DFN
Deutsches Forschungsnetz

Aufbau einer AAI im DFN

Ulrich Kähler, DFN-Verein
kaehler@dfn.de

Zeitplan

- **März 2006:**
  1. Treffen interessierter Teilnehmer
  Bibliotheken, GRIDs, eLearning, Anbieter

- **November 2006:**
  Fertigstellung grundlegender Dokumente
  (Policy, Verträge, Dienstbeschreibung, etc.)

- **Herbst 2006:**
  Aufbau der zentralen Dienste, Pilotbetrieb

- **Frühjahr 2007:**
  Beginn Vertragsabschlüsse und Betrieb

Was ist DFN-AAI ?

- **DFN-AAI**
  ist ein Dienst des DFN-Vereins für Wissen-schaftseinrichtungen und (auch kommerziellen) Anbietern von (Informations)-Ressourcen.

- **DFN-AAI** schafft das für notwendige **Vertrauensverhältnis** und einen **organisatorischen, technischen Rahmen** für den Austausch von Nutzerinformationen zwischen vielen Anwendern und vielen Anbietern.

Aufgaben des DFN-Vereins

DFN Deutsches Forschungsnetz

- Vorgabe von Richtlinien (Policy)
- Vertragsgestaltung und -abschluss
- zentrale betriebliche Aufgaben
- Public Relations
- internationale Vertretung

Zentrale betriebliche Aufgaben

- **Metadatenverwaltung** (im Aufbau)
- **Testsystem** (läuft)
- **WAYF-Server** (im Aufbau)
- **Zertifizierungsstelle (DFN-PKI)** (läuft)
- **Beratung, Schulung** (ab 2007)

Was ist DFN-AAI ?

- **DFN-AAI**
  ist ein Dienst des DFN-Vereins für Wissen-schaftseinrichtungen und (auch kommerziellen) Anbietern von (Informations)-Ressourcen.

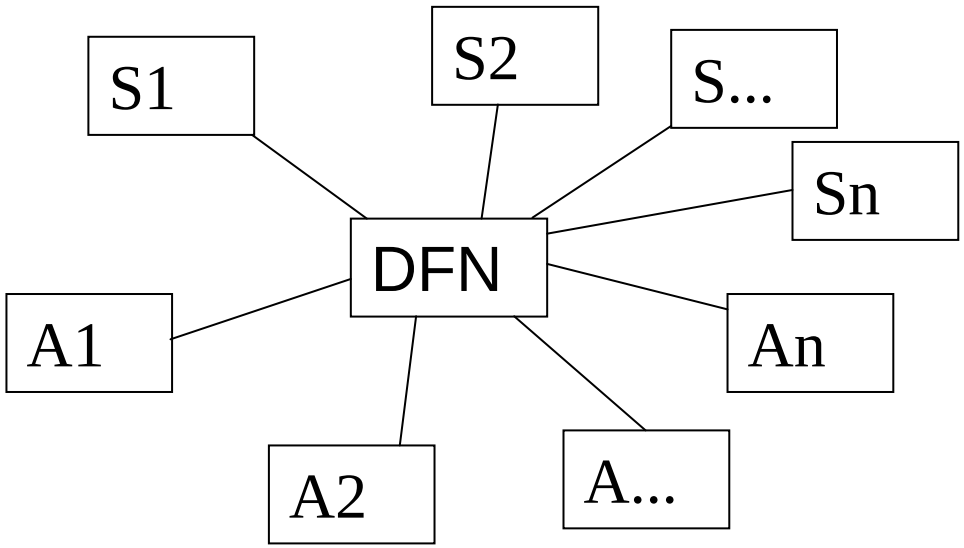
- **DFN-AAI** schafft das für notwendige **Vertrauensverhältnis** und einen **organisatorischen, technischen Rahmen** für den Austausch von Nutzerinformationen zwischen vielen Anwendern und vielen Anbietern.

Wo ist das Problem ?

