Die Zusammenarbeit der DFN–Projekte PCA und DDS am Beispiel der Veröffentlichung von Public–Key–Zertifikaten

Stefan Kelm
DFN–PCA, Hamburg
kelm@pca.dfn.de

Kurt Spanier
DFN Directory Services, Tübingen
kurt.spanier@directory.dfn.de

Gliederung

- **Kurzvorstellung: DFN−PCA**
- **Kurzvorstellung: AMBIX / DDS**
- **Veröffentlichung von PGP−Schlüsseln im X.500−Verzeichnis**
  - **Historie**
  - **Das AMBIX−Modell**
  - **Das Datenlieferungsformat**
- **Die Datenlieferung**
- **Zusammenfassung**
- **Vorführung**

Das DFN–Projekt PCA

- **Projekt DFN–PCA seit 1996**
- **Aufgabe: Aufbau und Pflege einer Zertifizierungsinfrastruktur (PKI)**
  - **Unterstützung bei Aufbau und Betrieb eigener CAs mittels frei verfügbarer Anwendungen, z.B. SSL (TLS), PGP, S/MIME**
  - **PKI basiert auf gemeinsam erarbeiteten Zertifizierungsrichtlinien (Policies)**
- **Zertifikatarten:**
  - **CA–Zertifikate, SSL–Server–Zertifikate, (PGP–Benutzer)**
  - **Anwender–Zertifikate durch lokale CAs**
  - **Weitere Anwendungen in Vorbereitung**
- **Die Hierarchie im Oktober 1999:**
  - **Erste CA im Mai 1997**
  - **26 PGP–CAs / 8 X.509v3 (SSL)–CAs / 0 PEM–CAs**
  - **Cross–Zertifizierungen / Nicht–DFN–Mitglieder**
  - **Kooperation auf internationaler Ebene**
- **Mitarbeiter**

Britta Liedtke, Ingmar Camphausen, Stefan Kelm

Die Veröffentlichung von PGP−Schlüsseln

- **Ausgangslage**

  »Jede zertifizierende Instanz der DFN−Hierarchie ist für die Bereitstellung der Zertifikate zuständig.«

  »Alle Zertifikate der DFN−Hierarchie sollen über ein DFN−weites X.500−Verzeichnis veröffentlicht werden.«

- **Derzeitige Praxis**
  - **Senden der Schlüssel an den weltweiten Keyserver−Verbund von pgp.net (WWW− und Email−Interface)**
  - **Ablage von Schlüsseln auf Informationsserven (WWW, FTP)**
  - **Vereinzelt: Ablage im X.500−Verzeichnis (proprietär)**

- **Die Situation für den Benutzer ist nicht zufriedenstellend**
  - **Überprüfung von Zertifikat*ketten* ist aufwendig**
  - **keine integrierten Lösungen**
  - **keine CA−übergreifenden Lösungen**
  - **bisherige Lösungen sind bestenfalls ''Workarounds''**

Motivation zur Zusammenarbeit

- **Probleme der bestehenden Keyserver–Lösung (Dank an Peter Gietz)**
  - **Instabile Software**
  - **Kein verteiltes System: Alle Keys auf allen Servern**
  - **Nicht beliebig skalierbar**
  - **Probleme bei der Replikation der Schlüssel**
- **Anforderungen an eine neue Lösung**
  - **Standardisierte Lösung**
  - **Schlüssel müssen nach verschiedenen Kriterien suchbar sein**
  - **Zertifizierungspfad muss verfolgt werden können**
  - **Schlüsselstatus muss abfragbar sein**
- **Fazit**
  - **CAs müssen alle Schlüssel in einer anwenderfreundlichen und gut administrierbaren Art und Weise veröffentlichen**
  - **Das KnowHow dafür ist verfügbar**

Die DFN–Projekte AMBIX und »Directory–Kompetenzzentrum« (DDS)

- **Projekt AMBIX seit 1994**
- **Aufgabe: Aufbau und Betreuung eines DFN–weiten E–Mail–Adreß–Verzeichnisses**
- **Projekt »Directory–Kompetenzzentrum« seit 1998 (DDS = DFN Directory Services)**
- **Aufgaben**
  - **Betreuung und Ausbau des E–Mail–Verzeichnisses**
  - **Betreuung des deutschland–zentralen DSAs PUMA**
  - **Entwicklung neuer Anwendungen im Bereich Directory**
  - **Beratung und Unterstützung von Anwendern im Bereich Directory**
  - **Bereitsstellung von Software der Firma »MessagingDirect« (vormals ISODE–Consortium)**
- **Mitarbeiter**

  Dr. Markus Sauer, Peter Gietz, Dr. Kurt Spanier, Bernhard Winkler, Eleni Anargirou

X.500–Datenbestand in Deutschland

- **Organisationen: ca. 260**
  - **von AMBIX verwaltet: ca. 130**
  - **auf PUMA verwaltet: ca. 100**
- **Personen: ca. 120.000 +**
  - **von AMBIX verwaltet: ca. 40.000**
  - **Uni Gießen: ca. 35.000**
  - **Tübingen: ca. 17.000**
  - **Uni Köln: ca. 11.000**
  - **Uni Konstanz: ca. 7.500**
  - **FH Nürnberg: ca. 5.800**

  - **Uni Stuttgart: ca. 10.000 (?)**
  - **LRZ–München: ???**
  - **PUMA: ca. 2.000**

»Standardisierung« der Ablage von PGP–Schlüsseln im X.500–Verzeichnis

- **1994: Erster IETF–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 DDS 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; Teilergebnisse der spärlichen Diskussion aufgenommen**
- **Seither Weiterentwicklung des Schemas als Grundlage eines »vorübergehenden« nationalen Alleingangs (RFC–Draft ist geplant)**

Das DDS–Modell in Kürze

- **PGP–Schlüssel werden in eigenständigen Einträgen abgelegt**
- **Schema ist gültig für PGPv2.x, PGPv5.x und PGPv6.0**
- **Zugriff ist möglich über DAP und LDAP (Browser, Web–X.500–Gateways, PGP)**
- **Zur Ablage der Informationen werden drei Objektklassen definiert:**
  - **pGPKeyContainer für Schlüssel–relevante Informationen**
  - **cAInformationObject für CA–relevante Informationen**
  - **pGPServerInfo für Key–Server–interne Informationen (wird von PGP benötigt)**
- **Im Personeneintrag wird über ein LDAP–URL und ein DN–Attribut auf den Schlüsseleintrag verwiesen**

X.500−Objektklasse für PGP−Schlüssel

pGPKeyContainer

pGPKeyEntryName	Name des Eintrags
pGPKey	ASCII−armored Schlüssel
pGPUserID	User−ID(s)
pGPPrimaryUserID	Primäre User−ID
pGPKeyID	Key−ID(s)
pGPFingerPrint	Fingerprint(s)
pGPKeySize	Schlüssellänge in Bit
pGPKeyType	Schlüssel−Algorithmus

---

pGPKeyCreateTime	Schlüsselerzeugung
pGPKeyExpireTime	Schlüsselverfall
pGPKeyRevoked	0 = gültig, 1 = revoked
pGPUsage	Verwendungszweck
uSerDN	X.500−DN der Person
description	Beschreibung

