

# Mobile Payment

Vom Wirrwarr zur stabilen Realität

Forschungsgruppe für Industrielle Software (INSO)

Technische Universität Wien

Dr. Gerald Madlmayr



# Bezahlen in Österreich

- ▶ Unterscheidung von Debit, Credit und Prepaid
  - ▶ Debit: Maestro (Mastercard), V-Pay (Visa)
  - ▶ Credit: MasterCard, Visa, Diners, Amex, JCB
  - ▶ Prepaid: Maestro Karten (zB AMS) oder Quick (Geldbörse)
- ▶ Bankomatkarte
  - ▶ 8,5 Mio. Bankomatkarten in Österreich (2015: 99 %+ NFC)
  - ▶ 17,9 Mrd. Umsatz bei 359 Mio. Transaction (POS)
  - ▶ Ca. 50 EUR pro Zahlung
  - ▶ 42 TX pro Karte pro Jahr
  - ▶ alle 9 Tage eine Zahlung
  - ▶ + 18,7 Mrd. Behebungen bei 148 Mio. Abhebungen (ATM)
- ▶ Kreditkarte
  - ▶ 2,85 Mio. Kreditkarten in Österreich
  - ▶ 10,2 Mrd. Umsatz bei 95 Mio. Transaktionen
  - ▶ Ca. 107 EUR pro Zahlung
  - ▶ 33 TX Pro Karte pro Jahr
  - ▶ alle 11 Tage eine Zahlung
- ▶ Vergleich: Amazon ca. 35 Mio. TX/Tag im 12/2014



Quelle: ÖNB 2012

# Bezahlen in Österreich

- ▶ Quick
  - ▶ 50.000 Akzeptanzstellen In Österreich (Paylife only)
  - ▶ Davon 10.000 in Automaten (Altersfreigabe für Zigaretten)
  - ▶ 26 Mio. Transaktionen in 2013, 100 Mio. Volumen
  - ▶ 9 Mio. Karten im Umlauf
  - ▶ Kooperationen mit EduCard und Unis (zB JKU)
  - ▶ Auch Kontaktlos
  
- ▶ Mobiles Bezahlen
  - ▶ Vero Pay (national, Barcode basierend)
  - ▶ Paybox Bank AG (national, SMS/Anruf basierend)
  - ▶ Google Wallet, Apple Pay (international, NFC/HCE basierend)
  - ▶ PayPal, WireCard, dgl. (international, Web basierend)
  - ▶ SoftCard (USA, NFC/SIM basierend)

