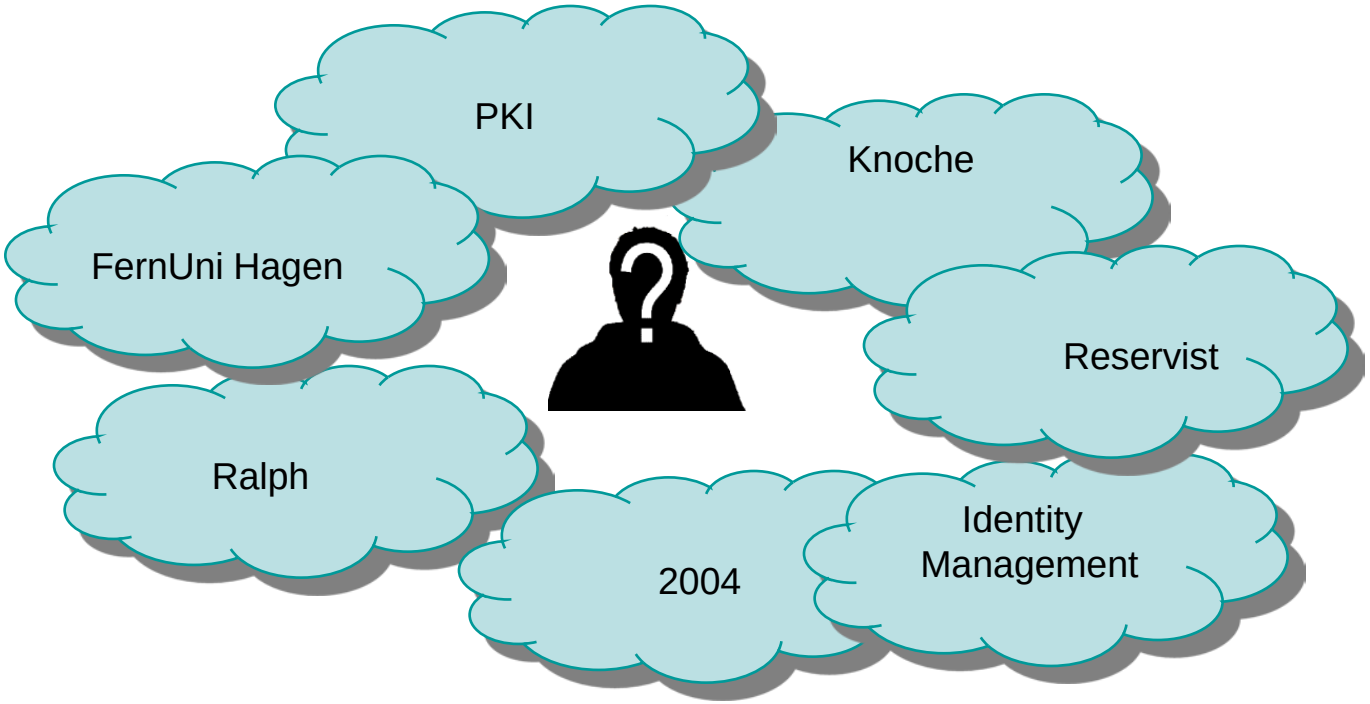
FernUniversität in Hagen

Mit Webtrust in den Browser

Ralph Knoche

ZMI


PKI
Knoche
FernUni Hagen
Reservist
Ralph
2004
Identity
Management

Der Bereich ID-Management…

- Administration der Identity Management Software BMC Control-SA

  → Installation / Konfigurationsarbeiten

- Weiterentwicklung des Identity Managements

  → Anbindung von neuen Datenquellen (z.B. Customer Relationship Management)

  → Ankopplung von neuen Zielsystemen (z.B. Active Directory)

Der Bereich PKI…

- (Kryptographische) Absicherung des Studienbetriebs und der Verwaltungseinrichtungen

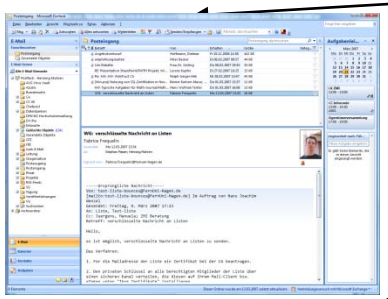
  → verschlüsselte / signierte E-Mail-Kommunikation
  → verschlüsselter / authentisierter Datenzugriff auf sensible Daten

