25 August 2020 Study · Mobile Security

Privacy-Preserving Service Composition

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 This content is no longer updated.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.

Version 2020-08-13
Source https://technology2.a-sit.at/en/publications/privacy-preserving-service-composition/

Service compositions are implemented through the interplay between actors of different organizations. Many composition systems use a middleware, which coordinates the service calls according to specified workflows. These middlewares pose a certain privacy issue, since they may

read all the exchanged data. Furthermore, service compositions may require that only selected subsets of data that was initially supplied by the user are disclosed to the receiving actors.

Traditional public key encryption only allows encryption for a particular party and lack of the ability to efficiently define more expressive access controls for a one-to-many communication. Besides privacy-preserving requirements, it may be necessary for participants in service compositions to be able to verify which actor has modified or added data during a process to ensure accountability of performed actions.

This work introduces a concept for efficient, privacy-preserving service composition using attribute-based encryption in combination with outsourced decryption as well as collaborative key management. Our concept enables end-to-end confidentiality and integrity in a one-to-many communication using fine-grained access controls, while minimizing the decryption effort for devices with low calculation capacity, which enables to use smartphones at the client side. The feasibility of the proposed solution is demonstrated by an implemented proof-of-concept including a performance evaluation.