Der neue Personalausweis: Interessante Sicherheitsaspekte für Informatiker

Jun.-Prof. Dr. Christoph Sorge
Universität Paderborn
Institut für Informatik

GI-Regionalgruppe OWL, 19.09.2011

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Elektronischer Reisepass „ePass“

- Einführung am 1. November 2005
- Speicherung von Gesichtsbild und (später eingeführt) Fingerabdrücken des Besitzers auf Chip mit Funkschnittstelle („RF-Chip“)
- Grundlage: Standards der ICAO
- Bewusste Entscheidung gegen kontaktbehaftetes Auslesen wegen Verschleißanfälligkeit; kontaktbehaftete Lösung hätte auch anderes Pass-Format erfordert

Sicherheitsverfahren elektronischer Reisepass

- Passive Authentication
- Active Authentication
- Basic Access Control
- Extended Access Control v1

Passive authentication

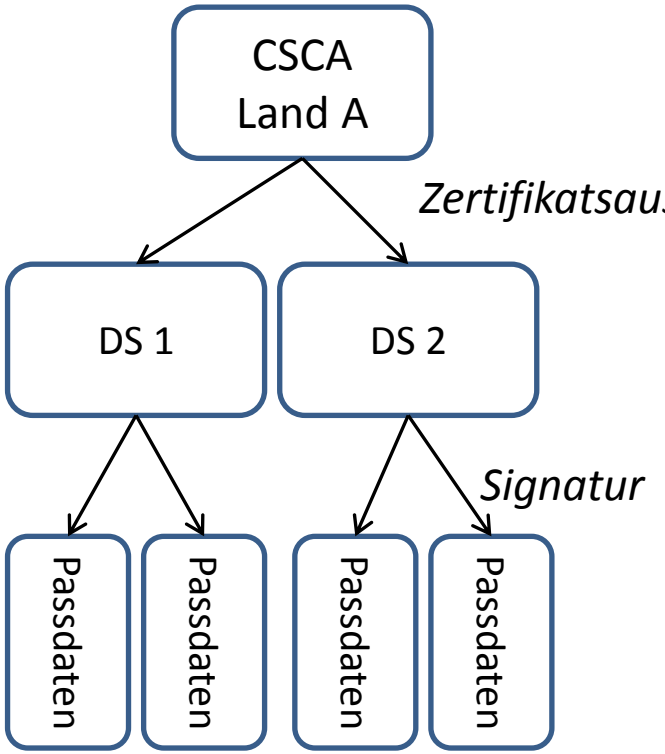
- Ziel des elektronischen Reisepasses: Fälschungen erschweren → Authentifizierung gespeicherter Daten erforderlich
  - Beispiel: Name, Gesichtsbild

- Vorgehen: Erstellung einer Signatur über gespeicherte Daten bereits bei Herstellung des Passes („passive authentication“)

- Passive Authentication hilft gegen Verfälschen von Daten – nicht gegen 1:1-Kopien

PKI für elektronische Ausweisdokumente

- Signatur-PKI: Berechtigung, Ausweisdaten für Passive Authentication zu signieren



Country Signing CA
(Für Deutschland: BSI)

Document Signer
(Ausweishersteller, z.B. Bundesdruckerei)

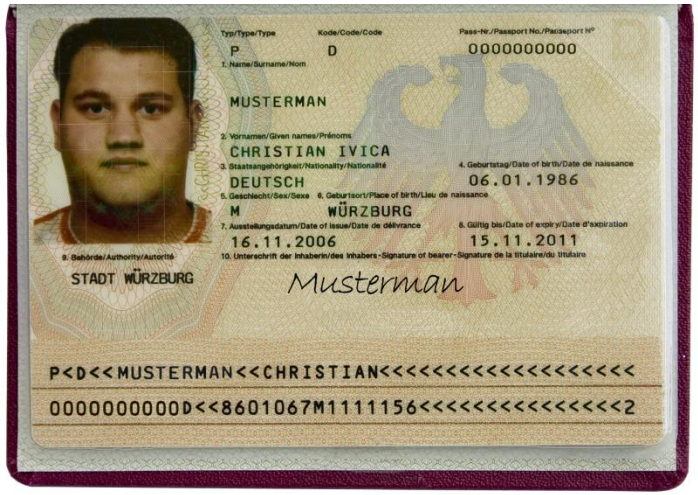
Pässe

Active Authentication

- Ziel: „Klonen“ (1:1-Kopie) eines Passes verhindern
- Idee: Pass hat Schlüsselpaar aus privatem und öffentlichem Schlüssel
- Öffentlicher Schlüssel mit Passive Authentication gesichert
- Pass muss Besitz zugehörigen privaten Schlüssels nachweisen
- Problem Relay-Angriff → Active Authentication nur in wenigen Staaten implementiert (nicht in Deutschland)

Basic Access Control

- Ziel: Schutz vor elektronischem Auslesen von Daten, die auch sichtbar im Pass enthalten sind
  - Beispiel:
    - Geburtsdatum kann in aufgeschlagenem Pass nachgelesen werden
    - Schutz vor Auslesen des Geburtsdatums „im Vorübergehen“ (ohne aufgeschlagenen Pass)



Basic Access Control

- Idee: Generierung von Schlüsselmaterial aus Informationen in bestehender maschinenlesbarer Zone des Reisepasses

- Enthaltene Daten
  - Ausstellungsland
  - Art des Dokuments (z.B. Reisepass, vorläufiger Reisepass)
  - Name
  - Seriennummer (in D: besteht aus Behörden- und Passnummer)
  - Nationalität
  - Geburtsdatum
  - Geschlecht
  - Ablaufdatum
  - Personenkennziffer (bei deutschen Pässen nicht enthalten)

