„Die gesamte Technik ist sicher“

Besitz und Wissen: Relay-Angriffe auf den neuen Personalausweis

Frank Morgner und Dominik Oepen
{morgner|oepen}@informatik.hu-berlin.de

Humboldt-Universität zu Berlin
Institut für Informatik, Lehrstuhl für Systemarchitektur
Unter den Linden 6, 10099 Berlin

27. Dezember 2010

Disclaimer

Was wir *nicht* gemacht haben

- Ausweise gehackt (wir besitzen keinen)
- Standard- oder Komfortleser gehackt (es gibt keine)
- QES gehackt (wird noch nicht angeboten)
- Rechtswissenschaften studiert

Was wir gemacht haben

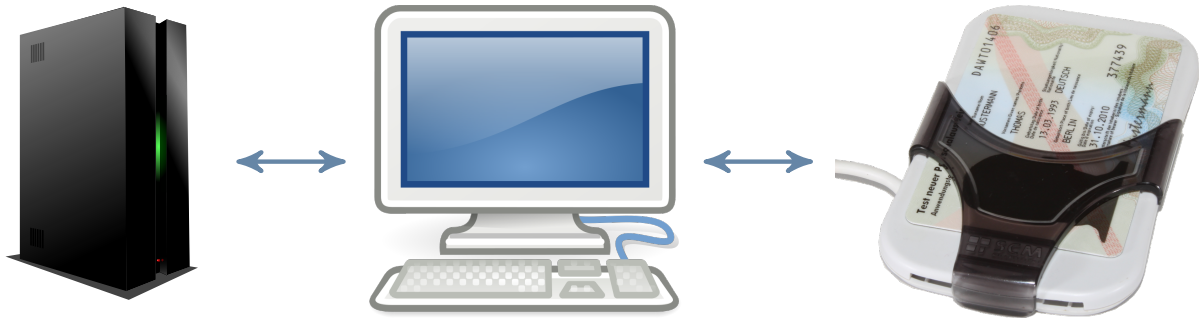
- Viel gelesen und diskutiert
- Testgeräte und -ausweise benutzt
- OpenPACE, Virtual Smart Card Architecture

Übersicht

Der neue Personalausweis

- Scheckkartenformat (ID-1)
- RFID-Chip (ISO 14443)
- Funktionen: ePass, eID, eSign
- Geheimnisse: CAN, eID-PIN, eSign-PIN

Extended Access Control



Dienstanbieter PC Reader + Ausweis

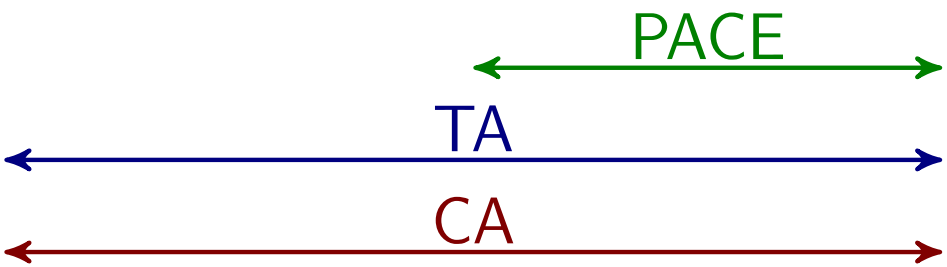


Abbildung: EAC am Beispiel der eID-Funktion mit einem Basisleser

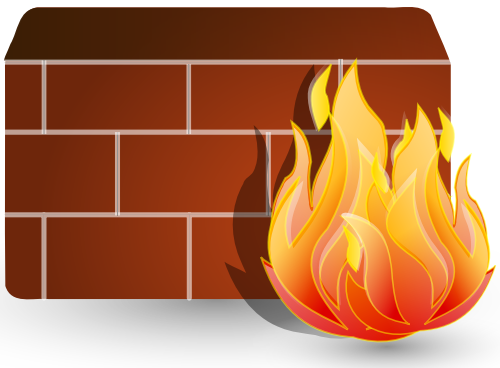
Lesegeräteklassen

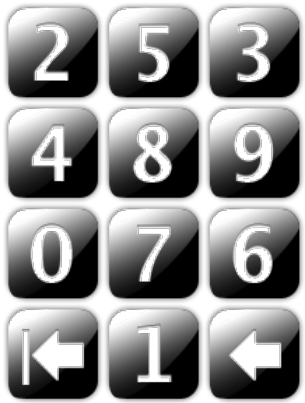
Basis	RFID-Interface
Standard	Tastatur, PACE, Firmwareupdate
Komfort	Display, Terminalzertifikat für eSign

Was bisher geschah...

