An introduction to identities, claims, and endorsements on the iov42 platform

The Current State of Digital Identities

Individual digital identities currently tend to be weak, as they are often based on email addresses and have little tangible link with other identity attributes, such as an individual's name, address, or date of birth. Moreover, there is usually little or no link between the physical representation of an identity (e.g. a driver's license) and a digital one.

What does an identity look like on the iov42 platform?

Trusting an identity is completely subjective and is based on the intended use. The requirements for establishing trust in an identity can be thought of as sitting on a sliding scale—starting at remaining anonymous all the way to completing a full KYC process.

For example, setting up a social media account often takes little more than providing an email address and password. On the other hand, if you want to set up a bank account, you will likely have to provide a government-issued I.D., some proof of residence, and some sort of taxpayer identification number, in addition to completing the paperwork from the bank. The iov42 identity model has been designed to accommodate this flexibility. This enables an identity subject to decide which claims they wish to make about their identity, and, more importantly, which claims they would like to share with others.

This is possible by representing identity as an identifier that has associated claims, such as those listed in the image to the right.

What are claims?

A claim can be any piece of information that asserts some fact related to a given identity. For example, my name is Joe Bloggs. I claim that:

- I was born on the first of January, 2000;
- I am a Swiss citizen;
- I work at iov42; and
- I live in Zurich.

When Joe Bloggs makes a claim about his identity, this claim is stored as a hash of the claim against his identity within the iov42 network. However, by itself, a claim is not very useful in contributing to the trust in an identity, since the identity holder could make a claim about pretty much anything. The key to building trust in any claim is to have it endorsed by third parties.



What are endorsements and how are they captured on the iov42 platform?

On the iov42 platform, endorsements are captured by the use of cryptographic signatures.

An endorsing party, independent of the identity holder, can endorse an identity's claim. The trust conveyed to a claim is dependent on who the endorsing party is and whether their identity contributes to the validity of the claim. For example, you would expect that the endorsement of your nationality by the Passport Office would convey a high level of trustworthiness for that particular claim, whereas the same endorsement by your hairdresser would not have the same level of trustworthiness.

Once an endorsing party signs a claim, it is submitted to the iov42 network, where it goes through consensus for validation. Once validated, the claim and related endorsement are added to the identity to enable a richer expression of the identity, which can later be used to assert trust in trusted transactions.

