Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE SIT

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Christoph Krauß
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-116
Fax 06151 869-224
christoph.krauss@sit.fraunhofer.de
www.key2share.de

KEY2SHARE

SMARTPHONE ALS SCHLÜSSELBUND

Moderne Smartphones bieten über diverse Apps unterschiedlichste Funktionen. Zwei der neuesten Technologien hierbei sind NFC (Near Field Communication) und BLE (Bluetooth Low Energy), die ein Smartphone zum Schlüssel innerhalb eines modernen Zutrittskontrollsystems werden lassen. Mit Key2Share hat das Fraunhofer SIT eine Zugangskontroll-Lösung entwickelt, die das Smartphone zum Schlüsselbund macht. Kein klobiger Schlüsselbund mehr: Haus-, Büro-, Garagen- sowie Autoschlüssel werden durch elektronische Schlüssel ersetzt und auf dem Smartphone gespeichert. Mit Key2Share lassen sich Schlüssel sogar zeitlich begrenzen und elektronisch verschicken.

Aufgrund ihrer Eigenschaften haben die elektronischen Schlüssel von Key2Share viele Vorteile gegenüber herkömmlichen Schlüsseln: Zusätzliche Schlüssel können kostenlos erzeugt und über das Internet oder über mobile Netzwerke ausgegeben werden. Besitzer von elektronischen Schlüsseln können diese weitergeben, indem sie bei Bedarf eine Kopie erstellen und als SMS- oder Email-Attachement verschicken. Im Falle eines Geräteverlusts lassen sich die elektronischen Schlüssel unkompliziert aus der Ferne für ungültig erklären, ohne dass der Besitzer das Schloss austauschen muss. Dies ist mit herkömmlichen physischen Schlüsseln nicht möglich. Zusätzlich können elektronische Schlüssel an Nutzungsregeln gebunden werden, die sowohl gültige Zeitfenster für die Nutzung definieren als auch die Anzahl der Öffnungen begrenzen. Das Konzept der Key2Share-Lösung wurde von den Sicherheitsexperten des Fraunhofer SIT gestaltet und nutzt kryptografische Protokolle nach dem aktuellen Stand der Technik, um die elektronischen Schlüssel auch während der Übertragung vor unerlaubtem Zugriff zu schützen. Zusätzlich verwendet Key2Share fortgeschrittene Plattform-Sicherheitsmechanismen, um die Schlüssel beim Speichern und Verarbeiten auf dem Smartphone zu schützen. So sind die elektronischen Schlüssel stets an ein mobiles Gerät gebunden. Dadurch können Angreifer die Schlüssel nicht stehlen, indem sie die Kommunikation abhören.

Für Nutzer, die Key2Share ohne Smartphone nutzen möchten, gibt es auch die Möglichkeit, mit Key2Share verwaltete Schlösser mittels NFC- oder BLE-Schlüsselanhängern zu öffnen oder schließen. Diese Schlüsselanhänger können auch als Ersatzschlüssel genutzt werden, falls der Akku des Smartphones des Key2Share-Nutzers leer ist. Die Technologie wurde an verschiedenste Anwendungsfälle angepasst, von Büro-Zugangsmanagement über Packstationen zu verteilten Schlüsseln beim Carsharing. Key2Share wird als App für die Smartphone-Plattformen Android und Windows Phone 8 bereitgestellt.

Features

- Sicheres Design / State-of-the-Art-Kryptographie
- Platzsparende Schlüssel
- Elektronische Ausgabe und Verteilung von Schließrechten
- Flexible Regelung der Schlüsselnutzung (bspw. begrenzte Anzahl von Schließvorgängen, begrenzte Zeitdauer, wöchentliche Zeitfenster, etc.)
- Keine zusätzlichen Kosten für die Schlüsselkopien
- NFC- und/oder BLE-Kommunikation zwischen Smartphone und Türschloss