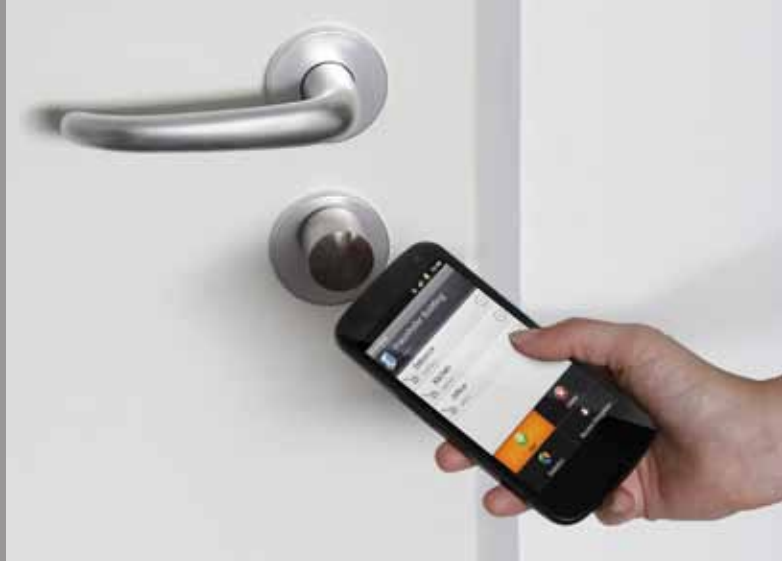
Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY



Fraunhofer Institute for Secure Information Technology SIT

Contact:
Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Rheinstrasse 75
64295 Darmstadt
Germany

Phone +49 6151 16-75560
Fax +49 6151 869-224
ahmad-reza.sadeghi@sit.fraunhofer.de
www.sit.fraunhofer.de/Key2Share

KEY2SHARE

SMARTPHONES AS A KEYRING

Smartphones and tablets have changed our daily lives in various ways. The increasing computing capabilities, communication interfaces, and apps have made these devices essential in our daily life. NFC-enabled smartphones can be used for access control that provides flexible functionality beyond traditional keys or access tokens such as smartcards. With Key2Share, Fraunhofer SIT has designed and developed a solution for access control with smartphones that offers a variety of features: Access rights can be distributed, revoked and delegated remotely, and can be bound to a usage policy (e. g., number of times an access would be allowed, or limited validity). This flexibility is beneficial in many use cases, such as an enterprise's access control to corporate facilities, new sharing services as locker concepts, parcel boxes or car sharing.

Challenges

Today smartphones are complex systems offering various attack surfaces to mobile malware. Hence, the electronic keys managed by Key2Share and corresponding usage policies must be protected without any negative impact on usability and user experience. Further challenges concern the integration of smartphone-based solutions into existing access control infrastructures.

Solution

Key2Share is a token-based access control system for NFC-enabled smartphones. The system allows Key2Share users to be granted access rights and to delegate such rights to other smartphone users. Access rights can be delegated as QR codes via email or MMS messages, or even be printed out. Key2Share system design addresses the bandwidth constraints of the NFC standard by using resource efficient cryptographic protocols. The signal for opening a door is transmitted via NFC and the lock opens without a noticeable delay. Key2Share is based on the state-of-the-art security protocols providing high security and flexibility. Further, it considers different approaches to protect cryptographic keys on the smartphone. The system can be integrated into the smartphone platform either purely in software and thus would not require hardware security anchors, or make use of security hardware such as smartcards for higher level of security. NFC compatibility to standards for the contactless smartcards allows for the seamless integration of smartphone-based solutions into existing access control infrastructures. Particularly, Key2Share is compliant to the 14443-4 standard for contactless smartcards which is for example also supported by Mifare DesFire contactless cards. This enables a step-wise integration of NFC-based smartphones into widespread contactless access control infrastructures. Key2Share is currently being developed for common Android smartphones but is not limited to Android.

Features

- Easy to use via app
- Remote distribution/revocation of keys
- Flexible delegation of access rights
- Context-based access policies
- Secure protocol
- Compatibility with contactless smartcards
- AES encryption and certificate-based registration

02/2013