- Ablauschen der PIN mit Basisleser (CCC/Plusminus)
- Relay via USB-over-IP (Max Moser, Thorsten Schröder)
- Schadsoftware über AusweisApp-Update (Jan Schejbal)

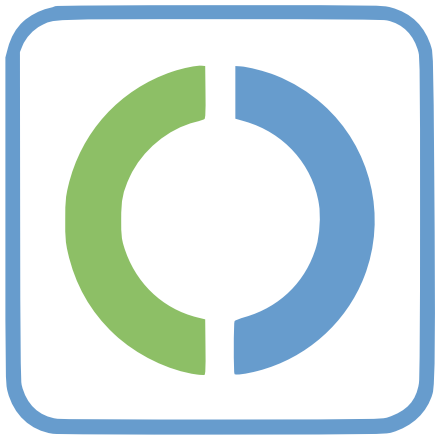
Vorgeschlagene Gegenmaßnahmen





- Firewall und Virenscanner
- Einspielen von Softwareupdates
- Ausweis vom Leser nehmen
- PIN-Eingabe über Bildschirmtastatur

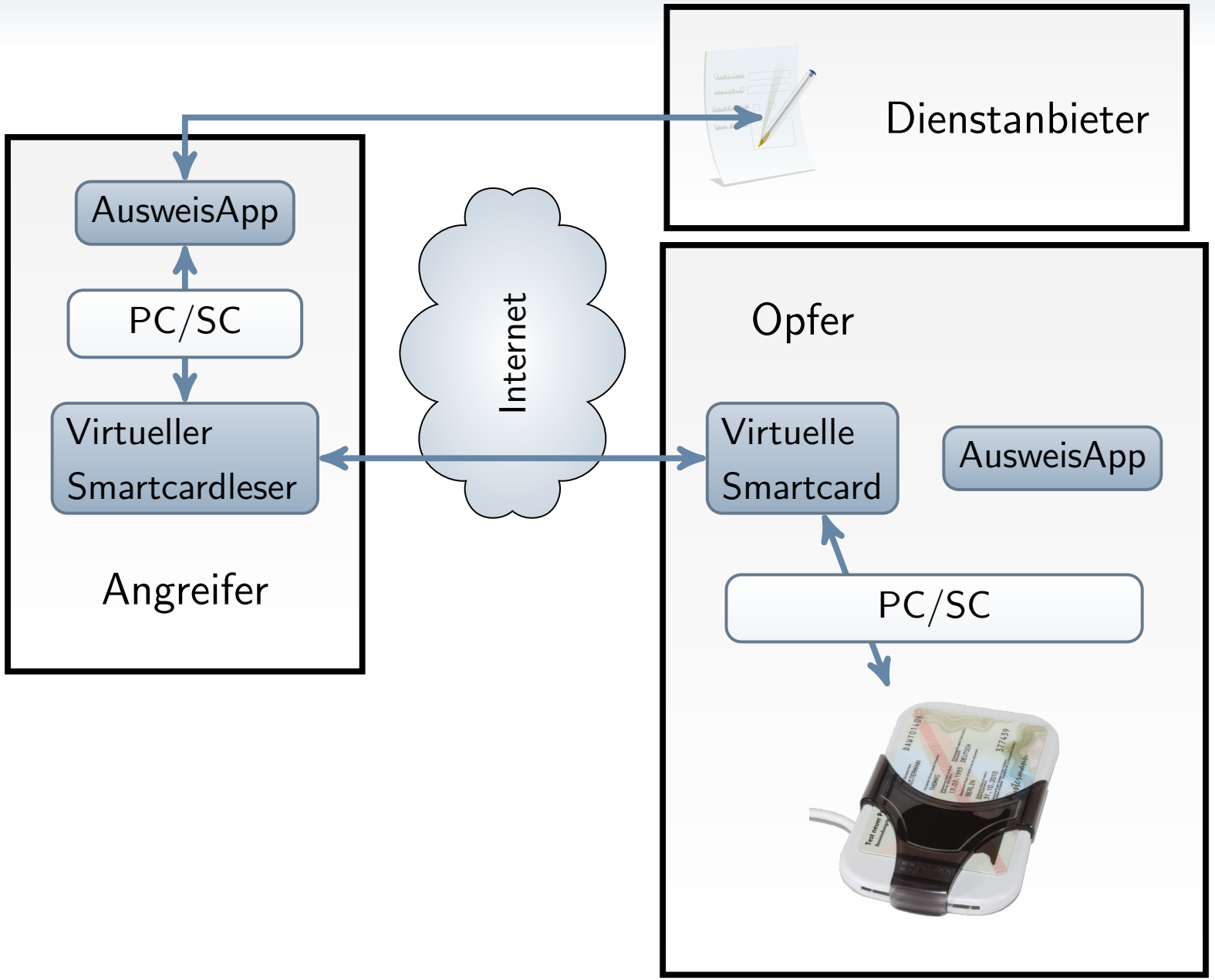
Vorgeschlagene Gegenmaßnahmen



- Firewall und Virenscanner
- Einspielen von Softwareupdates
- Ausweis vom Leser nehmen
- PIN-Eingabe über Bildschirmtastatur
- Komfort- oder Standardleser

Übersicht

Versuchsaufbau – Relay für eID



Annahmen

- Lesegerät ist für den Betrieb beim Opfer vorbereitet
- Neuer Personalausweis ist in Kommunikationsreichweite des Lesegeräts
- Schadsoftware läuft beim Opfer