Basic Access Control – Angriff

- Problem: Kleiner Schlüsselraum bei frühen elektronischen Reisepässen
  - Verwendete Informationen aus der maschinenlesbaren Zone: Nur Seriennummer, Geburtsdatum, Ablaufdatum (jeweils mit Prüfziffer)
    - Seriennummer innerhalb einer Behörde früher einfach aufsteigend vergeben
    - Ablaufdatum liegt innerhalb bekannten Zeitraums
    - Geburtsdatum kann ungefähr geraten werden
  - Je nach Schätzung ca. 30 bis 40 bits effektive Sicherheit

Schutz gegen Angriffe

- Aktive Angriffe: Angreifer versucht direkten Zugriff auf elektronischen Reisepass
  - Benötigte Zeit pro Zugriffsversuch: ~ 1 Sekunde
  - Auch kurze Schlüssellängen gewähren Schutz
- Passive Angriffe: Angreifer hört Kommunikation mit
  - Angreifer kann offline Schlüssel durchprobieren
- Lösungsansatz gegen beide: Verbesserte Erzeugung von Seriennummern
  - Zufällige Vergabe
  - Verwendung von Buchstaben zusätzlich zu Ziffern

Extended Access Control

- Basic Access Control als Basisschutz für Gesichtsbild und andere im Pass sichtbar abgedruckte Daten

- Für weitergehende Daten (z.B. Fingerabdrücke): Besseres Verfahren erwünscht → Extended Access Control
  - Zunächst kein ICAO-Standard, sondern durch EU getrieben
  - EAC spezifiziert Protokolle für beidseitige Authentifizierung: Chip Authentication und Terminal Authentication
  - Kommunikation der EAC-Protokolle zunächst mit Schlüsselmaterial aus BAC geschützt

Chip Authentication und Terminal Authentication

- Chip Authentication: Implizite Authentifizierung des Passes mit statischem Diffie-Hellman-Wert
  - Statischer öffentlicher Diffie-Hellman-Wert mit Passive Authentication geschützt
  - Einsatz des Diffie-Hellman-Verfahrens für Ableitung gemeinsamen Schlüssels
  - Verwendung des Schlüssels für Verschlüsselung weiterer Kommunikation → Pass kann Kommunikation nur mit „richtigem“ privaten Schlüssel lesen

- Terminal Authentication: Authentifizierung des Terminals (Lesegeräts) mit Zertifikat

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Der neue Personalausweis

- Ziele:
  - Erhöhte Praktikabilität durch kleines Format
  - Verbesserte Fälschungssicherheit
  - Möglichkeit zur Online-Authentifizierung
  - Erhöhte Verbreitung elektronischer Signaturen
- Einführung: 1. November 2010
  - Elektronischer Aufenthaltstitel (ähnliche Funktionalität): 1. September 2011

Elektronischer Personalausweis: Grundprinzip

- Verkleinerter Ausweis im „Scheckkartenformat“
- Enthält kontaktlosen Chip ähnlich dem Reisepass
  - Ergänzt um Zusatzfunktionen
- Enthält biometrische Daten
  - Gesichtsbild
  - Freiwillig: Fingerabdrücke
- Unterstützung neuer EAC-Verfahren
- PACE-Protokoll als Ersatz für BAC

Gespeicherte Daten

- Speicherung auf dem Chip
  - Familien-, Geburts- und Vornamen, Doktorgrad, Ordens-/Künstlername
  - Geburtstag und –ort
  - Anschrift
  - Seriennummer
  - Ablaufdatum
  - Biometrisches Gesichtsbild
  - ggf. Fingerabdrücke (freiwillig)

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Physikalische Sicherheitsmerkmale

- Guillochen (feine Linienmuster) und Mikroschrift → schwer kopierbar
- UV-Aufdruck: Text und unregelmäßige Muster
- Bei Kippen/Betrachtung unter verschiedenen Winkeln sichtbar
  - Holographische Darstellung des Ausweisbildes
  - Dreidimensionaler Bundesadler
  - …
- Taktile (ertastbare) Merkmale
- Quelle: personalausweisportal.de

