Ein Vorschlag zur Veröffentlichung von X.509-Zertifikaten

Oberseminar Theoretische Informatik, TU Darmstadt, 30.11.2004

Peter Gietz, CEO, DAASI International GmbH

Peter.gietz@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management

Agenda

- DFN Projekt: Directory Kompetenzzentrum
- Eigenschaften von LDAP
- LDAP und PKI
- PKI/LDAP Projekt in Baden Württemberg
- DFN-weite PKI?

DAASI International

Directory Applications
for Advanced Security
and Information Management

DFN Projekt Directory Kompetenzzentrum

DAASI International

Directory Applications
for Advanced Security
and Information Management

DFN Projekte als Keimzelle der DAASI International GmbH

- Seit 1994 vom BMBF finanzierte DFN-Forschungsprojekte zu Verzeichnisdiensten an der Universität Tübingen
- Wegen Aufbau und Betrieb von Diensten, die nicht durch Forschungsmittel Förderungsfähig sind musste neue Organisationsform gefunden werden
- Januar 2001 wurde deshalb die DAASI International GmbH gegründet
- Das letzte DFN-Projekt wurde von DAASI International durchgeführt: „Ausbau und Weiterbetrieb eines Directory Kompetenzzentrums“

DAASI International

Directory Applications
for Advanced Security
and Information Management

DFN-Projektergebnisse (Auswahl)

- Kompetenzzentrum DFN Directory Services
- Arbeiten zu zentraler Authentifizierung
  - Unified Login
  - Single Sign On
  - Zwei Lösungen:
    - Active Directory / Kerberos
    - OpenLDAP / SAMBA
- Arbeiten zu Verzeichnissen für PGP-Schlüssel und X.509-Zertifikate
  - Gemeinsamer Server für X.509 und PGP
  - Neues Speichermodell entwickelt und im Rahmen der IETF veröffentlicht (s.u.)

DAASI International

Directory Applications for Advanced Security and Information Management

Eigenschaften von LDAP

DAASI International

Directory Applications
for Advanced Security
and Information Management

Was ist LDAP

- Lightweight Directory Access Protocol
- Ein Datenbankmodell (X.500)
  - Hierarchische Datenstruktur
  - Objektorientierter Ansatz
  - Erweiterbar für beliebige Daten
- Ein Netzwerkprotokoll
  - Internetstandard
  - Flexibel erweiterbar
  - Verteilung der Daten im Netz
  - Spiegelung der Daten im Netz

LDAP Informationsmodell

- Ein Datensatz wird Eintrag (entry) genannt
- Ein Eintrag besteht aus Attributen
- Ein Attribut besteht aus Attributtyp und Attributwert
- Attributtyp Definition kann u.a. enthalten:
  - Attributsyntax
  - Single- oder multi-valued
  - verschiedene Vergleichsregeln (Matching Rules)
- Bestimmte Attributtyp-Wert-Paare bilden den Namen des Eintrags
- Jeder Eintrag hat mindestens ein *Objektklassen-Attribut* haben
  - Charakterisiert den gesamten Eintrag
  - Spezifiziert zu verwendende Attributtypen (*MUST und MAY*)
  - Objektklassen können Eigenschaften von übergeordneten Objektklassen ererben

Objektklassendefinition

ObjectClassDescription =
"(" whsp numericoid whsp ; ObjectClass identifier
["NAME" qdescrs]
["DESC" qdstring]
["OBSOLETE" whsp]
["SUP" oids] ; Superior ObjectClasses
[("ABSTRACT" / "STRUCTURAL" / "AUXILIARY")
whsp] ; default structural
["MUST" oids] ; AttributeTypes
["MAY" oids] ; AttributeTypes whsp ")"

Objektklassendefinition Beispiel

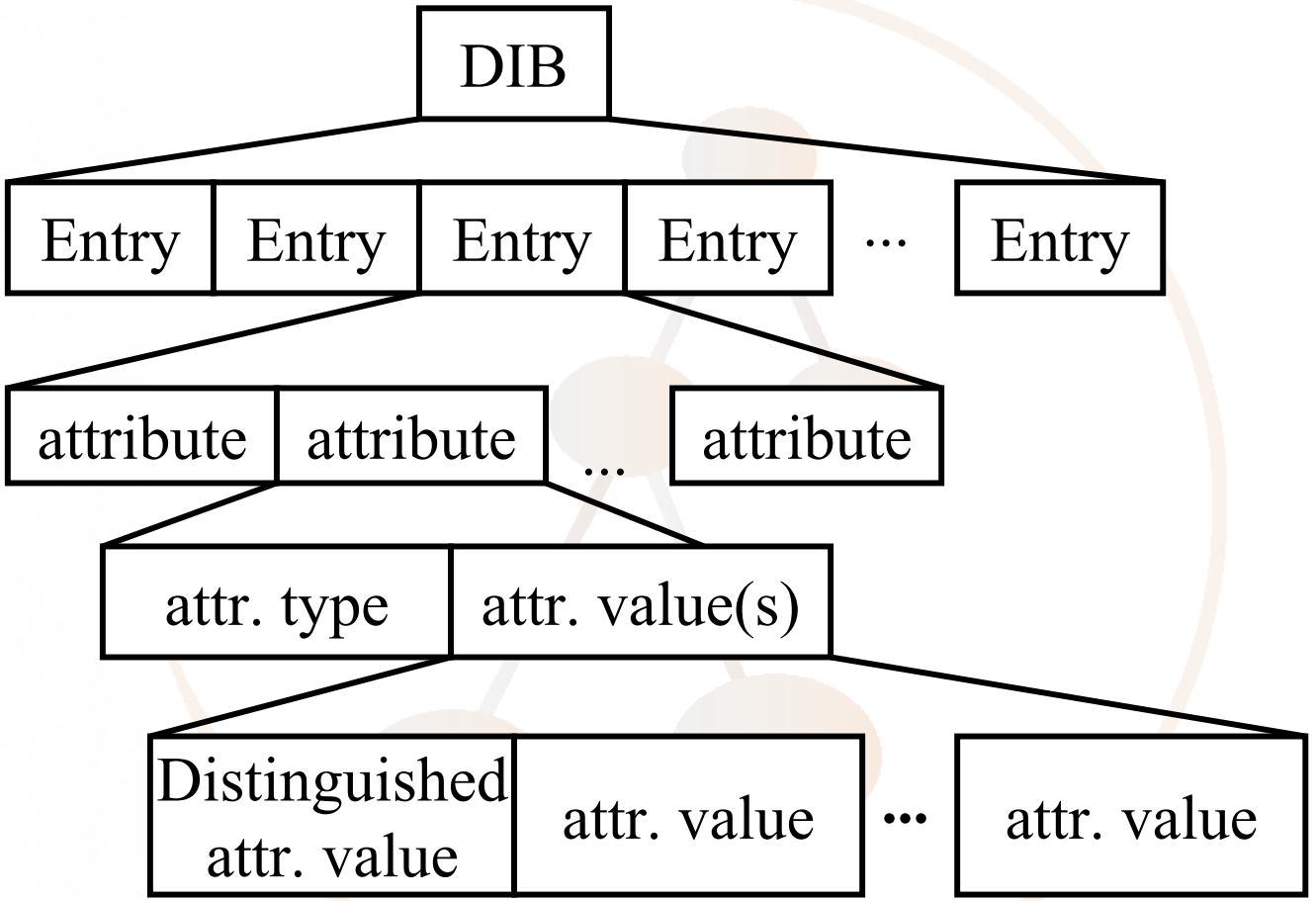
```
( 2.5.6.0 NAME 'top'
  ABSTRACT
  MUST objectClass )

( 2.5.6.6 NAME 'person'
   SUP top
   STRUCTURAL
   MUST ( sn $ cn )
   MAY ( userPassword $ telephoneNumber $
            seeAlso $ description ) )
```

