Auslagerung und „Root im Browser“
-
Zwei Erfolgsfaktoren der DFN-PKI

Marcus Pattloch (DFN-Verein)

DFN-Nutzergruppe Hochschulverwaltung

8 . Tagung in Halle, 8. Mai 2007

Übersicht

- Auslagerung von Zertifizierungsstellen
- Root im Browser
  - Migration, Verankerung in Standardbrowsern
- Weitere Neuigkeiten zur DFN-PKI
  - FAQ, Online-CA, Schnittstellen, Grid, DFN-AAI
- Ausblick
  - Redundanzkonzept der DFN-PKI
  - Integration lokaler PKI-Strukturen
- Zusammenfassung

Auslagerung von Zertifizierungsstellen

häufige Problemlage

- Viele Einrichtungen benötigen Zertifikate
- Ein Zertifizierungsdienst wird aufgesetzt, aber es stellt sich heraus
  - der Aufwand für den Betrieb einer eigenen Zertifizierungsstelle ist sehr hoch
  - insbesondere die Einstiegshürde ist sehr hoch
- Der Zertifizierungsdienst „kommt nicht zum Fliegen“

Wie bekomme ich ein Zertifikat?

Digitaler Ausweis

Ich benötige ein Zertifikat

↓

Registrierungsstelle

↓

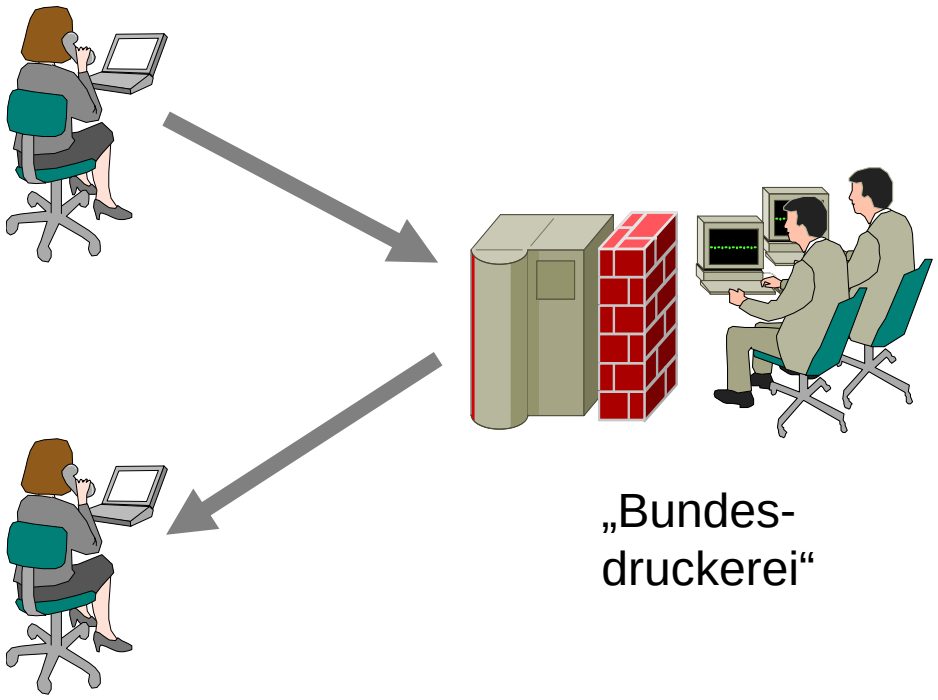
Zertifizierungsstelle

↓

Registrierungsstelle

↓

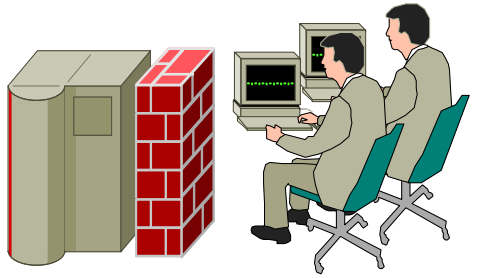
Ich habe ein Zertifikat



Auslagerung = Aufgabentrennung

- Registrierungsstelle
  - administrative Arbeiten
  - verbleibt in der Einrichtung
  - vergleichbar einer Meldestelle