Personalausweis: Kontrolle „vor Ort“

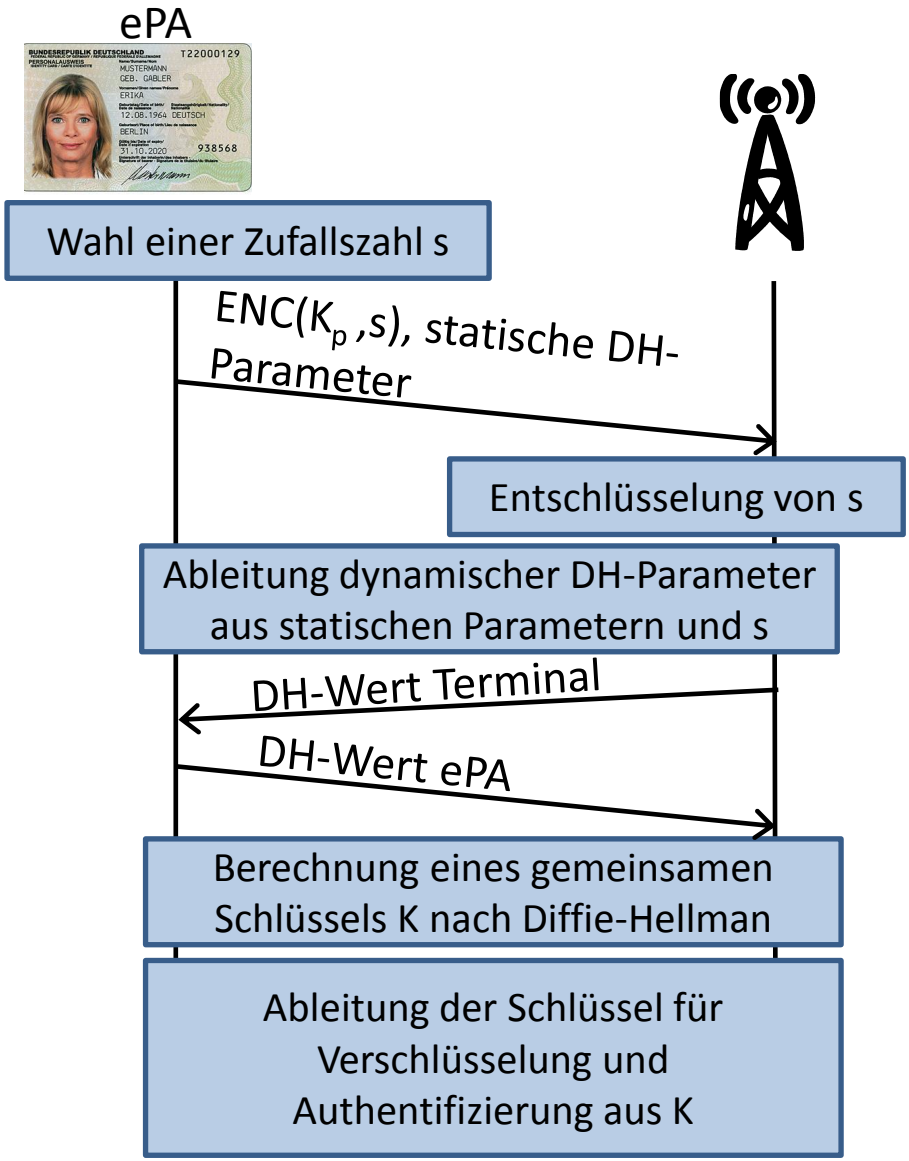
- Kontrollierende Behörde möchte Chip auslesen
  - Benötigt:
    - Hoheitliches Zertifikat
    - Aufgedruckte Card Access Number oder maschinenlesbare Zone
  - Umsetzung:
    - PACE-Protokoll zur Verifikation der Card Access Number
    - Extended Access Control v2
      - Terminal Authentication zur Zertifikatsverifikation
      - Chip Authentication zur Echtheitsprüfung des Chips

PACE-Protokoll

- PACE: Password Authenticated Connection Establishment
  - Nachfolger von BAC
  - Entwickelt durch das BSI für den elektronischen Personalausweis
  - Internationale Standardisierung im Gang
- Authentifizierung durch gemeinsames Geheimnis (Passwort) zwischen Ausweis und Lesegerät
  - Geheime Benutzer-PIN, aufgedruckte Card Access Number oder aus maschinenlesbarer Zone abgeleiteter Schlüssel
- Grundlage: Diffie-Hellman-Verfahren (DH)

PACE-Protokoll

- K_p: Aus gemeinsamem Geheimnis abgeleiteter Schlüssel
- Statische DH-Parameter: Generator, Modulus
- Dynamische DH-Parameter: Ableitung eines neuen Generators aus statischem Generator
  - Genaues Verfahren offen, u.U. weiterer DH-Austausch nötig
- Keine Offline-Angriffe möglich
  - Angreifer kann geratene K_p nicht offline verifizieren



Problem kurze PIN

- Vergebene Benutzer-PINs auch bei sicherem PACE-Verfahren zu kurz
  - Durchprobieren eigentlich in kurzer Zeit möglich