- Anbieter muss dem Anwender **vertrauen**.
- Es geht um **Geld.**
- **„Vertrauen“** heißt im Geschäftsleben: **„Vertrag“.**
- Es müssen **belastbare vertragliche Regelungen** getroffen werden.

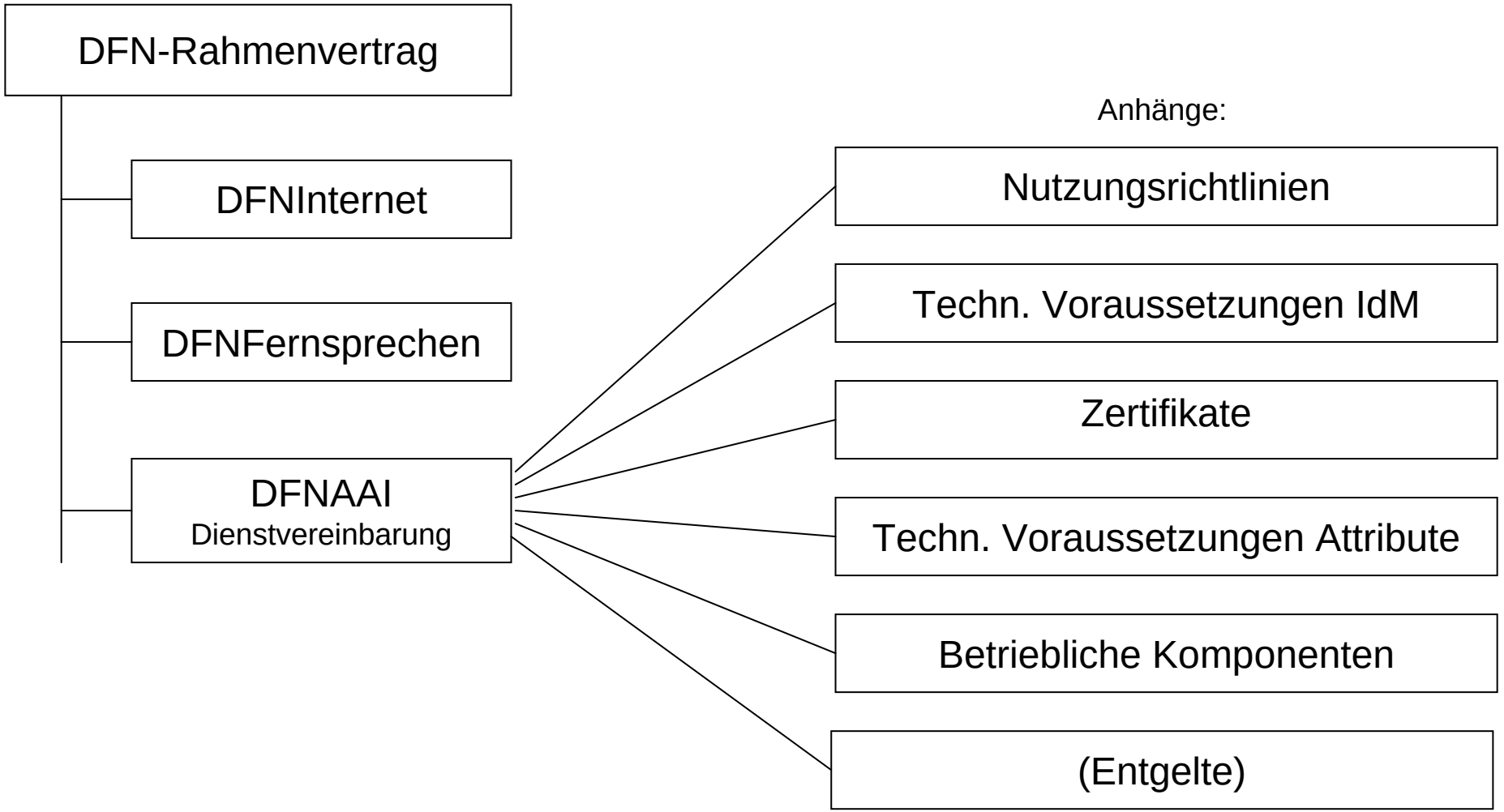
Der DFN-Verein

- ist zentraler Vertragspartner für alle Teilnehmer der AAI.

