Zertifizierung in der Schweiz

Jean Paul Kölbl
CEO IT-Secure.com AG

Vorstellung

- Solution Provider für IT-Sicherheit und Applikations-Integration
- Technologie Leader im Bereich PKI
- Audit, Review und Awareness unter anderem für Kreditkarten-Firma
- Projekte
  - Hochintegrierter PKI mit über 100 Applikationen und ca. 20‘000 Nutzern in einer Grossbank
  - Credit Suisse Group PKI
    - Architektur, Design und Implementation
  - Winterthur Versicherungen
    - Basierend auf Vorgaben von CSG PKI innerhalb von 4 Monaten in die Betriebsorganisation integriert und ausgerollt
  - Kanton Zürich → Projekt Soprano

Agenda

- Was ist E-Commerce?
- Die benötigten Sicherheitsfunktionen
- Was bieten Zertifikate
- Qualifizierte Zertifikate
- Was tut der Bund?
- E-ID. Was nützt sie?
- Und die privaten Anbieter?
- Was will der Markt?
- Fragen → Antworten

DEFINITION

E-Commerce ist die Eliminierung von Medienbrüchen in der Wertschöpfungskette

Das Risiko dabei:

Mit der Eliminierung von Medienbrüchen gehen auch manuelle oft unbewusst vorgenommene Sicherheitsüberprüfungen verloren

Welche Funtionen?

Grundlage des sicheren elektronischen Datenaustausches sind folgende 4 Funktionen

- P = Privacy (Verschlüsselung)
- A = Authentication (Identifikation)
- I = Integrity (Integrität)
- N = Non-Repudiation (nicht Abstreitbarkeit)

Was bieten Zertifikate?

- Privacy
  - Zertifikate ermöglichen aufgrund von asymmetrischer Kryptographie verschlüsselung von Daten für Sie selbst oder für beim Datenaustausch (Dokumente, E-Mail, SSL)
- Authentication
  - Mittels einem Zeritifkat können Sie eine Entität überprüfen (sofern Sie dem Ausgeber vertrauen)
- Integrity
  - Zertifikate ermöglichen Integritäts-Prüfungen mittels digitaler Signatur
- Non-Repudiation
  - Je nach Trust-Level und Anwendung schwierig zu implementieren....

Qualifizierte Zertifikate?

- Für Verträge die explizit die Schriftlichkeit fordern gemäss OR
- Geschätze Investitions-Kosten für den Aufbau der Infrastruktur und der Organisation gemäss ZertDV CHF 15 Millionen gemäss Bundes-Studie
- Betriebskosten bei 1 Million Nutzer pro Jahr: CHF 30 Mio gemäss Bundes-Studie
- Nicht gerechnet wurde Marketing, SmartCard Reader für den Nutzer und die Zinsen

Was tut der Bund?

- Studie erstellt „Braucht die Schweiz einen amtlichen, digitalen Ausweis?“ (http://www.ofec.admin.ch/themen/ri-ir/dig-id/studie-digiausweis-d.pdf)
- Motiviation des Bundes
  - Förderung des Wirtschaftsstandortes Schweiz
  - Stärkeres Vertrauen in ein vom Staat ausgestelltes Zertifikat
- Folgende Handlungsmöglichkeiten untersucht
  - Nichts tun
  - Sich an einem privaten Zertifizierungsdienstanbieter beteiligen
  - Der Bund macht es selbst (amtl. digitaler Ausweis)
- Resultat: das BIT führt einen internen Pilot durch, das EJPD erstellt bis Q4 2004 die gesetzlichen Grundlagen
- Ev. Bis 2007 einsatzbereit?

E-ID. Was nützt Sie?

- Harte Identifizierung einer Privat-Person
  - Garantierte Identität eines Bürgers
  - Name, Vorname, Geburtsdatum, Register-Nummer
- Welchen Nutzen hat diese Information für Sie?
  - Nachregistrierung nötig!
  - Wollen Sie von vorne beginnen?
- Nur für P2G und P2B!
- Wieviele Rollen haben Sie?
  - Eine E-ID kann kaum in Ihrem Geschäft für Ihre tägliche Arbeit eingesetzt werden

Und die privaten Anbieter?

- Nach der Schliessung von Swisskey wurde IGtop gegründet. Mit CHF 100‘000 ein Businessplan erstellt der aufzeigt, dass ein Zertifizierungsdienst nicht Kostendecken betrieben werden kann...
- Frage: benötigt die Privatwirtschaft wirklich qualifizierte Zertifikate? Ist weniger nicht mehr?
  - CSP-Forum erhält Aufgabe Trust-Levels zu definieren, die „weniger teuer“ sind und die verifiziert werden können
  - Die 3 Anbieter auf dem Markt (SwissCERT AG, Swisssign und swissetrust) erarbeiten diese Standards im CSP-Forum (www.csp-forum.ch)

Was braucht der Markt?

- **Unterschiedliche Trust Levels**
  - Finanzdienstleister, Versicherungen, Bund und Chemie haben zum Teil sehr hohe Anforderungen an den Trust Level
  - Migros e-Shop, Buchhandlungen, CD-Shops etc. bevorzugen einen tieferen, d.h. günstigeren Trust Level
- **Offene PKI-Systeme**
  (Zertifikate können von allen genutzt werden)
  - Bund und Kantone wollen explizit offene Systeme, die von allen Anbietern von E-Services verlässliche Information über die Identität des Zertifikatsbesitzers Auskunft geben

Was braucht der Markt..

- **Geschlossene PKI Systeme**
  (Zertifikate können nur in einem geschlossenen System benutzt werden)
  - das Registrieren der Nutzer, so wie es heute durchgeführt wird, ist sehr aufwendig und kostenintensiv.
  - Ein Dienstleister, der sich bereit erklärt, diese enormen Investitionen zu tätigen, möchte diese auch schützen – mit Recht!
    Dies ist mit offenen Systemen nicht möglich.
  - Jeder andere Dienstleister kann diese Zertifikate dann auch für seine Dienste nutzen.

Was braucht der Markt ...

- **Preis:** für Privatpersonen möglichst günstig
  - Registrierungsprozess muss vereinfacht werden, um Kosten zu sparen.
  - Für Institutionen die ein geschlossenes System nicht selbst betreiben, muss der Preis der "outgesourcten" Lösung deutlich günstiger sein, als ein Eigenbetrieb.
- **Benutzerfreundlichkeit:** Nur ein einziges Zertifikat
- **Fazit**
  - Stark konfliktäre Bedürfnisse
  - Mit herkömmlicher Technologie nicht zu lösen
  - Neue Konzepte sind gefragt (wie SwissCERT).

Fragen?

- Entwirrung statt Verwirrung?
- Präsentation steht ab Montag elektronisch zum Download bereit: www.it-secure.com →knowledge

- Nächste Präsentation: Daniel Büttiker, CEO SwissCERT AG