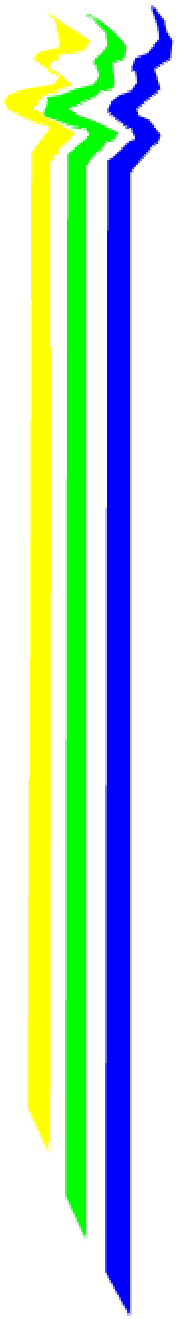
Verteilung von Zertifikaten

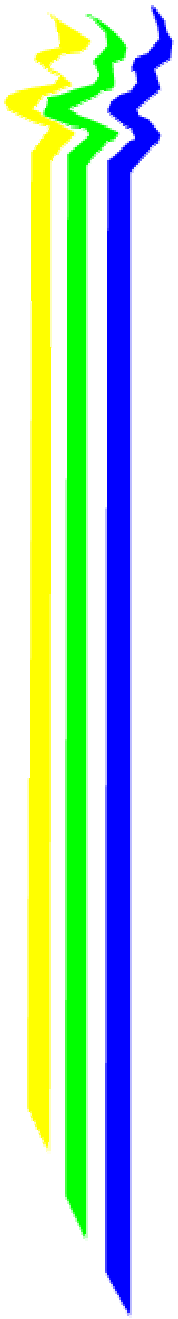
Der Verzeichnisdienst für PKI

Peter Gietz
DFN Directory Services
peter.gietz@directory.dfn.de



Agenda

- Warum Schlüssel verteilen?
- Klassisches Konzept: X.509
- IETF PKIX
- Anwendungen von X.509: S/MIME, SSL
- PGP Keyserver
- Neuere Serverkonzepte
- LDAP-basierte Server

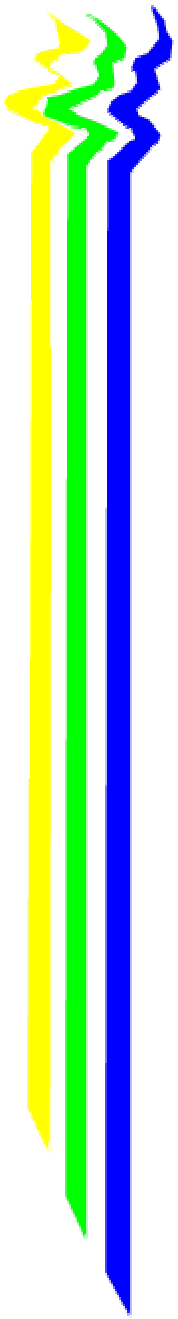


Warum Schlüsselverteilung?

- Grundvoraussetzung für PKI
- Verschlüsselung ohne vorherige Kommunikation
- Schlüssel muß nicht von jedem gespeichert werden (z.B. pubring.pgp)
- Reduzierte Kommunikation bei neuen Schlüsseln (1 zu n anstelle von n zu n)
- Update bei Veränderungen im Schlüssel

Wie veröffentliche ich meinen öffentlichen Schlüssel?

- Ohne Hilfe anderer:
  - Auf eigener Webpage
  - via FTP-file
  - via finger
- Mit Hilfe anderer:
  - Keyserver: Jemand betreibt ein öffentliches Verzeichnis von Schlüsseln, bzw. Zertifikaten
  - Directory: öffentliches Verzeichnis für beliebige Daten



