Verzeichnisdienst-Projekte im DFN
Geschichte, Status und Ausblicke

DFN Betriebstagung
Berlin, 12.11.2002

Peter Gietz, CEO, DAASI International GmbH
Peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management

Agenda

- AMBIX
  - Konzept
  - Datenschutz
  - Geschichte
  - AMBIX2002
  - Betrieb
- X.500
- DFN Directory Services
- Status des aktuellen Projekts
- Rückblick
- Ausblick

DAASI International

Directory Applications
for Advanced Security
and Information Management

AMBIX-D

- Erstes DFN Verzeichnisdienstprojekt an der Universität Tübingen beginnt April 1994
- Aufnahme von Mail-Benutzern in das X.500 Directory
- Aufbau eines Verzeichnisdienstes für alle DFN-Mitglieder, die nicht selber eines betreiben
- Selbsteintragsmöglichkeit via Webformular

DAASI International

Directory Applications
for Advanced Security
and Information Management

AMBIX und Datenschutz

- Durch Widerspruchsverfahren größere Datenbasis
- Lieferung der personenbezogenen Daten durch Organisationen über einfache ASCII basierte Datenformate
- Benachrichtigung der Betroffenen durch Email vom Projekt
  - Datenschutzinformation
- Folgende Optionen für den Benutzer:
  - Möglichkeit Daten zu ändern
  - Veröffentlichung zustimmen
  - Veröffentlichung widersprechen
  - Alle Daten löschen lassen

DAASI International

Directory Applications
for Advanced Security
and Information Management

AMBIX und Datenschutz (2)

- Es wird nur ein Minimaldatensatz gespeichert
- Der Export der Daten in Länder, die keinen adäquaten Datenschutz haben, wird verhindert
  - Überprüfung durch reverse lookup im DNS
  - Nur Country Code Top Level Domains (ccTLD)
    - .de, .nl, .it, .es, ...
  - Nur registrierte Proxies erlaubt
- Crawler von potentiellen Spammern werden erkannt und abgewiesen
- Spamfänger
  - Spezielle Scheineinträge eingefügt, deren Emailadresse sonst nirgends veröffentlicht sind
  - Bisher haben wir kein Spam auf diesen Adressen erhalten!

DAASI International

Directory Applications
for Advanced Security
and Information Management

AMBIX - Implementationsgeschichte

- 4 Software Generationen:
  - AWK-Server <-> C-Clients <-> X.500
  - RPC fähiger C-Server <-> C-Client <-> X.500
  - LDAPv2 Server <-> Perl Clients
  - LDAPv3 Server <-> Perl Clients (neue features)
- Zugang der Benutzer von Anfang an über WWW

DAASI International

Directory Applications
for Advanced Security
and Information Management

AMBIX 2002

- Neudesign der Software und Weboberfläche
- LDAPv3 auf OpenLDAP-Basis
- Neues Schema: dfnOrgPerson, dfnOrganization, ...
- Integration neuer Sichtbarkeitsoptionen
  - Nur in eigener Domain
  - Nur in Deutschland
  - Nur in datenschutztreibende Länder
  - Weltweit
- Crawler detection verbessert
- In Kürze die verschobene „PR-Aktion“ um für neue Teilnehmerorganisationen zu werben

DAASI International

Directory Applications
for Advanced Security
and Information Management

AMBIX Betrieb

- Kontinuierlicher Betrieb seit 1995
- Über 62.000 Datensätze
- Tausende von Emails beantwortet:
  - Bug reports
  - Fragen zu AMBIX, wie „warum sehe ich keine Personendaten“ -> Kurzeinführungen in DNS und Proxies
  - Anfragen zu Studiengängen
  - Geneaologische Anfragen
  - Spam
  - Kuriosa

DAASI International

Directory Applications
for Advanced Security
and Information Management

DFN Directory Services DDS

- Verzeichnisdienst-Kompetenzzentrum zur Beratung von Forschungsinstituten in Deutschland
- Anlaufstelle für Directory-Fragen
- Informationen zu X.500 und LDAP
- X.500 Software support und Betrieb des Country level DSA
- Koordinierte Umstellung von X.500(88) auf X.500(93)
- Am Kompetenzzentrum wurden zwei Diplomarbeiten zu LDAP betreut