Objektklassen

- Vererbung
  - Objektklassen können von anderen Objektklassen abgeleitet werden
  - Abgeleitete Objektklassen erben die Attributspezifikationen der Klasse von denen sie abgeleitet wurden
- Objektklassenarten
  - ABSTRACT
    - abstrakte nicht intantiierbare Klasse
    - Dient nur zur Vererbung
  - STRUCTURAL
    - Bezeichnet die Hauptcharacteristik eines Eintrags
  - AUXILIARY
    - Bezeichnet Zusatzeigenschaften eines Eintrags

Directory Information Base

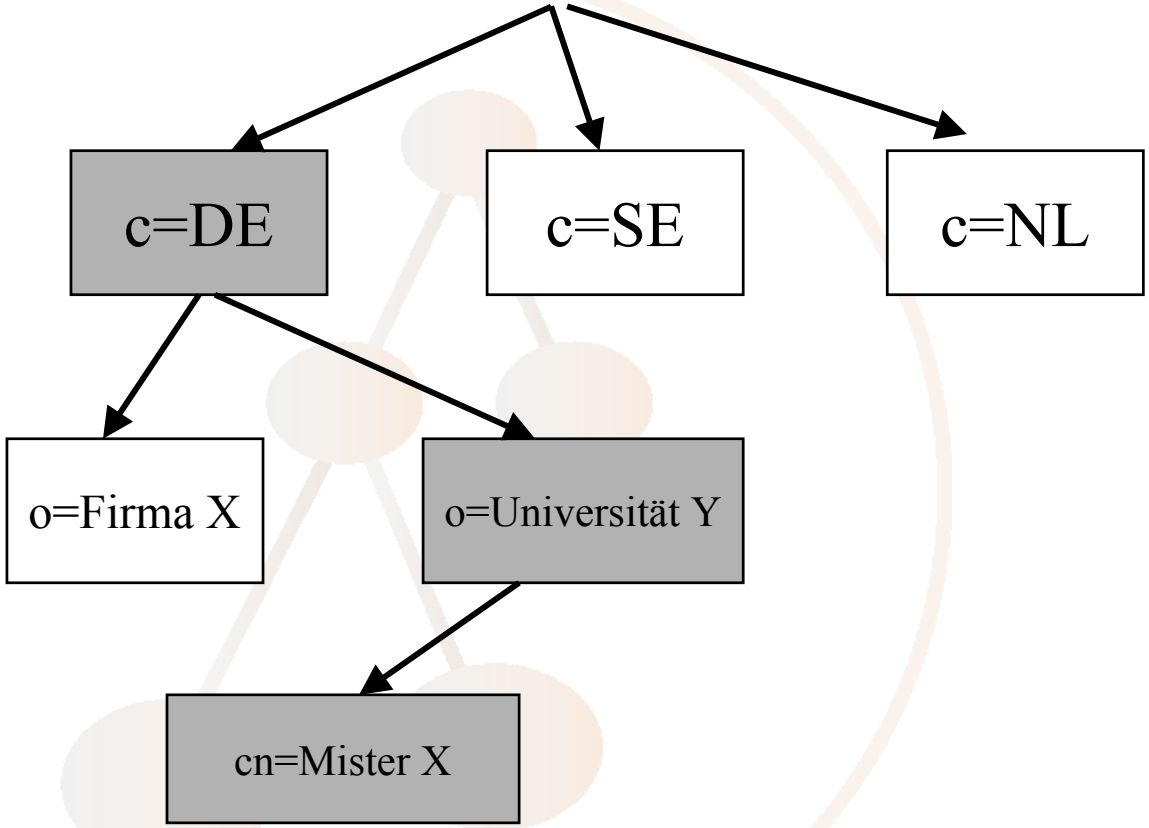


Directory Information Tree (DIT)
(Relative) Distinguished Name (RDN, DN)