PKI und Directory

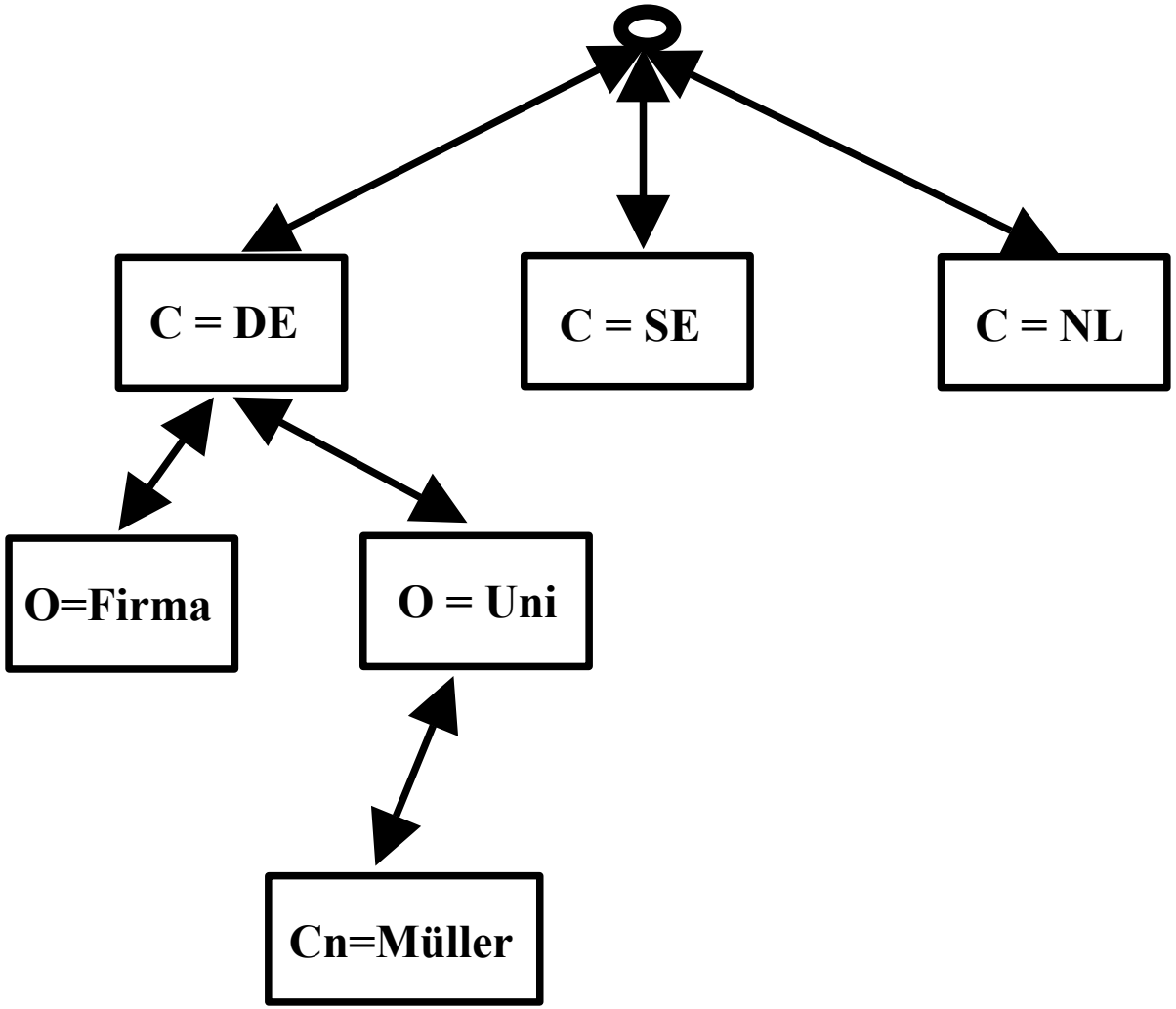
The Burton Group:
Network Strategy Report, PKI Architecture, July 1997:
(zitiert nach: S. Zeber, X.500 Directory Services and PKI Issues, http://nra.nacosa.nato.int/pki/hdocs/pkiahwg30/index.htm)

