# TUD-Chipkarte

## Digitale Identität
## für Studierende und Bedienstete

**Ronny John**
**Technische Universität Darmstadt**
**Hochschulrechenzentrum (HRZ)**

# Inhalt

*„Die TUD-Chipkarte als digitale ID*
*für Studierende und Bedienstete*
*der Technischen Universität Darmstadt“*

1. Projekt TUD-Chipkarte
2. PKI und Kartenmanagement
   → Fokus auf Prozesse für „Bedienstetenkarte“

# ❶ Projekt TUD-Chipkarte

TUD Chipkarte („TUDCard“) für Studierende und Bedienstete

- Funktionen und Anwendungen
- Kartentechnik und Karteninhalt
- Organisation



RJ

## Folie 3

**RJ5**

Aussehen:
- Vorder- und Hinterseite im TUD-Design
- sichtbarer Kryptoprozessor und eingebetter, unsichtbarer Funkchip
- Nummer für Bezahlfunktion auf Vorderseite
- optisch anonym“ --> ohne Foto, Name, Matrikel-Nr., R/W-Folie

Ronny John; 05.09.2006

# Projekt TUD-Chipkarte

1. Funktion „Digitale Identität“
   - Authentifizierung
     - Zugang zu Webanwendungen und Webseiten
       - E-Learning (Clix, Autorenwerkzeuge)
       - Verwaltungsanwendungen (HISPOS, HISLSF)
       - Unterlagen für Vorlesung und Übungen
     - mobiler Internet-Zugang über VPN
     - SmartCard-Logon in den HRZ-Rechnerpools
   - Signatur und Verschlüsselung
     - Signatur und Verschlüsselung von E-Mails und Dateien
     - signaturbasierte Zutrittskontrolle (HRZ-Rechnerpool)
2. Bezahlfunktion
   - Bargeldlos an alle Kassen und Automaten

# Kartentechnik und Karteninhalt

- Aussehen
  - optisch anonym“ → ohne Foto, Name, Matrikel, R/W-Streifen
- Kryptoprozessor
  - „Digitale Identität“ in Form eines Schlüsselpaares und Zertifikat mit Name, E-Mail und Benutzername des Inhabers
    - getrennte Schlüsselpaare für Signatur und Verschlüsslung
  - privater Schlüssel nicht auslesbar und mit PIN geschützt
  - kontaktbehaftet, 1024 Bit RSA, TCOS 2.03
- Funkchip
  - „elektronische Geldbörse“ mit Nummer für Bezahlfunktion (Schattenkonto), PKZ, Saldo, letzte Transaktion
  - Bezahlfunktion anonym: physische und logische Trennung zwischen „digitaler Identität“ und Bezahlfunktion
  - kontaktlos im Kartenkörper integriert, Typ „Mifare“

# Projekt TUD-Chipkarte

## Organisation

- Studierende erhalten erste Karte kostenlos
  - für die Gesamtdauer des Studiums gültig
- Karten für Bedienstete zentral finanziert
- „Roll-Out“ und Nutzung der Karten
  - Versand per Post durch externen Projektpartner oder über Hauspost
  - Kartenaktivierung mit selbstentwickeltem „Card Manager“
- Bezahlfunktion nach ersten Aufladevorgang aktiv
- Kartenverwaltung durch das Nutzerbüro des HRZ
  - Kartenverlust, Kartendefekt, Sperre, Neuausgabe
- Clearingstelle Bezahlfunktion: Studentenwerk Darmstadt

