta project aims to extend these standards and seeks recognition from other standardization bodies like IETF and ISO to drive adoption and enable interoperability across various contexts.**
Keywords:	**Interoperability, data sharing, datahubs, multichain ledgers, W3C standards, Verifiable Credentials Data Model,**

	Decentralized Identifiers, verifiable credential API, JWT, OAuth 2.0, IETF, SCCIT Working Group, ISO, supply chain, digital credential, Linked Data Proofs, privacy preserving, decentralized, traceability, provenance, lineage, digital assets, semantic web technologies, data breaches, centralized identity provider, standards recognition

Editor

Mohamad Jawhar

Table of Content

1. Introduction

The ability to share and trust data across different systems and platforms is critical to achieving interoperability. There are many different potential solutions to achieve interoperability between ledgers, from datahubs, to multichain ledgers, but in most cases they have the challenge that defining the solution and driving adoption to the standard takes many years and technical merit does not always imply success. For i-Delta we chose to leverage and extend existing standards for encapsulation of information in a way that they become verifiable, independently of the creator, holder or verifier of this information. These are W3C standards Verifiable Credentials Data Model , Decentralized Identifiers v1.0, verifiable credential API, in which partner members contributed to throughout the I-Delta project while JWT, OAuth 2.0 are existing well established standards that were utilized throughout the I-Delta project to facilitate communication. In this deliverable, we will discuss the role of these technologies in achieving interoperability.As next steps we are planning for these standards to be recognized by other standardization bodies like IETF, through the SCCIT Working Group or ISO.

2. Key Standards

- Verifiable Credentials Data Model: https://www.w3.org/TR/vc-data-model/
- Decentralized Identifiers: https://www.w3.org/TR/did-core/
- Verifiable Credentials API: https://w3c-ccg.github.io/vc-api/
- Traceability Vocabulary: https://w3c-ccg.github.io/traceability-vocab/
- Traceability Interoperability: https://w3c-ccg.github.io/traceability-interop/
- DID-Method-Web: https://w3c-ccg.github.io/did-method-web/

3. Standards Description

3.1. Verifiable Credentials

Verifiable credentials are a type of digital credential that enables the secure exchange of information between parties without relying on a centralized identity provider. These credentials can be used to verify an entity's identity, qualifications, or other types of information. They are built using the Verifiable Credentials Data Model and can be cryptographically signed by the issuer to ensure their authenticity using Linked Data Proofs or JWTs. They provide an open world semantic data model allowing multiple parties to add semantic meaning to their claims. Verifiable credentials follow a 3 party Issuer, Verifier and Holder model, allowing for privacy preserving mechanisms, and decentralization.

In the supply chain industry for instance, verifiable credentials can be used to verify the authenticity and integrity of products, such as their origin, quality, and compliance with regulations. For example, a manufacturer can issue a verifiable credential that certifies that a product has been produced under certain conditions, such as using sustainable materials or adhering to specific environmental standards. This credential can be shared with other parties, such as distributors and retailers, to verify the product's authenticity and compliance. The credential carries all of the information that is used to provide authenticity in it, and because it imbibes the claims with semantic meaning, makes sure that the Issuer’s intent has not been modified.

Verifiable credentials can be used to establish trust between different systems and platforms by allowing individuals and organizations to share only the information necessary for a particular transaction or interaction. For example, a verifiable credential could be used to verify that an individual is over 18 years old without disclosing their exact birthdate. By using verifiable credentials, organizations can reduce the risk of data breaches and maintain privacy while still enabling data sharing.

3.2. Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) are a type of digital identifier that allow individuals, organizations, and even physical objects to have a unique and persistent identity on a decentralized network. DIDs can be used to verify an entity's identity across different systems and platforms, and unlike traditional identifiers such as email addresses or usernames, DIDs are not tied to any central authority or third-party service provider, but are instead managed by the entities themselves using distributed ledger technology (such as blockchain) or other decentralized systems.

DIDs are designed to be globally unique, persistent and resolvable. This means that once a DID is created, it can be used to identify an entity across different systems and networks, and the DID itself can be used to retrieve information about the entity it represents. The individual or organization that controls the DID has complete control over their own data and can prove control over them by authenticating using cryptographic proofs such as digital signatures.

3.3. Verifiable Credential API

The verifiable credential API is an open standard that provides a way for applications to access and verify verifiable credentials. The API can be used to verify that a credential is valid, check the issuer's signature, and verify that the credential has not been tampered with. The API can be used with a wide range of applications and systems, making it an ideal tool for achieving interoperability.

By using the verifiable credential API, organizations can ensure that the verifiable credentials they receive are valid and trustworthy. This reduces the risk of data breaches and enables organizations to share information securely across different systems and platforms.

3.4. Traceability interoperability and vocabulary

The specification extends the core Verifiable Credential API definitions described in the VC-API specification and proposes a set of requirements and guidelines for implementing a decentralized, interoperable, and privacy-preserving system for traceability. This specification should enable different actors to trace the lifecycle of digital assets across different platforms and domains, and to verify their authenticity, integrity, and attribution.

The purpose of the "Traceability Interoperability" specification is to establish a standard way, particularly in supply-chain for different systems to track and share information about the provenance or lineage of digital assets, such as credentials or certificates. This includes information such as where the asset came from, who created it, and how it has been modified over time.

The "Traceability Vocabulary" specification aims to define a set of terms and relationships for expressing traceability information using semantic web technologies. It provides a vocabulary that can be used to describe traceability in a consistent and standardized way. By using a common vocabulary, different systems can more easily exchange and understand traceability information.

4. Summary

Verifiable credentials, decentralized identifiers, and verifiable credential API are critical tools for achieving interoperability. These technologies enable secure and trustworthy data sharing without relying on a centralized identity provider. By using these tools, organizations can reduce the risk of data breaches, maintain privacy, and establish trust between different systems and platforms. As these technologies continue to evolve, they will play an increasingly important role in achieving interoperability in a wide range of contexts. As next steps we are planning for these

standards to be recognized by other standardization bodies like IETF, through the SCCIT Working Group or ISO.