» ... 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.«

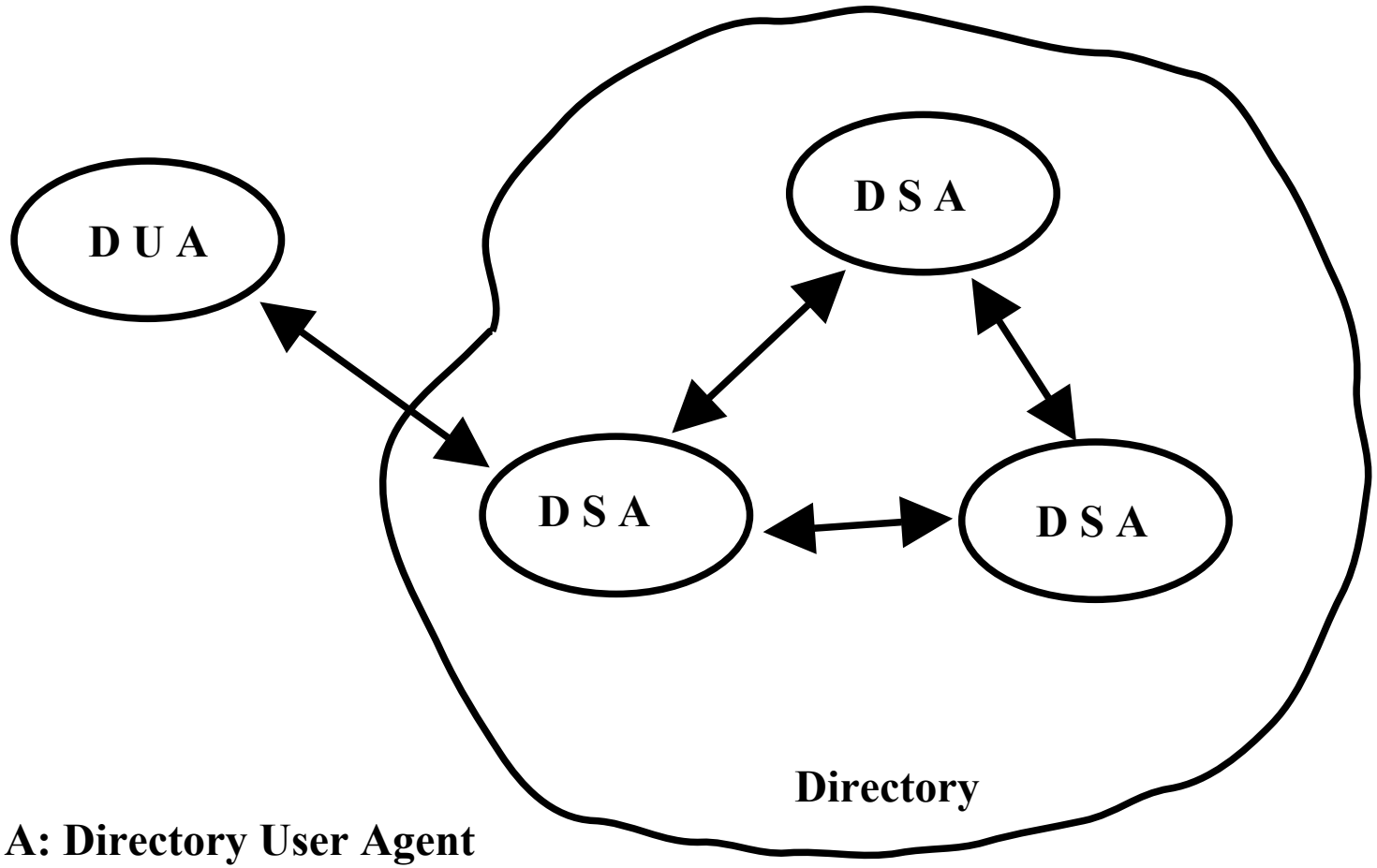
Was ist Directory?