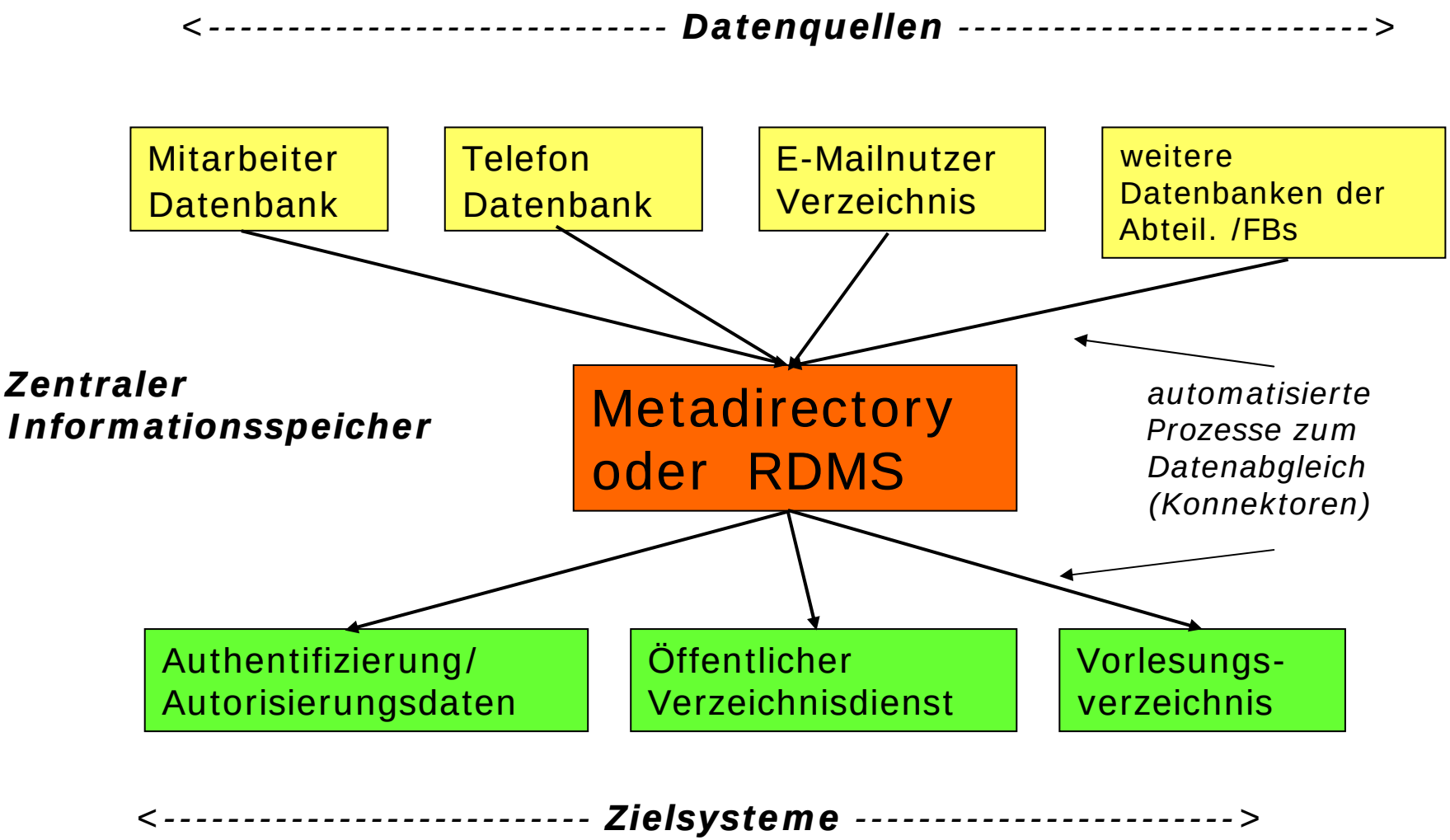


- schließt Dienstleistungsverträge ab.

