IDunion ToIP Utility case study

Published October 2020

Background Context

The IDunion consortium (formally known as SSI for Germany) is a public private partnership of companies and institutions, which implement and govern the IDunion utility.

The IDunion utility is intended to serve organizations that desire to participate in the digital trust ecosystem and require an enterprise grade governance framework that will:

- Establish an European Association as governing entity.
- Establish a dualistic structure with a management and supervisory board to enable separation of powers.
- Enforce permissioned-write access with contractual instruments that will conform to privacy regulations with focus on GDPR.
- Enable use-cases with a substantial level of assurance as specified in eIDAS.
- Maintain financial sustainability of the governing entity by membership fees and other potential income sources, which are currently evaluated.
- Require adherence to specified open standards and protocols.

In this context it is important to note that the network is operated as a test environment. While the whole environment is intended to have a productive character including the necessary legal contracts, the interactions with the ledger currently have limited legally binding obligations and consequences for the parties involved.

Stakeholders / Persona

The following subjects are stakeholders to the utility:

- The **consortium members** are: Main incubator GmbH, Robert Bosch GmbH, Bundesdruckerei GmbH, esatus AG and the Technical University of Berlin.
- The consortium includes several **associated partners** including: The Federal Office for Migration and Refugees of Germany; Ministry of Commerce, Innovation, Digitalization and Energy of the state of North-Rhine Westphalia;

BWI GmbH; Berlin Senate Department for Economics, Energy and Public Enterprises; Deutsche Börse AG; regio iT gesellschaft für informationstechnologie mbh; Verband der Vereine Creditreform e.V.; Commerzbank AG; Deutsche Bahn AG; The City of Cologne; ING Germany; Telekom Innovation Labs (Deutsche Telekom AG); Siemens AG; Bank-Verlag GmbH; GS1 Germany GmbH, Festo SE & Co KG;
- **Further partners** will join the consortium for the next phase of the project, however the necessary contracts still have to be signed.
- The project is supported and funded by the Federal Ministry of Economics and Energy of Germany. More information can be found [here](#).
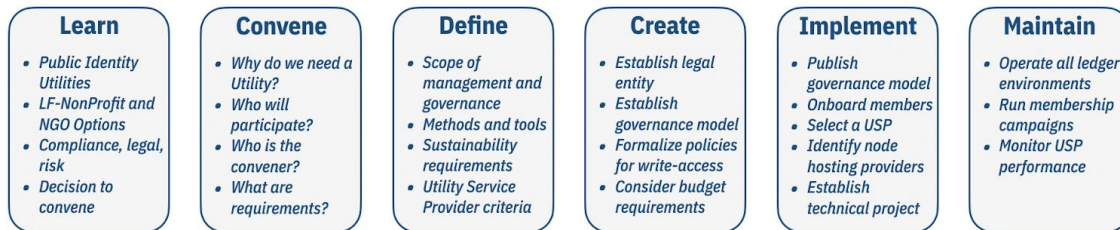
This utility story is convened by:
- Adrian Doerk (Convener): Head of Communication at the IDunion consortium, employed at the consortium leader main incubator GmbH.
- Helge Michael (Convener): Head of the IDunion project, employed at the consortium leader main incubator GmbH
- Dr. André Kudra (Convener): CIO at the esatus AG, Chair of the Utility WG at ToIP
- Anna Kathrin Pfeiffer (Convener): Head of legal / regulatory audit at the IDunion consortium, data protection officer (DPO) at the esatus AG.

User Stories

1. The companies and institutions mentioned above share a common business need for a public identity utility and decided to collaboratively explore the viability of a utility with a strong focus on the regulatory requirements of the European Union.
2. The consortium was selected for a government grant for the innovation competition "Showcase secure digital Identity" by the German government.
3. The consortium members established legal agreements for their collaboration, the use of software licences as well as for the roles within the network (Trustee, Steward, Endorser, Transaction author)
4. The stakeholders come together in several working groups according to the defined deliverables to work on the technical implementation, governance framework, regulatory aspects, communication, security, usability and use-cases.
5. The consortium members started a test network to implement the first use-cases.