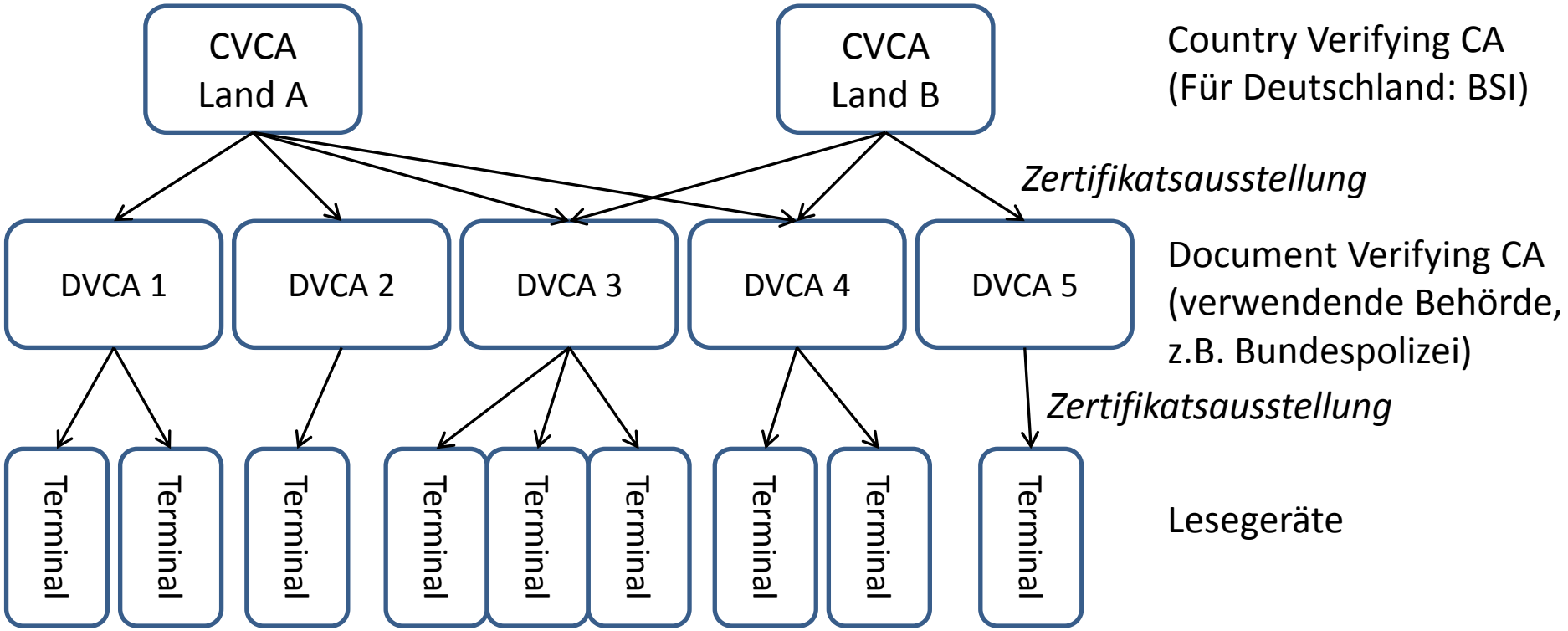
  → Nach 2 Fehlversuchen: PIN wird nicht mehr akzeptiert
  - Freischaltung der PIN durch aufgedruckte Card Access Number, dann ein weiterer Versuch möglich
  - Anschließend Freigabe nur noch durch langen PIN Unblock Key

EAC: Terminal Authentication Version 2

- Sitzungsschlüssel durch PACE etabliert, alle Nachrichten verschlüsselt und authentifiziert
- Terminal besitzt Zertifikat und privaten Schlüssel
- Ausweis schickt Challenge r
- Terminal signiert: (Identität des Ausweises||r||hash(DH-Wert des Terminals)||weitere Daten)

PKI für elektronische Ausweisdokumente

- Verifikations-PKI: Berechtigung, Ausweise zu lesen



Zertifikats-Gültigkeit in Deutschland

- CVCA: 26 Monate
  - Verwendung: 21 ½ Monate
- DVCA: 2 ½ Monate
  - Verwendung: 2 Monate
- Zertifikate der Terminals: 36 Stunden
  - Verwendung: 24 Stunden

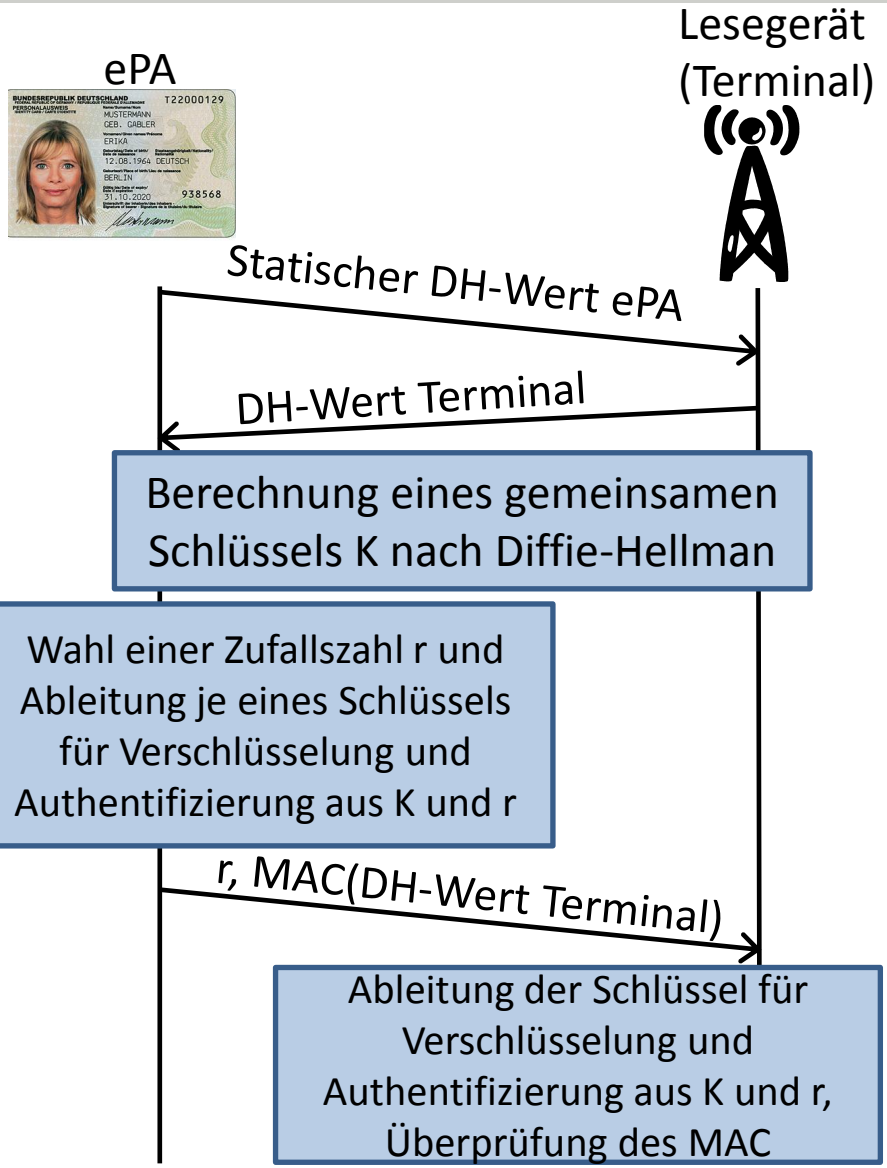
  → Verzicht auf Widerrufslösung möglich

