Neues Konzept für einen DFN-weiten Zertifikatsserver

17. DFN-Arbeitstagung über Kommunikationsnetze,

Düsseldorf, 12.6.2003

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?

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

- AMBIX – Aufnahme von Mailbenutzern in das X.500-Directory
  - Emailverzeichnis für die Forschung in Deutschland mit Webfrontend (ca 60.000 Datensätze)
  - Zentraler Verzeichnisdienst für Organisationen, die nicht selbst Verzeichnisdienste betreiben
- IDEV - Index Deutscher Email-Verzeichnisse
  - Deutschlandweiter X.500/LDAP Index
  - Crawler holt regelmäßig neue Daten der integrierten Verzeichnisdienste (einschließlich AMBIX)
  - Wir integrieren gerne Ihr LDAP oder X.500-Verzeichnis: Email genügt
- Zukunft dieser Dienste noch offen

DAASI International

Directory Applications for Advanced Security and Information Management

DFN-Projektergebnisse 2

- 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

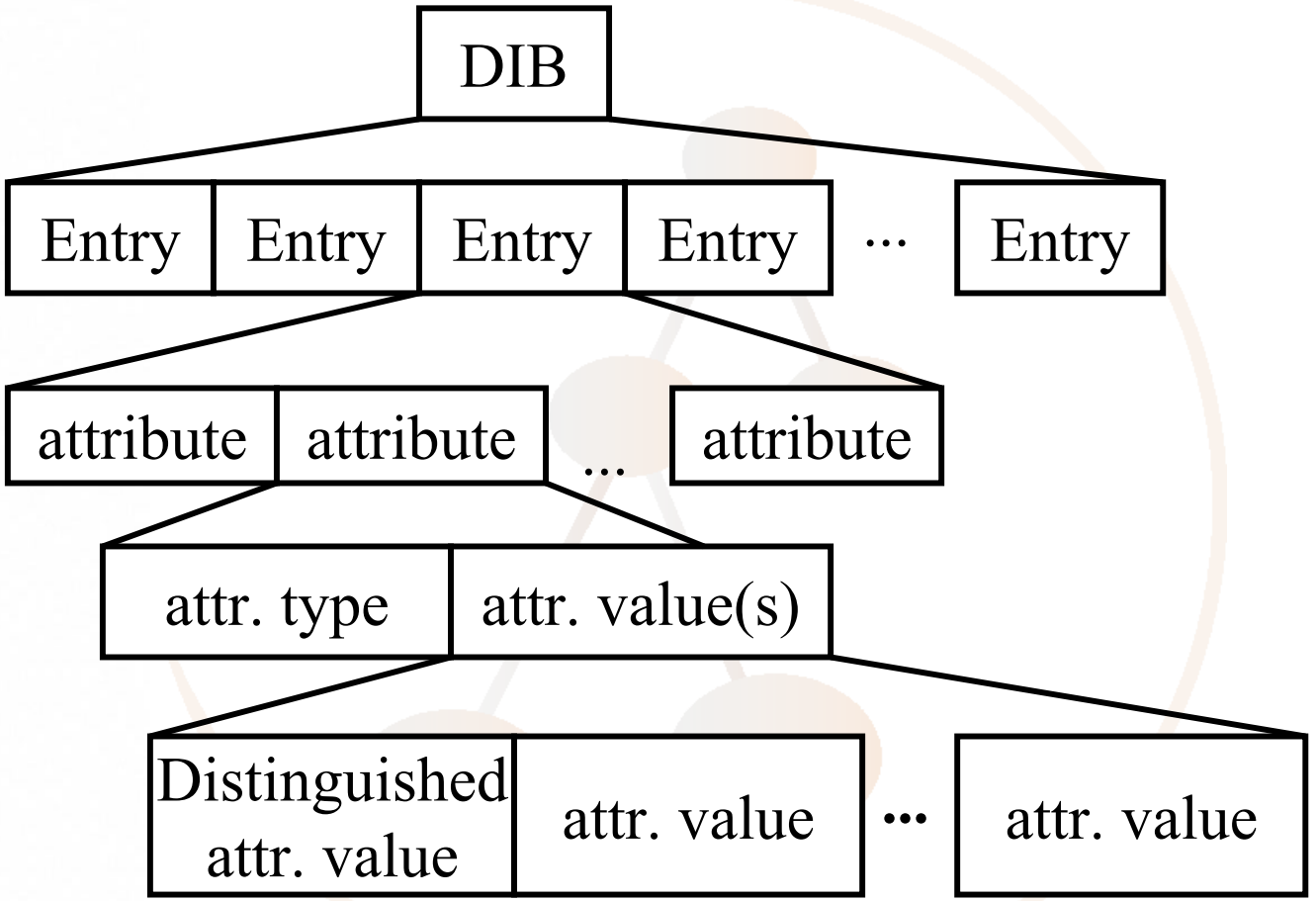
Was ist LDAP

- 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)
- 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

Directory Information Base

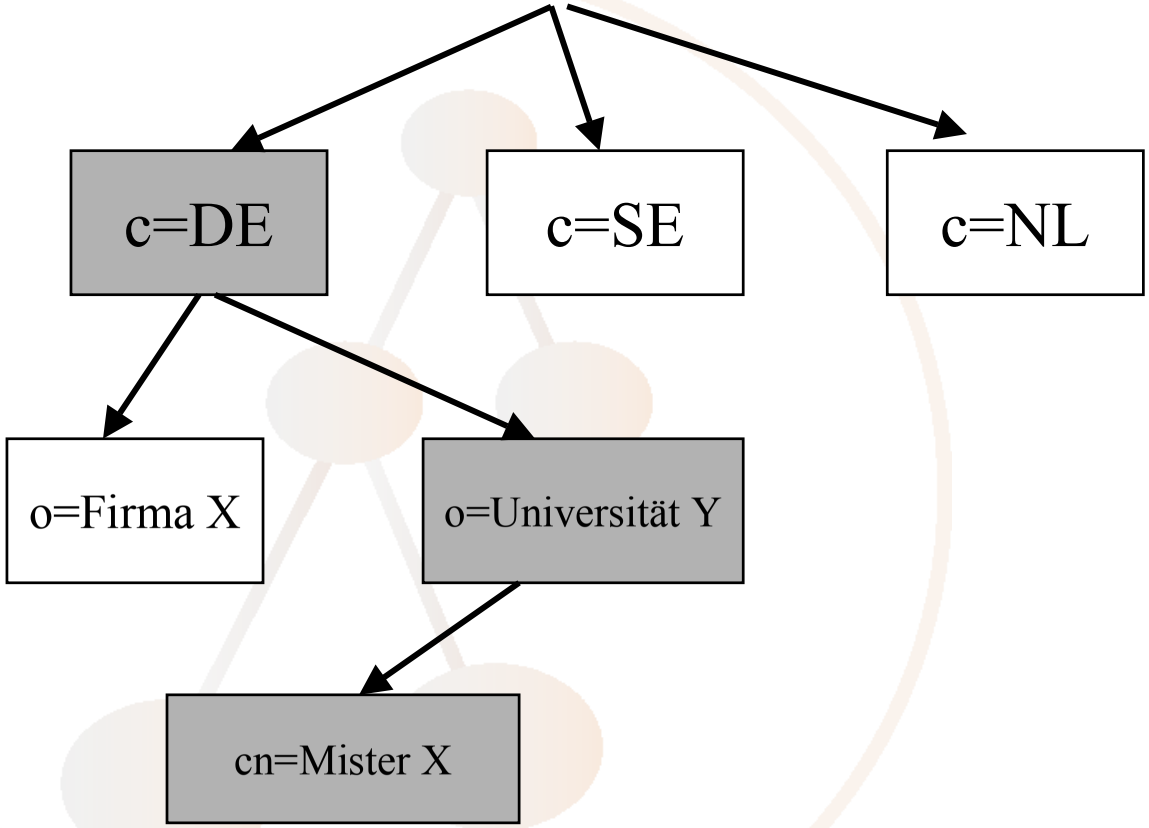


Directory Information Tree (DIT)
(Relative) Distinguished Name (RDN, DN)

