LDAP und die Ablage von PGP–Schlüsseln im X.500–Directory

Kurt Spanier, Zentrum für Datenverarbeitung, Universität Tübingen

Kurt.spanier@zdv.uni–tuebingen.de

Inhalt

- Einführung
- Grundlagen von X.500 und LDAP
- Internationale Ansätze für eine standardisierte Ablage von PGP–Schlüsseln im X.500–Verzeichnis
- Eine »Übergangslösung« für das Projekt AMBIX
- Infos und Kontakte

Sicherheit im Internet

- Kommunikation im Internet braucht Sicherheit: Authentification, Verification, Non−Repudiation, Encryption
- Asymmetrische Schlüsselverfahren (z.B. PGP) brauchen Öffentlichkeit der Public Keys
- Public Keys müssen auffindbar sein
- Ein Verzeichnissystem für Public Keys muß skalieren
- Das internationale X.500−Directory ist ein über LDAP zugängliches, skalierendes Verzeichnissystem

Die Grundlagen von X.500

- X.500 ist ein verteiltes System mit hierarchisch strukturierten Einträgen: z.B. Länder, Organisationen, Unterorganisationen, Personen
- Einträge legen über die Zuordnung zu Objektklassen die nutzbaren Felder (Attribute) für die Ablage von Informationen fest (Attributwerte)
- Namen von Einträgen sind global eindeutig (Directory Name; DN); Relative (Teil−)Namen (RDNs) müssen nur unterhalb desselben Eintrags eindeutig sein
- Das Datenmodell kann lokal erweitert werden

Zugriff auf das X.500: DAP und LDAP(v2)

- Standardgemäß erfolgt der Zugriff auf X.500 über das OSI−Directory−Access−Protocol (DAP)
- Zum Ersatz für das schwerfällige DAP wurde das Lightweight−Directory−Access−Protocol (LDAP) eingeführt, das auf TCP/IP beruht
- Mit dem Zugangsprotokoll wurde auch eine einfache Programmierschnittstelle für Clienten definiert, so daß Anwendungen leicht »directory−aware« gemacht werden können

Standalone LDAP–Server

- Erster Ansatz von LDAP war ein Daemon–Programm, das LDAP–Anfragen in DAP umwandelte (*ldapd*)
- Trotz einem zusätzlichen Programm war der Zugriff auf das X.500–Verzeichnis mit *ldapd* effizienter
- OSI–Directory–System–Agent (DSA) und *ldapd* wurden durch einen Standalone LDAP–Server ersetzt: *slapd*
- *slapd* unterstützt Platten–basierte Datenbank–Biblio–theken: ndbm, gdbm, Berkeley DB
- Freiverfügbare Weiterentwicklung: OpenLDAP