Utility Foundry Workflow

Learn	**Convene**	**Define**	**Create**	**Implement**	**Maintain**
• *Public Identity Utilities* • *LF-NonProfit and NGO Options* • *Compliance, legal, risk* • *Decision to convene*	• *Why do we need a Utility?* • *Who will participate?* • *Who is the convener?* • *What are requirements?*	• *Scope of management and governance* • *Methods and tools* • *Sustainability requirements* • *Utility Service Provider criteria*	• *Establish legal entity* • *Establish governance model* • *Formalize policies for write-access* • *Consider budget requirements*	• *Publish governance model* • *Onboard members* • *Select a USP* • *Identify node hosting providers* • *Establish technical project*	• *Operate all ledger environments* • *Run membership campaigns* • *Monitor USP performance*

Learn

- The used international standards and frameworks were examined independently by several consortium members between 2017-2019.
- Several consortium members independently determined Hyperledger Indy to be the most suitable open-source framework for the implementation of a public utility.
- While the concept of SSI offers multiple benefits for companies, institutions and individuals alike, the concept needs to be evaluated according to its suitability with European values and existing regulatory frameworks.
- Evaluation of existing governance structures such as the Sovrin Governance Framework (SGF) and the European Blockchain Service Infrastructure (EBSI) among others.

Convene

- The IDunion consortium is convened by the research and development unit of Commerzbank AG, the Main Incubator GmbH, which conducts research and development of SSI solutions since 2017.
- The Main Incubator GmbH already worked closely together with other consortium partners within the Lissi project before and a continued collaboration for the application of the government grant was a natural fit.
- The consortium had a kick-off event with all consortium partners and associated partners at the beginning of June 2020 and continues to hold regular meetings in the different working streams.
- The application for the German innovation competition "Showcase secure digital identities" serves as guidance for the deliverables and working streams for all members.

Define

- Definition of the roles required to run the network (Trustees, Stewards, Endorser, Transaction Author)

- Creation of a report regarding the examination of the legal compatibility of the solution with GDPR, eIDAS and other German regulatory requirements (Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) , IT-Sicherheitsgesetz (ITSiG))
- The IDunion governance body requires a legal entity. Several possibilities were examined and compared with the support of an external legal advisory firm. A european cooperative was selected to be the most suitable type to fit the needs of the diverse stakeholder group and to convey European values.
- Definition of the open-source framework hyperledger Indy for the implementation of the public utility.
- Creation of a report on interoperability with other European solutions. The report outlines how interoperability with other identity networks (e.g., MeineSichereID, Findy or Sovrin) can be ensured. Open source projects, such as Hyperledger Indy and Aries, are also highlighted, which are strongly intertwined with the intended network of the overall project.
- Identification of crucial regulatory topics, especially the conformity to GDPR and eIDAS. While the utility is believed to be GDPR compliant, there are several details, which still need to be confirmed with regulatory authorities.
- To be allowed to act as an node operator within the IDunion test network, a legal entity is required to:
  - Join the consortium as an associated member with the associated legal contracts
  - Pay for all expenses of the operation of the node on their own behalf.
  - The approval has been granted by the consortium members on a case-by-case basis.
- Defining critical cybersecurity issues by analyzing used standards, protocols, methods and algorithms as well as their implementation.
- IDunion relies on international standards to build the identity network and agent software. The following standards are core components:
  - Verifiable Credentials as specified by the W3C[1]
  - Decentralized Identifiers (DIDs) as proposed by the W3C[2] with the usage of anywise and peerwise DIDs.
  - DIDcomm Messaging Protocol[3] as specified by DIF for the communication between Agents.

  These standards are especially oriented towards interoperability between future identity solutions.

---

[1] W3C, Verified Credentials Data Model 1.0
[2] W3C, Decentralized Identifier v1.0 - working draft
[3] DIF, DIDComm Messaging Specification

Create

- Planning of the creation of an European cooperative. For this purpose, appropriate contracts are currently set up and under review of specialized law consultancies (as of October 2020).
- Established workflows for the governance of processes, policies and technical matters previously defined.
- Policies defining the rights of the different roles have been formalized in an authorization map.
- Different business model options have been evaluated. A final decision has yet to be made.

Implement

- A technical working stream was started to determine the technical components required to establish a test-network with several node operators.
- The consortium members already had experience with running nodes for distributed public utilities based on Hyperledger Indy, however to set up an own network required further exploration and communication.
- A launch ceremony was held to start the test network. The genesis file includes nine nodes. Further nodes were added the following weeks. The event was captured as Video (3:45 min) and as press-release.
- Node operators either choose a third-party cloud provider or run the node within their own IT-infrastructure.
- The governance model is further developed and consists of multiple documents.
- Endorser contracts were formulated so third-parties, which are not (associated) members of the IDunion consortium, can write on the permissioned ledger.
- Hyperledger Indy block explorers were set up to monitor the network. One is hosted by the esatus AG and one by British Columbia.
- More than 30 different use-cases are currently explored as pilot projects. The use-cases are clustered in different ecosystems: eCommerce, eGovernment, industry, eHealth, finance, identity and access management (IAM), IoT and mobility.

Maintain

- The test-network will be continuously used to run pilot use-cases and experimentations.
- The start of a productive implementation is planned for 2021