# ❷ PKI und Kartenmanagement

## Public-Key Infrastruktur (PKI)

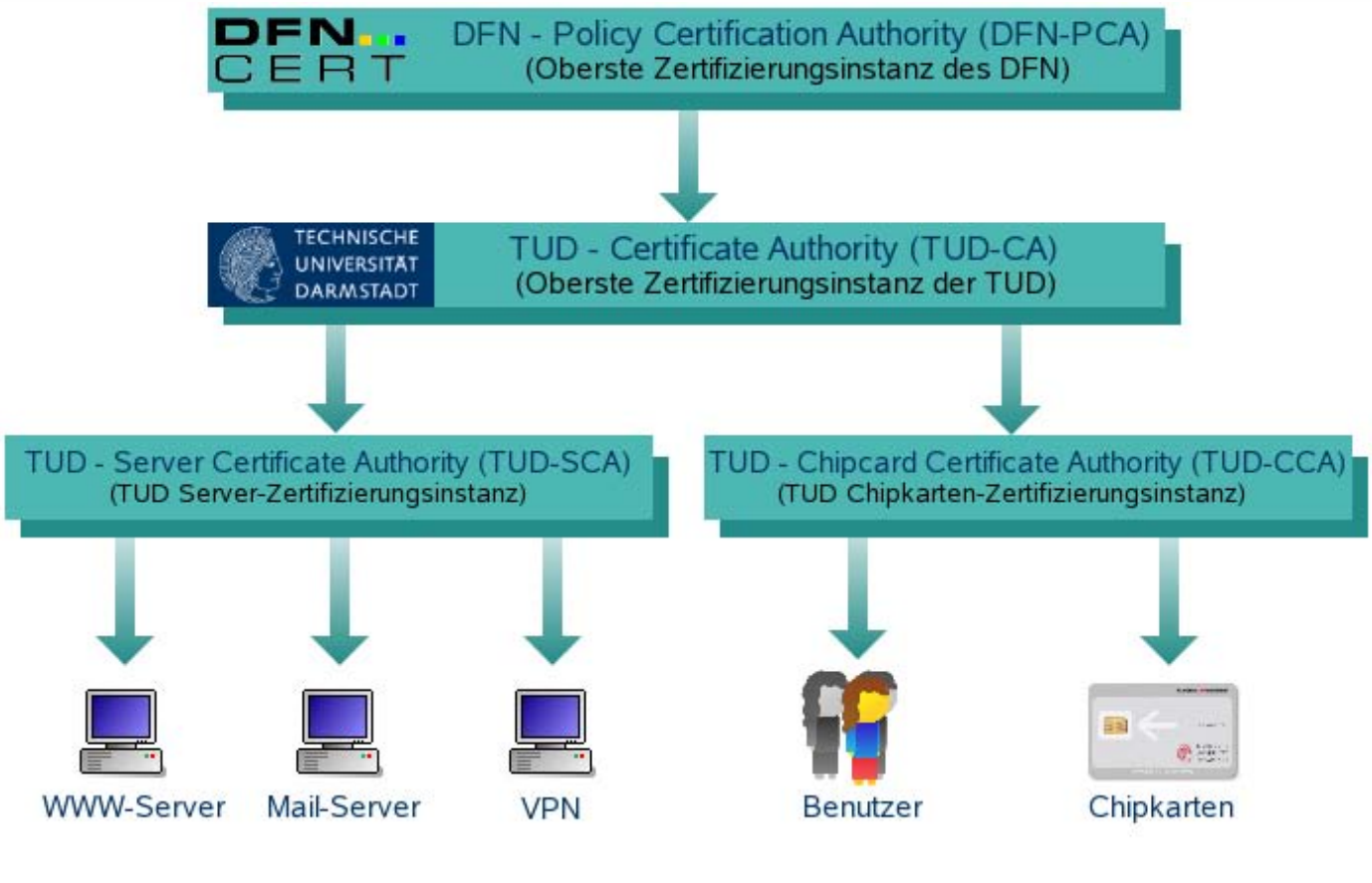
- Zertifizierungshierarchie
- Komponenten der PKI
- Verknüpfung der PKI-Komponenten
- **Registrierung durch Identitätsmanagement**