- Zertifizierungsstelle
  - technisch aufwändige Arbeiten
  - wird an DFN ausgelagert
  - vergleichbar der Bundesdruckerei



Vorteile der Auslagerung

- keine eigene Technik erforderlich, weder Hard- noch Software (nur Standard-Browser)
- lokaler Aufwand wird deutlich reduziert
  - Synergie für Anwender, die bereits eigene PKI-Strukturen betreiben
  - Einstieg für „kleine“ Anwender deutlich vereinfacht
- Entgelt im Dienst DFNInternet enthalten
- Regelbetrieb hat im Januar 2006 mit dem Übergang auf das X-WiN begonnen

Status Auslagerung (Mai 2007)

- Über 100 Einrichtungen haben ihre CA bereits an den DFN-Verein ausgelagert
  - ALP Dillingen, Bayerische Staatsbibliothek, Bessy, Bibliotheksservice-Zentrum Baden-Württemberg, Bundesanstalt f. Geowissenschaften u. Rohstoffe, Bundesanstalt für Wasserbau, Campus Berlin-Buch, Charite Berlin, DESY, DFN-CERT Services GmbH, DFN-Geschäftsstelle, Deutsches Klimarechenzentrum, Deutsches Krebsforschungszentrum, Deutsches Zentrum f. Luft- u. Raumfahrt e.V., DIPF, European Southern Observatory, FIZ Chemie Berlin GmbH, FH Augsburg, FH Biberach, FH Bielefeld, FH Düsseldorf, FH Dortmund, FH Erfurt, FH Flensburg, FH Frankfurt am Main, FH Fulda, FH Giessen-Friedberg, FH Ingolstadt, FH Kiel, FH Landshut, FH Lippe u. Höxter, FH Oldenburg Ostfriesland Wilhelmshaven, FH Osnabrück, FH Rosenheim, FH Südwestfalen, FH Stralsund, FH f. Technik u. Wirtschaft Berlin, Forschungszentrum Dresden-Rossendorf, Forschungszentrum Jülich, Freie Univ. Berlin, GeoForschungsZentrum Potsdam, Gesellschaft f. wissenschaftliche Datenverarbeitung Göttingen, GKSS, GSI, HAWK FH Hildesheim/Holzminden/Göttingen, Hahn-Meitner-Institut Berlin GmbH, Hochschulbibliothekszentrum NRW, HS Anhalt, HS Esslingen, HS Harz, HS Heilbronn, HS Magdeburg-Stendal, HS Neubrandenburg, HS Niederrhein, HS Ravensburg-Weingarten, HS Wismar, HS Zittau-Görlitz, HS für Musik und Theater Leipzig, HS f. Grafik u. Buchkunst Leipzig, HS f. Technik u. Wirtschaft Dresden (FH), HS f. angewandte Wissenschaften Hamburg, IPK Gatersleben, Jacobs University Bremen, Katholische Univ. Eichstätt-Ingolstadt, Leibnitz-Institut f. Atmonsphärenphysik Kühlungsborn, Leibniz-Institut f. Meereswissenschaften Kiel, Leibniz-Institut f. Polymerforschung e.V., Leibniz-Rechenzentrum, Max-Planck-Institut f. Gesellschaftsforschung, Rheinisch-Westfälische Technische HS Aachen, Robert Koch-Institut, T-Systems Enterprise Services, T-Systems SfR, TU Braunschweig, TU Chemnitz, TU Clausthal, TU Dresden, TU Harburg, TU Kaiserslautern, TU München, Univ. Bamberg, Univ. Bielefeld, Univ. Bremen, Univ. Dortmund, Univ. Freiburg, Univ. Gießen, Univ. Greifswald, Univ. Hamburg, Univ. Hannover, Univ. Köln, Univ. Kassel, Univ. Kiel, Univ. Konstanz, Univ. Lübeck, Univ. Leipzig, Univ. Münster, Univ. Magdeburg, Univ. Marburg, Univ. Passau, Univ. Rostock, Univ. Siegen, Univ. Stuttgart, Univ. Tübingen, Univ. Würzburg, Univ. Weimar, WiNShuttle, Wissenschaftszentrum Berlin, Zentrum f. Informationsverarbeitung u. Informationstechnik