- Angreifer ist im Besitz der benötigen Geheimnisse

Annahmen

- Lesegerät ist für den Betrieb beim Opfer vorbereitet
- Neuer Personalausweis ist in Kommunikationsreichweite des Lesegeräts
- Schadsoftware läuft beim Opfer
- Angreifer ist im Besitz der benötigen Geheimnisse
- Leser filtert keine APDUs

Relay mit Standard- und Komfortleser

Schutz von Wissen

PIN-Phishing und anderes Social Engeneering?

Relay mit Standard- und Komfortleser

Schutz von Wissen

PIN-Phishing und anderes Social Engeneering?

Schutz von Zugriff

PACE ist lediglich Abfolge von APDUs

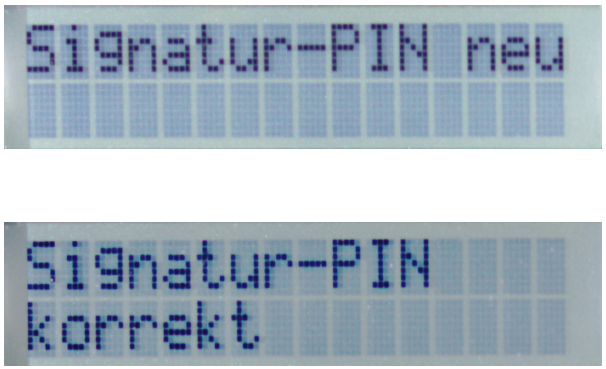
Tabelle: TR-03119 – `EstablishPACEChannel(InputData)`

Pos	Name	Beschreibung
1	`PinID`	Typ des Geheimnisses (MRZ, CAN, PIN, PUK)
⋮	⋮	
5	`PIN`	Geheimnis kann von der Applikation vorgegeben werden, „z.B. gespeicherte CAN“

