Ein X.500 basierter PGP-KeyServer

AK BelWü Netzdienste AG
8. Juli 1999

Dr. Markus Sauer,
DFN Directory Services Deutschland
Zentrum für Datenverarbeitung, Universität Tübingen

Inhalt

Anforderungen

•

Objektklassen / Attribute / DIT

•

Integration in das X.500-Directory

•

Anbindung an AMBIX-Datenbestand

•

Akquisition und Verarbeitung der Daten

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 5.0i for non-commercial use

mQCNAzdlCAgAAAEEAJ2W+ZHzVk+UThtAkxOcEhPPPERF71pJEzixNPyFK55GWxdT
5a0/RAKkEDeCgejc5tuz+fHqF+X7vzwz88s4gtkjWj+YTMOqHOKfLAH0iQmAXVTD
KeCsYxV5TK4mQOz/y3ks3jFYt+2pg+HyDuNpLkBvrkrweeFRNcKm2VY/8ydFAAUR
tCxNYXJrdXMgU2F1ZXIgPE1hcmt1cy5TYXVlckBkaXJlY3RvcnkuZGZuLmRlPokA
lQMFEDdlAdb28v6AvoKyTQEBFRgEALsWMF+QHblwjhYlGf8F5iANBWPKtS8or2+C
+x6bm6pOxFCwGDruN/VwXm7BbzN4oqJxfi8xDWAa29T7MgdymseAJklNs7X3esr0
Wu9+yBzmG6Nzwv5Uk8Q4cszW5/Xy26CqGjWZzkUVZpaPXqVvX2Y092Xm+4g6EeVA
pv5gadjIiQCVAwUQN2UICMKm2VY/8ydFAQHDKAP6AqGwSGqOMh62+Dkr+2lNP5mf
9iI0CQfyWoX85AZHp7bY7n5wAUEY0yZY9IwOFAAqbtVgtDo1gIvacZ49NxPM6wsS
/TSrJ0hLC3TU6R3ro9X8tUxnC5dty5xv4+LtWchQbfXHl6ANWh+FKzWMEwy18o2E
7u3EeUciblyKIdBmqtQ=
=vM3u
-----END PGP PUBLIC KEY BLOCK-----
```


