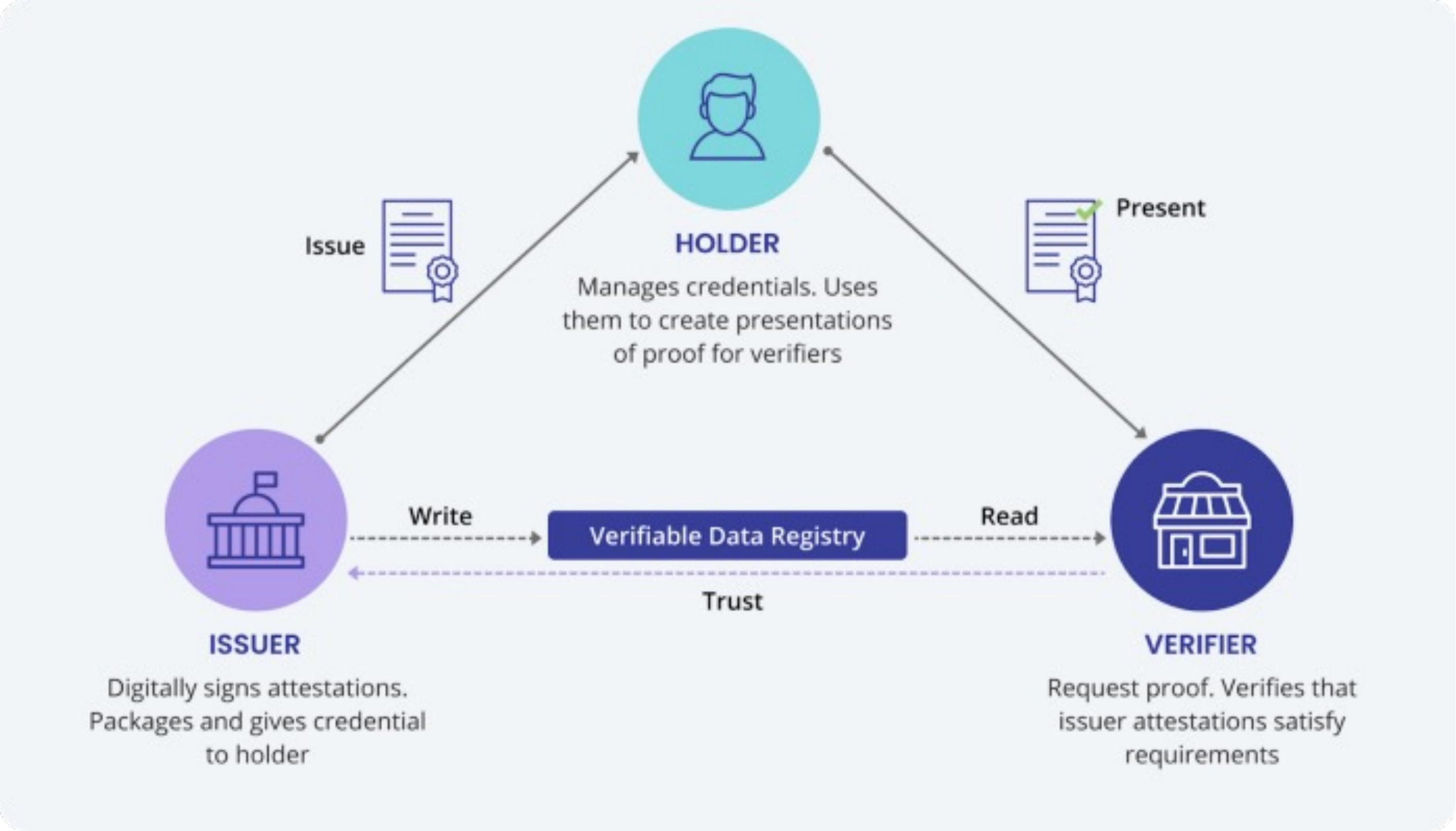
Introduction

In today's world, individuals have no control over their data. In the physical world, individuals 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 OpenID Connect, individuals can secure their data. This thesis wants to show, that using digital credentials, individuals can govern over their data and only reveal what's necessary.

SSI and VCs

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.


