UZI Certificate Credential

Abstract

This proposal describes a method for issuing Verifiable Credentials by leveraging the existing chains of trust provided by X.509 certificates.

Status of this document

This document is in draft.

Introduction

With the introduction of the Self Sovereign Identity approach and thechniques, high trust application can leverage the possibility of combining several identity claims. This allows for more flexible and fine grained authorization rules and thus data protection. These techniques however are quite new and we find ourselves in a tipical chicken-egg situation: personal wallets can be the solution for SSI authentication needs, but without available credentials, these wallets have no real value. Issuers however won't start issuing until wallets are a tried and proven technology. How can we bypass this catch-22?

Digital trust is not new. There are already a lot of parties who acts as a QTSP and provide trust attributes in the form of X.509 certificates. In the Netherlands for the care domain this is done by the CIBG who issues UZI certificates for individuals and systems.

This specification introduces a method of issuing UZI Verifiable Credentials based on the did:x509 method.

Chain of trust

The goal of this method is creating a verifiable chain of trust from the UZI Verifiable Credential back to the trusted UZI certificate authority. The certificate subject can issue a credential using the

private key which corresponds to the UZI Certificate. It issues this credential to its usual `did` such as a `did:web`. The issuer of this credential is an identity of the `did:x509` method and contains the relevant values in the id.

```
did:x509:0:sha256:abc::san:2.5.5.5:value
```

Revision #1
Created 11 October 2024 13:11:46 by Steven van der Vegt
Updated 11 October 2024 16:46:10 by Steven van der Vegt