Die deutschlandweite Föderation DFN-AAI als Grundlage für die verteilte Authentifizierung und Autorisierung

Universitätsbibliothek Freiburg, DFN-Verein Berlin, Version 1.0, 1.7.2008

Zweck einer Föderation

Zweck

Die Infrastruktur zur verteilten Authentifizierung und Autorisierung, die in den vergangenen Jahren aufgebaut wurde[1], basiert auf Shibboleth[2] und damit auf einem föderativen Ansatz: Die Heimateinrichtungen authentifizieren ihre Benutzer und stellen Dienstanbietern Informationen über die Benutzer zur Verfügung, die es den Dienstanbietern ermöglichen zu entscheiden, ob die Benutzer auf eine geschützte Ressource zugreifen dürfen oder nicht. Um das hierfür notwendige Vertrauensverhältnis und einen organisatorischen Rahmen für die Austausch der notwendigen Informationen zu schaffen, schließen Heimateinrichtungen und Dienstanbieter sich in landesweiten Föderationen zusammen[3].

Aufgaben der DFN-AAI

Vorgabe von Richtlinien

Richtlinien

Die Definition von Richtlinien (Policies) und die Überwachung ihrer Einhaltung sind die wichtigsten Aufgaben der DFN-AAI. Die Richtlinen schaffen den Rahmen für das Vertrauensverhältnis zwischen den Mitgliedern der DFN-AAI und ermöglichen der DFN-AAI ein geschlossenes Auftreten gegenüber potentiellen neuen Partnern. Es wurden insbesondere technische und organisatorische Mindestanforderungen für Authentifizierungssysteme und Standards für den Austausch von Informationen über die Benutzer festgelegt.

Verwaltung von Metadaten und Betrieb des Lokalisierungsdienstes

Metadaten, Lokalisierungsdienst

Die DFN-AAI verwaltet alle für ein Shibboleth basiertes System notwendigen Informationen über die Mitglieder (Adressen der Authentifizierungs- und Autorisierungsserver, verwendete Zertifikate) in einem zentralen Verzeichnis und stellt diese ihren Mitgliedern zur Verfügung. Auf dem Verzeichnis basiert auch der zentrale Lokalisierungsdienst (Discovery Service), über den die Benutzer ihre Heimateinrichtung auswählen können. Der Betrieb dieses Dienstes wird daher auch von der DFN-AAI übernommen.

Betrieb einer Zertifizierungsstelle

Zertifizierung

Um die Sicherheit und Authentizität der zwischen Benutzern, Dienstanbietern und Heimateinrichtungen ausgetauschten Daten zu gewährleisten, wird die Kommunikation mit Zertifikaten abgesichert. Im Prinzip können hierfür beliebige Zertifikate verwendet werden, da kommerzielle Zertifikate aber hohe Kosten verursachen können und selbst signierte Zertifikate die Schaffung eines Vertrauensverhältnisses erschweren, betreibt das DFN eine Zertifizierungsstelle (DFN-CERT) und bietet ihren Mitgliedern damit eine möglichst kostenfreie Zertifizierung an. Welche Zertifikate bzw. Zertifizierungsstellen zulässig sind, legt die DFN-AAI in ihren Richtlinien fest.

Technischer Support

Support

Die DFN-AAI unterstützt ihre Mitglieder auch bei der Installation und Konfiguration der notwendigen Softwarekomponenten (hotline@aai.dfn.de).

[1] siehe Management-Report
[2] siehe http://shibboleth.internet2.edu/
[3] siehe http://shibboleth.internet2.edu/related-links.html

Aufgaben des AAR-Projektes

Aufbau

Das Projekt AAR wird in Zusammenarbeit mit dem DFN die notwendigen Grundlagen für den Aufbau einer Infrastruktur zur verteilten Authentifizierung und Autorisierung in Deutschland schaffen und den insbesondere in der Einführungsphase des neuen Systems notwendigen technischen Support leisten. Auch die Verwaltung der Metadaten und der Betrieb des Lokalisierungsdienstes können bis zum Ende der Projektlaufzeit Mitte 2008 von den Projektpartnern übernommen werden. Im Rahmen des Projekts wurden bereits Vorschläge für Richtlinien erarbeitet. Die Durchsetzung der Richtlinien und der dauerhafte Betrieb der notwendigen Dienste erfordern aber den Aufbau einer deutschlandweiten Föderation (DFN-AAI) in einem geeigneten organisatorischen und rechtlichen Rahmen.

Kontaktadressen

Universitätsbibliothek Freiburg
Werthmannplatz 2
79098 Freiburg

Ansprechpartner:
Ato Ruppert, Bernd Oberknapp