RDN: c=DE
(countryName)

RDN: o=Universität Y
(organizationName)

RDN: cn=Mister X
(commonName)



DN: cn=Mister X, o=Universität Y, c=DE

DAASI International
Directory Applications for Advanced Security and Information Management

Funktionsmodell

- Authentifizierungs-Operationen:
  - bind
  - unbind
  - abandon
- Abfrage-Operationen:
  - search
  - compare
- Update-Operationen:
  - add
  - delete
  - modify
  - modifyDN

Search Filter

- Equality
  - Only for attributes with equality matching rule
  - e.g.: (cn=Mister X) only entries with common name equals “Mister X”
- Substring
  - Only for attributes with substring matching rule
  - e.g. (cn=Mister*) all entries with cn beginning with “Mister”
- Approximate
  - Implementation dependent
  - e.g.: (cn~=Mister) all entries with cn sounding similiar to “Mister”
- Negation operator
  - e.g. (!(cn=Mister X)) all entries but the one with cn equals “Mister X”

Search Filter Extensions

- LDAPv3 defines an extensible matching filter
  - syntax: attr [“:dn”] [“:” matchingrule] “:=“ value
    - attr is an attribute name
    - “:dn” says that also the attribute in the dn should be searched as well
    - matching rule given by an OID or associated descriptive name
  - examples:
    - (cn:1.2.3.4.5.6:=Mister X) use matching rule 1.2.3.4.5.6 for comparison
    - (o:dn:=company) search for o=company in attributes and also in DN

Unterschiede zu relationalen Datenbanken

- Es gibt standardisierte Datenschemata
- Entitätsinformationen bleiben an einem Platz
- Mehrfachwerte sind unproblematisch
- Unbegrenzte Anzahl von Datentypen
- Vergleichsregeln sind Teil des Datenmodells
- Änderungen des Datenschemas einfach möglich (Lego-Prinzip)
- Netzzugriff von vorneherein vorgesehen:
  - Datenreplikation und Datenverteilung über das Netz

Zusammenfassung: Vorteile von LDAP

- Objektorientierte Datenmodellierung
- Offener Standard ermöglicht Unabhängigkeit von Herstellern
- Verteilung ermöglicht beliebige Skalierbarkeit
- Replikation ermöglicht beliebig hohe Ausfallssicherheit
- Hohe Sicherheit durch Zugriffskontrolle und Authentifizierung
- Daten sind über TCP/IP basiertes Netzwerkprotokoll zugänglich
- Die gleichen Daten können von verschiedenen Anwendungen verwendet werden
- Es gibt eine stabile Open-Source-Implementierung: WWW.OPENLDAP.ORG

LDAP als Zertifikatsserver

DAASI International

Directory Applications
for Advanced Security
and Information Management

Public Key Infrastructure (PKI)

- Asymmetrisches Verschlüsselungsverfahren
  - Schlüsselpaar: Öffentlicher und Privater Schlüssel
  - Digitale Signatur mit privatem Schlüssel kann mit öffentlichen Schlüssel verifiziert werden
  - Mit dem öffentlichen Schlüssel kann man einen Text so verschlüsseln, dass er nur mit dem privaten Schlüssel entschlüsselt werden kann
- Zertifikat
  - Wird von einer Third Trusted Party, einer Certification Authority (CA) erstellt
  - CA bestätigt Identität zum öffentlichen Schlüssel mittels einer digitalen Signatur
  - Werden als ASN.1 Struktur definiert

PKI and Directory

The Burton Group: Network Strategy Report, PKI Architecture, Jul 1997: (Quoted after: S. Zeber, X.500 Directory Services and PKI issues, http://nra.nacosa.nato.int/pki/hdocs/pkiahwg30/index.htm

"... Customers should always consider PKI a directory-enabled set of services and infrastructure. Without directory services, PKI will be exponentially harder to implement and manage. Consequently, customers should't deploy PKI widely without an accompanying directory plan"

DAASI International

Directory Applications for Advanced Security and Information Management

Zertifikatsserver für PKI

- Der Verzeichnisdienst
  - hält Zertifikate im Netz vor
  - Ermöglicht Zugriff durch Anwendungen
  - Dokumentiert zurückgerufene Zertifikate in sog. Certificate Revocation Lists (CRL)
  - Kann somit Grundlage eines Online Certificate Status Protocol (OCSP) Dienst bilden
- Entweder betreibt eine CA den Verzeichnisdienst selber, oder liefert Zertifikate auf einem gesicherten Weg an den Betreiber

Der gegenwärtige Standard

- Attributtyp userCertificate wird zum Speichern des Zertifikats verwendet
  - Gesamtes Zertifikat in einem Attributwert
  - Multi-Value Attribut
  - Wird einem Personeneintrag hinzugefügt
- Problem:
  - Es kann nicht im Zertifikat gesucht werden
  - bei vielen Zertifikaten einer Person muss der Client alle Zertifikate holen und einzeln analysieren, um das richtige Zertifikat (z.B. das mit Key usage: encryption) zu finden

Bisherige Vorschläge

- Neue Spezifikation der Standardlösung:
  - Zeilenga, K., “LDAP X.509 Certificate Schema”, draft-zeilenga-ldap-x509-00.txt, work in progress, 17 October 2004
- Generisches Encoding:
  - Legg, S., "Generic String Encoding Rules for ASN.1 Types", RFC 3641, October 2003.
- Die intelligentere aber komplexe Lösung
  - Legg, S., "Lightweight Directory Access Protocol (LDAP) and X.500 Component Matching Rules”, RFC 3687, February 2004
    - “This document defines generic matching rules that can match any user selected component parts in an attribute value of any arbitrarily complex attribute syntax.”
  - Chadwick, D. and S. Mullan, “Returning Matched Values with the Lightweight Directory Access Protocol version 3 (LDAPv3, RFC 3876, September 2004
    - “This document specifies an LDAPv3 control to enable a user to return only those values that matched (i.e., returned TRUE to) one or more elements of a newly defined "values return" filter. This control can be especially useful when used in conjunction with extensible matching rules that match on one or more components of complex binary attribute values.”