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

Open LDAP

- Open Source Implementierung von LDAPv3
- Internationales Entwicklerteam
  - Hauptentwickler Kurt Zeilenga von IBM finanziert
  - Sehr nah an Standardisierungsgremien
  - Stetige Weiterentwicklung
- Wird in vielen Projekten im Produktionsbetrieb eingesetzt
  - Im Forschungsbereich
  - Im kommerziellen Bereich
- http://www.openldap.org

Vorteile von OpenLDAP

- LDAPv3 Standardkonform
- Stabil und performant
- Verschiedene Datenbank-Backends einsetzbar
- Gute Sicherheitsmechanismen (TLS, etc.)
- Gute Zugriffskontrollmechanismen, z.B. abhängig von:
  - Subtree
  - Einzelnen Attributen
  - Authentifizierungsgrad
  - IP-Adresse
- Stabiler Replikationsmechanismus
  - Auch Teilreplikation möglich

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

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

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

- Vorläufer unseres Lösungsansatzes
  - Greenblatt, B., "LDAP Object Class for Holding Certificate Information", Internet Draft (expired), Februar 2000, draft-greenblatt-ldap-certinfo-schema-02.txt
- Die intelligentere aber zu komplexe Lösung
  - Legg, S., "LDAP & X.500 Component Matching Rules", Internet Draft (work in progress), October 2002, draft-legg-ldapext-component-matching-09.txt
  - Chadwick, D. and S. Mullan, "Returning Matched Values with LDAPv3", Internet Draft (work in progress, expired), June 2002, draft-ietf-ldapext-matchedval-06.txt

