Security Class 3

für den Portalverbund

Peter Pfläging
IKT Architekt
Stadt Wien, MA 14
eMail: peter.pflaeging@wien.gv.at

Was ist die SecClass3?

- Wo:
  - Transaktion auf sensible Daten (§ 4 (2) und § 18 (2) DSG2000)
  - Schutzbedarf „hoch“ nach IT-Sicherheitshandbuch

- Wie:
  - Authentifiziert durch Wissen und Eigenschaft an in einem geschützten Bereich betriebenen Gerät
  - Authentifiziert durch Wissen und Besitz an in einem geschützten Bereich3 betriebenen Gerät
  - Authentifiziert durch Wissen und Besitz an einem mobilen Endgerät mit erhöhtem Grundschutz

Implementierung

- Internes Netz mit gemanagtem Gerät
  - lokales Netz
  - VPN
  - Gerät mit aktuellen Updates & Virenschutz
- Wissen und Besitz
  - Karte oder Gerät mit PIN-Code
  - TAN Listen
  - One Time Passwort mit Gerät
  - SMS Verifikation mit fixem Handy
  - Bürgerkarte

Mögliche Karten und Geräte

- Secure Cards
  - PKCS#15 Karte (ISO/IEC 7816-15)
    - PKCS#11 oder Windows CSP Treiber für Browser
  - Z.B.: „Aladdin eToken“
    - Proprietärer Treiber
  - A-Trust Karte mit oder ohne qualifiziertem Zertifikat
    - A-Sign Client für Encryption Certificate
  - Qualifiziertes Zertifikat mit Bürgerkartenumgebung und MOA-ID
    - BKU am Client und MOA-ID im Portal

Andere Methoden

- „One Time Password“
  - RSA Token
  - TAN Listen
  - OTP nach RFC 2289
- Wird am Portal typischerweise mit
  - TACACS (RFC 1993) oder
  - RADIUS (RFC 2865) implementiert
- SMS TAN
  - wie bei Online Banking
  - Selbst zu implementieren
- Fingerprintleser
  - Wissen und Eigenschaft! (nicht zu empfehlen!)

Erfahrungen

- Technologieprobleme:
  - Timeout in den Verbindungen
  - Gleichzeitige Nutzung von mehreren Diensten / Karten
  - Rollout
- Organisatorische Probleme
  - Rollout über „Registration Officer“
  - Was passiert, wenn die Karte vergessen wird?
- „Menschliche Probleme“
  - Akzeptanz (Personalvertretungen!)
  - Bedienbarkeit
  - Schulung

Implementierungstiefe

- Im Browser beim Portal Logon
  - leicht implementierbar
  - spezifisch für Web Portal Lösungen
  - keine Integration in das Betriebssystem

- Beim Logon an den Rechner
  - durchgängige Lösung
  - Bei Ziehen der Karte ist Gerät gesperrt
  - schwieriger zu implementieren
  - Ohne Karte kein Arbeiten
  - Windows & Active Directory Support mangelhaft

Fragen?

Vielen Dank

Peter Pfläging

- http://www.buergerkarte.at
- http://de.wikipedia.org/wiki/PKCS
- http://rsa.com/rsalabs/node.asp?id=2124
- http://www.opensc-project.org/
- http://de.wikipedia.org/wiki/Einmalpasswort
- http://www.cryptoshop.com/
- http://www.a-trust.at/