```
Type Bits KeyID      Created    Expires    Algorithm       Use
pub 1024 0x3FF32745 1999-06-14 ---------- RSA             Sign & Encrypt
f16    Fingerprint16 = D3 6B 49 DB 7A 13 51 7D  F7 8C 56 0D 63 32 D2 45
uid  Markus Sauer <Markus.Sauer@directory.dfn.de>
sig       0xBE82B24D 1999-06-14 DFN-DIRECTORY, CERTIFICATION ONLY KEY
SIG       0x3FF32745 1999-06-14 Markus Sauer <Markus.Sauer@directory.dfn.de>
```

Anforderungen:

- PGP-Server auf Basis eines 93'DSA oder SLAPD
- Volle Anbindung des PGP-Servers an X.500-Directory
- Unterstützung der gängigen PGP-Clients (Win95/98/NT)
- Skalierbarkeit
- *“Standardkonform“*

Objektklassen und Attribute

OBJEKTKLASSE	Beschreibung
pGPKeyContainer	allg. PGP-Key Informationen
pGPSubKeyContainer	PGP-SubKey Informationen
cAInformationObject	Zusatzinformations bei zert. PGP-Key
pGPServerInfo	PGP-Keyserver Informationen

pGPKeyContainer

Attribute	Wert	opt.
pGPKey	ASCII-armored PGP-Key	
pGPPrimeUserID	User-ID	
pGPUserID	User-ID(s)	
keyOwner	Status of Owner (USER/CA/RA)	
pGPContainerVersion	Version of modeldefinition (1.03)	
keyCreationMode	Mode of Key creation (OWN/AUTO/CA/UNKNOWN)	x
withPGPRevCert	revokation certificate is deposited	x
pGPVersion	PGP-version of the Key	x
pGPKeyCreateTime	date of key creation	x