- X.500 Datenbank-Standard
- ISO/ITU 1988, 1993, 1997
- weltweit verteilte Daten
- alle Daten stehen weltweit zur Verfügung
- hierarchisch organisierter Datenbaum
- objektorientiertes Design (vererbbare Objektklassen)
- erweiterbares Datenmodell

Directory Information Tree, DIT



Client und Server



D U A: Directory User Agent

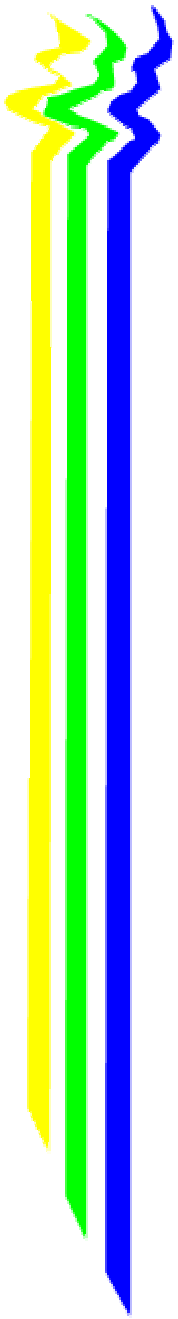
D S A: Directory System Agent

LDAP

- Lightweight Directory Access Protocol
- Aktuelle Version 3
- IETF-Standard (RFC 2251-2256)
- Nicht nur Access Protocol, sondern wie X.500 vollständiges Client-Server-System
- Alle Directory-Implementierungen haben LDAP-Schnittstelle (X.500, Novell NDS, MS AD)
- Viele Clientaplikationen haben LDAP-Schnittstelle (z.B. Mailprogramme, Browser)

Directory als Key-Server

- Veröffentlichungsorgan für öffentliche Schlüssel und Zertifikate
- erhält Schlüssel vom User
- erhält Zertifikate von CA
- Muss zurückgezogene Schlüssel dokumentieren: CRL (Certificate Revocation List)
- Muss Status eines Zertifikats zu einem bestimmten Zeitpunkt dokumentieren



X.509, das klassische Konzept

- The Directory: Authentication Framework
- Teil des OSI-Verzeichnisstandards X.500
- Definiert Datenmodell, z.B.:
  - userCertificate; cACertificate
  - crossCertificatePair
  - certificateRevocationList
- Definiert Authentifizierungsmechanismen
- Zertifikat enthält DN der CA und des Users

X.509v3

- Neuer Erweiterungsmechanismus:
  - extensions
- Vordefinierte Erweiterungen:
  - Key Information: identifier, usage ...
  - Policy Information: certificate policy ...
  - User and CA Extensions: alternative names..
  - Certification Path Constraints
- X.509v3 wird von vielen als von X.500 unabhängig gesehen.

IETF WG pkix

- Ziel: Aufbau einer Internet PKI auf Basis von X.509-Zertifikaten
- Unterstützt die Security Protokolle:
  - S/MIME
  - TLS (= SSL)
  - IPSec
- Status: 9 RFCs, 21 Drafts (Überblick -> <draft-ietf-pkix-roadmap-05.txt>)

