Abstract

Integrating verifiable credentials into the secure ecosystem of enmeshed

The growing need for secure and privacy-preserving communication systems was a key motivation in the development of enmeshed, a framework that enables individuals and organizations to communicate securely and privately. This thesis explores the integration of verifiable credentials into the enmeshed ecosystem, enhancing the framework's trustworthiness and expanding its capabilities.

Verifiable credentials are a powerful mechanism for securely exchanging and verifying digital information. By incorporating verifiable credentials into enmeshed, the framework gains the ability to establish trust between identities and securely share credentials such as proof of identity, qualifications, and attributes.

The thesis focuses on the technical aspects of integrating verifiable credentials into enmeshed, including the design and implementation considerations. It examines the different types of verifiable credentials, such as self-issued credentials and credentials issued by trusted authorities, and their applicability within the enmeshed ecosystem.

The implemented features of this thesis allow the creation of digital certificates in the verifiable credential standard and requesting those certificates from an end user by leveraging the enmeshed secured transfer channel. This enables the full support of the introduced user stories: a student requests a verifiable birth date certificate from a school as the trusted party and the learning platform requesting proof that the student is above the age of 16. With this approach the student can prove his birth date without the school and the learning platform communicating with each other. This enhances privacy, security, user experience and data sharing capabilities by a huge degree.

The thesis also investigates the potential challenges and considerations in integrating verifiable credentials into enmeshed, such as credential life-cycle management, revocation mechanisms, and privacy preservation. It proposes solutions and approaches to address these challenges, ensuring a robust and privacy-enhanced integration.