DFN-PCA: PGP-Schlüsselinformationen

Low-Level Policy

PCA (Wurzelzertifikat):

Benutzer-ID:
`DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005) <http://www.dfn-pca.de/>`
Schlüssel-ID: `FDCB1C33`
Schlüssellänge: 2048 Bits — Erstellungsdatum: `2003/10/26`
Fingerprint: `96 B0 AD 7F B8 DC 00 18  DC A0 70 53 1C 3B 4D A5`

User-CA:

Benutzer-ID:
`DFN-User-CA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005) <http://www.dfn-pca.de/>`
Schlüssel-ID: `BB62BBA7`
Schlüssellänge: 2048 Bits — Erstellungsdatum: `2003/10/26`
Fingerprint: `4F 89 24 B6 71 D4 7B 92  D3 9E AA EB D3 A1 28 ED`

DFN-PCA (Kommunikationsschlüssel für 01.01.2004 – 31.12.2004):

Benutzer-ID:
`DFN-PCA (2004), ENCRYPTION Key <dfnpca@dfn-pca.de>`
Schlüssel-ID: `94E799B5`
Schlüssellänge: 2048 Bits — Erstellungsdatum: `2003-11-07`
Fingerprint: `A9 F8 2D C4 09 CC DA 7F  DC 67 8F E5 28 DE AA AC`

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

X.509 Policy

DFN Top Level CA Generation 1 (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 Generation 1.2:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 65372663 (0x3e581f7)
        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 09:15:02 2003 GMT
            Not After : Dec  1 09:15:02 2007 GMT
        Subject: C=DE, O=DFN-CERT Services 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)
                Modulus (2048 bit):
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                46:53:52:F5:93:A6:20:41:C1:66:D6:9F:15:E0:67:3E:8A:F7:8D:D2
            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
            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 = 2F:00:44:09:42:62:7B:CA:A6:BD:7C:F1:07:B1:63:14:F5:BB:1D:EB
    MD5 Fingerprint =  DE:8D:B3:7A:DA:68:E9:7C:D1:7B:FB:42:EE:F5:42:91
```

DFN Server CA Generation 1.1:

```
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
```