Neue Dienste mit LDAP und X.500

Vortrag gehalten beim Belwue Netzdienste AK
am 8. Juli 1999

Peter Gietz, Markus Sauer,
DFN-Directory Services,
Zentrum für Datenverarbeitung, Universität Tübingen

Agenda

- Zur Zukunft des Directory (PG)
- DDSD Personenverzeichnis - AMBIX (MS)
- Warum brauchen wir neue PGP Keyserver (PG)
- Ein X.500 basierter PGP Keyserver (MS)
- Konzept eines europaweiten LDAP Index (PG)

Zur Zukunft des Directory

- Augenblicklicher Status
- Hybrides Directory
- LDAP
- Aufgaben in Deutschland

Augenblicklicher Status

- Directory vorwiegend White und Yellow Pages Service
- International koordiniert durch NameFLOW von DANTE
- Mehrere Millionen Personeneinträge
- Viele veraltete Einträge
- Infrastruktur basiert auf Quipu X.500(88)
- Nicht Jahr 2000 kompatibel
- LDAP Server treten an Stelle von X.500 DSAs

Hybrides Directory

- Umstieg auf X.500(93)
- Backbone von Firstlevel DSAs eines X.500(93) Produktes (Isode)
- Knowledge Information wird über einen Root DSA geshadowed
- Konnektivität zu LDAP und anderen X.500 Servern (88 und 93)

LDAP

- Viele Länder gehen zu reinen LDAP Lösungen über
  - Schweden: TISDAG (http://tisdag.sunet.se/)
  - Norwegen: Norwegian Directory of Directories (draft-hedberg-alvestrand-ndd-00.txt)
  - Holland: http://www.surfnet.nl/surfnet-zoektools/search.html
  - Griechenland: http://ds.grnet.gr/index_en.html
- LDAP noch unvollständig:
  - Replikation (IETF WG ldup)
  - Authentifizierung (IETF WG ldapext)
  - Access control (IETF WG ldapext)
- Plan eines LDAP DIT
- Viele neue Anwendungen
  - Betriebssystemintegration (NIS)
    - Linux (http://www.rage.net/ldap/)
    - SUN (Solaris 8)
    - Windows 2000 (Active Directory)
  - Routing policy (IETF WG policy, DEN)
  - PKI

Aufgaben in Deutschland

- Zwingender Umstieg auf X.500(93)
- LDAP Integration
- Integration in den europäischen Gesamt-Index, auf Basis der im EC-Projekt DESIRE II entwickelten Software
- Voranbringen von PGP
- Definition von Untergliederung und Sichtweisen für c=DE (geographisch, Schulen, KuMB, DFN, YP, WP ...)
- Richtlinien für die Güte eines Eintrags:
  - Minimal-Datensatz für O, OU und CN Einträge
  - Minimalanzahl von Einträgen unterhalb eines O-Eintrags
  - Qualität der Aktualisierungsmechanismen
  - Anforderung an die Erreichbarkeit von DSAs
- Namensrichtlinien
- Homogener Einsatz von Gateway-Software und deren Darstellungskonfigurationen
- Homogenere Access Controll

- Zu diesen Themen wollen wir im Herbst ein DS-Manager Treffen organisieren, zu dem auch LDAP-Server-Betreiber eingeladen sind.

Warum brauchen wir neue PGP Keyserver

- Vorzüge von PGP
- Probleme des existierenden PGP Keyserver
- Was bisher geschah
- Probleme bei der Speicherung von PGP Keys im Directory
- Anforderungen

Vorzüge von PGP

- Augenblicklich meistgenutzte Public Key Infrastruktur
- Geeignet zum Signieren, Integritätssicherung, Verschlüsseln (asymmetrisch und symmetrisch), Authentifizierung
- Flexibles Format: verschiedene Algorithmen und Schlüssellängen, Subkeys
- CA Trustmodell anwendbar

Probleme des existierenden PGP Keyserver

- Die klassische Lösung: PKS von Marc Horrowitz (http://www.mit.edu/afs/net.mit.edu/project/pks/thesis/paper/thesis.html)
- Kein verteiltes System: Alle Keys auf allen Servern
- Nicht beliebig skalierbar
- Probleme bei der Replikation der Schlüssel

Was bisher geschah

- Hedberg: „Definition of X.500 Attribute Types and a Object Class to hold public PGP keys“ Februar 1996 (seit September 1996 obsolet)
- AMBIX-PGP@mail500.uni-tuebingen.de
- pgp-directory@dante.org.uk (http://www.dante.net/np/listarchives/pgp)
- OpenKeyServer von Highware (http://www.highware.com/main-oks.html)
- NAI PGP Certificate Server (http://www.nai.com/products/security/commercial.asp)

Probleme bei der Speicherung von PGP Keys im Directory

- Eine Person kann mehrere Keys haben
- Ein Key kann mehrere UserIds haben
- Ein Key kann mehrere Subkeys haben

Anforderungen

- Standardisierte Lösung
- Keys müssen nach verschiedenen Kriterien suchbar sein
- CA Zertifizierung muss intergierbar sein
- Zertifizierungspfad muss verfolgt werden können
- Key-Status muss abfragbar sein
- Key Information müssen sowohl unter einem Personeneintrag als auch in einem eigenen Keyspace gespeichert werden können

Konzept eines europaweiten LDAP Index

- DESIRE II
- Verteiltes Indexsystem
- Architektur
- Indexobjekt Sammlung
- Indexobjekt Verteilung

DESIRE II

- Der europäische LDAP Index wird als Teil des DESIRE II Projekts entwickelt
- Development of a European Service for Information on Research and Education
- Gefördert von der EU (Telematics Applications Programme)
- 10 europäische Partner
- Information discovery, am WWW orientiert
- Integration anderer verteilter Informationen
- Metadatenmanagement

Verteiltes Indexsystem

- Hierarchische Topologie
- LDAP v3 Technologie (Referrals)
- Serverseitig betrieben
- Datenserver werden registriert
- Common Indexing Protocol (kommt gerade als RFCs heraus)
- Tagged Index Object

Weitere Infos

- www.directory.dfn.de
- ambix-d@directory.dfn.de
- Der PGP-Keyserver laeuft auf: as.directory.dfn.de:11010
- www.desire.org
- http://www.ietf.org/internet-drafts/draft-gietz-ldapindex-00.txt