Gültigkeitsprüfung und Änderung von Schlüsseln

- Zertifikatsprüfung durch Personalausweis erfordert aktuelles Datum
  - Initial: Produktionsdatum als aktuelles Datum
  - Nach Prüfung eines neuen Zertifikats: Aktuelles Datum = Gültigkeitsbeginn des Zertifikats
- Gültigkeit von Ausweisen: Bis zu 10 Jahre → Zertifikate könnten sich ändern
  - Aktueller CVCA-Schlüssel bei Produktion im Ausweis gespeichert
  - Bei Änderung des CVCA-Schlüssels: Ausweis erhält Link-Zertifikat – neuer öffentlicher Schlüssel mit altem Schlüsselpaar signiert
    - Pass tauscht alten CVCA-Schlüssel gegen neuen aus

EAC: Chip Authentication Version 2

- Ziele:
  - Chip wird als authentisch erkannt
  - Schlüssel zur Absicherung gemeinsamer Kommunikation werden abgeleitet und ersetzen vorher verwendete
- Voraussetzung: Statischer DH-Wert des Ausweises kann geprüft werden → Verwendung der Passive Authentication
- Wiederverwendung des DH-Werts des Terminals aus der Terminal Authentication
- Explizite Authentifizierung des Chips



Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

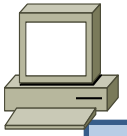
Personalausweis: Online-Einsatz

- Online-Händler möchte Daten aus Chip auslesen
  - Benötigt:
    - Berechtigungszertifikat
    - Geheime Benutzer-PIN
  - Umsetzung:
    - PACE-Protokoll zur Verifikation der Benutzer-PIN
    - Extended Access Control v2
      - Terminal Authentication zur Zertifikatsverifikation
      - Chip Authentication zur Echtheitsprüfung des Chips

Auslesen von Attributen

- Auslesen von Attributen nur mit passendem Berechtigungszertifikat möglich
  - Beispiel: Jugendschutzsysteme benötigen lediglich das Alter → kein Auslesen der Anschrift
- Vergabestelle für Berechtigungszertifikate: Bundesverwaltungsamt (für Anwendungen der Privatwirtschaft) – technische Durchführung durch D-Trust
- Übermittelte Daten nicht signiert
  - Soll Nutzen für Datenhandel reduzieren
  - Authentifizierung implizit durch Chip Authentication
- Anwendungssoftware soll Attributsfreigabe durch Nutzer bestätigen lassen

Online-Einsatz



Demo

Agenda

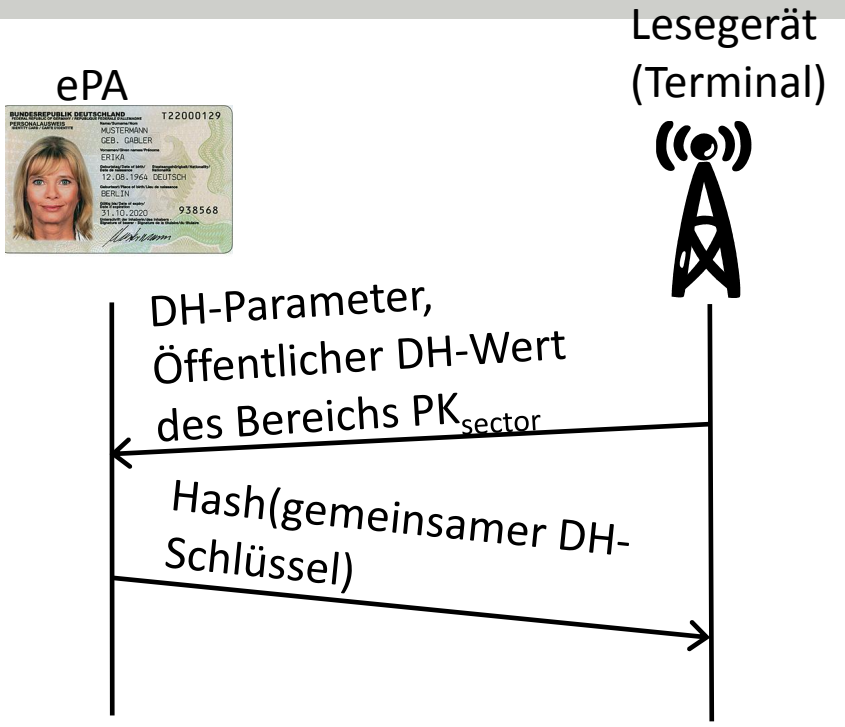
- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Restricted Identification

- Ziel: Generierung eines „bereichsspezifischen Identifikators“ – Identifikator, unter dem eine Person in einem Bereich *wieder*erkannt werden kann
  - z.B. als Schlüssel in einer Datenbank
  - Auch ohne Kenntnis der realen Identität des Ausweisinhabers
  - Bereich: z.B. Steuerbehörden, einzelner Betreiber einer Website
  - Bereichsspezifischer Identifikator eines Bereichs nicht aus bereichsspezifischen Identifikatoren anderer Bereiche ableitbar
    - Tracking einer Person über verschiedene Bereiche nicht möglich

Restricted Identification: Protokoll

- ePA hat geheimen DH-Wert SK_{ID}
- ePA wendet Diffie-Hellman an – Ergebnis eigentlich gemeinsamer DH-Schlüssel, aber keine Verwendung als Schlüssel
  - Verwendung des Hashs als bereichsspezifischer Identifikator
- Österreichische Bürgerkarte verwendet ähnliches Verfahren, aber dortiger Identifikator: Hash(geheimer Schlüssel des Ausweises || Bereichs-Identifikator) – was ist der Vorteil von Diffie-Hellman?