ASN.1

- Abstract Syntax Notion One
- Abstarktes Konzept unabhängig von spezifischen Kodierungen wie Basic Encoding Rules (BER)
- Einfache Datentypen, z.B.
  - PrintableString, INTEGER, BOOLEAN, ...
- Komplexe Datentypen:.
  - SET, SEQUENCE, SET OF, SEQUENCE OF, CHOICE
- Ist mit ABNF abbildbar

Beispiele von Component Matching Filter

- Suche im Attributtyp objectClasses nach einem Component name, welcher den Werrt „foobar“ hat:
  - (objectClasses:componentFilterMatch:=
    item:{ component „name.*“,
    rule caseIgnorMatch, value „foobar“ })
- Suche objectClasses Definitionen, die keine Description haben:
  - (objectClasses:componentFilterMatch:=
    not:item:{ component „description“,
    rule presentMatch, value NULL })

Warum nicht ausreichend

- Component Matching ist sehr flexibel einsetzbar
- Obwohl als Standard Track Dokument gibt es nur zwei Implementierungen
- Da die meisten LDAP-Implementierungen nicht ASN.1 basiert sind, ist die Suche in ASN.1-Strukturen teuer zu implementieren
- Sowohl Clients als auch Server müssen verändert werden
  - Extensible Matching Rule
  - Vordem Vergleich müssen Teile nicht relevant für den Vergleich substituiert werden
- Für das Problem der multiplen Zertifikate nur zusammen mit der Erweiterung ValuesReturnFilter control sinnvoll einsetzbar, die ebenfalls sowohl im Client als auch im Server implementiert sein muss
- Lässt sich nicht in Index-Scenarios einsetzen
- Dennoch ist Compound Matching eine zukunftsträchtige Technologie

Neuer Vorschlag

- IETF-Draft: Gietz, P., Klasen, N., „Internet X.509 Public Key Infrastructure Lightweight Directory Access Protocol Schema for X.509 Certificates“, draft-ietf-pkix-ldap-pkc-schema-01, October 2004
- Jedes Zertifikat wir in einem eigenen Eintrag gespeichert
- Zusätzlich zum Zertifikat werden Inhalte der wichtigsten Zertifikatsfelder in LDAP Attributen abgelegt („Metadaten-Ansatz“)

