DFN-AAI

Sicherheitsaspekte und rechtliche Fragen

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

Gliederung

- **Sicherheitsaspekte**
- Rechtliche Fragen

Sicherheit

- Die Sicherheit in der DFN-AAI ist eine entscheidende Voraussetzung für deren Nutzung
- Sicherheit umfasst mehrere Komponenten
  - Vertraulichkeit
  - Integrität
  - Authentizität
  - Verfügbarkeit
- DFN-PKI hat sich als wichtige Basis etabliert

Kleiner Exkurs: DFN-PKI (1)

- DFN-PKI
  - Infrastruktur für digitale Zertifikate im DFN
  - DFN betreibt zentrale Komponenten, wodurch der lokale Aufwand stark reduziert wird
  - Konzept der Auslagerung erlaubt auch „kleinen“ Einrichtungen die Nutzung von Zertifikaten
  - starkes Sicherheitsniveau in der DFN-PKI, z.B. durch persönliche Identifizierung
  - hohes betriebliches Sicherheitsniveau durch jährliche Audits
  - ohne zusätzliches Entgelt nutzbar

Kleiner Exkurs: DFN-PKI (2)

- Erfahrungen nach 2,5 Jahren Regelbetrieb
  - mehr als 200 Einrichtungen nutzen bereits die Angebote der DFN-PKI
  - jede Woche kommt ca. eine Einrichtung hinzu
  - breites Spektrum an Anwendern, von kleinen Einrichtungen, die bisher keine PKI hatten, bis zu großen Einrichtungen mit viel PKI-Erfahrung
  - Dienstangebot der DFN-PKI „passt“

Sicherheit: Vertraulichkeit

DFN Deutsches Forschungsnetz

- Wie ist gewährleistet, dass die in der DFN-AAI übermittelten Daten nicht durch unbefugte Dritte ausgespäht werden?
- Lösung
  - Verwendung digitaler Zertifikate der DFN-PKI
  - Daten werden bei der Übermittlung automatisch verschlüsselt
  - unbefugtes Entschlüsseln praktisch nicht möglich
  - starke Policy der DFN-PKI ist Basis (z.B. persönliche Identifizierung)

Sicherheit: Integrität

- Wie ist gewährleistet, dass die in der DFN-AAI übermittelten Daten nicht unbemerkt verändert werden?
- Lösung
  - Verwendung digitaler Zertifikate der DFN-PKI
  - Daten werden bei der Übermittlung automatisch mit Prüfsummen versehen
  - unbefugte Veränderung von Daten wird automatisch erkannt

Sicherheit: Authentizität

- Wie ist gewährleistet, dass die in der DFN-AAI beteiligten Instanzen (Personen, Server) wirklich die sind, die sie vorgeben zu sein?
- Lösung
  - Verwendung digitaler Zertifikate der DFN-PKI
  - digitales Zertifikat als „elektronischer Ausweis“
  - Server müssen digitales Zertifikat haben und sind dadurch eindeutig und nachvollziehbar ausgewiesen
  - Personen können - je nach Sicherheitsbedarf - ein digitales Zertifikat verwenden

Sicherheit: Verfügbarkeit

- Wie ist gewährleistet, dass die DFN-AAI hoch verfügbar zur Verfügung steht?
- Lösung
  - Redundanzkonzept für technische Komponenten der DFN-PKI und der DFN-AAI
  - betriebliche Prozesse auf hohe Verfügbarkeit ausgelegt

Gliederung

- Sicherheitsaspekte
- **Rechtliche Fragen**

Recht: verschiedene Blickwinkel

- Rechtliche Sicht aus verschiedenen Blickwinkeln
  - Datenschutz
  - Datensicherheit
  - Personalrat
  - Haftung
  - Telemediengesetz
  - Signaturgesetz

Recht: Datenschutz

- Authentifizierung durch die Hochschule
  - Vorteil: Anonymität gegenüber Anbieter
  - Voraussetzung: Vorhandenes IdM
    - Datenschutzrechtliche Fragen bei Errichtung
    - Landesrechtliche Besonderheiten
  - Problem: Grundsatz der Zweckbindung
    - Authentifizierung ist ggf. zweckändernde Nutzung
      - Erfordert gesetzliche Erlaubnis oder Einwilligung

Recht: Einwilligung

– **Lösung:** Elektronische Einwilligung auf der Startseite:

Beispiel:

Mit der Verwendung der zu meiner elektronischen Hochschulidentität gespeicherten Daten zur Prüfung der Berechtigung zur Nutzung von mir ausgewählter Dienste bin ich einverstanden.

User ID …

Passwort …

Recht: Datensicherheit

- Vertraulichkeit durch Verschlüsselung
  - § 9 BDSG und vglb. Normen LDSGe
    - Technische und organisatorische Maßnahmen
  - Schutz der Übermittelten Inhalte vor unautorisierten Zugriffen

Recht: Personalrat

- Mitarbeiter als Nutzer
  - Authentifizierung in der Einrichtung ermöglicht festzustellen, welcher Nutzer auf welchen Anbieter zugegriffen hat (nicht Inhalte)
- Technische Leistungs- und Verhaltenskontrolle
  - z.B. § 72 Abs. 3 Nr. 2 LPersVG NRW
  - Objektive Eignung hierzu ausreichend
- Personalrat sollte beteiligt werden!

Recht: Haftung

- Missbräuchliche Nutzung
  - Weil z.B. Identität nicht korrekt gepflegt (kein neues Problem)
  - DFN - Anbieter: Haftungsbeschränkungen geregelt
    - DFN steht für die korrekte **Übermittlung**
    - DFN wirkt darauf hin, dass IdM von Hochschulen gepflegt ist
- Aufgabe Hochschulen
  - Hochschule - Anbieter: Lizenzvereinbarungen prüfen!
  - Gewährleistung ordentlicher Pflege IdM

- **Unter dem Strich**: Mit AAI wird Haftungsrisiko ggü. heutigem Stand aber durch Einbindung IdM eher geringer!

Recht: Haftung

- Nutzer kann Angebot nicht nutzen, weil IdM nicht erreichbar oder nicht korrekt ist
  - Beispiel: Anmeldung zur Prüfung kann nicht erfolgen, weil DFN-AAI nicht verfügbar

  -> Frist verstreicht
- Haftungsbeschränkungen
- Alternativen
- Kulanz
  - z.B. durch Fristverlängerung

Recht: Telemediengesetz (TMG)

- Für Hochschulen relevant, wenn sie selbst Anbieter sind:
  - Informationspflichten §§ 4 – 6 TMG
  - Verantwortlichkeit §§ 7 – 10 TMG
  - Datenschutz §§ 11 – 15 TMG
- Wird hier nicht weiter behandelt

Recht: Signaturgesetz

- DFN-PKI: Fortgeschrittene Signatur
  - erfüllt nicht die Erfordernisse der Schriftform i.S.v. § 126a BGB und § 3a VwVfG

- Hierauf kommt es bei Server- und Einzelzertifikaten auch nicht an
  - Geeignetheit zur Herstellung eines Vertrauensverhältnisses
  - DFN-PKI: Starke Policy und **persönliche Identifizierung**

Fragen ...?