## Kartenmanagement

- Architektur
- **Kartenaktivierung**
- Key-Backup und Key-Recovery

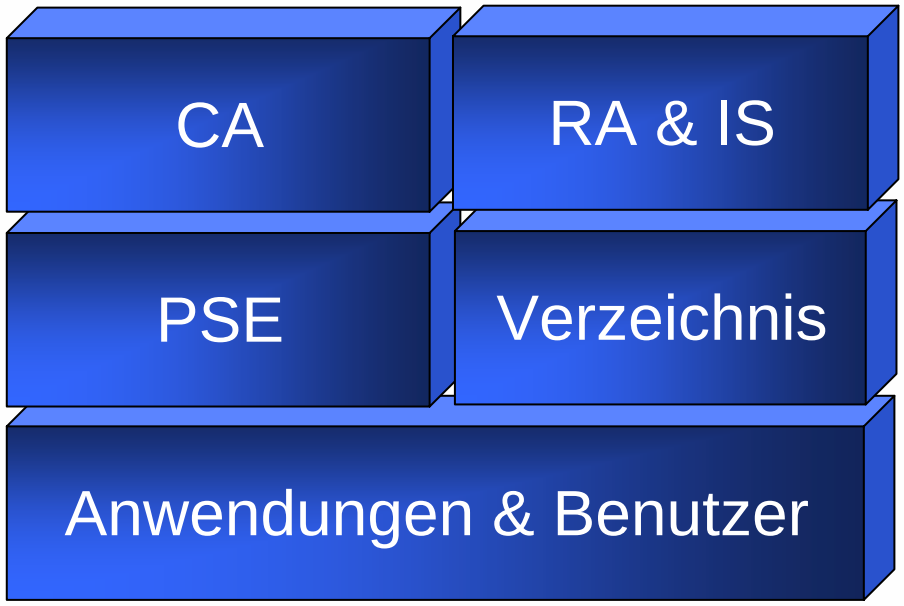
# PKI und Kartenmanagement

- Zertifizierungshierarchie



# PKI und Kartenmanagement

- Komponenten der PKI
  - CA, RA & IS: Trustcenter Software „FlexiTrust“ (FlexSecure GmbH)
  - PSE: TUD-Chipkarte
  - Verzeichnis: Novell eDirectory



