DFN-AAI Sicherheitsanforderungen und neue Attribute

ZKI-AK Verzeichnisdienste,

Hamburg, 11.-12.10.2007

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management

Agenda Überblick

- Gedanken zu Sicherheitsanforderungen
- Gedanken zur Erweiterung der Attribute

DAASI International
Directory Applications for Advanced Security and Information Management

Relevante Fragenbereiche

- Gibt es überhaupt eine geeignete zentrale Benutzerverwaltung
  - über die Authentifizierungsprozesse abgewickelt werden können
  - in der zum Zwecke der Autorisierung föderationsrelevante Informationen über die Benutzer gepflegt werden.
- Welche relevanten Attribute werden vorgehalten
  - Zur Basisrolle (Studierender, Dozent, Angestellter, Mitglied, etc.)
  - Zugehörigkeit zu einzelnen Organisationseinheiten oder Fakultäten
  - Eindeutige Ids, sowie Kontaktdaten

DAASI International
Directory Applications for Advanced Security and Information Management

Relevante Fragenbereiche

- Aktualität der Daten
  - Ob Account frühzeitig nach Eintritt in die Hochschule (ob als Studierender oder Mitarbeiter) angelegt werden
  - ob Accounts bzw. föderationsspezifische Attributinformationen auch zeitnah nach dem Austritt aus der Hochschule deaktiviert bzw. gelöscht oder geändert werden (z.B. die Basisrolle von „student“ zu „alumn“ ändern).

DAASI International
Directory Applications for Advanced Security and Information Management

Relevante Fragenbereiche

- Password-Policy
  - Je einfacher ein Passwort zu erraten ist (z.B. mittels eines Dictionary-Attack), desto eher ist die Möglichkeit gegeben, dass sich ein Unberechtigter über den Account eines Benutzers authentifiziert.
- Passwort-Sicherheit
  - ob das Passwort nur über verschlüsselte Verbindungen (z.B. SSL bzw. TLS) abgefragt wird und deshalb nicht von einem Unberechtigten abgehört werden kann.
- Alternativ zu LoginID und Passwort würden sich User-Zer-tifikate im Rahmen einer X.509-basierten Publick Key Infrastructure (PKI) als noch stärkerer Authentifizierungsmechanismus eignen.
  - Vorhandensein einer sicheren PKI in den einzelnen Hochschulen

Sicherheitsanforderungen: Minimal

1) Alle im System vorhandenen elektronischen Prozesse (IdP, SP und WAYF) müssen sich über ein X.509-Zertifikat authentifizieren. Nur so kann verhindert werden, dass Föderationsfremde, eigene Dienste (IdPs oder Sps) einbinden können.
2) Um die X.509-Zertifikate überprüfen zu können, müssen sie alle innerhalb derselben PKI erstellt worden sein, d.h. alle Zertifizierungsstellen (CAs) müssen unterhalb derselben Root-CA liegen. Hier kommt im Wesentlichen die Root-PCA des DFN in Betracht.
3) Alle Datenströme, die innerhalb der Föderation für Authentifizierungs- und Autorisierungszwecke verschickt werden, müssen verschlüsselt übertragen werden, so dass es nicht möglich ist, Passwörter abzuhören, oder Attributinformation zu manipulieren.

DAASI International
Directory Applications for Advanced Security and Information Management

Sicherheitsanforderungen: Passwörter

1) Alle Passwörter, die für die Authentifizierung innerhalb der Föderation verwendet werden, dürfen nie unverschlüsselt über das Netz geschickt werden, damit sie nicht von Unberechtigten abgehört werden können. Dies bedeutet, dass alle Systeme, die solche Passwörter abfragen, eine unverschlüsselte Abfrage verbieten müssen.
2) Alle Passwörter müssen einer Passwort-Policy unterzogen werden, sodass einfach zu erratende Passwörter (wie z.B. „maria“) nicht mehr verwendet werden dürfen. Als Mindestanforderung sollte ein Passwort mindestens 7 Zeichen lang sein und mindestens einen Großbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.
3) Alle Benutzer sollten auf die Passwortproblematik hingewiesen werden, insbesondere, darauf dass

Sicherheitsanforderungen: Attribute

1) Alle teilnehmenden Hochschulen sollten eine Benutzerverwaltung haben, die zuverlässig und zeitnah aktuelle Attribute über die Benutzer vorhält, sodass wirklich nur noch Berechtigte Dienste der Föderation in Anspruch nehmen können. Hierbei bedeutet „zeitnah“, dass innerhalb von 2 Wochen ausgetretene Mitarbeiter bzw. exmatrikulierte Studierende ihre Berechtigung auf Föderationsdienste verlieren.
2) Die Attribute sollten nicht nur Basisrollen (Studierender, Mitarbeiter, Lehrkörper) enthalten, sondern auch die Zugehörigkeit zu einer bestimmten Einrichtung (Mitarbeiter) bzw. Fakultät (Studierende), sowie, über ein mit eduPersonEntitlement kompatibles Attribut, bestimmte spezifische Berechtigung.
3) Die Aktualität der Attribute muss innerhalb von zwei Wochen den Gegebenheiten entsprechen.

