# Linking of Verifiable Credentials - A Comparative Analysis of Various Binding Approaches

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

This thesis investigates how Verifiable Credentials (VCs) can be hierarchically linked in the Swiss e-ID ecosystem, extending its insights to broader applications. Utilizing a custom built framework, it evaluates various linking methods, aiming to support the design of the e-ID and other Self-Sovereign Identity (SSI) systems.

## Introduction

Following the 2021 rejection of the „Federal Act on Electronic Identification Services“ by Swiss voters, the Swiss government is now planning a new SSI based direction. This thesis delves into the concept of hierarchical linking of VCs within such an SSI system. Hierarchical linking reduces data redundancy and strengthens trust by making lower-level credential verification dependent on higher-level credentials.

## Goal

The primary aim of this thesis is to meticulously analyze and establish a framework for selecting appropriate linking methods within SSI systems. The thesis is designed to serve as an extensive guide for stakeholders, including both governmental and private entities, contemplating the adoption of a digital identity system. By examining various methods and case studies, the thesis aims to shape the Swiss E-ID infrastructure, offering recommendations suited to public and private digital identity needs.

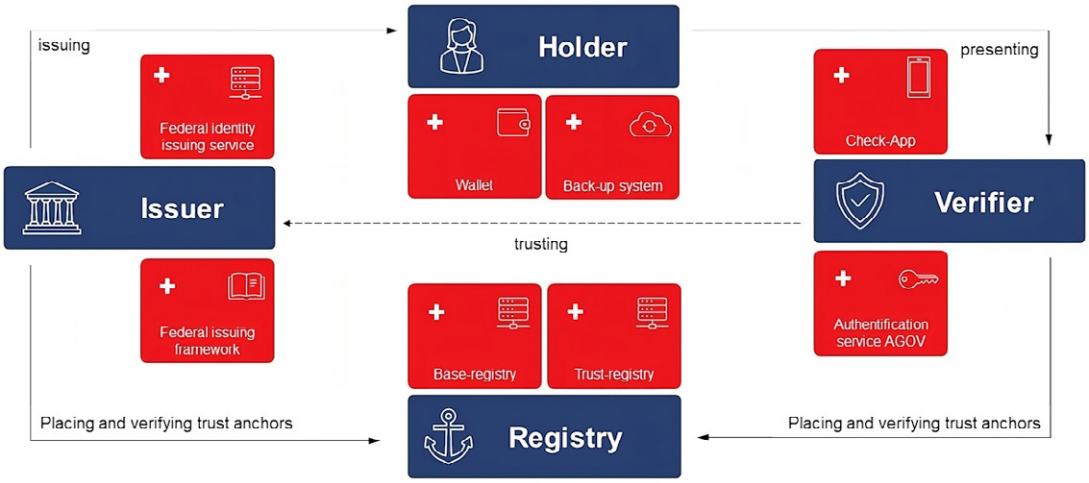
## Results

The research indicates no universal linking method, advocating for a multi-profile architecture. A „profile“ in this context refers to a set of specific requirements tailored to particular scenarios, such as the e-ID or work-related applications. This design allows various profiles to coexist on a single device, catering to different needs while maintaining appropriate security standards. It recommends linked secrets for their strong privacy attributes in linking the e-ID with other VCs and suggests URI-linking and Hashlinks for better structure and revocation processes.

## Future Directions

Highlighting uncertainties in BBS+ linked secrets, the thesis advocates for a multi-profile architecture as a a safeguard against potential failures. The recommended course for the Swiss e-ID is to start with prooven methods, focusing on URI-Linking and Hashlinks. Simultaneously, efforts should be directed toward enhancing BBS+ signatures for a privacy-focused outcome. This approach balances economic and EU interoperability needs, positioning Switzerland as a pioneer in privacy-centric SSI initiatives.

Simon Reto Gfeller
IT Security
sido11412@gmail.com




Overview of the planned Swiss e-ID architecture [https://github.com/e-id-admin/open-source-community/blob/737f665682c3e6f9d8be1221c8f05ced6bee175b/discussion-paper-tech-proposal/discussion-paper-tech]