Unlinkability of Verifiable Credentials in a practical approach

Degree programme: BSc in Computer Science
Thesis advisors: Prof. Dr. Annett Laube, Prof. Dr. Reto Koenig
Expert: Dr. Andreas Spichiger (Swiss Federal Chancellery)

In today's world, individuals have no control over their data. When presenting credentials, like an ID, more data than necessary is disclosed. Digitalising these credentials using technologies like Verifiable Credentials, the BBS Signature Scheme and OpenID Connect, individuals are able to only disclose what is needed, thus regaining privacy and security.

Introduction

Self sovereign identity (SSI) is a concept, where a holder of a data can choose what is revealed to whom. To be able to apply this concept, different technologies are needed. Verifiable Credentials (VC) are a type of digital credentials, which can be verified by the receiving party, called a verifier. The verifiable part of these credentials are cryptographic signatures. If the verifier trusts the issuer of the credentials, they can verify the validity, integrity and authenticity of the presented content. For the generation of these signatures, the BBS Signature Scheme, created by Dan Boneh, Xavier Boyen, and Hovav Shacham (BBS) is used in this thesis. In physical credentials there are different security mechanisms, that allow a verifier to check the presented data, like holograms on an ID. While presenting an ID reveals all the data on the credential, digital credentials signed with BBS allow for selective disclosure. Presenting VCs with a BBS Signature leads to linkability between presentations, as a signature is a unique identifier. This is a big problem for privacy. BBS can create proofs, which are unique for each generation. These proofs demonstrate to a verifier the knowledge of the original signature, without reveling it, thus removing the link.

Goal

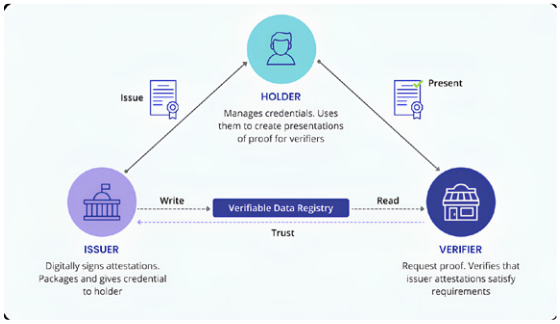
The goal of this thesis is to analyse, if the combination of these technologies in a real-world use case, breaks the unlinkabilty provided by BBS.

Results

How to use VCs with BBS was not straight forward, as various problems and security concerns became apparent. But these were all cleared up by different solutions, thus retaining selective disclosure and unlinkability. OpenID Connect for Verifiable Presentations had as well some security concerns, which were also solved.
The results of this thesis show, that using these technologies together, a future where SSI is the standard, is possible. Using the mentioned technologies as a basis, future research may contribute to a more secure digital world for individuals.

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://w3id.org/security/data-integrity/v2",
    "https://raw.githubusercontent.com/rob..."
  ],
  "type": [
    "VerifiableCredential"
  ],
  "credentialSubject": {
    "first_name": "John",
    "last_name": "Doe",
    "birth_date": "1.1.1970"
  },
  "proof": {
    "type": "DataIntegrityProof",
    "cryptosuite": "bbs-2023",
    "created": "2024-05-20T11:40:13.934Z",
    "verificationMethod": "did:key:zUC...",
    "proofPurpose": "assertionMethod",
    "proofValue": "u2V0ChdhA..."
  }
}
```

Example of a VC



The Trust Triangle

Joël Gabriel Robles Gasser
IT Security
078 699 91 71
joel.roblesgasser@proton.me