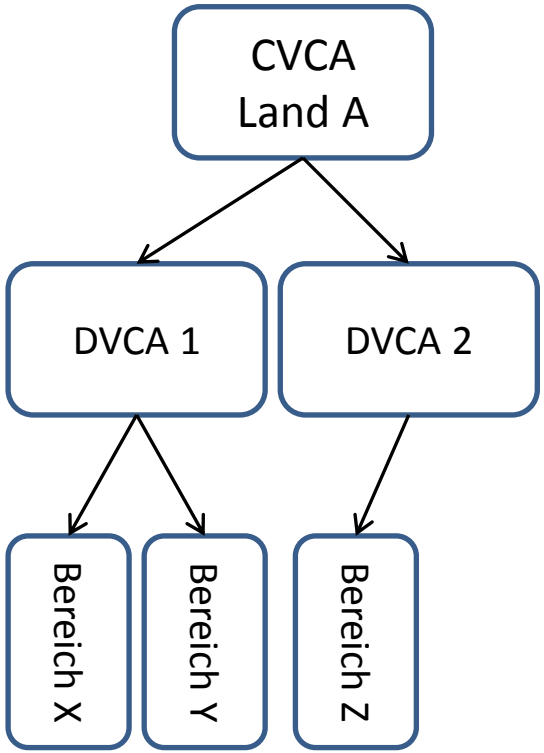


Problem der Restricted Identification

- Protokoll muss über sicheren Kanal ausgeführt werden
  - Terminal muss wissen, dass bereichsspezifischer Identifikator von echtem Ausweis berechnet wird – sonst beliebige Manipulation möglich
  - Chip Authentication vorher nötig
- Chip Authentication ermöglicht Tracking bei Verwendung ausweisspezifischer Schlüssel
- Lösung des BSI: Verwendung des gleichen Schlüsselpaars für Chip Authentication in ganzer Charge von Ausweisen

Widerruf bei der Restricted Identification

- Vergabe der öffentlichen DH-Werte für einen Bereich: Document Verifying CAs
  - CVCA generiert privaten DH-Wert $SK_{Revocation}$ und zugehörigen öffentlichen DH-Wert $PK_{Revocation}$
  - $PK_{Revocation}$ und DH-Parameter werden veröffentlicht
  - DVCA wählt pro Bereich privaten DH-Wert SK_{sector} und berechnet PK_{sector} nach Diffie-Hellman aus SK_{sector} und $PK_{Revocation}$



Widerruf bei der Restricted Identification (2)

- CVCA erhält öffentlichen DH-Wert PK_{ID} eines zu sperrenden Chips
- CVCA berechnet $PK_{ID\text{-}rev}$ nach Diffie-Hellman aus $SK_{Revocation}$ und PK_{ID} und leitet $PK_{ID\text{-}rev}$ an alle DVCAs weiter
- DVCAs berechnen für jeden Bereich zugehörigen bereichsspezifischen Identifikator nach Diffie-Hellman aus SK_{sector} und $PK_{ID\text{-}rev}$
- Nachteil des Verfahrens: CVCA und DVCAs können gemeinsam Anonymität brechen
- Vorteil des Verfahrens: CVCA und DVCAs müssen zusammenarbeiten, um Anonymität zu brechen

Altersverifikation

- Ziel: Verifikation, dass Nutzer ein Mindestalter erreicht hat
  - z.B. für Zugriff auf Webseiten mit nicht jugendfreien Inhalten
  - Unterstützung mehr als eines Mindestalters
  - Keine feste Speicherung erreichter Altersstufen
  - Keine Preisgabe genauer personenbezogener Daten (z.B. Geburtsdatum)

- Lösung
  - Nach erfolgreicher Chip Authentication: Terminal schickt Datum an Ausweis
  - Ausweis antwortet, ob Geburtsdatum vor genanntem Datum liegt
  - Ausweis antwortet nur einmal pro PACE-Authentifizierung

Wohnortnachweis

- Ausweis enthält Gemeinde-Schlüssel

- Wohnortverifikation analog zu Altersverifikation
  - Ggf. auch nur bundesland-genaue Abfrage möglich → Übermittlung nur von Teilen des Gemeinde-Schlüssels

Anbieter (Beispiele)

- Schufa: Registrierung und Login für Online-Portal meineschufa.de
- Allianz, Huk24, Gothaer, Hannoversche Leben, CosmosDirekt-Versicherung, …: Login Online-Dienste für Versicherte bzw. Identifizierung bei Vertragsschluss
- Petitionsplattform openpetition: Mitzeichnen von Petitionen mit Namens-/Wohnortnachweis
- Liste von Anbietern: www.personalausweisportal.de

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Exkurs: Elektronische Signaturen und das Signaturgesetz

- „Elektronische Signaturen“: Juristischer Begriff für Signaturen über digitale Daten

- Signaturgesetz kennt einfache, fortgeschrittene und qualifizierte Signaturen
  - Einfache Signatur: Daten, die der Authentifizierung dienen
  - Fortgeschrittene Signatur: Zusätzlich kryptographische Verfahren
  - Qualifizierte Signatur: Signaturschlüssel sicher gespeichert und Signatur nur nach 2-Faktor-Authentifizierung möglich; es wird ein „qualifiziertes Zertifikat“ verwendet

Qualifizierte elektronische Signatur

- Idee der qualifizierten elektronischen Signatur: Elektronisches (weitgehendes) Äquivalent zur handschriftlichen Unterschrift bereitstellen
  - Erfüllung von Formerfordernissen („elektronische Form“ nach §126a BGB)
  - Beweiskraft

- Bisher begrenzte Verbreitung in der Praxis
  - Hohe Kosten für Zertifikate, Signaturkarten etc.

