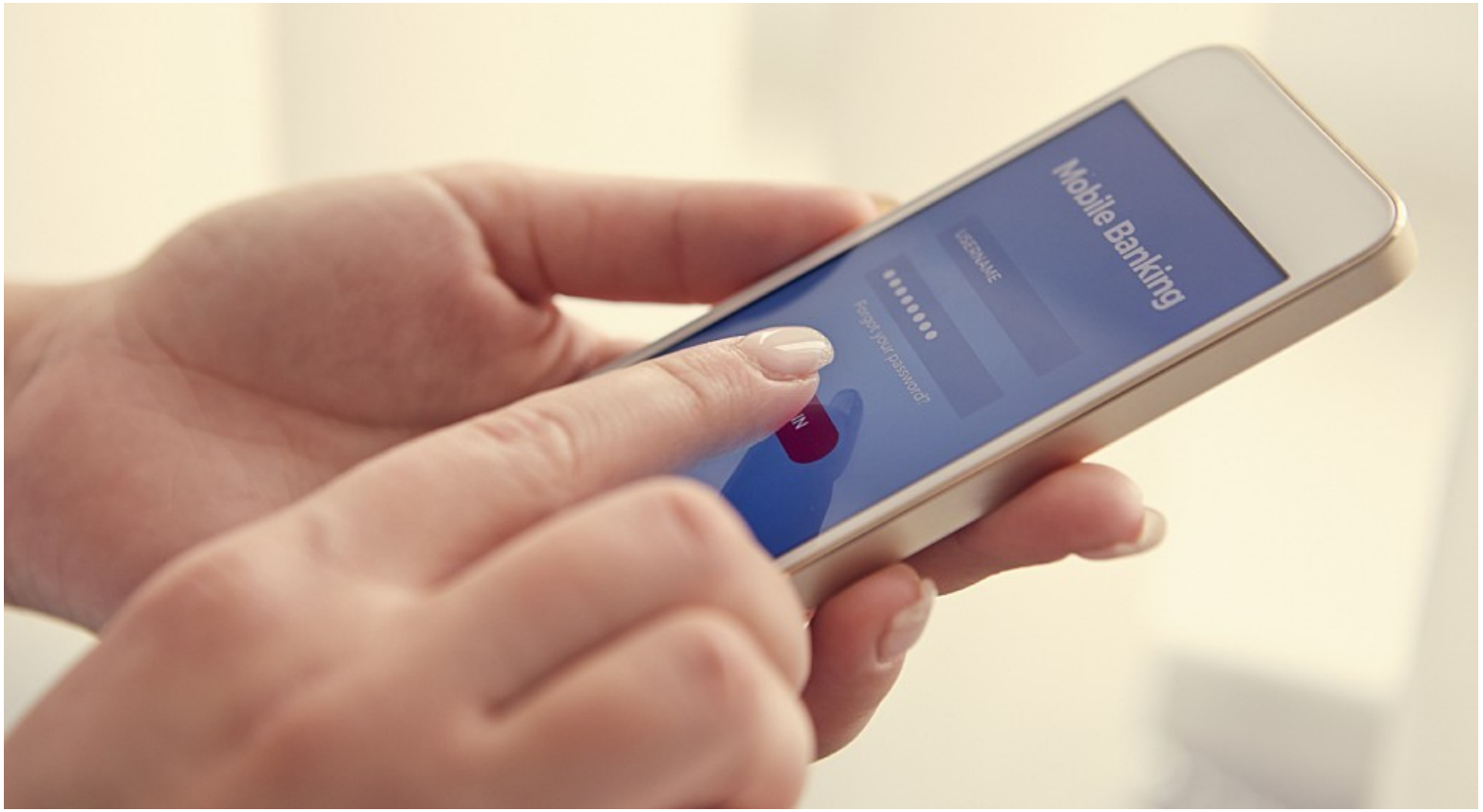
Mobile Banking TAN-Verfahren

Dr. Bernd Borchert

(Univ. Tübingen)