pGPKeyExpireTime	date of key expiration	x
cn	Name of Key-Owner	x
sn	Surname of Key-Owner	x
mail	e-Mail addresse of Key-Owner	x
description	description of Key-Owner	x
uSER-DN	DN of the key owner	x

pGPSubKeyContainer

Attribute	Wert	opt.
pGPKeyEntryName	Name of entry	
pGPKeyID	PGP Key-ID	
pGPFingerPrint	Fingerprint of PGP-Key	
pGPKeySize	Length of PGP-Key in bits	
pGPKeyType	Key-algorithms	
pGPSuBContainerVersion	Version of modeldefinition (1.03)	
pGPUsage	purpose	x
pGPKeyRevoked	0 = valid , 1 = revoked	x
pGPDisabled	0 = valid , 1 = invalid	x

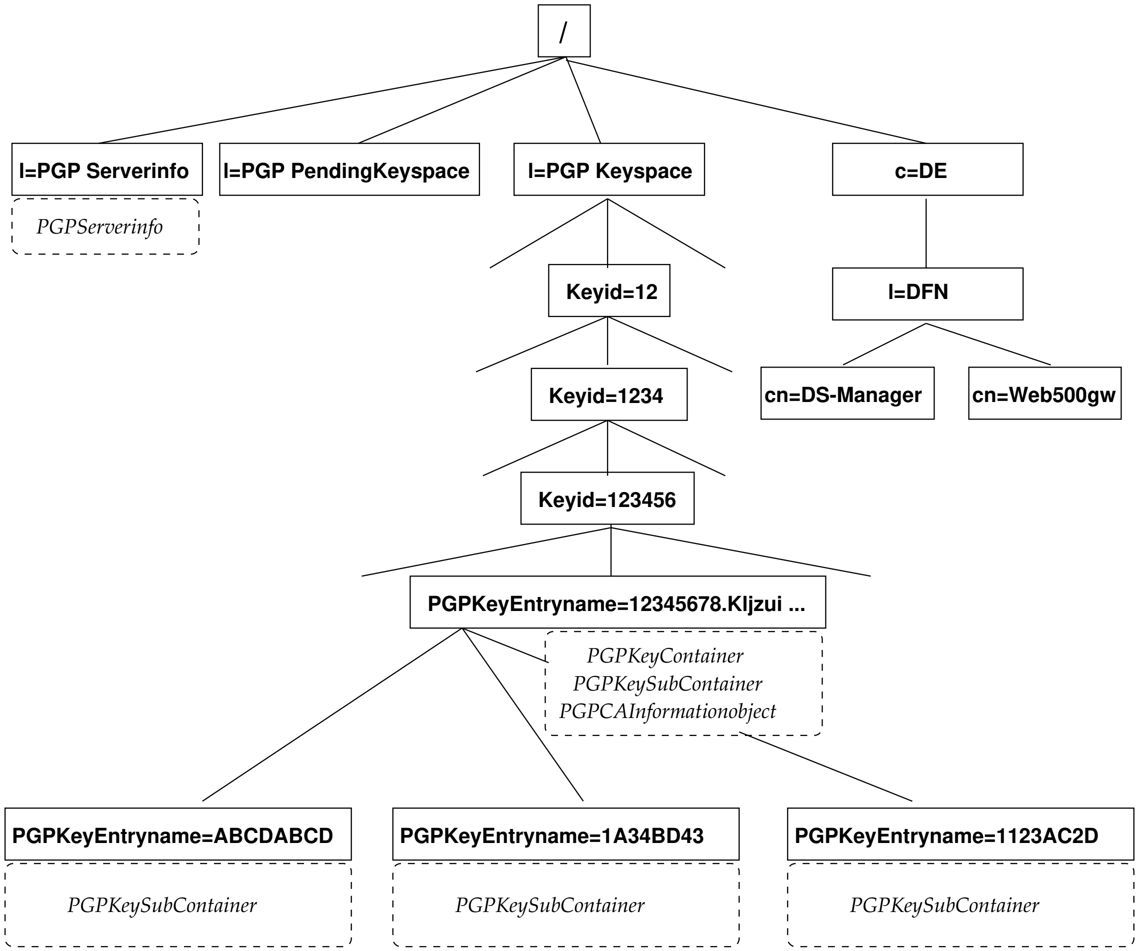
cAInformationObject

Attribute	Wert	opt.
cACertKeyLink	DN of a certified CA-Key	
cAExternalCertDN	DN of a certifing CA	
cAExternalCertURL	common URL of a certifing CA	
cAPolicy	URL to CA-policy (or RA-policy)	
cADN	DN of CA (or RA)	x
cACRLLink	URl of the CRL of a CA	

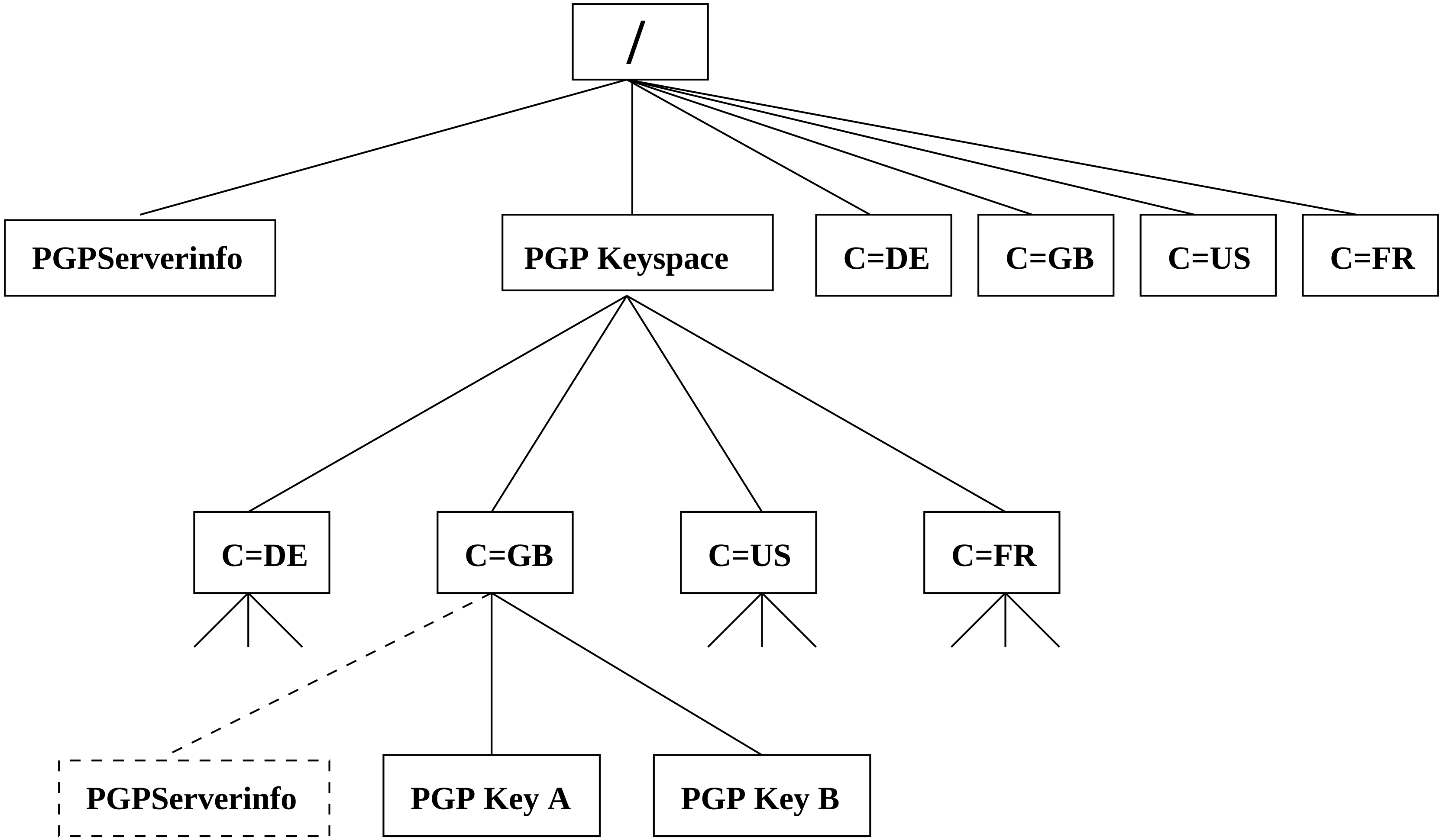
pGPServerinfo

Attribute	Wert	opt.
cn	Name of Entry (cn=pGPServerinfo)	
baseKeySpaceDN	base-DN of the aktive PGP-keys	
basePendingDN	base-DN of the pending PGP-keys	x
pGPServerID	ID of the server	
pGPContainerVersion	Supportet PGP modelversion	
pGPCAList	DN-list of participating CAs	x
pGPCAExList	DN-list of not participating CAs	x

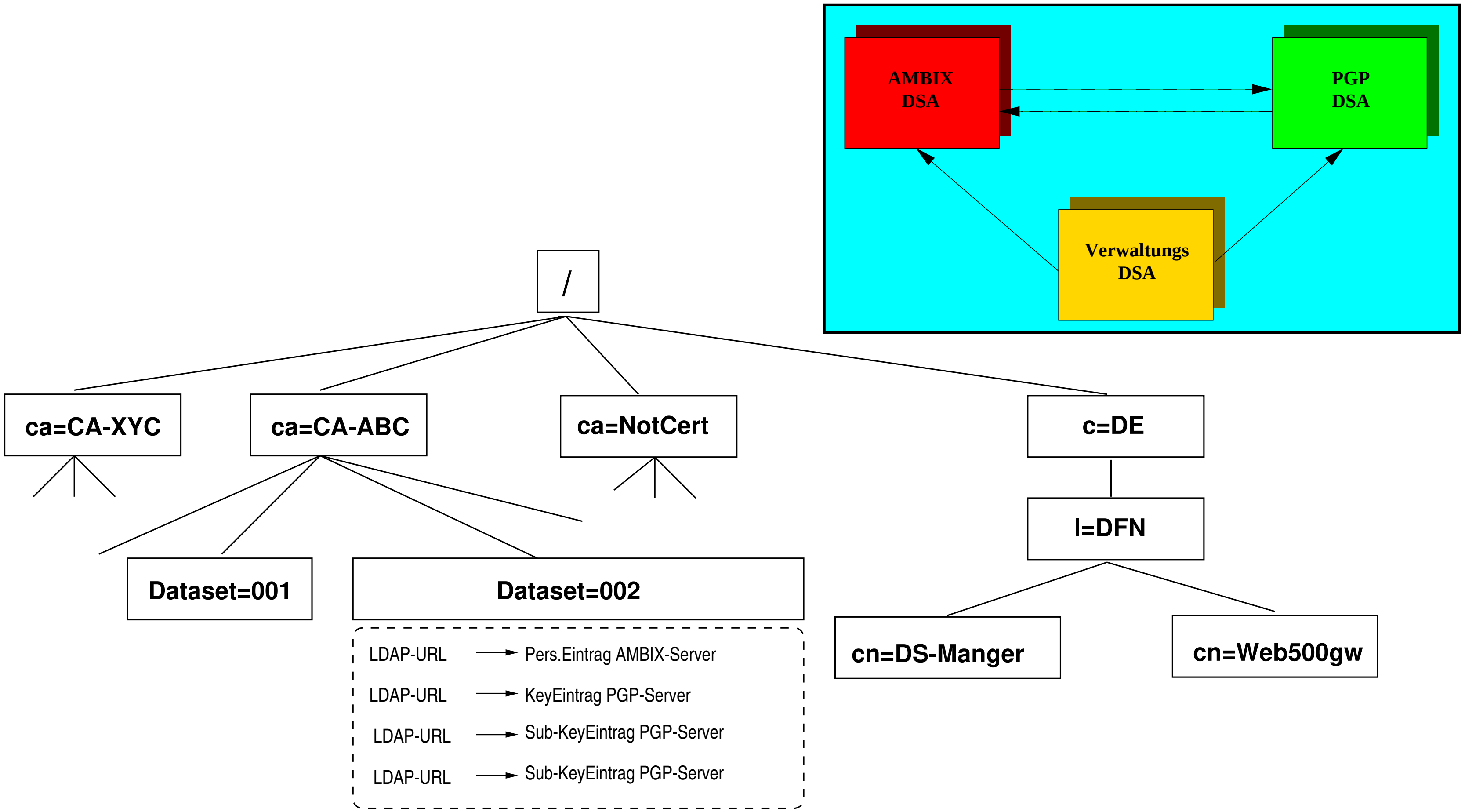
Directory Informational Tree



