

# Projekt PKI-LDAP

## Das Teilprojekt Zentrale Server

Treffen des ZKI Arbeitskreis Verzeichnisdienste,  
Ilmenau, 15.-16.12.2004

Peter Gietz, CEO, DAASI International GmbH  
[Peter.gietz@daasi.de](mailto:Peter.gietz@daasi.de)



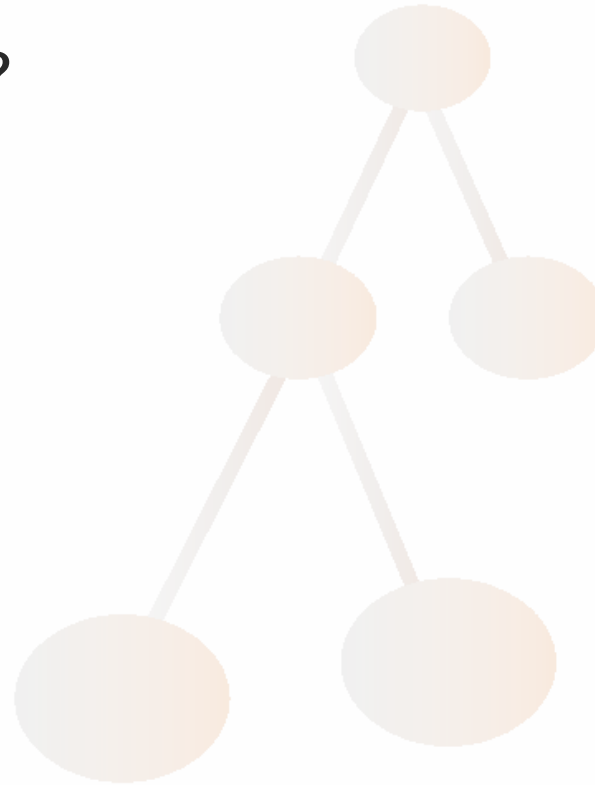
**DAASI**  
International

Directory Applications  
for Advanced Security  
and Information Management



# Agenda

- PKI/LDAP Projekt in Baden Württemberg
- LDAP und PKI
- DFN-weite PKI?



# PKI/LDAP Projekt in Baden Württemberg



# 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



# 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



# 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



# LDAP als Zertifikatsserver



# 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, July 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 shouldn't deploy PKI widely without an accompanying directory plan”*



# 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
- Abstraktes 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 Wert „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-Szenarios einsetzen
- Dennoch ist Compound Matching eine zukunftssträchtige 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 wird 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, „Metadaten“, etc. in Planung