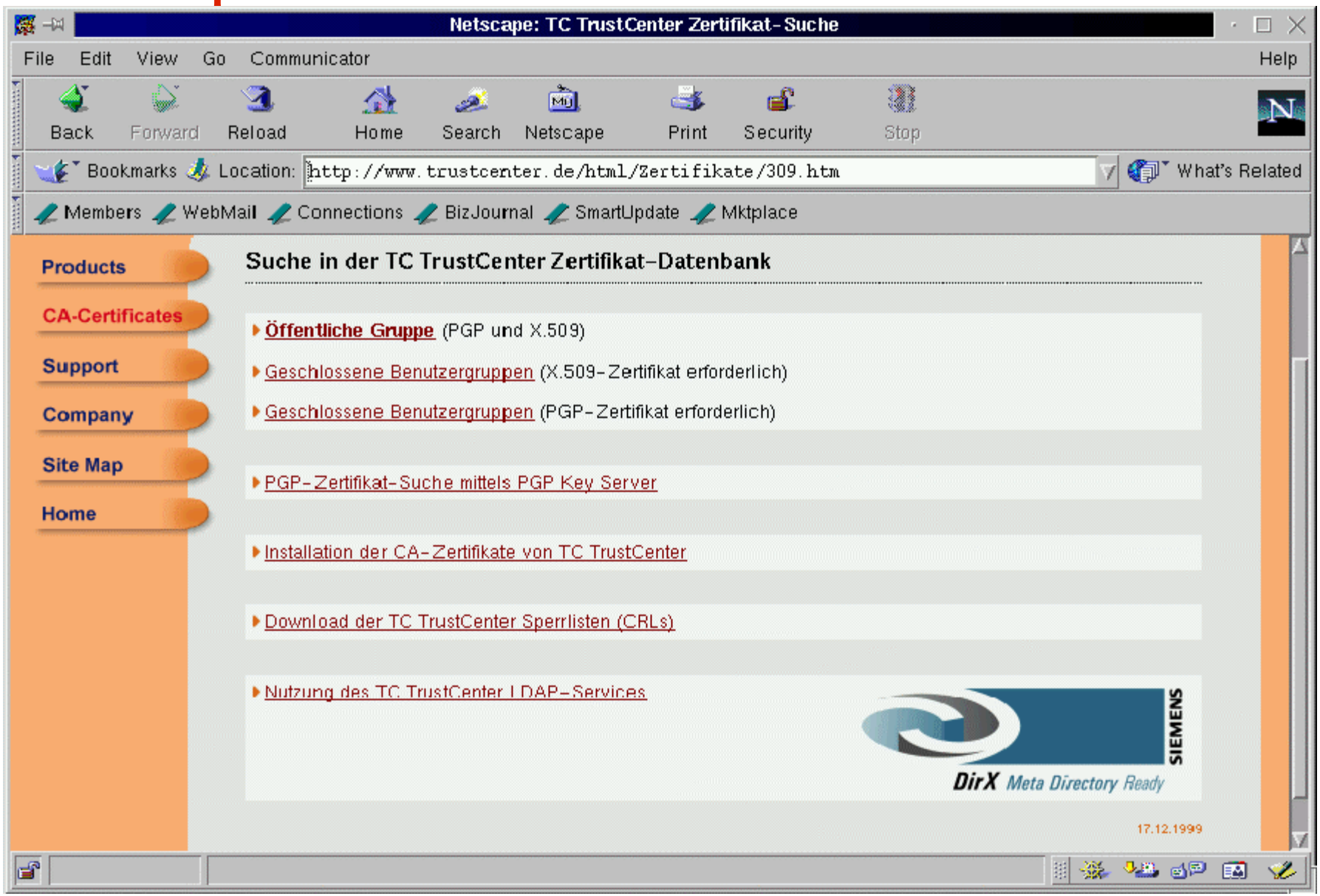
PKIX und Verteilung

- Datenmodell (profiles)
  - Certificate und CRL -> RFC 2459; <draft-ietf-pkix-new-part1-00.txt>
  - Attribute Certificate
    -> <draft-ietf-pkix-acx509prof-02.txt>
- Simple Certification Verification Prot. (SCVP)
  -> <draft-ietf-pkix-scvp-01.txt>
- Online Certificate Status Protocol (OCSP)
  -> RFC 2560; <draft-ietf-pkix-ocspx-00.txt>
- PKI Operational Protocols:
  - LDAPv2 -> RFC 2559
  - LDAPv3 -> <draft-ietf-pkix-ldap-v3-01.txt>
  - FTP/HTTP -> RFC 2585