X.500−Objetklasse für CA−Informationen

cAInformationObject

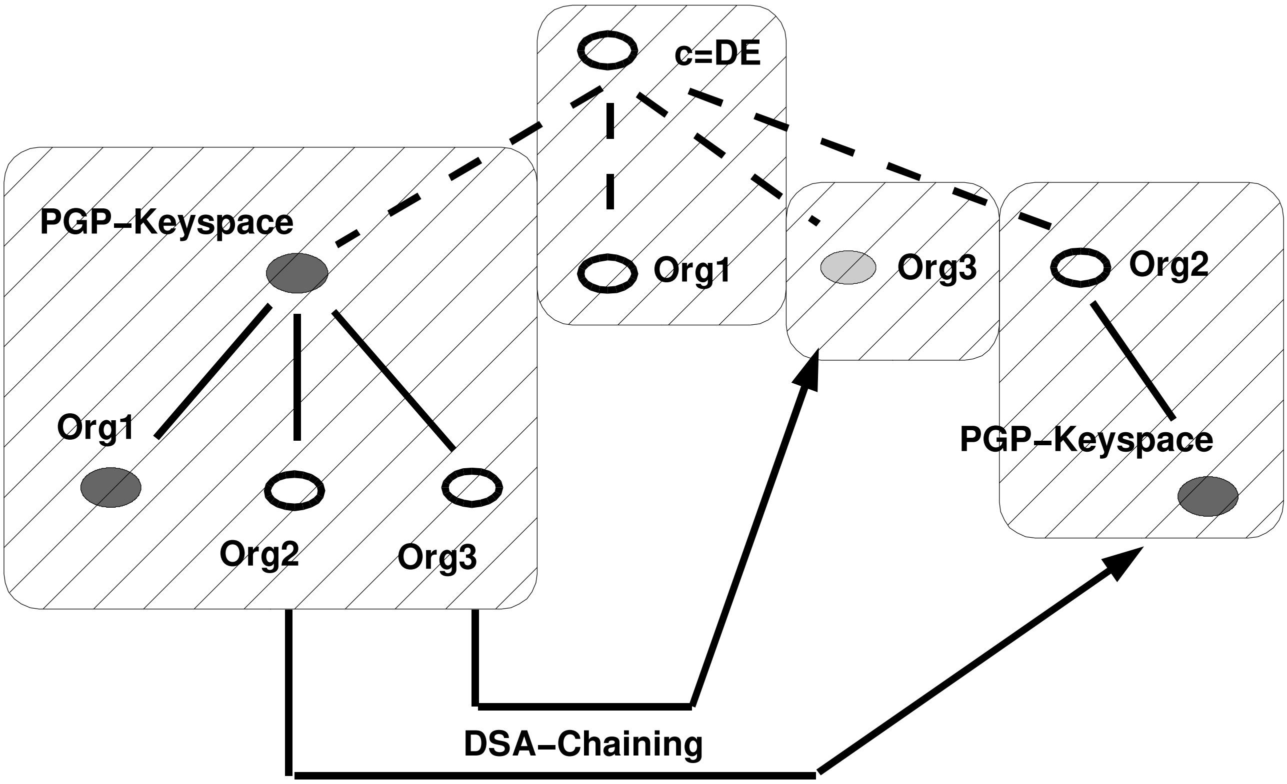
cACertKeyLink	**DN des zertifizierenden Schlüssels**
cACertKeyURL	**URL des zertifizierenden Schlüssels**
cADN	**DN der CA (oder RA)**
cAURL	**URL der CA (oder RA)**
keyOwner	**Schlüssel−Eigentümer (USER, CA, CA−Root, RA)**
keyCreationMode	**Schlüssel−Erzeugung (OWN, AUTO, CA)**
cAPolicy	**URL der CA−Policy**
cACRLLink	**URL der CA−CRL**
withPGPRevCert	**Revocation−Zertifikat (ja/nein)**

X.500−Objetklasse für Server−Info (PGP−spezifisch)

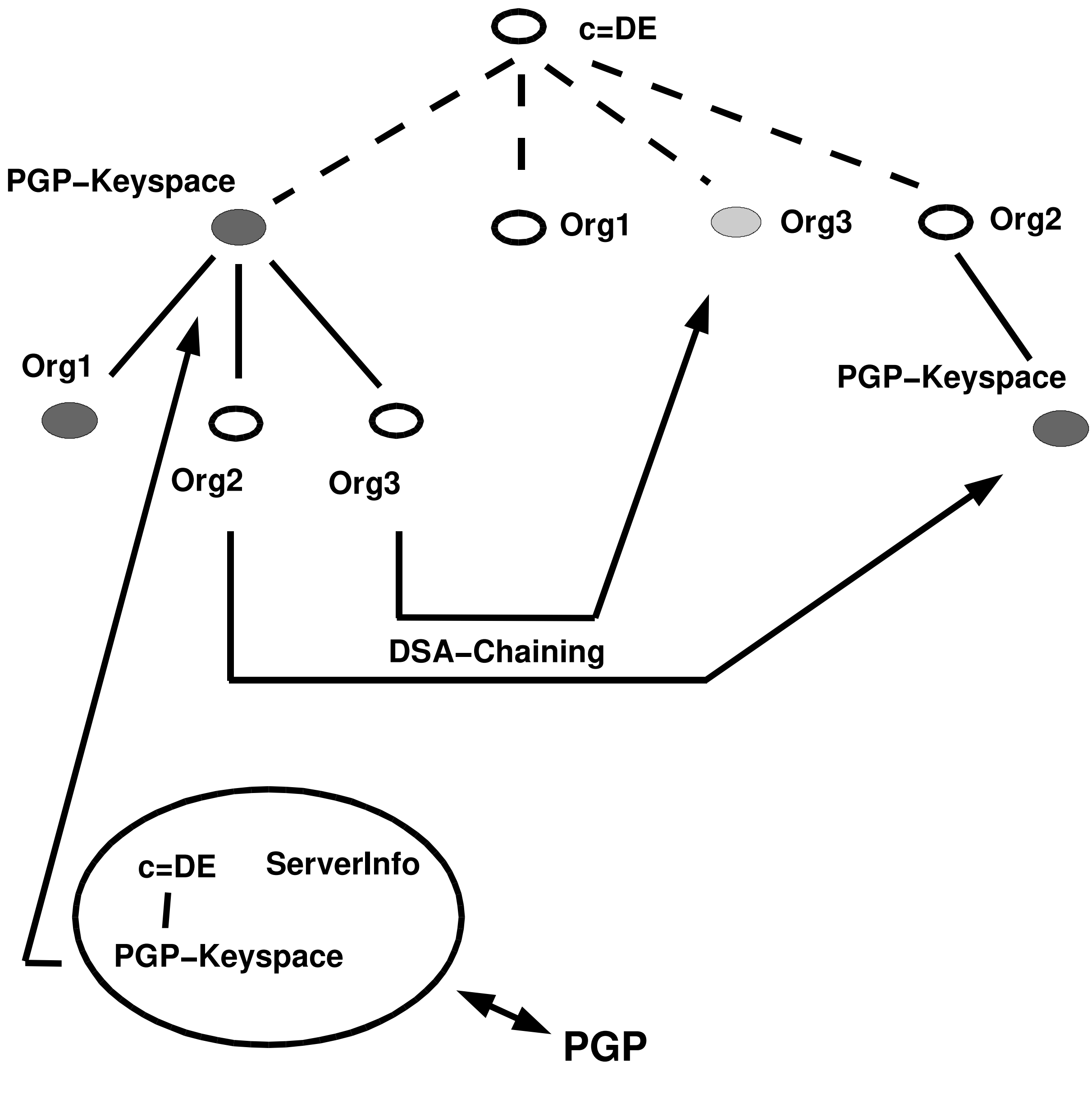
pGPServerInfo

cn	**Name des Eintrags (cn=pGPServerInfo)**
baseKeySpaceDN	**Start−DN des Schlüssel−Bereichs**
basePendingDN	**Start−DN von in Bearbeitung befindlichen Schlüsseln**

