DREAMLAB
TECHNOLOGIES

Datenschutz Forum Schweiz

SuisseID

Delegate

- Nicolas Mayencourt
  - CEO / Senior Security Analyst
  - > 10 Jahre IT-Security
  - Nicolas.Mayencourt@dreamlab.net

Was ist die SuisseID

- Signaturzertifikat gemäss ZertES (QC)
- Standardisiertes Authentisierungszertifikat (IAC)
- (Eindeutigen) SuisseID-Nummer
- SuisseID Identity Provider Service (IdP)
- Bereitgestellt von ZertES zertifizierten Anbieterin
- Zwingend immer BEIDE Funktionen

DREAMLAB
TECHNOLOGIES

Herausforderungen?

Herausforderungen

- PKI Infrastruktur
- Smartcards
- PCs
- Anwendungen
- Recht

Grundsätzlich:
Keine E2E Kontrolle, mehrere Parteien involviert

PKI Infrastruktur

- Single Point of Failure
  - Vertrauen basiert auf der Sicherheit der PKI
  - Keyleaks
  - Fehlerhafte Prozesse
  - Gezielte Angriffe auf die Infrastruktur

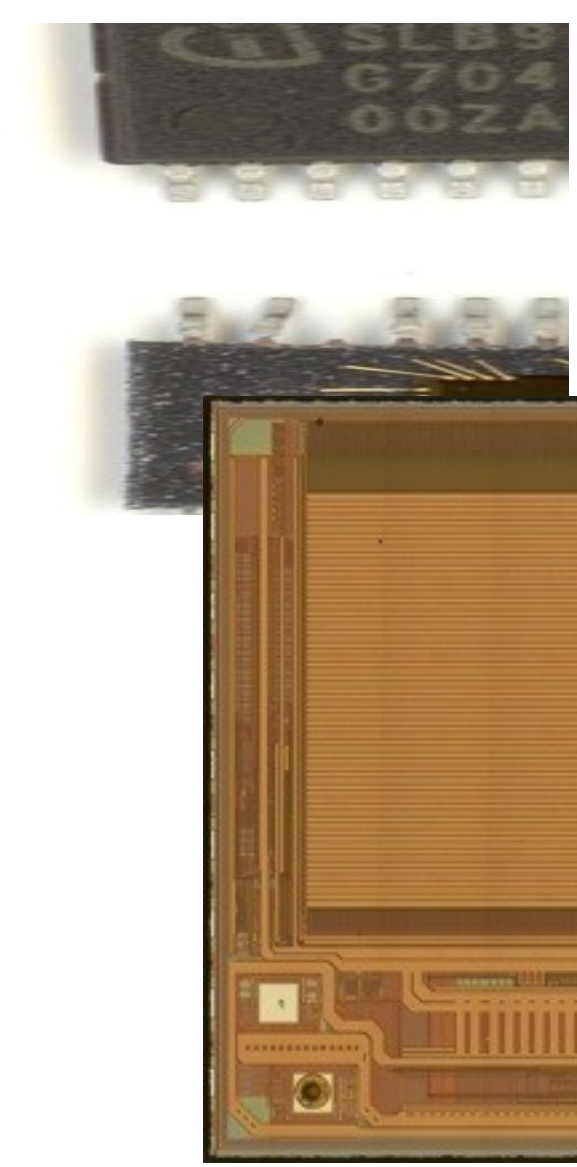
- Die CSPs werden jedoch durch qualifizierte Fachpersonen auf Compliance geprüft

Smartcards

- Sichere Architekturen sollten Angriffe von ausserhalb des Chips abwehren können (Sidechannel Angriffe)
- Nicht möglich eine Smartcard 100% sicher zu entwickeln
  - Jeder Chip ist physikalisch angreifbar
- Multifunktionskarten == Multirisk
  - IAC und QC haben unterschiedlichen Schutzbedarf, jedoch identische interfaces

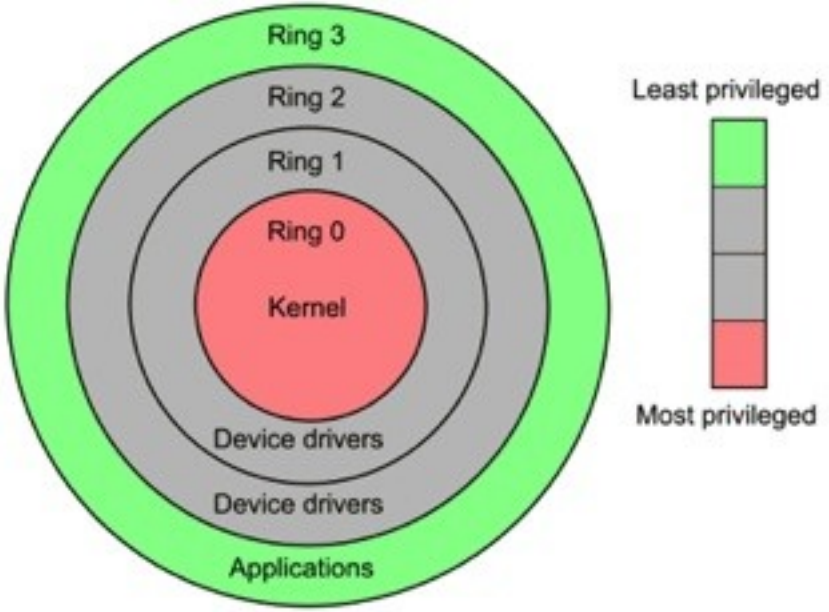
Physikalische Angriffe

Physikalische Angriffe



PCs sind unsicher!