DAASI International

Directory Applications
for Advanced Security
and Information Management

DDS und Puma

- Betrieb des Country level DSA im Rahmen des europäischen Projekts NameFLOW
  - von der TU-Chemnitz übernommen
- Betrieb und support der vom DFN lizensierten Software:
  - Verschiedene ISODE Quipu Versionen (X.500(88))
  - X.500(93) Software von Messaging Direct (Nachfolgeorganisation von ISODE)
- BTW: Isode ist kürzlich wieder auferstanden; Steve Kille meldet sich zurück

DAASI International

Directory Applications
for Advanced Security
and Information Management

DDS - Deutschlandweiter Index

- Deutschlandweiter X.500/LDAP Index
- Crawler holt regelmäßig neue Daten der integrierten Verzeichnisdienste
- Insgesamt ca. 120.000 Datensätze
- Integration des AMBIX Systems
- Wir integrieren gerne Ihr LDAP oder X.500-Verzeichnis: Email genügt

DAASI International

Directory Applications
for Advanced Security
and Information Management

DDS – DFN-Vertretung in Gremien

- International:
  - NameFLOW Projekt (DANTE)
  - TERENA Task Force LDAP Service Deployment
  - Andere TERENA Aktivitäten, z.B. Middleware Workshop
  - IETF
- National:
  - Beratung im Rahmen des Signaturgesetzes
  - TeleTrusT AG7 PKI
  - DFN-BTs

DAASI International

Directory Applications for Advanced Security and Information Management

DDS – Neue Organisationsform

- Betriebliche Arbeiten können nicht dauerhaft über Forschungsprojektmittel finanziert werden!
- Verschiedene Konzepte wurden angedacht:
  - An-Institut an der Universität Tübingen
  - Gemeinnützige GmbH mit Uni Tü und DFN als Gesellschafter
  - Kommerzielle GmbH mit DFN als Gesellschafter
  - Weil alles andere nicht geklappt hat: GmbH der Familie Gietz

DAASI International

Directory Applications
for Advanced Security
and Information Management

DAASI International GmbH

- Wir bieten:
  - Consulting
  - Design
  - Implementierung
  - Schulung
- Aber auch:
  - Serverhosting
  - Datenmanagement
- Technologische Expertise in:
  - Verzeichnisdiensttechnologien
  - PKI
  - Informationsmanagement (XML)

DAASI International

Directory Applications
for Advanced Security
and Information Management

Technologie-Unabhängigkeit

- Offene Standards
- Open Source Software
- Produktunabhängigkeit
- Aber auch Expertise in anderen Verzeichnisdiensttechnologien
  - X.500 Implementierungen
  - Andere LDAP Implementierungen (Sun, Netscape, IBM)
  - Active Directory
  - Novell Directory Services

DAASI International

Directory Applications
for Advanced Security
and Information Management

Kundenzielgruppen

- Durch Kontakte und Erfahrungen sind deutsche Forschungseinrichtungen die Hauptzielgruppe
  - Wir kennen die Probleme der organisatorischen Abläufe an Universitäten
  - Wir kennen die Bedürfnisse und die zu integrierenden Altsysteme
  - Durch OpenSource Software können wir Ihnen günstige Angebote machen
- Gesundheitswesen
- Behörden auf allen Ebenen
- Mittelständische Betriebe

DAASI International

Directory Applications
for Advanced Security
and Information Management

Universitätsprojekte

- Elektronisches Telefon- und Mitarbeiterverzeichnis an der Universität Tübingen
  - X500.uni-tuebingen.de
  - Datenmanagement
  - Produktion des gedruckten Telefonbuchs
- Aufbau eines Mitarbeiterverzeichnisses an der Universität Münster
- Bedarfsanalyse zu einem Metadirectory am Universitätsklinikum Tübingen

DAASI International

Directory Applications
for Advanced Security
and Information Management

Forschung

- Weitere Beteiligung an der Forschung und Standardisierung
  - TERENA
  - IETF
  - Global Grid Forum
  - Digital Library Bereich
  - Forschungs- und Entwicklungsprojekte
    - In Europa, im Bund und in den Ländern
  - PKI Initiativen der deutschen Industrie (Teletrust)
  - Verzeichnisdienstkonzept der PKI-1 der Verwaltung