Integration in das X.500-Directory



Anbindung an AMBIX-Datenbestand



AMBIX: Das DFN–E–Mail–Verzeichnis

Homepage Gesamtindex Hilfe zur Suche Hilfe zum Selbsteintrag

Über diesen Link gelangen Sie direkt auf den gesamten Key–Server Datenbestand.

Markus Sauer <Markus.Sauer@directory.dfn.de>

UserID
Markus Sauer <Markus.Sauer@directory.dfn.de>
pgprevoked
0
pgpdisabled
0
KeyID
3FF32745
Keysize
01024
FingerPrint
D3 6B 49 DB 7A 13 51 7D F7 8C 56 0D 63 32 D2 45
Ascii–Armored Key (base64 encoded)


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAzdlCAgAAAEEAJ2W+ZHzVk+UThtAkx0cEhPPPERF71pJEzixNPyFK55GWxdT
5a0/RAKkEDeCgejc5tuz+fHqF+X7vzwz88s4gtkjWj+YTM0qH0KfLAH0iQmAXVTD
KeCsYxV5TK4mQ0z/y3ks3jFYt+2pg+HyDuNpLkBvrkrweeFRNcKm2VY/8ydFAAUR
tCxNYXJrdXMgU2F1ZXIgPE1hcmt1cy5TYXVlckBkaXJlY3RvcnkuZGZuLmRlPokA
lQMFEDdlAdb28v6AvoKyTQEBFRgEALsWMF+QHblwjhYlGf8F5iANBWPKtS8or2+C
+x6bm6p0xFCwGDruN/VwXm7BbzN4oqJxfi8xDWAa29T7MgdymseAJklNs7X3esr0
Wu9+yBzmG6Nzwv5Uk8Q4cszW5/Xy26CqGjWZzkUVZpaPXqVvX2Y092Xm+4g6EeVA
pv5gadjIiQCVAwUQN2UICMKm2VY/8ydFAQHDKAP6AqGwSGq0Mh62+Dkr+2lNP5mf
9iI0CQfyWoX85AZHp7bY7n5wAUEY0yZY9Iw0FAAqbtVgtDo1gIvacZ49NxPM6wsS
/TSrJ0hLC3TU6R3ro9X8tUxnC5dty5xv4+LtWchQbfXHl6ANWh+FKzWMEwy18o2E
7u3EeUciblyKIdBmqtQ=
=vM3u
-----END PGP PUBLIC KEY BLOCK-----
```


