REBOOTING THE WEB OF TRUST

DESIGNING THE FUTURE OF DECENTRALIZED SELF-SOVEREIGN IDENTITY

A WHITE PAPER FROM RWOT XI: THE HAGUE

A credential profile comparison matrix to facilitate technical and non-technical decision making

by Andre Kudra, Torsten Lodderstedt, Paul Bastian, Mirko Mollik, Maaike van Leuken, and Caspar Roelofs

RWOT XI GOLD SPONSORS:

DCD

Dutch Blockchain Coalition
connect and create

NGI ESSIF-LAB

VREDE EN RECHT
The Hague

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

Abstract

This paper introduces a *comparison matrix* for the wide variety of credential formats — such as W3C Verifiable Credentials, AnonCreds, and ISO-standard Mobile Driving License (mDL) — and the various related signing algorithms, revocation mechanisms, and key-management systems (collectively referred to as **credential profiles**). The credential profile comparison matrix is a living document that serves as an accessible resource for an in-depth evaluation of the technical requirements and their technical and non-technical implications for different use-cases and objectives. This paper also explains the rationale behind this matrix, describes the various properties that are included in the matrix and their definitions, and serves as an application guide on how to use the matrix for more informed technical and non-technical discussions and decision making.

This work is the outcome of a collaborative writing session during RWOT11 in September 2022 and continues the work kicked off in an IIW XXIV session in April 2022 and worked on offline afterwards. The work should be considered an iterative process, with the matrix being a living document that will require continuous updating while facilitating discussion among technical and non-technical experts.

Keywords

Verifiable Credentials, Credential Format, Credential Profile, Signing Algorithm, Revocation Mechanism, Key Management, SSI Components, ToIP Layer 3, Comparison Matrix, AnonCreds, mDl, Zero Knowledge Proofs

Introduction

There is an increasing agreement among technical experts as well as industry leaders and governmental agencies and regulators that Verifiable Credentials (VCs) are a necessary and useful means to enable broad digitalization. VCs allow for securely transferring data among parties, under full control of the data subjects, and are increasingly being discussed and implemented in both the private and public sector.

There appears to be a shared understanding of the advantages and disadvantages of various types of VCs, especially among technical experts. However, where technical specifications oftentimes refer to these VCs by a single common denomination, such as AnonCreds or W3C JSON-LD VC, a lot of technical and non-technical underpinnings, assumptions, and prerequisites remain inexplicit.

So even among technical experts, discussions and technical decision-making often take place without a shared understanding of the full technical feature set and requirements underpinning those technical decisions. Without making these underpinnings explicit, such discussions can remain restricted and unable to cross technological and philosophical paradigms. This is problematic also for less technical stakeholders, such as business innovators, industry leaders, or governmental institutions and regulators interested in VCs, who rely on technical expert guidance for their own strategic decision making. Thus, there is a need for accessible resources providing comprehensive definitions and in-depth comparisons of the wide variety of VCs and their underpinnings that can help in both technical and non-technical discussions and decision making.

In this paper, we introduce the concept of *credential profiles* to acknowledge that VCs are used in a wide variety of configurations that include different credential formats, signing algorithms, revocation mechanisms, and key-management systems. By comparing these profiles in a *credential profile matrix*, we provide an accessible resource for an in-depth evaluation of the technical requirements and their technical and non-technical implications for different use-cases and objectives.

Such a matrix can serve as a tool to fulfill three functions for innovators, industry, developers, security researchers, and in general people that want to use credentials in their use cases:

1. an *education function*, i.e. it is a means for gaining a better understanding of credentials and a wide variety of inherent aspects, some of them highly technical, others business and application related; and
2. a *discussion facilitation function*, i.e. a concise and comprehensive repository of facts about credentials allowing and facilitating an objective comparison and discussion; and
3. a *decision support function*, i.e. a tool for comparing properties and finding the right approach for a specific use case in question.

In this paper, we aim to describe the rationale behind the credential profile matrix, how it was constructed, and how it is intended to facilitate informed technical and non-technical decision making. This introduction highlighted the need for a deeper and more accessible analysis of the various credential types and their technological underpinnings, requirements, and implementations. In the methodological section section, we will briefly outline the process for constructing the profile comparison matrix and the methodological choices that were made in defining the targeted stakeholders. In the results section, we will summarize the properties that have been included in the profile comparison matrix and their definitions. Finally, in the discussion we will highlight several preliminary lessons learned and outline a path to move this initiative forward.