DAASI International

Directory Applications
for Advanced Security
and Information Management

TERENA

- Europäische Vereinigung der Nationalen Forschungsnetze (DFN, SurfNet, etc.)
- Forschung und Pilotierung von Netztechnologien und –Anwendungen
  - Konferenzen
  - Projekte
  - Task Forces
- www.terena.nl

TERENA und Verzeichnisdienste

- TF-LSD: Task Force LDAP Service Deployment
  - Charter: www.terena.nl/task-forces/tf-lsd
  - Koordiniert Aktivitäten zu
    - LDAP-Index-basierten Europäischen White-Pages-Verzeichnisdienst
    - PKI-Koordinierung (in Zusammenarbeit mit TF-AACE, Authentication and Authorisation Coordination in Europe)
- Projekt DEEP (DAASI International)
  - Development of an European EduPerson
  - Phase 1 Bedarfsanalyse via Webfragebogen
  - www.daasi.de/surveys/DEEP

DAASI International

Directory Applications
for Advanced Security
and Information Management

TERENA und Verzeichnisdienste (2)

- Projekt LDAP Schema Registry (DAASI Int.)
  - Informationssystem zum Auffinden bzw. Registrieren von definierten Schemata
  - Policy für Datenaufnahme
    - Bedingung: gute Metadaten
    - OpenLDAP basierte Datenbank
    - Standardschema basiert
  - WWW.daasi.de/projects/Schemaregistry

DAASI International

Directory Applications
for Advanced Security
and Information Management

DFN Projekt – letzte Phase

- Konzentration auf Anwendungen
- Weiterbetrieb der Dienste
- 2 Teilprojekte
  - LDAP basiertes Unified Login
  - PKI Zertifikatsserver

DAASI International

Directory Applications
for Advanced Security
and Information Management

Unified Login

- Problem:
  - Benutzer haben Zugriff auf viele Rechner
  - Auf jedem Rechner eigene LoginID und Passwort
  - Benutzer muss sich viele Passwörter merken
  - Unterschiedliche Password-Policies
  - ➔ sehr hoher Administrationsaufwand

DAASI International

Directory Applications
for Advanced Security
and Information Management

Unified Login (2)

- Lösung:
  - Zentraler verzeichnisdienstbasierter Authentifizierungsdienst
  - Unix-Clients
    - Können mittels NSS / PAM-LDAP direkt auf LDAP-Server zugreifen
    - Aber auch Anbindung an MS Active Directory (AD) möglich mit Kerberos
  - Windows-Clients
    - Einfache Integration in AD
    - Aber auch über SAMBA Anbindung an LDAP-Server möglich

Unified Login (3)

- Mit dem Authentifizierungsdienst lässt sich nicht nur das Login realisieren
- Er lässt sich auch in verschiedene Netzanwendungen integrieren, z.B.:
  - IMAP, POP, SMTP auth, FTP, HTTP auth, RSH, SSH, etc. etc.
- Single Sign On (SSO)

Unified Login (4)

- Vorteil:
  - Ein Passwort für alle Rechner
    - Der User muss sich weniger merken
    - Der Administrator wird erheblich entlastet
- Nachteil:
  - Ein Passwort für alle Rechner
    - Single point of failure
    - Größerer Schaden bei Kompromittierung

Zertifikatsserver für PKI

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 should'nt deploy PKI widely without an accompanying directory plan"

DAASI International

Directory Applications for Advanced Security and Information Management

Zertifikatsserver für PKI (2)

- Veröffentlichungsmedium für öffentliche Schlüssel bzw. Zertifikate
  - Um ohne vorherige Kommunizierung von Schlüsseln für jemanden ein Dokument zu verschlüsseln, das nur mit dessen privatem Schlüssel entschlüsselt werden kann
  - Um eine mit dem privaten Schlüssel generierte digitale Signatur überprüfen zu können
- Im Zertifikat wird die zu einem öffentlichen Schlüssel zugehörige Identität von einer vertrauenswürdigen Stelle (Certification Authority, CA) durch digitale Signatur bestätigt

Zertifikatsserver für PKI (3)

- Der Verzeichnisdienst
  - hält Zertifikate im Netz vor, auf die Standardanwendungen (S/MIME und PGP) zugreifen können
  - dokumentiert zurückgerufene Zertifikate in sog. Certificate Revocation Lists (CRL)
  - kann somit Grundlage eines Online Certificate Status Protocol (OCSP) Dienstes bilden
- Entweder betreibt eine CA den Verzeichnisdienst selber, oder liefert Zertifikate auf einem gesicherten Weg an den Betreiber

