Vorlesung (WS 2014/15)

Sicherheit: Fragen und Lösungsansätze

Dr. Thomas P. Ruhroth

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

[mit freundlicher Genehmigung basierend auf einem Foliensatz von Prof. Dr. Claudia Eckert (TU München)]

Literatur:

Claudia Eckert: IT-Sicherheit: Konzept - Verfahren - Protokolle, 7., überarb. und erw. Aufl., Oldenbourg, 2012.

E-Book: http://www.ub.tu-dortmund.de/katalog/titel/1362263

Agenda

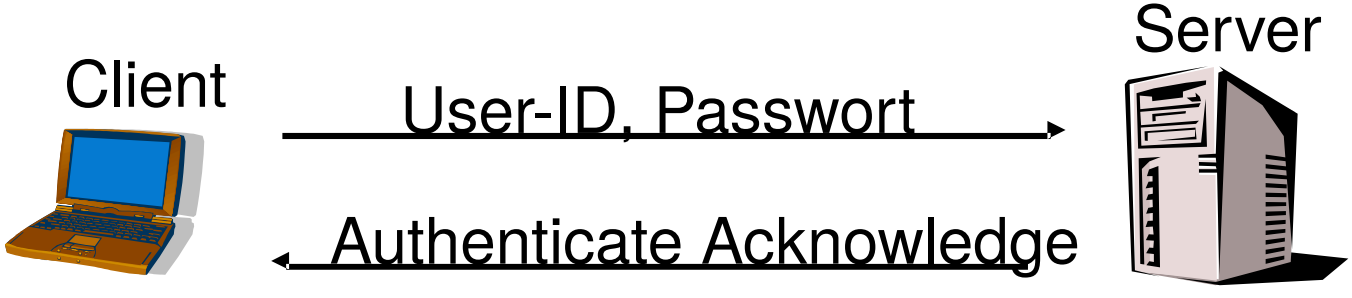
- Kerberos
- Reisepass
- Personalausweis
- Kennen von Authentisierungssystemen

PAP und CHAP

Sehr einfache Protokolle: PAP, CHAP Layer-2 Protokolle

PAP (RFC 1334)

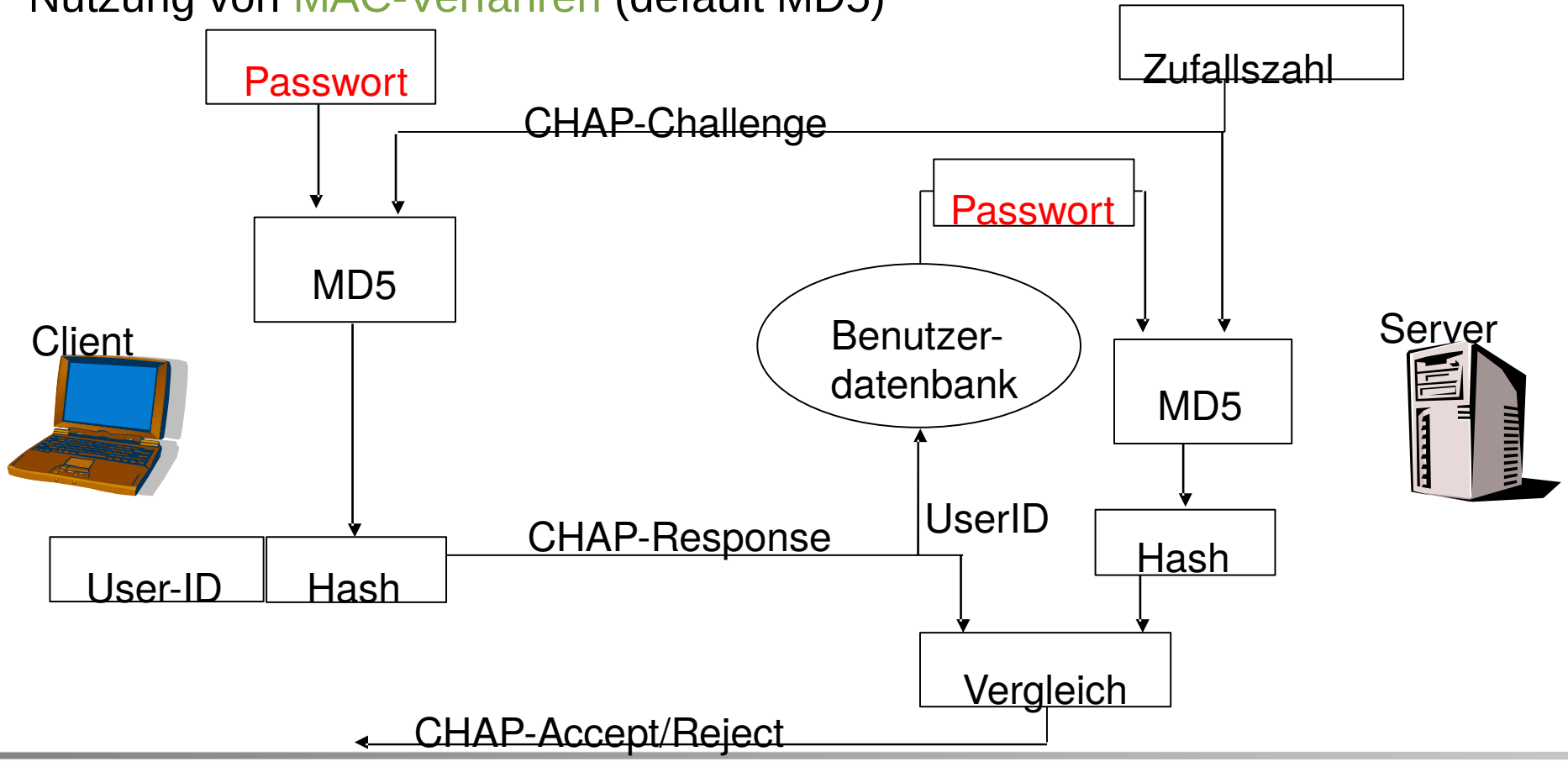
- Passwort-basierte Authentifizierung
- Unverschlüsselte Übertragung von Kennung u. Passworten