DIT–/Server–Struktur I

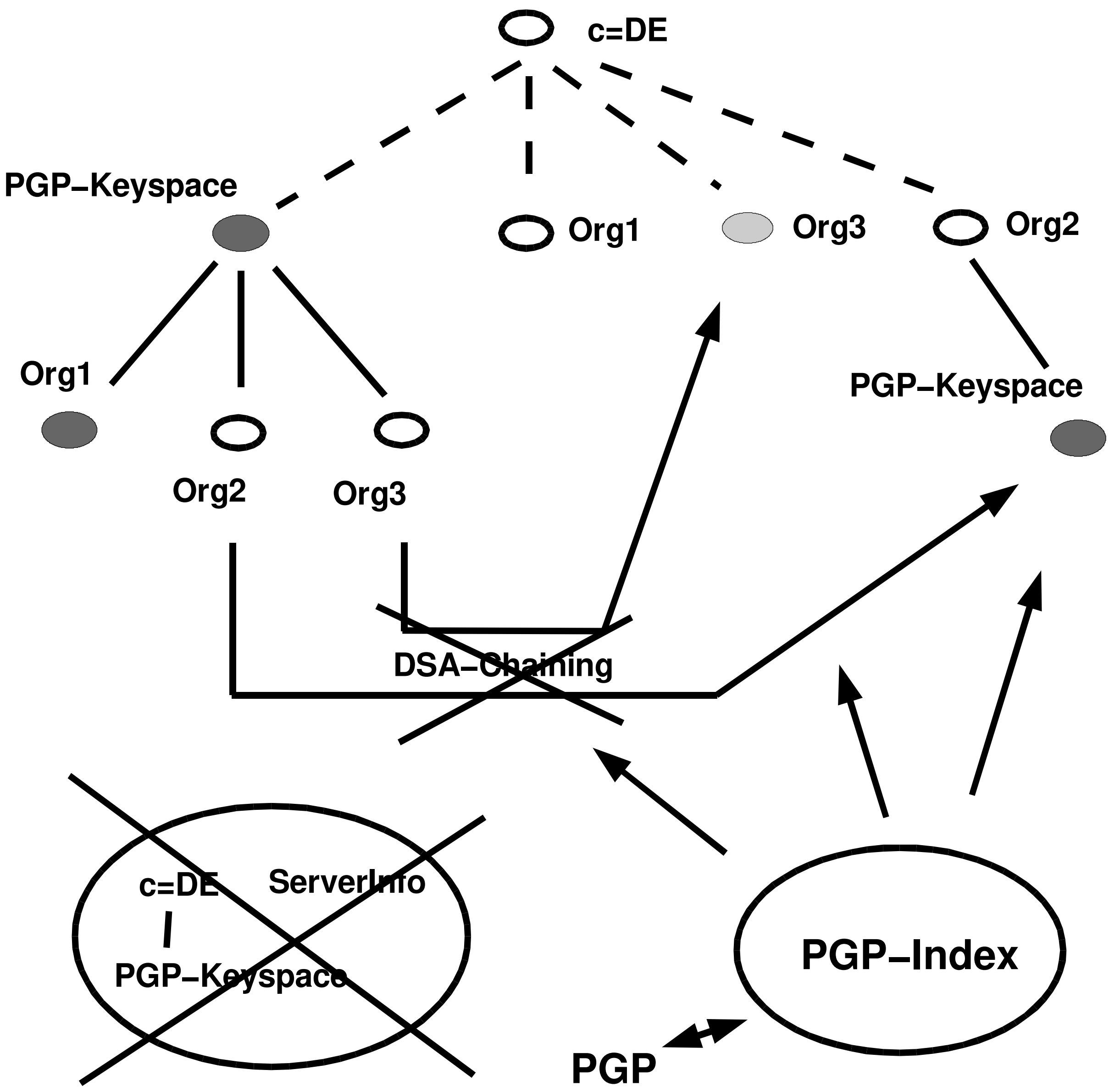


DIT–/Server–Struktur II



PGP: Zusammenarbeit PCA – DDS

DIT–/Server–Struktur III



Datenlieferungsformat I

CA: DFN PCA
SIG: Signatur–Key DFN–PCA
CA–URL: http://www.pca.dfn.de/dfnpca
CA–POLICY: http://www.pca.dfn.de/dfnpca/policy/wwwpolicy.html
CA–CRLLINK: http://www.pca.dfn.de/dfnpca/certify/pgp/pgpcrl.html

DATA

BEGIN–OF–KEYDEF

DATASET: PCA–Root
ACTION: new–dataset
KEYOWNER: CA

KEY: –––––BEGIN PGP PUBLIC KEY BLOCK–––––
Version: 2.6.2i

mQENAzal89oAAAEIAOEMbUtVDJhl6hOzY10DG6/TBb8QwUvNPBC ...
...
OY/sdJK7ue3R/aihWUHcOnA2/vNH4GU=
=/17y
–––––END PGP PUBLIC KEY BLOCK–––––
END–OF–KEY

CREATIONMODE: CA
REVCERT: YES
DESCRIPTION: TOP LEVEL CA des DFN
LABEL: Zertifizierungsschlüssel der DFN PCA

END–OF–KEYDEF

Datenlieferungsformat II

CA: DDS CA
SIG: Signatur–Key DDS–CA

DATA

BEGIN–OF–KEYDEF
DATASET: 0001
ACTION: new–dataset
KEYOWNER: USER

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

...
-----END PGP PUBLIC KEY BLOCK-----
END–OF–KEY

CREATIONMODE: USER
REVCERT: YES
USER: cn=Karl–Peter Gietz,o=AMBIX,l=DFN,c=DE
DESCRIPTION: AMBIX Mitarbeiter
LABEL: Mein PGP–Key
END–OF–KEYDEF

BEGIN–OF–KEYDEF
DATASET: 0002
ACTION: new–dataset
KEYOWNER: USER

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

Datenlieferung durch CAs in der Praxis

- **Lieferung von Daten durch die CA**
  - **Zertifizieren von Benutzerschlüsseln**
  - **Erstellen des Dateikopfes**
  - **Erstellen von Datensätzen pro User−Schlüssel**
  - **Signieren und Verschlüsseln der Datei**
  - **FTP−Übermittlung an DDS**
- **Verarbeitung von Daten durch DDS**
  - **Entschlüsseln und Prüfen der Signatur**
  - **Erzeugen der X.500−Datensätze pro Schlüssel**
  - **Erzeugen der Zertifizierungskette pro Schlüssel**
  - **Ablegen der Schlüssel im X.500−Verzeichnis**
  - **ggf. Nachtrag von Schlüsse−Verweises in User−Einträgen**
- **Änderung/Korrektur/Ergänzung von Schlüsseln durch CA und/oder Benutzer**