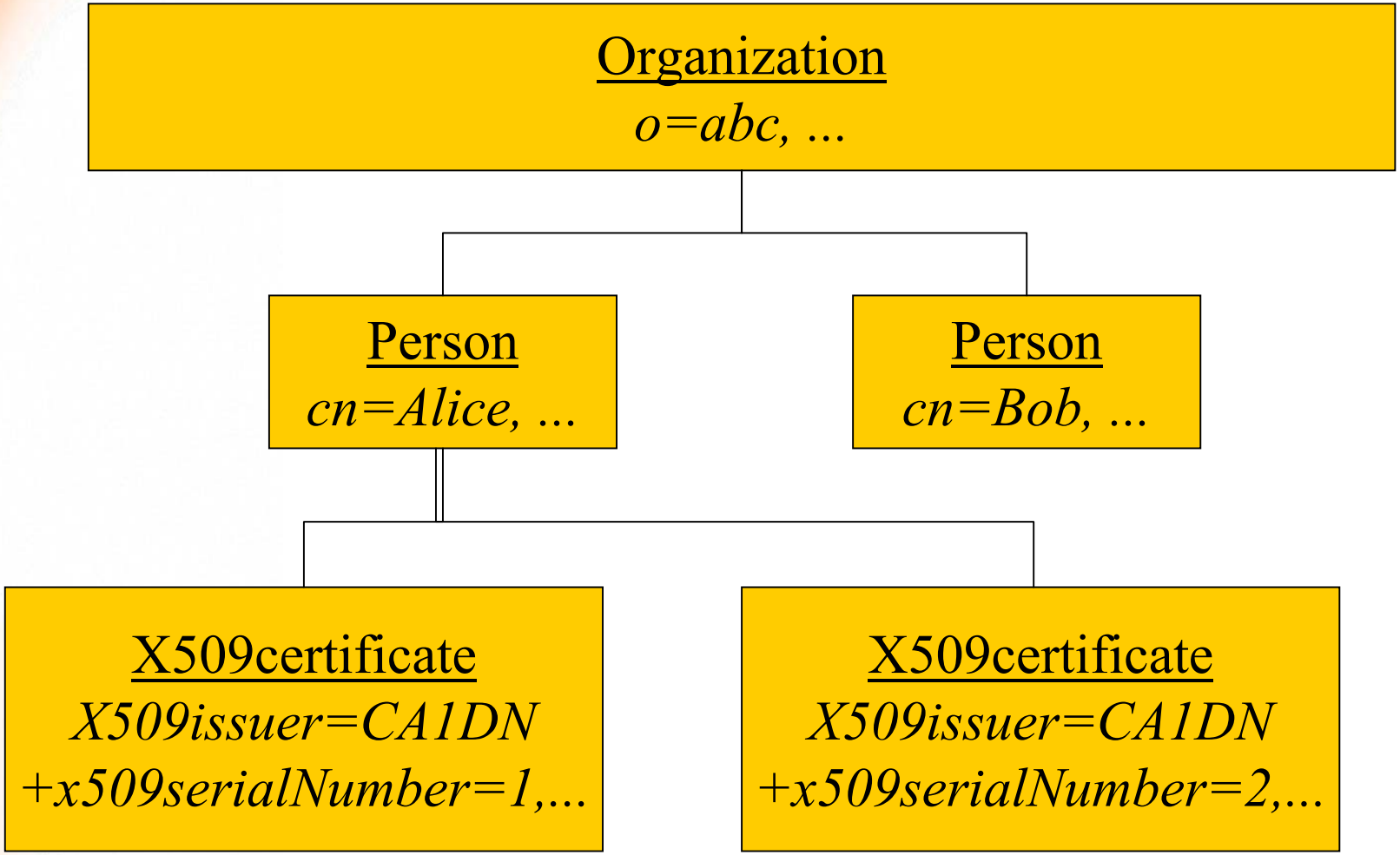
Parallel-Dokumente

- Chadwick, D. and M. Sahalayev, "Internet X.509 Public Key Infrastructure - LDAP Schema for X.509 CRLs", draft-ietf-pkix-ldap-crl-schema-03.txt (work in progress), 25 October 2004
- Chadwick, D. and M. Sahalayev, "Internet X.509 Public Key Infrastructure - LDAP Schema for X.509 Attribute Certificates", draft-ietf-pkix-ldap-ac-schema-02.txt (work in progress), 25 October 2004
- Weitere Dokumente zu Crosscertificates, Qualified certificates, „Metametadaten“, etc. in Planung

Vorteile

- Lösung lässt sich mit bestehenden Servern implementieren
- Anpassung der Clients ist einfach, da nur der (einfache) Suchfilter modifiziert werden muss
- Flexibilität bei der DIT-Struktur
- Die Zertifikate können im Rahmen eines Indexsystems indiziert werden