CHAP

CHAP (RFC 1334, 1994)

- CR basierend auf pre-shared Secret
- Nutzung von MAC-Verfahren (default MD5)



Anforderungen an ein sicheres Authetisierungsprotokoll

Anforderungen an ein sicheres Authentisierungsprotokoll

- Wechselseitige Authentifikation der Partner
- In verteilten Umgebungen: Single-Sign-on
- Schlüsselaustausch für vertrauliche und integere Datenübertragung

Lösungsansätze

- ‚Vater' aller Dinge: Needham-Schroeder-Protokoll
- Basis: vertrauenswürdiger Authentifizierungsserver AS
- Pre-Shared Secrets: jeder Client *A* hat geheimen Master-Key K_A mit AS vereinbart
- Aufgabe des AS: Authentifikation und Schlüsselverteilung

Kerberos-Protokoll

4.4.2 Kerberos-Protokoll

Kerberos-Protokoll

Name: gr. Mythologie: 3-köpfiger Hund, der den Eingang zum Hades bewacht.

- 1983 im Athena Projekt am MIT entwickelt (+ IBM,DEC)
- zZ. im Einsatz:Version 4 (einige Sicherheits-Probleme)

  Version 5 (RFC 4120 http://tools.ietf.org/html/rfc4120)

Ziele von Kerberos:

- Authentifikation von Subjekten, genannt Principals:
  u.a. Benutzer, PC/Laptop, Server
- Austausch von Sitzungsschlüsseln für Principals
- Single-Sign-on für Dienste/Personen in einer administrativen Domäne (realm, bzw. auch Inter-realm)

Kerberos-Design

Kerberos-Design

- Pro Domäne ein vertrauenswürdiger Server: KDC
  - Authentifizierung der Clients seiner Domäne:
  - Ausstellen von Authentifizierungstickets
- **Basis:** Needham-Schroeder-Variante mit Timestamps
- Symmetrische Kryptographie als Basis:
  - Verschlüsselung: muss: AES256-CTS-HMAC-SHA1-96
    sollte: AES128-CTS-HMAC-SHA1-96,
    DES-CBC-MD5, DES3-CBC-SHA1-KD
  - Integrität muss: HMAC-SHA1-96-AES256
    sollte: DES-MD5, HMAC-SHA1-DES3-KD,
    HMAC-SHA1-96-AES128
- Weitere Verfahren können verwendet werden

Single-Sign-on

Single-Sign-on (SSO):

- Zur Dienstnutzung eines der Principals muss sich der Benutzer nicht beim Principal erneut authentifizieren
- Principals verwalten keine Authentifikationsinformationen

Pre-shared Secrets: geheime Master-Keys:

- **jeder Nutzer *A*** hat geheimen Master-Key K_A mit KDC vorab vereinbart: symmetrischer, geheimer Schlüssel
  - aus gehashtem Passwort des Nutzers abgeleitet,
  - mit gleichem KDC-Key verschlüsselt im KDC abgelegt.
- **Jeder Server-Rechner (Principal) *S*** in der Domäne hat mit KDC ebenfalls geheimen Master-Key K_S vereinbart

