DFN-PCA: PGP-Schlüsselinformationen

Low-Level Policy

PCA (Wurzelzertifikat):

Benutzer-ID:
DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003) <http://www.dfn-pca.de/>
Schlüssel-ID: F2D58DB1
Schlüssellänge: 2048 Bits — Erstellungsdatum: 2001/11/20
Fingerprint: DE 31 69 0D BC 6A E7 79 4D CD A1 B5 81 80 FE 7B

User-CA:

Benutzer-ID:
DFN-User-CA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003) <http://www.dfn-pca.de/>
Schlüssel-ID: 7A9D7B59
Schlüssellänge: 2048 Bits — Erstellungsdatum: 2001/11/20
Fingerprint: 7A 0A DC 7B D6 B3 91 1D E6 75 6F E0 A7 43 AA 48

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

X.509 Policy

DFN Top Level CA (Wurzelzertifikat):

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1429501 (0x15cffd)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA, \
                CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
        Validity
            Not Before: Dec  1 12:11:16 2001 GMT
            Not After : Jan 31 12:11:16 2010 GMT
        Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA, \
                 CN=DFN Toplevel 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 Subject Key Identifier:
                06:0B:FA:B5:F8:48:78:A3:20:B1:0B:3E:CF:A0:D0:C4:D1:7F:7D:D0
            X509v3 Authority Key Identifier:
                keyid:06:0B:FA:B5:F8:48:78:A3:20:B1:0B:3E:CF:A0:D0:C4:D1:7F:7D:D0
                DirName:/C=DE/O=Deutsches Forschungsnetz/OU=DFN-CERT GmbH/OU=DFN-PCA \
                        /CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
                serial:15:CF:FD
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            X509v3 CRL Distribution Points:
                URI:http://www.dfn-pca.de/certification/x509/g1/data/crls/root-ca-crl.crx
                URI:http://www.dfn-pca.de/certification/x509/g1/data/crls/root-ca-crl.crl
            Netscape Revocation Url:
                https://www.dfn-pca.de/cgi/check-rev.cgi?
            Netscape CA Policy Url:
                http://www.dfn-pca.de/certification/policies/x509policy.html
            Netscape Comment:
                The DFN Top-Level Certification Authority
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11418.300.1.1
                  CPS: http://www.dfn-pca.de/certification/policies/x509policy.html

    SHA1 Fingerprint = 8E:24:22:C6:7E:6C:86:C8:90:DD:F6:9D:F5:A1:DD:11:C4:C5:EA:81
    MD5 Fingerprint =  3E:1F:9E:E6:4C:6E:F0:22:08:25:DA:91:23:08:05:03
```

DFN Server CA:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1430858 (0x15d54a)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA, \
                CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
        Validity
            Not Before: Dec  1 12:39:27 2001 GMT
            Not After : Dec  1 12:39:27 2005 GMT
        Subject: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, 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:
                E1:3E:0D:4F:98:9C:2E:5F:B8:A2:F4:42:83:A0:16:A9:2B:97:8B:39
            X509v3 Authority Key Identifier:
                keyid:06:0B:FA:B5:F8:48:78:A3:20:B1:0B:3E:CF:A0:D0:C4:D1:7F:7D:D0
                DirName:/C=DE/O=Deutsches Forschungsnetz/OU=DFN-CERT GmbH/OU=DFN-PCA \
                        /CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
                serial:15:CF:FD
            X509v3 CRL Distribution Points:
                URI:http://www.dfn-pca.de/certification/x509/g1/data/crls/root-ca-crl.crx
                URI:http://www.dfn-pca.de/certification/x509/g1/data/crls/root-ca-crl.crl
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            Netscape CA Policy Url:
                http://www.dfn-pca.de/certification/policies/x509policy.html
            Netscape Comment:
                This certificate was issued by the DFN-PCA, the Top
                Level Certification Authority of the German Research
                Network (Deutsches Forschungsnetz, DFN).
                The key owner's identity was authenticated in
                accordance with the DFN-PCA x509 Policy.
            Netscape Revocation Url:
                https://www.dfn-pca.de/cgi/check-rev.cgi
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11418.300.1.1
                  CPS: http://www.dfn-pca.de/certification/policies/x509policy.html

    SHA1 Fingerprint = C8:41:74:CE:DA:C2:02:87:B0:33:51:FE:67:07:CF:17:19:C1:12:F3
    MD5 Fingerprint =  A3:66:10:4B:AF:2C:6F:ED:D3:96:5B:33:4D:12:94:FC
```