Neuer Vorschlag

- userCertificate ist das bereits standardisierte Attribut zum Speichern des Zertifikats
- Problem:
  - 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
- Unsere Lösung:
  - Metadaten-Ansatz: Zusätzlich zum Zertifikat werden Inhalte der wichtigsten Zertifikatsfelder in LDAP Attributen abgelegt

Vorteile

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

DAASI International

Directory Applications
for Advanced Security
and Information Management

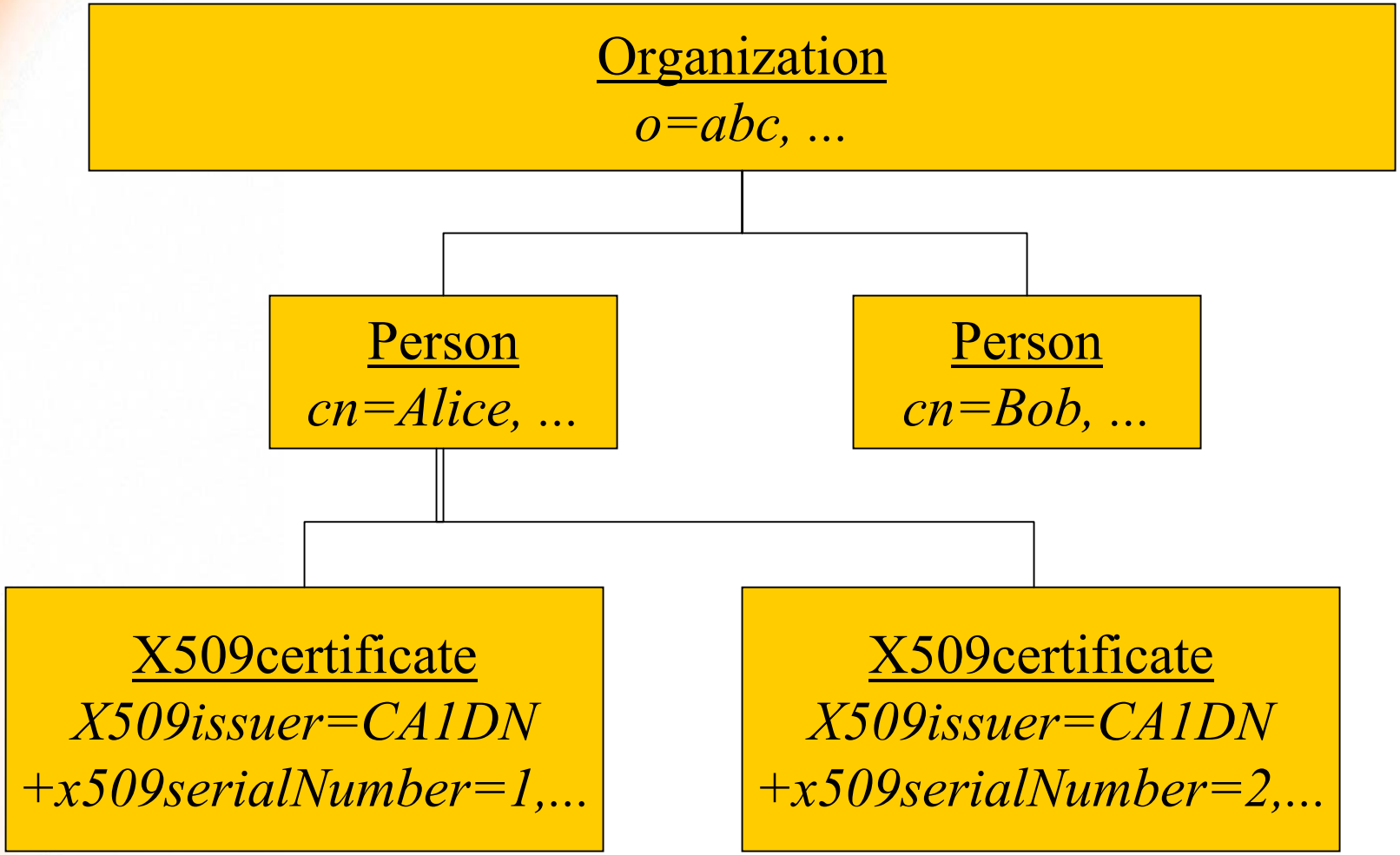
Objektklasse: x509certificate

(1.3.6.1.4.1.10126.1.5.4.2.1 NAME 'x509certificate'