„Root im Browser“

Root im Browser (1)

- Ziel
  - in der DFN-PKI ausgestellte Zertifikate sollen bis zu einem in den Standardbrowsern vorhandenen Zertifikat verkettet sein
- Vorteile
  - keine „pop-up Boxen“ bei Webservern
  - Signaturen werden weltweit als gültig erkannt
- Status
  - intensive Vorauswahl und Verhandlungen
  - zur DFN-MV 12.2006 erfolgreich abgeschlossen

Root im Browser (2)

- Wurzel der DFN-PKI ist in Standardbrowser verlinkt
  - Wurzel der DFN-PKI wurde signiert durch „Deutsche Telekom Root CA 2“ (2048 bit)
  - „Deutsche Telekom Root CA 2“ ist Bestandteil des kommerziellen Zertifikatgeschäfts der Deutschen Telekom
  - Signatur erfordert starkes Vertrauen in Sicher-heitsniveau der signierten Wurzel der DFN-PKI
  - Jährliche Audits der DFN-PCA!

Root im Browser (3)

- Um die Verlinkung möglich zu machen, waren wichtige Voraussetzungen zu erfüllen
  - alle Zertifizierungsstellen (CAs) müssen bei der DFN-PCA in Hamburg betrieben werden
  - Begehung der Infrastruktur bei der DFN-PCA in Hamburg --> positive Begutachtung
  - Zertifikate nur nach persönlicher Identifizierung
- Neues Sicherheitsniveau „Global“
  - Neue Policy Version 2.1 (inkl. Classic und Basic)

Wichtige Änderungen in Policy

- Neue Policy Version 2.1
  - Integration der drei Sicherheitsniveaus Global, Classic und Basic in einem Dokument
- Laufzeit von Zertifikaten
  - Server max. 5 Jahre
  - Nutzerzertifikate max. 3 Jahre
  - CA-Zertifikate max. 12 Jahre (max. bis 2019)
- Schlüssellänge Global mind. 2048 bit RSA
  - manchmal Probleme mit älteren Chipkarten

Verankerung Wurzelzertifikat

- Mozilla
  - anwendungsspezifisch, z.B. Firefox, Thunderbird
  - Verkettung ab Sommer 2007 im Vertrag geregelt
- Verankerung im Internet Explorer
  - bei Windows Systemen ist wegen des zentralen Zertifikatspeichers das Betriebssystem entscheidend, nicht die Browserversion
  - Windows XP, Windows 2000: OK, damit Verankerung auch auf „jetzigen“ Systemen
  - Windows Vista: OK, aber neue Vorgehensweise von MS mit einigen „Überraschungen“

Migration nach Global

- Alle Anwender, die die „Root im Browser“-Eigenschaft nutzen wollen, können ihre CA von „Classic“ nach „Global“ migrieren
  - dabei auch Umstellung auf neue Policy und neue Webschnittstellen
- Kollegen der DFN-PCA haben seit Januar alle Anwender mit Classic CA kontaktiert
  - über 80 Classic CAs nach Global migriert
  - Migrationsprozess weitgehend abgeschlossen

Weitere Neuigkeiten zur DFN-PKI

DFN-PKI: Neue Funktionen

- Dienstleistung der DFN-PKI wurde zudem in mehreren Punkten verbessert, insb.
  - Self-Service Schnittstelle freigegeben für große Anzahl von Zertifikaten („Batch“)
  - Webschnittstellen wurden überarbeitet und funktional erweitert
  - schnelle Zertifikatausstellung durch Online-CA