Zusammenfassung

- **Vorteil der einheitlichen Veröffentlichung von PGP–Schlüsseln im X.500 wird durch geringfügigen Mehraufwand »erkauft«: Erzeugung und Lieferung der PGP–Dateien**
- **Aktueller Stand des DDS–Modells**
  - **PGP–Testserver auf Basis eines Standalone–LDAP–Servers läuft und wird in Zusammenarbeit mit der DFN–PCA und der CA der Uni Stuttgart mit ersten Daten gefüllt (dient auch zum Verfeinern des Schemas, z.B. Für PGP 6.5.1i)**
  - **Policy für den Betrieb des Servers ist nahezu fertig**
  - **Datenlieferungsformat für CAs ähnlich den Organisations– und Personendatenformaten ist definiert**
  - **Programme zum Verarbeiten von Datenlieferungen sind fertig**
  - **Möglichkeiten zum Selbsteintragen und Ändern/Ergänzen von PGP–Schlüsseln für AMBIX–Personen sind einsatzbereit**
  - **Detaillierte Präsentation der Ergebnisse auf dem *Tutorium der DFN–PCA* (geplant: Frühjahr 2000) ist angestrebt**

Adressen und Infos

- **Mail–Adresse Projekt PCA**

  dfnpca@pca.dfn.de

- **WWW–Server Projekt PCA**

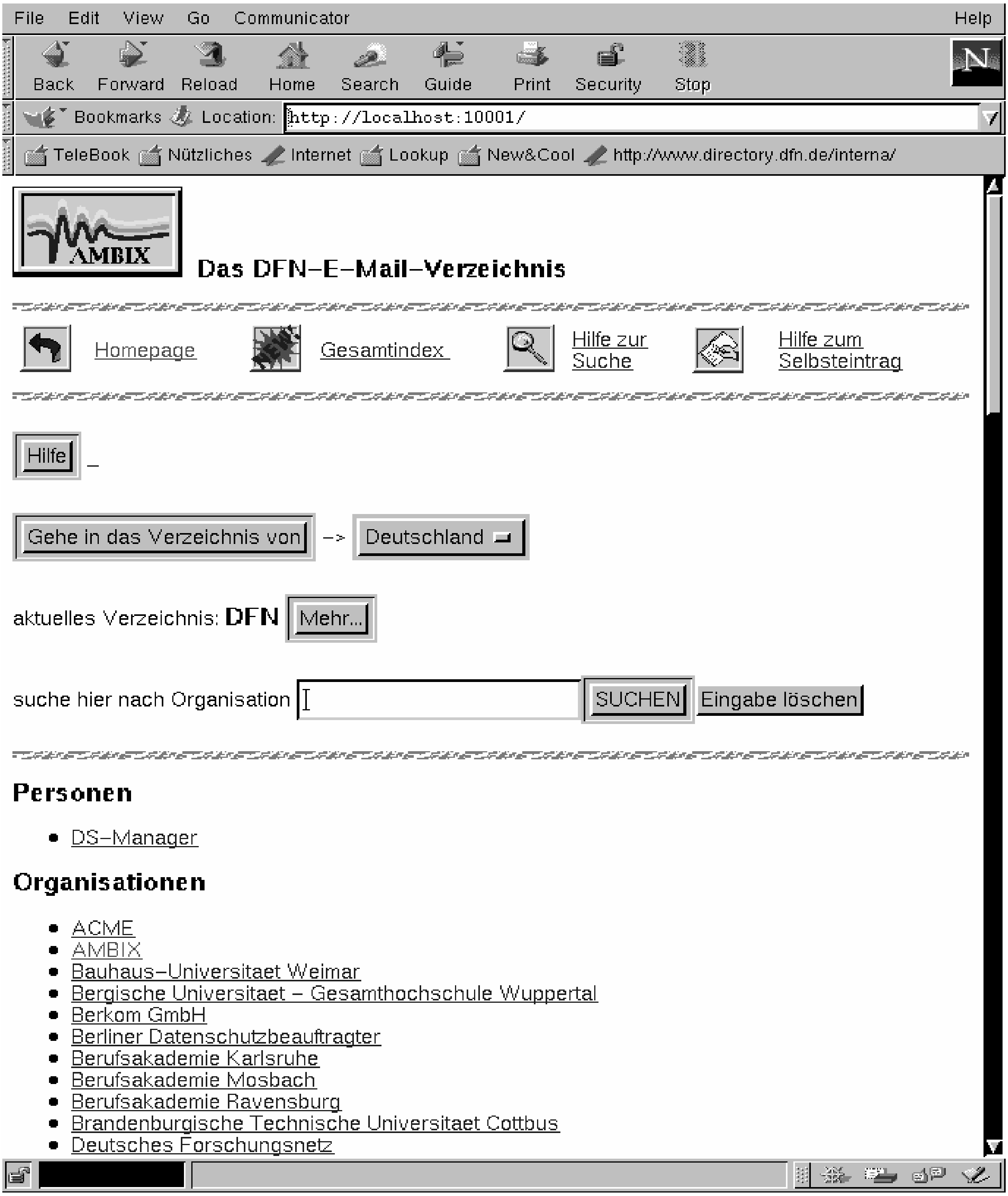
  http://www.pca.dfn.de

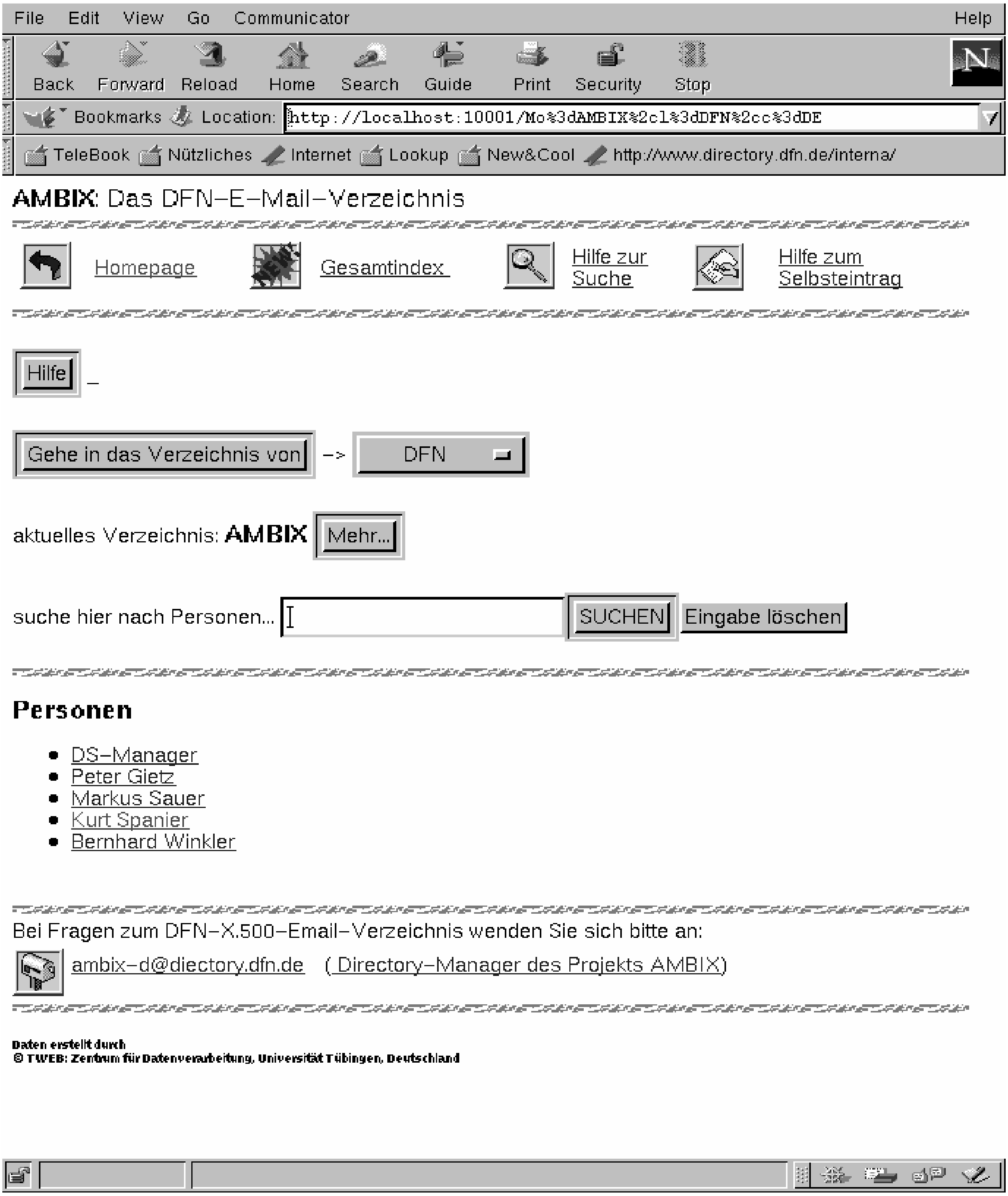
- **Mail–Adresse Projekt DDS**

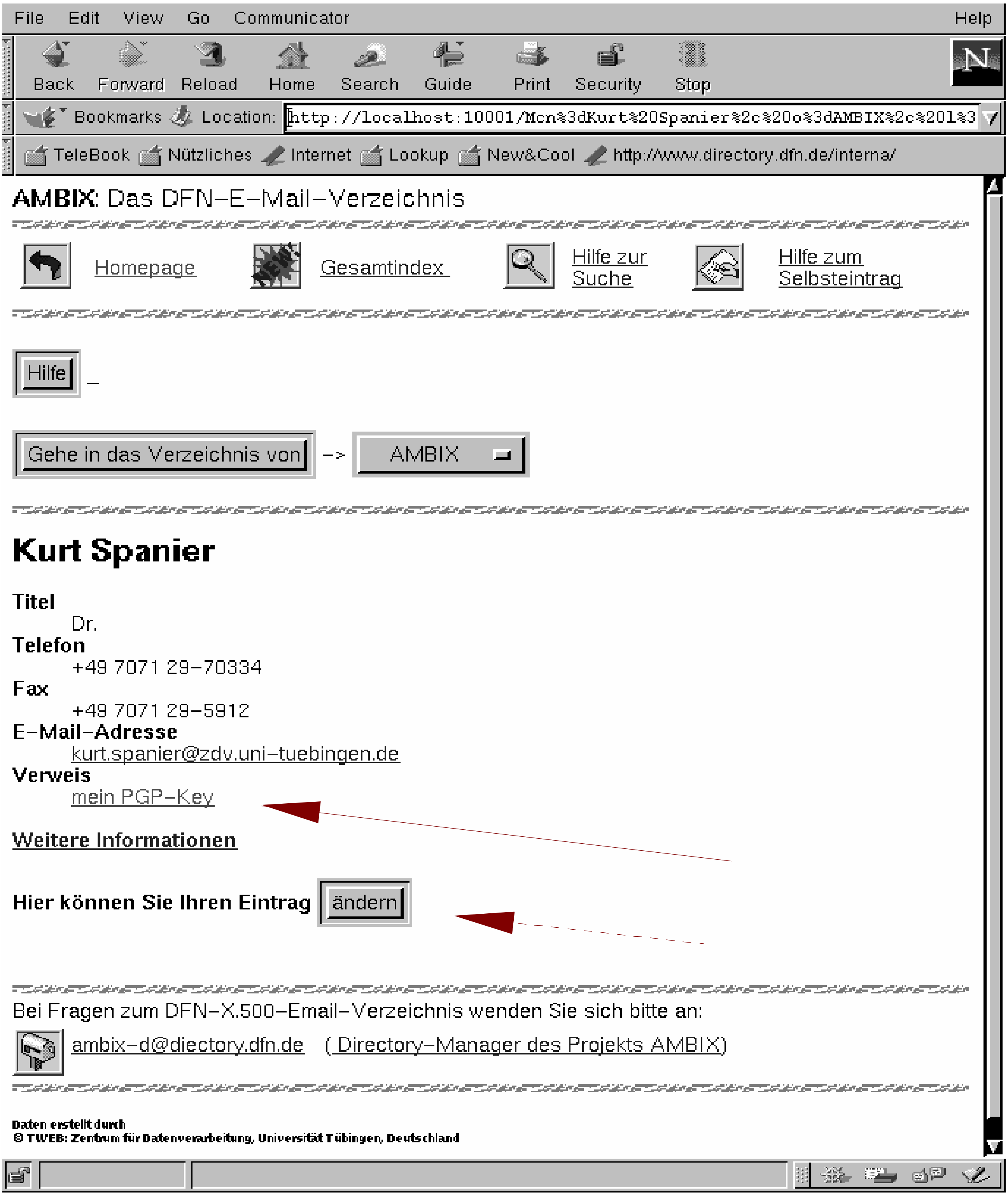
  ambix–d@directory.dfn.de

- **WWW–Server Projekt DDS**

  http://www.directory.dfn.de