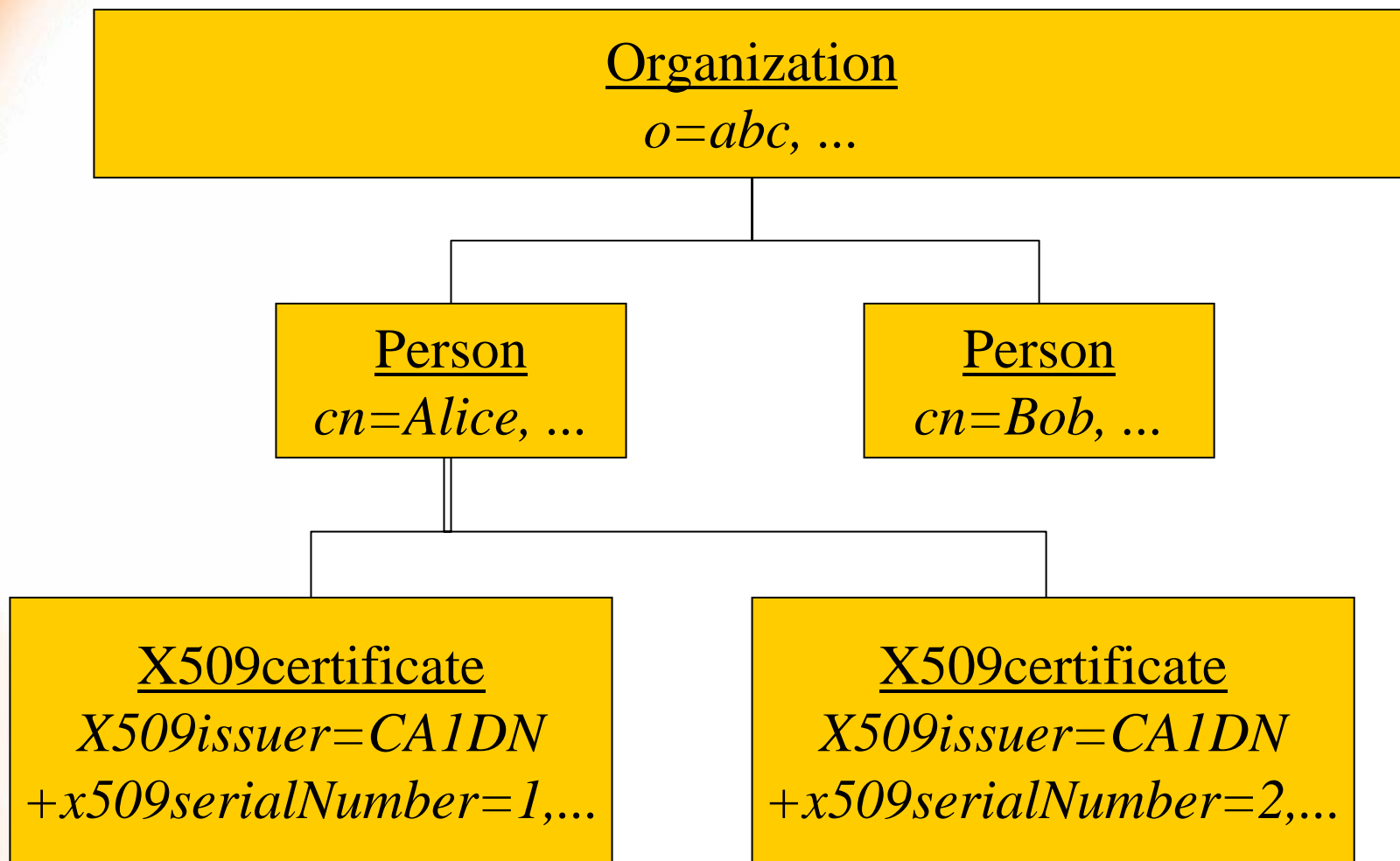


# Vorteile

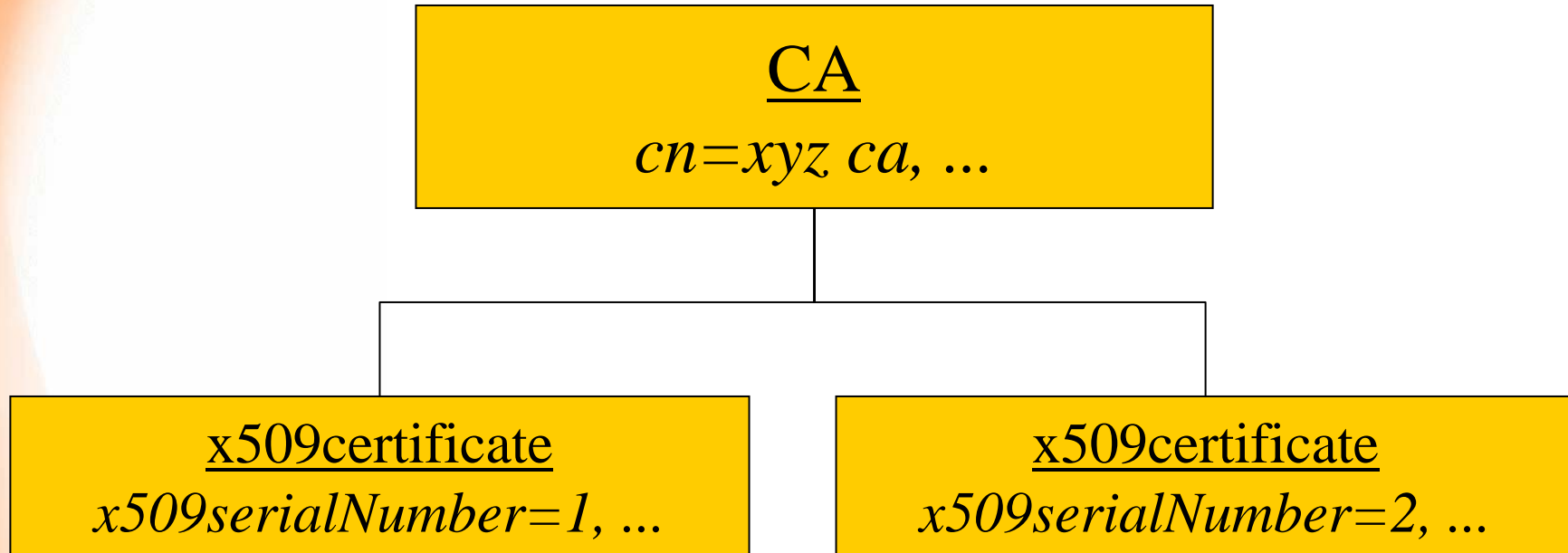
- Lösung lässt sich mit bestehenden Servern implementieren
- Anpassung der Clients ist einfach, da nur der (einfache) Suchfilter modifiziert werden muss
- Flexibilität bei der DIT-Struktur
- Die Zertifikate können im Rahmen eines Indexsystems indiziert werden