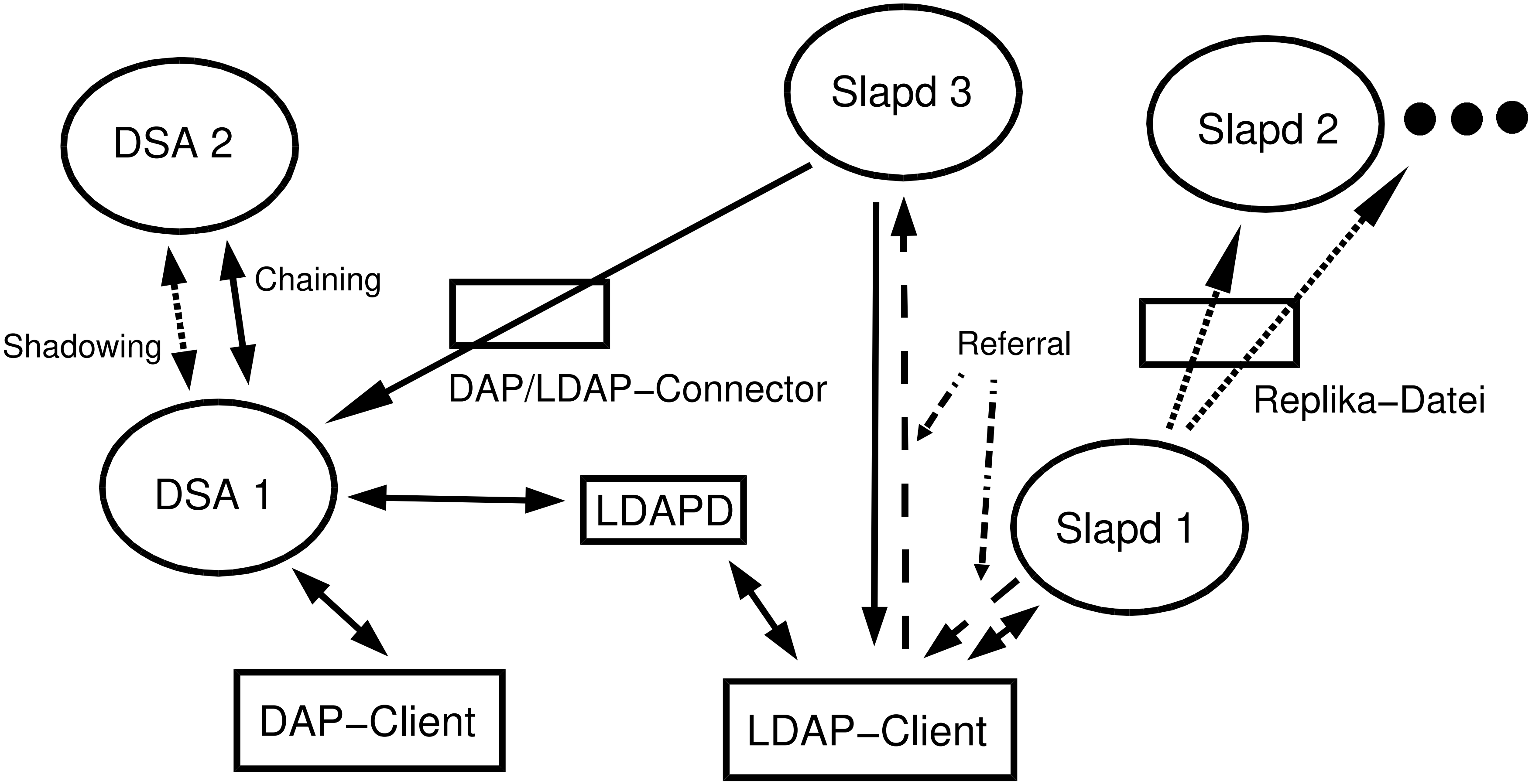
Weiterentwicklung von LDAP: LDAPv3

- X.500−Datenmodell weiterhin als Basis
- LDAPv2−Operationen BIND, UNBIND, ADD, DELETE, SEARCH, COMPARE, ABANDON, MODIFY und MODRDN werden beibehalten
- Neue Operationen können hinzugefügt werden, z.B. Dynamic Directory mit REFRESH−Operation
- Optionen können Operationen erweitern, z.B. binäre oder sprachspezifische Attributwerte, Sortierung
- Client und Server können Sicherheitsmechanismen aushandeln

Datenverteilung und LDAP−Server

- Standalone LDAP−Server können Anfragen an andere Server verweisen (Referral); Client muß ggf. Verweisen durch erneute Anfrage nachgehen
- »Knowledge−Information« ist nicht in LDAPv3 definiert
- Verteilen von Datenkopien erfolgt durch einen externen Mechanismus (Replika− und LDIF−Dateien)

Möglichkeiten zum Einsatz von X.500–Servern



Versuche zur standardisierten Ablage von PGP−Keys

- 1994: Erster IETF−ASID−Draft von Roland Hedberg
- 1994: Tübinger Modell; Einbindung in TWEB und *finger*
- beide Modelle haben den Nachteil, daß nur ein Schlüssel im Personeneintrag hinterlegt werden kann
- Ende 1998: Vorstoß von AMBIX und dem CA−Betreiber der Universität Stuttgart über eine DANTE−Mail−Liste
  - Eigenständige Einträge für PGP−Schlüssel und CA−relevante Informationen; Verweise bei Personen
  - Internationale Diskussion mangelhaft

»Kurzfristige Übergangslösungen«

- Implementation eines PGP−Schemas durch Alex Iliynsky, Moskau, im OpenLDAP−*slapd*
  - Nachteil: unnötige Änderung des *slapd*−Servers aufgrund eines komplizierten Daten−Schemas; OpenLDAP akzeptiert die Änderung nicht
- Neuer Vorschlag des Projekts AMBIX für einen »vorübergehenden« nationalen Alleingang
  - Keine Code−Änderung an Servern
  - Geringfügige Erweiterung der Zugangs−Software (TWEB)
  - Zugriffsmöglichkeit für PGP mit LDAP−Schnittstelle