File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://localhost:10001/
TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/
AMBIX
Das DFN–E–Mail–Verzeichnis
Homepage
Gesamtindex
Hilfe zur Suche
Hilfe zum Selbsteintrag
Hilfe
Gehe in das Verzeichnis von –> Deutschland
aktuelles Verzeichnis: DFN Mehr...
suche hier nach Organisation SUCHEN Eingabe löschen
Personen
DS–Manager
Organisationen
ACME
AMBIX
Bauhaus–Universitaet Weimar
Bergische Universitaet – Gesamthochschule Wuppertal
Berkom GmbH
Berliner Datenschutzbeauftragter
Berufsakademie Karlsruhe
Berufsakademie Mosbach
Berufsakademie Ravensburg
Brandenburgische Technische Universitaet Cottbus
Deutsches Forschungsnetz


File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://localhost:10001/Mo%3dAMBIX%2cl%3dDFN%2cc%3dDE
TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/
AMBIX: Das DFN–E–Mail–Verzeichnis
Homepage
Gesamtindex
Hilfe zur Suche
Hilfe zum Selbsteintrag
Hilfe
Gehe in das Verzeichnis von –> DFN
aktuelles Verzeichnis: AMBIX Mehr...
suche hier nach Personen... SUCHEN Eingabe löschen
Personen
DS–Manager
Peter Gietz
Markus Sauer
Kurt Spanier
Bernhard Winkler
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
© TWEB: Zentrum für Datenverarbeitung, Universität Tübingen, Deutschland