MUST (x509serialNumber $ x509signatureAlgorithm $ x509issuer $
x509validityNotBefore $ x509validityNotAfter $
x509subject $ x509subjectPublicKeyInfoAlgorithm)

MAY (mail $ x509subjectKeyIdentifier $ x509keyUsage $
x509policyInformationIdentifier $
x509subjectAltNameRfc822Name $
x509subjectAltNameDnsName $
x509subjectAltNameDirectoryName $
x509subjectAltNameURI $
x509subjectAltNameIpAddress$
x509subjectAltNameRegisteredID $
x509isssuerAltNameRfc822Name $
x509isssuerAltNameDnsName $
x509isssuerAltNameDirectoryName $
x509isssuerAltNameURI $
x509isssuerAltNameIpAddress $
qx509isssuerAltNameRegisteredID $

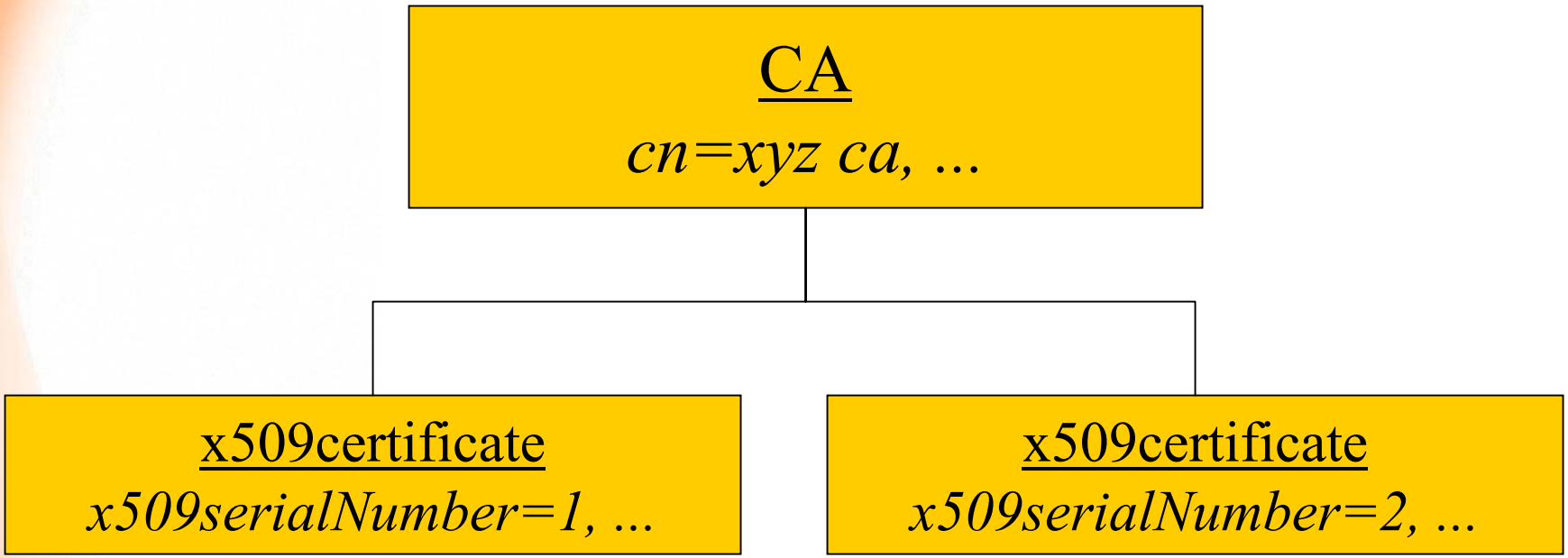
DIT-Struktur im Personenverzeichnis



DAASI International

Directory Applications
for Advanced Security
and Information Management

DIT-Struktur im Zertifikatsverzeichnis



DAASI International
Directory Applications
for Advanced Security
and Information Management

Implementierung

- Schema in OpenLDAP implementiert
- Client, der Zertifikat analysiert und entsprechende Metadaten als LDIF ablegt
- Proof of concept gelungen

