13 July 2017 Study · Digital Identity · Privacy & Crypto

Rich End-to-End Encryption

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/rich-end-to-end-encryption/

This project discusses the requirements of a solution to decouple the authentication process from an application that uses the Skytrust service.

The recent project „Skytrust“ being about moving the cryptographic key data from the application to an external service succeeded in relieving the cryptographic key data itself from unwanted attention. However, authentication data used to authorise key usage takes its place in being the weak point. These data are collected by the application and forwarded suitably – hence, the application has access to the now very sensitive authentication data. A better approach would be to also collect the authentication data outside the application. An intermediate authentication data collector service between application and key service is necessary to achieve the functionality. An intermediate, however, calls for end-to-end encryption. The challenge is to collect and route the authentication data without the need for breaking the end-to-end encrypted communication, while being able to add the data.

This project discussed the requirements of a solution, gives an overview of related work and finally presents a concept which tackles the challenge. The concept is then backed by a real-world use case. The project, however, leaves important problems unsolved so that the concept is as-is not ready for production. All in all, the project succeeds in getting an in-depth understanding of the motivation, the related work and the use cases to finally present one possible solution to the challenges given.