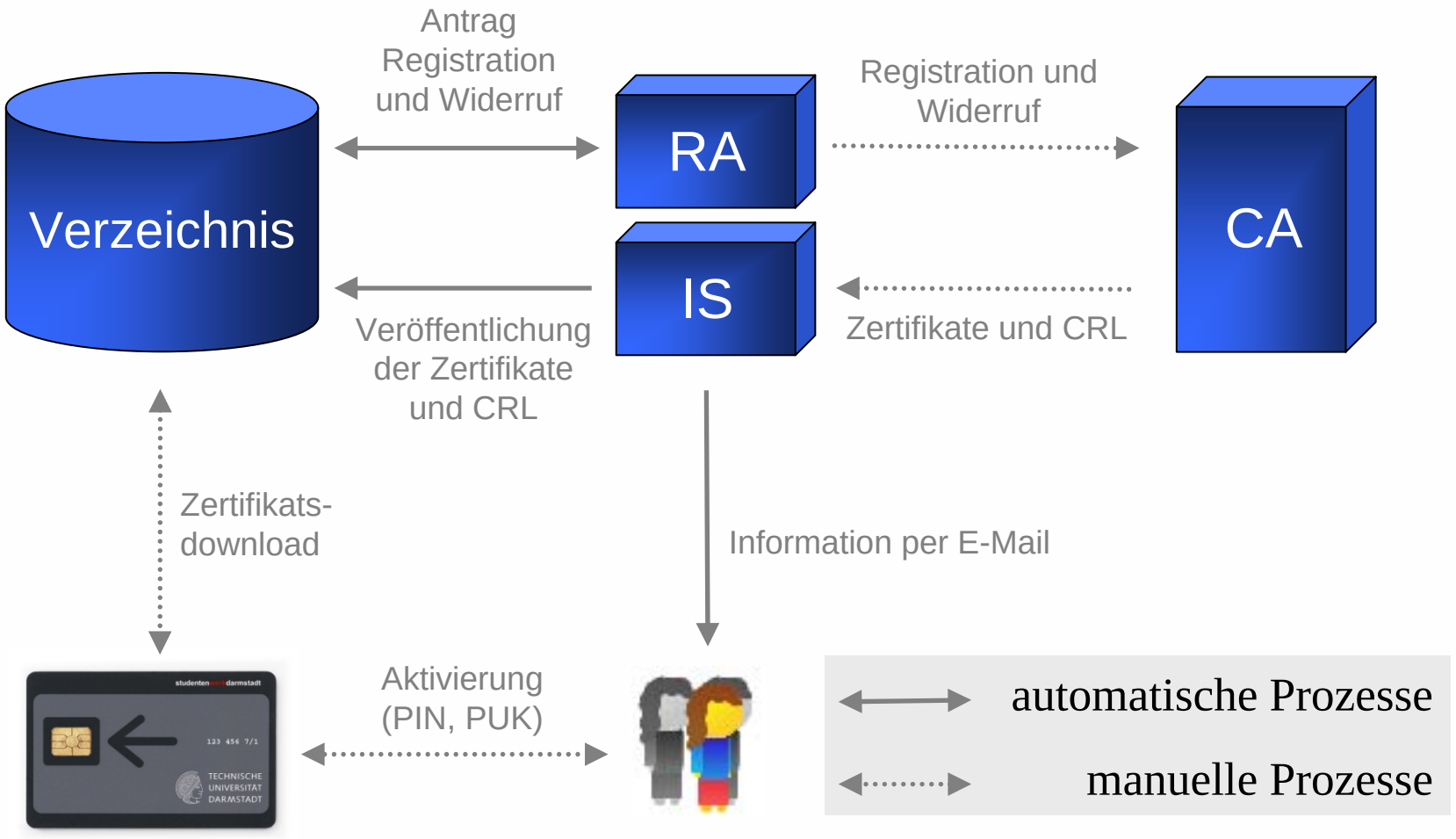

CA: Certification Authority

RA: Registration Authority

IS: Infrastructure Services

PSE: Personal Security Environment

# Verknüpfung der PKI-Komponenten



# Registrierung durch Identitätsmanagement (1)

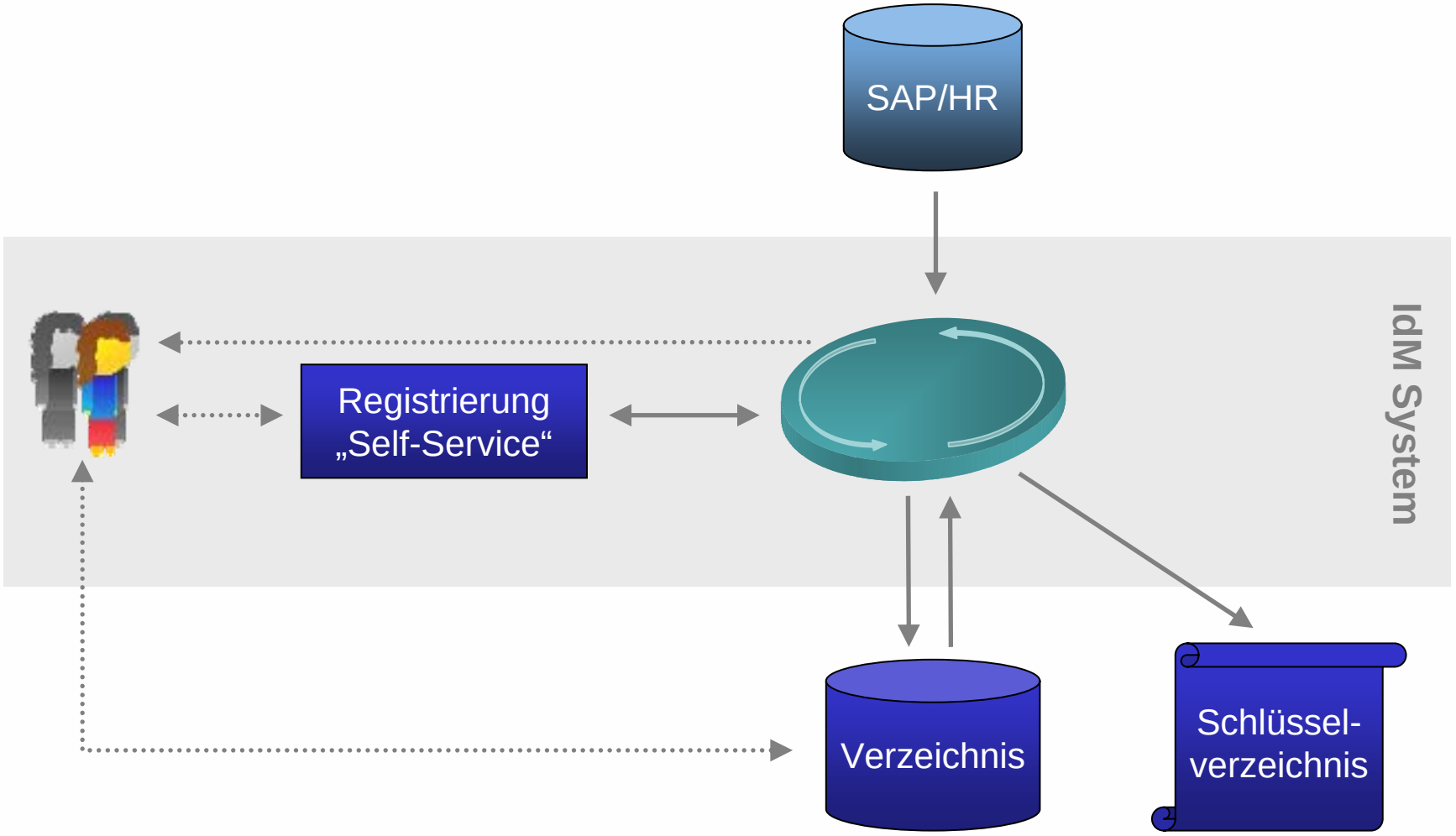
1. Datenimport aus SAP/HR
   - implizite Prüfung der Identität (Einstellung - Personalbogen)
   - alle Bediensteten werden im IdM als Identitäten erfasst
   - automatische Pflege der Daten
2. Einmalige Registrierung im web-basierten „Self-Service“
   - Information über gespeicherte Daten
   - Auswahl eines Benutzernamen – „TUD-ID“
   - Passwort setzen
   - ggf. Verknüpfung mit bisherigen („alten“) Benutzerkonto
   - Abfrage weitere Daten, die nicht in SAP/HR gepflegt werden:
     - E-Mail Adresse (…@xxx.tu-darmstadt.de)
     - dienstl. Telefon- und Faxnummer
     - Gebäude- und Raumnummer des Arbeitsplatzes

