Einsatz von Zertifikaten im Bereich der DFN-AAI

6. Shibboleth Workshop

- Frankfurt, 8. Mai 2008 -

Marcus Pattloch (DFN-Verein)

pki@dfn.de

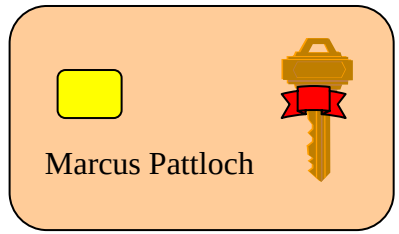
Was ist ein Zertifikat?

- Zertifikat = persönlicher Ausweis im Internet
- jeder, der ein Zertifikat besitzt, kann im Netz authentisch auftreten
- jeder, dem ich im Netz mein Zertifikat zeige, kann sicher sein, wer ich bin

- z.B. in Form einer „Chipkarte“

  (aber: nicht jede Chipkarte

  enthält ein Zertifikat)



Was können Zertifikate?

- Zertifikate ersetzen Passwörter
  - grundsätzlich EIN Zertifikat pro Person (jeder hat auch nur einen Ausweis)
  - Schluss mit vielen verschiedenen Passwörtern (die man sich doch nicht merken kann)
  - Sicherheit von Zertifikaten grundsätzlich deutlich höher als von Passwörtern
  - einfache Nutzung der Zertifikate möglich (weitgehend transparent)

Anwendungsgebiete (Beispiele)

DFN Deutsches Forschungsnetz

- Signatur
  - Signieren von .pdf Dokumenten
  - Signieren von E-Mails
- Authentisierung
  - Zugriff auf geschützte Webbereiche
  - Anmelden an Rechnern oder Datenbanken (ssh, IPsec)
  - Server weisen sich aus (SSL, https)
- Vertraulichkeit
  - Verschlüsseln von Dokumenten und E-Mails

Nutzung von Zertifikaten

- Zertifikate der DFN-PKI werden im Betrieb der DFN-AAI an mehreren Stellen eingesetzt
- Einsatzzwecke von Zertifikaten in DFN-AAI
  - beim Betrieb von Shibboleth
  - zur Authentifizierung der Webserver, die die Dienste anbieten
  - zur Authentifizierung von Nutzern

Zertifikate 1: Shibboleth intern

- Zertifikate beim Identity Provider und beim Service Provider
  - Beide Instanzen müssen sich bei der Shibboleth-internen Kommunikation gegenseitig „elektronisch ausweisen“
- Zertifikate zum Signieren der Metadaten
  - Metadaten enthalten wichtige betriebliche Daten über die Föderation
  - Authentizität der Metadaten erforderlich

Zertifikate 2: Webserver

- In der DFN-AAI gibt es folgende Webserver
  - Service Provider: stellt seine Informationen den Nutzern zur Verfügung
  - Identity Provider: stellt die Formulare zur Anmeldung von Nutzern zur Verfügung
  - WAYF-Server: stellt Nutzern ein Formular zur Auswahl ihrer Heimateinrichtung zur Verfügung
- Alle Webserver müssen Zertifikate zur Authentifizierung verwenden

Zertifikate 3: Nutzer

- Derzeit verwenden Nutzer zur Authentifizierung meistens Username/Password
- Alternativ kann die Authentifizierung auch per Nutzerzertifikat erfolgen
- Zukünftig kann auf Basis der Stärke der Authentifizierung die Nutzung von Diensten geregelt werden, z.B.
  - Zugriff auf „kritische Dienste“ nur bei starker (zertifikatbasierter) Authentifizierung

Zertifikate in der DFN-AAI

www.pki.dfn.de/aai

FAQ zu Zertifikaten in der DFN-AAI

DFN-PKI Sicherheitsniveau Global

- Zertifikate sind mit in Standardbrowsern vorhandenem Zertifikat verkettet
  - MS / Internet Explorer
    - Windows verwendet zentralen Zertifikatspeicher
    - Windows XP, Windows 2000: OK
    - Windows Vista: OK, aber mit „Überraschungen“
  - Mozilla
    - anwendungsspezifisch, z.B. Firefox, Thunderbird
    - Verkettung (hoffentlich endlich) ab Sommer 2008
- Gültigkeit von Zertifikaten
    - Server max. 5 Jahre, Nutzerzertifikate max. 3 Jahre

Zusammenfassung

- Zertifikate werden in der DFN-AAI an verschiedenen Stellen benötigt
- DFN unterstützt Teilnehmer durch DFN-PKI
  - Ausstellung von Nutzer- und Serverzertifikaten
  - Beratung und Hilfe bei Nutzung von Zertifikaten

✓ Web: www.pki.dfn.de/aai

✓ Kontakt: pki@dfn.de