Methodology

For the creation of the credential profile matrix, a group of domain experts gathered first at the Internet Identity Workshop in its 34th incarnation (IIW XXIV) in Mountain View in April 2022. They kicked off the project with listening to experts for different VC types and formats and starting to gather data in a structured way, to ultimately be able to compare them in defined categories. This led to a definition for a *credential profile*: a configuration of the credential format, signing algorithm, revocation algorithm, and key management. These properties are then further drilled down, 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.

For example, what is typically refered to as AnonCreds resolves to the credential profile "AnonCreds + CL + Indy Revocation + did:indy + link secrets".

The work of the expert group has continued after the event in dedicated working sessions. RWOT11 in September 2022 was used to work on the structure and content of the matrix as well as on this accompanying paper. For completeness and correctness, the comparison matrix will be validated within the community of people interested in and working on SSI, Verifiable Credentials, and Decentralized Identity. This implies that this application guideline is a living document, as we might encounter more interesting properties while validating the comparison matrix.

Stakeholder Selection

The comparison matrix is meant to provide value to various stakeholder groups. The specific target groups and what benefit they will be able to draw from it are discussed below.

- **Community experts.** Thought leaders of the identity and trust services community got together to share their expert knowledge, collect and preserve it in a joint repository, and entertain discussion around it.
- **Technology innovators.** Those who are able and willing to follow the leading edge of the verifiable credential space can decide what technology to deploy in their innovative work without depending on their gut.
- **Industry leaders.** Decision takers at the executive level who have a technical background and are interested in the verifiable credential space can judge its relevance for their industry or business domain.
- **Policymakers and regulators.** Decision makers and their technically capable advisors can evaluate possible technologies and the implications of their implementation for their governmental use cases and mandates.
- **Software developers.** Highly technical audiences can dive deep into particular aspects of verifiable credentials and understand which properties they need to include in the application software they are creating.
- **Security researchers.** Security-oriented audiences can find out details of security mechanisms and cryptographic procedures in a credential profile, which is relevant for independent vetting of verifiable credentials.
- **Others!** Anyone considering deploying verifiable credentials in their use cases will gain rich insights into the matter and will benefit from the expertise brought in by the content contributors and expert discussion outcomes.

Scope

Credential means digital credentials in the comparison matrix and in this application guideline. Physical credentials are out of scope. The credential profile should also only include the most common credential profiles as we are making the comparison matrix.

Our focus is on open-source solutions, so that when conclusions based on the comparison matrix are made, they can actually be used.

We only consider the properties of underlying technologies directly relevant to the credential profile and what those properties mean for the properties of the credential profile. Based on this criterion, we place exchange protocols out of scope, including the possibility for offline verification of credentials, as this is a property emerging from the exchange protocol. A property can also manifest itself on different levels of the Trust Over IP (ToIP) technology stack, or on a governance level. In the comparison matrix, only the property on the credential profile level is considered.

The credential format and the signature algorithm are in scope, as the choice in these technologies directly impact the properties of the credential profile. This also holds for key management and revocation mechanisms.

Guide

The credential profile comparison matrix is maintained as a living spreadsheat in Google Sheets. In the following sections we will describe the properties listed in the comparison matrix. Some properties are present in various tables. We will discuss these first. Then we will list the properties specific to the credential format, signature algorithm, revocation algorithm, key management, and trust management.

Common Properties

Various properties are applicable to different tables in the matrix. The properties will be discussed in the following sections.

Intellectual Property Rights

Information on the status of patents and knowledge of possible IP rights are important for the adoption of new technologies. The document lists the known status of existing or expired patents or links to the IPR Policies that were in effect for the creation of standards and specifications. However, the existence of IPR policies does not guarantee the non-existence of patents from parties that were not involved in the process.

Specification

Specifications are essential for interoperability and security assessments. Whenever specifications are publicly available then a link should be provided.

Standardization

The standardization column describes under which standardization body and which working group the technology is standardized. It also describes what the status of the standard is or which standards track is intended for the future of emerging technologies.

Implementation Support

For developers it is important to know to what extent the technology has been implemented. Therefore information is provided on which or how many software libraries are available.

