

Zertifikatsinformationen

Die Sparkasse Fürstenfeldbruck setzt zur sicheren Kommunikation per E-Mail ein System ein, das sowohl den Standard S/MIME als auch PGP beherrscht.

S/MIME Unternehmenszertifikat Sparkasse Fürstenfeldbruck CA

Das S/MIME Unternehmenszertifikat der Sparkasse Fürstenfeldbruck ist mit dem Algorithmus SHA-1 der Secure E-Mail CA der Sparkasse Fürstenfeldbruck signiert. Der zugrunde liegende Schlüssel hat eine Gültigkeitsdauer von 20 Jahren und eine Länge von 2048 Bit.

Der Schlüssel der Secure E-Mail CA der Sparkasse Fürstenfeldbruck ist von der Finanz Informatik Technologie Service (FITS) Root-CA signiert und hat eine Gültigkeitsdauer von 20 Jahren. Der diesem CA-Zertifikat zugrundeliegende Schlüssel hat eine Länge von 2048 Bit.

Der Schlüssel der Finanz Informatik Technologie Service Root CA besitzt eine Gültigkeitsdauer von 27 Jahren und eine Schlüssellänge von 1024 Bit.

Der Zertifikatsstandard bezieht sich auf das X.509 Format.

Die Zertifikate können unter auf unserer Internetseite über den Link

<https://www.sparkasse-ffb.de/content/dam/myif/sk-fuerstenfeldbruck/work/dokumente/pdf/service/sichere-e-mail/zertifikatsinfo.pdf>

heruntergeladen werden. In der Datei ist die gesamte X.509 Zertifikatskette enthalten (S/MIME Unternehmenszertifikat der Sparkasse Fürstenfeldbruck, Secure E-Mail CA der Sparkasse Fürstenfeldbruck, Finanz Informatik Technologie Service Root CA).

Fingerprint der Zertifikatsdatei:

Dateiname	Dateigröße	Hash-verfahren	Checksumme
Domainzertifikat-Sparkasse-FFB.zip	2.393 Bytes	MD5	bc31 420f 9c1b 6a18 b2f5 6f02 7799 9a3f
		SHA1	706d b1f9 4c8b ea7e 96fd 87aa 85ac 97b4 3884 c1ab
		SHA256	999d 5c51 c493 dc47 b8c4 9b6e b4af 176b 232e 46dd 0a77 9ee3 c348 bfd5 b814 e41d

Fingerprint der enthaltenen Zertifikate:

Zertifikat	Hash-verfahren	Fingerprint
QuoVadis Root Certification Authority	SHA1	de3f 40bd 5093 d39b 6c60 f6da bc07 6201 0089 76c9
QuoVadis Swiss Advanced CA G2	SHA1	a0 20 6d 6d 49 5d ba 4a 85 d3 77 20 b2 7a b8 8b 0e ed d5 9d

PGP Unternehmensschlüssel Sparkasse Fürstenfeldbruck

Für die Nutzer von PGP stehen die öffentlichen Schlüssel über den Link https://www.sparkasse-ffb.de/content/dam/myif/sk-fuerstenfeldbruck/work/dokumente/pdf/service/sichere-e-mail/pgp_domainschluesel_sparkasse_ffb.zip zur Verfügung.

Aufgrund von Kompatibilitätsproblemen mit neueren GnuPG-Versionen nutzen wir seit 09.08.2013 einen neuen Domainschlüssel.

Fingerprint der Schlüsseldatei:

Dateiname	Dateigröße	Hashverfahren	Checksumme
PGP-Domainschlüssel-Sparkasse-FFB.zip	2.892 Bytes	MD5	f9c5 ebf1 242b c30f 5666 39cd f5b9 f8d6
		SHA1	3876 38da 88a2 03be 7bdc bb8f 81cf dea1 ab22 23bd

Fingerprint der enthaltenen Schlüssel:

Zertifikat	Datum	Schlüssel ID	Länge	Fingerprint
Sparkasse Fuerstenfeldbruck Secure E-Mail PGP CA	09.08. 2013	0xCCBA5130	4096 Bit	FB17 CC2A 68E1 DD9F 26A5 F8FB 7BE3 A90C CCBA 5130
Sparkasse Fuerstenfeldbruck Secure E-Mail PGP CA	10.11. 2009	0x448C34BE	2048 Bit	530C 967C F82C 8405 57F5 EB08 6E3E C652 448C 34BE

Weiterführende Links

Web-Mailoberfläche für Sichere E-Mail:
<https://securemail.sparkasse.de/Sparkasse-Fuerstenfeldbruck/>