- Registrierung durch Identitätsmanagement (2)
  3. Erstellung eines Accounts im Benutzerverzeichnis
     - nach Registrierung
     - abgeleitet und verknüpft mit Identität im IdM
     - Basis für Chipkartenverwaltung
  4. Ausgabe einer Chipkarte an den Bediensteten
     - nach Registrierung
     - Nummer und öffentlicher Schlüssel der ausgegebenen Karte wird zusammen im Account vermerkt
     - direkte Identifikation über Chipkarte möglich: privater Schlüssel Karte → Kartennummer → öffentlicher Schlüssel Account

# Registrierung durch Identitätsmanagement (3)

5. Zertifikatsantrag
   - erfolgt automatisch, wenn alle Daten im Benutzerverzeichnis vorhanden:
     - Name und E-Mail Adresse
     - ausgegebene (zugewiesene) Chipkarte
   - RA prüft online Status im Benutzerverzeichnis und erstellt automatisch einen Zertifizierungsantrag
6. Veröffentlichung des Zertifikats
   - automatisch nach Generierung durch die CA
   - Schlüsselverzeichnis = Personenverzeichnis
     - Verteilung / Synchronisation durch IdM
   - Speicherung des Zertifikats auf die Chipkarte

# Registrierung durch Identitätsmanagement (4)



# Registrierung durch Identitätsmanagement (5)

- Vorteile
  - Insgesamt nur zwei Kontakte
  - Bedienstete müssen nicht persönlich erscheinen
    - Brief mit PIN für Registrierung per Hauspost
    - Versand der Karte per Hauspost
    - Registrierung des Accounts im web-basierten „Self-Service“
  - Aktivierung der Karte + Zertifikatsdownload per „Card Manager“
    - Java „Web Start“ - Anwendung
    - am Arbeitsplatz oder zentralen Kiosk-PCs
  - Registrierung einfach
    - geringer Personalaufwand
  - Erhalt der Gesamtsicherheit der PKI

