Informationen zur DFN-PKI

Der DFN-Verein organisiert mit dem Dienst DFN-PKI eine Public Key Infrastruktur, um digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Dabei liegt der Schwerpunkt auf fortgeschrittenen Zertifikaten auf Basis des X.509 Standards.

Viele Hochschulen und wissenschaftliche Einrichtungen wollen für eine sichere Kommunikation Zertifikate einsetzen, die Voraussetzungen und Anforderungen sind dabei allerdings sehr unterschiedlich. Der Dienst DFN-PKI bietet deshalb folgende Möglichkeiten zur Lösung der technischen und organisatorischen Aufgaben an:

- Auslagerung einer Zertifizierungsstelle an den DFN-Verein
- Betrieb einer eigenen Zertifizierungsstelle in der DFN-PKI
- Ausstellung von Grid Zertifikaten
- Ausstellung von Zertifikaten für die DFN-AAI
- Ausstellung von Einzelzertifikaten in der DFN-PKI
- Ausstellung von PGP-Zertifikaten

X.509 Zertifikate in der DFN-PKI werden in verschiedenen Sicherheitsniveaus entsprechend der jeweiligen Policy ausgestellt:

Sicherheitsniveau	Identifizierung	Wurzelzertifikat	Betreiber der CA
Global	Persönlich	In Standardbrowsern verankert	DFN-Verein
Classic	Persönlich	Selbstsigniert	DFN-Verein, Anwender, Dritte
Basic	Auch schwächer als persönlich	Selbstsigniert	DFN-Verein, Anwender, Dritte

PGP-Zertifikate werden nach der DFN-PGP Policy ausgestellt.

Dieses Dokument enthält die aktuell in der DFN-PKI gültigen Wurzelzertifikate.

Weitere Informationen zum Dienst DFN-PKI: **www.pki.dfn.de**

Kontakt

Unterstützung bei organisatorischen Fragen (Nutzungsbedingungen, Verträge, Entgelte)	Unterstützung bei technischen Fragen (Zertifikaterstellung, Konfiguration, Policies)
Gerti Foest Dr. Marcus Pattloch	Jürgen Brauckmann Reimer Karlsen-Masur Jan Mönnich
E-Mail: pki@dfn.de	E-Mail: dfnpca@dfn-cert.de
DFN-Verein Alexanderplatz 1 D-10178 Berlin	DFN-CERT Services GmbH Sachsenstraße 5 D-20097 Hamburg
Telefon: +49 30 884299 955 Telefax: +49 30 884299 70	Telefon: +49 40 808077 580 Telefax: +49 40 808077 556

1. X.509 Wurzelzertifikate

• Sicherheitsniveau Global

Deutsche Telekom Root CA2 (Wurzelzertifikat)

Subject-DN	C=DE, O=Deutsche Telekom AG, OU=T-TeleSec Trust Center, CN=Deutsche Telekom Root CA 2
Issuer-DN	C=DE, O=Deutsche Telekom AG, OU=T-TeleSec Trust Center, CN=Deutsche Telekom Root CA 2
Zertifikat-Download	http://www.pki.dfn.de/root/globalroot
Fingerprint SHA-1	85:A4:08:C0:9C:19:3E:5D:51:58:7D:CD:D6:13:30:FD:8C:DE:37:BF
Fingerprint MD5	74:01:4A:91:B1:08:C4:58:CE:47:CD:F0:DD:11:53:08
gültig ab	09.07.1999
gültig bis	10.07.2019
Seriennummer	38 (0x26)
Schlüsselalgorithmus	RSA
Schlüssellänge	2048 bit
Zertifikatsperrlisten (CRLs)	http://www.pki.dfn.de/crl/globalcrl
Certification Practice Statement (CPS)	http://pki.telesec.de/service/DT_ROOT_CA_2/cps.pdf

Zertifikat der DFN-PCA
mit Browser-Integration durch Verkettung mit Deutsche Telekom Root CA2 Zertifikat

Subject-DN	C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Global - G01
Issuer-DN	C=DE, O=Deutsche Telekom AG, OU=T-TeleSec Trust Center, CN=Deutsche Telekom Root CA 2
Zertifikat-Download	http://www.pki.dfn.de/root/globalroot
Fingerprint SHA-1	F0:28:8F:DA:C6:3A:F7:9A:31:9A:E9:72:F3:95:09:0E:A3:EF:E9:45
Fingerprint MD5	CA:5A:00:CF:78:D1:4B:A7:E1:7F:DE:59:67:71:3A:BC
gültig ab	Dec 19 10:29:00 2006 GMT
gültig bis	Jun 30 23:59:00 2019 GMT
Seriennummer	199 (0xc7)
Schlüsselalgorithmus	RSA
Schlüssellänge	2048 bit
Zertifikatsperrlisten (CRLs)	http://www.pki.dfn.de/crl/globalcrl
Policy (CP und CPS)	http://www.pki.dfn.de/policies