Idee: Trennung der

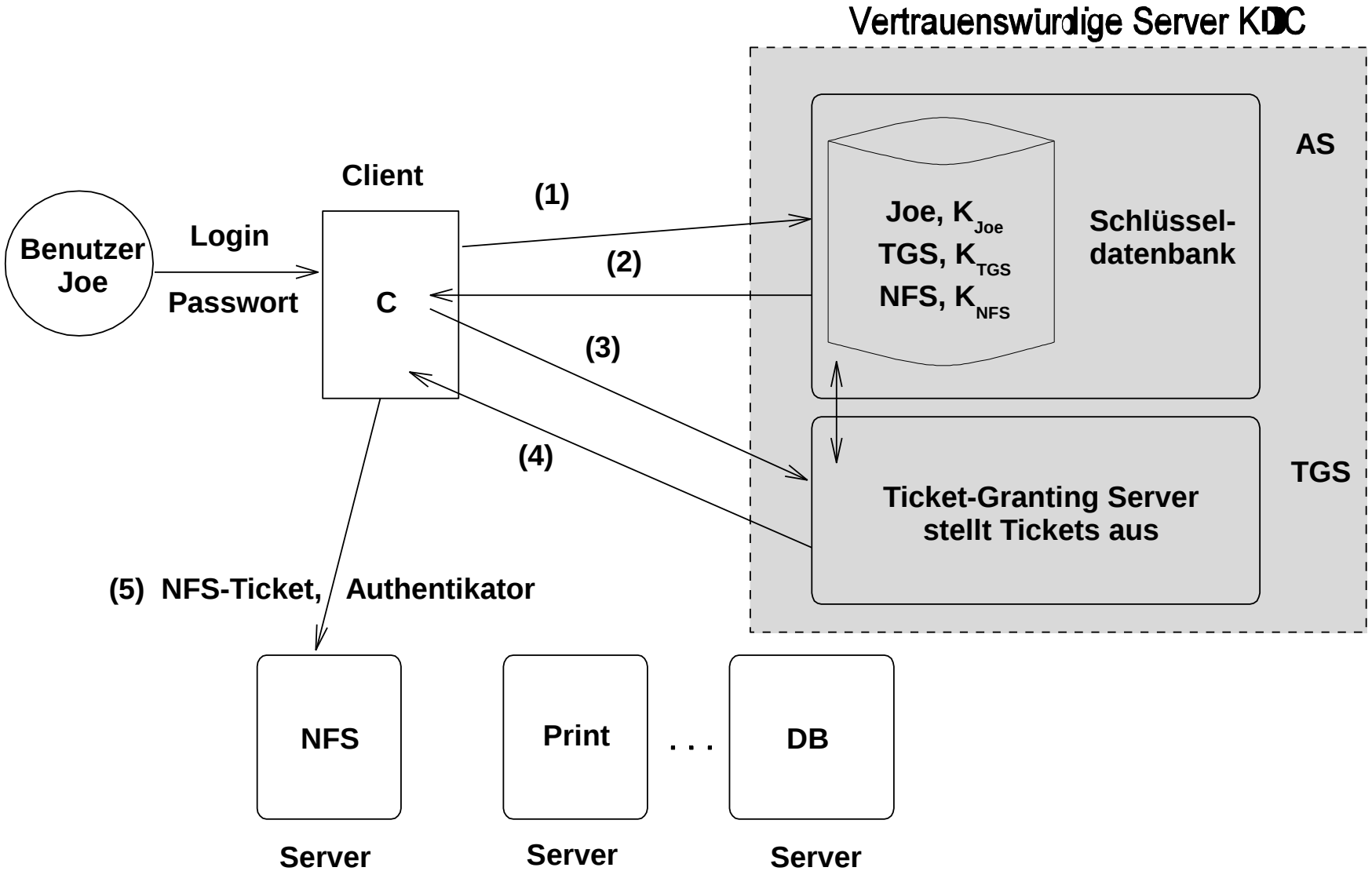
- Authentisierung (zentral): durch den (die) KDC(s) (Policy-Decision-Point)
- und der Prüfung auf Aktualität, Plausibilität, Zulässigkeit, durch Server (Policy-Enforcement-Point)

Vorgehen:

- Benutzer *A* (Principal) beantragt beim KDC einen Authentifikationsnachweis, um mit Dienst *S* zu kommunizieren.
- Der KDC stellt ein Authentifikationsticket für Principal *A* aus.
- Principal *S* kann Gültigkeit des Tickets überprüfen

Bem.: Ticket enthält **keine** Autorisierung zur Dienstnutzung,
d.h. Rechtemanagement ist dezentral, durch *S*

Schematischer Ablauf



Protkollschritte

Tickets

Authenticators

	Von	An	Nachricht
1.	Client	KDC	Joe, TGS, *Nonce*1, E([Joe, Time]), K_{Joe})
2.	KDC	Client	E([$K_{Joe,TGS}$, *Nonce*1], K_{Joe}), E($T_{Joe,TGS}$, K_{TGS})
3.	Client	TGS	E(A_{Joe}, $K_{Joe,TGS}$) E($T_{Joe,TGS}$, K_{TGS}) NFS, *Nonce2*
4.	TGS	Client	E([$K_{Joe,NFS}$, *Nonce2*], $K_{Joe,TGS}$) E($T_{Joe,NFS}$, K_{NFS})
5.	Client	NFS	E(A_{Joe}, $K_{Joe,NFS}$), E($T_{Joe,NFS}$, K_{NFS})

Ticket: $T_{c,s}$: gültig für den Principal *C* und den Server *S*

- $T_{c,s} = (S, C, addr, timestamp, lifetime, K_{c,s})$, es gilt
  - *S* Name des Servers, *C* Name des anfordernden Clients,
  - *addr* dessen IP-Adresse, aktuelle Zeit, Lebenszeit des Tickets (*lifetime*),
  - Sitzungsschlüssel $K_{c,s}$ für Kommunikation zw. *S* und *C*
- Ticket wird mit Master-Key von *S* verschlüsselt, $E(T_{c,s}, K_s)$

Authenticator-Konzept: (für dezentrale Prüfungen)

- Für Zugriff auf *S* durch *C*: Authenticator wird von Client *C* erzeugt und mit dem Ticket $T_{c,s}$ an Principal *S* gesendet $A_C = \{C, addr, timestamp\}K_{c,s}$
- Principal *S* entschlüsselt Authenticator und prüft Gültigkeit

Sicherheitsanalyse von Kerberos? Stärken? Schwächen?