- Certification Authority (CA): Betrieb eines Zertifikatsservers

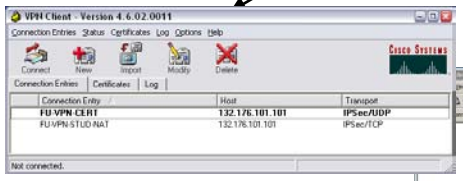
- PKI-Hosting Services (8 Kunden)

- Weiterentwicklung der kryptographischen Komponenten (Public Key Infrastruktur, PKI)

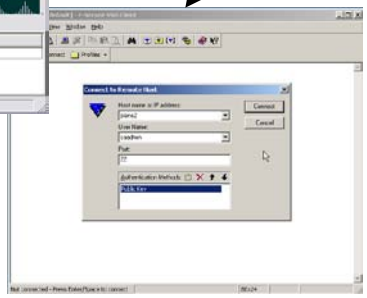
  → Programmierung von zertifikatsbasierten Webanwendungen
  → Anwendungsintegration von Zertifikaten



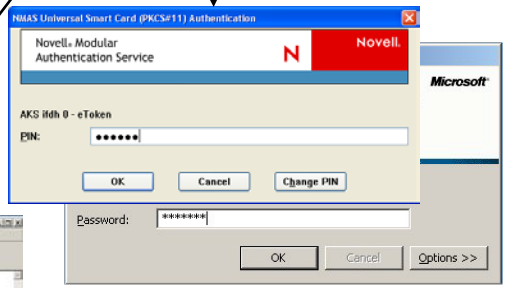
E-Mails



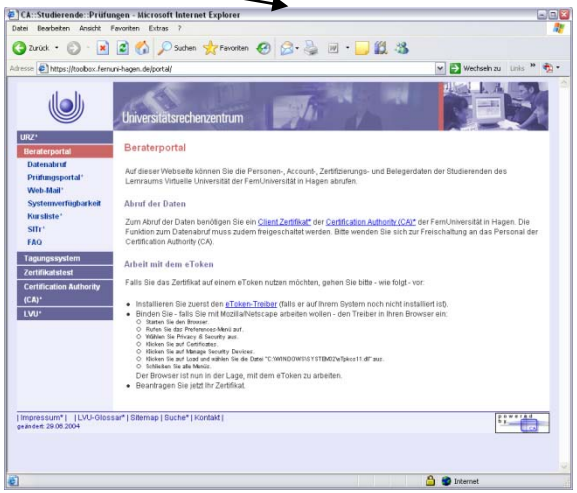
VPN



SSH



PC-/Netz-Login



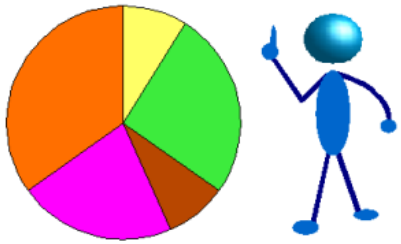
Eigene Anwendungen

Ein paar Statistiken:

Wir verwalten...

69.667 Accounts in Control-SA
56.508 davon sind Studierende
67.053 Zertifikate
34.353 davon sind gültig

(Stand 07.12.08)