• Sicherheitsniveau Classic

Zertifikat der DFN-PCA (Wurzelzertifikat)

Subject-DN	C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Classic - G01
Issuer-DN	C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Classic - G01
Zertifikat-Download	http://www.pki.dfn.de/root/classicroot
Fingerprint SHA-1	12:63:41:60:D0:8C:FE:6A:87:6D:F7:86:D3:AD:C2:F7:74:FF:21:9F
Fingerprint MD5	EF:08:E6:9F:6A:C7:25:2C:58:8C:55:FD:45:13:31:0A
gültig ab	Feb 28 00:29:37 2005 GMT
gültig bis	Apr 28 00:29:37 2013 GMT
Seriennummer	1 (0x1)
Schlüsselalgorithmus	RSA
Schlüssellänge	2048 bit
Zertifikatsperrlisten (CRLs)	http://www.pki.dfn.de/crl/classiccrl
Policy (CP und CPS)	http://www.pki.dfn.de/policies

• Sicherheitsniveau Basic

Zertifikat der DFN-PCA (Wurzelzertifikat)

Subject-DN	C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Basic - G01
Issuer-DN	C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Basic - G01
Zertifikat-Download	http://www.pki.dfn.de/root/basicroot
Fingerprint SHA-1	35:5E:69:67:8E:B5:D7:2B:5D:C8:82:27:68:47:F2:7C:0D:3C:41:56
Fingerprint MD5	76:95:48:F0:40:72:3C:2B:A6:A1:A1:FD:CC:AF:7F:F4
gültig ab	Feb 28 00:25:34 2005 GMT
gültig bis	Apr 28 00:25:34 2013 GMT
Seriennummer	1 (0x1)
Schlüsselalgorithmus	RSA
Schlüssellänge	2048 bit
Zertifikatsperrlisten (CRLs)	http://www.pki.dfn.de/crl/basiccrl
Policy (CP und CPS)	http://www.pki.dfn.de/policies

- **Sicherheitsniveau Grid**

Zertifikat der DFN-PCA (Wurzelzertifikat)

Subject-DN	C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Grid - G01
Issuer-DN	C=DE, O=DFN-Verein, OU=DFN-PKI, CN=DFN-Verein PCA Grid - G01
Zertifikat-Download	http://www.pki.dfn.de/root/gridroot
Fingerprint SHA-1	1C:BB:D4:BA:97:7B:3A:B9:FF:CD:4A:97:77:50:87:9C:6A:2E:8E:38
Fingerprint MD5	41:39:4A:58:2E:F0:45:B2:29:28:F1:72:AB:F7:05:08
gültig ab	Jul 7 13:35:15 2005 GMT
gültig bis	Sep 7 13:35:15 2013 GMT
Seriennummer	1 (0x1)
Schlüsselalgorithmus	RSA
Schlüssellänge	2048 bit
Zertifikatsperrlisten (CRLs)	http://www.pki.dfn.de/crl/gridcrl
Policy (CP und CPS)	http://www.pki.dfn.de/policies

2. PGP DFN-PKI Schlüsselinformationen (DFN-PGP-Policy: 2008-2009)

Für die DFN PGP-CA werden folgende Wurzelzertifikate eingesetzt:

1. DFN-PGP-PCA
   Erstellungsdatum: 12. Dezember 2007

Benutzer-ID: DFN-PGP-PCA, CERTIFICATION ONLY KEY (DFN-PGP-Policy: 2008-2009) <http://www.pki.dfn.de/pgp>
Schlüssellänge/-algorithmus: 2048 Bit / RSA Key-ID: 0x7282B245 Key-Fingerprint : 39 D9 D7 7F 98 A8 F1 1B 26 6B D8 F2 EE 8F BB 5A

2. DFN-PGP-User-CA
   Erstellungsdatum: 12. Dezember 2007

Benutzer-ID: DFN-PGP-User-CA, CERTIFICATION ONLY KEY (DFN-PGP-Policy: 2008-2009) <http://www.pki.dfn.de/pgp>
Schlüssellänge/-algorithmus: 2048 Bit / RSA Key-ID: 0x6362BE8B Key-Fingerprint: 30 96 47 77 58 48 22 C5 89 2A 85 19 9A D1 D4 06