Qualifizierte elektronische Signatur

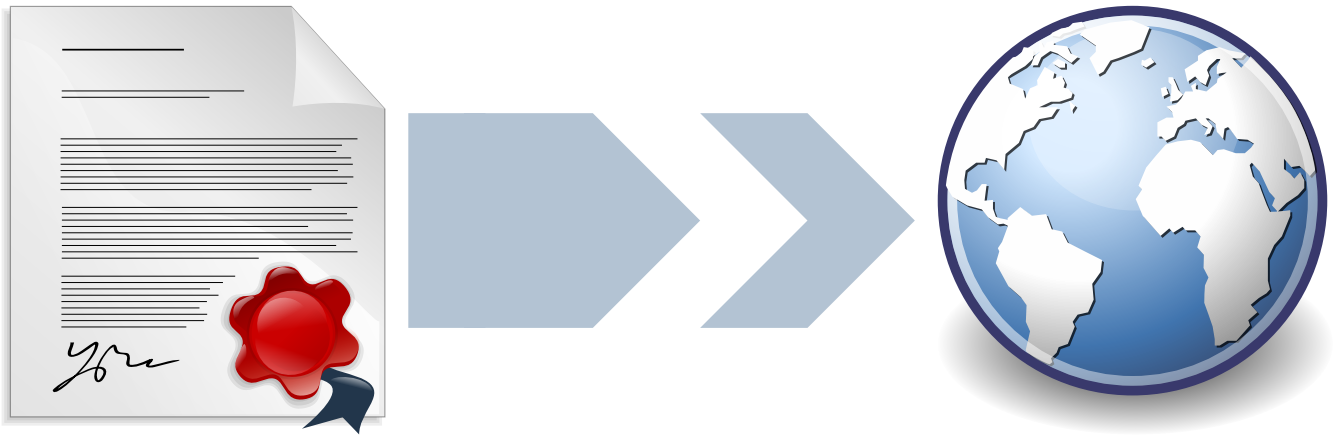
- Mittlerer Schutzbedarf bei eID: Ausweisinhaber haftet nicht
- Hoher Schutzbedarf bei eSign: QES ist rechtsverbindlich

Nachladen der QES



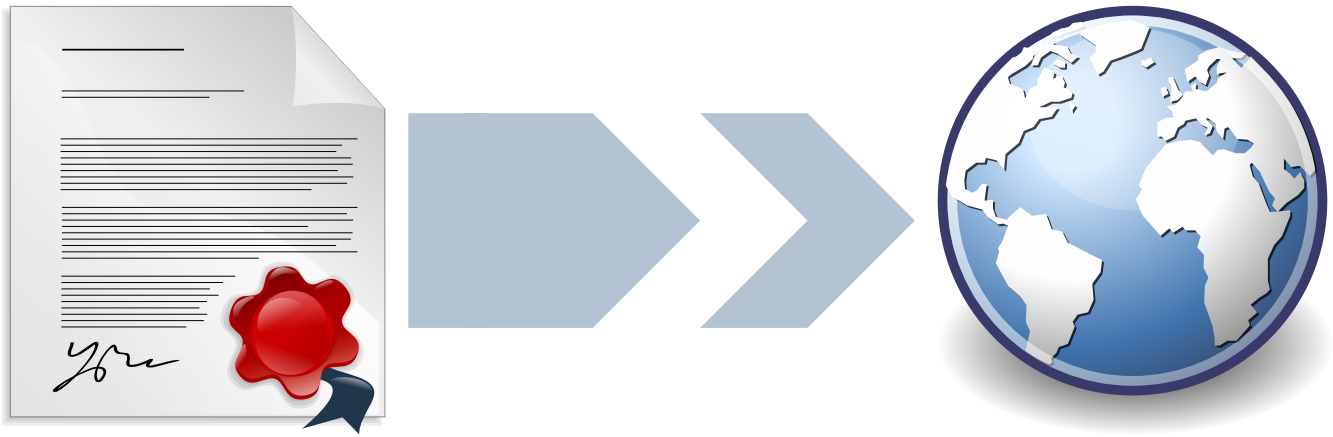
1. Setzen der eSign-PIN mittels eID-PIN und Komfortleser
2. Schlüsselpaarerzeugung durch den ZDA
   - 2.1 Identifizierung mittels eID
   - 2.2 Erzeugen des Signaturschlüssels auf dem Ausweis
   - 2.3 Nachladen des qualifizierten Zertifikats