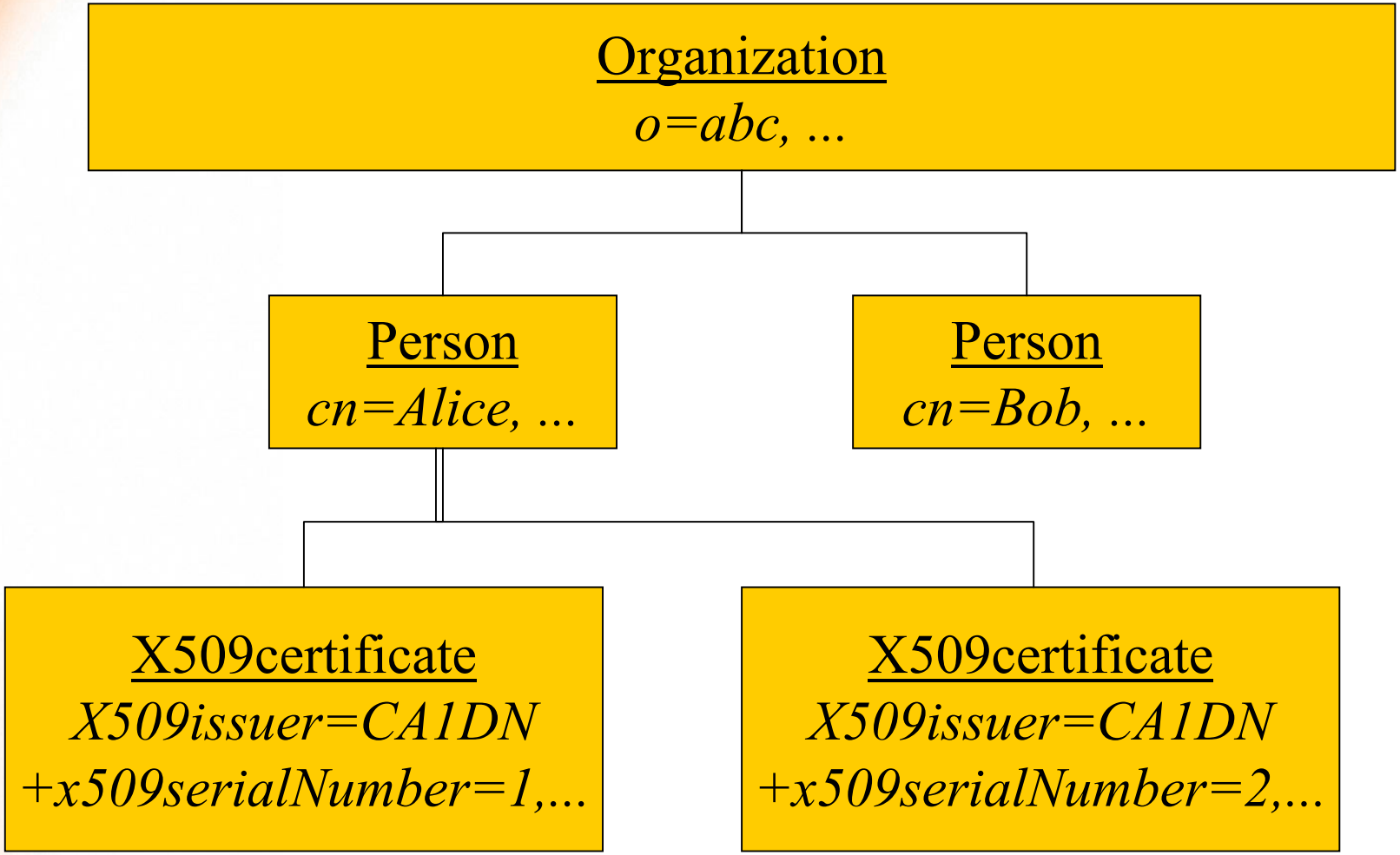
Neuer Vorschlag

- Unsere Lösung:
  - IETF-Draft: Gietz, Klasen, An LDAPv3 Schema for X.509 Certificates
  - Jedes Zertifikat wir in einem eigenen Eintrag gespeichert
  - Zusätzlich zum Zertifikat werden Inhalte der wichtigsten Zertifikatsfelder in LDAP Attributen abgelegt („Metadaten-Ansatz“)

