Zielsetzung

Vertrauenswürdige, rechtlich belastbare Kommunikation in Datennetzen durch Authentifizierung (nicht Autorisierung) für

- Webbasierte Selbstbedienungsfunktionalitäten (neue Dienste-Struktur an Hochschulen)
- Kommunikation zwischen Personen (z. B. E-Mail)
- Datenschutz durch Verschlüsselung

- ➢ Einrichtung einer landesweiten PKI für asymmetrische Verschlüsselungsverfahren (X.509-Norm) unter Beachtung der lokalen Autonomie der teilnehmenden Einrichtungen.
- ➢ Weiterentwicklung der lokalen CA-Strukturen.
- ➢ „PKI enabled Applications“.

Lösungsansatz PKI

Zentraler Indexserver bildet Index über lokale Veröffentlichungsinstanzen der einzelnen CA-Einrichtungen.

- Alle Zertifikatsinformationen zentral verfügbar
- Zentrales Informationsportal für den Endbenutzer
- Datenaustausch über standardisierte LDAP-Schnittstelle und damit
  -> max. Autonomie der teilnehmenden Einrichtungen
- Beliebig erweiterbar

Zusätzlich:
Zentraler OpenLDAP-Server als Veröffentlichungsinstanz und Referenz für lokale Zertifikatsverzeichnisdienste.

CA - problematischer IST-Zustand

- Eingebunden in die Hierarchie der DFN-PCA

Mangelnde Akzeptanz aufgrund von
- Unkomfortablen Benutzerschnittstellen
- Aufwendigen Identifizierungsverfahren
- Schlechter Unterstützung/Dokumentation durch Applikationen
- Fehlende Sensibilisierung für die Datenschutzproblematik

Daher bisher nur Testbetrieb bzw. kleine Teilnehmerzahlen.

Kritischer Faktor für den Erfolg des Projekts: Massenbetrieb der CAs

CA – SOLL-Zustand

Realisierung der Voraussetzungen für benutzerfreundlichen Massenbetrieb

- Evaluation und Einsatz benutzerfreundlicher CA-Software (OpenCA, WindowsCA)
- Vereinfachte Identifizierungsverfahren (z. B. Studentensek. als RA)
- Full Service, d. h. Erstellung und Bereitstellung der Zertifikate durch die CA auf Antrag des Teilnehmers oder automatisch durch Mitgliedschaft
- Lange Zertifikatslaufzeiten
- Geeignete Zertifikatsspeicher
- Bereitstellung von „Kochrezepten“ für die Erstellung von Zertifikaten für einen möglichst breiten Anwendungsbereich (Zertifikatserweiterungen, DN)

„PKI enabled Applications“

Unterstützung praxisrelevanter Anwendungsszenarien

- Webbasierte Portale, hier insbes. überregionale Authentisierung
- VPN-Einwahl in WLAN-Strukturen
- S/MIME-Dienste

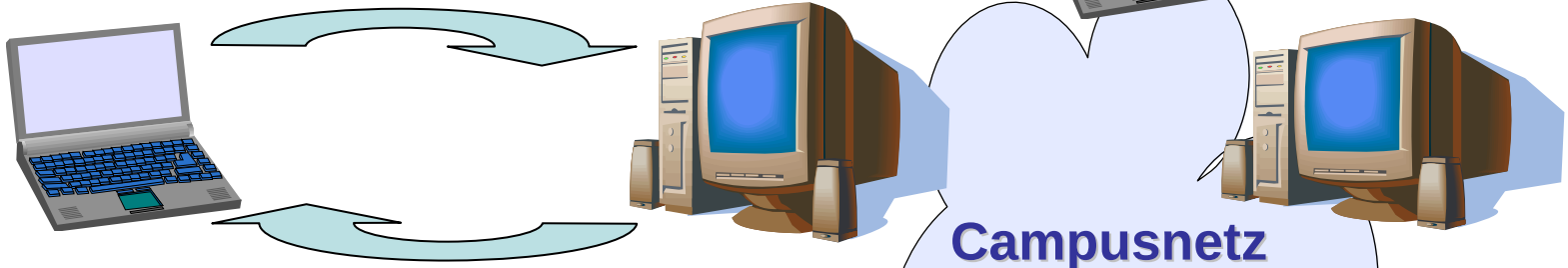
„PKI enabled Applications“

Teilprojekt Universität Konstanz/Projektphase I – „PKI enabled Network Services“

Authentisierung bei der VPN-Einwahl in WLAN-Strukturen mittels Zertifikat

- Basierend auf der X.509 Identity Certificate Norm
- Cisco IPsec VPN Concentrator 3000
- Umstellung von Preshared Keys auf Zertifikate

- Schritt 1: Authentifizierung des Concentrators gegen Client mittels Zertifikat
- Schritt 2: Ersetzung des „Xauth-Mechanismus“ durch Identity-Zertifikate



Console
Windows XP
VPN-Client (4.04E)

Campusnetz

Offline-CA (Notebook)
- Thinkpad, SuSE 9.1
- OpenCA SNAP 20040730 (module: ca, node)
- OpenSSL SNAP 20040813
- Apache 2.0.50
- MySQL (Suse)

RA Server (mixcoatl)
- Dell, SuSE 9.0
- OpenCA SNAP 20040730 (module: ra, node, ldap, pub)
- OpenSSL SNAP 20040813
- Apache (Suse)
- MySQL (Suse)

LDAP Server (Xaero)

SuSE (OpenLDAP)

Test-3030
Release. 4.17

Betrieb-3030
Release. 3.X

Architektur und Software-Releases Testumgebung

Meilensteine für Projektphase II/1

- Dokumentationen bzw. Vorgehensbeschreibungen als eine Art „Kochrezept“ als Resultat der Testszenarios und prototypischen Umsetzungen aus der Phase I.
- Definition einer Policy (CP/CPS) mit belastbaren Zertifikatsprofilen zum Einsatz in möglichst zahlreichen Applikationen (Standardanwendungen).
- Umsetzung der Änderungsvorgaben für die Zertifizierungsinstanzen in der Policy zur Erreichung der Benutzerakzeptanz und damit zur Realisierung des Massenbetriebs.
- Implementierung von Lösungen zur Gewährleistung von Datenschutz in den lokalen und zentralen Veröffentlichungsinstanzen.

Meilensteine für Projektphase II/2

- Tests und Evaluationen verfügbarer Standardanwendungen. Ziel ist eine möglichst breite Auswahl benutzerfreundlicher Systeme (Anwenderdoku.).
- Heranführung der beispielhaft realisierten Anwendungen aus dem Bereich der neueren Technologien an die Praxistauglichkeit. Dies betrifft die „PKI enabled Network Services“ und die „PKI enabled Web Applications“.
- Intensive Öffentlichkeitsarbeit um u. a. die Zusammenarbeit mit kommerziellen Software Anbietern aus dem Verwaltungsbereich weiter auszubauen.