Nachladen der QES



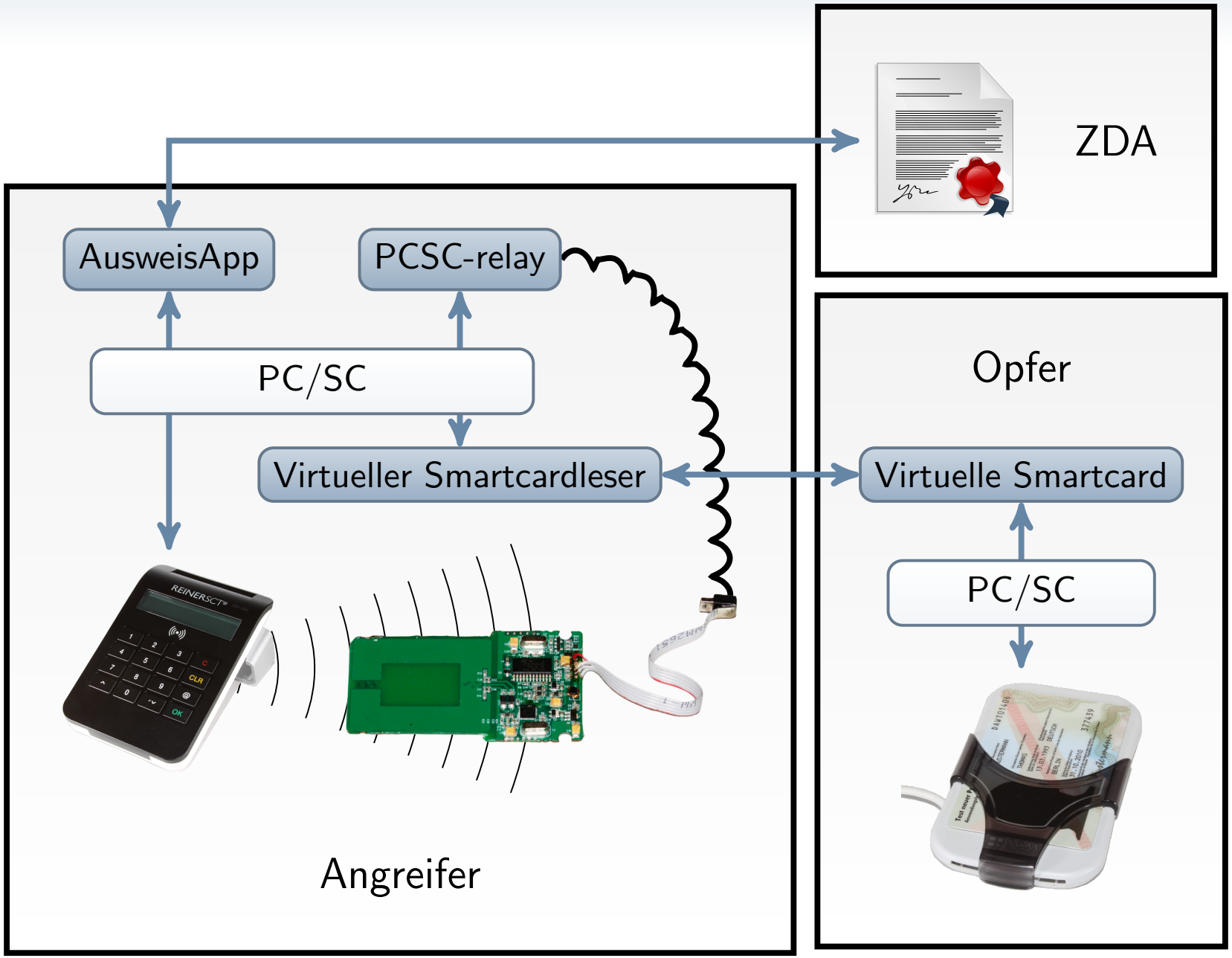
1. Setzen der eSign-PIN mittels eID-PIN und Komfortleser
2. Schlüsselpaarerzeugung durch den ZDA
   - 2.1 Identifizierung mittels eID
   - 2.2 Erzeugen des Signaturschlüssels auf dem Ausweis
   - 2.3 Nachladen des qualifizierten Zertifikats
   - 2.4 Veröffentlichung des Zertifikats durch ZDA