Anwendungen von X.509 Zerts

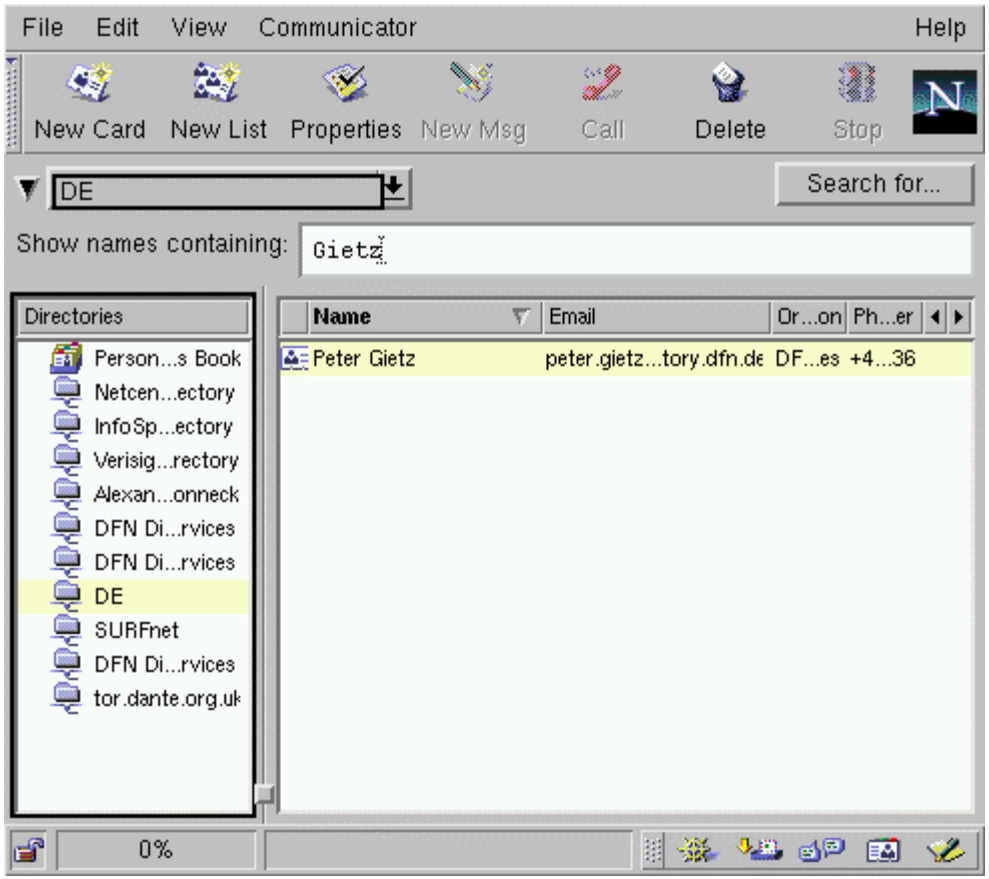
- Zertifikatsgestützte Sicherheit auf verschiedenen Ebenen:
  - Network Layer:
    IPSec (Internet Protocol Security)
  - Transport Layer:
    SSL (Secure Socket Layer) =
    TLS (Transport Layer Security)
  - Application Layer:
    S/MIME (Secure Multipurpose Internet Mail Extensions)
    PGP (Pretty Good Privacy) ab Version 6.x