File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://localhost:10001/Mcn%3dKurt%20Spanier%2c%20o%3dAMBIX%2c%201%3
TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/
AMBIX: Das DFN–E–Mail–Verzeichnis
Homepage
Gesamtindex
Hilfe zur Suche
Hilfe zum Selbsteintrag
Hilfe
Gehe in das Verzeichnis von
–>
AMBIX
Kurt Spanier
Titel
Dr.
Telefon
+49 7071 29–70334
Fax
+49 7071 29–5912
E–Mail–Adresse
kurt.spanier@zdv.uni–tuebingen.de
Verweis
mein PGP–Key
Weitere Informationen
Hier können Sie Ihren Eintrag
ändern
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
© TWEB: Zentrum für Datenverarbeitung, Universität Tübingen, Deutschland

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: http://localhost:10001/Wldap://localhost:20000/pGPKeyEntryName=E8C0

TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/

Dr. Kurt Spanier (DDSD) <kurt.spanier@zdv.uni–tuebingen.de>

UserID
    Dr. Kurt Spanier (DDSD) <kurt.spanier@zdv.uni–tuebingen.de>
Schlüsseltyp
    RSA
KeyID
    E8C01575
Schlüssellänge
    01024
FingerPrint
    81 D9 7B EA BC FB F6 81 C4 12 FE 50 74 19 DC 82
Ascii–Armored Key (base64 encoded)

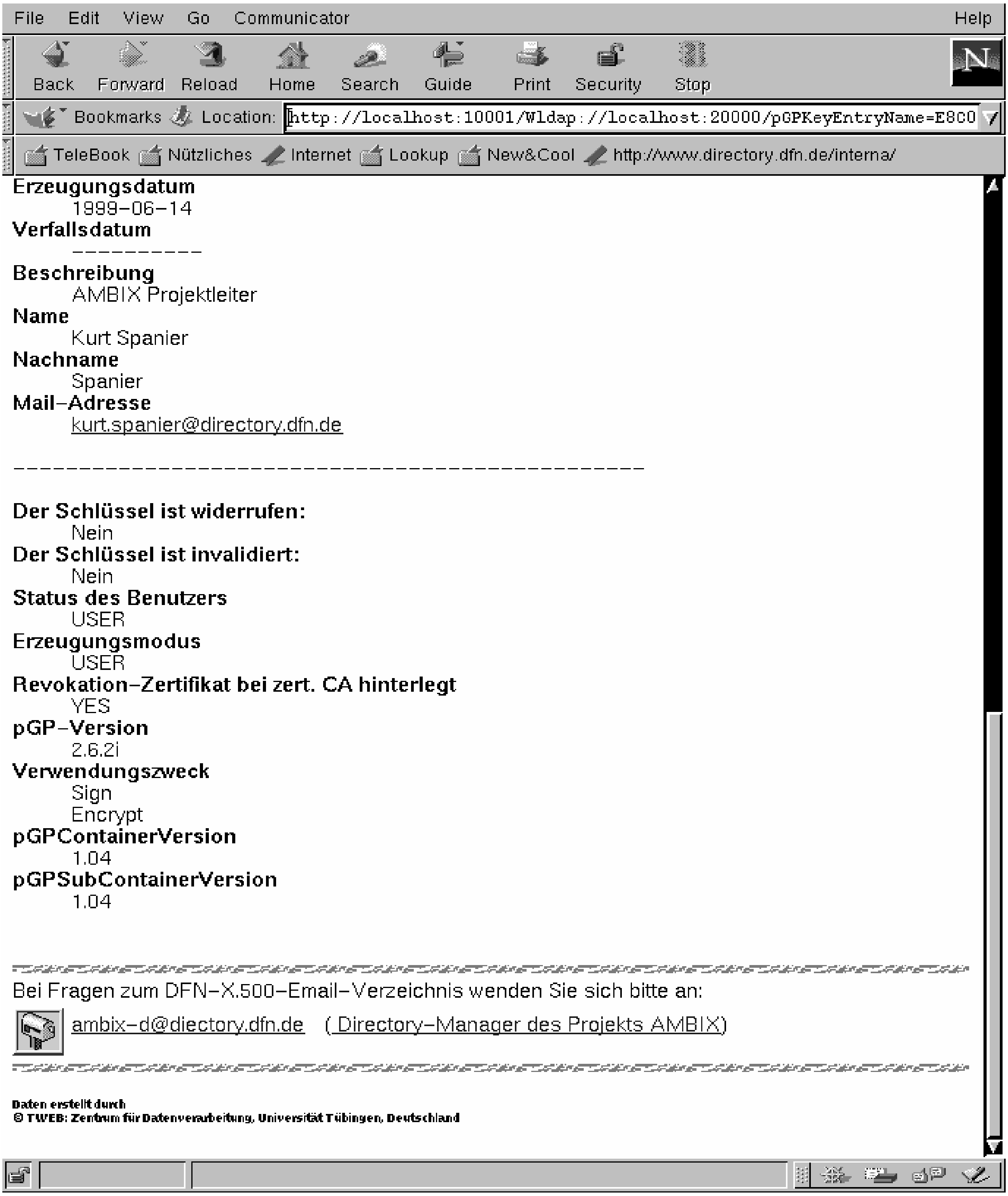
Sie können diesen Key mit Cut+Paste in einer Datei abspeichern – Hinweiszu Cut+Paste: Unter Linux markieren Sie den Text mit der linken Maustaste und speichern Ihn in ein offenes Dateifenster mit der rechten Maustaste / Unter Windows speichern Sie den markierten Text mit Bearbeiten/Kopieren und setzen Ihn in einem Editorfenster mit Bearbeiten/Einfügen :–)