## Kartenmanagement: Architektur (1)

- in das Benutzerverzeichnis integrierte angepasste Trustcenter-Software (RA & IS)
  - bekannt → Nutzung bestehender Ressourcen
  - zentralisiert und sicher (Redundanz, Backup…)
  - hohe Automatisierung und skalierbar
- Verwendung vorbeschlüsselter Chipkarten
  - öffentlicher Schlüssel sofort bekannt und nach Versand für Zertifizierung verfügbar
- Versand per Hauspost
  - Reduzierung des Betreuungspersonals
  - besserer Service für die Bediensteten

# Kartenmanagement: Architektur (2)

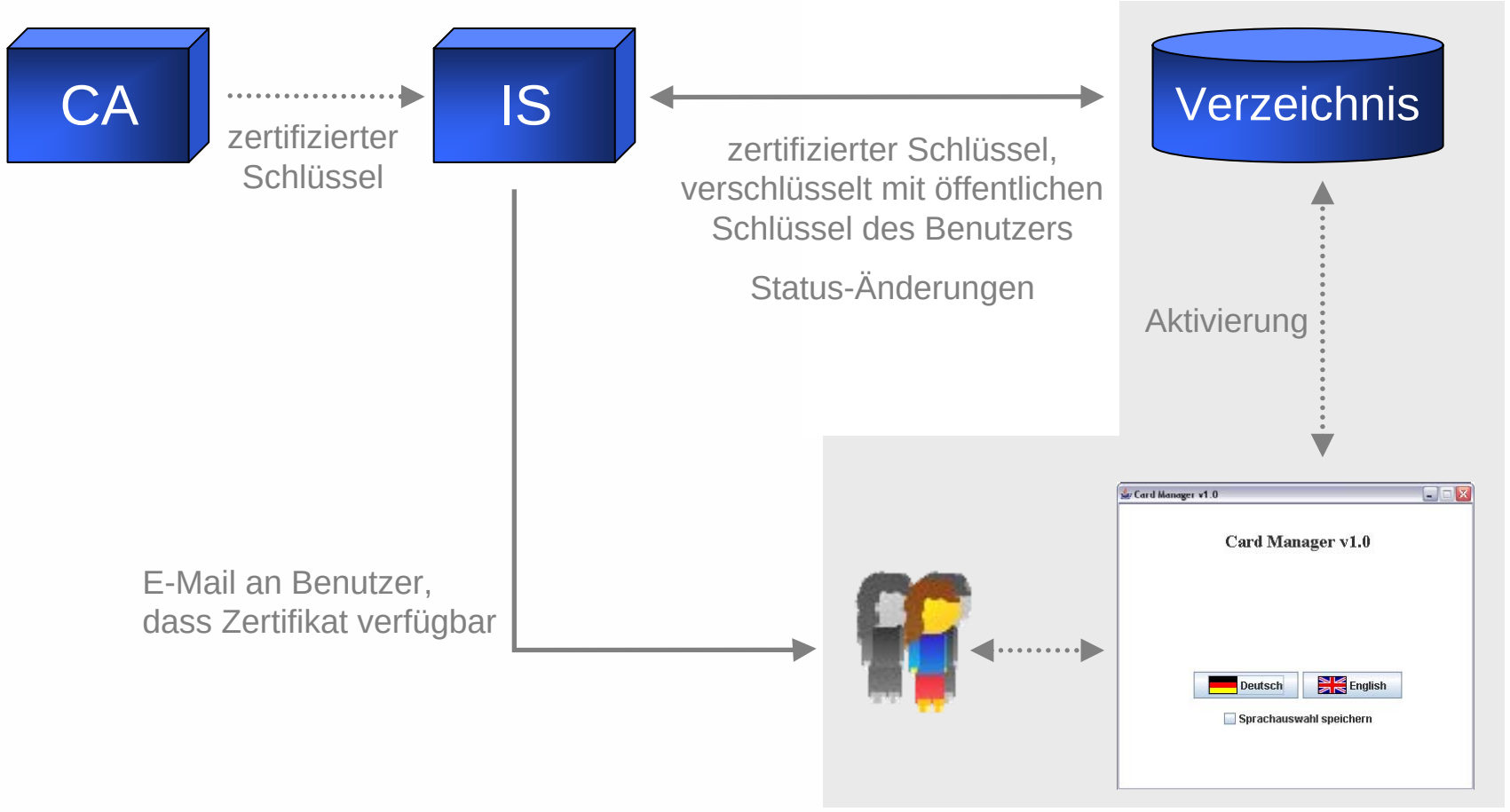
- kein PIN-Brief
  - einfacher Kartenversand und flexible Kartenausgabe (Ersatz…)
  - „Null-PIN“ Verfahren: eigene Überprüfung, ob Karte bereits eingesetzt wurde
  - „blinded PUK“ auf der Karte (mit öffentlichen Schlüssel verschlüsselt)
  - Stärkung der Vertrauenswürdigkeit
- „Card Manager“ als Java „Web Start“ - Anwendung
  - Kartenaktivierung im „Self-Service“
  - Java, damit plattformunabhängig
  - einfache Administration (Beispiel: Aktualisierung der Software)

