Decentralized Identity Interop Profile (DIIP)

Decentralized Identity Interop Profile (DIIP)

An increasing number of organizations are recognizing the potential of Self-Sovereign Identity (SSI) and are developing ideas and pilot projects. However, the significant fragmentation of identity systems and chains has resulted in the emergence of multiple decentralized solutions that cannot communicate with each other.

Interoperability is essential

Interoperability is essential and should be ensured at the outset of various developments. This can be achieved by adopting the same set of standards, known as a Technical Interoperability Profile (hereinafter referred to as "Interop Profile"). Therefore, the DBC is collaborating with partners to create the Decentralised Identity Interop Profile (DIIP).

Why DIIP?

Collaboration is crucial when it comes to an Interop Profile. However, the adoption also depends on the knowledge, skills, and architecture of organizations. While Interop profiles already exist, field exploration reveals that they do not adequately align with the current knowledge and capabilities of organizations.

In the establishment of the Decentralized Identity Interop Profile (hereinafter referred to as "DIIP"), we have, therefore, opted for the most user-friendly profile to facilitate the introduction of SSI. This approach enables organizations to swiftly understand the potential benefits of SSI and accelerate its adoption. These components have been carefully selected to seamlessly align with the European Reference Architecture of eIDAS. Furthermore, they can be easily further developed. In the future, we anticipate transitioning to more advanced standards, with the transition being documented in a future version of DIIP.

DIIP: Form follows Function

DIIP does not claim to be comprehensive for every use case. Given that we have not fully mapped out the extent of the systemic changes that SSI will entail, creating a comprehensive Interop profile to support all future use cases is a complex endeavor. Such an attempt could prematurely lock us into specific standards, potentially stifling innovation. For this reason, we adopt the principle of "Form Follows Function," inspired by Louis Sullivan, for DIIP.

The "Function" of this profile is to provide a user-friendly starting point for SSI implementation and data exchange with other parties. Consequently, the "Form" of DIIP exhibits a straightforward structure that aligns with the knowledge level of developers and architects, catering to most fundamental use cases. However, in the coming years, more advanced use cases are likely to emerge, potentially necessitating different requirements for the "Form."

Within the governance team responsible for upholding the profile's integrity, decisions will be made to expand DIIP to ensure that the new "Form" is also interoperable with other DIIP-based use cases. Thus, DIIP will gradually evolve in tandem with developments in technology and demand from applications.

How Does DIIP Relate to the ARF?

In February 2023, the European Union unveiled the initial version of the Architecture Reference Framework (ARF). On Github, all the standards that EU member states must and may apply in the development of a wallet compliant with the eIDAS 2.0 guidelines are documented. This marks a significant step towards European interoperability. The ARF distinguishes between two types of configurations: Type 1 and Type 2.
Type 1 is mandatory and complies with the requirements for exchanging data with a high Level of Assurance, including Personal Identification Data (PID), which represents the digital version of your identity document. Type 2 is optional and offers more flexibility than Type 1, enabling use cases with a lower Level of Assurance (LoA). Both configurations incorporate both ISO standard 18013-5 and the W3C standard for Verifiable Credentials based on JSON and JWT(SD). Additionally, the Type 2 configuration allows for JSON-LD Verifiable Credentials.

The ISO standard is employed within the ARF for the "Proximity" flow, which involves presenting digital credentials to someone in the physical world. The W3C standards are utilized for the remote flow through OpenID4VCI/P and SIOP to present your data online. DIIP thus aligns with the ARF's requirements for the remote flow, ensuring that any use case developed using DIIP will also function within the eIDAS 2.0 infrastructure. Furthermore, we have incorporated several components into DIIP that are not yet specified in the ARF, such as a revocation mechanism and means to identify forms on websites and organizations. Our exploration of use cases has revealed that these components are indispensable, hence adhering to the principle of "Form Follows Function."

DIIP Governance

An incrementally evolving Interop profile that adapts to the requirements stemming from use cases necessitates a robust governance structure. Without such governance, there is a risk of individuals creating their own add-ons to the profile, which may no longer be interoperable with the rest. Consequently, we have established a community governance model, wherein there is no central body making decisions regarding the inclusion of elements in the Interop profile. Parties actively involved with DIIP have a say in the decision-making process. During **DIIP meet-ups**, we discuss the elaborated use cases and identify missing functionalities. A (portion of the) community then investigates how to fill the gaps in functionality. This process takes into consideration interoperability with the rest of the profile, the potential reusability of the form for other applications, and the compatibility of the proposed standard with expected developments. Once a new addition is ready, it is incorporated into DIIP, accompanied by an explanation of the functions that the new addition is intended to support. In cases where competing components exist, reasons for their non-inclusion are articulated.

What Components Comprise DIIP?

DIIP consists of seven standardized open-source components with a maturity level ranging from medium to high. These components enable the majority of basic use scenarios in the field of SSI. While it is possible to select additional components, scenarios involving extra components are not interoperable within this profile. If you require more features for your use case, we invite you to present it to the DIIP community so that we can collectively determine how to accommodate the necessary functionality in a way that benefits other use cases as well.

DIIP Components:

1. OpenID for Verifiable Credential Issuance
2. OpenID for Verifiable Presentations
3. SIOP V2
4. DIF Presentation Exchange
5. W3C Verifiable Credential JWT
6. DID methods: DID:WEB and DID:JWK
7. Signature types ES256
8. Revocation method: StatusList 2021

For a comprehensive description of these components, please refer to our **GitHub** repository.

Which Providers Are Compatible?

Both Sphereon and Animo support this Interop profile and have made their wallet solutions compatible with DIIP. We hope that more providers will follow suit, and we are in discussions with various parties to facilitate this.

Who Is Involved in the development of DIIP?

DIIP was initiated by the Dutch Blockchain Coalition (DBC). The first version was developed collaboratively by the DBC in partnership with TNO, Animo, and Sphereon. It is an open initiative that welcomes participation and utilization from anyone interested.

Who Is Currently Using DIIP?

The DBC and the aforementioned parties will adopt DIIP as a standard in new projects involving SSI. For example:

- Company Passport
- Future Mobility Data Marketplace
- Salt Logistics

Examples

One example is the DBC website itself. Since the annual DBC Conference in June, attendees can log in to the website using a compliant SSI wallet and a "DBC Conference Attendee" credential. This login grants access to the DBC Zone, a restricted section of the DBC website. Within the DBC Zone, you will find a DIIP page with more detailed information about DIIP, examples, GitHub repositories, and data for meetups. Interested in trying it out? Click on "**Log in**."

How Can I Get Involved?

To join DIIP, please contact the SSI lead of the DBC, Alexander van den Wall Bake, via email at **alexander.vandenwallbake@dutchblockchaincoalition.org**.

Note: DIIP was formerly known as DDIP.

SSI Explainer

SSI Explainer

Alexander van den Wall Bake
Lead Self-Sovereign Identity (SSI)