

SSI eIDAS Legal Report

The purpose of the SSI eIDAS Legal report is to show how eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market.

Introduction on SSI

By **digital identity**, we refer to the techniques that allow people and organisations to identify themselves and act on networks, using more or less strong authentication mechanisms.

An important property of digital identity is that it sometimes allows authentication; that is to say, the possibility that we associate technical means that allow us to demonstrate who we are on the Internet and that we act on one of our identities: these are “active” identities, unlike our “passive” identity information or that reside in databases.

Digital identity technologies have evolved significantly in the last 25 years, including hierarchical public key infrastructures and federated, user-centric, delegated authentication.

Digital identity management systems based in **distributed ledger technologies (DLT)** may play an important role in the implementation of a personal right to identity, with a strong view on self-determination and personal autonomy, at least when we refer to natural persons.

One of the interesting use cases of DLT refers to the so-called **self-sovereign identity (SSI)**, which is the one created and managed by each person individually, without the intervention of third parties. SSI has been proposed as the next step in the evolution of identity management, and is supposed to increase subject’s electronic privacy, because it reduces two of the main risks associated with authentication delegation systems. Namely, the possibility of identity theft with respect to data managed by the identity provider, and, more importantly, the monitoring of user behaviour by the identity provider, that have access to authentication transaction metadata, something that allow the creation of user profiles.

eIDAS regulation – the Trust Framework

Creation of trust in Internet transactions has been identified as one of the main needs for the proper functioning of the Information Society and, from the perspective of the European Union, of the Digital Single Market. The eIDAS Regulation constitutes the main trust framework in the European Union and the European Economic Area for natural and legal persons in the Internet.

eID and trust services are buildings blocks of the Digital Single Market, allowing the establishment of cross-border electronic relationships in the e-Government field. Designing SSI solutions aligned with the eIDAS Regulation is a key identified need: minimum disclosure, full control and necessary proofs requirements must be legally enabled; that is, backed up by the necessary or applicable legal framework to protect both the subject and service providers, either public or private.

Legal scenarios and recommendations to leverage SSI with the eIDAS regulation

The objective of this report is to evaluate the potential legal issues that are important to an SSI solution and make some recommendations to be used as policy input for the eIDAS 2020 review. The report outlines short-term objectives, where changes in the Regulation would not be necessary, but also mid to long-term scenarios requiring major changes in the Regulation to comply with the SSI design principles.

The different scenarios described in the report are aligned with the proposed architectural and procedural considerations designed in the SSI eIDAS Bridge project and the European Self Sovereign Identity Framework (ESSIF) use case of the CEF Blockchain building block, EBSI.

Very short-term scenarios

- Use notified eIDs to issue Verifiable Credentials (VCs).
- Use qualified certificates to sign/seal VCs with the eIDAS Bridge.
- Use current eID nodes to issue SAML assertions based on a VC/VP (Verifiable Presentation).

Short-term scenarios

- Adopt new eID technical specifications based on ESSIF for identification.
- Issue qualified certificates based on a Decentralised Identifier (DID) method + VC specification.

Mid to long-term scenarios

- Adopt new eID technical specifications based on ESSIF for identification.
- Issue qualified certificates based in a DID method + VC specification.
- Regulate identity hubs as a trust service, in support of the Once Only Principle (OOP).
- Regulate delegated key management (wallets) as an independent trust service.
- Regulate specific type of DLT/node as a trust service.

SSI compliant – trust
framework for eIDAS

Trust Services

- This legal report was carried out by Dr. Ignacio Alamillo Domingo, Lawyer, CISA, CISM, researcher at iDerTec (University of Murcia)
- This work has been co-funded by the ISA² and CEF Digital programmes, in the context of the SSI eIDAS Bridge project, and the European Self-Sovereign Identity Framework (ESSIF) of the European Blockchain Services Infrastructure (EBSI).

Visit the [joinup](#) site to know more about the SSI eIDAS bridge, or the [EBSI](#) page to know more about ESSIF.

Want to read the full report?



SCAN ME

ISA²



CEF Digital
Connecting Europe