Beispiel: TC Trustcenter



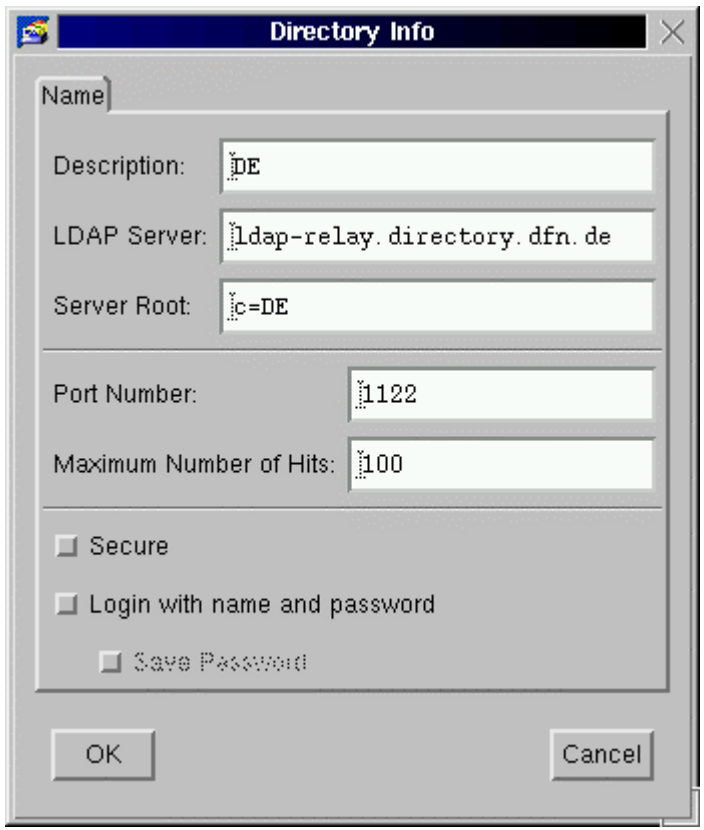
Netscape Adressbuch

Netscape 4.61, Menufolge:
Communicator; Address Book´



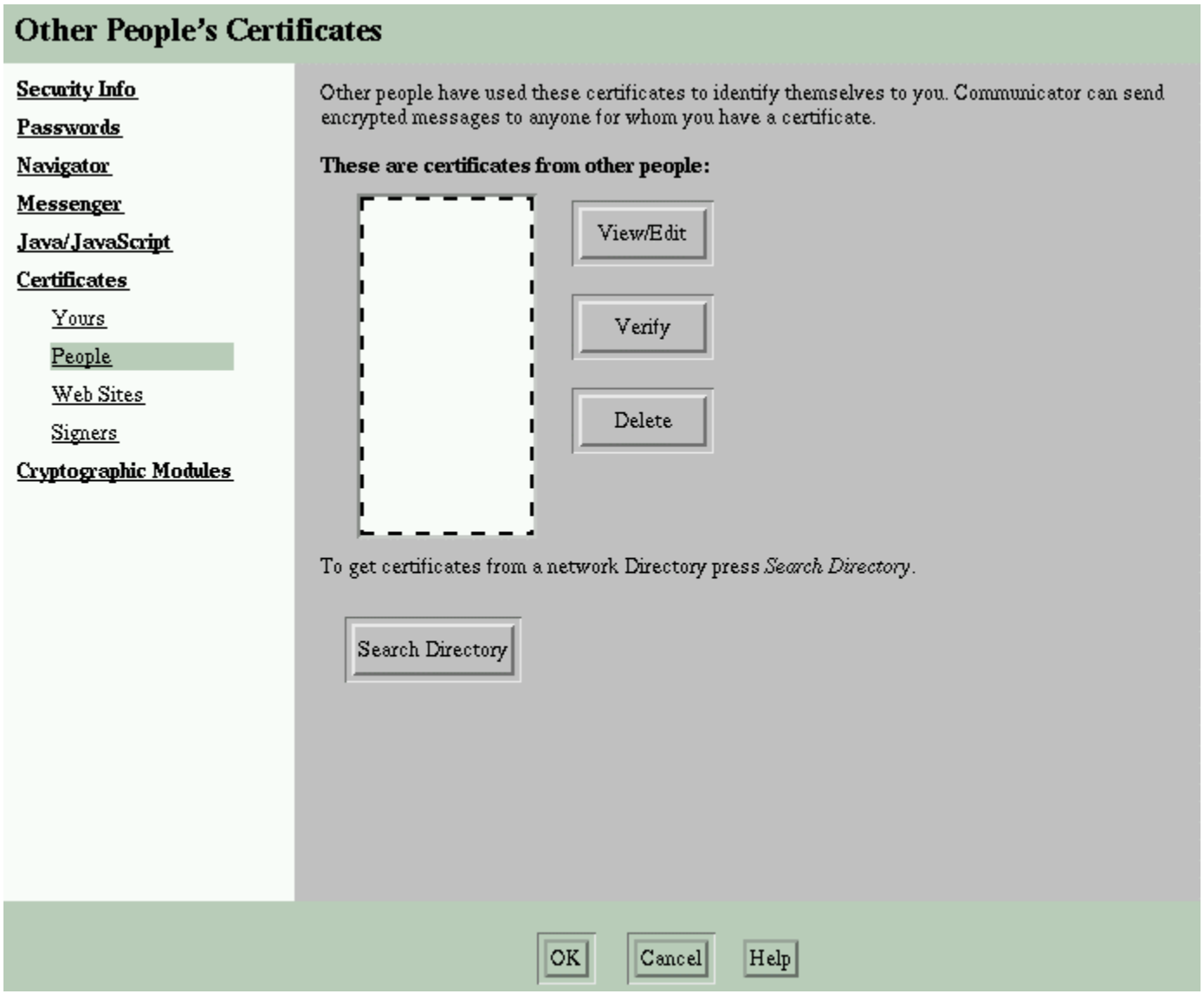
Neues Directory in Netscape

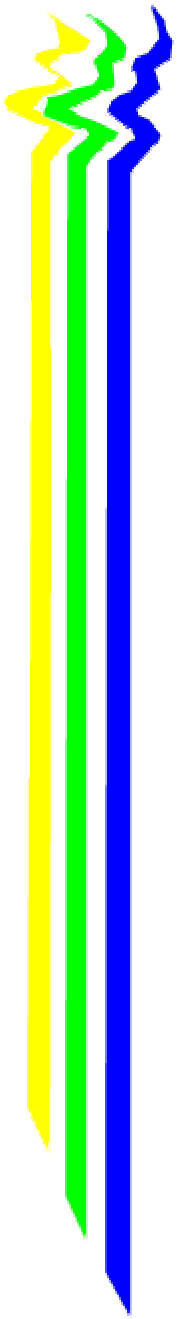
Netscape 4.61, Menufolge:
Communicator; Address Book´; File; New Directory



Netscape Zertifikatsuche

Netscape 4.61, Menufolge: Security, People





PGP Keyserver

- Zuerst nur Replikation von pubring via email
- Marc Horowitz Keyserver (PKSD)
  - seit 1995
  - eigenes Datenbank-Backend
  - email und HTTP Interface
  - Funktionsmodell (add, revoke, etc.)
  - Netz von Servern
  - Jeder Server hat alle Keys
  - Synchronisation via email

PGP Keyserver Statistik
(Stand: Februar 2000)

- 20 sich synchronisierende Server
- Knapp 1 Million Schlüssel
- 1,06 GB Pubring
- Viel mehr DSS/SH- als RSA-Schlüssel
- Viele Schlüssel nur selbstsigniert
  (=islands of trust)

PKSD Probleme

- Kein verteiltes System.
- Ständige Synchronisation erzeugt hohe Netzlast.
- Chaos beim Ausfall eines Servers im Verbund.
- Keine Garantie, daß ein Key auf alle Server gelangt.
- Nicht beliebig skalierbar.

Neue Serverkonzepte