# PKI und Kartenmanagement

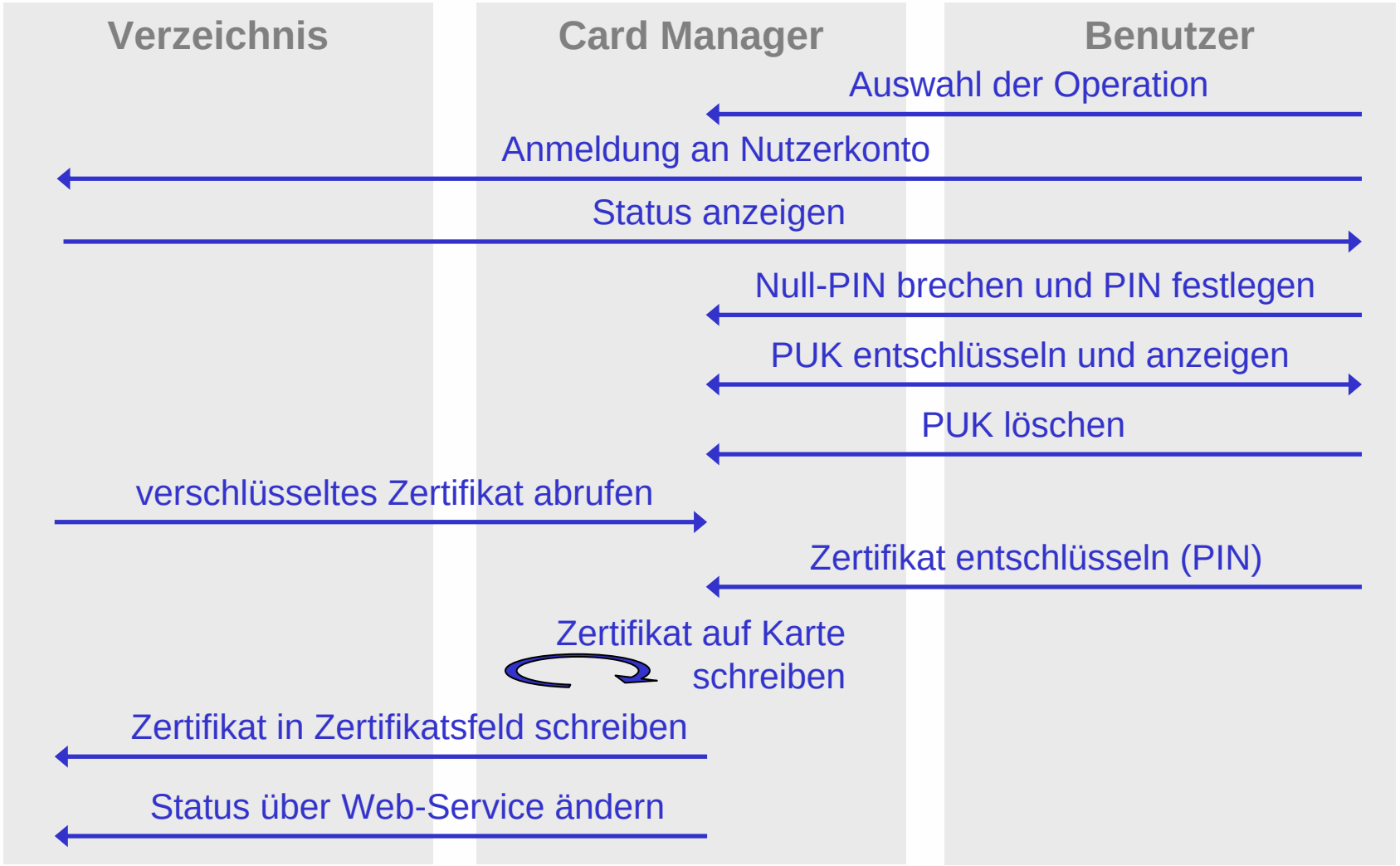
- Im Detail: Kartenaktivierung (1)
  - Ablage des zertifizierten Schlüssels
  - Verwendung des „Card Managers“
    - Brechen der „Null-PIN“
    - Anzeigen und Löschen der PUK
    - „Download“ des Zertifikats auf die Karte
  - „Veröffentlichung“ des zertifizierten Schlüssels
  - Status-Änderungen