Vorteile

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

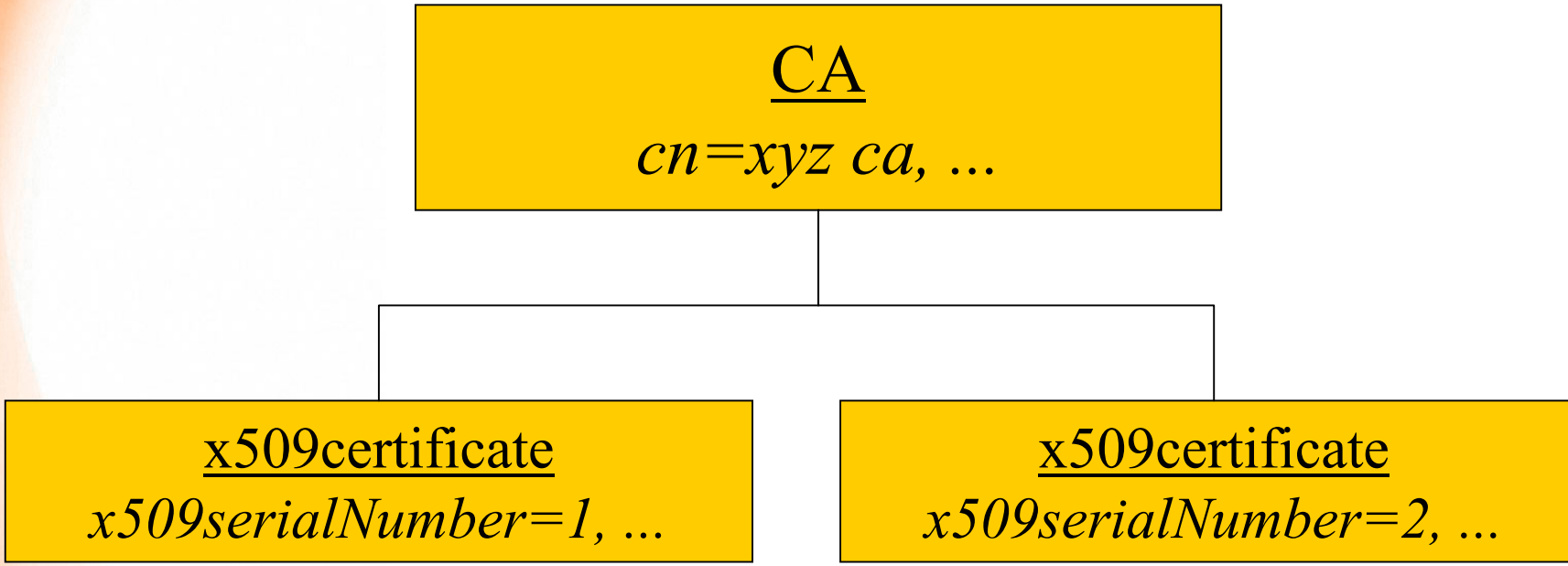
DIT-Struktur im Personenverzeichnis



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

objectclass (1.3.6.1.4.1.10126.x..x..x NAME 'x509certificate' ABSTRACT
MUST (x509serialNumber $ x509signatureAlgorithm
$ x509issuer $ x509validityNotBefore $ x509validityNotAfter
$ PublicKeyInfoAlgorithm)
MAY (mail $ x509authorityKeyIdentifier $ x509authorityCertIssuer
$ x509authorityCertSerialNumber $ x509subjectKeyIdentifier
$ x509keyUsage $ x509policyInformationIdentifier
$ x509subjectAltNameRfc822Name $ x509subjectAltNameDnsName
$ x509subjectAltNameDirectoryName $ x509subjectAltNameURI
$ x509subjectAltNameIpAddress $ x509subjectAltNameRegisteredID
$ x509isssuerAltNameRfc822Name $ x509isssuerAltNameDnsName
$ x509isssuerAltNameDirectoryName $ x509isssuerAltNameURI
$ x509isssuerAltNameIpAddress $ x509isssuerAltNameRegisteredID
$ x509extKeyUsage $ x509FullcRLDistributionPoint
$ x509certHolder))

DAASI International
Directory Applications
for Advanced Security
and Information Management

Datenmodell 2

- **Zwei von der abstrakten Objektklasse abgeleiteten Klassen:**

objectclass (x.x.x.x NAME '**x509userCertificate**'
SUP x509certificate
MUST x509userCert MAY x509subject)

objectclass (x.x.x.x NAME '**x509cACertificate**'
SUP x509certificate
MUST x509cACert $ x509subject)

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“

- Komplementär-Texte zu CRLs und Attributzertifikaten:
  - Chadwick, D. W., Sahalayev, M. V., Internet X.509 Public Key Infrastructure LDAP schema for X.509 CRLs, draft-ietf-sahalayev-pkix-ldap-crl-schema-00.txt, February 2003
  - Chadwick, D. W., Sahalayev, M. V., Internet X.509 Public Key Infrastructure LDAP Schema for X.509 Attribute Certificates, draft-ietf-pkix-ldap-ac-schema-00.txt, February 2003
- Entwicklung eines „Proxy-Servers“, der zwischen neuem Schema und altem Standard übersetzt von David Chadwick, University of Salford, im Rahmen eines TERENA-Projekts