Mobile Banking

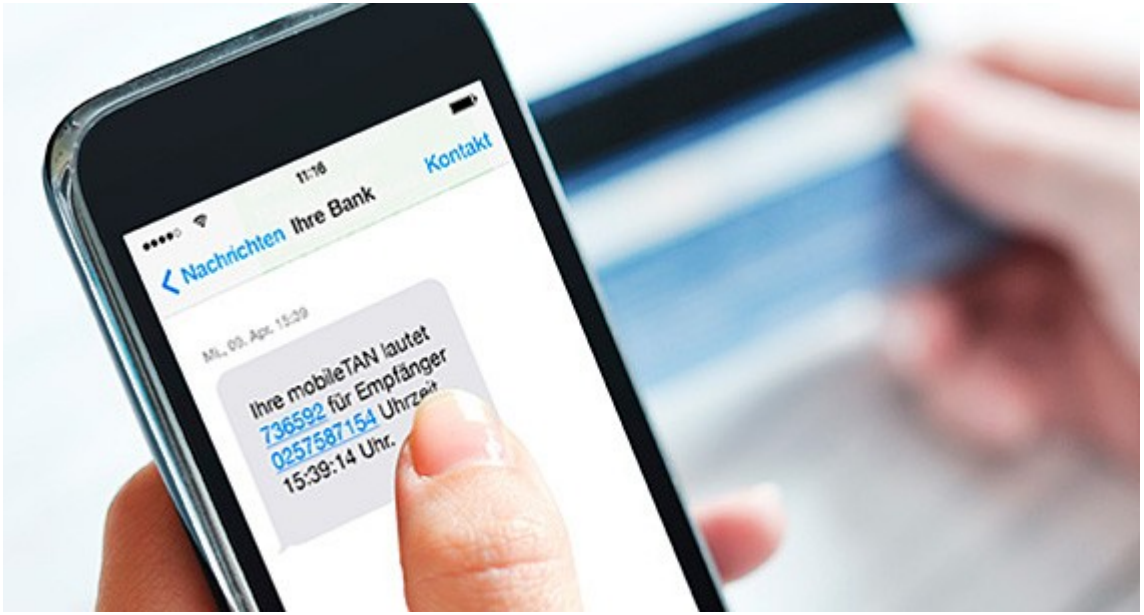
Mobile Banking = Online Banking auf Smartphone oder Tablet



Schon ca. 30% aller (lesenden) online Zugriffe auf Bankkonten sind mobil, Tendenz steigend.

Was ist mit mobilen Überweisungen?

SMS-TAN



- wäre von der Usability her ideal

- aber leider unsicher, aus verschiedenen Gründen, vor allem wg. fehlender “Kanaltrennung”

- so unsicher, dass die deutschen Banken sich SMS-TAN Mobile Banking schon 2009 selber untersagt haben (DK Beschluss)

iTAN

- iTAN unsicher:
    - kopierbar
    - Phishing-anfällig
    - kein *dynamic linking*, damit nicht PSD2-konform

- Usability: ok, ist “mobil”

Chip-TAN

- sicher

- aber leider unbequem:

    - Handling problematisch

    - Hauptproblem: der Kunde muss das Lesegerät dabei haben. Das widerspricht der Idee von “Mobilität”

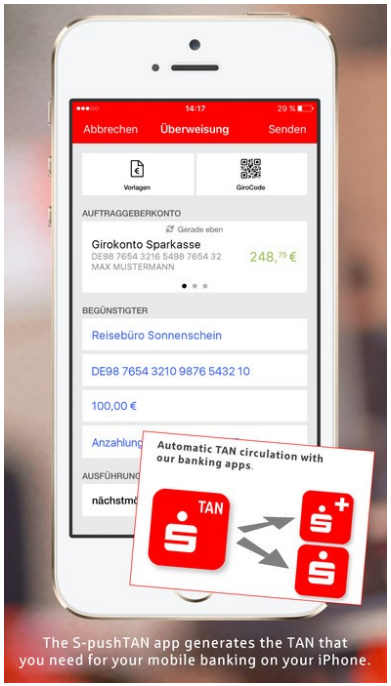
Photo-TAN (extra Gerät)

- sicher

- Handling besser als Chip-TAN

- Hauptproblem bleibt: der Kunde muss das Gerät dabei haben --> keine “Mobilität”

App-TAN



Push-TAN (Sparkassen), Photo-TAN-App (Commerzbank), etc.