Sicherheitsanforderungen: PKI

1) Immer noch können Passwörter Unberechtigten in die Hände fallen, wenn Benutzer nicht die notwendige Vorsicht walten lassen. Deshalb ist anzustreben, Authentifizierung mittels Benutzerzertifikaten durchzuführen, die auf einem Hardware-Token gespeichert sind. Hierbei muss ein Benutzer sowohl Zugang zu seinem Zertifikat haben, als auch das Wissen über das Passwort, welches den dazugehörigen privaten Schlüssel schützt

DAASI International
Directory Applications for Advanced Security and Information Management

Datenschutzanforderungen

- Alle Datenflüsse mit personenbezogenen Daten müssen dokumentiert werden, insbesondere welche personenbezogenen Daten von Benutzern von der Heimatorganisation an andere Organisationen innerhalb der Föderation weitergegeben werden. Diese Dokumentation muss für jeden Benutzer einsehbar sein.
- Der Benutzer muss spezifizieren können, ob und welche seiner personenbezogenen Daten vom IdP der Heimatorganisation innerhalb der Föderation weitergegeben werden. Es versteht sich von selbst, dass ein Benutzer, der die Weitergabe jeglicher Daten verbietet, keine oder nur wenige Föderationsdienste in Anspruch nehmen kann.
- AAI-Prozesse innerhalb der Föderation dürfen gelogt werden. Allerdings ist darauf zu achten, dass die Logfiles entsprechend der jeweils gültigen Datenschutzgesetz-gebung nach einer

DFN-AAI Attribute

- Einige der bisher definierten Attribute in Text Version 0.8 sind diskussionswürdig:
  - eduPersonPrimaryAffiliation
  - eduPersonPrimaryOrgUnitDn
- Für Autorisierungszwecke sind die Multivalue-Varianten wesentlich besser geeignet
- eduPersonOrgUnitDn macht nur Sinn, wenn ein Organigramm im LDAP abgebildet ist.
- eduPersonTargetedId sollte im Text besser erklärt werden

DAASI International
Directory Applications for Advanced Security and Information Management

DFN-AAI Attribute

- Neue Anforderungen an DFN-AAI-Attributempfehlungen aus eLearning-Kreisen (VHB-AAI):
- Folgende optionalen Attribute „unmittelbar relevant und auch für andere Anwendungen interessant“:
  - Geschlecht, Geburtsdatum, Matrikelnummer, Studiengang, akademischer Titel
  - Personalnummer, Geburtsort, Studienabschlussart/Fachsemester/Lernniveau/ Sprachniveau
- Für die meisten dieser Anforderungen gibt es bereits Spezifikationen (aus inetOrgPerson und hisPerson bzw. schacPerson
- Problematisch sind Studiengang und -abschluss: Wir benötigen eine entsprechende Ontologie der Studienfächer in Deutschland

DAASI International
Directory Applications for Advanced Security and Information Management

DFN-AAI Attribute

- Neue Anforderungen an DFN-AAI-Attributempfehlungen aus dem Grid-Bereich (D-Grid IVOM) :
  - Um sicherzustellen, dass ein Zertifikat zu der Person gehört, die sich gerade beim IdP authentifiziert hat, sollte der IdP auch das Zertifikats-SubjectDN an den SP weitergeben können

DAASI International
Directory Applications for Advanced Security and Information Management

DFN-AAI Attribute

- **Mein Vorschlag:**
  - **Attribut-Text sollte in einer neuen Version 0.9 Klarstellungen zu TargetedId und Primary-Attributen enthalten**
  - **Für einzelne Bereiche (eLearning, Grid) sollten Zusatztexte entwickelt werden, die als Empfehlung innerhalb der DFN-AAI gelten sollen**
    - **Allerdings sollten diese Texte die Datenschutzrechtliche Relevanz (Geburtstag, etc.) deutlich machen.**
    - **Eine Föderation ist kein Organisationsübergreifendes IdM!**

DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit!

- **Kontakt und weitere Informationen:**
  - **DAASI International GmbH**
    Wilhelmstr. 106
    D-72074 Tübingen

    Web: http://www.daasi.de
    Mail: info@daasi.de

  - **Bei späteren Fragen zum Kurs:**
    Mail: peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management