Neuer Personalausweis und qualifizierte elektronische Signatur

- Personalausweis als sichere Signaturerstellungseinheit
  - Sichere Erzeugung eines Schlüsselpaars auf Ausweis
  - Signaturerstellung durch Ausweis
  - Initial kein Zertifikat enthalten

- Benötigt: qualifiziertes Zertifikat
  - Ausstellung durch privaten Zertifizierungsdiensteanbieter
  - Elektronische Authentifizierungsfunktion gegenüber ZDA

- PACE-Protokoll zur Authentifizierung des Signierenden gegenüber dem Ausweis

- Bisher kein Anbieter auf dem Markt, keine Unterstützung durch AusweisApp

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Beantragung des Ausweises

- Antragsprozess grundsätzlich wie bisher
  - Allerdings: Deutlich höhere Gebühr: 28,80 EUR für Bürger ab 24 Jahren
- Neu: Bundesdruckerei sendet Brief mit Sperrkennwort, Start-PIN und PUK an Meldeanschrift
  - Ausweis geht an Meldebehörde
- Freischaltung der Online-Authentifizierung ohne Start-PIN bei Meldebehörde möglich
  - Gebührenpflichtig bei späterer Freischaltung

Sperrung

- Bei Verlust des Ausweises
  - Sperrung der Online-Authentifizierung unter Angabe des Sperrkennworts: Telefonisch 0180-1-33 33 33
    - Sperrkennwort kann (persönlich) bei Meldebehörde erfragt werden
  - Außerdem: Meldebehörde über Verlust informieren
  - Signaturfunktion ggf. separat widerrufen lassen (beim Zertifizierungsdiensteanbieter)

Rechtliches

- Ausweispflicht (§ 1 Abs. 1-3 PAuswG)
  - Pflicht, Ausweis zu besitzen und berechtigter Behörde auf Verlangen vorzulegen
    - Personalausweis oder Pass
    - Gilt ab 16 Jahren
  - Keine Pflicht, Ausweis mitzuführen

- Ausweis als „Pfand“?
  - Neu: „Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben.“ (§ 1 Abs. 1 Satz 3 PAuswG)

nPA-basierte Authentifizierung in eigenen Anwendungen

nPA-basierte Authentifizierung in eigenen Anwendungen

- Erfordert Berechtigungszertifikat
- Vergabestelle für Berechtigungszertifikate verlangt
  - Begründung für enthaltene Datenfelder
  - Erfüllung funktionaler Anforderungen gemäß BSI-Richtlinien
  - Erfüllung von Datenschutz- und Datensicherheitsanforderungen

Gebühren: § 3 PAuswGebV

- Gebühren für Berechtigungszertifikate
  - Erteilung einer Berechtigung: 102 Euro
  - Versagung einer Berechtigung: 80 Euro
  - Rücknahme / Widerruf einer Berechtigung: 115 Euro

nPA-basierte Authentifizierung in eigenen Anwendungen (2)

- Umsetzungsmöglichkeiten
  - Lokaler eID-Server
  - Selbstbetriebener, über Internet mit Webserver verbundener eID-Server
  - Outsourcing
    - Auftragsdatenverarbeitung gem. § 11 BDSG
    - Durchführender Anbieter muss Vergabestelle für Berechtigungszertifikate bekanntgegeben werden
    - Geschätzte Kosten für Kommunen laut Bundesarbeitsgemeinschaft der kommunalen IT-Dienstleister: 6.000 bis 8.000 Euro – sinkende Kosten mit steigender Verbreitung erwartet

Sicherheitsanforderungen beim eID-Server-Betrieb

- Geforderte Sicherheitsmaßnahmen: Einhaltung des Stands der Technik / Identifizierung von Gefährdungen
  - Wenig Überraschendes, BSI zählt Anforderungen in TR-03130 auf
  - Zusätzlich Beachtung weiterer BSI-Richtlinien zu Schlüssellängen etc.

- Außerdem: Bereitstellung von Download-Links zur AusweisApp, Prüfung der Aktualität der AusweisApp,…

- Details: *Richtlinie Technische und organisatorische Anforderungen zur Nutzung von Berechtigungszertifikaten vom 17. Mai 2011*, veröffentlicht durch Bundesverwaltungsamt im eBundesanzeiger (nimmt Bezug auf BSI-Richtlinien)

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Sicherheitsprobleme

- Durch CCC und andere Experten kritisierte Sicherheitsprobleme
  - Verwendung von Kartenlesern ohne PIN-Pad
  - Anfälligkeit für Relay-Angriffe
  - Sicherheitslücken in AusweisApp
  - Hinterlegungsverbot als Indiz für Sicherheitsprobleme

Verwendung von Kartenlesern ohne PIN-Pad

- Szenario
  - Trojanisches Pferd auf Nutzer-PC installiert
  - Nutzer gibt PIN ein → Angreifer erhält PIN