- Usability: ok, Mobility: ja
- war anfangs nur für 2-Geräte Szenario erlaubt, inzwischen bei fast allen Banken auch für 1-Gerät (2 Apps)
- Problem: Sicherheit beim 1-Geräte Szenario (= Mobile Banking)
    - Trojaner, die das Betriebssystem gekapert haben
    - Fake-Apps
    - Kanaltrennung tatsächlich erfüllt?
    - ist zwar mit etwas “Härtung” nach neuestem Stand (Feb. 2017) laut EBA PSD2-tauglich
    - aber die Erfüllung der PSD2 Strong Customer Authentication bleibt fraglich wg. der Unabhängigkeits-Anforderung angesichts von Betriebssystem-Trojanern: ein solcher Trojaner hört Online-Passwort und den im App-Speicher gespeicherten geheimen Schlüssel ab: damit sind diese beiden Faktoren nicht unabhängig voneinander, denn wenn der eine Faktor abgehört werden kann, kann auch der andere abgehört werden.

App-TAN gehackt (Okt. 2016)

ANZEIGE

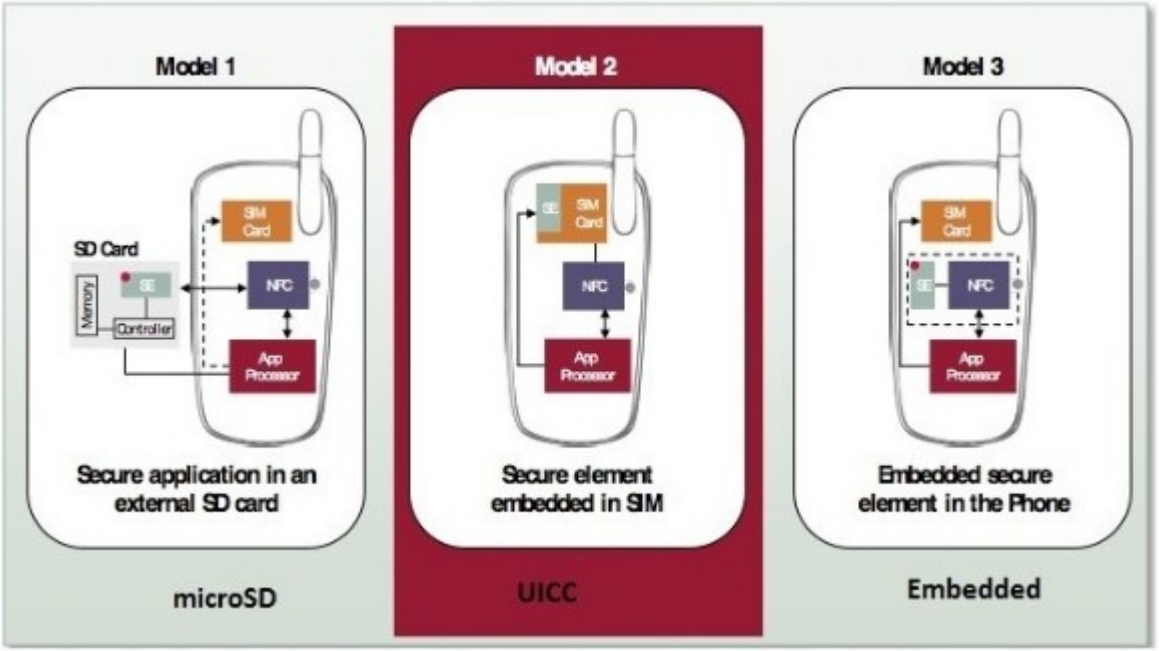
17. Oktober 2016, 17:11 Uhr IT-Sicherheit

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)

- 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

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 Überweisung signieren. Das ist möglich, weil ein Trojaner das SE heimlich ansprechen kann und gleichzeitig die Peripherie und vor allem das Display kontrolliert.