Elektronischer Reisepass

Elektronischer Reisepass

Fallstudie: Digitale Identität (ePass, nPA)

Elektronischer Reisepass ePass in Deutschland

- mit passivem RFID-Chip (inklusive Antenne), CC-zertifiziert
- kontaktloser Chip, verschlüsselte Datenübertragung zwischen Lesegerät und Chip
- Kryptographischer Co-Prozessor auf Chip

Ziele des ePasses

- Fälschungssicherheit erhöhen
- Missbrauch verringern

Personenbezogene Daten:

Name, Geburtsdaum, Geschlecht, Nationalität,

Gesichtsbild, Fingerabdrücke

Fälschungssicherheit

Fälschungssicherheit:

- Daten auf dem Chip sind gehasht und es wird ein signierter Hashswert auf dem Chip abgelegt: Manipulationsprüfungen
- zur Signaturverifikation: weltweite PKI ! (nicht trivial!)

Daten auf dem Chip

in Datengruppen abgelegt

DG1 Enthält die gleichen Daten,

die auch in der MRZ stehen

DG1	Stufe 1	Maschinenlesbare Zone
DG2	Stufe 1	Gesichtsbild
DG3	Stufe 2	Fingerabdrücke
DG14	Stufe 2	Chip Authentication Public Key, signiert von Aussteller
DG15	Stufe 1, optional	Active Authentication Public Key
Document Security Object	Stufe 1	Hashwerte aller Datengruppen sowie Signatur über diese Werte

Passiver Authentifikation

Passive Authentifikation durch Lesegeräte (z.B. Grenzkontrolle)

(1) Lesen des Document-Security-Objekts vom Chip:

- Basic Access-Control
- Verschlüsselte Übertragung des DSO

(2) DS-Zertifikat und CCA-Zertifikat besorgen

(3) Prüfen der Zertifikat-kette: CCA, DS

(4) Prüfen der Signatur der Passdaten

(5) Auslesen der Daten aus Pass

(Gesichtsbild, …)

(6) Berechnen des Hash-Wertes und Vergleich mit DSO-Wert

DG1	Stufe 1	Maschinenlesbare Zone
DG2	Stufe 1	Gesichtsbild
DG3	Stufe 2	Fingerabdrücke
DG14	Stufe 2	Chip Authentication Public Key, signiert von Aussteller
DG15	Stufe 1, optional	Active Authentication Public Key
Document Security Object	Stufe 1	Hashwerte aller Datengruppen sowie Signatur über diese Werte

Aktive Authentifikation

Aktive Authentifikation durch Lesegeräte (optional)

Ziel: Erkennen von geklonten Pässen

Basis: Pass besitzt eigenes asymmetrisches Schlüsselpaar

- **Privater Key:** in sicherem, nicht auslesbarem Speicher auf dem Chip
- Public Key ist auslesbar

Authentifikation:

- CR: Pass gegenüber Lesegerät

DG1	Stufe 1	Maschinenlesbare Zone
DG2	Stufe 1	Gesichtsbild
DG3	Stufe 2	Fingerabdrücke
DG14	Stufe 2	Chip Authentication Public Key, signiert von Aussteller
DG15	Stufe 1, optional	Active Authentication Public Key
Document Security Object	Stufe 1	Hashwerte aller Datengruppen sowie Signatur über diese Werte

Zugriffskontrolle

(1) Zugriff auf nur geringfügig sensitive Daten:

- Basic Access Control: BAC MRZ-Daten, Gesichtsbild
- Lesegerät benötigt optischen Zugriff auf Pass

(2) Zugriff auf sensitive Daten:

- Fingerabdruck, …
- Extended Access-Control:
  - Lesegerät muss bei Zugriff seine Berechtigung nachweisen: Zertifikat-basierter Ansatz

DG1	Stufe 1	Maschinenlesbare Zone
DG2	Stufe 1	Gesichtsbild
DG3	Stufe 2	Fingerabdrücke
DG14	Stufe 2	Chip Authentication Public Key, signiert von Aussteller
DG15	Stufe 1, optional	Active Authentication Public Key
Document Security Object	Stufe 1	Hashwerte aller Datengruppen sowie Signatur über diese Werte

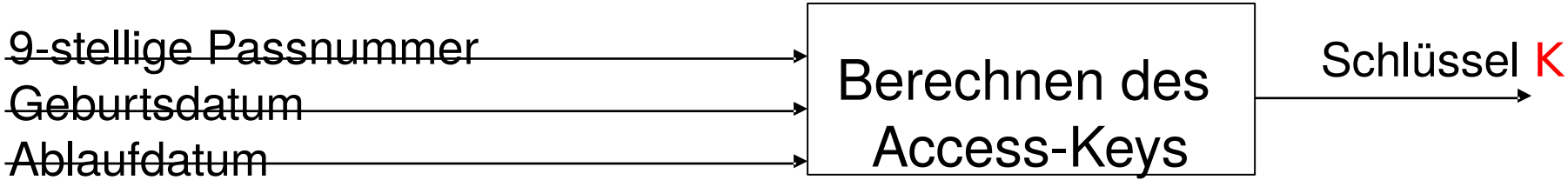
Basic Access-Control

BAC: Basic Access-Control:

Idee: analog zum jetzigen Schutz: Daten auf herkömmlichen Pass werden ausgelesen, wenn der Pass willentlich an Beamten übergeben wird

Vorgehen: Wechselseitige Authentifikation: symmetrisches CR

- **erster Schritt**: Lesegerät gegenüber ePass (RFID-Chip):
  - Lesegerät berechnet Access-Key *K* aus Daten, die in MRZ des Passes stehen, d.h. optisches Auslesen der Daten ist erforderlich, explizites Überlassen des Passes
- **Zweiter Schritt:** Wechselseitige Authentifikation



Nach erfolgreicher Authentifikation:

- verschlüsselte Kommunikation (Daten auslesen) zwischen Lesegerät und Chip, Verschlüsselung: 112 Bit 3DES-CBC
- Kommunikationsschlüssel: aus den jeweils 56-bit Teil-Schlüsseln, K_{reader} und K_{chip} berechnet.
- Teilschlüssel werden bei der Authentifizierung jeweils mit dem Access-Schlüssel K verschlüsselt übertragen
- **Problem:** kein starker Schutz

Extended Access Control

- Terminal soll sich authentifizieren: Terminal Authentication
- Pass/Chip soll sich authentifizieren: Chip Authentication
- Verbesserte Schlüsselvereinbarung: DH-basiert

Extended Access-Control (Forts.)

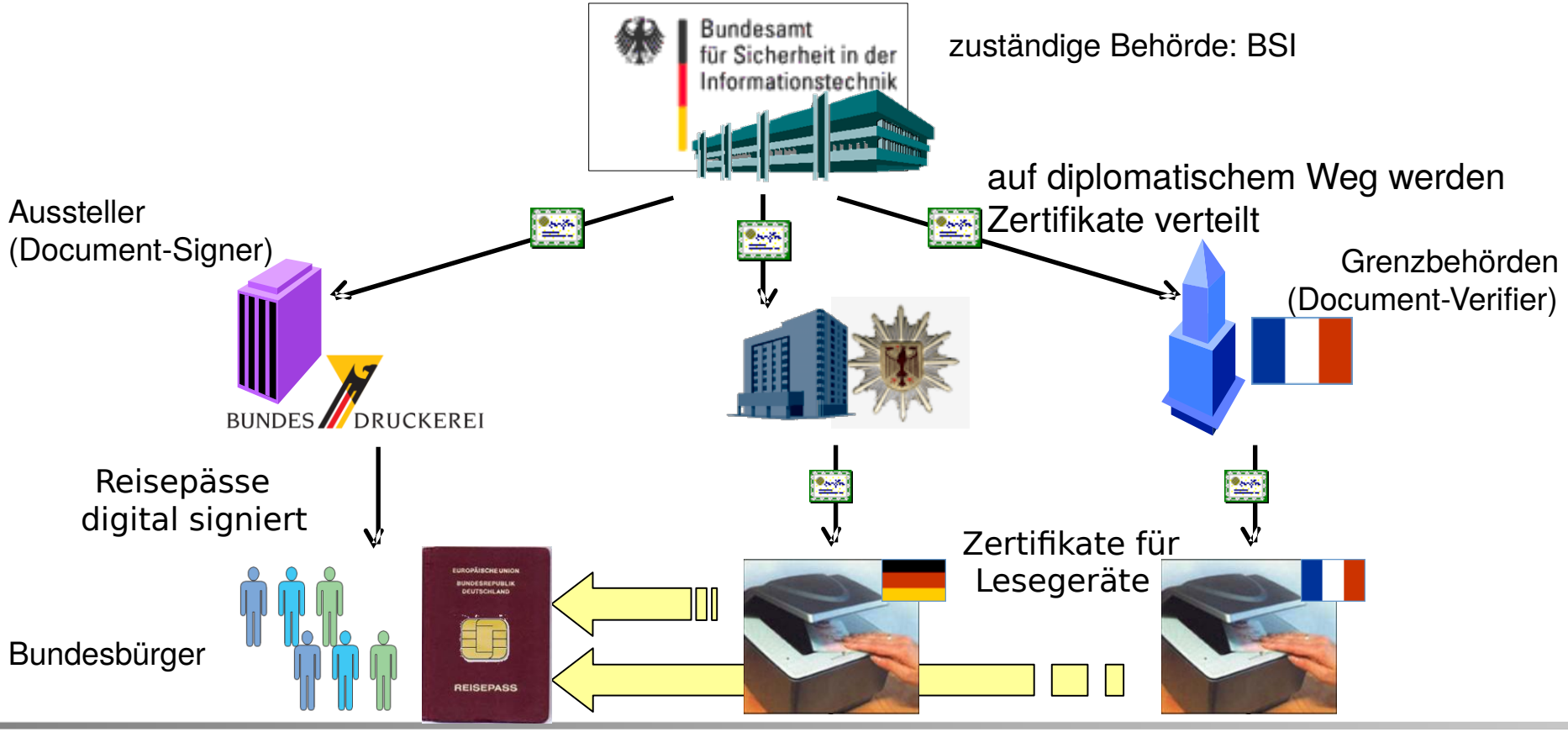
- Zertifikat-basierte Authentifikation des Lesegeräts,
  - Reisepass ausgebende Instanz bestimmt, welches ausländische Lesegerät welche Zugriffsrechte erhält
  - DH oder ECDH möglich