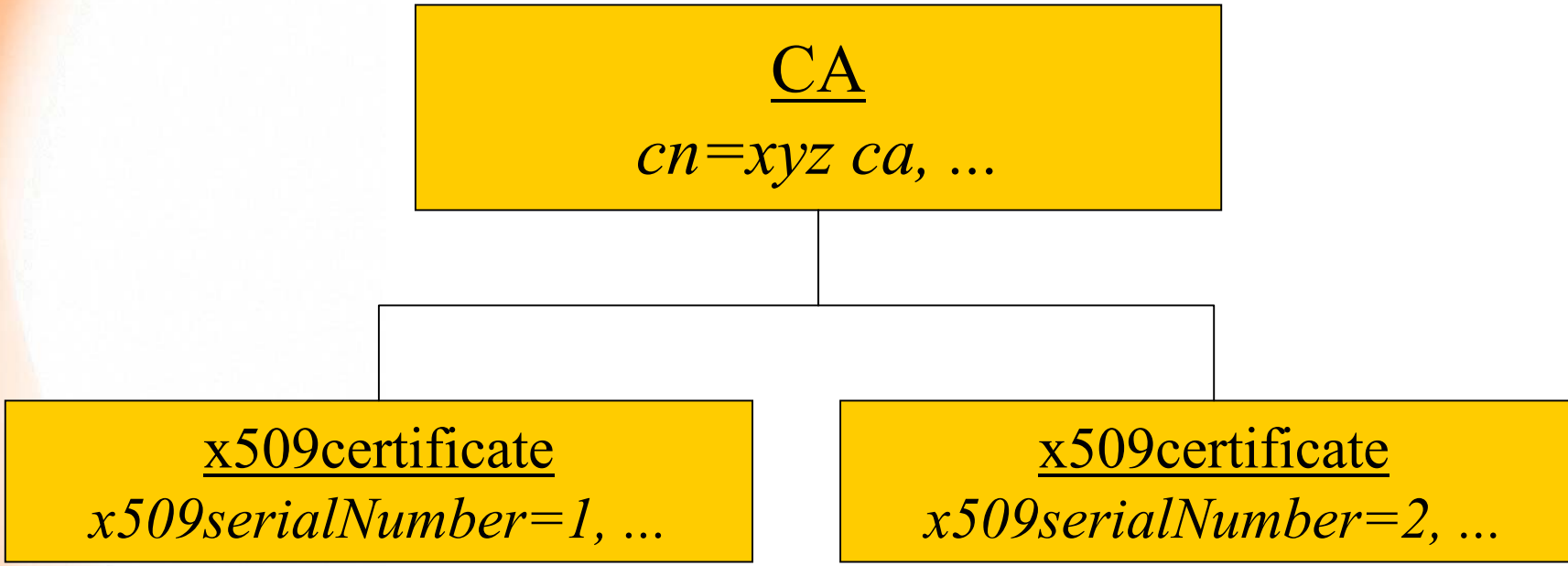
DIT-Struktur im Personenverzeichnis



DAASI International

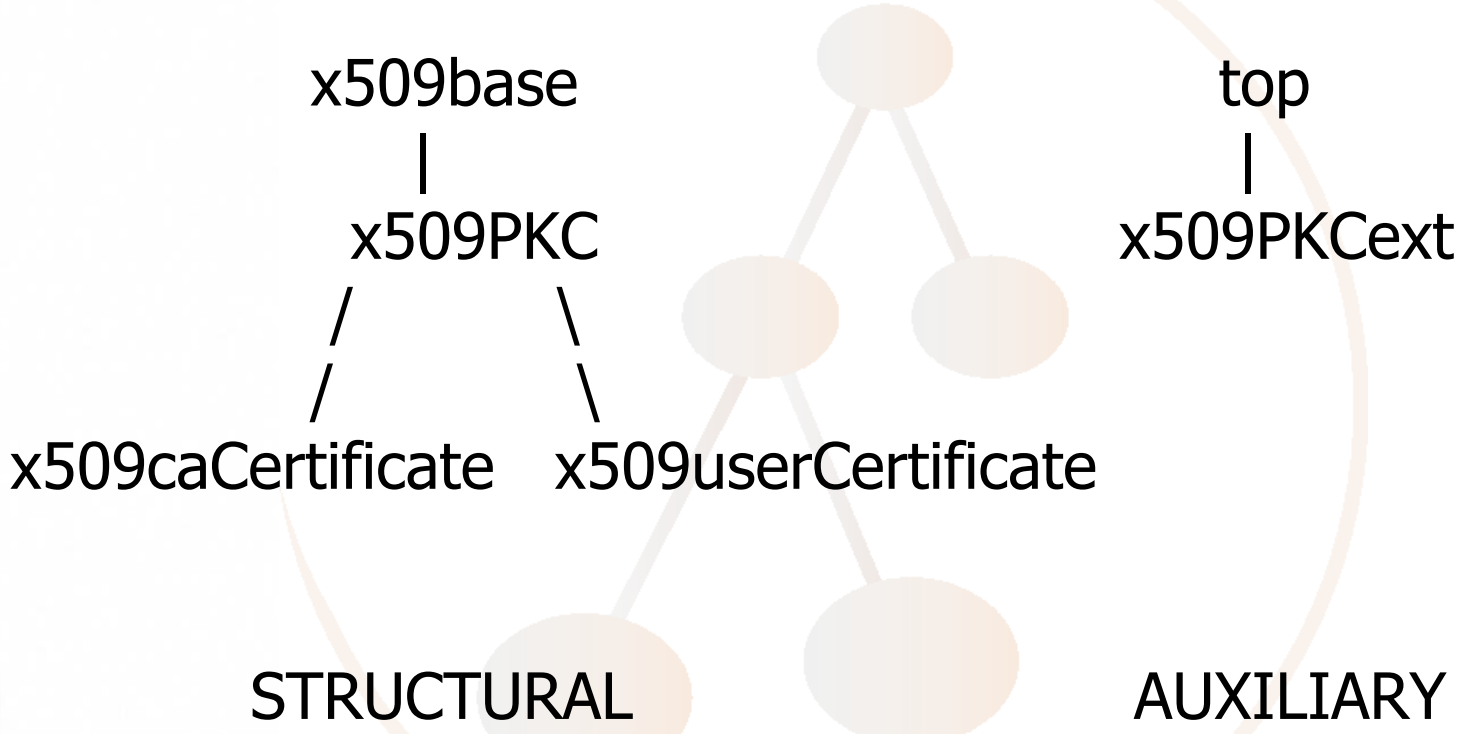
Directory Applications
for Advanced Security
and Information Management

DIT-Struktur im Zertifikatsverzeichnis



DAASI International
Directory Applications for Advanced Security and Information Management

Das Datenmodell: Objektklassenvererbung



DAASI International

Directory Applications
for Advanced Security
and Information Management

Datenmodell: Objektklassen

```
( 1.3.6.1.4.1.10126.1.5.4.2.1
        NAME 'x509base'
        ABSTRACT
        MAY x509version )

( 1.3.6.1.4.1.10126.1.5.4.2.3
        NAME 'x509PKC'
        SUP x509base
        ABSTRACT
        MUST ( x509serialNumber $
                x509signatureAlgorithm $ x509issuer $
                x509validityNotBefore $ x509validityNotAfter $
                x509subjectPublicKeyInfoAlgorithm )
        MAY  ( x509certHolder $ x509issuerSerial ) )
```

DAASI International

Directory Applications
for Advanced Security
and Information Management

Datenmodell: Objektklassen 2

```
( 1.3.6.1.4.1.10126.1.5.4.2.4
        NAME 'x509userCertificate'
        SUP x509PKC
        STRUCTURAL
        MUST userCertificate
        MAY  x509subject )

( 1.3.6.1.4.1.10126.1.5.4.2.5
        NAME 'x509caCertificate'
        SUP x509PKC
        STRUCTURAL
        MUST ( caCertificate $ x509subject ) )
```

Datenmodell: Objektklassen 3

```
( 1.3.6.1.4.1.10126.1.5.4.2.6
        NAME 'x509PKCext'
        SUP top
        AUXILIARY
        MAY  ( x509authorityKeyIdentifier $ x509authorityCertIssuer $
               x509authorityCertSerialNumber $ x509subjectKeyIdentifier
               x509keyUsage $ x509policyInformationIdentifier $
               x509subjectRfc822Name $ x509subjectDnsName $
               x509subjectDirectoryName $ x509subjectURI $
               x509subjectIpAddress $ x509subjectRegisteredID $
               x509issuerRfc822Name $ x509issuerDnsName $
               x509issuerDirectoryName $ x509issuerURI $
               x509issuerIpAddress $ x509issuerRegisteredID $
               x509basicConstraintsCa $ x509basicConstraintsPathLen $
               x509extKeyUsage $ x509fullCRLDistributionPointURI ) )
```

Datenmodell: Objektklassen 4

```
( 1.3.6.1.4.1.10126.1.5.4.2.2
        NAME 'x509certificateHolder'
        AUXILIARY
        MAY  ( x509certLocation ) )
```

Arbeiten im DFN-Projekt

- Implementierung des Schemas in einem OpenLDAP-Server
- Programm, welches Zertifikate analysiert und LDAP-Einträge erzeugt, die dem Metadaten-Schema entsprechen
- Hybriden Server mit X.509- und PGP-Zertifikaten