- Plazierung 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 Bankserver geprüft:
    - Datenschutz-Problem
    - Unsicher: Trojaner macht sich eine Kopie der Biometrie-Datei und kann sich ab dann als der Bankkunde 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/Darf die Bank 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

Die Erweiterungen für App-TAN (Secure Element/SIM/eSIM, Biometrie) machen App-TAN nicht richtig sicher, bestenfalls die mit TEE.

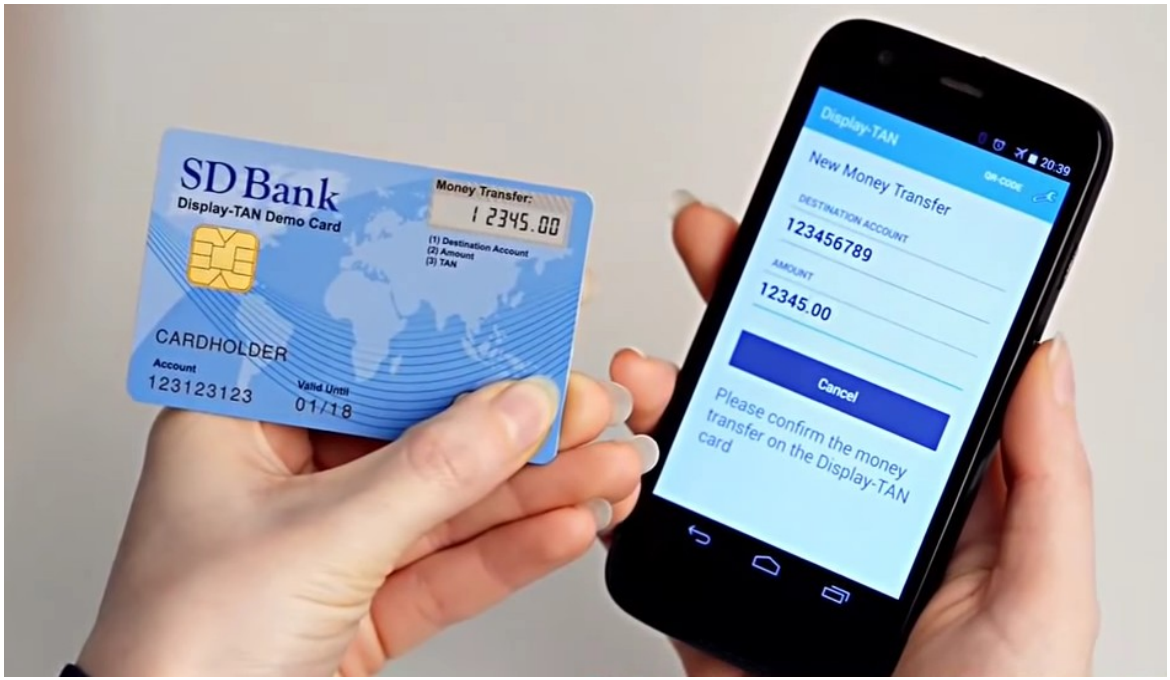
Externe TAN-Generatoren wie Photo-TAN sind dagegen sicher.
Deshalb die naheliegende Idee (seit 1998):

Den TAN-Generator in die Bankkarte einbauen!

Das wäre gleichzeitig sicher und mobil.