Das AMBIX−Modell in Kürze

- PGP−Schlüssel werden in eigenständigen Einträgen abgelegt, auf eigenständigen Servern
- Zur Ablage der Informationen werden drei Objektklassen definiert:
  - pGPKeyContainer für Schlüssel−relevante Informationen
  - cAInformationObject für CA−relevante Informationen
  - pGPServerInfo für Server−interne Informationen
- Im Personeneintrag wird über ein LDAP−URL auf den Schlüsseleintrag verwiesen

X.500–Objektklasse für PGP–Schlüssel I

<u>pGPKeyContainer</u> (obligatorische Attribute)

pGPKeyEntryName	Name des Eintrags
pGPKey	ASCII–armored PGP–Key
pGPKeyID	Schlüssel–ID
pGPUserID	UserID(s)
pGPFingerPrint	Fingerprint des Schlüssels
pGPKeyLength	Schlüssel–Länge in Bit
pGPAlgorithm	Schlüssel–Algorithmen (MD5, SHA1, RSA, DH/DSS etc.)
pGPContainerVersion	Version der Modelldefinition (1.02)

X.500−Objektklasse für PGP−Schlüssel II

<u>pGPKeyContainer</u> (optionale Attribute)

pGPVersion	PGP−Version des Schlüssels
pGPCreationTime	Datum der Schlüssel−Erzeugung
pGPExpirationTime	Datum des Schlüssel−Ablaufs
pGPUsage	Verwendungszweck nach X.509
pGPKeyRevoked	0 = gültig, 1 = zurückgezogen
cn	Name des Schlüssel−Inhabers
sn	Nachname des Inhabers
mail	Mail−Adresse des Inhabers
description	Freitext−Beschreibung

X.500–Objektklasse für CA–Zertifizierung

<u>cAInformationObject</u>

cACertKeyLink	DN eines zertifizierenden CA–Schlüssels
cAExternalCertDN	DN einer zertifizierenden CA
cAExternalCertURL	allg. URL einer zertifizierenden CA
cAPolicy	URL der CA–Policy
cADN	DN einer CA
cACRLLink	URL der CRL einer CA
keyOwner	Schlüssel–Eigentümer (USER, CA, RA)
keyCreationMode	Art der Schlüssel–Erzeugung (OWN, AUTO, CA, UNKNOWN)
withPGPRevCert	Hinterlegung eines Revocation–Certificates (0 = nein, 1 = ja)

