

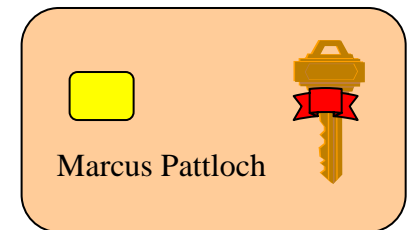
Einsatz von Zertifikaten im Bereich der DFN-AAI

6. Shibboleth Workshop
- Frankfurt, 8. Mai 2008 -

Marcus Pattloch (DFN-Verein)

pki@dfn.de

- Zertifikat = persönlicher Ausweis im Internet
- jeder, der ein Zertifikat besitzt, kann im Netz authentisch auftreten
- jeder, dem ich im Netz mein Zertifikat zeige, kann sicher sein, wer ich bin
- z.B. in Form einer „Chipkarte“
(aber: nicht jede Chipkarte enthält ein Zertifikat)



- Zertifikate ersetzen Passwörter
 - grundsätzlich EIN Zertifikat pro Person (jeder hat auch nur einen Ausweis)
 - Schluss mit vielen verschiedenen Passwörtern (die man sich doch nicht merken kann)
 - Sicherheit von Zertifikaten grundsätzlich deutlich höher als von Passwörtern
 - einfache Nutzung der Zertifikate möglich (weitgehend transparent)

- Signatur
 - Signieren von .pdf Dokumenten
 - Signieren von E-Mails
- Authentisierung
 - Zugriff auf geschützte Webbereiche
 - Anmelden an Rechnern oder Datenbanken (ssh, IPsec)
 - Server weisen sich aus (SSL, https)
- Vertraulichkeit
 - Verschlüsseln von Dokumenten und E-Mails

- Zertifikate der DFN-PKI werden im Betrieb der DFN-AAI an mehreren Stellen eingesetzt
- Einsatzzwecke von Zertifikaten in DFN-AAI
 - beim Betrieb von Shibboleth
 - zur Authentifizierung der Webserver, die die Dienste anbieten
 - zur Authentifizierung von Nutzern

- Zertifikate beim Identity Provider und beim Service Provider
 - Beide Instanzen müssen sich bei der Shibboleth-internen Kommunikation gegenseitig „elektronisch ausweisen“
- Zertifikate zum Signieren der Metadaten
 - Metadaten enthalten wichtige betriebliche Daten über die Föderation
 - Authentizität der Metadaten erforderlich

- In der DFN-AAI gibt es folgende Webserver
 - Service Provider: stellt seine Informationen den Nutzern zur Verfügung
 - Identity Provider: stellt die Formulare zur Anmeldung von Nutzern zur Verfügung
 - WAYF-Server: stellt Nutzern ein Formular zur Auswahl ihrer Heimateinrichtung zur Verfügung
- Alle Webserver müssen Zertifikate zur Authentifizierung verwenden

- Derzeit verwenden Nutzer zur Authentifizierung meistens Username/Password
- Alternativ kann die Authentifizierung auch per Nutzerzertifikat erfolgen
- Zukünftig kann auf Basis der Stärke der Authentifizierung die Nutzung von Diensten geregelt werden, z.B.
 - Zugriff auf „kritische Dienste“ nur bei starker (zertifikatbasierter) Authentifizierung



DFN-AAI Zertifikate Home / DFN-AAI Zertifikate

DFN-AAI Zertifikate

Wenn Sie am Dienst DFN-AAI teilnehmen - egal ob als Identity-Provider oder Service-Provider - benötigen Sie Zertifikate. Um diese Zertifikate zu erhalten, unterstützt Sie der DFN-Verein mit dem Dienst DFN-PKI, an dem bereits viele DFN-Anwender teilnehmen.

Wählen Sie bitte aus einer der folgenden Möglichkeiten aus:

- [Sie haben bereits ein Zertifikat der DFN-PKI](#)
- [Sie haben ein Zertifikat aus einer anderen Zertifizierungshierarchie](#)
- [Sie haben noch kein Zertifikat \(und möchten sich ein Zertifikat beschaffen\)](#)

Weitere Informationen zur DFN-PKI finden Sie über die linke Navigationsleiste.

Für alle Fragen zu Zertifikaten in der DFN-AAI schicken Sie bitte eine E-Mail an pki@dfn.de.

Weiterführende Links:

- [Überblick DFN-PKI](#)
- [DFN-AAI](#)
- [DFN-AAI Portal](#)

Verantwortlich: [DFN-PKI-Team](#)

 [Druckansicht](#) erstellt am: 06.12.2007 aktualisiert am: 07.12.2007

Suche:

[Termine](#)
[Sitemap](#)
[Disclaimer](#)
[Impressum](#)