Nachladen der QES



1. Setzen der eSign-PIN mittels eID-PIN und Komfortleser
2. Schlüsselpaarerzeugung durch den ZDA
   - 2.1 Identifizierung mittels eID
   - 2.2 Erzeugen des Signaturschlüssels auf dem Ausweis
   - 2.3 Nachladen des qualifizierten Zertifikats
   - 2.4 Veröffentlichung des Zertifikats durch ZDA
3. Signieren mit eSign-PIN und Komfortleser

Versuchsaufbau – Relay für eSign



Reaktionen auf Relay-Angriffe

Ergänzung der Signaturverordnung

- Der ZDA „hat sich vom Signaturschlüssel-Inhaber den Besitz der sicheren Signaturerstellungseinheit [...] bestätigen zu lassen“
- Mechanismen werden im Rahmen der Zertifizierung geprüft

Standard- und Komfortleser: Authentisierungsfilter

- Genaue Mechanismen nicht vorgeschrieben
- Erste Leser werden nach ITSEC zertifiziert werden
- Bisher kein CC Protection Profile

Übersicht

Authentizität von Komfortlesern

- AusweisApp prüft
  die Bezeichnung des Lesers
- Logo des neuen Personalausweises
  auf dem Chipkartenleser

Authentizität von Komfortlesern (Forts.)

Das Problem: Skimming

Ein Komfortleser besitzt sowohl Zugriff auf den Ausweis als auch die Geheimnisse (CAN/eID-/eSign-PIN).

Authentizität von Komfortlesern (Forts.)

Das Problem: Skimming

Ein Komfortleser besitzt sowohl Zugriff auf den Ausweis als auch die Geheimnisse (CAN/eID-/eSign-PIN).

Terminalschlüssel als starkes Token

- Terminal Authentication mit dem Komfortleser kann ausschließlich von einer Karte durchgeführt werden.
- Terminalzertifikate können nicht zurückgezogen werden.

Übersicht

Ergebnisse

Authentisierungsfaktor „Besitz“

- Es genügt der Zugriff auf die Chipkarte

Authentisierungsfaktor „Wissen“

- eID-PIN anfällig für „Social Engeneering“
- Setzen der eSign-PIN mittels eID-PIN
- CAN: Brute-Force in 4.5 Tagen (Verstoß gegen TR-03110?)

Vertrauenswürdige Geräte

- Schwer verifizierbar
- Drohende „Privilege Escalation“

Fazit

Authentifizierung mit nPA sicherer

- Zugriff auf ein physisches Objekt notwendig
- Starke Kryptografie

Signatur mit nPA sicherer

- Kommunikation zum Ausweis ist verschlüsselt.