Vertragsgestaltung / -abschluss



Identity Management



Anforderungen an IdM

DFN Deutsches Forschungsnetz

- Qualitätsanforderungen
  - Verlässlichkeit
    Sicherheitsstufen, Missbrauchverhinderung
  - Aktualität
    zeitnahe Änderung
  - Nachvollziehbarkeit
    Dokumentation, Logging
  - Ausfallsicherheit
    Back-up-Systeme

- Einklang mit rechtlichen Vorgaben
  - Datenschutzgesetz

Attribute aus AAI-Sicht

DFN Deutsches Forschungsnetz

Nr	Attribut	LDAP-Name des Attributs	aus Objektklasse				Klassifizierung	
1	Name	cn (common name)	x					x
2	Nachname	sn (surname)	x				x	
3	Vorname	GivenName			X			x
4	AngezeigterName	DisplayName			X			x
5	User ID	Uid			X			x
6	Zertifikat	userCertificate			X			x
7	Postadresse (Dienst)	postalAddress		x				x
8	Telefonnummer (Dienst)	telephoneNumber	x					x
9	Faxnummer (Dienst)	FacsimileTelephoneNumber		x				x
10	E-Mailadresse (Dienst)	Mail			X		x	
11	Handynummer	Mobile			X			x
12	Organisationsname	organisationName (o)		x				x
13	Organisationseinheit (OU) z.B. Abteilung	organisationalUnitName (ou)		x				x
14	DN der Organisation	eduPersonOrgDN				x		x
15	DN der Organisationseinheit	eduPersonOrgUnitDN				x		x
16	DN der wichtigsten OU	eduPersonPrimaryOrgUnitDN				x		x
17	Name in Form von Netz-ID	eduPersonPrincipalName				x	x	
18	Art d. Zugehörigrigkeit zur eigenen Organisation	eduPersonAffiliation				x		x
19	Hauptsächliche Art der Zugehörigkeit	eduPersonPrimaryAffiliation				x		x
20	Art d. Zugehörigkeit plus Domain Namen	eduPersonScopedAffiliation				x	x	
21	Berechtigung	eduPersonEntitlement				x	x	
22	Eindeutiges Pseudonym f. Anbieter	eduPersonTargetedID				x	x	
23	Spitzname	eduPersonNickname				x		x

Nutzung von Zertifikaten

- In der DFN-AAI kommen Zertifikate in drei Bereichen zum Einsatz
  - beim Betrieb von Shibboleth
  - zur Authentifizierung der Webserver, die die Dienste anbieten
  - zur Authentifizierung von Nutzern

Zertifikate 1: Shibboleth intern

- 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

Zertifikate 2: Webserver

- 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 verwenden zur Authentifizierung Zertifikate