Überblick DFN-PKI
CA - Auslagerung
CA - Selbst betrieben
Grid Zertifikate
DFN-AAI Zertifikate
 DFN-PKI Zertifikat
 Anderes Zertifikat
 Zertifikat beschaffen
Einzelzertifikate
FAQ DFN-PKI
Policies
Wurzelzertifikate
Sperrlisten (CRL)
Teilnehmer der DFN-PKI
Test-PKI Zugang
PGP-Zertifikate
Zeitstempeldienst
Kontakt und Support
DFN-Verein

www.pki.dfn.de/aai



https://www.pki.dfn.de/index.php?id=faqpki-aa&L=0

DFN
Deutsches
Forschungsnetz

FAQ DFN-AAI

Home / FAQ DFN-PKI / FAQ DFN-AAI

Überblick DFN-PKI
CA - Auslagerung
CA - Selbst betrieben
Grid Zertifikate
DFN-AAI Zertifikate
Einzelzertifikate
FAQ DFN-PKI
FAQ Allgemein
FAQ Mozilla
FAQ Windows/IE
FAQ Weitere Software
FAQ DFN-AAI
Policies
Wurzelzertifikate
Sperrlisten (CRL)
Teilnehmer der DFN-PKI
Test-PKI Zugang
PGP-Zertifikate
Zeitstempeldienst
Kontakt und Support
DFN-Verein

FAQ DFN-AAI

Fragen und Antworten zu Zertifikaten in der DFN-AAI

1. [Wofür werden Zertifikate in der DFN-AAI eingesetzt?](#)
2. [Welche Anforderungen werden an Zertifikate in der DFN-AAI gestellt?](#)
3. [Welche Zertifikate können in der DFN-AAI verwendet werden?](#)

1. Wofür werden Zertifikate in der DFN-AAI eingesetzt?

In der DFN-AAI kommen Zertifikate an verschiedenen Stellen zum Einsatz:

- ♦ **Betrieb von Shibboleth:** Zertifikate *müssen* für die gegenseitige Authentifizierung von Identity Providern und Service Providern sowie für die Signatur der Metadaten, die wichtige betriebliche Daten über die DFN-AAI enthalten, eingesetzt werden.
- ♦ **Authentifizierung der Webserver:** Alle Webserver der Service Provider und Identity Provider in der DFN-AAI *müssen* zur Authentifizierung Zertifikate verwenden.
- ♦ **Authentifizierung der Nutzer:** Derzeit verwenden Nutzer zur Authentifizierung meistens Username/Password. Alternativ *kann* die Authentifizierung auch per Nutzerzertifikat erfolgen. So kann zukünftig auf Basis der Stärke der Authentifizierung die Nutzung von Diensten geregelt werden, z.B. der Zugriff auf „kritische Dienste“ nur bei starker, zertifikatbasierter Authentifizierung.

2. Welche Anforderungen werden an Zertifikate in der DFN-AAI gestellt?

Zertifikate für die DFN-AAI müssen sich an der Zertifizierungsrichtlinie (CP) der DFN-PKI für die [Sicherheitsniveaus Global, Classic](#) oder [Grid](#) orientieren.

Nach Abschnitt 3.2.3 dieser Zertifizierungsrichtlinie bedeutet das bei Nutzerzertifikaten insbesondere, dass die Identitätsprüfung persönlich anhand eines amtlichen Ausweispapiers mit Lichtbild erfolgen muss. Bei Serverzertifikaten muss u.a. die Prüfung der eindeutigen Zuordnung eines Zertifikats zur entsprechenden Einrichtung erfolgt sein.

3. Welche Zertifikate können in der DFN-AAI verwendet werden?

In der DFN-AAI können Zertifikate der folgenden Klassen uneingeschränkt verwendet werden:

- ♦ DFN-Verein PCA Global - G01
- ♦ DFN-Verein PCA Classic - G01
- ♦ DFN-Verein PCA Grid - G01
- ♦ VeriSign Class 3 Public Primary Certification Authority
- ♦ TC TrustCenter Class 3-Zertifikate
- ♦ GridKa-CA - GermanGrid

In der DFN-AAI können Zertifikate der folgenden Klassen mit Einschränkungen (in Klammern angegeben) verwendet werden:

- ♦ TC TrustCenter Class 2-Zertifikate (nur Serverzertifikate)
- ♦ Thawte Premium Server CA (nur wenn das Serverzertifikat kein "OU=Domain Validated" enthält)

Weitere Zertifizierungsstellen können nach Abschluss der Prüfung der zugehörigen Zertifizierungsrichtlinien hinzukommen.

Suche:

Termine
Sitemap
Disclaimer
Impressum

- Zertifikate sind mit in Standardbrowsern vorhandenem Zertifikat verkettet
 - MS / Internet Explorer
 - Windows verwendet zentralen Zertifikatspeicher
 - Windows XP, Windows 2000: OK
 - Windows Vista: OK, aber mit „Überraschungen“
 - Mozilla
 - anwendungsspezifisch, z.B. Firefox, Thunderbird
 - Verkettung (hoffentlich endlich) ab Sommer 2008
- Gültigkeit von Zertifikaten
 - Server max. 5 Jahre, Nutzerzertifikate max. 3 Jahre

- Zertifikate werden in der DFN-AAI an verschiedenen Stellen benötigt
- DFN unterstützt Teilnehmer durch DFN-PKI
 - Ausstellung von Nutzer- und Serverzertifikaten
 - Beratung und Hilfe bei Nutzung von Zertifikaten

✓ Web: www.pki.dfn.de/aai

✓ Kontakt: pki@dfn.de