Fazit

Authentifizierung mit nPA sicherer

- Zugriff auf ein physisches Objekt notwendig
- Starke Kryptografie

Signatur mit nPA sicherer

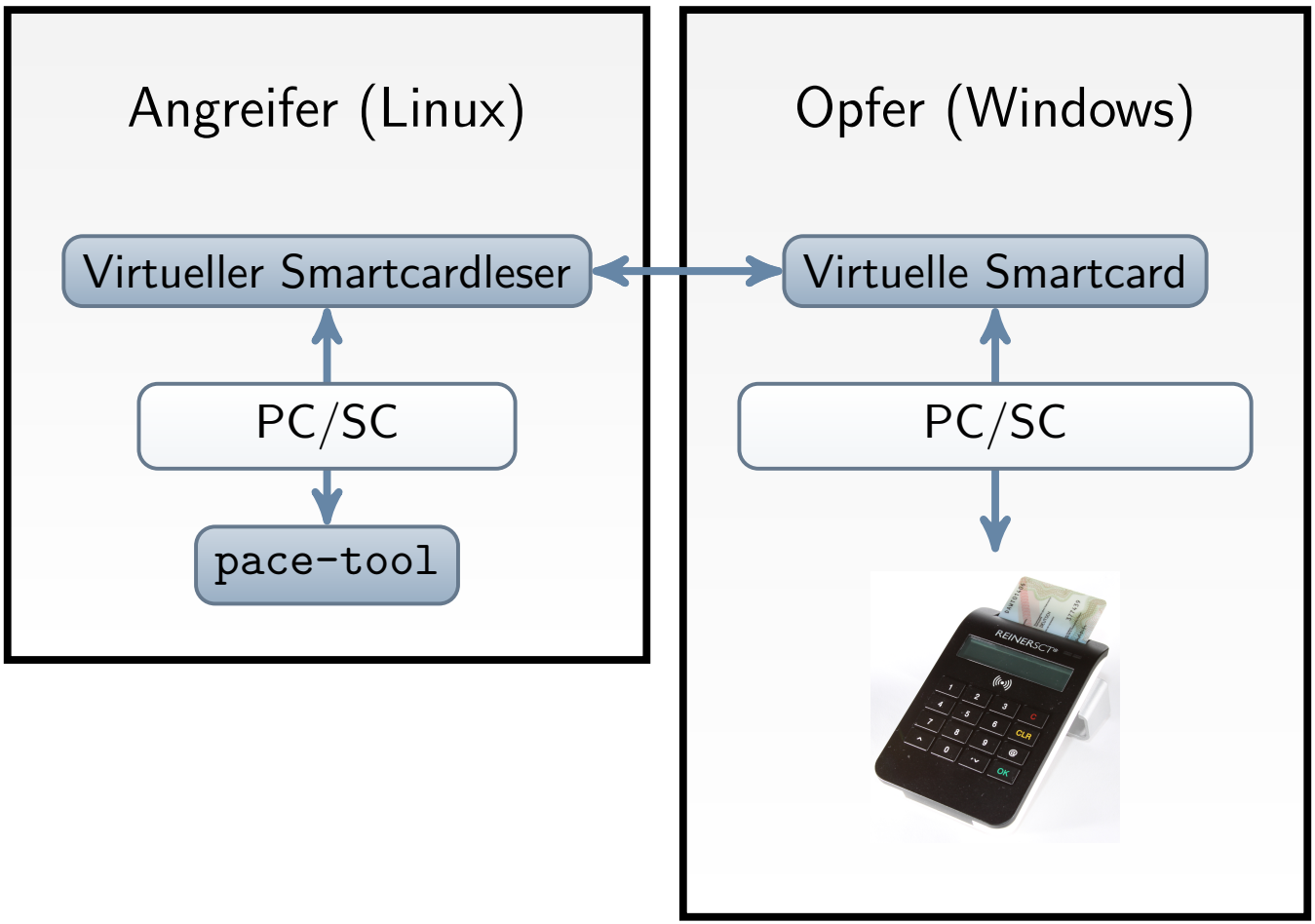
- Kommunikation zum Ausweis ist verschlüsselt.

