# Contactless Confidential

COTECH

Passwordless. Encrypted. At-Rest.

Motivation

Saving company data on mobile devices is practical, but when data is lost – it can be expensive. Depending on the situation, losing customer data can cost more than 5000 €. Losing Intellectual Property is priceless. Data leaks lead to a low company reputation and potentially fines according to the EU-GDPR.

In order to avoid that from happening, you have to protect your data on mobile devices even more than on desktops or servers. For mobile devices encryption of data at rest is crucial to prevent data leaks. But this requires key and password management.

Contactless Confidential solves both problems: All passwords will be replaced by cryptographic keys on external smart cards. Users don't have to type strong passwords on touch screens. Our product reduces the time users spend on security processes and enables them to view their documents faster.
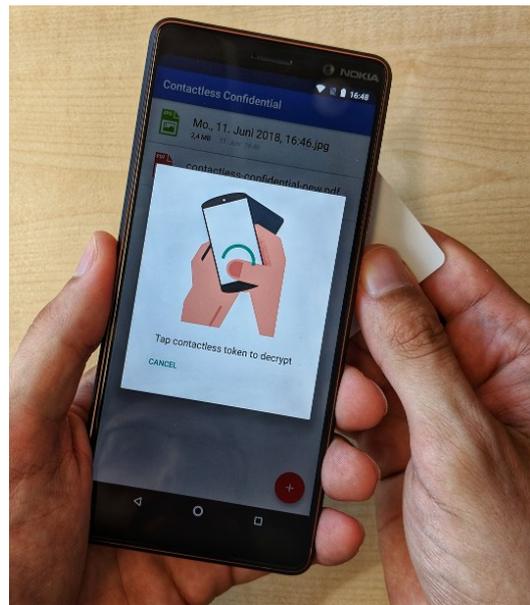

Offline Access

The binding of data to a specific card allows encrypting data at rest. All documents are saved securely when they are not in use.

Modern mobile operating systems allow for full disk encryption, but this encryption only prevents data access if the device is switched off. Thus in reality, full disk encryption doesn't prevent data leaks as smartphones are lost or stolen while they are still on.

Contactless Confidential decrypts data only when it is needed for the duration of use. This means that data leaks are actually prevented.
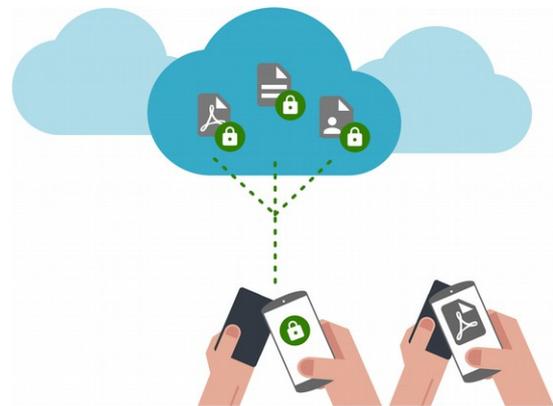
Cards cannot be copied

Tapping the card to the phone executes the essential parts of the encryption process on the card and not on the device. The key for the data is stored in a secure memory on the card. All attempts to read keys will destroy this memory.

Our encryption is superior to traditional password based encryption as it uses cryptographic keys.

User Experience

Aggregated ranking with 40 participants, published 2017 in ACM IMWUT Journal.

Bad   Okay   Good

www.cotech.de
contact@cotech.de
+49 531 3913154

Confidential Technologies GmbH
Institut für Betriebssysteme
Mühlenpfordtstr. 23, D-38106 Braunschweig