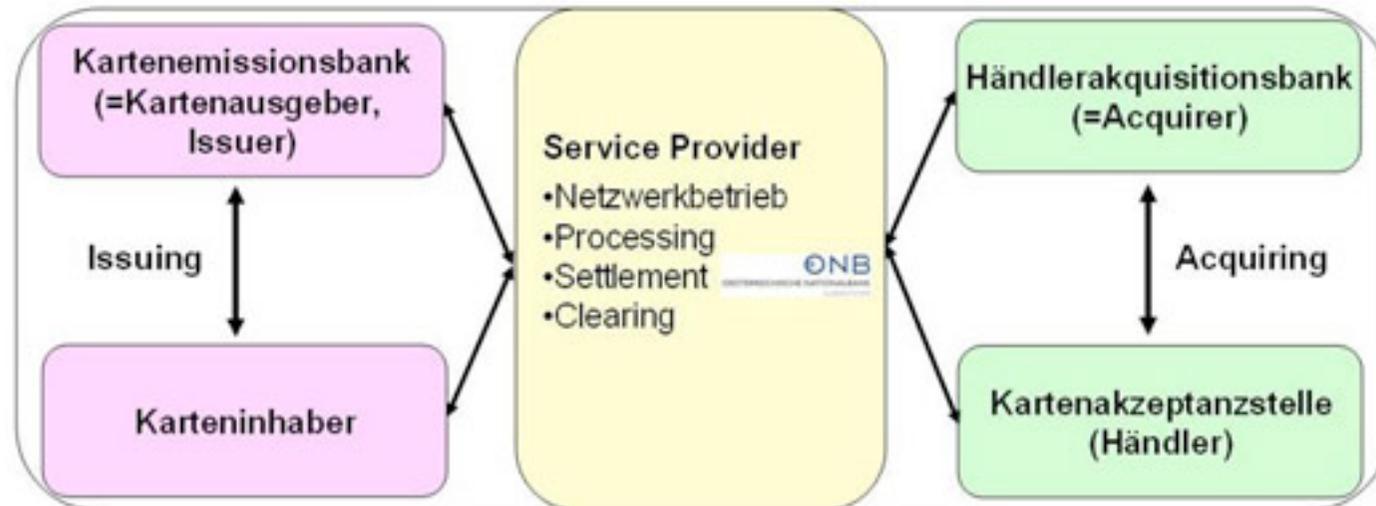
Quelle: Paylife

# Player im Markt

- ▶ Ausgebende Stelle für Bezahlungsmittel (= Issuer)
  - ▶ Player: Banken/PSA, Paylife, Card Complete, Wein&Co, dgl.
  - ▶ Haben den Kunden und geben ihm eine Karte
  - ▶ Achtung: nicht zwangsläufig Bankverbindung beim Issuer!
- ▶ Bereitstellen von Akzeptanzstellen (= Acquirer)
  - ▶ Player: Paylife, Card Complete, B+S, Hobex, Rea Card, ConCardis
  - ▶ Stellen Terminals am POS bereit
  - ▶ Kümmern sich um Auszahlung an den Händler und Einzug vom Kunden
  - ▶ Kosten für Terminal + Transaktion Fee (= Disagio; zwischen 0,9 % - 3 %)
- ▶ Verarbeiten der Transaktionen (= Prozessor)
  - ▶ Player: Atos, FirstData, SIX, ...
  - ▶ Settlement, Clearing, Netzbetrieb, Kontoführung, Autorisierung dgl.