DFN-Test-PKI

- Prozesse können „geübt“ werden
  - Schnittstelle für Nutzer
  - Schnittstelle für Registrierungsstellen
  - Ausstellung von (Test-) Zertifikaten
- DFN-Test-PKI steht Anwendern zur Verfügung
  - angepasst an aktuelle Schnittstellen / Funktionen
  - Benutzeranleitung ist online verfügbar
- Bei Interesse Zugangskennung unter:

pki@dfn.de

FAQ der DFN-PKI

www.pki.dfn.de/faqpki

Grid-Zertifikate

- Ausstellung von Grid-Zertifikaten
  - fast alle Grid-Anwendungen benötigen Zertifikate
  - Grid-Zertifikate ausschließlich im Rahmen der EUGridPMA (DFN akkreditiert seit Juni 2005)
  - Grid-Zertifikate der DFN-PKI werden weltweit anerkannt
- Angebot neuer Typ von Grid-Zertifikaten
  - SLCS (Short Lived Credential Services)
  - Proxy-Zertifikate

Zertifikate in der DFN-AAI

- Authentifizierung
  - Identifizierung von Entitäten („wer bin ich?“)
- Autorisierung
  - Steuerung der Zugriffsmöglichkeiten auf Ressourcen („was darf ich?“)
- wichtige Basis: Public-Key Infrastruktur (PKI)
  - Zertifikate der DFN-PKI werden im Betrieb der DFN-AAI eingesetzt

✓ Mehr zur DFN-AAI in nachfolgenden Vorträgen

Ausblick

Ausblick DFN-PKI

- Einrichtung ausgelagerter CAs für neue Anwender
- Erweiterung der Dienstleistung der DFN-PKI nach Bedarf von Anwendern
  - neue Funktionen, Grid-Umfeld, DFN-AAI, ...
- viele (auch nicht-technische) „Kleinigkeiten“
  - Anleitungen PKI-Nutzung, PKI-Tutorien, FAQs, Zertifikate unter Vista, „Extended Validation“, ...
- neues Redundanzkonzept (s. folgende Folie)
- Integration lokaler Strukturen (s. f. Folie)

Betrieb der DFN-PKI

- Hohe Verfügbarkeit ist wichtige Grundlage
  - z.B funktionieren manche Anwendungen ohne online CRL/OCSP-Prüfung nicht
- Redundanzkonzept im Aufbau
  - „Verdoppelung“ der betrieblichen Infrastruktur
  - Geräte an unterschiedlichen Standorten
  - Systeme werden im warm/hot Standby gefahren
- Verfügbarkeit des Dienstes DFN-PKI wird deutlich erhöht
  - Webschnittstellen, CRLs, OCSP, LDAP, ...

Lokale Strukturen

- Einige Anwender haben lokale PKI-Strukturen
  - Verknüpfung mit Chipkartenprojekten
  - Integration in Nutzerportale
  - Verwendung eigener CA-Software
- Ziel: Nutzung der Vorteile der DFN-PKI Global
  - Einbau einer „Software-Weiche“ erlaubt Integration in DFN-PKI Global unter Beibehaltung lokaler Technik und Prozesse
  - Gespräche mit SW-Herstellern und Anwendern
  - Lösung noch in 2007

Zusammenfassung

Zusammenfassung

- Auslagerung erfreut sich großer Zustimmung
- Mit der „Root im Browser“ wird die DFN-PKI funktional stark erweitert
- Diverse Erweiterungen in Vorbereitung, z.B
  - Integration lokaler PKI-Strukturen
  - Betrieb der DFN-PKI wird durch neues Redundanzkonzept weiter „professionalisiert“

✓ Kontakt:	pki@dfn.de
✓ Web:	www.pki.dfn.de