Zum Signaturschlüssel (Chain of Trust)
Signaturkey der CA DFN Directory Services Deutschland
Erzeugungsdatum
1999–06–14
Verfallsdatum

Beschreibung
AMBIX Mitarbeiter
Keytype
RSA
Name
Markus Sauer
Nachname
Sauer
Mail–Adresse
markus.sauer@directory.dfn.de
Status des Benutzers
USER
Erzeugungsmodus
USER
Revokation–Zertifikat bei zert. CA hinterlegt
YES
pGP–Version
2.6.2i
Verwendungszweck
Sign
Encrypt
pGPContainerVersion
1.04
pGPSubContainerVersion
1.04

Bei Fragen zum DFN–X.500–Email–Verzeichnis wenden Sie sich bitte an:

ambix–d@diectory.dfn.de (Directory–Manager des Projekts AMBIX)

Daten erstellt durch

Akquisition und Verarbeitung der Daten

- Datenlieferung durch CAs in def. Format.
- Selbsteintrag durch AMBIX-User via WWW-Online-Formular
  - Neuanlage von Einträgen
  - Löschen von Einträgen
  - Ungültig Markieren von Einträgen
  - Schlüssel revoken
- Verarbeitung durch LDAP-Client (PERL)

```
ORG:                 CA Universitaet Tuebingen
SIG:                 sig001
FORMAT:              1.01

DATA

BEGIN-OF-KEYDEF
DATASET:             user-19990612-007
ACTION:              new-dataset
KEY:                 -----BEGIN PGP PUBLIC KEY BLOCK-----
                     Version: 2.6.3i

                     mQCNAzdlCAgAAAEEAJ2W+ZHzVk+UThtAkxOcEhPPPERF71pJEzixNPyFK55GWxdT
                     7u3EeUciblyKIdBmqtQ=
                     =vM3u
                     -----END PGP PUBLIC KEY BLOCK-----
END-OF-KEY
KEYOWNER:            USER
CREATIONMODE:        OWN
# optionale Angaben
LABEL:               new PGP-Key fuer private Mails
USER:                cn=Hans Mustermann,o=AMBIX,l=DFN,c=DE
CN:                  Hans Mustermann
SN:                  Mustermann
MAIL:                hans.mustermann@directory.dfn.de
DESCRIPTION:         PGP Schlüssel zur Signatur und Verschlüsselung priv. Mails
REVCERT:             YES
END-OF-KEYDEF
```

Zusammenfassung

- Konzept und Realisierung eines X.500 PGP-Servers (93'DSA oder SLAPD)
- Volle Anbindung des PGP-Servers an X.500-Directory
- Unterstützung der gängigen PGP-Clients (Win95/98/NT)
- PGP-Server beliebig skalierbar
- DV bereit für Datenlieferungen
- Online-Formular kurz vor Fertigstellung