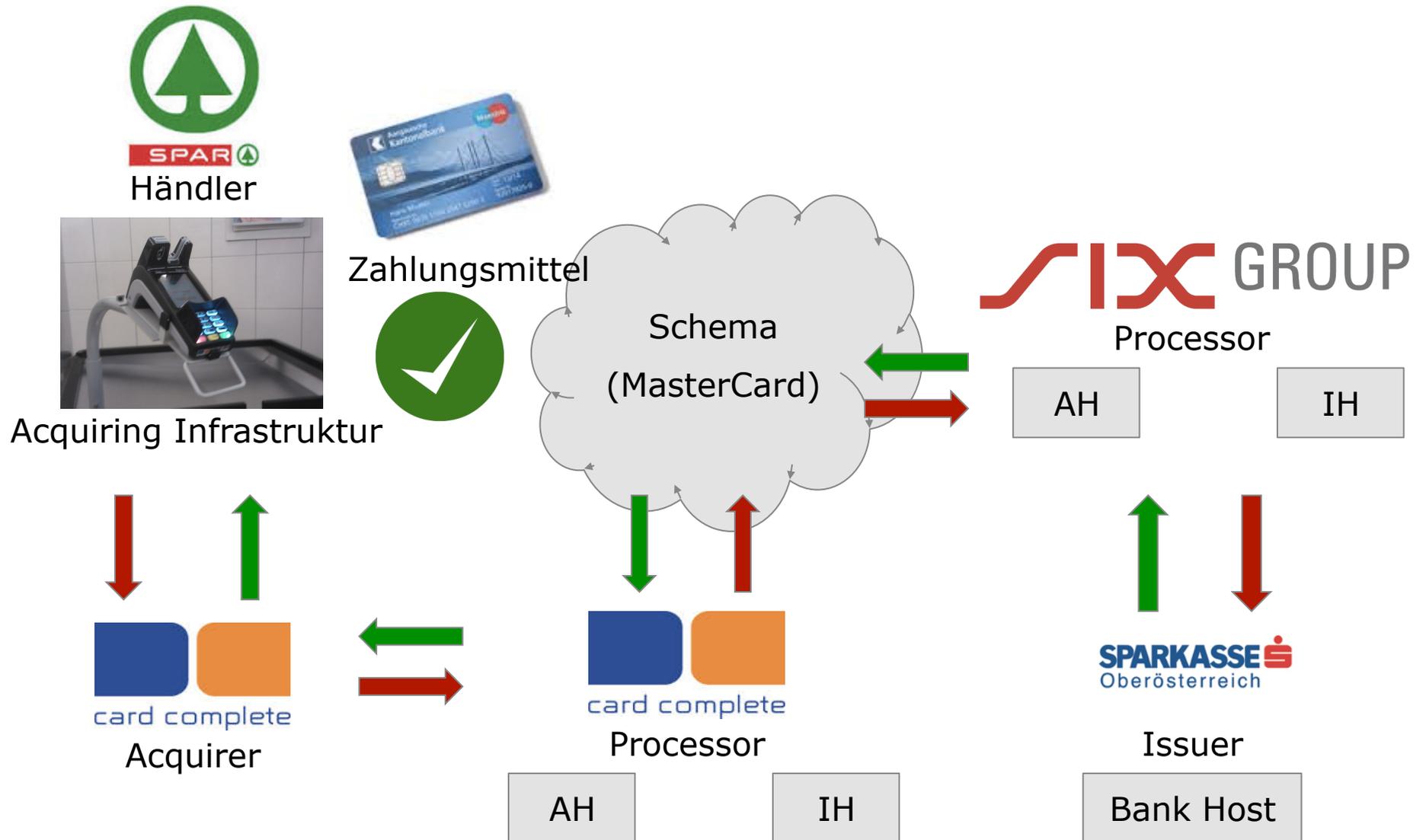
Quelle: ÖNB

# Ökosystem – 4 Parteienmodell

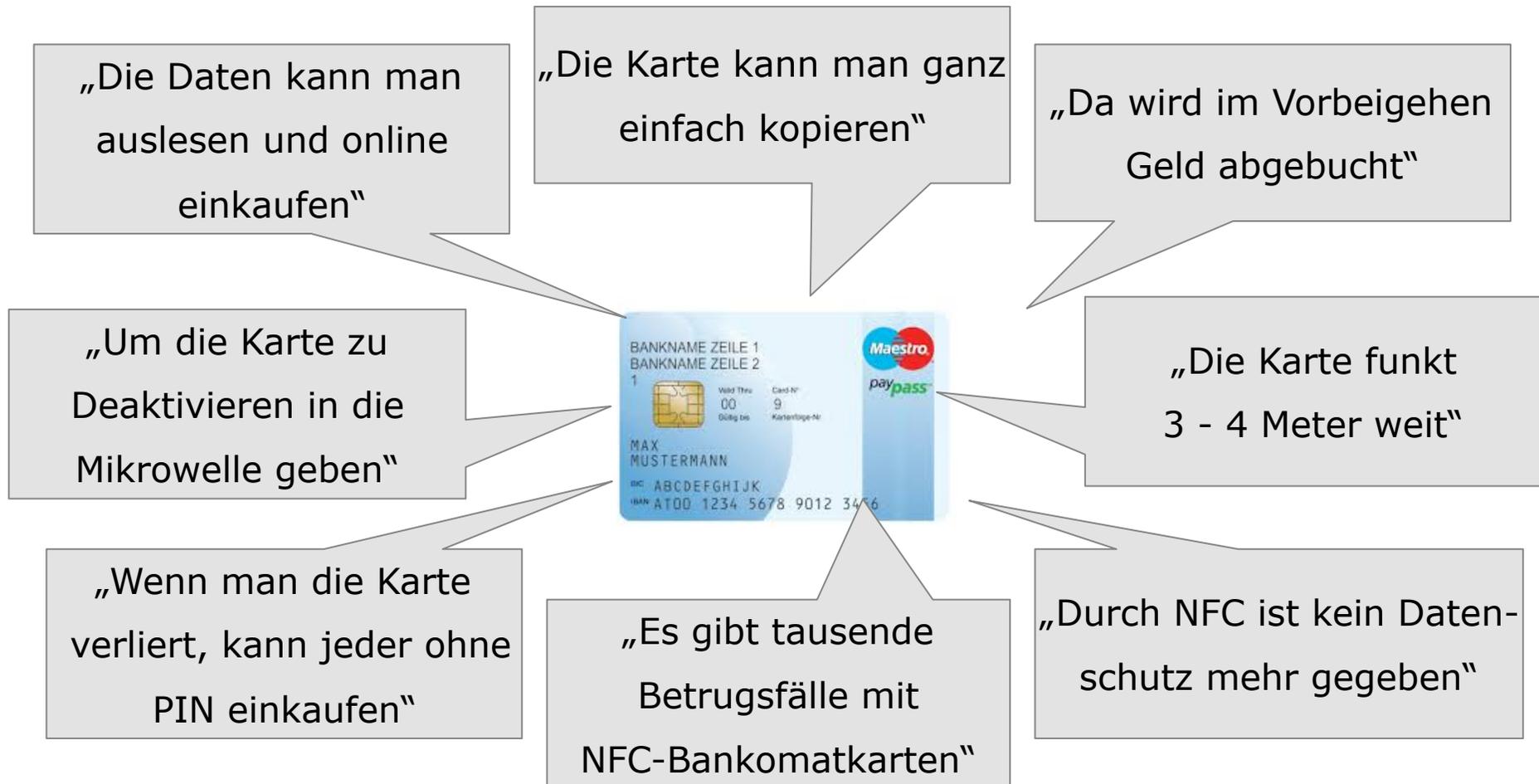


Quelle: ÖNB

# Transaktionslauf Debit, Beispiel 2



## Bezahltechnologie NFC & Vorurteile



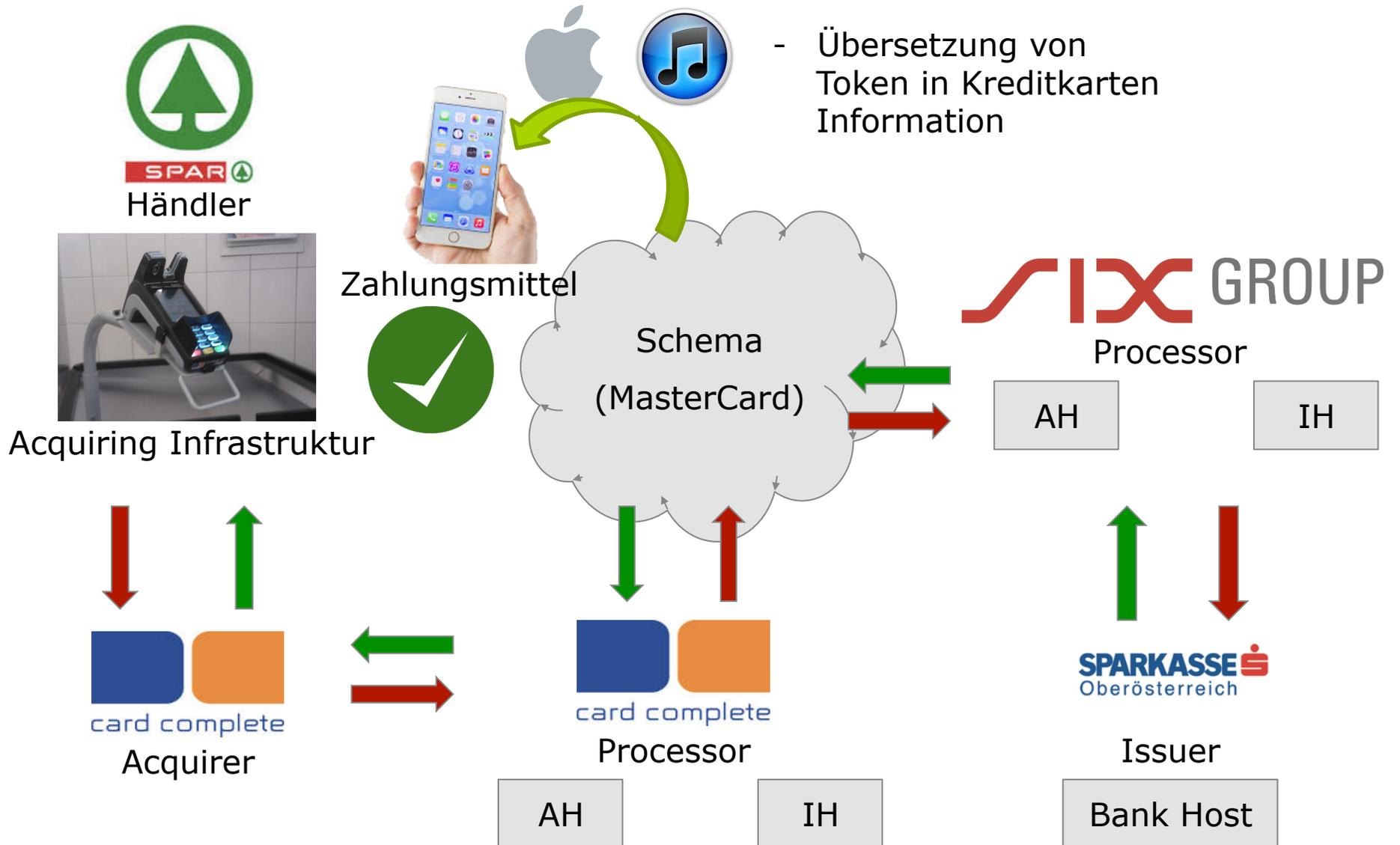
## Bezahltechnologie NFC

- ▶ Erstmals seit Einführung von Bezahlkarten kann sich das Bezahlmedium ändern.
  - ▶ Telefon
  - ▶ Sticker
  - ▶ Schlüsselanhänger
- ▶ Endgeräte brauchen dafür ein sicheres Element, in welchem die Kartendaten sicher abgelegt werden.
  - ▶ Simulation einer Chipkarte über NFC („Card Emulation“)
- ▶ Alternativ: Nutzung von kurzlebigen „Tokens“, die eine Anwendung aus dem Hintergrundsystem holt
  - ▶ Kartendaten sind im Hintergrundsystem („Cloud“) abgelegt.

## Google Wallet & Apple Pay

- ▶ Mobile Anwendung („Wallet“) am Telefon stellt die Geldbörse dar und kann mehrere virtuelle Karten beinhalten.
  - ▶ Kartendaten werden allerdings nicht im Telefon gespeichert.
  - ▶ Hintergrundsystem (zB iTunes, Google Wallet) hält Karten Daten und generiert „Einmal-Token“ mit Ablaufdatum
  - ▶ Telefon speichert die Tokens und kann diese im Bezahlungsfall an das Terminal senden via NFC.
  - ▶ Token wird vom Terminal entgegen genommen und online validiert.
- ▶ Apple & Google bekommen Informationen über Transaktionsdaten
  - ▶ Datenschutz/Privacy Issue
  - ▶ Zahlung online mit Online Verbindung möglich (Roaming)