- Was kann der Angreifer tun?
  - Im Ausweis gespeicherte Daten auslesen?
    - Nein – verschlüsselter Kanal geht vom Ausweis bis zum Inhaber eines Berechtigungszertifikats

Verwendung von Kartenlesern ohne PIN-Pad

- Szenario
  - Trojanisches Pferd auf Nutzer-PC installiert
  - Nutzer gibt PIN ein → Angreifer erhält PIN

- Was kann der Angreifer tun?
  - Sich gegenüber beliebigem Diensteanbieter als Ausweisinhaber ausgeben und z.B. Bestellungen aufgeben
    - Ja – möglich, solange Ausweis auf Kartenleser liegt

Verwendung von Kartenlesern ohne PIN-Pad

- Szenario
  - Trojanisches Pferd auf Nutzer-PC installiert
  - Nutzer gibt PIN ein → Angreifer erhält PIN
- Gegenmaßnahme
  - Gesetzliche Regelung, § 27 Abs. 3 PAuswG: elektronische Authentifizierung nur in sicherer Umgebung
    - Nicht realistisch

Verwendung von Kartenlesern ohne PIN-Pad

- Szenario 2 (tatsächlich implementiert, Jan Schejbal, Januar 2011)
  - Phishing-Angriff: Website enthält Javascript-Anwendung mit Aussehen der AusweisApp
  - Nutzer ist PIN-Eingabe in AusweisApp gewöhnt und sendet PIN an Angreifer

- Fazit
  - Verbreitung von Kartenlesern ohne PIN-Pad („Basis-Lesegeräte“) vornehmlich aus Kostengründen
  - Kritik berechtigt: Angriffe bei Verwendung von Basis-Lesegeräten möglich
  - Aber: Auch bei Basis-Lesegeräten Verbesserung gegenüber Status Quo (Authentifizierung mit Nutzername / Passwort)

Anfälligkeit für Relay-Angriffe

- Szenario
  - Personalausweis an Ort A
  - Weiterleitung sämtlicher Kommunikation an Ort B (Angreifer-Standort)
  - Beispiel: Angreifer an Ort B führt eID-Funktion mit dort nicht vorliegendem Personalausweis durch
  - Besonders problematisch bei Signatur oder bei Beantragung eines qualifizierten Zertifikats: An Ort A reicht Basis-Lesegerät
- Fazit
  - Problem kaum zu verhindern
  - Angriff funktioniert aber nur bei Kenntnis der PIN durch den Angreifer

Relay-Angriff in der Praxis

- Praktisch vorgestellter Relay-Angriff (Jan Schejbal, August 2011)
  - Voraussetzung: OWOK-Plugin installiert (z.T. mit „IT-Sicherheitskit“ ausgeliefert: Ermöglicht Nutzung des Lesegeräts für Authentifizierung mit „Login-Card“)
  - Nutzung des Plugins zu beliebiger Kommunikation mit Personalausweis (als läge er dem Angreifer vor)
  - PIN nötig, kann aber durch vorheriges Phishing bekannt sein
  - Sicherheitslücke mittlerweile geschlossen

Sicherheitslücke in AusweisApp

- Innerhalb eines Tages nach Veröffentlichung der AusweisApp: Sicherheitslücke entdeckt
  - Update-Funktion ermöglichte Einspielen von Schadsoftware

- Fazit
  - Sicherheitslücken in Software kaum vermeidbar
  - Regelmäßige Aktualisierungen zur Risiko-Reduktion
  - Sicherheitskritische Funktionen möglichst auf Hardware verlagern → Kartenleser mit PIN-Pad

Hinterlegungsverbot als Indiz für Sicherheitsproblem?

- Aufgabe des Gewahrsams an einem Ausweis darf nicht verlangt werden
  - Sicherheitsproblem als Grund?

- Fazit
  - Hinterlegungsverbot als Schutz der Card Access Number und Schutz vor Missbrauch der elektronischen Authentifizierung
  - Ohne hoheitliches Zertifikat und ohne Kenntnis der PIN: Kein Vorteil für Angreifer
    - Angreifer kann aber aufgedruckte Daten lesen

  → Sicherheitsrisiko hier minimal (aber: Nicht „123456“ als PIN verwenden!)

Agenda

- ePass
- Neuer Personalausweis
  - Offline-Einsatz
  - Online-Einsatz
  - Besondere Funktionen beim Online-Einsatz
  - Elektronische Signaturfunktion
  - Administrative Aspekte
  - Angriffe
- Fazit

Fazit

- Gutes Konzept, kleine Wermutstropfen
  - Fortschritt gegenüber Status Quo
  - Durchdachtes Konzept für technischen Datenschutz
  - Aber: Sorgfalt des Nutzers erforderlich
    - Dringend empfohlen: PIN-Eingabe nur auf sicheren Geräten (Lesegerät mit PIN-Pad: Standard-/Komfortlesegerät)
  - Konzepte durchdacht, Sicherheitsbeweise für Teile vorhanden
    - Aber: Fehler in Umsetzung möglich, schwierig von „außen“ zu entdecken

Kontakt

Christoph Sorge

Universität Paderborn, Institut für Informatik

Bis 06.10.: Fürstenallee 11, 33102 Paderborn, Tel. 05251-60-6691

Ab 07.10.: Warburger Straße 100, 33098 Paderborn, Tel. 05251-60-1760

Web: http://www.cs.upb.de/?netsec

E-Mail: christoph.sorge@uni-paderborn.de