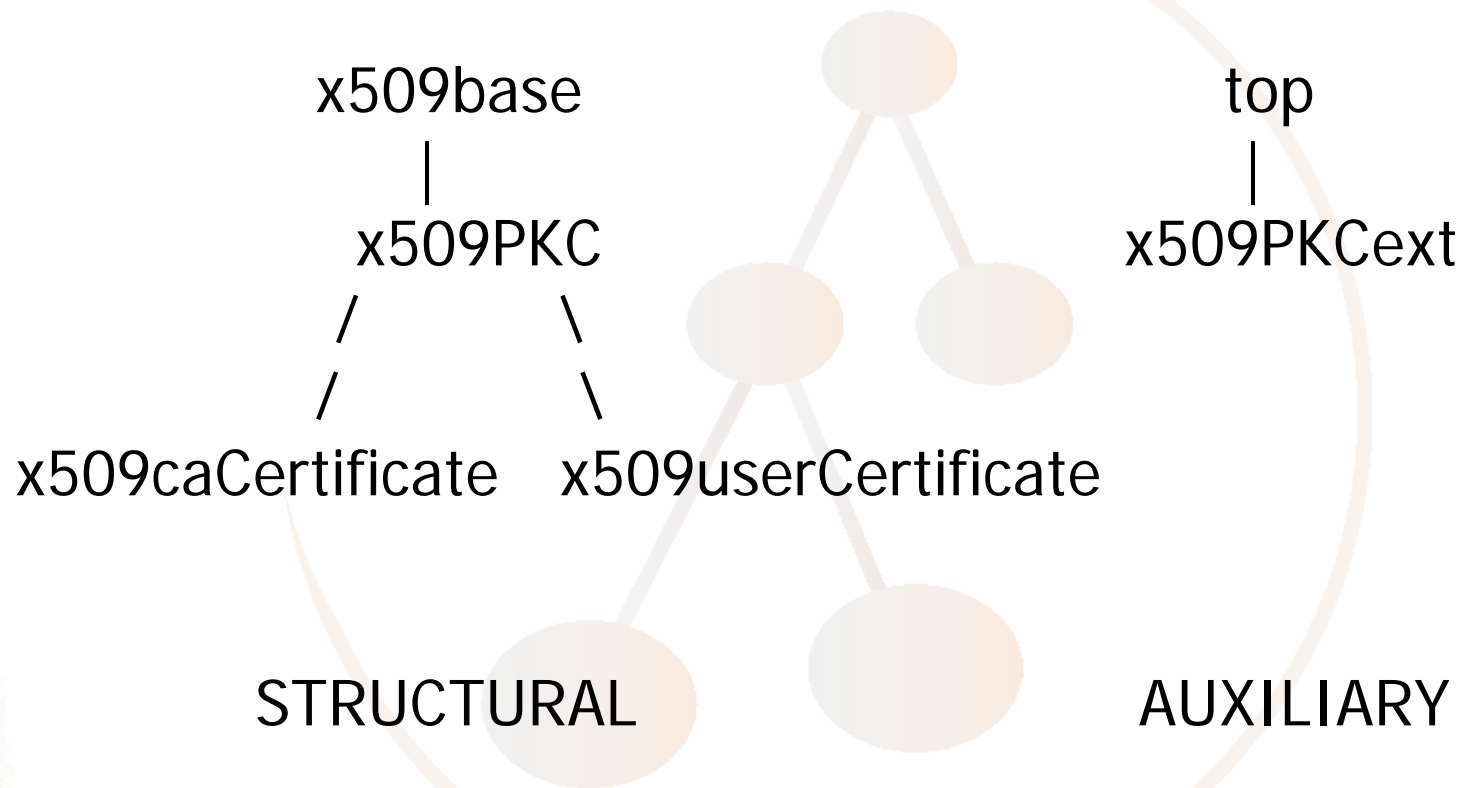
# DIT-Struktur im Personenverzeichnis



# DIT-Struktur im Zertifikatsverzeichnis



# Das Datenmodell: Objektklassenvererbung



# 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 ) )



# 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

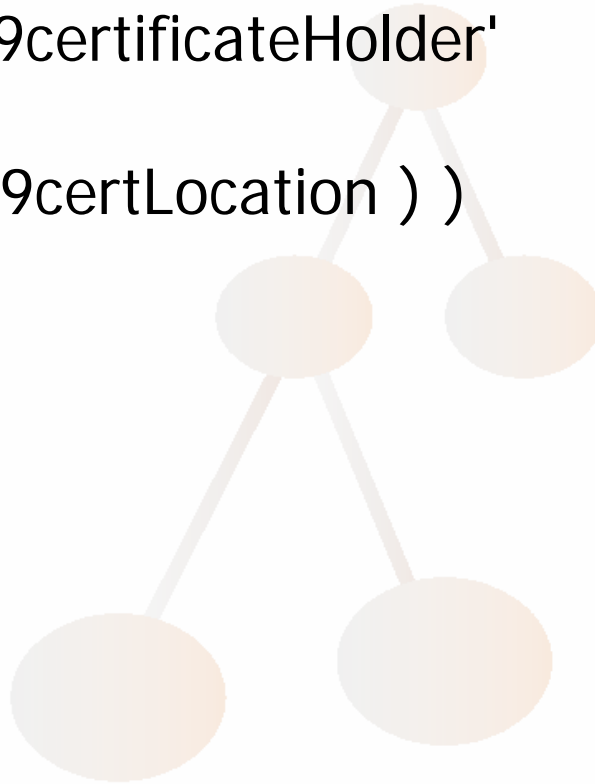
MAY ( x509authorityKeyIdentifier \$ x509authorityCertIssuer \$  
x509authorityCertSerialNumber \$ x509subjectKeyIdentifier \$  
x509keyUsage \$ x509policyInformationIdentifier \$  
x509subjectRfc822Name \$ x509subjectDnsName \$  
x509subjectDirectoryName \$ x509subjectURI \$  
x509subjectIpAddress \$ 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 ) )