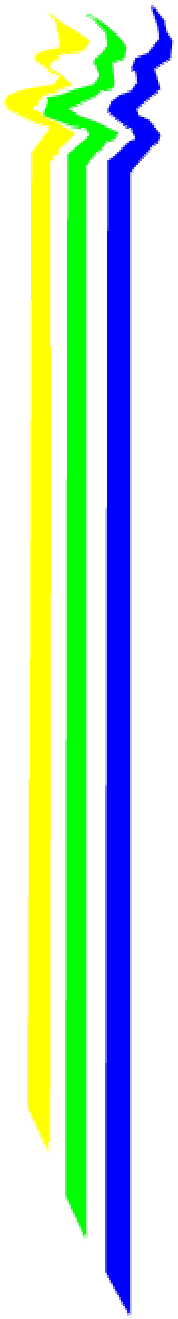
- PKSD mit verbessertem Datenbank-Backend (z.B. Open Keyserver von Highware)
- Keyserver auf Basis von DNSSec (vgl. www.ietf.org/html-charter/dnssec-charter.html)
- Synchronisation via multicast (vgl. G. Baumer, Distibuted Server for PGP Keys synchronised by multicast, www.vis.ethz.ch/~baumi/sa/thesis/thesis.html)
- Keyserver auf LDAP Basis (z.B. PGP Certificate Server von NAI, www.nai.com)

LDAP PGP-Keyserver Anforderungen

- Standardisierte Lösung:
  - Datenmodell
  - Funktionsmodell
- Schlüssel nach verschiedenen Kriterien suchbar
- Zertifizierungspfad verfolgbar
- Schlüsselstatus abfragbar

Prozess der Standardisierung

- 1994 erster Draft von Roland Hedberg
- 1994 erste proprietäre Lösung in Tübingen
- Beide Modelle können nicht mehrere Schlüssel einer Person zuordnen
- 1998 neue Initiative von DANTE
- DDS und CA der Uni-Stuttgart beteiligen sich und kündigen erste Versionen von Internet-Drafts an
- Roadmap: Draft im Sommer 2000



Status

- PGP-Testserver auf LDAP-basis
- Policy für den Betrieb
- Datenmodell definiert
- Datenlieferungsformat für Cas
- Software für die Verarbeitung
- Selbsteintragsmöglichkeit via WWW