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

mQCNAzdlB2kAAAEEAJsvq1NEYOloQ1dxpzRHP6eCfLJjBMhBBxsg0q/rMoncwStv
LfvzvrTGqnGsYlLd7w6dOxMgor6bGniyTOLEN9qPLcx84ZZ7f59QPdR8kMnET7LN
2zTrutsESrewQ7H5X8/zfDI67z7J39ogE0xsdiHg3g3PKb/FSixNvHDowBV1AAUR
tDtEci4gS3VydCBTcGFuaWVyIChERFNEKSA8a3VydC5zcGFuaWVyQHpkdi51bmkt
dHVlYmluZ2VuLmRlPokAlQMFEDdlAH/28v6AvoKyTQEBjAsD/A1hTDcOKFOkRupE
Vav9Qr5Ir33iK9/DpAin/LVX4xC9W4BaqQlOpKaZbCOuG2BxmnOcG1zK7r5ixrI2
Y0rjCrnqEkWDR6edcYNjnpEEco8Nqk7hz6J4ucQPXT/FJU01AQtWQS/MpCvRUiki
ZmJ+yr1bkJD6WHWmyqVt9ABJA4KTiQCVAwUQN2UHaSxNvHDowBV1AQG+PgQAiy3c
FBHrioyIrpAWBwde0hVjmufE28mzm8H0j1JUpZSntADiR6Bylic1Xv1al4a/FBzK
B/2mfxuBImu7heaXxEIYQzAUNWSHXy+Bo6fWg12Ku3Ekq5Yccxh/XPqK/WMQilWS
8ZJlTCWxxwJB9BYJZefAqYcNLP/xKMrYXukBnRE=
=7oSH
-----END PGP PUBLIC KEY BLOCK-----
```


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

Beschreibung
    AMBIX Projektleiter



Erzeugungsdatum
1999–06–14
Verfallsdatum

Beschreibung
AMBIX Projektleiter
Name
Kurt Spanier
Nachname
Spanier
Mail–Adresse
kurt.spanier@directory.dfn.de

Der Schlüssel ist widerrufen:
Nein
Der Schlüssel ist invalidiert:
Nein
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
© TWEB: Zentrum für Datenverarbeitung, Universität Tübingen, Deutschland

File Edit View Go Communicator Help

Back Forward Reload Home Search Guide Print Security Stop

Bookmarks Location: http://localhost:10001/Wldap://localhost:20000/pGPKeyEntryName=BE82

TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/

DFN-DIRECTORY, CERTIFICATION ONLY KEY (LowLevel: 1999-2000) <not-for-mail>

UserID
DFN-DIRECTORY, CERTIFICATION ONLY KEY (LowLevel: 1999-2000) <not-for-mail>
Schlüsseltyp
RSA
KeyID
BE82B24D
Schlüssellänge
01024
FingerPrint
4B 66 37 7D 79 1B 4E E9 00 2C CD B2 13 B4 25 C1
Ascii-Armored Key (base64 encoded)

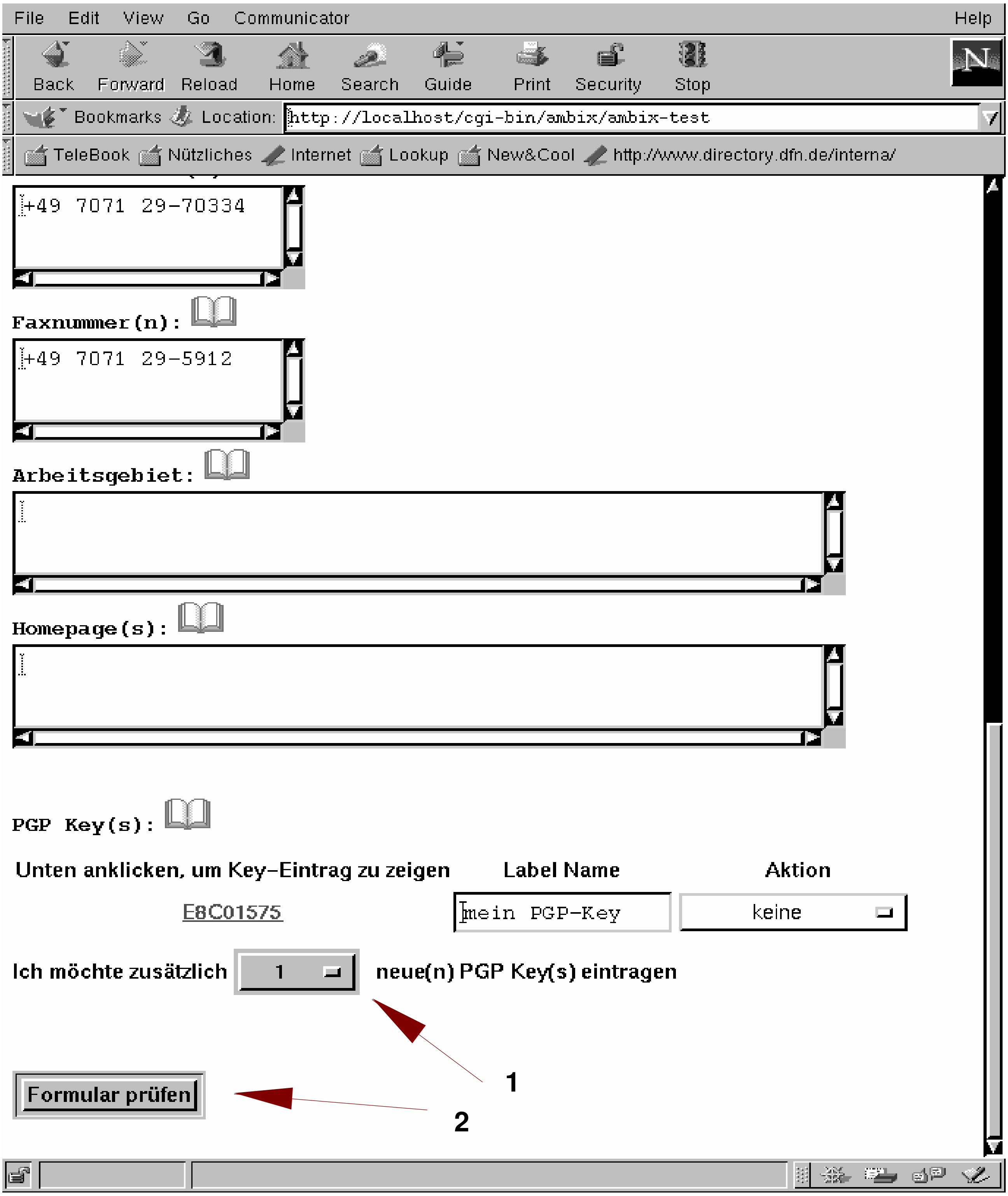
Sie können diesen Key mit Cut+Paste in einer Datei abspeichern - Hinweiszu Cut+Paste: Unter Linux markieren Sie den Text mit der linken Maustaste und speichern Ihn in ein offenes Dateifenster mit der rechten Maustaste / Unter Windows speichern Sie den markierten Text mit Bearbeiten/Kopieren und setzen Ihn in einem Editorfenster mit Bearbeiten/Einfügen :-)

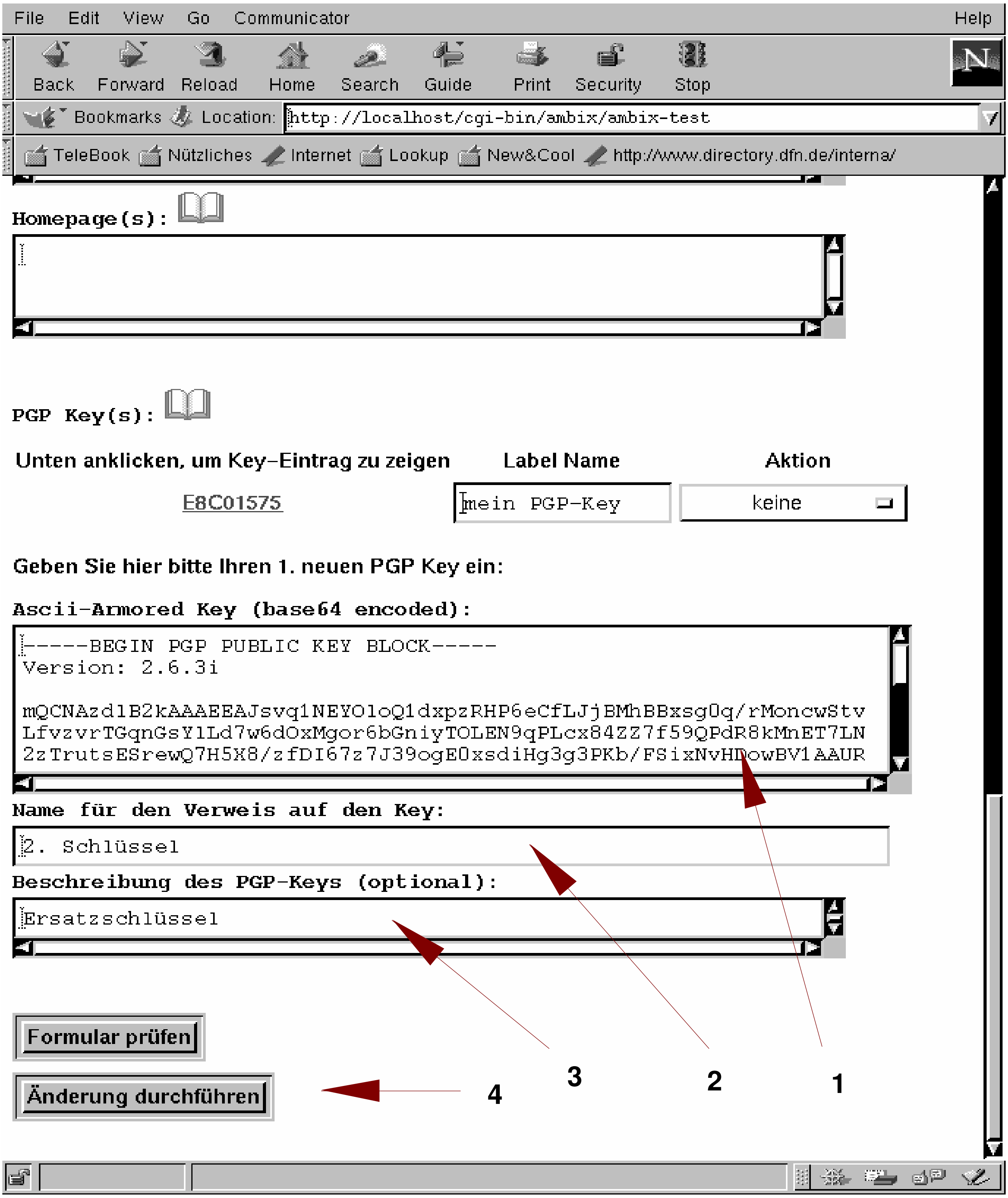

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAzdk6CYAAAEEAMHR8L6uPSrchXAD2mu4Dr6JxjUeLsXw1ePMEn24W4JnJTaF
kPWgcuRQd7WhXJZ3xJpuO0SFfYRqG8ViYIe3jGOKqrh5KZ4OsuDAGw218P7qz6tA
PlpAlaFR25PrzNN8uKt0MzKBLJV7XeZpN+Xxs9VVWw+e/WjXEfby/oC+grJNAAUR
tEpERk4tRElSRUNUT1JZLCBDRVJUSUZJQ0FUSU9OIE9OTFkgS0VZIChMb3dMZXZl
bDogMTk5OS0yMDAwKSA8bm90LWZvci1tYWlsPokAlQMFEDdk6NF4WnHpCU4PzQEB
Q5UD/0NV8ttTh62Wam7q1oc0R4DFKuNZSAlUHfhTUJfiej4OFUkEqsH/aZ2QHz8s
foAFVs5ynjjzzNgeHu3LqqiyjcEDjHdnSv1CMc4mrx24nAa1JnJGyUPj8co6Cikc
BnOowNA1CNXNDtIB9o4429pzsN58vYD7Xt3bqm/y9I9Ze1/5iQCVAwUQN2ToJvby
/oC+grJNAQEWxwP9FnX8GGRF52t+P3IVAQuOf15wFsEj1eoSk9Z8j8Jc8RCvxK/q
DzuiJaKQNNUNHU+17df7jpfU4SkMb3y0J/YFDDiDbsHhrP53TuVjdiJXHsM5V6U6
6UuBC1tKDqu20zIykBD+Qg94WGerdTV9wzmKC2gYMJz1s8+csu3D0erV4Cg=
=IEEO
-----END PGP PUBLIC KEY BLOCK-----
```