# Im Detail: Kartenaktivierung (2)

- Ablage des zertifizierten Schlüssels



# Im Detail: Kartenaktivierung (3)



## Key-Backup und Key-Recovery

- Zweites Schlüsselpaar für Datenverschlüsselung
  → Sicherung des privaten Schlüssels notwendig
- Key-Backup während der Vorbeschlüsselung durch Projektpartner
- Key-Recovery eines Schlüssels im Mehraugenprinzip
  - 2 Gruppen mit jeweils 5 Operatoren
  - Wiederhergestellter Schlüssel als PKCS#12 Datei mit integrierten aktuellen Zertifikat an Benutzer senden
  - Transportpasswort für PKCS#12 Datei über Hauspost
  - PKCS#12 Datei kann in Anwendungen importiert werden
    - Umschlüsselung der verschlüsselten Daten
    - Weiterverwendung der verschlüsselten Daten

# Key-Backup im Detail

- Sicherung der privaten Schlüssel im PKCS#12 Format
  - PKCS#12 Datei nach Kryptoprozessor-Nummer benannt
  - 40 Zeichen Transportpasswort für PKCS#12 Dateien
  - erste Hälfte des Transportpasswortes mit Schlüssel der ersten Operator-Gruppe verschlüsselt
  - zweite Hälfte des Transportpasswortes mit Schlüssel der zweiten Operator-Gruppe verschlüsselt
- Operator-Schlüssel auf Chipkarten mit individueller PIN
- Sicherung auf nichtflüchtigen, mehrfach duplizierten Datenspeicher
  - CD-ROM
  - MO-Medium

# Key-Recovery im Detail

- Wiederherstellung eines privaten Schlüssel mit selbstentwickeltem „Key-Recovery Tool“
  1. Übertragung der Kryptoprozessor-Nummer und des aktuellen Zertifikats auf Offline-Laptop
  2. Zugehörige PKCS#12 Datei mit Kryptoprozessor-Nummer von CD-ROM lesen
  3. erste und zweite Hälfte des Transportpasswortes mit Operatorkarten entschlüsseln
  4. PKCS#12 Datei mit Transportpasswort entschlüsseln
  5. Neue PKCS#12 Datei für Benutzer mit wiederhergestellten privaten Schlüssel und aktuellem Zertifikat erzeugen
  6. Sicherung der neuen PKCS#12 Datei mit zufallsgeniertem Transportpasswort

# Vielen Dank für Ihre Aufmerksamkeit!

## Kontakt und weitere Informationen

Ronny John
Telefon: (0 61 51) 16-45 73
Ronny.John@hrz.tu-darmstadt.de
http://www.tu-darmstadt.de/hrz/chipkarte/