Die PKI besteht aus:

- Country-Verifying-CA (CVCA), von denen jeder Staat genau eine haben muss. Sie stellen Zertifikate für DV aus und bestimmen die Gültigkeitsdauer und Zugriffsrechte
- Document-Verifiers (DV): Einheiten, die IS verwalten, die logisch zusammengehören, Zertifikat-Ausstellung Beispiel: BGS könnte einen eigenen DV betreiben
- Inspection-Systems (IS): Lesegeräte, greifen auf ePässe zu

BSI erstellt Zertifikate für

- die Bundesdruckerei (Document-Signer)
- Bundespolizei / Grenzbehörden anderer Länder (Document- Verifier)



EAC-Ablauf

EAC-Ablauf

(1) **DH-Schritte** zum Austausch der Publik-Keys Chip besitzt DH-Key (Datenfeld 14)

(2) **Chip-Authentifizierung:** DH-Verfahren

- Chip verwendet statisches DH-Schlüsselpaar,
- Öffentlicher Schlüssel ist signiert im Chip abgelegt
- Remote-Terminal erzeugt flüchtiges DH-Schlüsselpaar

Chip kann gemeinsamen Schlüssel *KA* berechnen, da Chip den privaten Schlüssel dafür verwendet:

Chip weist die Kenntnis von *KA* nach:

Secure Messaging mit Schlüssel *K* (abgeleitet aus *KA*)

(3) **Terminal Authentifizierung**

4.6.2 Elektronischer Personalausweis

Elektronischer Personalausweis nPA

Ausgabe seit November 2010

Überblick und Architektur

1. hoheitliche Personenkontrolle (Polizei, Grenzkontrolle) mit biometrischen Daten
2. eID: elektronisch prüfbaren Identität, Online-Authentisierung: E-Business, E-Government, …
3. Option zur Verwendung qualifizierter Signaturen

Aufbau:

- Smartcard-Format ID-1
- kontaktloser, ISO 14443-konformer, passiver RFID-Chip
- Signalisierungsreichweite auf ca. 10 cm begrenzt

Daten auf dem nPA

Daten auf dem nPA

- Name, Geburtsdatum, Alter, Geschlecht, Nationalität,
- Nur im Chip: Gesichtsbild, optional Fingerabdrücke

Daten auf dem Chip: in 16 Datengruppen (DG) strukturiert

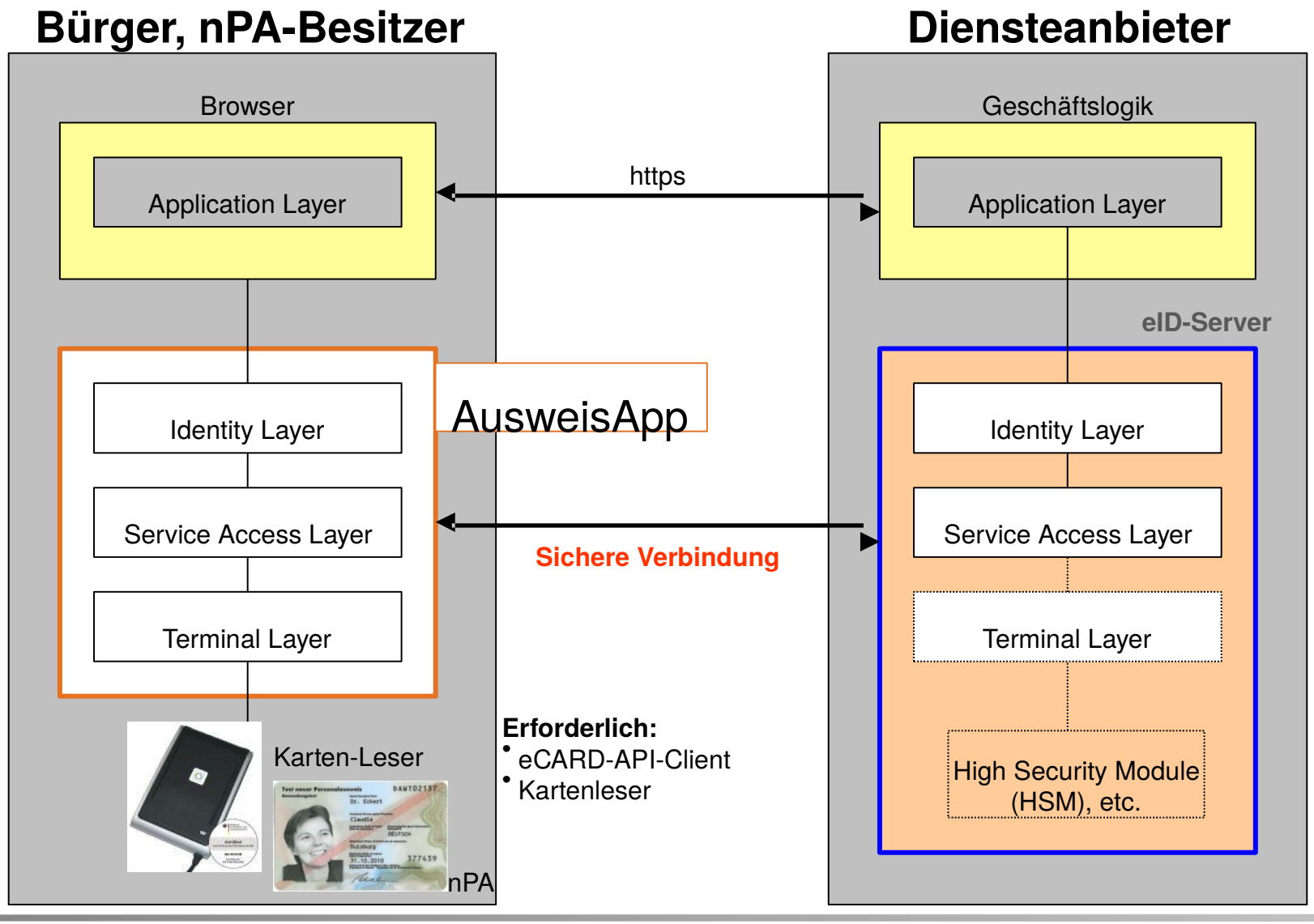
- DG 1: Daten, die auch in der MRZ (Machine-Readable Zone) stehen
- DG 2: digitales Gesichtsbild,
- DG 3: optional Fingerabdruck