# 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

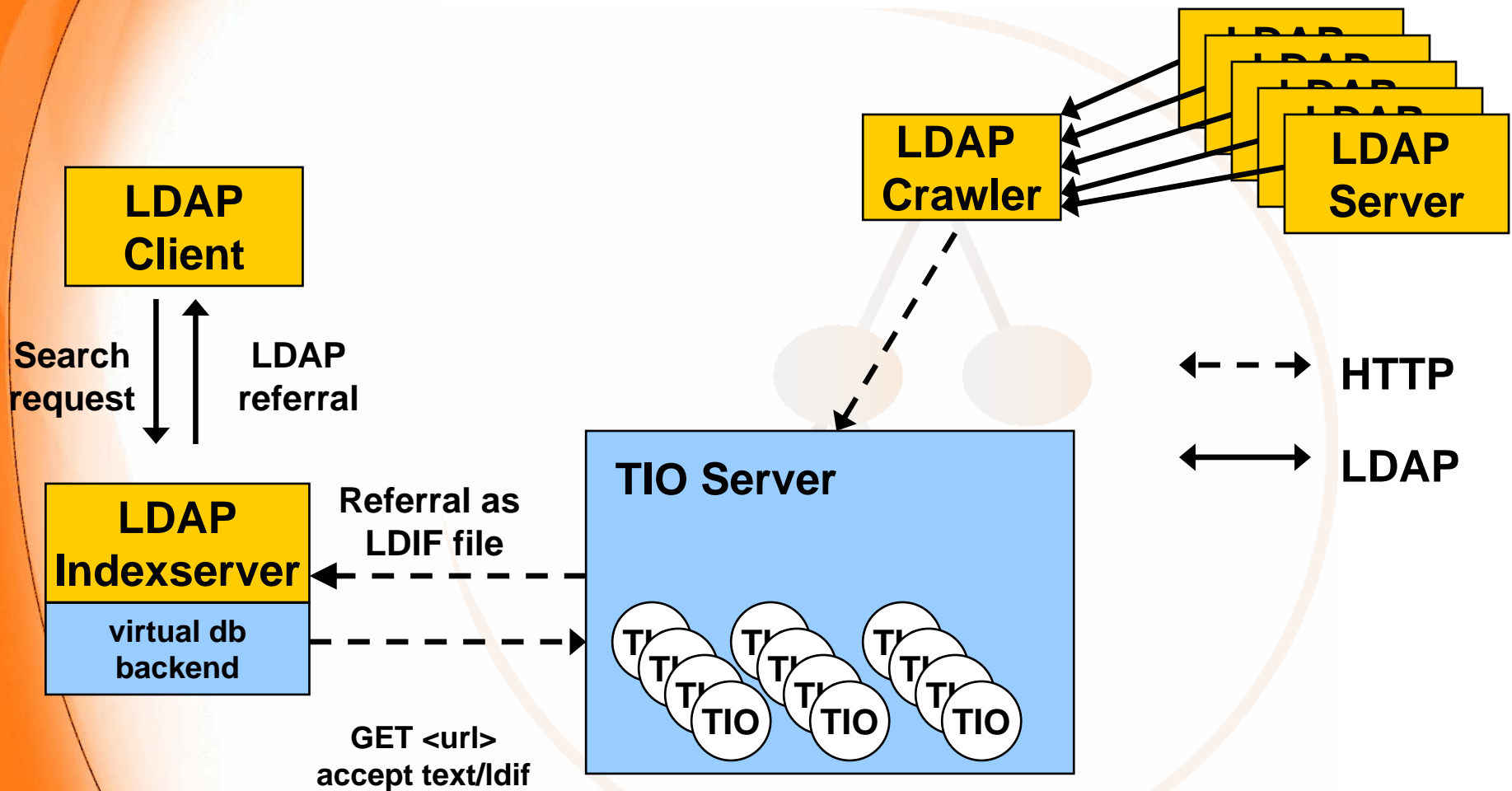


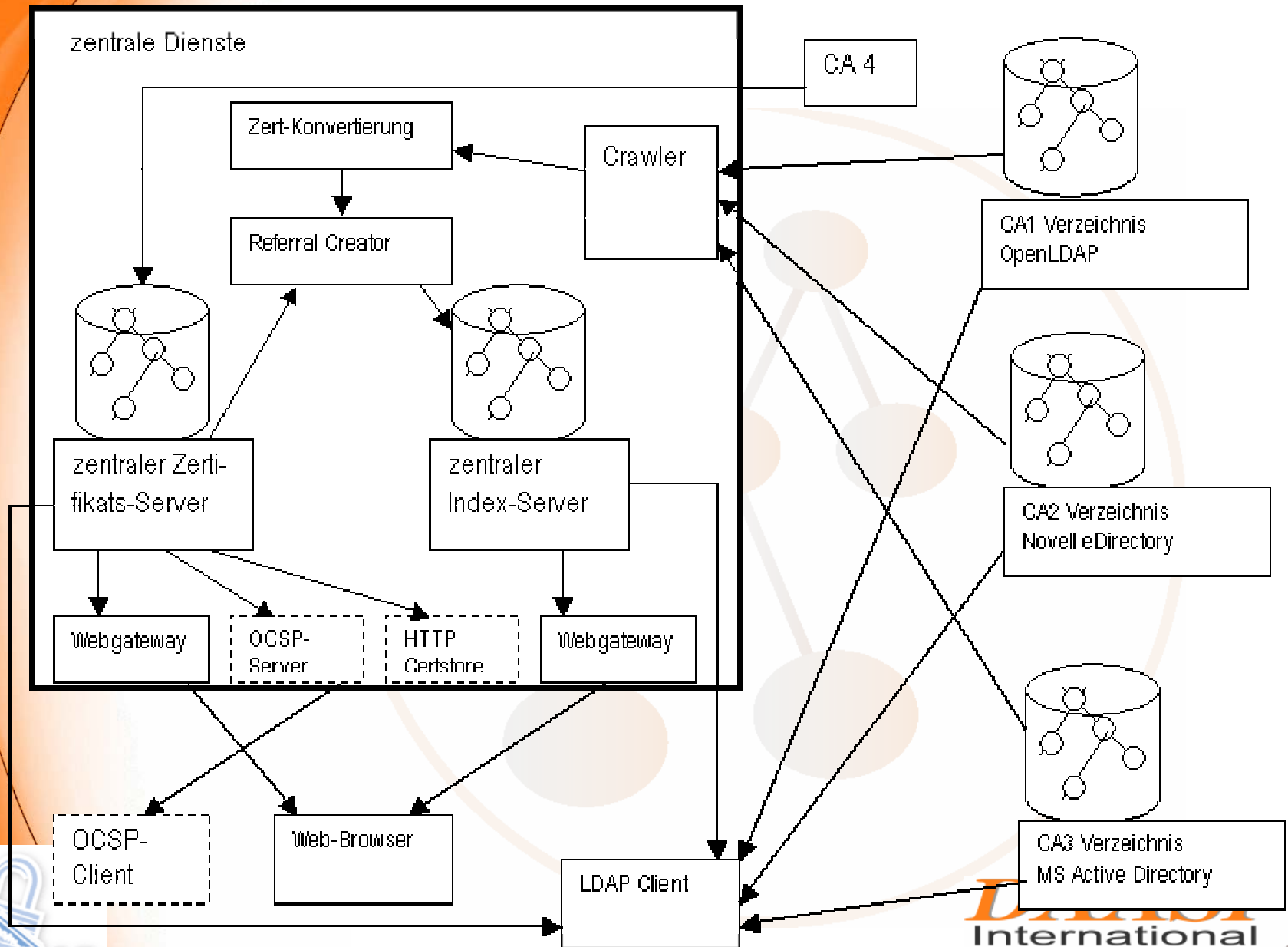
# Weitere Einsatzmöglichkeit

- 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

