

# Die Sicherheit von Smartphones als Fernsteuerungsgeräte für IoT Devices

Dr. Bernd Borchert  
(Univ. Tübingen)



# Beispiel

**Was macht diese Frau hier gerade?**



# Beispiel

**Was macht diese Frau hier gerade?**



**Antwort:** Sie öffnet gerade ihre Wohnungstür im 3000 km entfernten Berlin, für ihre Schwester, die angerufen hatte und jetzt vor der Tür steht.

# Das Smartphone als Auslösegerät – eine große Versuchung!

Smartphone als Auslösegerät:

- sehr naheliegend. Eine große “Versuchung” für IoT Anbieter.

Aber damit noch ein Problem mehr im IoT Gesamtsystem: Smartphone-Trojaner

Zwei Standard-Fragen von Leuten, denen dieses Problem zum ersten Mal bewusst wird:

1. Können Smartphone-Trojaner denn überhaupt in das Smartphone-Betriebssystem hineinkommen?
2. Kann denn nicht die App entdecken, dass das Smartphone gerootet/befallen ist?

Problem-Verschärfung: Alles auf einem Gerät: auch Passwort und/oder Biometrie werden auf dem Smartphone eingegeben

Banking/Payment: die gleiche “Versuchung”, die gleichen Probleme. Die Banken geben aber der Versuchung nach (EU PSD2 wurde unter Einfluss der Banken so aufgeweicht, dass Smartphone-Lösungen jetzt erlaubt sind)

Kann man das Smartphone denn nicht sicherer machen?  
→ nächste Seiten



# App-TAN gehackt (Okt. 2016)

München 1°

## Süddeutsche Zeitung

SZ.de Zeitung Magazin

Shop Jobs Immobilien Anz

Login

Politik Wirtschaft Panorama Sport München Bayern Kultur Wissen Digital Chancen Reise Auto Stil mehr...

ANZEIGE

Home > Digital > IT-Sicherheit > Hacker knacken Photo-Tan-Verfahren für mobile Banking

17. Oktober 2016, 17:11 Uhr IT-Sicherheit

## Mobiles Banking: Hacker knacken Photo-Tan-App



Zwei IT-Sicherheitsforschern der Friedrich-Alexander-Universität ist es gelungen, bei Banking-Apps der Deutschen Bank, Commerzbank und Norisbank den Geldfluss umzuleiten. (Foto: Commerzbank AG)



Feedback

- Banken bieten Kunden an, Überweisungen über das Smartphone zu tätigen. Dazu wird unter anderem das Photo-Tan-Verfahren als App angeboten.
- Dabei werden Auftragsdaten in einer bunten Grafik verschlüsselt.
- Zwei IT-Sicherheitsforschern ist es nun gelungen, auf die



# Mastercard Bezahl-App (April 2017)

## DEUTSCHE BANK BRINGT ALS ERSTE BANK MOBILE PAYMENT.

von Maik Klotz am 03. April 2017 in FinTech, Mobile Payment, News

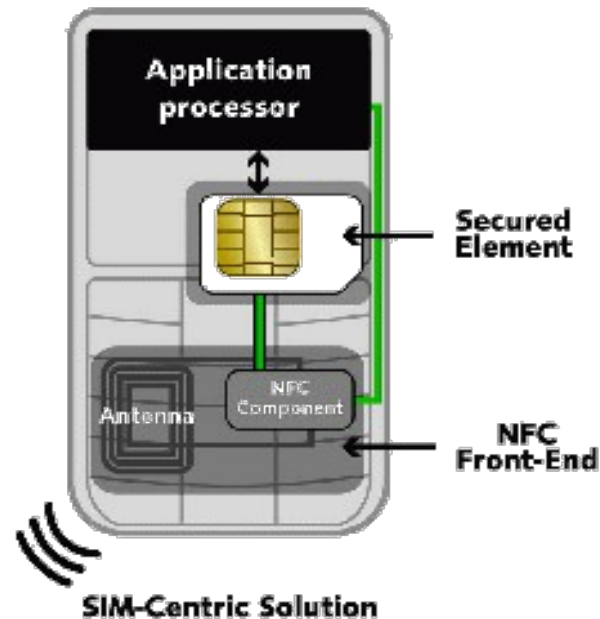


Mobile Payment mit der App der Deutschen Bank

Die Deutsche Bank schafft Fakten und bringt im April als erste deutsche Bank für alle Kunden ein mobiles Bezahlfahrer, das flächendeckend verfügbar ist und an mehr als **80.000 Akzeptanzstellen** nutzbar. Technisch zumindest. Aber braucht man das?