DAASI International

Directory Applications
for Advanced Security
and Information Management

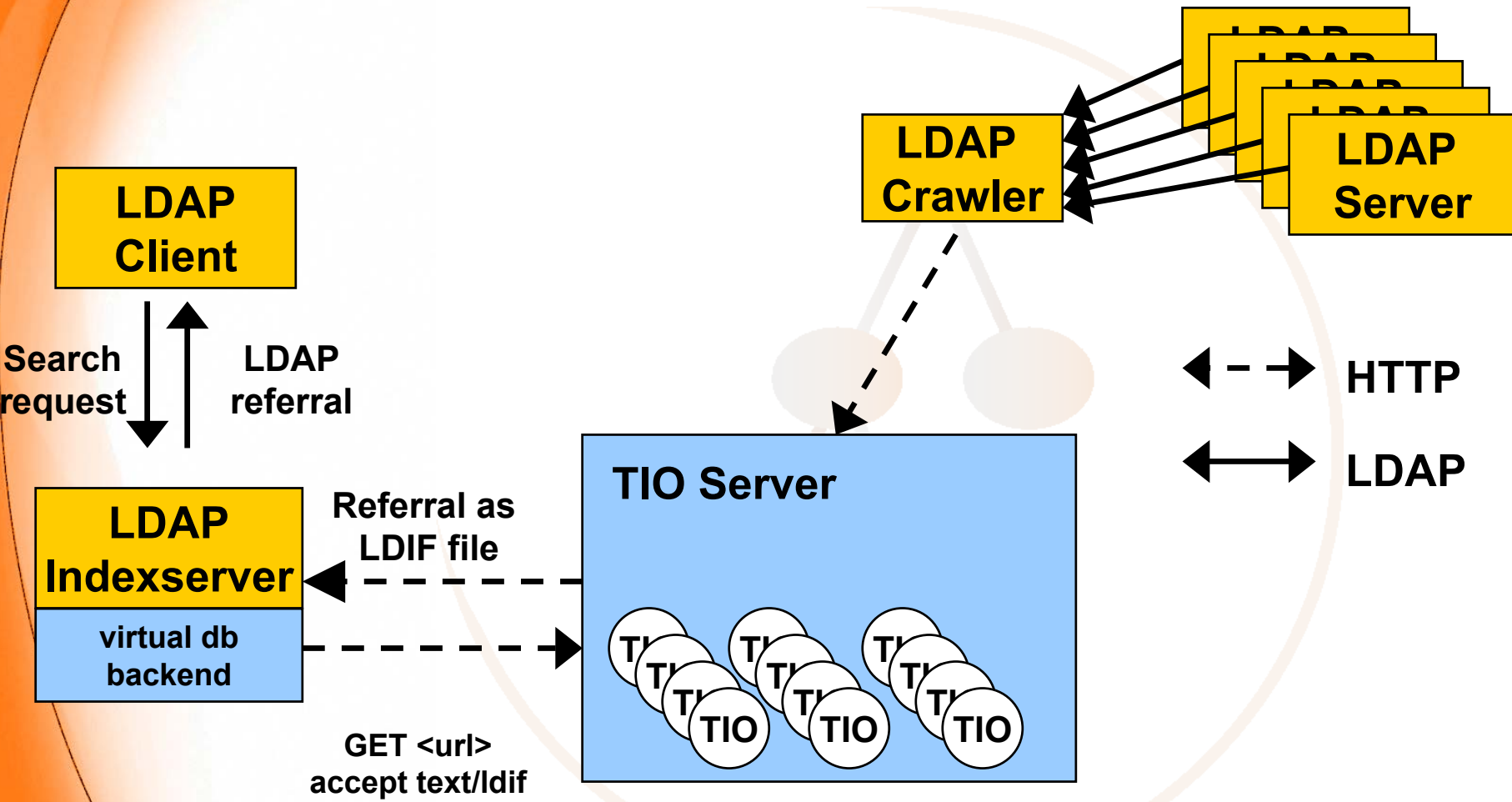
Die „Wirkungsgeschichte“

- Entwicklung eines „Proxy-Servers“, der zwischen neuem Schema und altem Standard übersetzt von David Chadwick, University of Salford, im Rahmen eines TERENA-Projekts
- Weitere Implementierungen, z.B. an der TU-Darmstadt für die RegTP

Weitere Einsatzmöglichkeit

- Integration der Chadwick-Software zur noch besseren Einbindung heutiger Clients
- Dadurch, dass Zertifikats-Informationen in einzelnen Attributen gespeichert sind, können diese im Rahmen eines Indexsystem genutzt werden
  - Common Indexing Protocol (CIP): RFC 2651-2654
  - Beliebig viele LDAP-Zertifikatsserver können so zu einem Informationssystem zusammengefasst werden
  - Dezentrale Datenpflege bei einzelnen CAs
  - Zentraler Zugriff auf alle Zertifikate

Common Indexing Protocol Architektur



DAASI International

Directory Applications for Advanced Security and Information Management

PKI/LDAP Projekt in Baden Württemberg

DAASI International

Directory Applications
for Advanced Security
and Information Management

PKI/LDAP Projekt Plan

- Thema: Landesweite PKI auf Basis von indizierten Verzeichnisdiensten mit standardisierten LDAP Zugriffsmechanismen
- Arbeitsprogramm:
  - Evaluierung bestehender CAs und Verzeichnisdienste in BW
  - Zentrale Serverdienste (s.u.)
  - Unterstützung und Koordinierung der dezentralen Verzeichnisdienste
  - Realisierung von auf PKI beruhenden Mehrwertdiensten (S/MIME, SSL, Webauthorisierung, User-Interfaces)
  - Öffentlichkeitsarbeit

DAASI International

Directory Applications
for Advanced Security
and Information Management

PKI/LDAP Projekt Plan 2

- Projektdauer: 2 Jahre (zuzgl. > 8 Monate Vorbereitungs- und Entscheidungszeit)
- Teilnehmer: Universitäten Freiburg, Heidelberg, Hohenheim, Karlsruhe, Konstanz, Mannheim, Stuttgart, Ulm, und Tübingen, sowie DAASI International GmbH
- Umfang: 10 Personenjahre
- Untergliederung in verschiedene Teilprojekte