# Tokenization Beispiel



# Issuing einer Anwendung auf ein sicheres Element

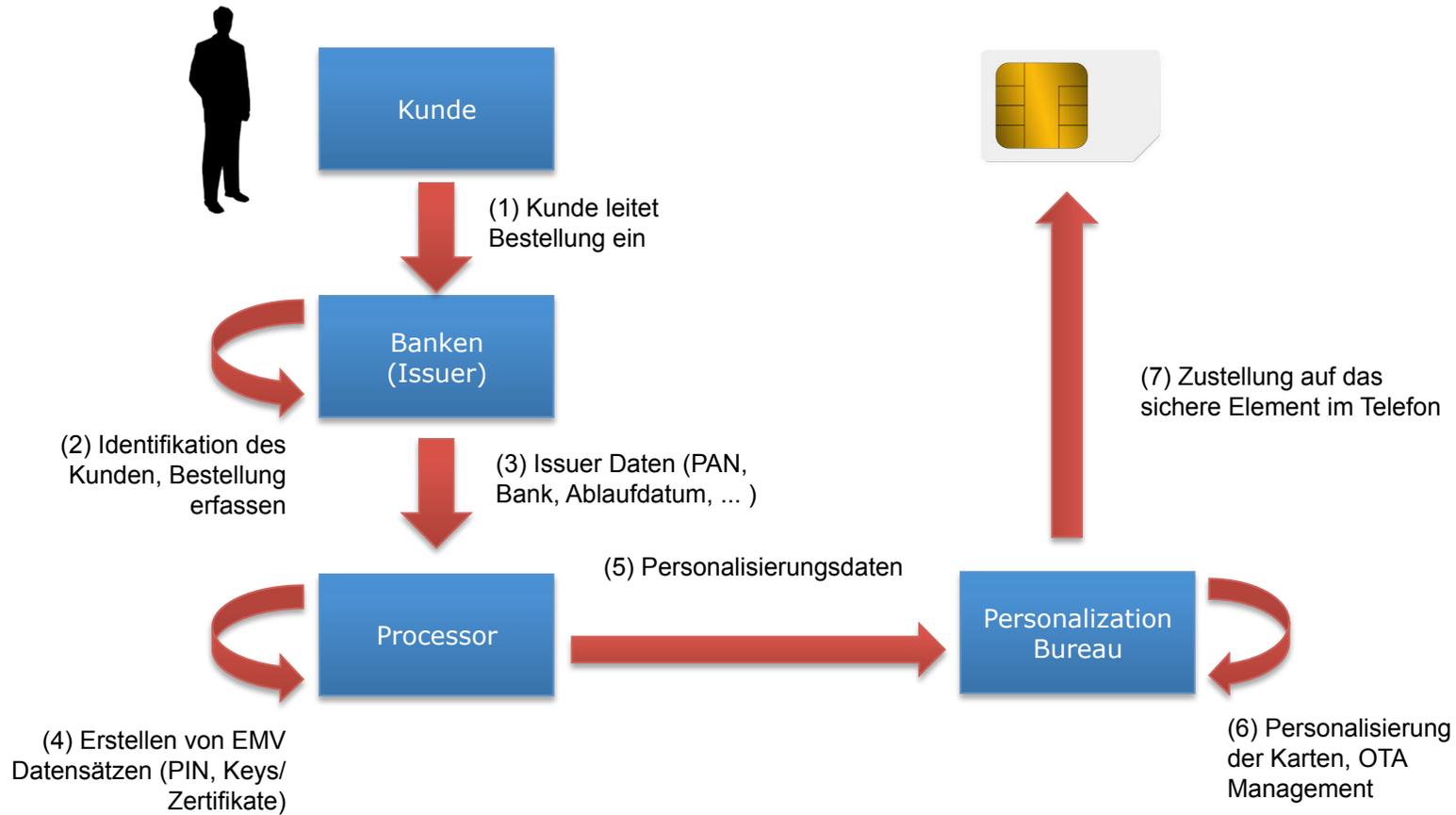
## ▶ Vorteile

- ▶ Kartendaten in einem Smartcard Chip („Sicherheit“)
- ▶ Offline Fähigkeit (Nutzung im Ausland)
- ▶ Kontrolle
- ▶ Individuelle kryptographische Sicherung jedes einzelnen Sicheren Elements