Fälschungssicherheit:

- Privater Chip-Schlüssel

  wird signiert, sicher abgelegt

DG1	Stufe 1	Maschinenlesbare Zone
DG2	Stufe 1	Gesichtsbild
DG3	Stufe 2	Optional bei nPA Fingerabdrücke
DG14	Stufe 2	Chip Authentication Public Key , signiert von Aussteller
DG15	Stufe 1, optional	Active Authentication Public Key
Document Security Object	Stufe 1	Hashwerte aller Datengruppen


Bürger, nPA-Besitzer
Diensteanbieter
Browser
Application Layer
https
Geschäftslogik
Application Layer
eID-Server
AusweisApp
Identity Layer
Service Access Layer
Terminal Layer
Sichere Verbindung
Identity Layer
Service Access Layer
Terminal Layer
High Security Module (HSM), etc.
Karten-Leser
nPA
Erforderlich:
• eCARD-API-Client
• Kartenleser

Schutzziele und verwendete Mechanismen

- Integrität und Authentizität des Datenursprungs
  - SHA-1, Digitale Signatur (RSA, DSA, ECDSA)
  - PACE-Algorithmus
- Anti-Cloning: Aktive Authentisierung durch den RFID-Chip
  - Chip-Authentisierung: DH, ECDSA mit 224-Bit-Schlüssel
- Vertraulichkeit:
  - Verschlüsselte Übertragung: AES, 128-Bit-Schlüssel
  - SSL-Verbindung zw. Browser und Dienstleister
  - Kryptographischer Co-Prozessor auf Chip
- Terminal-Authentisierung
  - Authentisierung des Diensteanbieters
  - Validierung des Berechtigungszertifikats

Die eID-Funktion des nPA

- Eindeutige digitale Identität für Online-Aktivitäten oder auch unternehmensinterne Aktionen, z.B. Zugangskontrolle

Vordringliches Ziel: eID-Funktion für Online-Authentisierung:

Online-Zugriff durch Diensteanbieter auf nPA-Daten erfordert:

- Berechtigungszertifikat für Online-Anbieter (Server)
- Explizite Einwilligung des nPA-Besitzers durch
  - PIN-Eingabe: 6-stellige Benutzer-PIN