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

Beschreibung
CA DFN Directory Services Deutschland


File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://localhost/cgi-bin/ambix/ambix-test
TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/
+49 7071 29-70334
Faxnummer(n):
+49 7071 29-5912
Arbeitsgebiet:
Homepage(s):
PGP Key(s):
Unten anklicken, um Key-Eintrag zu zeigen
Label Name
Aktion
E8C01575
mein PGP-Key
keine
Ich möchte zusätzlich
1
neue(n) PGP Key(s) eintragen
Formular prüfen
1
2


File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://localhost/cgi-bin/ambix/ambix-test
TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/
Homepage(s):
PGP Key(s):
Unten anklicken, um Key-Eintrag zu zeigen
Label Name
Aktion
E8C01575
mein PGP-Key
keine
Geben Sie hier bitte Ihren 1. neuen PGP Key ein:
Ascii-Armored Key (base64 encoded):
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i
mQCNAzdlB2kAAAEEAJsvq1NEYOloQ1dxpzRHP6eCfLJjBMhBBxsg0q/rMoncwStv
LfvzvrTGqnGsYlLd7w6dOxMgor6bGniyTOLEN9qPLcx84ZZ7f59QPdR8kMnET7LN
2zTrutsESrewQ7H5X8/zfDI67z7J39ogE0xsdiHg3g3PKb/FSixNvHDowBV1AAUR
Name für den Verweis auf den Key:
2. Schlüssel
Beschreibung des PGP-Keys (optional):
Ersatzschlüssel
Formular prüfen
Änderung durchführen
4
3
2
1


File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://localhost/cgi-bin/ambix/ambix-test
TeleBook Nützliches Internet Lookup New&Cool http://www.directory.dfn.de/interna/
Wichtiger Hinweis: Ihre Änderungen werden erst durchgeführt, wenn Sie mit dem Button am Ende dieser Seite die Änderung bestätigen!
Bitte kontrollieren Sie nochmals die Richtigkeit Ihrer Daten:
Organisation
AMBIX
Kurt Spanier
Titel
Dr.
Telefon
+49 7071 29-70334
Fax
+49 7071 29-5912
E-Mail-Adresse
kurt.spanier@zdv.uni-tuebingen.de
bestehende Verweise
mein PGP-Key
neue Verweise
2. Schlüssel
Zu diesem Verweis wird folgender neuer PGP-Key-Eintrag angelegt:
Dr. Kurt Spanier (DDSD) (kurt.spanier@zdv.uni-tuebingen.de)
UserID Dr. Kurt Spanier (DDSD) (kurt.spanier@zdv.uni-tuebingen.de
KeyID E8C01575
Schlüssellänge 1024
FingerPrint 81 D9 7B EA BC FB F6 81 C4 12 FE 50 74 19 DC 82
Ascii-Armored Key (wie eingegeben)
Erzeugungsdatum 1999-06-14
Verfallsdatum ----------
Beschreibung Ersatzschlüssel
Schlüsseltyp RSA
Verwendungszweck Sign & Encrypt
Änderung bestätigen