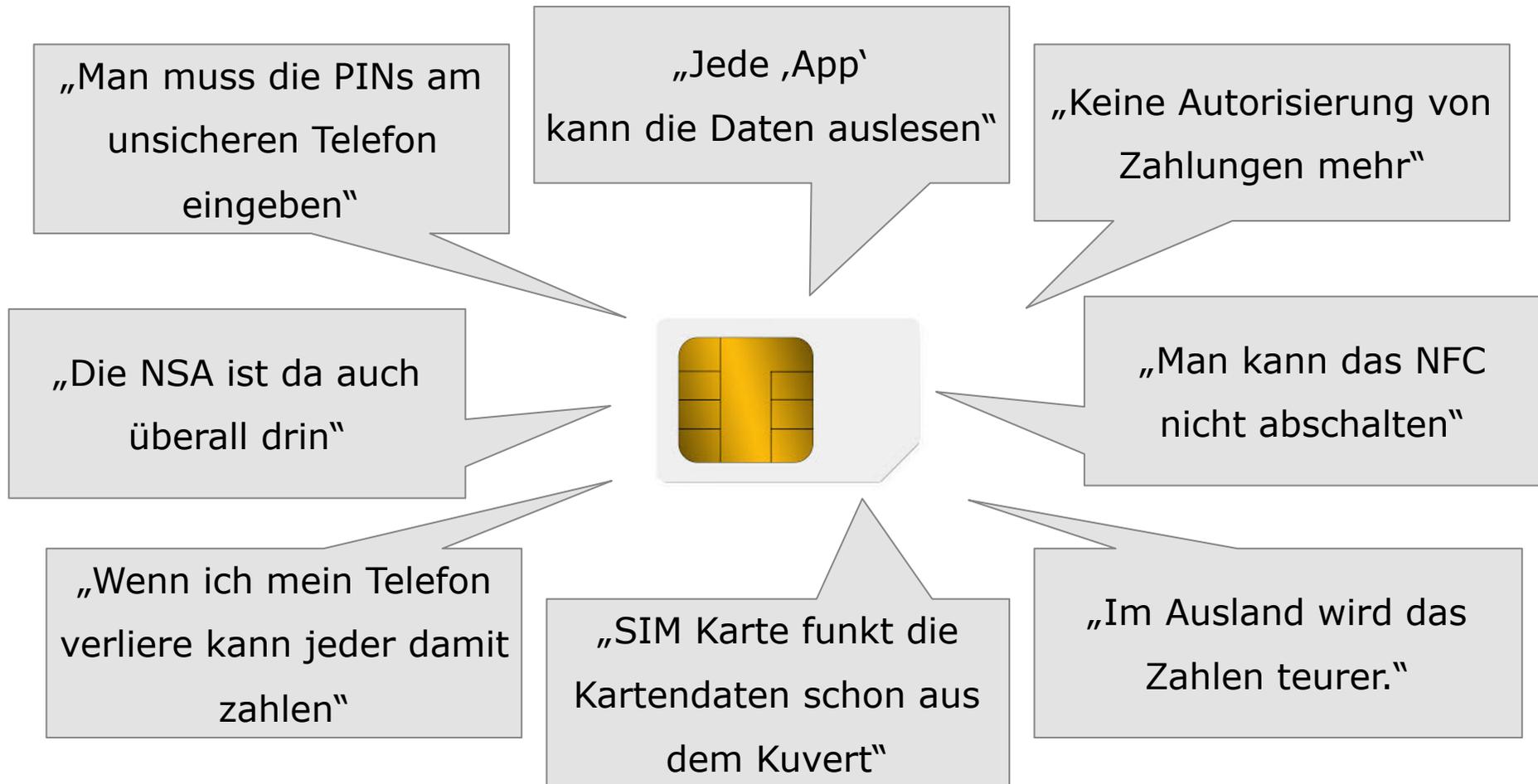
## ▶ Nachteile

- ▶ Komplexität
- ▶ Endgerät braucht sicheres Element (Kosten)
- ▶ Close-Loop Systeme wie Apple Pay

# Issuing einer Anwendung auf ein sicheres Element



## Secure Elements & Vorurteile



# Maßnahmen & Erkenntnisse

- ▶ ~~Kunden erziehen~~
  - ▶ Bequemlichkeit siegt. Immer.
  - ▶ Hohe Usability stellt Nutzerakzeptanz sicher
  - ▶ Smarte Autorisierung einer Transaktion hilft
- ▶ „Neuer 2. Faktor“ für rein mobilen Kanal (ja, kostet)
- ▶ End-2-End Verschlüsselung auf Anwendungsebene
- ▶ Gemeinsam an einer Lösung arbeiten, wenn nicht alleine realisierbar
  - ▶ 4 Augen sehen mehr als 2 (ja, kostet)
  - ▶ Aber kein blindes Vertrauen („seeing is believing“)
  - ▶ Professionalität: Wer nichts weiß, muss alles glauben
- ▶ „Zertifiziert“ heißt nicht automatisch „sicher“
- ▶ Risiko Management
  - ▶ Wissen was man tut
  - ▶ Reality Check

## Wrap up

- ▶ Mobile Payment vor allem durch NFC am POS „im Kommen“
  - ▶ Auch QR Code, Bluetooth Low Energy (BLE) für andersartige Interaktion möglich
- ▶ Wallet für Mobiles bezahlen am POS
  - ▶ Apple Pay und Google mit online-Token-Ansatz
  - ▶ Secure Element Ansatz mit offline Fähigkeit
- ▶ Kunde vertraut Apps und Endgeräten
  - ▶ Systeme müssen so gebaut sein, dass das System davon ausgehen kann, dass Apps und Endgerät nicht vertrauenswürdig sind.
  - ▶ Hohe Benutzbarkeit sicherstellen

# Mobile Payment

Vom Wirrwarr zur stabilen Realität

Forschungsgruppe für Industrielle Software (INSO)

Technische Universität Wien

Dr. Gerald Madlmayr