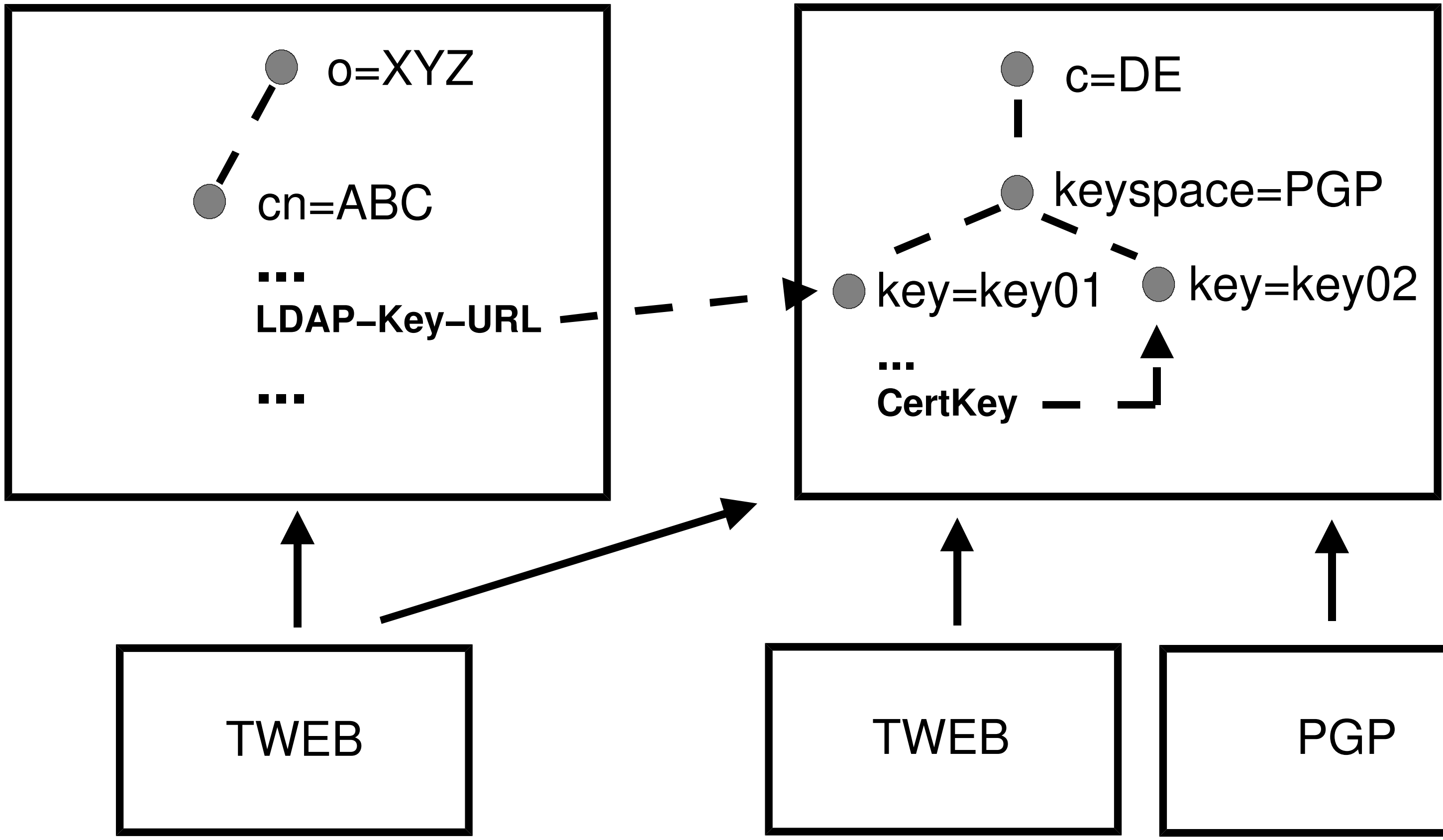
X.500–Objektklasse für Server–Info

pGPServerInfo

cn	Name des Eintrags (cn=pGPServerInfo)
baseKeySpaceDN	Basis–DN der aktiven PGP–Schlüssel
basePendingDN *	Basis–DN in Bearbeitung befindlicher Keys
pGPServerID	Freiwählbare Identifikation des Servers
pGPContainerVersion	unterstützte PGP–Modell–Versionen
pGPCAList *	DN–Liste von beteiligten CAs
pGPCAExList *	URL–Liste von nicht–beteiligten CAs (soweit bekannt)

* = optionale Attribute

Keyserver–Infrastruktur



Datenformat für Schlüssel–Lieferungen

ORGANISATION: <Organisations–Kürzel>
CA : <DN des CA–Schlüssels>
[SIG : <DN des CA–Signatur–Schlüssels>]
VERSION : <Version der Datendefinition (z.B. 1.02)>
DATA
DATASET : <ID Datensatz (z.B. Seriennummer bei der CA)>
ACTION : <new | update | revoke | remove | removeAll>
USER : <DN des Personeneintrags>
KEY : <ASCII–armored PGP–Key>
END–OF–KEY
*****
END–OF–KEY–DEFINITION

Policy für den AMBIX−PGP−Server (v 0.1)

- Schlüssel mit Zertifikaten von CAs der DFN−Hierarchie oder von diesen cross−zertifizierter CAs
- Liefern durch CAs und Personen des AMBIX−Bestands
- PGP 2.x und PGP 5.x; Signatur mit RSA prüfbar
- Auf mögliche CRLs einer CA wird nur verwiesen
- Löschanweisungen vom Benutzer oder der CA; Authorisierung erfolgt über Signatur
- Automatische Löschung von Schlüsseln: ca. 6 Monate nach Ablauf der Gültigkeit oder Löschen des Benutzers

Weitere Arbeiten

- Veröffentlichen des Datenformats und der Policy auf den WWW−Seiten des Projekts AMBIX
- Entwicklung von Programmen zur Datenverarbeitung
- TWEB−Erweiterung zum Darstellen von LDAP−URLs
- Testimplementation
- Anpassen des Modells an PGP 6.x
- Erweiterung des Modells um z.B. SSL−Schlüssel (X.509v3)

Infos und Kontakte

DFN–Directory–Services Deutschland

AMBIX | Zentraler DSA PUMA | X.500–Beratung | ISODE–Software

- Web–Seiten: http://www.directory.dfn.de/
- E–Mail–Adresse: ddsd–info@directory.dfn.de
- Mitarbeiter

  Dr. Ralf Schneider, Dr. Markus Sauer, Bernhard Winkler,
  Dr. Kurt Spanier