HOLDER
Manages credentials. Uses them to create presentations of proof for verifiers
Issue
Present
ISSUER
Digitally signs attestations. Packages and gives credential to holder
Write
Verifiable Data Registry
Read
Trust
VERIFIER
Request proof. Verifies that issuer attestations satisfy requirements

The Trust triangle

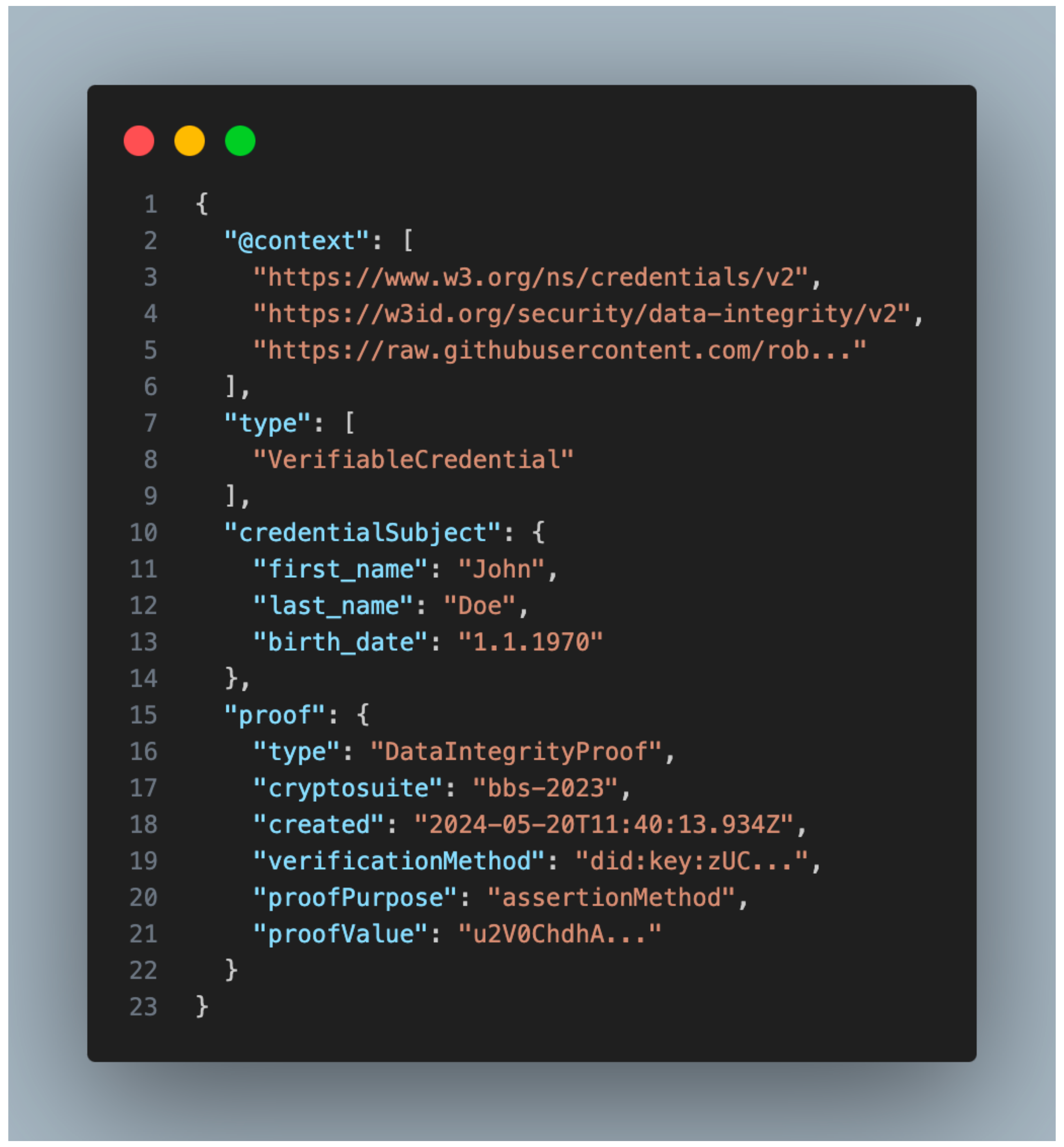
Goal

The goal of this thesis is to analyze, 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

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Unlinkability of Verifiable Credentials in a practical approach

Bachelor Thesis 2024

Course of study Computer Science

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