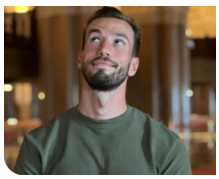
Swiss eID (swiyu) and Verifiable Credentials for Diplomas

In cooperation with my fellow students Micha Harzbecker and Polina Lisetska

Student



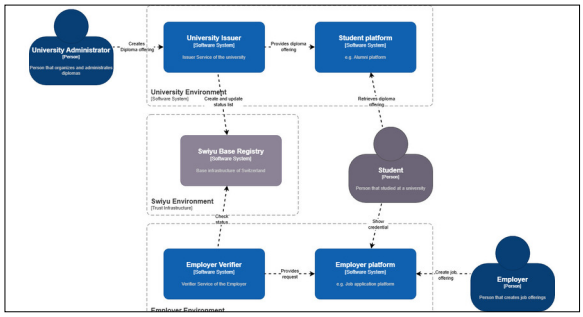
Simon Dietschi

Einleitung: Traditional centralized management of digital identities has become increasingly vulnerable to security breaches and data theft, with over 350 million user records leaked in 2023 alone. Consequently, decentralized paradigms enable users to manage their own identity data autonomously without relying on a central authority, which significantly improves both privacy and security compared to conventional systems. In the specific context of Switzerland, this technological shift is being realized through the state-recognized electronic identification known as the e-ID, which was approved by the public in a recent vote. The Swiss government is currently developing the necessary technical backbone for this system, referred to as the swiyu trust infrastructure, which is expected to launch fully in 2026 but is already available as a public beta environment for testing. This infrastructure is designed to enable residents to prove their identity digitally for government and business processes while retaining the greatest possible control over their personal data. Despite these digital advancements, the education sector often still relies on traditional paper-based certificates or simple pdf documents, which are inefficient to verify and susceptible to forgery. This project focuses on bridging that gap by applying the emerging swiyu infrastructure to the digital issuance and verification of academic diplomas. By treating a university diploma as a cryptographically secured verifiable credential, we aim to create a system that ensures authenticity and simplifies verification processes for employers while strictly adhering to high data protection standards.

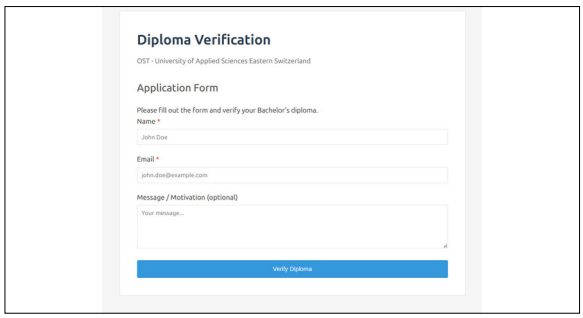
Ziel der Arbeit: The primary objective of this work was to evaluate whether the swiyu trust infrastructure, which is currently in a public beta phase, is ready to be used for issuing official university diplomas. We aimed to move beyond theoretical concepts and build a functional technical prototype that includes both a test issuer to represent the university and a test verifier to represent an employer. A significant part of the project involved defining a specific credential schema that contains all essential diploma information while remaining compatible with the technical requirements of the swiyu wallet. Furthermore, the thesis aimed to analyze the security of the system, specifically looking at cryptographic standards and potential privacy challenges.

Ergebnis: We successfully implemented a working prototype where a university can issue a digital diploma and a third party can verify its authenticity instantly. During the implementation, we found that the swiyu wallet currently has limitations when displaying complex nested data, which forced us to design a flat diploma structure and exclude the detailed transcript of records for the time being. From a security perspective, the system uses the ES256 algorithm which is secure by today's standards, but we identified that this might be vulnerable to quantum computing in the distant future, which is a concern for documents that must remain valid for decades. Ultimately, we concluded that while the cryptographic technology effectively prevents document forgery, it cannot fix human or procedural errors, such as a university administrator issuing a valid credential to the wrong student.

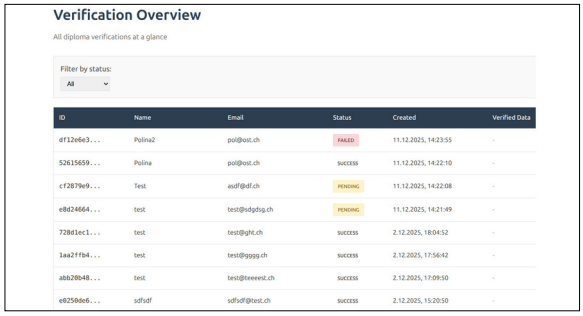
Issuance and Verification Concept
Eigene Darstellung



Shows a form whichs allows an applicant to verfiy that he owns a valid certificate.
Eigene Darstellung



Admin panel to see all the verified, pending or failed requests
Eigene Darstellung



Referent
Dr. Daniel Tschudi

Korreferent
André Clerc, TEMET AG, Zürich

Themengebiet
Internet-Technologien und -Anwendungen, Software