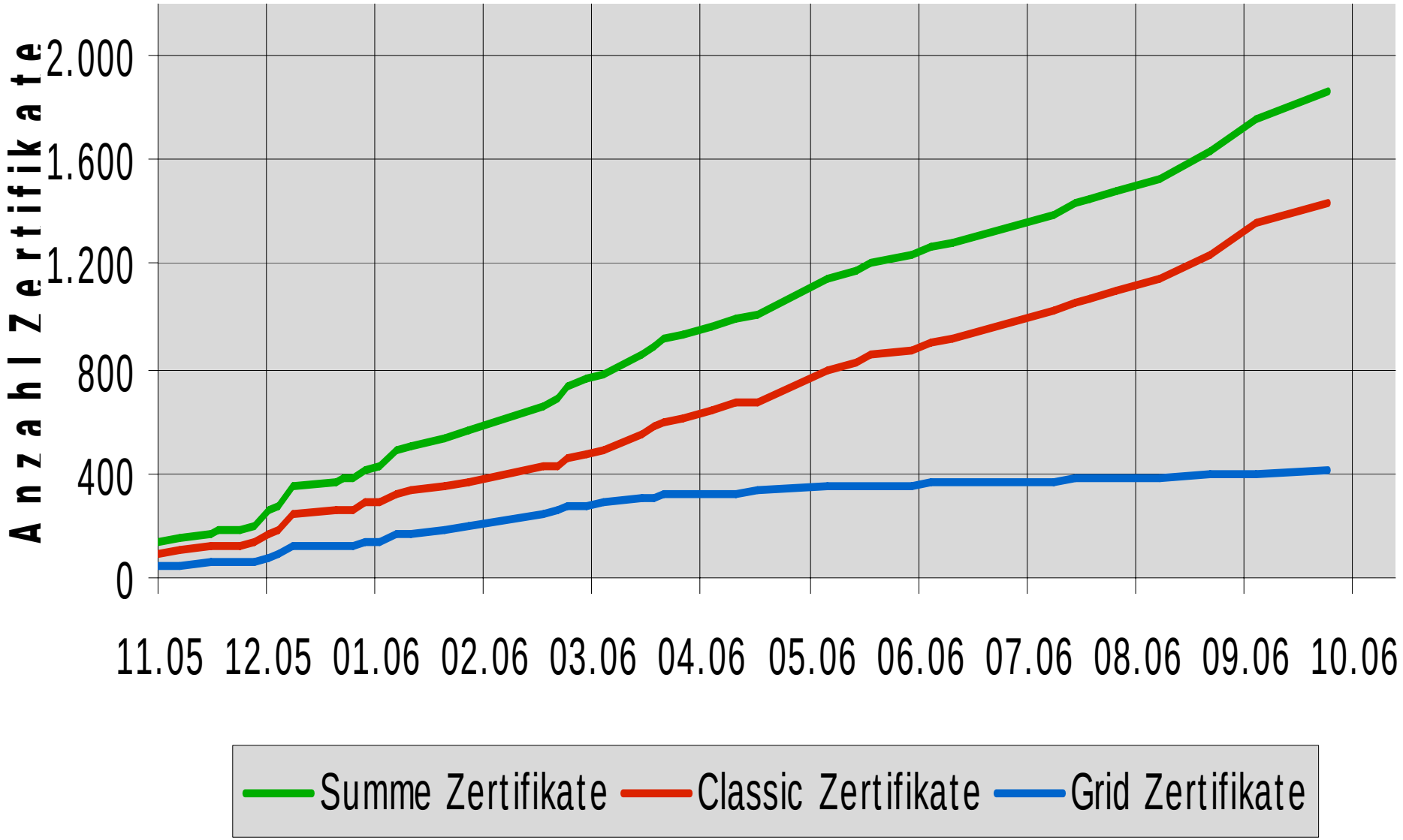
Zertifikate 3: Nutzer

- 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

Zusammenfassung

- Der Betrieb der DFN-AAI erfordert an diversen Stellen den Einsatz von Zertifikaten
- Mit der DFN-PKI steht eine etablierte Zertifizierungsinfrastruktur zur Verfügung
- Zertifikate der DFN-PKI können in der DFN-AAI genutzt werden
  - Alternativen sind möglich, wenn die Policyanforderungen der DFN-PKI eingehalten werden
- Infos zur Zertifikaten: www.dfn.de/pki

Zertifikate in der DFN-PKI



Zeitplan

- **März 2006:**
  1. Treffen interessierter Teilnehmer
  Bibliotheken, GRIDs, eLearning, Anbieter

- **November 2006:**
  Fertigstellung grundlegender Dokumente
  (Policy, Verträge, Dienstbeschreibung, etc.)

- **Herbst 2006:**
  Aufbau der zentralen Dienste, Pilotbetrieb

- **Frühjahr 2007:**
  Beginn Vertragsabschlüsse und Betrieb

Kontakt

Für alle Fragen rund um die DFN-AAI:

E-Mail: aai@dfn.de