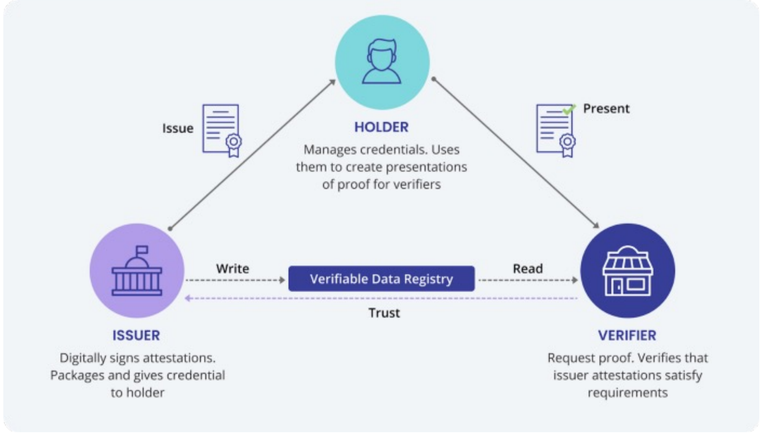
Summary

In today's world, users have no control over their data. In the physical world users have different credentials, like an ID or a driver's license. When presented to a verifier, all the data on those credentials are shown, thus disclosing more data than needed. Digitalizing these credentials using different technologies like Verifiable Credentials, the BBS Signature Scheme and Open ID connect, users can secure themselves from oversharing data. This thesis wants to show, that using digital credentials, users can govern over their data, and only reveal what's necessary.

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 theses 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 (BBS) is used in this thesis. In physical credentials there to are different security mechanisms, that allow a



The Trust triangle

verifier to check the presented data, like holograms on an ID. On the contrary to physical credentials, where presenting shows the full data, digital credentials signed with BBS allows a user to selectively disclose data. But BBS has one more trick up its sleeve, besides the selective disclosure. If one would just reveal the VC with the signature, unlikability would be broken, as the signatures can also be an identificatory. Using BBS, one can generate a proof of knowledge, which proofs to a verifier the knowledge about the original signature. If there is a new proof generated per presentation, no link can be created.

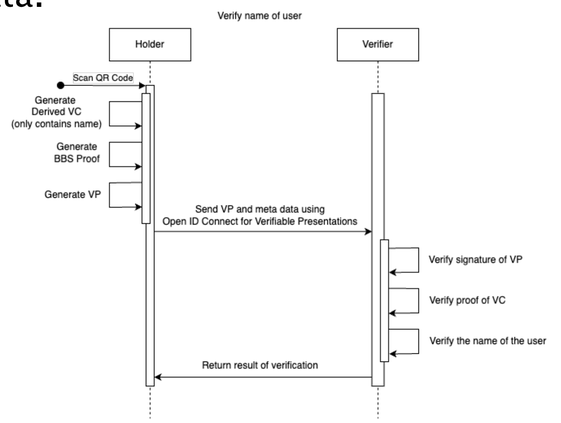
Goals

The Goal of this thesis is to analyze how the different technologies work together. In each step we also analyze if selective disclosure still works, no data leakage occurs, and if there was no link between the presentations.

Results

The first step was the unification between BBS and VC. After modifying the VC to be able to input it into BBS and analyzing the results, we found a small data leak, which came from an an algorithm. Randomizing the result of the algorithm using a hash function, solved this issue. The messaging layer Open ID Connect for Verifiable Presentations did not result in any data leakage but had other security concerns. To avoid replay attacks, a nonce was used. There is also the problem of session fixation attacks, which were solved with a redirect, so that the secret for the VP was sent to a different endpoint than the initial one. With those facts, we can say that the creation and transportation of digital credentials is safe allows users to govern over their data.

Sequence diagram of verification of the name of a user



Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Unlikability of Verifiable Credentials in a practical approach

Absolvent: Joël Robles
Advisors: Annett Laube, Reto Koenig
Expert: Andreas Spichiger

Bachelor Thesis 2024
Course of study Computer Science