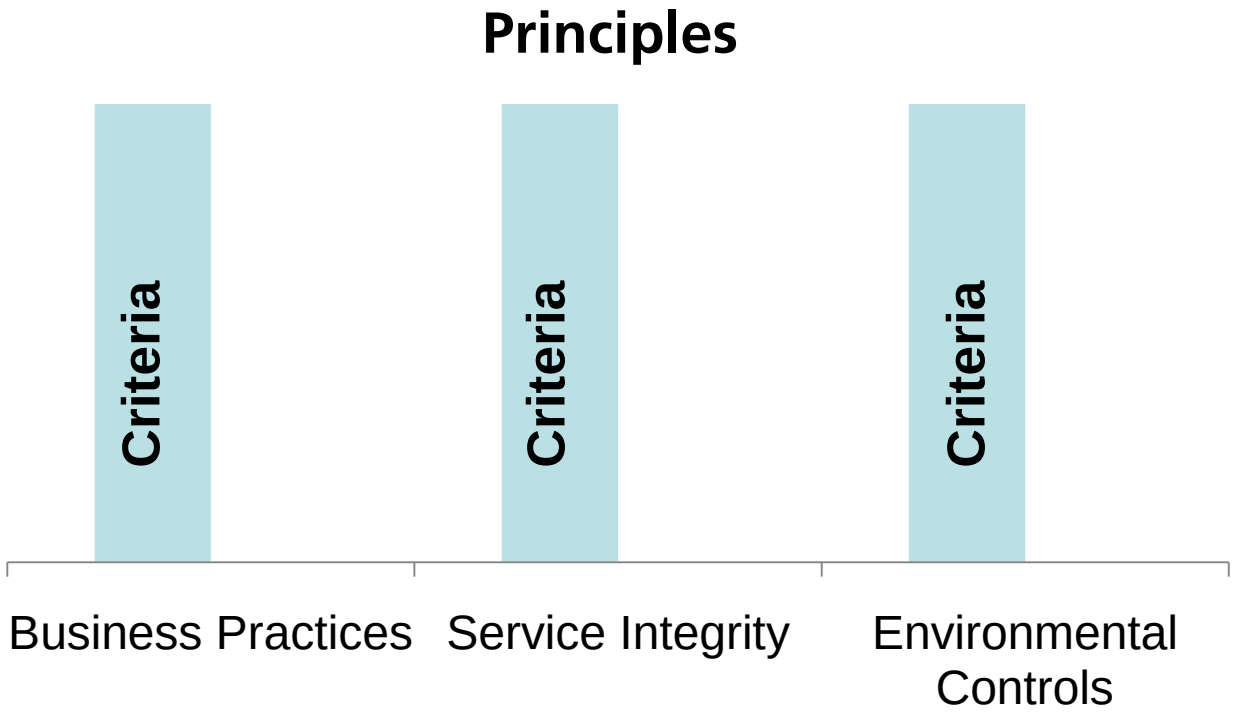
Das Webtrust Projekt

Problem: Das aktuelle Wurzelzertifikat ist nicht im Browser integriert!

- Wurzelzertifikat vom DFN-Verein unterschrieben (Basic Policy)
- DFN Global Policy nicht für die FernUni akzeptabel

=> Resultat: Studierende erhalten Fehlermeldung

- CA muss Webtrust zertifiziert sein
- AICPA (amerikanischen Vereinigung der Wirtschaftstreuhänder) & CICA (Kanadischem Pendant) ausgearbeitet
- Entwickelten Richtlinien für Webtrust-Prüfungen


Principles
Criteria
Criteria
Criteria
Business Practices
Service Integrity
Environmental Controls

Business Practices

*The certification authority discloses its key and **certificate life cycle management** business and information privacy practices and provides its services in accordance with its disclosed practices.*

Service Integrity

The certification authority maintains effective controls to provide reasonable assurance that:

- *Subscriber information was properly authenticated (for the **registration activities** performed by ABC-CA).*
- *The **integrity of keys** and certificates it manages is established and protected throughout their life cycles.*

Environmental Controls

The certification authority maintains effective controls to provide reasonable assurance that:

- *Subscriber and relying party information is restricted to **authorized individuals** and protected from uses not specified in the CA's business practices disclosure*
- *The continuity of key and certificate life cycle management operations is maintained;*
- ***CA systems development**, maintenance, and operation are properly*

Projektbeginn: 2. Quartal 2007

Projektablauf:

1. Ausschreibung
2. Vorlage von Dokumentationen
3. Vorprüfung
4. Erstellen weiterer Dokumentationen
5. Hauptprüfung

1. Tag	2. Tag	3. Tag	4. Tag	5. Tag
- Prüfung von **Aufbau- und Ablauforganisation** (Organigramme, Verfahren, Richtlinien, Arbeitsanweisungen, Vertretungsregeln) - **Review** von Auswahl und Eignung der Mitarbeiter - Schulungskonzept	- Disaster Recovery - **Business Continuity Planning** (Notfallszenarien, Notfalltests, Redundanz, Wiederherstellungs-zeiten, Ausfallzeit best. Systeme, Hochverfügbarkeits-maßnahmen, 24/7-Verträge Virtualisierung etc.) - **Begehung RZ/Serverräume** und Beurteilung der baulichen, umwelttechnischen und sonstigen physischen Sicherheitsmaßnahmen, **Zutrittsschutz** - Einsichtnahme in Backupmedien - Prüfung von Protokollen zur Datensicherung	- Prüfung des **logischen Zugangs** zu Daten und Programmen, **Zugriffsschutz** -Verfahren im Hinblick auf Erteilung, Änderung und Löschung von Benutzerzugängen und Berechtigungen - Prüfung von **Zertifikatsmanagement** (laut CP und CPS)	- **Programmentwicklung** und Beschaffung (Ablauf, Tests, Freigaben, Dokumentation) - **Änderungsmanagement** (Antrags- und Genehmigungsverfahren, Freigaben, Testsysteme und Tests, Migrationen) - **Jobs und Schnittstellen** (Dokumentation, regelmäßige Tätigkeiten, Sicherstellung von Vollständigkeit und Richtigkeit der Datenübertragung bei Schnittstellen) - **Problemmanagement** in Bezug auf Systeme (Monitoring, Auswertung und Analyse, Problembehebung, Verantwortlichkeiten und Tracking, Fehlerdatenbank)	- Prüfung in der Woche offen gebliebener Punkte - Besprechung der ersten Ergebnisse und des weiteren Verlaufs der Zertifizierung

Vorprüfung Juni 2008

Ergebnis: Erster Prüfbericht

----- snip -----

Asset Management dokumentieren: Klassifikation der Geschäftswerte (Bewertung finanziell und existenziell)

Risikomanagement dokumentieren: Assets müssen auf Schwachstellen untersucht werden => Individueller Risikowert

