Comparing Credential Formats

- by Dr. Andre Kudra, esatus AG, Germany
- Credential Formats analyzed and compared by an international expert group
- #Credentials #Formats #Signature #Revocation #Key-Management

This is a proposed collaborative paper to be worked on at RWOT 2022, Den Haag, Netherlands, 26-30 September.

Comparing Credential Formats

Dr. Andre Kudra (esatus), Paul Bastian (Bundesdruckerei), Dr. Torsten Lodderstedt (yes.com), further contributors to the collaborative work started at IIWXXXIV (to be invited)

Summary

Verifiable Credentials (VCs) have arrived in the mainstream. They are often referred to by a simple denomination, like *AnonCreds* or *W3C JSON-LD VC*, which hides the complexity behind them. Even among experts not always all foundational traits are totally clear to everyone. To remediate this situation, a group of domain experts gets together to analyze common VC types and formats. Their goal is to create a comparison matrix and an accompanying paper to make the variety of VCs transparent to all interested stakeholders. At RWOT 2022, this work will be driven forward.

1. Current situation

There seems to be broad agreement that *Verifiable Credentials (VCs)* are needed and a most useful means to enable broad digitalization. VCs allow moving around data between parties under full control of data subjects. Hence they have arrived in the mainstream discussion and practical application. VCs seem to be well understood, at least by experts, and their advantages and disadvantages should be very clear. Oftentimes in technical specs and architectural reference frameworks they are referred to by a common denomination, like *AnonCreds* or *W3C JSON-LD VC*. In fact, behind such a simple call sign a lot of - not only technical - underpinnings and assumptions are hidden. It is not a simple task to have all facts readily at hand or fully understand them all. Even among experts not always an eyes-level discussion can take place because not all foundational traits of VCs are totally clear to everyone. This leads to many discussions being entertained without a full feature set being known and understood by everyone in the same way and at the same level. I.e. just because one party believes it is most obvious what the distinct traits of a VC format are, the other one may not be aware. In some cases, a philosophical or even paradigm-lead debate arises, because parties cannot discuss on eyes level. For laymen, in-depth

discussions about VCs are mostly fully abstract. They have to rely on expert guidance to dive in and make up their mind for a decision. Desirable is that all stakeholders, experts and laymen, can draw from a consolidated, objective analysis and information base.

2. Approach

To remediate this situation, a group of domain experts got together first at the Internet Identity Workshop in its 34th incarnation (IIWXXIV) in Mountain View in April 2022. They kicked off with listing the common VC types and formats, to ultimately be able to compare them in defined categories. The desired tangible outcome is a comparison matrix which provides all relevant details and sheds light on VCs for all interested stakeholders. This will be accompanied by a paper outlining the work done as well as illustrating and discussing the key findings. The work of the expert group has continued in the meantime in dedicated working sessions. A scheme for main categories has been carved out, differentiating *credential format*, *signing algorithm*, *revocation algorithm*, and *key management* for both *issuer* and *holder*. Categories are drilled down further, e.g. looking at technical traits like *selective disclosure*, *crypto agility*, or *hardware support*, and adoption criteria like *standardization*, *technology readiness level*, or *implementation support*. Significant *Combos* have been put together, e.g. the denominator *AnonCreds* resolves to "AnonCreds + CL + Indy Revocation + did:indy + link secrets" as Combo.

RWOT in September 2022 will be used to drive the work forward and work on both matrix in structure and context and the accompanying paper.

3. Constituting components

Common credential types are a combination - Combo - of credential format, signing algorithm, revocation algorithm and key management. *[Detailed here.]*

4. Combos - Common credential types

Particular Combos - e.g. AnonCreds, JSON-LD VCs with BBS+, ISO mDL, ICAO DTC - are often referred to. This section presents rationales why those are common ones. *[Detailed here.]*

5. Discussion of selected Combos

Due to their diversity in traits, the common Combos have varying application scenarios and intensity of market acceptance i.e. production deployments and practical use. *[Detailed here. Structure to be discussed.]*

6. Conclusions

[Summary and conclusions here. Structure to be discussed.]

7. References

[1] x