Display-TAN

Bankkarte mit Display und Bluetooth



Sicher **UND** mobil

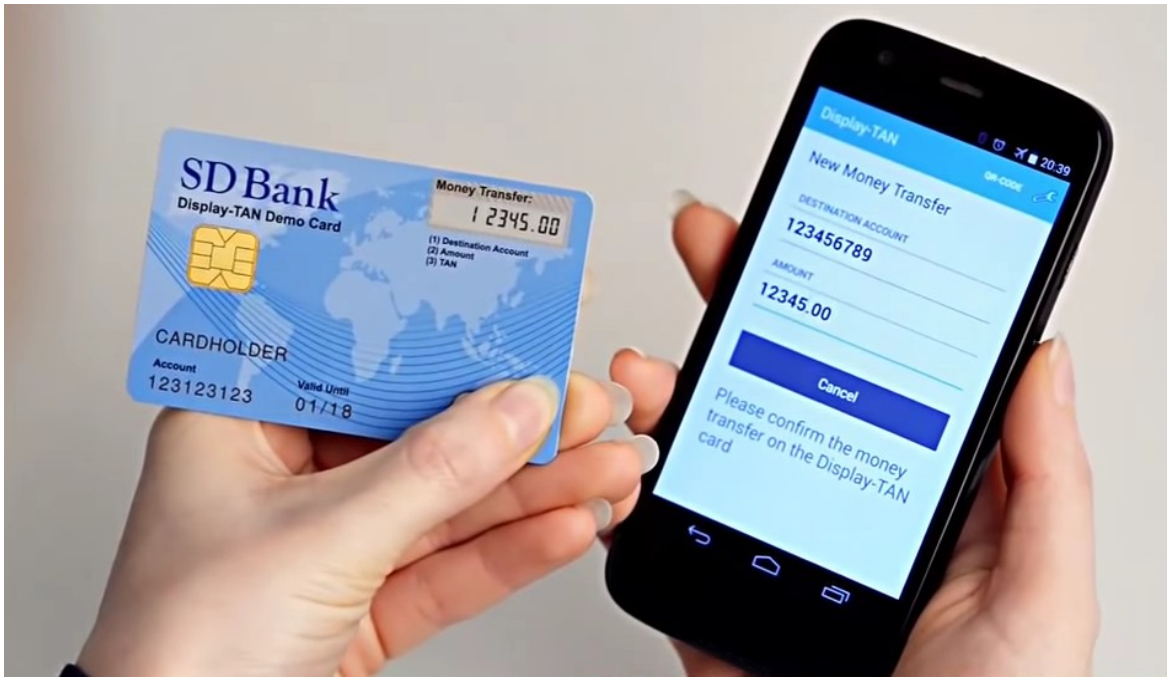
- sicher, weil die TAN-Erzeugung sich auf der Bankkarte abspielt, nicht auf dem Smartphone
- mobil, weil der Bankkunde nichts anderes braucht als das, was er sowieso dabei hat
- wg. Bluetooth (statt NFC) geht das mit praktisch allen neueren Smartphones und Laptops
- Video: https://www.youtube.com/watch?v=WGQS5ZIPRzM

NFC-TAN = Variante Karte ohne Display und mit NFC: keine Kosten, aber nicht sicher, und geht nicht mit iPhones.

NFC-TAN mit TEE auf dem Smartphone zur sicheren Visualisierung der Transaktionsdaten: sicher.

Usability-Vorteile von Smartphone+Karte

Display-TAN, NFC-TAN, NFC/TEE-TAN



Usability im Vergleich zu App-TAN:

- auf den ersten Blick nicht so bequem, denn die Karte muss rausgeholt werden

- auf den zweiten Blick: 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 Mobile Banking TAN-Verfahren

Entweder **sicher** aber **nicht mobil**

Problem: extra Gerät

- Chip-TAN
- Photo-TAN (extra Gerät)

oder **mobil** aber **nicht sicher**

Problem: Smartphone-Trojaner

- SMS-TAN
- iTAN
- App-TAN
- Secure Element
- TEE (eventuell sicher)
- Smartphone-Biometrie

Smartphone+Karte: sicher **UND** mobil