- Kein Secure Element, d.h., die “tokens” liegen im normalen Speicher des Smartphones!

# App-TAN + Secure Element (SE)



- SIM, e-SIM, embedded Secure Element, Micro-SD
- Schlüssel ist zwar sicher untergebracht, aber er kann missbraucht werden: Der Trojaner lässt das SE einfach eine erfundene/manipulierte Transaktion signieren. Das ist möglich, weil ein Trojaner das SE heimlich ansprechen kann und gleichzeitig die Peripherie und vor allem das Display kontrolliert.
- Platzierung des geheimen Schlüssels auf dem SE ist problematisch, nur mit Trust-Servern möglich:
  - bei SIM und e-SIM mit Trust-Servern der Telkos. Die Telkos sind aber teilweise schon aus den Trust-Server Projekten ausgestiegen (Deutsche Telekom Ausstieg Okt. 2016)
  - bei embedded SE's mit Trust-Servern der Smartphone-Hersteller. Problem: nicht alle Smartphones haben SE, außerdem Variantenvielfalt.

# App-TAN + Trusted Execution Environment (TEE)



- wie Secure Element, aber mit Kontrolle der Peripherie/Display (indem die Hauptprozessoren des Smartphones in einem vom Betriebssystem unerreichbaren sicheren Modus arbeiten)
- ziemlich sicher, abhängig von Typ/Implementierung
- Kinibi (Trustonic) hat z.B. ca. 300.000 lines of code --> Komplexitätsproblem
- Trust-Server Problematik, siehe SE
- Verbreitung schwach



# App-TAN + Biometrie



Fingerprint, Selfie, Voice, etc.

- Fall A: Biometrie wird beim Server geprüft:
  - Datenschutz-Problem (bei Banken etc.)
  - Unsicher: Trojaner macht sich eine Kopie der Biometrie-Datei und kann sich ab dann als der Kunde ausgeben. Auch bei Voice möglich: Voice-Cloning (seit 2001)
  - nach Abhören kein Zurücksetzen/Neuvergabe wie beim Passwort möglich
- Fall B: Biometrie wird auf dem Smartphone geprüft:
  - Reicht die Sicherheit? Kann man einem Smartphone-Hersteller so vertrauen?
  - Falls kein getrenntes Biometrie-Modul mit privatem Schlüssel: Was hindert einen Trojaner daran, einfach dem Bankserver gegenüber zu behaupten, die Biometrie sei positiv geprüft worden?

# Fazit App-TAN Erweiterungen

## Fazit:

Auch die Sicherheits-Verbesserungen Secure Element und/oder Biometrie bringen keine “wasserdichte” Sicherheit gegenüber Smartphone-Trojanern.