Technology Readiness Level

The Technology Readiness Level (TRL) is a measurement for the maturity of a technology that was developed by NASA. The values range from 1 to 9 with increasing values meaning increased maturity. In short these levels describe: - TRL 1: scientific research is beginning and those results are being translated into future research and development - TRL 2: basic principles have been studied and practical applications can be applied to those initial findings, little to no experimental proof of concept for the technology - TRL 3: active research and design begin, often a proof-of-concept model is constructed - TRL 4: proof-of-concept technology is ready, multiple component pieces are tested with one another - TRL 5: technology is identified as a breadboard technology and must undergo more rigorous testing - TRL 6: technology has a fully functional prototype or representational model - TRL 7: technology has been demonstrated as a working model or prototype in a space environment - TRL 8: technology has been tested and “flight qualified” and it’s ready for implementation into an already existing technology or technology system - TRL 9: technology has been “flight proven” during a successful mission

More information on TRL can be found here.

The TRL of various technologies in the matrix (credential format, signing algorithm) are given, based on the implementation support for that technology.

Properties of Credential Format

Apart from the common properties, the matrix provides information for the credential format on selective disclosure, predicates, and crypto-agility. These properties will be described in the following sections.

Selective Disclosure

Selective disclosure allows a holder to present a subset of the attributes of the credential issued by the issuer. This minimizes the amount of the holder’s information that is shared with the issuer. For example, the government issues a passport credential to Alice. The passport includes a variety of attributes, such as Alice’s first name, last name, birthdate, social security number, et cetera. When Alice want to buy alcohol at the supermarket, she has to prove to the supermarket that she is of legal drinking age (`18+`) to buy alcohol. In the classical setting where Alice shows her passport to the supermarket, the supermarket sees all the attributes on her passport, even though they just need her birthdate. Using a credential format’s selective disclosure capabilities, she can simply present her birthdate, with which the supermarket can verify that she is over `18`.

Selective disclosure can be achieved through the use of a signature algorithm that supports selective disclosure, such as BBS+ or CL signatures, or by using a salted hash approach in the credential format’s design. In the latter case, the salted hashes of the claims that can potentially be selectively disclosed are signed by the credential issuer (not the claims itself). The holder will then present the credential containing the signed hashes along with the actual claim values she wants to disclose and the verifier needs to check whether the disclosed values produce the same hash (i.e. are the values asserted by the credential issuer).

Selective disclosure can also be achieved through governance, namely a community can agree on signing each attribute separately, such that each attribute can also be presented separately. As mentioned before, in our matrix we only look at choices at the credential profile level, hence we only look at whether selective disclosure is achieved through the signature algorithm.

Predicates

Predicates allow the holder to further decrease the amount of information shared with the holder. Predicates check a value against a certain condition, resulting in true or false. Recall the example of Alice wanting to buy alcohol in the supermarket. Alice can prove that she is older than `18` using the predicate *age* `≥18`. As Alice’s age is `20`, the predicate `20≥18` is true. This way Alice can prove that she is allowed to buy alcohol without revealing her birthdate or even her age.

Just like selective disclosure, predicates can be created on various levels. On a governance level, the issuer could issue common predicates to holders, such as `18+` and `65+`. In the matrix, we only consider predicates through the capability of performing Zero-Knowledge Proofs in the credential profile.

More information about predicates and zero-Knowledge-Proofs can be found here.

Crypto Agility

To support long term security the cryptographic algorithms that are used for encrypting, signing, and hashing should be updatable without losing features. Crypto agility could mean - to increase the amount of bits for the keys - to replace the algorithm with a new one

It is difficult to predict the time when an algorithm has to be updated. Typical scenarios are: - the algorithm is broken and security is suddenly lost - the amount of computation power is high enough to perform a brute force attack in an acceptable amount of time - there are faster algorithms that make the process more efficient without losing features or lowering the security level

A relevant source is the recommendation of the German BSI (Federal Office for Information Security). They have published a technical guideline for recommendations and key lengths listing the algorithms and parameters to use. It must be mentioned that this is only a recommendation and not a direct law.

Encoding Scheme

There are various ways to encode the information within the credential, such as JSON, CBOR, Go Structs, etc.

Rich Schemas / Semantics

Rich schemas are hierarchically composable graph-based representations of complex data.

Security Considerations

When referencing with external semantics, such as a JSON schema, there is a risk of monitoring the usage of a credential:

The **host provider** is able to analyse the requests for the resource and find similarities: using information such as the user agent and IP address, they can find out which type of credentials are from one holder since verifiers and issuers normally use cloud systems.

