SSI Explainer

Self-Sovereign Identity (SSI) is a movement aimed at introducing trust, autonomy, and privacy into the digital realm. **This is not a straightforward task**. The introduction of SSI represents a systemic change that requires many parties to reorient their thinking, adapt to new technologies, and shift their perspective on relationships (both in terms of their relationship with customers or citizens and with competitors, suppliers, ecosystem partners, etc.). Such a significant transformation also comes with an entirely new vocabulary. This page endeavors to explain the most common concepts and directs readers to other sources for further information.

How SSI Works: The Triangle of Trust

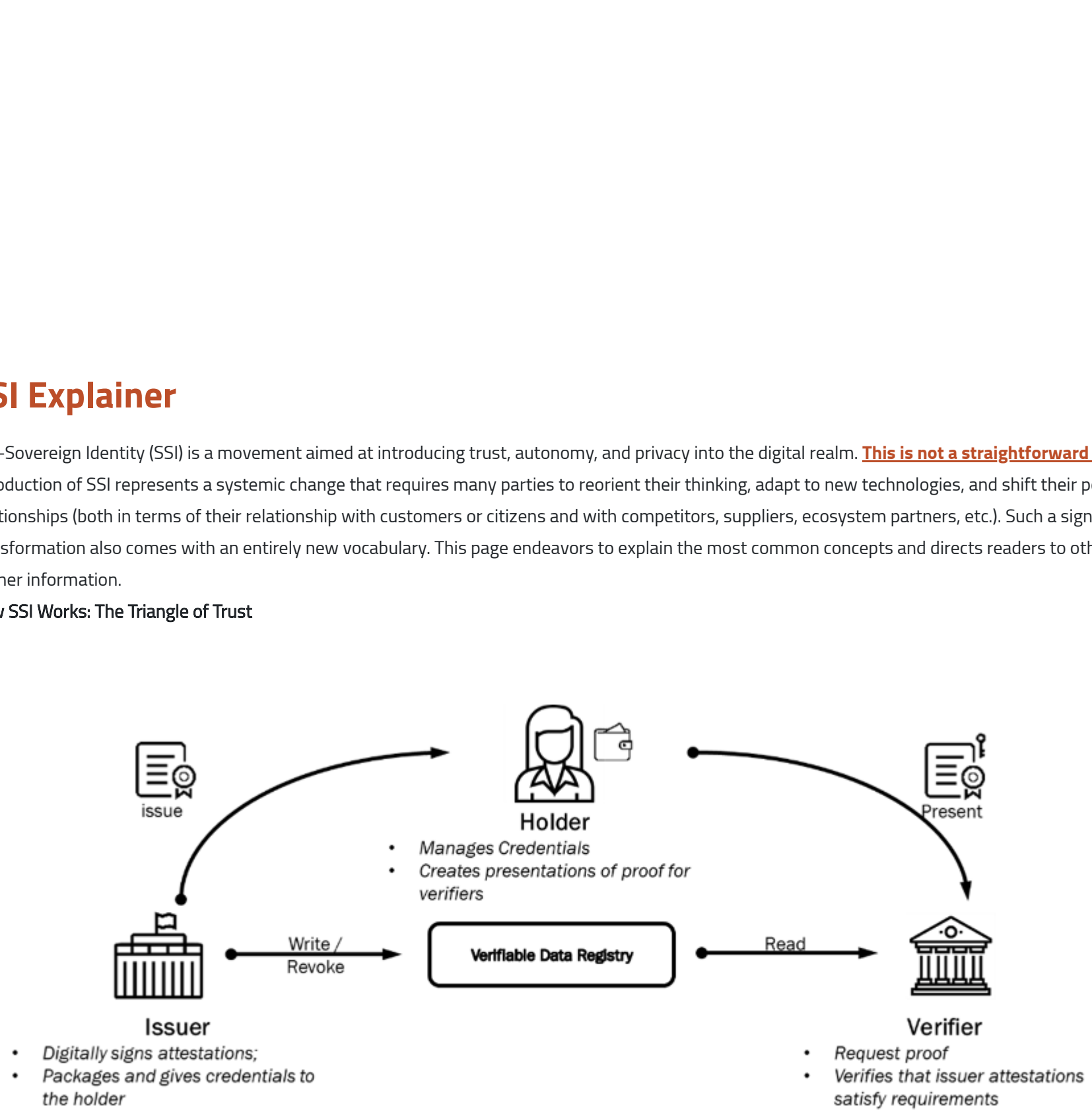

Image 1. The Triangle of Trust: How does the exchange of credentials work with SSI?

The Triangle of Trust elucidates the fundamental process of how data from an Issuer (or issuer) in the form of credentials reaches a Verifier (or requester, also known as a Relying Party). Unlike traditional digital data transfer where the Verifier retrieves data directly from the Issuer, the subject of the data (the Holder) controls the data transfer.

The Holder seeks data from the Issuer, such as a driver's license, diploma, or doctor's prescription. The Issuer signs and seals these data (both using cryptographic techniques), after which the Holder can retrieve and store them in their wallet (also known as a digital wallet). The Issuer may also place an attribute in a register (Verifiable Data Registry) to indicate the validity of the data. This attribute contains no information about the data or the subject of the data. If the Issuer wishes to revoke the issued credential (e.g., revoking a driver's license after a serious traffic violation), the Issuer revokes the validity statement in the Verifiable Data Registry.

When the Holder intends to engage in a transaction with another party, this party becomes the Verifier. For example, when someone wishes to rent a car, and the rental company requests the driver's license. The Holder then presents these data to the Verifier, including the cryptographic information that verifies the accuracy of the data. The Verifier can check in the Verifiable Data Registry to confirm that these data are still valid and have not been revoked.

The Terminology

The concept of Self-Sovereign Identity (SSI) introduces its own terminology. For explanations of these terms, we refer you to the glossary provided by the **ESSIF lab**. You can also find numerous other informative models there to deepen your understanding of SSI.

What is a Technical Interop Profile?

A Technical Interoperability Profile is a set of technical protocols and standards to which various parties have committed themselves. This ensures that the data issued for a specific use case is also usable in other use cases that adhere to the same Technical Interoperability Profile. In this context, the DBC has initiated **DIIP**.
If you have questions about a concept or term and would like to learn more, please contact Alexander van den Wall Bake at **alexander.vandenwallbake@dutchblockchaincoalition.org**.

No messages were found. Please try again later!

Contact

Dutch Blockchain Coalition

070-4190309

info@dutchblockchaincoalition.org

o.v.v. Victor van der Hulst

An initiative of

Ga direct naar

Dutch Digital Delta

Use cases

Dutch National Blockchain Course

About us