DFN-PCA: PGP-Schlüsselinformationen

Low-Level Policy

PCA (Wurzelzertifikat):

Benutzer-ID:
`DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001) <not-for-mail>`
Schlüssel-ID: `63EB5391`
Schlüssellänge: 2048 Bits — Erstellungsdatum: `2000/12/28`
Fingerprint: `CF AF 6C 29 4E 57 4E 0E  E8 1C BD B4 54 FD 2A AB`

User-CA:

Benutzer-ID:
`DFN-User-CA, CERTIFICATION ONLY KEY (Low Level: 2001) <http://www.pca.dfn.de/dfnpca/>`
Schlüssel-ID: `90D2FCB1`
Schlüssellänge: 2048 Bits — Erstellungsdatum: `2001/01/04`
Fingerprint: `52 C1 3A D2 53 57 E0 35  9F 07 8C D9 36 16 16 85`

DFN-PCA (Kommunikationsschlüssel):

Benutzer-ID:
`DFN-PCA, ENCRYPTION KEY <dfnpca@pca.dfn.de>`
Schlüssel-ID: `E77ADB85`
Schlüssellänge: 2048 Bits — Erstellungsdatum: `1998/04/21`
Fingerprint: `48 BE 74 79 7F 5D BD 4C  65 2B 98 53 DD 5A 03 05`

DFN-PCA: PEM / X.509v1-Zertifikatinformationen

Medium-Level Policy

PCA (Wurzelzertifikat):

```
SubjectName:  C=DE, O=Deutsches Forschungsnetz, OU=PCA (Medium-Level)
IssuerName:   C=DE, O=Deutsches Forschungsnetz, OU=PCA (Medium-Level)
Validity:     NotBefore: Mon May  5 14:39:35 1997 (970505123935Z)
              NotAfter:  Thu Dec 31 12:00:00 1998 (981231110000Z)
Fingerprint:  BC99 C72C 0972 B5CC 9F13 DAD4 A588 F1A0
SubjectKey:   Algorithm rsa (OID 2.5.8.1.1), Keysize = 2048
```

Low-Level Policy

PCA (Wurzelzertifikat):

```
SubjectName:  C=DE, O=Deutsches Forschungsnetz, OU=PCA (Low-Level)
IssuerName:   C=DE, O=Deutsches Forschungsnetz, OU=PCA (Low-Level)
Validity:     NotBefore: Mon May  5 15:16:04 1997 (970505131604Z)
              NotAfter:  Thu Dec 31 12:00:00 1998 (981231110000Z)
Fingerprint:  8FCD 2151 532B C0EF 84CB BABA 1AA7 9CFD
SubjectKey:   Algorithm rsa (OID 2.5.8.1.1), Keysize = 2048
```

DFN-PCA: SSL / S/MIME / X.509v3-Zertifikatinformationen

World Wide Web Policy

DFN Top Level CA (Wurzelzertifikat):

```
Certificate:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA, \
            CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
    Validity
        Not Before: Oct 29 18:03:10 1998 GMT
        Not After : Dec 31 18:03:10 2001 GMT
    Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA, \
             CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
    X509v3 extensions:
        Key Usage:                    keyCertSign cRLSign
        Basic Constraints:            allowed to act as a CA !
        Identifier: Certificate Type
            Critical: no
            Certified Usage:
                SSL CA
                E-mail CA
                Object Signing CA
    MD5 Fingerprint=45:BB:9B:C8:8A:A4:84:8B:2D:A0:08:8F:9E:B6:B8:10
```

DFN Server CA:

```
Certificate:
    Version: 3 (0x2)
    Serial Number: 21 (0x15)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA, \
            CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
    Validity
        Not Before: Nov  2 16:47:24 2000 GMT
        Not After : Dec 30 18:00:00 2001 GMT
    Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA, \
             CN=DFN Server Certification Authority/Email=certify@pca.dfn.de
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
    X509v3 extensions:
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage:
            Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            F7:7B:75:D0:70:7A:A4:2A:44:03:5C:08:D3:AC:99:D1:1D:D3:09:76
        X509v3 CRL Distribution Points:
            URI:http://www.pca.dfn.de/dfnpca/certify/ssl/dfnpca.crx
            URI:http://www.pca.dfn.de/dfnpca/certify/ssl/dfnpca.crl
        Netscape Cert Type:
            SSL CA
    MD5 Fingerprint=69:2B:7C:0C:E9:9E:BD:4B:DA:60:9F:65:17:00:C8:ED
```

Stand: 10. Januar 2001