

Validation - The Missing Link

By Rieks Joosten rieks.joosten@tno.nl

A Verifiable Credential (VC), or better perhaps, a Verifiable Presentation (VP), is requested by a particular party for the purpose of processing the data it contains. This processing leads to some result, e.g. a decision to register someone or something, or to provide some product or service.

In order for this processing to be valid, the input data must also be valid. We choose the term ‘validation’ to refer to the process by which a party determines whether or not data is *valid* for a particular kind of processing, which means that it will accept the result of such processing as valid. Note that one can only talk about ‘validation’ in the context of a particular party, a particular kind of processing, and an associated result.

W3C VCC distinguishes between validation and verification, which is the evaluation of whether a verifiable credential or verifiable presentation is an authentic and timely statement of the issuer or presenter, respectively. Verification of a credential or presentation does not imply evaluation of the truth of the claims encoded therein. Verification is basically a technical matter that can be performed objectively: it includes checking that: the credential (or presentation) conforms to the specification; the proof method is satisfied; and, if present, the status check succeeds.

The W3C VC Data Model v1.1 has placed validation out of its scope (see its definition), and rightfully so, because validation is a subjective, i.e. party-specific matter. Here is an example (taken from the eSSIF-Lab framework’s term ‘validate’). Consider a VC that is comparable to a passport. At any point in time that it is presented, the passport has either expired, or not. Establishing this is part of verification. However, when presenting a passport at TNO’s premises for the purpose of identifying oneself as a visitor, it is ok as long as the passport hasn’t expired for over 5 years. In another case, when presenting a passport at a Chinese embassy for the purpose of obtaining a visitor visa for China, the passport must not expire within 6 months. This shows that validating the same passport is not an objective (uniform), but rather a subjective matter.

Nevertheless, validation is a topic that should be properly addressed, if only to explain to parties how certain characteristics of VCs/VPs can be used in such processes. Annex A of the VC Data Model has already made a start, but is limited to the contribution that the various parts of VCs and VPs can make to the validation processes of arbitrary parties.

This paper wants to address the topic of ‘validation’ in a more generic way, that also includes more traditional ways that can be considered part of validation, such as checking PKI (server) certificates of IT components that provide data, by relying on the governance framework of a community, etc. So the research questions that this paper seeks to provide one (or more) answer(s) to is:

- What does an individual (yet arbitrary) party (organization or natural person), that wants to obtain data for a particular kind of processing so as to produce a specific result, need in terms of assurances, such that it
 - can trust (the veracity of) the data it obtains, and
 - reduces the risk of the outcome (that it will produce) being invalid, to a level that it can accept.
- In the (envisaged) Trust over IP (ToIP) architecture, what mechanisms do (or should) exist to assist parties to obtain the assurances it needs (for a particular kind of processing)?
- Can we extend the list of eSSIF-Lab mental models with one that addresses validation (and the difference with verification)?

It is envisaged that a paper that provides answers to such questions can be highly relevant - for furthering the VC (and other) standards; - for adoption of SSI by parties that want to obtain data that is valid for their specific purpose; - for parties that want to provide data that others can use (and hence will need to provide various assurances in one way or another)