When the **issuer** is also hosting the schema for his credentials, he is able to add a unique identifier to each new credential. This added tracking information allows the issuer to track the usage of a unique credential like

```
"@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://www.example.com/credentials/examples/v1.NSxma92am2s8wnnxz8"
],
```

where `NSxma92am2s8wnnxz8` is the unique identifier for a credential that is used for tracking.

Properties of Signature Algorithm

Apart form the common properties, the matrix provides information for the signature algorithm regarding hardware support and unlinkability. These properties will be described in the following sections.

Recognition by Government Organizations

For regulated use cases, the national regulation agencies provide a list of recommended and accepted cryptographic algorithms, e.g. BSI TR-2102 or NIST-published Federal Information Processing Standard (FIPS) 186-5, Digital Signature Standard (DSS). This property describes whether the designated signature algorithm is recommended by national government agencies.

Hardware Support

Hardware support is required for regulated and high-security use cases to prevent key duplication and theft and with that credential replay. Existing hardware modules to sign inside the smartphones are Trusted Execution Environments (TEE), Secure Enclaves, Secure Elements (SE), TPMs (Trusted Platform Modules), Embedded Universal Integrated Circuit Cards (eUICC), external authenticators, and more. In the backend, HSMs (Hardware Security Modules) or TPMs (Trusted Platform Modules) can be used by issuers or cloud wallets to secure the keys. While some specialised hardware devices support multiple advanced signature algoritms, the hardware-backed crypto processors on most common mainstream devices often support only a limited set of established signature algorithms. Therefore, the use of modern cryptography algorithms is limited for these use cases.

Unlinkability

Unlinkability is the property that an attacker cannot distinguish whether two or more items withinin a system (comprising these and possibly other items) are related or not. Within an identity ecosystem this applies for example if one verifier can link two credentials of a holder or two selective disclosures of the same credential or whether two colluding verifiers can link two seperate presentations of the same credential. This excludes the fact that linkability can also happen by the revealed attributes themselves or that unlinkability can be achieved by the infrastructure, e.g. just-in-time issuance.

Post-Quantum Security

With the computing power of quantum computers advancing, we need to think about post-quantum security with regard to SSI. Most widely used signature algorithms are not post-quantum secure and allow attackers after quantum computers have become computationally efficient enough to issue themselves credentials like they are issued right now by a recognized entity. So Eve can issue herself a university degree years from now, making it look like the credential was issued in 2022 by her university, as she can easily create the signature using a quantum computer.

In the comparison matrix, with regard to cryptography, we discuss signatures and their properties: selective disclosure and predicates. Currently, there are no common credential profiles that use signature algorithms that are post-quantum safe. NIST has recently announced their choice in post-quantum safe signature algorithms. The question is whether selective disclosure and predicates can still be provided with these algorithms. Predicates can still be achieved through post-quantum safe zero-knowledge proofs, such as zk-STARK and Aurora. For selective disclosure, it is not clear yet whether it can still be achieved through the post-quantum safe signature algorithms.

Performance

The performance of signature algorithms can impact the user-friendliness of the wallet implementing the credential profile. We express the generation of the signature in terms of seconds.

Properties of Revocation Algorithm

Revocation is when the issuer no longer vouches for the correctness of the information in the credential that was issued to the holder. A reason for revocation could be that the information in the credential is simply not true any more (holder is not a student anymore) or the information has to be periodically renewed (like a passport).

Category

Different approaches for revoking credentials exist, such as bitlists, deny-lists, and accumulators. A bitlist is a list where each issued credential has a position in the list. The verifier can then check this position to see whether the credential has been revoked or not. A deny-list is like a block list, each revoked credential is added to the list. A cryptographic accumulator is a cryptographic proof the holder generates and presents to the verifier to show that the credential has not been revoked.

Observability

To check whether the credential is revoked or not, the verifier consults a list (under control of the issuer) or receives a proof from the holder. Observability is about whether the verifier can still check the revocation status of the credential after the presentation transaction with the concerned holder.

Traceability

This property is about whether an issuer can observe a verifier checking that a certain credential has been revoked. This would pose a threat to issuer unlinkability.

Offline Friendliness

In some use cases presentations have to be verified in an offline setting, such as when presenting a mobile driving license to a police officer on the road. The verifier should then also be able to check the revocation status of the credential. This property defines whether a revocation algorithm allows for an offline workflow.

Properties of Key Management

To have interaction with a different party, for example to exchange credentials or presentations, you have to be able to authenticate the other party. This means that parties need identifiers that are typically bound to the party's public key, which allows for authentication of that party through a challenge-response.