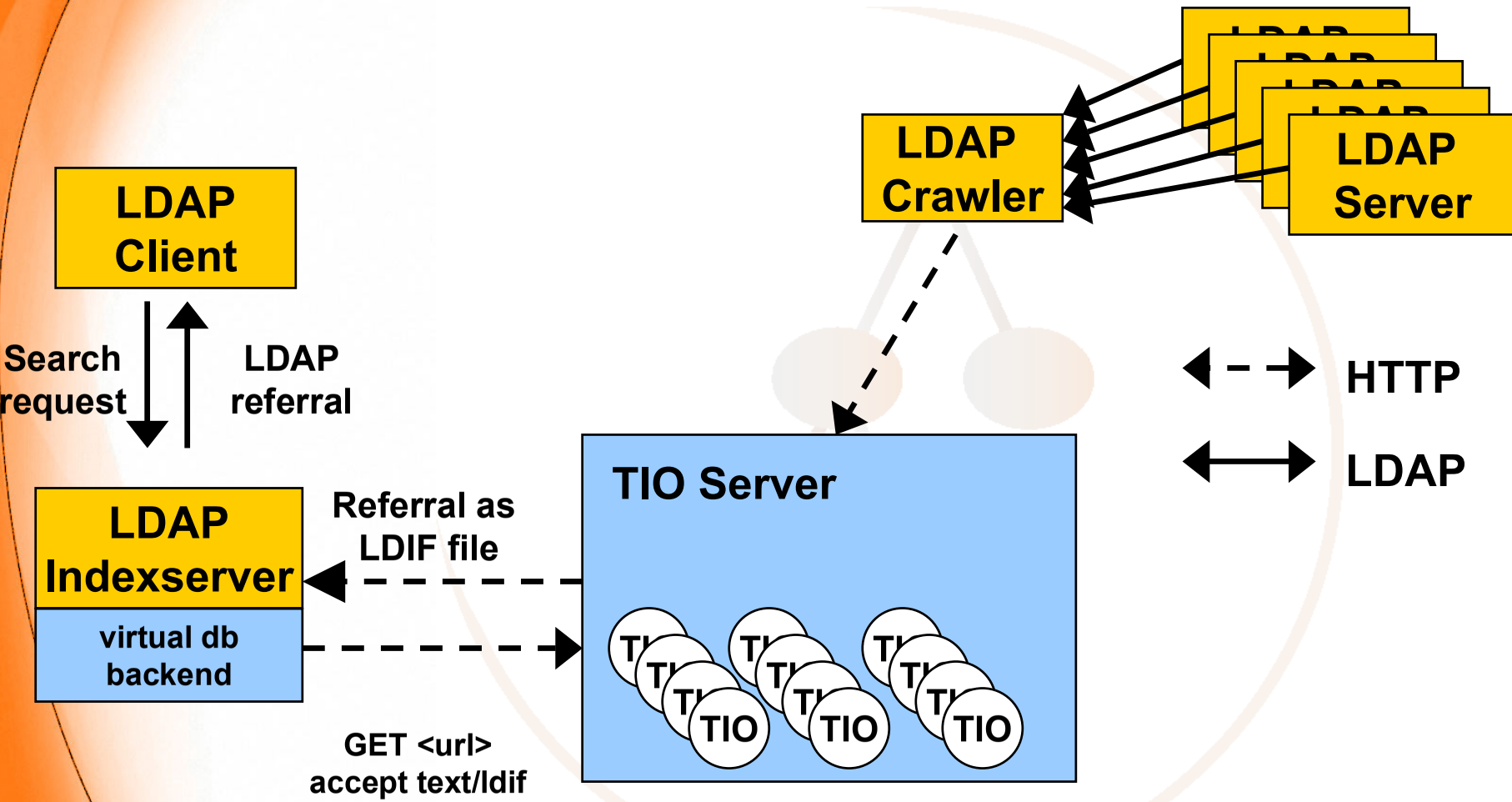
DAASI International

Directory Applications for Advanced Security and Information Management

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

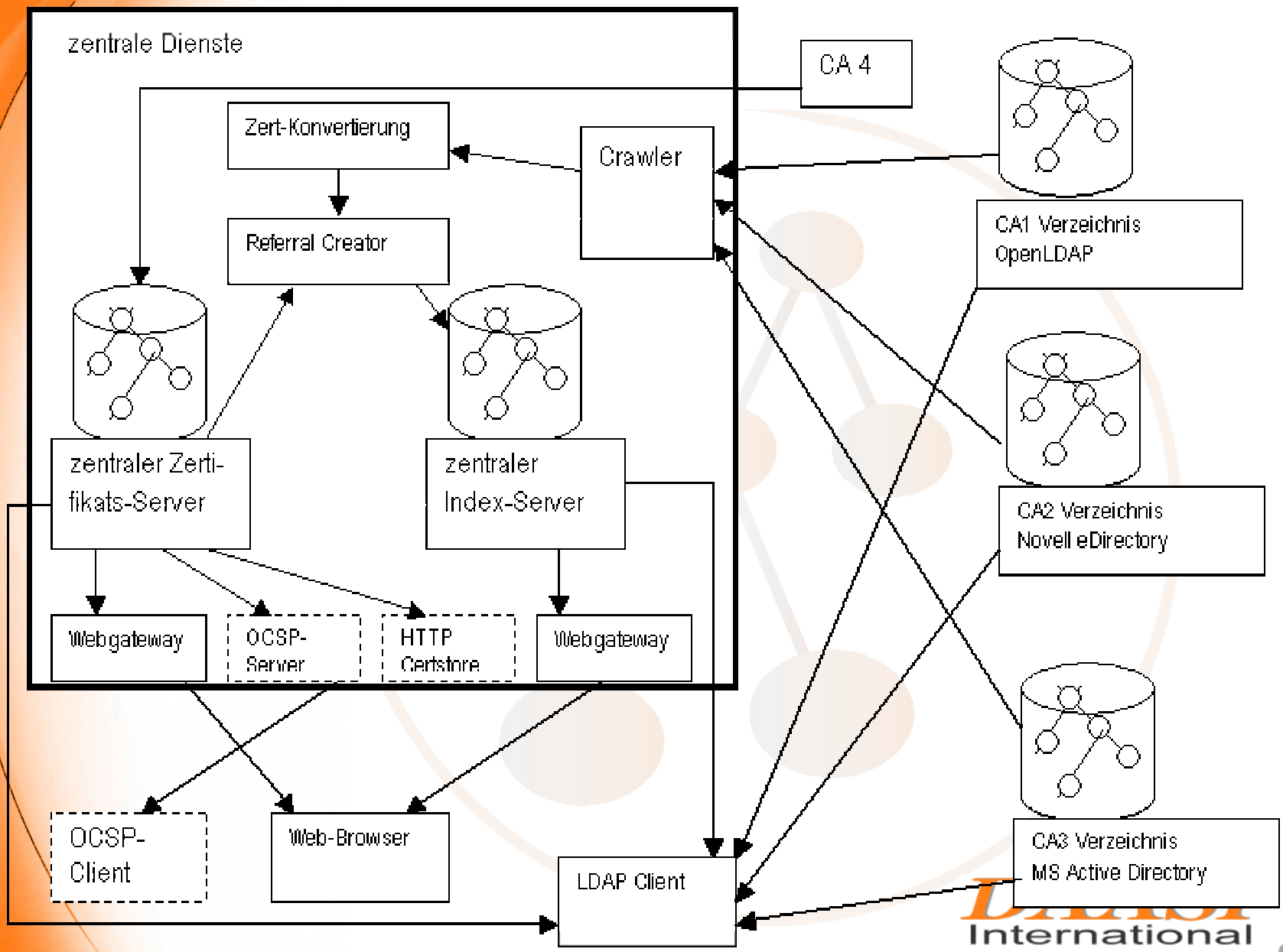
Directory Applications
for Advanced Security
and Information Management

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

Was tun?

- Arbeitsgruppe bilden
- In DFN-Mitgliedsversammlung diskutieren
- Projekt-Konzept entwickeln
  - CA-Verbund oder eine zentrale CA mit Registration Authorities (RAs) an den Organisationen

DAASI International

Directory Applications
for Advanced Security
and Information Management

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