- Der Trust-Anker (Smartcard) kann nicht über einen sicheren Kanal angesprochen werden
- Vertrauenskette unterbrochen
- Eine Applikation (Ring 3) kann nicht verhindern, dass sie von einer Malware aus dem Ring 0 (Treiber, Kernel) attackiert wird.



PCs sind unsicher!

- SuisseID sharing via USB
  - Unsichere Leser werden eingesetzt
  - Überraschung -> PCs sind unsicher

  - USB Schnittstelle wurde umgeleitet
  - Angreifer im “Besitz” der Karte sowie der entwendeten PIN

PCs sind unsicher!

- Einige Reaktionen
  - Da ist der Endbenutzer aber selber schuld, wenn er ungenügend geschützt ist
  - Jaja, aber Trojaner sind REINE Theorie!
  - Hersteller untersuchen jetzt die Bedrohung ausgehend von der USB Schnittstelle (Reaktives Vorgehen wie bei Anti-Viren)

PCs sind unsicher!

- Achtung!
  - Trojaner, wie zum Beispiel Stuxnet sind leider Realität, auch für CSPs
  - 27C3 wurde ein ähnlicher relay Angriff demonstriert, welcher jedoch die PC/SC Schnittstelle anstelle von USB nutzt
    - Selbes Problem, neue Schnittstelle
    - ALLE Schnittstellen in einem PC sind nicht vertrauenswürdig, GAAANZ SICHER!
  - Multifunktionskarten bergen Risiken, was ebenfalls am 27C3 gezeigt wurde

Applikationen

- Allgemein: PCs sind unsicher
  - Applikationen werden auf dem PC ausgeführt
  - Genau desshalb setzen nahezu alle Finanzinstitute auf Transaktionssignierung
    - Benötigt mind. Klasse 3 Leser
- QC
  - Integrität als Grundlage der Authentizität
  - Mindestens einer der verfügbaren Signer ist immer noch unsigniert und kann nach belieben verändert werden
  - PDF Kollisionen seit Aug 2010 dokumentiert

Rechtliche Aspekte

- SuisseID != E-Banking/Kreditkarten
  - Endkundenrisiko bei Banken und Kreditkarten Missbrauch ist heute faktisch nahezu 0
    - Kulanz
    - Teilhaftung
    - Regelung bezüglich Datensicherheit (PCI)
  - Bei einer rechtsverbindlichen Unterschrift haftet im Zweifelsfall der Endbenutzer alleine
  - Diverse, unklar definierte Gesetzestexte

Rechtliche Aspekte

- ZertES Art. 6 Absatz 3
  Bei der Gestaltung des Signaturprüfungsvor-gangs ist darauf zu achten, dass folgende Anforderungen mit hinreichender Sicherheit gewährleistet sind:

  a. Die zur Überprüfung der Signatur verwendeten Daten entsprechen den Daten, die der Überprüferin oder dem Überprüfer angezeigt werden.

  b. Die Signatur wird zuverlässig überprüft und das Ergebnis dieser Überprüfung wird korrekt angezeigt.

Rechtliche Aspekte

- OR Art. 59a Haftung für Signaturschlüssel
  1. Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes über die elektronische Signatur vom 19. Dezember 2003 verlassen haben.
  2. Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern.
  3. Der Bundesrat umschreibt die Sicherheitsvorkehrungen im Sinne von Absatz 2.

Inverse Haftung?

- Der Endbenutzer muss die volle Verantwortung über sein System und die Dienstleistungskette tragen?

  - Gewisse Bereiche KANN er nicht beeinflussen
  - Es existieren teilweise KEINE Lösungen (Antiviren OSX?, iPad?...)
  - Selbst Spezialisten können nur schwer nachweisen, ob ihr System “Trojaner-Free” ist

Unsere Sicht

Desto breiter eine Lösung eingesetzt wird, desto attraktiver wird diese für potentielle Angreifer

- Bessere Leser
  - Mindestens Klasse 3, lieber System-unabhängig
- Bessere Mechanismen
- Klarere Rechtsverhältnisse
- Auftrennung der Zertifikatsfunktionen nach Schutzbedarf

Unsere Sicht

Fazit:

Die Frage ist wie die (Rest-) Risiken behandelt werden

Juristisch, technisch und organisatorisch

Ihre Sicht

- Wie geht es wohl weiter?
- Wie reagiert die Schweiz auf Schwachstellen?
- Wie wird mit Missbrauch umgegangen?
- Rechtsinterpretation?

Game Over