Infrastructure for Key Resolution

Some key management systems require an infrastructure to resolve public keys and/or to validate the binding of the identifier to the key. Examples of such an infrastructure are witness networks, DLTs, or web servers.

Key Rotation

It can be beneficial to rotate keys every once in a while for freshness, but also allowing for generating a new key pair for when the old pair was compromised. This property defines whether the public key in a credential can be replaced by a new one.

Key History

Even though key rotation means that no new credentials will be connected to that key, it does not necessarily mean that the credentials linked to a deprecated key are invalid. This property is about whether a history of deprecated keys related to a certain identifier can be retained and obtained, allowing for the verification of older credentials.

Party

The credential profile comparison matrix also indicates which party (issuer versus holder) can use a certain key management system. Not all types of identifiers are desirable to use for both issuer and holder. Issuer keys need to be publicly verifiable and stable, whereas a key for holder binding only needs to be used by a single credential (or a couple of them) under a certain holder's control.

Properties of Trust Management

As displayed in the trust triangle, the verifier has to have a certain amount of trust in the issuer in order to accept the presentation of the holder, based on a credential issued by the issuer to the holder.

Description

For each method, we list a description on what the approach to trust management is.

Discussion

The credential comparison matrix is a work in progress. The matrix will become more complete through validation within the SSI community. It has already sparked deep and interesting discussions on existing revocation mechanisms and their limitations, potential attacks, and ways to resolve these issues.

Objectivity and Subjectivity

We have tried to be as objective as possible while filling in the matrix, but this was difficult for characteristics such as the complexity of existing implementations and the technology readiness level. We have tried to solve this by giving examples, such that the reader can follow our reasoning.

Summary

In our view, the credential comparison matrix delivers on the desired multiple functions:

- an **education function**, i.e. it is a means for getting a better understanding of credentials and a wide variety of inherent aspects, some of them highly technical, others business and application related; and
- a **discussion facilitation function**, i.e. a concise and comprehensive repository of facts about credentials allowing and facilitating an objective comparison and discussion; and
- a **decision support function**, i.e. a tool for comparing properties and finding the right approach for a specific use case in question.

We hope you find the credential profile comparison as useful as we do. Please contact us if you have any suggestions or if you want to contribute.

Additional Credits

Lead Author: Andre Kudra

Authors: Andre Kudra, Torsten Lodderstedt, Paul Bastian, Mirko Mollik, Maaike van Leuken, and Caspar Roelofs

Sample APA Citation

Kudra, A., Lodderstedt, T., Bastian, P., Mollik, M., van Leuken, M., and Roelofs, C. (2023). A credential profile comparison matrix to facilitate technical and non-technical decision making. Rebooting the Web of Trust XI. Retrieved from https://github.com/WebOfTrustInfo/rwot11-the-hague/blob/master/final-documents/credential-profile-comparison.pdf.

About Rebooting the Web of Trust

This paper was produced as part of the Rebooting the Web of Trust XI design workshop. On September 26th to 30th, 2022, over 60 tech visionaries came together in The Hague, The Netherlands to talk about the future of decentralized trust on the internet with the goal of writing at least 5 white papers and specs. This is one of them.

• **RWOT Board of Directors:** Christopher Allen, Joe Andrieu, Erica Connell.

• **RWOT11 Coordination Team:** Will Abramson, Christopher Allen, Joe Andrieu, Shannon Appelcline, Erica Connell, Eric Schuh, Carsten Stöcker.

• **Workshop Credits:** Will Abramson (Producer), Christopher Allen (Founder), Shannon Appelcline (Editor-in-Chief), Erica Connell (Host), Amy Guy (Ombudsperson), Willemijn Lambert (Graphic Recorder), Eric Schuh (Ombudsperson), Carsten Stöcker (Co-Producer, Demo Organizer), Dorothy Zablah (Facilitator).

• **Gold Sponsors:** The City of the Hague, Digital Contract Design, Dutch Blockchain Coalition, The Hague University of Applied Sciences, eSSIF-Lab.

• **Contributing Sponsors:** Blockchain Commons, Legendary Requirements, Spherity.

Thanks to all our attendees and other contributors!

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/rwot11/issues

The twelfth Rebooting the Web of Trust design workshop is scheduled for September 18-22, 2023, in Champagne, Germany. Sign up for announcements at https://weboftrust.info/subscribe/. If you'd like to be involved or would like to help sponsor the event, email: Leadership@WebOfTrust.info