Attraktiveres Angriffsziel

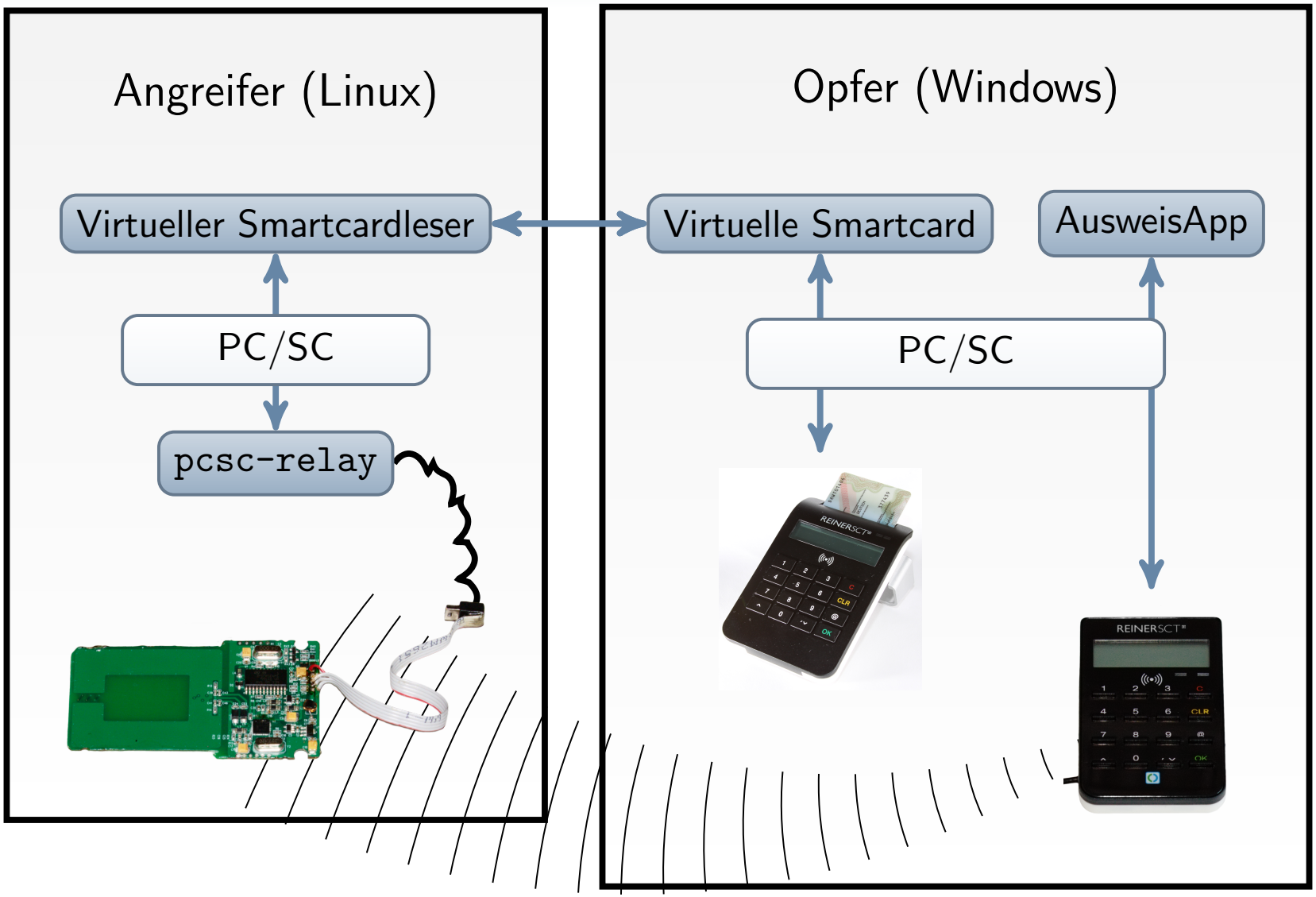
- eSign und eID auf derselben Chipkarte, eSign kann nicht separat deaktiviert werden
- Höherer Schaden bei Missbrauch

Übersicht

Demo


Angreifer (Linux)
Virtueller Smartcardleser
PC/SC
pace-tool
Opfer (Windows)
Virtuelle Smartcard
PC/SC
REINERSCT

Demo


Angreifer (Linux)
Opfer (Windows)
Virtueller Smartcardleser
Virtuelle Smartcard
AusweisApp
PC/SC
PC/SC
pcsc-relay

Mitigation

Maßnahmen gegen Relay-Angriffe

- APDU-Firewall für Standard- und Komfortleser
- Keine Basisleser oder öffentlichen Terminals benutzen?
- Kartendisplay?: Dynamische PIN
- „Distance Bounding“?

Ungewolltes Nachladen der QES verhindern

- Wirklich sicherer zweiter Kanal zur Prüfung des Besitzes
- eSign-PIN setzen?