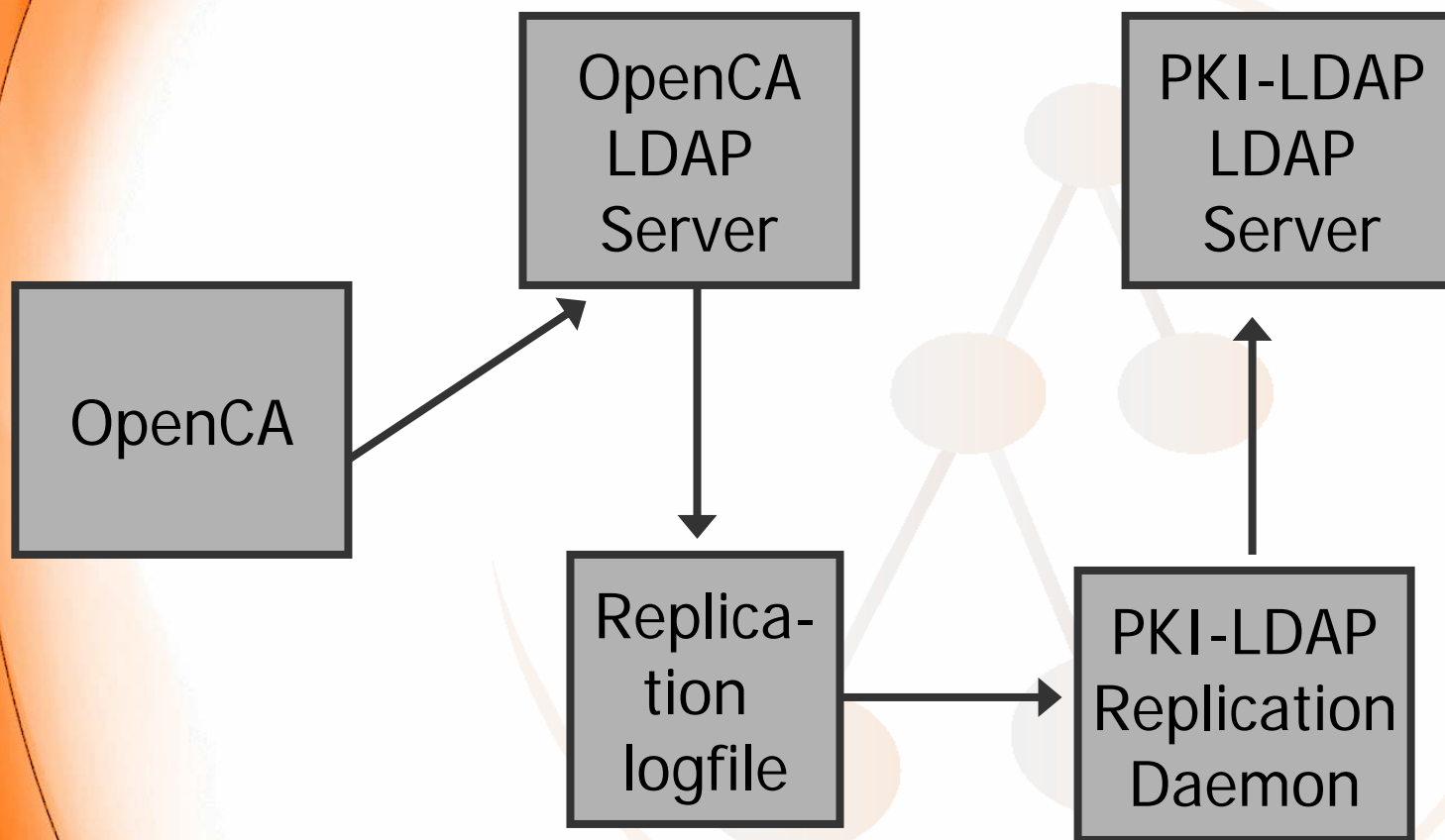


# Common Indexing Protocol Architektur





# Integration in OpenCA



# 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 (Privileged 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](mailto:Info@daasi.de)
- DFN Directory Services:  
<http://www.directory.dfn.de>  
[Info@directory.dfn.de](mailto:Info@directory.dfn.de)