DAASI International

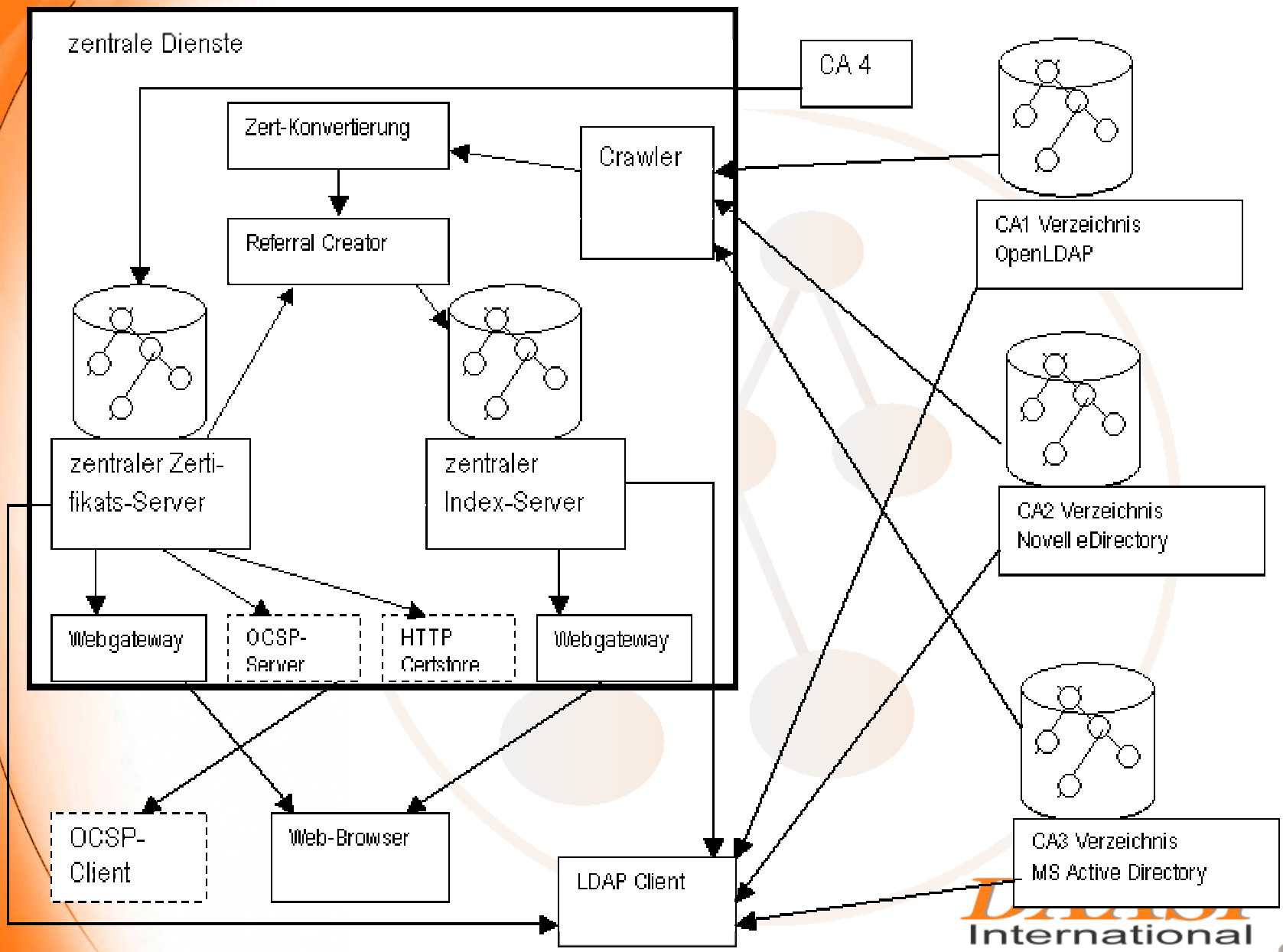
Directory Applications
for Advanced Security
and Information Management

Teilprojekt zentrale Server

- Teilaufgaben:
  - Zentrales Zertifikatsverzeichnis für an die Projektinfrastruktur angeschlossenen CAs die keinen eigenen Verzeichnisdienst betreiben
  - Index-Server, der Informationen der von an die Projektinfrastruktur angeschlossenen Verzeichnisdiensten
  - Referenzserver auf Open-Source-Basis für teilnehmende CAs

DAASI International

Directory Applications
for Advanced Security
and Information Management



DFN-weite PKI?

- **Motivation:**
  - **Ermöglicht Intra-Domain-Authentifizierung**
    - Entweder: jeder der ein Zertifikat einer Universität besitzt darf an anderen Universitäten Ressourcen nutzen
    - Oder: PKI als Grundlage einer Attributzertifikats-Infrastruktur (Priviledge Management Infrastructure, PMI) mit Spezial-Authorisierungen
    - Oder: PKI als Grundlage für Proxy-Zertifikate, wie sie zur Authorisierung im Grid-Computing verwendet werden
  - **Synergie-Effekte**
    - Gemeinsame Policies
    - Informationsaustausch
    - Produkt-Evaluationen
  - **Ein weiterer Schritt zum deutschen Forschungsraum**

Bestehende Voraussetzungen

- Langjährige Aktivitäten der DFN-PCA (heute innerhalb der DFN-Cert GmbH)
  - Gemeinsame Certification Policy
  - Zertifizierungsinfrastruktur
  - CA-Support
- Ergebnisse der DFN-Verzeichnisdienstprojekte
  - Neues Datenschema
  - Testimplementierung
  - Software
- Erfahrungen aus dem PKI/LDAP-Projekt können zukünftig einfließen

Vielen Dank für Ihre Aufmerksamkeit!

- Kontakt und weitere Informationen:
  - DAASI International GmbH:
    http://www.daasi.de
    Info@daasi.de
  - DFN Directory Services:
    http://www.directory.dfn.de
    Info@directory.dfn.de

DAASI International
Directory Applications for Advanced Security and Information Management