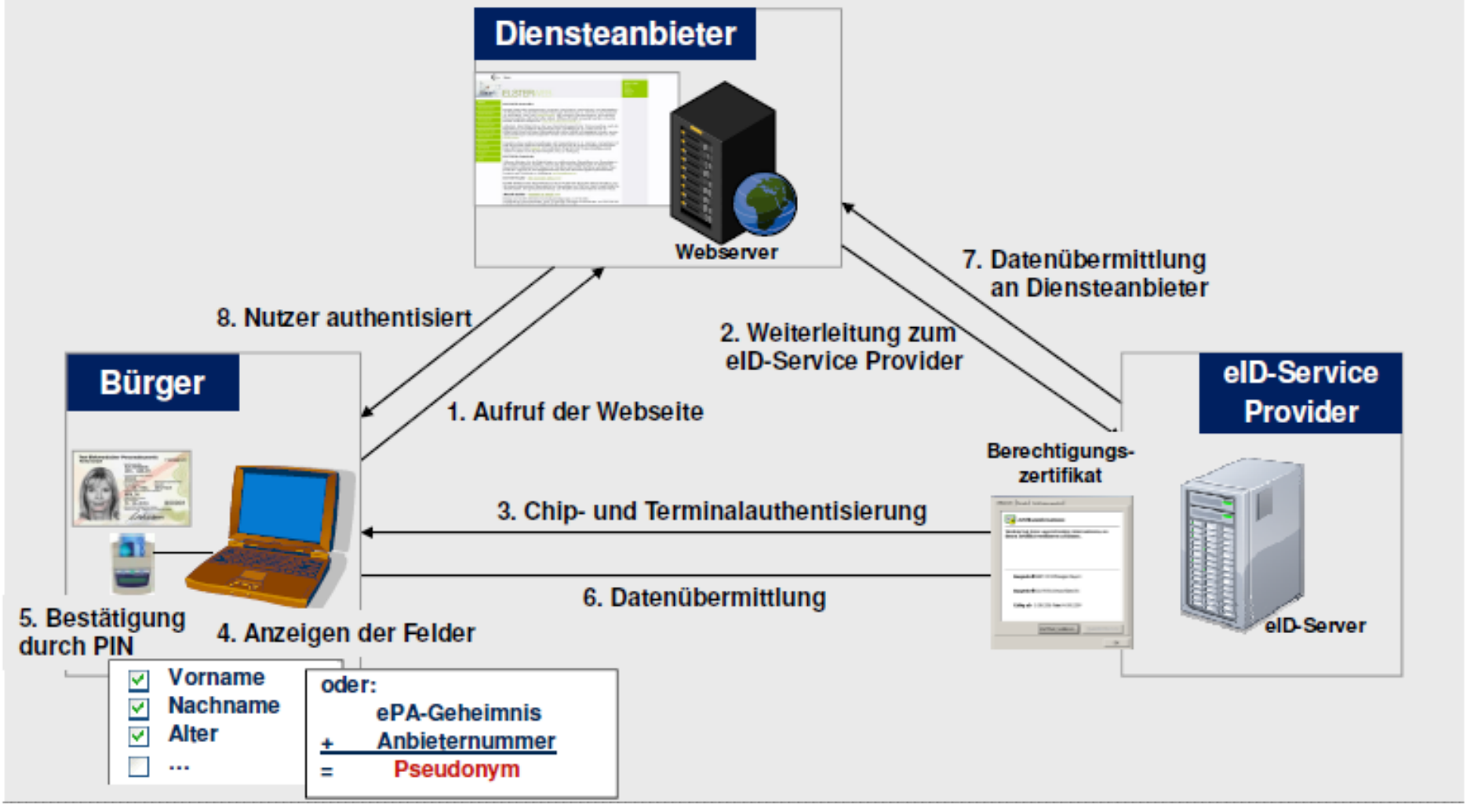
Bemerkung:

Bei der Online-Authentisierung: 2 Terminals (d.h. Lesegeräte)

Lokales Terminal: beim Benutzer, direkte Interaktion mit Chip

Remote Terminal: Rechner/Server beim Diensteanbieter

Allgemeiner Ablauf
bei der Online-Authentisierung



Zugrundeliegende Sicherheits-Protokolle

PACE:

- Verschlüsselte DH-Parameter
- Schlüssel aus PIN abgeleitet

Terminal-Authentisierung:

- asymmetrisches CR mit Berechtigungszertifikat

Chip-Authentisierung: aktiv

- DH-Schlüsselvereinbarung: *K*

PACE

PACE (Password Authenticated Connection Establishment)

- Vom BSI entwickelt, Authentifikation ohne PKI, offline

Idee von PACE:

- Passwort-geschütztes DH-Protokoll zwischen Chip und Lesegerät zum Aushandeln von Schlüsseln
  - gemeinsame PIN ist das Passwort
- Benutzer-PIN für eID-Funktion: Nutzer-Authentifikation
  - 6-stellig, im Chip gespeichert,
  - ePA-Besitzer gibt sie am Lesegerät ein
- Karten-PIN für hoheitliche Kontrollen: keine Nutzer-Auth.
  - 6-stellig, in MRZ auf der Karte, optisch auslesbar
  - Lesegerät muss optischen Zugriff haben
  - Nutzer-Authentisierung zusätzlich: Gesichtsbildvergleich

PACE verwendet asymmetrische Kryptographie: ECC

- bei jeder Authentisierung erzeugen Chip und lokales Terminal je ein flüchtiges DH-Schlüsselpaar: ephemeral key pair
- mittels DH wird ein gemeinsamer Schlüssel berechnet
- Abwehr von Man-in-the-Middle-Angriffen:
  - Chip sendet eine verschlüsselte Zufallszahl an das lokale Terminal
  - der Schlüssel wird mit Hashfunktion aus der PIN abgeleitet
- das lokale Terminal muss zur Entschlüsselung ebenfalls die PIN und Hashfunktion kennen: DH-Geheimnis berechnen
- Aus gemeinsamen DH-Geheimnis wird gemeinsamer symmetrischer AES-Schlüssel für Secure Messaging zw. Chip und lokalem Terminal abgeleitet.

Fazit

Fazit: Sicherheitsmaßnahmen im nPA

- Fälschen erschweren: Anti-Cloning-Maßnahmen:
  - Private-Key im geschützten Speicher des Chip
- Authentizität der Daten im Chip: Signieren der Daten
- wechselseitige Authentisierung im Online-Umfeld:
  - Nutzer mit PIN gegenüber seinem nPA
  - nPA mit seinem Private-Key gegenüber Service
  - Serviceanbieter: Zertifikat u. Private-Key gegenüber nPA
- Vertraulichkeit: kontrollierte Zugriffe auf Daten im RFID-Chip
  - Leserechte im Berechtigungszertifikat des Dienstes
  - Einverständnis des Benutzers: PIN-Eingabe
  - Verschlüsselte Kommunikation

Rechtesysteme