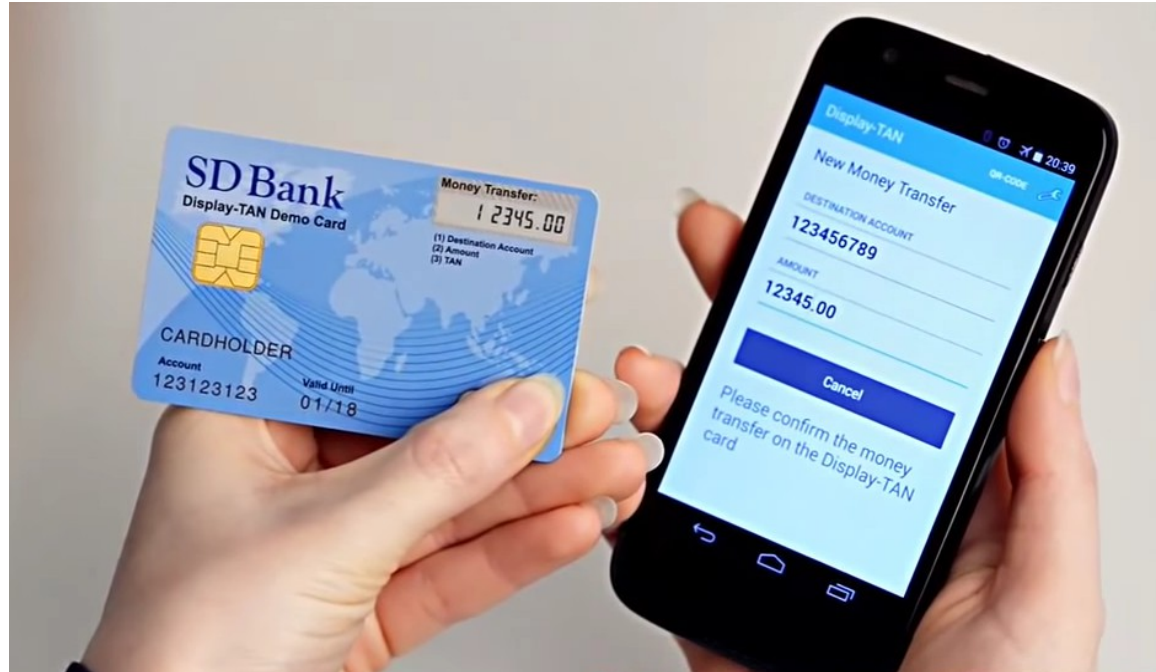
Ein externes Sicherheits-Token wäre sehr sinnvoll, vor allem bei relevanten Auslöseaktionen.

- Token sollte vom Smartphone aus per Funk (NFC, Bluetooth) erreichbar sein
- Token sollte Display haben
- Token im Scheckkarten-Format wäre ideal

Gibt es das?

# Display-TAN

## Karte mit Display und Bluetooth



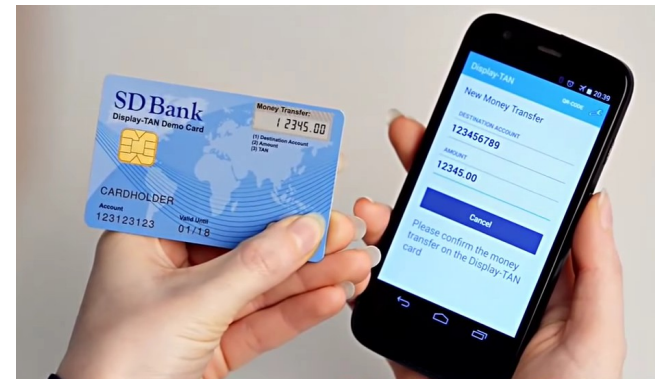
Sicher **UND** mobil

- sicher, weil die TAN-Erzeugung sich auf der Karte abspielt, nicht auf dem Smartphone
- mobil, weil der Bankkunde nichts anderes braucht als das, was er sowieso dabei hat
- wg. Bluetooth (statt NFC) geht das mit praktisch allen neueren Smartphones und Laptops
- Video: <https://www.youtube.com/watch?v=WGQS5ZIPRzM>

Variante Karte ohne Display und mit NFC: wesentlich billiger, aber nicht so sicher, und geht nicht mit iPhones.

# Usability-Vorteile von Smartphone+Karte

## Vergleich Smartphone vs. Smartphone+Karte



Sicherheit? keine Frage - die Kartenlösung ist wesentlich sicherer.

Aber was ist mit der Usability? ist nicht die Smartphone Lösung viel bequemer?

- auf den ersten Blick ja, denn die Karte muss jedesmal rausgeholt werden
- auf den zweiten Blick: es gibt kein Pairing des Smartphones - das hat handfeste Usability-Vorteile:
  - keine Initialisierung des Smartphones - App-Download genügt
  - Gebrauch mit wechselnden mobilen Endgeräten möglich (Privat-Handy, Firmen-Handy, Tablet, Laptop,...)
  - bei neuen oder spontan ausgeliehenen Geräten: App-Download genügt – keine Initialisierung
  - bei Smartphone-Diebstahl/Verlust/Verkauf/Weitergabe: keine Sorge um den geheimen Schlüssel

# Zusammenfassung Smartcard vs. Smartphone

Smartphones als IoT Auslösegeräte sind unsicher, auch mit Biometrie und/oder Secure Elements



Besser ist es also, relevante Aktionen mit einem externen Token bestätigen zu lassen:

