
RUB

RUHR-UNIVERSITÄT BOCHUM

# Wieso, weshalb, warum... ein Schlüsselmanagement?

Sicherer Einsatz einer RFID-basierten Chipkarte im Studierendenumfeld

23. DFN-Konferenz "Sicherheit in vernetzten Systemen"
Hamburg, 10. Februar 2016

**DARIO CARLUCCIO und DR. CHRISTOPH WEGENER**

RUB

# Über die Referenten
# Dipl.-Ing. Dario Carluccio

- Ausbildung zum Kommunikationselektroniker, **Nixdorf Computer AG**
- Studium der Elektrotechnik, **Ruhr-Universität Bochum**
  - Schwerpunkte: Hochfrequenztechnik, Medizintechnik, Nanoelektronik
  - Diplomarbeit: "Electromagnetic Side Channel Analysis for Embedded Crypto Devices"
- Senior Engineer, Projektleiter, Niederlassungsleiter bei **Escrypt GmbH - Embedded Security**
- IT-Leiter (Teilzeit) der Fakultät für Elektrotechnik und Informationstechnik, Ruhr-Universität Bochum
- Freiberuflich
  - Consulting IT-Sicherheit, Schwerpunkte:
    - Konzeption, Auditierung, Dokumentation
    - Eingebettete Systeme, Chipkartensicherheit
  - IT-Security Schulungen
    - TISP - TeleTrusT Information Security Professional



*

# Über die Referenten
# Dr. Christoph Wegener

- **IT-Leiter der Fakultät für Elektrotechnik und Informationstechnik**, Ruhr-Universität Bochum
- Gründer der **wecon.it**-consulting
  - Informationssicherheit und Datenschutz

- Gründungsmitglied der **Arbeitsgruppe Identitätsschutz im Internet (a-i3)**
- Gründungsmitglied des German Chapter der **Cloud Security Alliance (CSA)**
- Gründungsmitglied der **sys4 AG**

- Auditor und **Sachverständiger**
- CCSK, CISA, CISM, CRISC
- **Zertifizierter Datenschutzbeauftragter** (GDDcert und TÜV Nord)
- Fachautor/-lektor/-gutachter, verschiedene Lehrtätigkeiten

# Agenda

- Grundlegendes zu Chipkarten
  - Einsatzgebiete und grundlegende Funktionen
  - Spezifische Risiken
- Angriffsmöglichkeiten im Überblick
  - Physische Angriffe (Karte und Terminal)
  - Logische Angriffe (Terminal und Applikation)
- Lösungsansätze
  - Technische Einsatzmöglichkeiten von Schlüsseln
  - Organisatorische Fragestellungen
- Zusammenfassung und Fazit


RUHR-UNIVERSITÄT BOCHUM

# Grundlegendes zu Chipkarten

DARIO CARLUCCIO und DR. CHRISTOPH WEGENER
*

# Grundlegendes zu Chipkarten
# Einsatzgebiete

- **Vielfältige** Einsatzgebiete
  - Ausweis- und Zutrittssysteme (Türen, Parkhäuser, …)
  - Bezahlsysteme (Offline und Online)
  - Mobilfunksysteme (SIM-Karten)
  - …
- Oft **unabhängig** von eingesetzter **Technologie** (kontaktbehaftet / kontaktlos)
- Oft **mehrere Anwendungen** pro Karte



*

# Einsatzbeispiele Ruhr-Universität Bochum

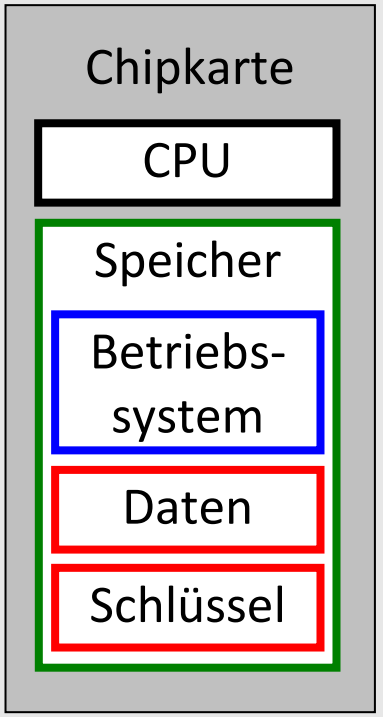
- **Bezahl**vorgänge
  - Mensen und Cafeterien *(kontaktlos)*
  - Drucken und Kopieren
  - Bibliothek
- **Zutritt**skontrolle
  - Parkraumbewirtschaftung *(kontaktlos)*
- **Authentifizierung**
  - Anmeldung am Campus-System
  - Verwaltung der Studien-/Prüfungsleistungen



*

# Grundlegendes zu Chipkarten
# Aufbau und Funktionsweise

- Eine Chipkarte beinhaltet
  - Daten- und Schlüssel**speicher**
  - Karten**betriebssystem**
  - **kryptographische Algorithmen**




- Dabei wird der Speicher oft dynamisch vergeben.

- Grundlegende Funktionen
  - **Authentisierung**
    (über Besitz, ggf. zusätzlich über Wissen)
  - Nutzung eines **sicheren** (= vertrauenswürdigen) **Speichers**
    (Kontostand, Schlüssel)
  - Zugriff auf **kryptographische Funktionen**
    (bspw. beim Einsatz von E-Mail-Verschlüsselung)

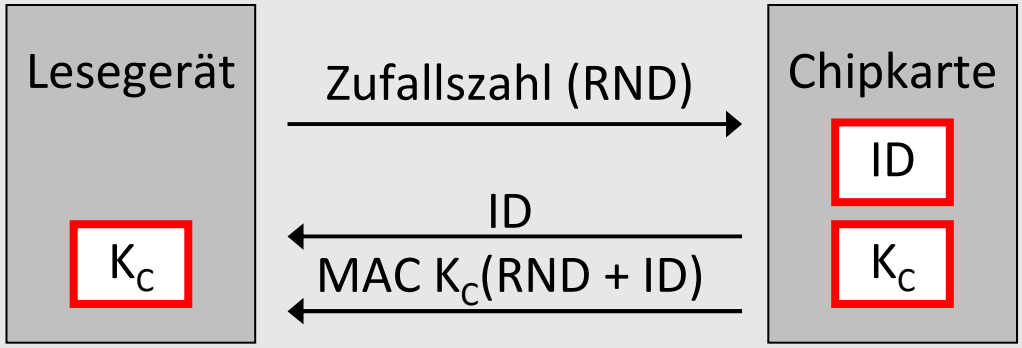


*

RUB

# Grundlegendes zu Chipkarten
# Anwendungsbeispiel Authentisierung (1)

- **Lesegerät**
  - sendet **Zufallszahl** (*RND*) an Chipkarte




- **Chipkarte**
  - bildet **kryptographische Prüfsumme** (*MAC*) und sendet Prüfsumme zusammen mit **Identität** (*ID*) zurück.
  - Dazu wird der **interne Schlüssel** ($K_C$) verwendet.

- **Lesegerät**
  - prüft die **empfangene Antwort** (*MAC* und *ID*)
  - und muss dazu den internen **Schlüssel** $K_C$ der Karte **kennen**.

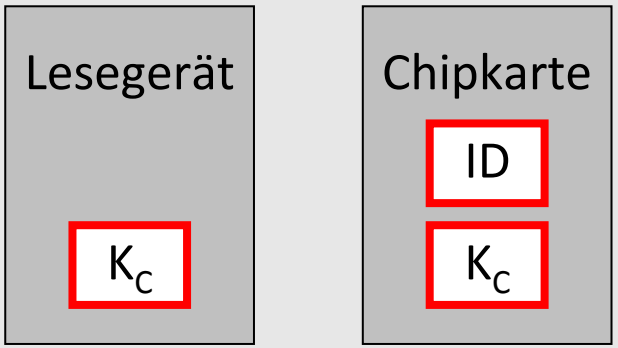


*

# Grundlegendes zu Chipkarten
# Anwendungsbeispiel Authentisierung (2)

- Anforderungen an das System
  - muss **Schlüssel $K_C$ schützen** (Aspekt der **Vertraulichkeit**)
  - muss **Identität *ID* schützen** (Aspekt der **Integrität**)

- System gebrochen, falls …
  - **Schlüssel $K_C$ bekannt** wird
  - **Identität *ID* unberechtigt geändert** werden kann.

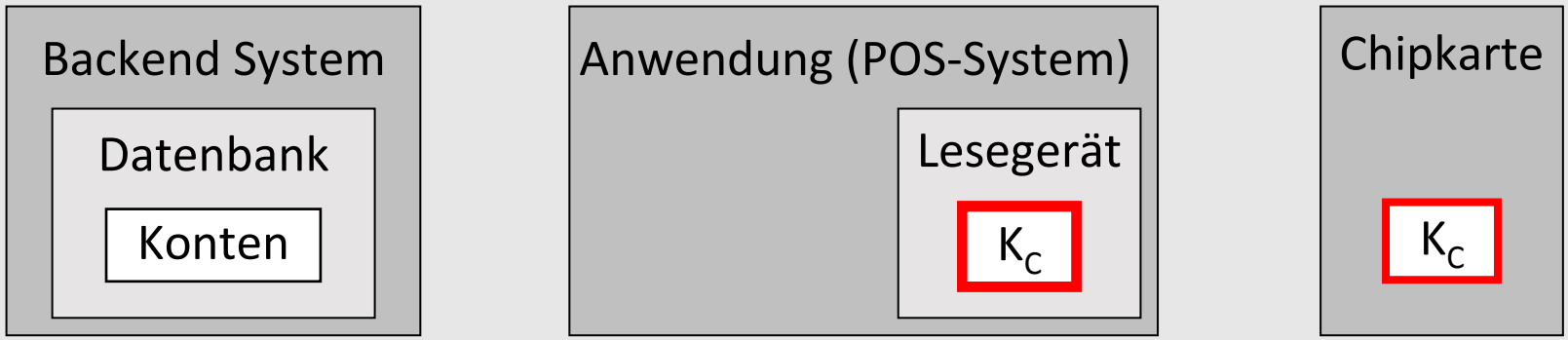





*

# Grundlegendes zu Chipkarten
# Grundlegende Probleme

- **System** besteht aus mehreren, teilweise **zahlreichen Komponenten**, die entsprechend zu schützen sind
  - Karte und Lesegerät
  - Client- und Backend-System




- Keine vollständige Kontrolle des Betreibers über die eingesetzten Karten
  - **Nutzer** hat **physischen Zugriff** auf die Karten
  - Und damit **weitreichende Angriffsmöglichkeiten**



*

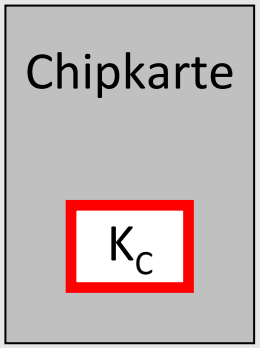

RUHR-UNIVERSITÄT BOCHUM

# Angriffsmöglichkeiten im Überblick

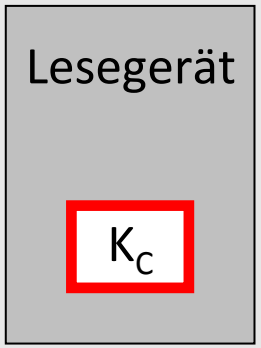
DARIO CARLUCCIO und DR. CHRISTOPH WEGENER

# Angriffsvektoren (1)

- Angriff auf die **Chipkarte**
  - Schlüssel $K_C$ wird bekannt
  - Immenser Schaden möglich, falls nur ein $K_C$ für alle Applikationen und/oder Karten
  - Identität *ID* kann manipuliert werden

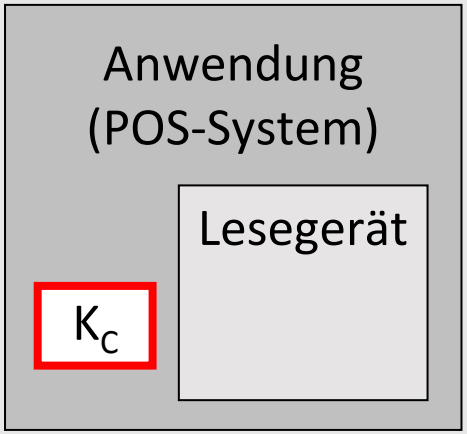



- Angriff auf den **Kartenleser**
  - Schlüssel $K_C$ wird bekannt
  - Immenser Schaden möglich, falls nur ein $K_C$ für alle Applikationen und/oder Karten
  - Karte kann unberechtigt genutzt werden

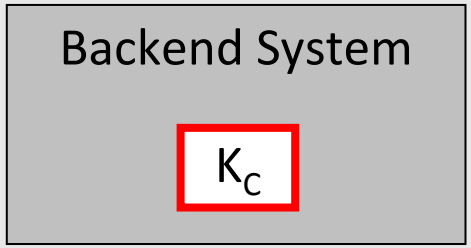


# Angriffsvektoren (2)

- Angriff auf die **Anwendung**
  - Schlüssel $K_C$ wird bekannt
  - Immenser Schaden möglich, falls nur ein $K_C$ für alle Applikationen und/oder Karten
  - Unberechtigte Aktionen möglich




- Angriff auf das "**Backend System**"
  - Schlüssel $K_C$ wird bekannt
  - Immenser Schaden möglich, auch wenn Schlüssel $K_C$ pro Karte verschieden



# 100%ige Sicherheit oder Bullshit-Bingo ;)

- Das Ziel ist 100%ige Sicherheit!
  - **100%ige Sicherheit gibt es nicht !!!!elf!!**
- Sinnvoller Ansatz: ein **Risiko-basiertes** Vorgehen
  - **Schaden** bei einem erfolgreichen Angriff **minimieren**

- Ein **Angriff** darf **nicht** das **gesamte System betreffen**
  - Systemweit identische Schlüssel vermeiden
  - Schlüssel nur in geschützter Umgebung einsetzen und besonders sichern
- **Angemessenes Schlüsselmanagement** erforderlich!

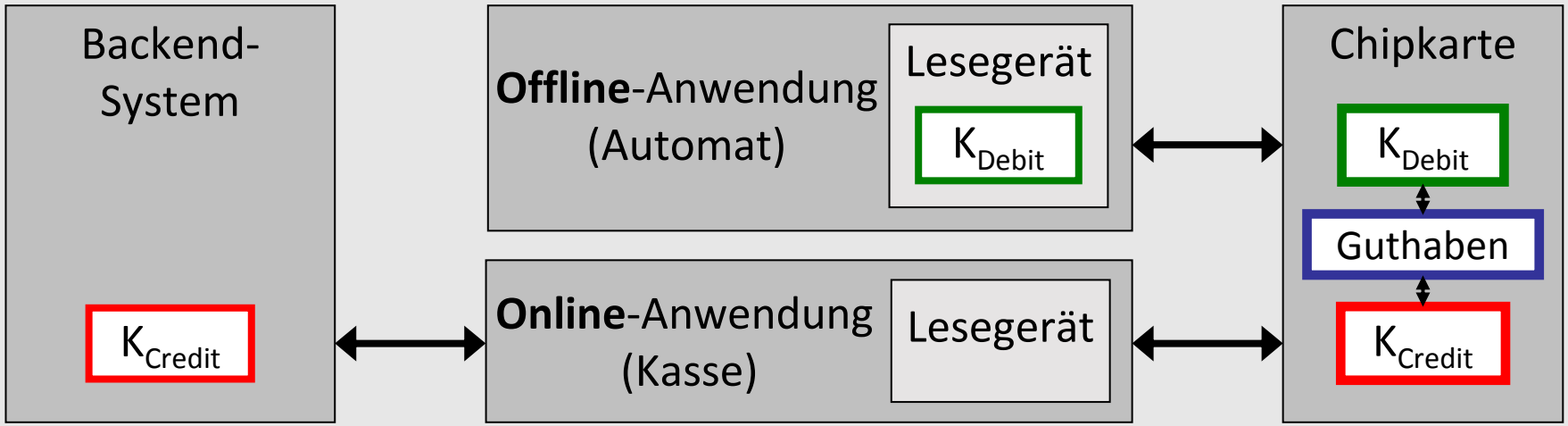

RUHR-UNIVERSITÄT BOCHUM

# Lösungsansätze

DARIO CARLUCCIO und DR. CHRISTOPH WEGENER

# Nutzung Funktions-spezifischer Schlüssel Beispiel "Mifare DESFire EV1"

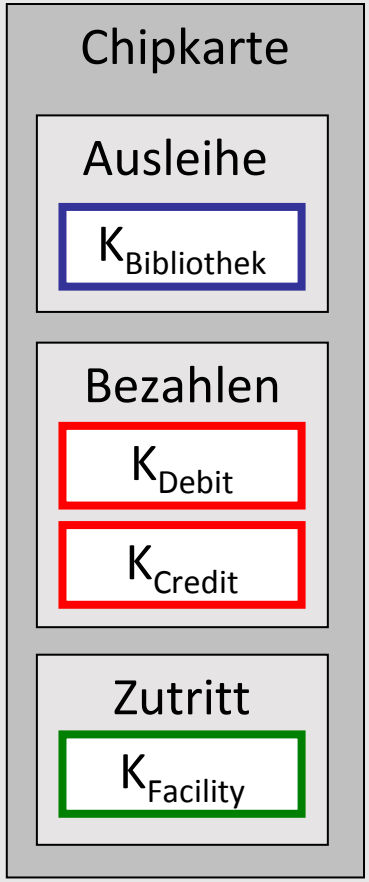
- Für **unterschiedliche Funktionen** innerhalb einer Anwendung auf der Karte werden **unterschiedliche Schlüssel** verwendet
- Beispiel: Zahlungskarten mit unterschiedlichen Schlüsseln zum Aufbuchen (*Credit Key*) und Bezahlen (*Debit Key*)
  - Der **Debit Key** ist (aus Betreibersicht) **unkritischer** als der Credit Key.
  - Dies hat Folgen für die notwendigen Sicherheitsannahmen.



# Nutzung Applikations-spezifischer Schlüssel Beispiel "Mifare DESFire EV1"

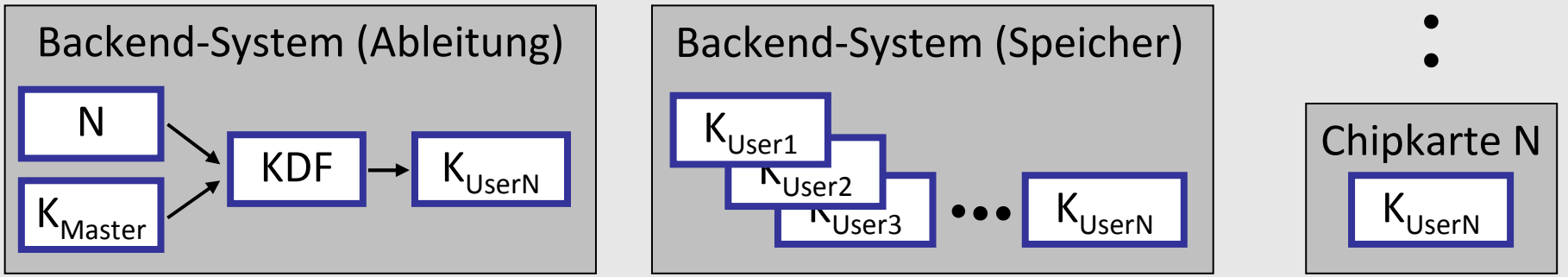
- Für **jede Anwendung** auf der Karte werden **spezifische Schlüssel** verwendet
- Bei Bekanntwerden **eines Schlüssels** ist nur die **jeweilige Applikation** direkt betroffen

- Schützt nicht vor Angriffen auf die Karte, falls kein Karten-spezifischer Schlüssel
- Schützt vor Angriffen auf das Backend eines Applikationsinhabers
  ➲ andere Applikation sind nicht betroffen



# Einsatz Karten-spezifischer Schlüssel

- Jede Karte nutzt **spezifische Schlüssel**
- Ein Angreifer erhält durch Angriff auf eine einzelne Karte nur deren spezifischen Schlüssel
  - Angriff auf alle Karten skaliert i.d.R. nicht
- Erfordert aber eine "**Schlüsselverwaltung**"
  - **Ableitung** der Karten-spezifischen Schlüssel aus einem ***Master Key***
  - Alternative: Speichern aller ausgegebenen Schlüssel (benötigter Speicher bei 100.000 Nutzern ca. 2,4 MB)



# Speicherort der Schlüssel

- Neben der Karte hat der Angreifer **weitere Möglichkeiten**, an den/die Schlüssel $K_C$ zu gelangen
  - am **Kartenleser**
  - am **Client**-System (bspw. dem PC)
  - auf dem **Backend**-System

- Bestmöglicher Schutz durch **Authentisierung im Backend**
  - Backend-System kann gut gesichert werden
  - **Zugriff** auf die Schlüssel im Backend **speziell absichern** (bspw. mittels **Mehr-Augenprinzip**)



*

# Organisatorische Maßnahmen – 1

- Initiale Bedatung der Karten
  - Von wem werden die **Schlüssel** wie **erzeugt**?
  - Wie werden die Schlüssel **transportiert**?
- Übergabe von Applikationen auf der Karte
  - Gibt es eine **Richtlinie** für die Übergabe von Applikationen?
  - Werden **Transportschlüssel** eingesetzt?
- Schlüsselbackup
  - Wie können die Schlüssel im Verlustfall **reproduziert** werden?

# Organisatorische Maßnahmen – 2
# Beispiele zum Schlüsselbackup

- Einfache Möglichkeit
  - **Ausdruck** aller Schlüssel
  - Einfach, **skaliert** aber **nicht** gut

```
K = 462d72de05994b7f
    58394dffaedf4634
```

- Vier-Augenprinzip
  - **Aufteilen** des Schlüssels
  - Einfach, aber **nur** für **vier Augen** einfach umsetzbar

```
K1= 462d72de05994b7f
```

```
K2= 58394dffaedf4634
```

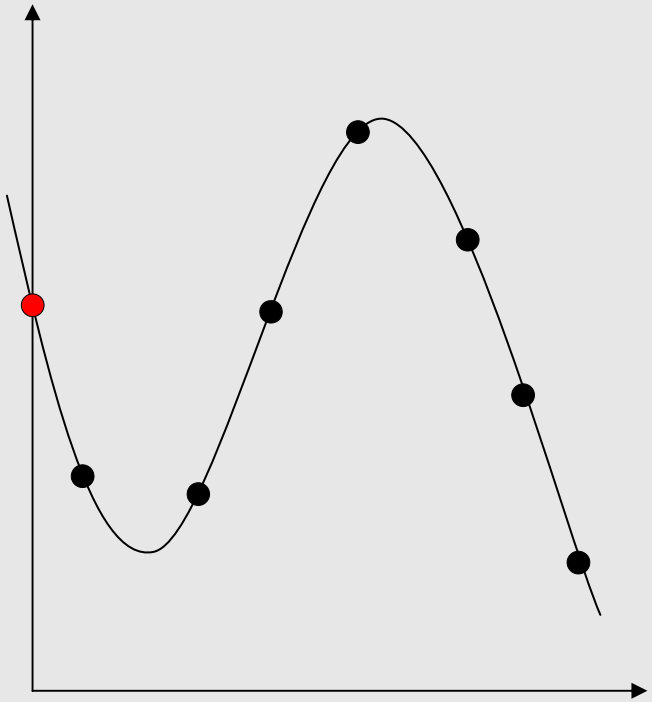
- Mehr-Augenprinzip mit *m aus n*
  - Vorgehen analog zu **Shamir's Secret Sharing**

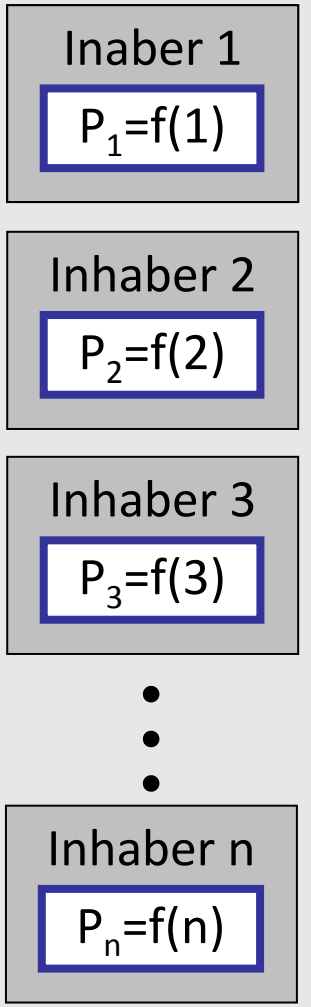


*

# Organisatorische Maßnahmen – 3
# **Shamir's Secret Sharing**

- Polynom vom Grad *m-1*
- Geheimnis = f(0)
- Jedem der *n* Nutzer ist ein Punkt auf der Kurve bekannt, z.B.:
  - Nutzer 1: f(1)
  - …
  - Nutzer *n*: f(n)
- Das Polynom kann mit beliebigen *m* Punkten rekonstruiert und so das geteilte Geheimnis f(0) ermittelt werden.








*

# Das S5-Modul zur Schlüsselableitung

- HW-Basis ist **RaspberryPi**
- Anbindung über **serielle Schnittstelle** (ausschließlich!)
- Stromausfall und Öffnen des PC-Gehäuses führen zur **Löschung** des **Master-Schlüssels**
- Schlüsseleingabe mittels **Mehr-Augen-Prinzip** auf Basis von **Shamir's Secret Sharing**


Bild von Daniel Moczarski, RUBITS



*


RUHR-UNIVERSITÄT BOCHUM

# Verantwortlichkeiten

DARIO CARLUCCIO und DR. CHRISTOPH WEGENER

*

# Wer hat Verantwortung für das Schlüsselmanagement?

- Derjenige, der im Falle eines Angriffes **mit** der **Karte in Verbindung** gebracht wird.

- Der **Herausgeber** der **Karte** für
  - die Schlüssel des Betriebssystems (*PICC Master Key*) und
  - die Schlüssel der Kernanwendungen (Studierendenausweis).

- Der **Inhaber** der **Applikation** für
  - die Schlüssel seiner Applikation.



*

# Konsequenzen eines Angriffs

- **Konsequenzen** eines erfolgreichen Angriffs
  - auf **eine Applikation** wirkt sich **nur dort** aus.
  - auf **das Betriebssystem** wirkt sich auf **alle Applikationen** aus.
  - die **Privacy** kann nach einem **erfolgreichen Angriff nicht** mehr **garantiert** werden.


RUHR-UNIVERSITÄT BOCHUM

# Zusammenfassung und Fazit

DARIO CARLUCCIO und DR. CHRISTOPH WEGENER

# Zusammenfassung und Fazit

- Einsatz von "Chipkarten" **erfordert** ein sinnvolles **Schlüsselmanagement**
  - Schlüssel finden sich an **zahlreichen Orten**
  - **All diese** gilt es entsprechend zu **sichern**!
- Ohne entsprechende Maßnahmen nützt die sicherste Chipkarte nichts!
- **Gute Planung im Vorfeld** ist notwendig für den **Erfolg** des Gesamtprojekts!

# Kurze Checkliste

- **Anforderungen analysieren**
  - Wer soll (muss!) Zugriff auf welche Daten haben?
  - Wer ist für die einzelnen Prozesse verantwortlich?
- Passende **Schlüssel nutzen**
  - Funktions-/Applikations-/Karten-spezifische Schlüssel
- **Organisatorischen Maßnahmen** treffen
  - Transportschlüssel nutzen und ändern
  - Mehr-Augen-Prinzip beim Zugriff auf Schlüssel nutzen
  - Klare Verantwortlichkeiten definieren
- **Gesamtsystem** im Auge behalten
  - "Eine Kette ist nur so stark wie ihr schwächstes Glied!"

# …aber wir kaufen doch eine fertige Lösung!

- Aussagen gelten auch, wenn man eine fertige Lösung kaufen will
  - Genaue **Spezifikation** der Anforderungen **notwendig**!
  - **Anbieter** haben i.d.R. **kein intrinsisches Interesse**
  - Man muss sie "überzeugen" ;)

- Auch im Nachgang ist eine **Migration** zu einer **sicheren Lösung** denkbar und **möglich**!

# Danke für Ihre Aufmerksamkeit ☺

Dario Carluccio
dario.carluccio@rub.de

Dr. Christoph Wegener
christoph.wegener@rub.de