DAASI International

Directory Applications
for Advanced Security
and Information Management

Standardisierung

- Erster Draft im Februar eingereicht
- Vortrag beim pkix-Meeting zur 53. IETF
  - Rege Diskussion und Akzeptanz beim Meeting
  - Jedoch nicht auf der Mailingliste (pkix ist sehr beschäftigt)
- Jetzt zweite Version eingereicht
- Plötzlich rege Diskussion mit wertvollen Beiträgen von Leuten wie Russ Housley und Kurt Zeilenga
- Vortrag nächste Woche beim pkix-Meeting zur 55. IETF
- Nächste Version des Drafts in Vorbereitung
  - Eventuell als pkix draft

DAASI International

Directory Applications for Advanced Security and Information Management

Rückblick

- Kooperation mit anderen DFN-Projekten
  - Es wurde uns immer Kooperationsbereitschaft signalisiert (WinShuttle, DFN-PCA)
  - Wenn es aber um aktive Datenlieferungen ging, haperte es: „Zu viel anderes zu tun“
  - Kooperation hätte in den Projektplänen stehen müssen
- Kooperation mit DFN Mitgliedern
  - Zum Teil sehr reibungslos und kooperativ
  - Andere ließen sich nicht motivieren, bei AMBIX mitzumachen

Rückblick (2)

- LDAP-Umfrage war ein Desaster: Nur ein halb ausgefülltes Formular kam zurück
- Kooperation mit DFN Geschäftsstelle
  - Immer gute Kooperation mit Frau Schröder
    - Vielen Dank hierfür
  - Entscheidungsprozesse im DFN kamen in der Regel sehr spät oder gar nicht zustande
  - Neue „AMBIX PR Aktion“ musste bisher zurückgehalten werden

DAASI International

Directory Applications
for Advanced Security
and Information Management

Weiterbetrieb Option 1

- Weiterbetrieb von AMBIX und DE-Index im Rahmen der Video-Conferencing-Aktivitäten des DFN
  - Ergänzung von Informationen für und über VC-Teilnehmer
  - Abbildung der VC-Infrastruktur (Geräte, Gatekeeper, MCUs, etc.) im Verzeichnis
  - Idee eines LDAP basierten VC-Reservierungsdienstes
- Wenn VC-Dienst im Pilotbetrieb kostenfrei ist, muss AMBIX auch vorerst kostenfrei bleiben
- Projekt jedoch ungewiss

DAASI International

Directory Applications
for Advanced Security
and Information Management

Weiterbetrieb Option 2

- Projektidee „Metadirectory Competence Center“
  - Analyse von Anforderungen an Metadirectories im DFN-Umfeld
    - Welche Prozesse sollen unterstützt werden?
    - Personalverwaltung, Studierendenverwaltung
    - Raumbelegungsverwaltung, Elektronisches Vorlesungsverzeichnis
  - Testen, inwieweit aktuelle MD-Software (Siemens, Novell, etc.) im DFN-Umfeld geeignet ist.
  - MD Software auf Open Source Basis erstellen
    - Konnektoren für OpenLDAP
    - z.B. für HIS Datenbanken

DAASI International

Directory Applications for Advanced Security and Information Management

Weiterbetrieb Option 2

- Wir suchen Kooperationspartner für Projekt „Metadirectory Competence Center“
- Antrag direkt beim Projektträger DLR
  - (Deutsches Zentrum für Luft- und Raumfahrt; www.pt-dlr.de/PT-DLR)

DAASI International

Directory Applications
for Advanced Security
and Information Management

Weiterbetrieb insges. 4 Optionen

- 1.) Im Rahmen eines Video-Conferencing-Projekts
- 2.) Im Rahmen eines Metadirectory-Projekts
- 3.) Im Rahmen eines DFN-“Mehrwertdienstes“
- 4.) Im Rahmen von Einzelverträgen zwischen DFN-Mitgliedern und DAASI International

- Ende November wird „PR Aktion“ durchgeführt

DAASI International
Directory Applications for Advanced Security and Information Management

Fazit

Ich glaube, wir könnten dem DFN weiterhin behilflich sein

- DFN Directory Services
  - Ambix2002.directory.dfn.de
  - Directory.dfn.de
  - Info@directory.dfn.de
- DAASI International
  - www.daasi.de
  - Info@daasi.de

DAASI International

Directory Applications for Advanced Security and Information Management