CP & CPS Ergänzungen

Root Key Ceremony

HSM Card Set personalisieren

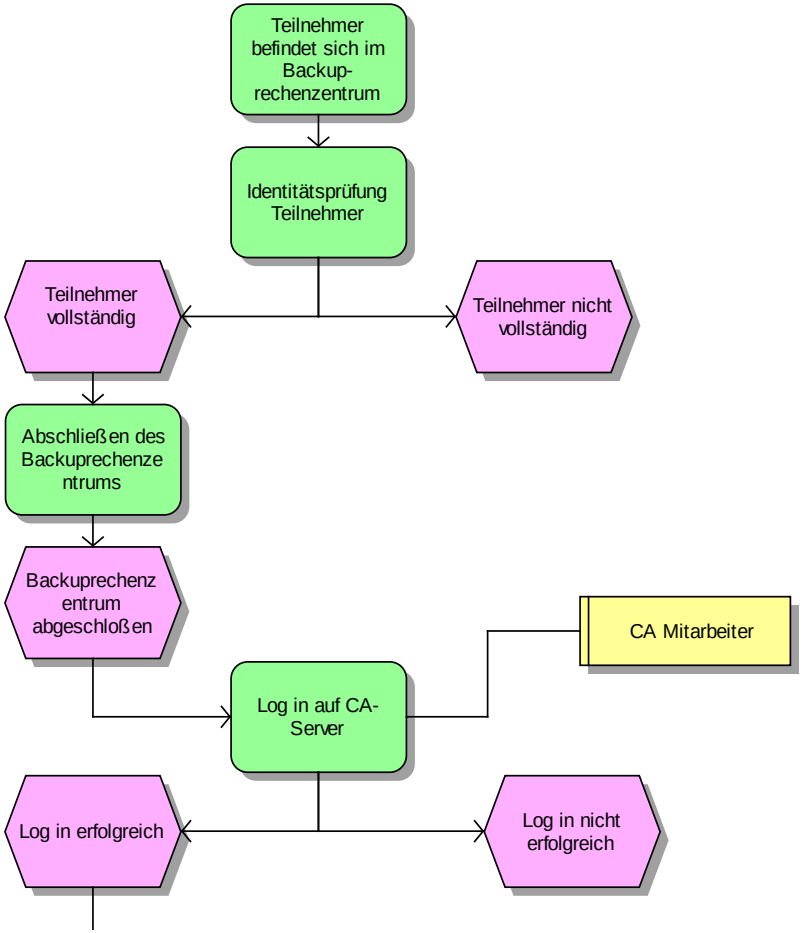
Fehlender Timeout auf CA-Server

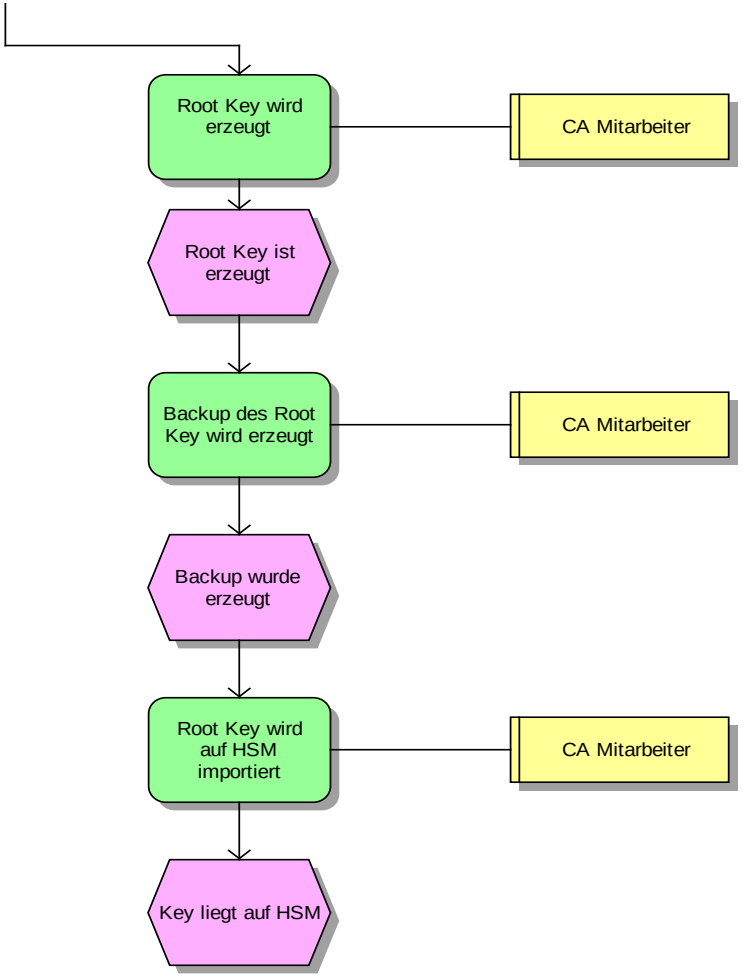
Richtlinien: Datenträgerentsorgung, Schlüsselarchivierung, Schlüsselzerstörung
Umgang mit Dritten und Ermittlungsbehörden, Review Prozess…

----- snip -----

Hauptprüfung: Januar 2009

- Ähnlich der Vorprüfung
- Zusätzlich Root Key Ceremony


Teilnehmer befindet sich im Backup-rechenzentrum
Identitätsprüfung Teilnehmer
Teilnehmer vollständig
Teilnehmer nicht vollständig
Abschließen des Backuprechenzentrums
Backuprechenzentrum abgeschloßen
CA Mitarbeiter
Log in auf CA-Server
Log in erfolgreich
Log in nicht erfolgreich


Root Key wird erzeugt
CA Mitarbeiter
Root Key ist erzeugt
Backup des Root Key wird erzeugt
CA Mitarbeiter
Backup wurde erzeugt
Root Key wird auf HSM importiert
CA Mitarbeiter
Key liegt auf HSM

Ergebnis: Bestanden

- Nachbesserungen nur im Detail
- Internes KPMG Audit
- Bericht nach webtrust.org

=> Webtrust Siegel

Browser Verhandlungen

Root Certificate Programm:

- Root-Zertifikat (Attributierung, Schlüssellänge …)
- Prüfbericht
- Individuelle Prüfung
- Automatische Verteilung in Browser
- Wintersemester 2009/2010

Fazit

- Erste Uni weltweit die MS Browserintegration anstrebt
- Enormer Aufwand um eine vertrauenswürdige Zertifizierungsstelle aufzusetzen
- Aufwand gerechtfertigt um Online-Sicherheit zu gewährleisten

Wo wäre die Sicherheit, wenn jeder x-beliebige eine eigene vertrauenswürdige Zertifizierungsstelle aufsetzten kann?

FernUniversität in Hagen

Q & A ?

Ralph Knoche
Ralph.Knoche@fernuni-hagen.de
+49 (2331) 987 – 2829
caadmin@fernuni-hagen.de

ZMI