PATTERN 02 - Verifiable Credentials, “the digital wallet”

What is the pattern about?

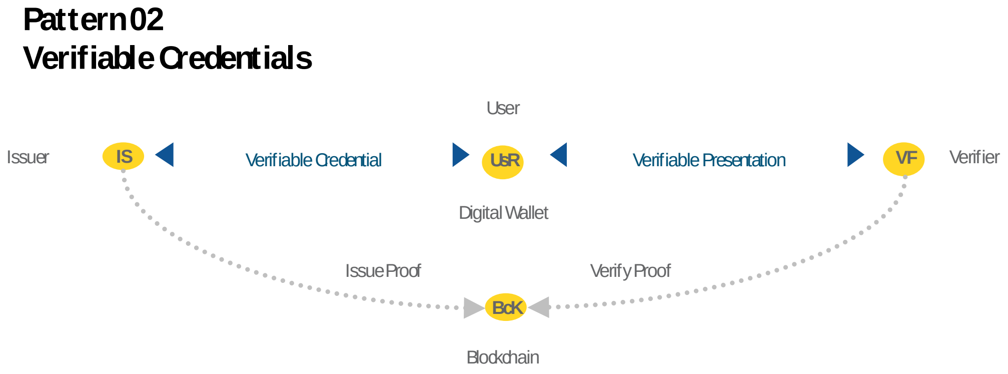
At conceptual level, this model is similar to a wallet of documents. However, instead of verifications through physical checks, these are now possible using digital means thanks to cryptography and blockchain technology. In this pattern, official documents (or credentials) are fundamentally a set of claims about someone or something. The verifiable credential can contain claims about the citizen having a given nationality, holding a certain degree, etc. These claims are then:

- minted in a digital document, usually known as a verifiable credential;
- confirmed by a competent authority using electronic signatures.

Furthermore, cryptographic hashes could be recorded on a blockchain alongside with the status of the Verifiable Credential. It is important to highlight that, due to performance and data privacy concerns, the blockchain should not store the data itself. Once these steps are completed, this will enable the data to be verified at any time using cryptographic methods. The data and documents can at this point be stored in a **digital wallet** by the citizen or organization i.e. the Holder of information. The citizen can then create a verifiable presentation, containing data from one or several credentials, as supporting evidence to real-life transactions such as changing address, applying for a job, etc. Verification processes are possible to automate, below are a few examples:

- The hash of the document itself (i.e. to verify the integrity of information);
- The Issuer (i.e. to verify the issuer of the official document) and
- The Holder (i.e. to verify to whom the official document was issued to).

How does the pattern work?



Pattern 02
Verifiable Credentials

The above diagram shows that, unlike the first pattern, any Verifier checking the authenticity of a digital document (a.k.a. a verifiable presentation) can rely on cryptographic verifications without needing to contact its Issuer. Furthermore, it is typically up to the Holder of the document to share it with the Verifier. This means that the Holder controls the information that it wants to share with others. Furthermore, selective disclosure of information may also be possible when information is standardized and advanced cryptographic methods, such as Zero-Knowledge Proofs, are used. Similar to the previous pattern, verifiable credentials depend on several infrastructural elements:

- The first element is, without any surprise, a fully functioning, permissioned, but publicly available, blockchain network that can be trusted by European public administrations. This involves, among other things, strong governance arrangements and security controls;
- Similar to the previous pattern, a digital identification framework is again a crucial prerequisite for this pattern to work. In a typical blockchain paradigm, this means that every public administration, business and citizen would need to get a “decentralized ID” (DID) according to

Self-Sovereign Identity principles. DIDs are a new type of identifier that enable verifiable, decentralized digital identity.

- As DIDs say nothing about the actual person or organization associated to it, a scalable solution is needed to link DIDs reliably to their associated 'legal' entity;
- Finally, citizens and businesses would need to have a trusted and secure digital wallet, connected to the blockchain, to hold their DID and documents.

The European Commission and the Member States are currently working on a Pan-European initiative, the European Blockchain Services Infrastructure (EBSI[1]) to address the above challenges both at technical and legal level. As this pattern tries to bring greater data control to citizens and businesses over their data, the participation of the GovTech ecosystem is even more crucial than in the previous pattern. Once all the infrastructural elements are in place, their participation can greatly accelerate the dissemination of emerging tech in everyday applications connecting governments to their citizens. This is likely to take some time and require incentives in this direction.

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi