

Prüfprotokoll: 30.07.2025, 11:29:27 MESZ

Fachliche Prüfung:

Fachliche Prüfrichtlinie:	Kumulierte Ergebnis der einzelnen Signaturprüfungen ohne Berücksichtigung des Signaturniveaus.
Ergebnis der fachlichen Prüfung:	gültig
Meldungen:	Alle geprüften elektronischen Signaturen sind gültig.

Zusammenfassung Dokumente und Signaturprüfungen:

Nr. Dokument	Signiert durch	Signaturniveau	Signaturprüfung
1. Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf	Moritz Michael Wagner	EU-qualifizierte elektronische Signatur (EUMS-TL)	gültig

Dokument bzw. Containerstruktur:

CAdES-Dokument: Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf.pkcs7	
Signierte Datei oder Inhalt:	Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf
Signatur durch:	Moritz Michael Wagner
Signaturtyp:	Detached
Ergebnis der Signaturprüfung:	gültig
PDF-Dokument: Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf	
1. Revision	

Übersicht Prüfung der Signaturen:

CAdES: Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf.pkcs7	
Zeitpunkt der Durchführung der Prüfung:	30.07.2025, 11:29:26 MESZ
Signierte Datei oder Inhalt:	Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf
Signatur durch:	Moritz Michael Wagner
Niveau und Typ der Signatur:	EU-qualifizierte elektronische Signatur (EUMS-TL)
Behaupteter Signaturzeitpunkt:	29.07.2025, 16:47:24 MESZ
Prüfzeitpunkt der Signatur:	Behaupteter Signaturzeitpunkt
Ergebnis der Signaturprüfung:	gültig

Prüfung der Signaturen im Detail:

CAdES-Signatur B: Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf.pkcs7	
Zeitpunkt der Durchführung der Prüfung:	30.07.2025, 11:29:26 MESZ
Signierte Datei oder Inhalt:	Schreiben_an_Amtsgericht_Saarbrücken_1_Instanz_.pdf
Signatur durch:	Moritz Michael Wagner
Niveau und Typ der Signatur:	EU-qualifizierte elektronische Signatur (EUMS-TL)

Ermittlung des Signaturniveaus und des Typs	
Ergebnis:	EU-qualifizierte elektronische Signatur (EUMS-TL)
Meldungen:	Es wurde ermittelt, ob das digitale Zertifikat als ein EU-qualifiziertes Zertifikat für elektronische Signaturen, Siegel oder

Website Authentifizierung ausgestellt wurde. Bei Signaturen und Siegeln wurde zusätzlich ermittelt, ob sich die Signaturerstellungsdaten auf einer QSCD befinden. Die Ermittlung erfolgte auf Basis einer hoheitlichen Vertrauensliste (EUMS-TL). EU-qualifiziertes Zertifikat bestätigt durch Angaben im Zertifikat und in der verwendeten EUMS-TL. Die Signaturerstellungsdaten befinden sich auf einer QSCD.

Entscheidungsgrundlagen laut Vertrauensliste

Diensteanbieter:	Bundesnotarkammer
Dienstetyp:	Qualifizierter Vertrauensdienst zur Generierung von qualifizierten Zertifikaten (http://uri.etsi.org/TrstSvc/Svctype/CA/QC)
Dienstestatus:	Gewährt (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted_)
Ermittlungszeitpunkt des Dienstestatus:	06.12.2022, 15:45:49 MEZ
Startdatum des Dienstestatus:	17.02.2021, 17:30:00 MEZ
Zusätzliche Qualifizierungen des Zertifikats:	Zertifikat für elektronische Signaturen (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures_)
Link zu Details der verwendeten Vertrauensliste:	Vertrauensliste #1

Entscheidungsgrundlagen laut Angaben des VDA im Zertifikat

- Zertifikat für elektronische Signaturen gemäß eIDAS-Verordnung
- Qualifiziertes Zertifikat gemäß Signaturdirektive oder eIDAS-Verordnung
- Privater Schlüssel und öffentlicher Schlüssel im qualifizierten Zertifikat auf SSCD gemäß EU-Signaturdirektive oder auf QSCD gemäß eIDAS-Verordnung

Behaupteter Signaturzeitpunkt:	29.07.2025, 16:47:24 MESZ
Prüfzeitpunkt der Signatur:	Behaupteter Signaturzeitpunkt
Ergebnis der Signaturprüfung:	gültig
Verwendete Prüfrichtlinie mit Link:	Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO) #1
Verwendeter Algorithmenkatalog:	Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms v1.2 / BNetzA 2017)

Integritätsprüfung

Strukturspezifische Prüfung:	gültig
Mathematische Signaturprüfung:	gültig
Signaturalgorithmus:	SHA256 RSA (n = 3072) (e = 65537) PSS
Signaturalgorithmus für QES geeignet bis:	ohne Ablaufdatum
Ausgewählter Eignungszeitpunkt:	Zeitpunkt der Durchführung der Prüfung
Eignung zu diesem Zeitpunkt:	gültig

Zertifikatprüfungen

Gültigkeitsmodell für die Zertifikatskette:	Schale
Gültigkeitsmodell definiert in:	Verwendete Prüfrichtlinie
Prüfung des Zertifikats von Moritz Michael Wagner:	gültig

Angaben aus dem Zertifikat

Name des Inhabers:	Moritz Michael Wagner
--------------------	-----------------------

Inhaber

Name	Moritz Michael Wagner
Vorname	Moritz Michael
UID	DE.BRAK.83ab3cfb-5422-4eba-a55d-bbd655fea00b.13a2
Seriennummer	FS-10067172
Familienname	Wagner
Land	DE

Aussteller

Organisation	Bundesnotarkammer
Organisationseinheit	Zertifizierungsstelle
Name	BNotK rqSigt CA 2020
Organisationskennung	DE122788238
Land	DE

Allgemeines

Typ	X.509
Version	3
Gültig ab	06.12.2022, 15:45:49 MEZ
Gültig bis	05.12.2027, 15:45:49 MEZ
Seriennummer	2567194791560628543
	23 a0 82 0f b4 34 49 3f

Öffentlicher Schlüssel

Algorithmus	RSA/PKCS#1 v1.5
Schlüssellänge	3072 Bit
Modulus	00 e4 f5 b4 af 21 c5 08 88 17 fe 7e 67 f3 66 9d 9f e9 83 e8 3e 48 23 f9 6b 04 60 83 ed 12 76 96 77 09 08 7e a7 ba 70 52 e4 52 a9 ef a4 bb 62 36 5a 20 82 81 15 20 68 ad d4 68 af 2b b9 c8 eb 54 11 9b 5b 32 8b e8 75 a0 2f 20 9c 23 a9 01 5d 81 a4 e5 83 72 67 13 a5 bf 2e a9 3a 1b bd 2e ee 9c dd ec a3 b1 f5 44 20 7b f5 87 53 7b 38 90 ae 8e 9f 68 25 0a c0 b2 d8 5a 42 ea 89 cd 24 7b 3a 7d 7d 4e cd 9f 92 85 04 38 0f fe 89 64 cb 0a d4 4c 86 55 07 af 84 d4 23 4d e7 f4 4b e4 aa 55 3b 38 92 85 95 e1 59 2e d3 53 98 44 52 bf 62 b6 3d 3f 20 2f a0 d4 b1 88 c3 97 89 a8 50 91 0f 0e ea b9 b1 54 f0 a4 8f 18 7b 1e ff 4d 7c 22 a0 0f d3 4a 6e ca 2a ab 43 8b 33 96 30 8d 45 d1 aa 09 66 5d ab de ef eb ff 6b 6e a9 71 72 32 ab 76 cb 82 45 8d 77 61 07 19 e5 28 3f 15 fc bd 82 bd f6 62 83 1f 8f 60 e2 7c 10 5e 58 89 d9 9c e5 29 60 07 4b fb 94 62 49 3e 65 68 84 8e 77 f2 c4 89 72 30 89 91 53 60 14 d2 d8 cc 09 03 4c ec 2e b7 cf e3 ae 98 23 90 5c e2 7c d5 cd c2 d1 b6 48 fc 59 53 8a 9b 83 cf 27 b7 20 5f 4f 7b aa a8 03 64 21 07 86 aa c0 4c 8d e5 eb 79 cb 92 20 81 d5 cc 42 ce d5 4e c9 90 55 da ca e1 6d f0 8b 6a 18 ea 18 f2 fc 19 fb 41 46 4c 41 0b 49 60 72 8b 49 7b f7 c3 c0 01
Exponent	01 00 01

Signatur des Ausstellers

Signaturalgorithmus	SHA512withRSA/PSS
Signatur	0b 88 ad 18 98 6d 51 17 de fd 2a 6e 3b 0a f1 1c 63 94 6d 1d ef 19 6b 1f cf 81 22 da 5e b3 b1 b5 26 01 58 ad 83 32 7b d7 e9 71 26 a0 83 27 30 29 2a 8f 0b ae 58 ed 54 b5 4f 6e 40 96 5e 1c 3e 40 37 f9 e7 04 4d c6 31 91 86 85 3c 5e 4a 82 19 4d a4 04 28 2a a3 c4 d2 d6 97 48 59 c4 51 60 ac 35 c9 48 b7 eb ec 28 0a 4e 68 ab 6d ca 91 cd 87 44 f0 b6 14 da 09 fe 4f d2 ec 87 88 39 52 96 a9 f6 76 a5 69 02 16 c1 67 d2

79 89 fd d2 62 9f f5 84 b7 55 c8 f0 6e 2c 32 e3 49 f0 75 37 34 de c4 9f fb ef 73 98
 2a 94 71 8d 7f b5 b1 a2 d9 55 7e c0 89 36 ed 98 94 b7 78 b6 60 b6 f8 db 67 00 0b
 45 a1 44 ee f9 bb cc 38 c4 c0 40 47 13 60 2c 38 5a b1 3a a5 6b 93 cf 8c f8 d8 85 a4
 8d a5 38 c8 7a a1 56 9e ac 74 03 c1 e7 75 17 b9 73 fe 60 e0 9b 2d e7 c8 de 87 e2
 ea 02 1a 6c 8b 68 f9 81 48 fd e0 0e 6d e6 9f 15 de 5d 6c a2 49 68 e6 37 49 14 45
 f1 17 b8 98 9b 4d 93 04 43 85 73 c5 69 5a 2b 69 04 8f 12 90 66 b9 e2 a0 36 e8 61
 43 4a fc 5b 41 98 45 04 ce 99 f2 93 8e 5b b7 b6 f9 b6 de d1 41 29 c9 40 d6 e4 3f
 21 4e 24 83 a4 5a 44 76 75 41 a7 7d 85 42 e1 6d 62 7c 2a 79 38 25 c9 dd e8 b5 e1
 c8 28 35 fe 13 cd 08 9a c3 ac d6 15 2e 55 33 8b 41 f1 99 e9 27 8b b7 3b 0a d6 12
 05 48 d6 a5 e4 14 45 c3 ed 86 0a 45 f8 2e 1d f6 e0 34 c3 ec 84 1e 0d b2 c1 c3 d9
 5d 07 28 88 96 4a 9b ce 13 36 2c 6f 51 78 35 a8 b4 fa 78 0e e7 18 8e da 94 24 95
 9a 3c 3d f4 c2 ec e5 e5 bc 6d a5 1a a9 86 28 ca cf 86 b1 84 54 5f 41 78 40 e6 68 15
 8c 92 d7 a8 4a 74 b6 da 28 ea 2d 44 87 c2 67 f6 96 af a7 8e f4 fc 12 6d a0 fb c9 be
 bb ad 1a 38 47 9d 99 eb 51 be 50 69 67 39 91 32 91 a0 8b 88 7e

Fingerabdruck

SHA-1	bd bf 70 19 a3 7e da 3f 63 77 d5 57 55 4e 05 1d 54 dd da 9c
MD5	f1 37 1a bf 8a 56 8c c5 4c 81 e6 b6 e0 ac bd 50

Erweiterungen

Erweiterung	Allgemeine Einschränkungen (2.5.29.19)
Kritisch	Ja
Erweiterung	Zugangsinformationen des Ausstellers (1.3.6.1.5.5.7.1.1)
Kritisch	Nein
Zugriff auf	Ausstellerzertifikat
	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Zugriff auf	Online-Zertifikat-Status-Protokoll (OCSP)
	http://ocsp.zs.bnotk.de/eqsig
Erweiterung	Angaben zum qualifizierten Zertifikat (1.3.6.1.5.5.7.1.3)
Kritisch	Nein
	Qualifiziertes Zertifikat gemäß Signaturdirektive oder eIDAS-Verordnung (OID 0.4.0.1862.1.1)
	Privater Schlüssel und öffentlicher Schlüssel im qualifizierten Zertifikat auf SSCD gemäß Signaturdirektive oder auf QSCD gemäß eIDAS-Verordnung (OID 0.4.0.1862.1.4)
PKI Offenlegungserklärung (en)	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
PKI Offenlegungserklärung (de)	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Typ des qualifizierten Zertifikats	Zertifikat für elektronische Signaturen gemäß eIDAS-Verordnung (OID 0.4.0.1862.1.6.1)
Erweiterung	Zertifizierungsrichtlinien (2.5.29.32)
Kritisch	Nein
Zertifikatsrichtlinie	1.3.6.1.4.1.41460.5.1.1.2.1.4
	Certificate Practice Statement
	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Zertifikatsrichtlinie	1.3.6.1.4.1.41460.5.2.1.1.2.2.5
	Certificate Practice Statement
	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Zertifikatsrichtlinie	1.3.6.1.4.1.41460.5.3.1.1.2.2.3
	Certificate Practice Statement
	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	8b cb 83 86 29 8d f8 61 13 1d 4a 62 e9 89 8e 1f 01 e5 5a 7a
Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	69 2b 3f 5b 06 5c 24 ba 76 78 5d bb f1 fc b0 ac ec b5 02 cd
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja 01000000 Nichtabstreitbarkeit

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	2567194791560628543
Gültigkeitszeitraum:	06.12.2022, 15:45:49 MEZ bis 05.12.2027, 15:45:49 MEZ
Angaben zur Zertifikatsqualität:	EU-qualifiziertes Zertifikat Signaturalgorithmus auf qualifizierter sicherer Signaturerstellungseinheit (QSCD) Zertifikat für elektronische Signaturen gemäß eIDAS-Verordnung

Zertifikatsprüfung

Zertifikatsherkunft:	Mit der Prüfanfrage übermittelt
Mathematische Prüfung der Zertifikatsignatur:	gültig
Signaturalgorithmus:	SHA512 RSA (n = 4096) (e = 65537) PSS
Signaturalgorithmus für QES geeignet bis:	ohne Ablaufdatum
Ausgewählter Eignungszeitpunkt:	Zeitpunkt der Durchführung der Prüfung
Eignung zu diesem Zeitpunkt:	gültig
Prüfzeitpunkt des Zertifikats:	Behaupteter Signaturzeitpunkt
Prüfzeitpunkt der Signatur innerhalb Gültigkeitsintervall des Zertifikats:	gültig
Sperrstatus des Zertifikats:	gültig

Prüfung der Sperrstatusinformationen

Art der Sperrstatusermittlung:	OCSP-Antwort
Herkunft der Sperrstatusinformationen:	Online bezogen vom Vertrauensdiensteanbieter
Signatur durch:	BNotK rqSig OCSP Signer 2020
Ermittelter Status mindestens korrekt bis:	30.07.2025, 11:29:26 MESZ
Neuere Statusinformationen spätestens verfügbar ab:	nicht vorhanden
Signaturzeitpunkt der OCSP-Antwort bzw. CRL:	30.07.2025, 11:29:26 MESZ
Prüfzeitpunkt der Signatur der OCSP-Antwort bzw. CRL:	Behaupteter Signaturzeitpunkt
Ergebnis der Signaturprüfung der OCSP-Antwort bzw. CRL:	gültig

Verwendete Prüfrichtlinie mit Link:	Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO) #1
-------------------------------------	--

Integritätsprüfung

Mathematische Signaturprüfung:	gültig
Signaturalgorithmus:	SHA256 RSA (n = 3072) (e = 65537) PSS

Signaturalgorithmus für QES geeignet bis:	ohne Ablaufdatum
Ausgewählter Eignungszeitpunkt:	Zeitpunkt der Durchführung der Prüfung
Eignung zu diesem Zeitpunkt:	gültig

Zertifikatprüfungen

Gültigkeitsmodell für die Zertifikatskette:	Schale
Gültigkeitsmodell definiert in:	Verwendete Prüfrichtlinie
Prüfung des Zertifikats von BNotK rqSig OCSP Signer 2020:	gültig

Angaben aus dem Zertifikat

Name des Inhabers: BNotK rqSig OCSP Signer 2020

Inhaber

Organisation	Bundesnotarkammer
Organisationseinheit	Zertifizierungsstelle
Name	BNotK rqSig OCSP Signer 2020
Organisationskennung	DE122788238
Land	DE

Aussteller

Organisation	Bundesnotarkammer
Organisationseinheit	Zertifizierungsstelle
Name	BNotK rqSigt CA 2020
Organisationskennung	DE122788238
Land	DE

Allgemeines

Typ	X.509
Version	3
Gültig ab	27.12.2024, 15:41:13 MEZ
Gültig bis	26.09.2034, 16:41:13 MESZ
Seriennummer	4370895103649344012
	3c a8 89 f0 53 83 6a 0c

Öffentlicher Schlüssel

Algorithmus	RSA/PKCS#1 v1.5
Schlüssellänge	3072 Bit
Modulus	00 c6 1f e0 67 b2 19 49 b6 02 be 51 6e 0d ae 1f 89 fa d9 0a ef d3 27 49 ae fd 27 0d 64 2c e2 1d b6 e7 c0 92 6d 45 42 c3 3b 02 fc 91 43 58 0a 02 df ec 10 fb 88 e9 0f 32 39 07 0a 11 6e 44 44 3b 8e 67 40 44 22 61 9d d4 26 c7 60 ea cf 12 98 a1 de 72 09 51 b7 0b ac 7a 9b ad 83 c8 88 bd b6 fb d2 c3 ef f0 9a f9 69 2d df 65 f7 19 2c 4c a0 c0 df 3d b3 db 87 ff 0c 64 70 c1 46 fe 6a cb b3 f5 f7 44 d5 d8 b0 ce 64 1f 67 ea 5a 1e a9 ca 27 b4 1a d7 99 cb ae 0a 92 fe a8 8f 28 12 70 5d 9d d0 fb db cd 62 b7 93 20 cc 68 ea c0 64 8b a3 13 eb bb 06 42 4b a8 12 80 37 de ff c7 71 c3 36 fd 28 3f d7 7d 2f 96 78 35 b0 37 93 f8 ad b6 6b 99 e3 8a 5c 27 e4 31 2b a7 15 c0 0c 77 7a 0e 66 63 e2 b0 4c a3 60 4c 18 66 50 bb e0 3b 20 ce 13 7d b9 88 1e 0d b8 2f 3c d7 69 86 b1 77 cc 7c a4 35 9f 46 87 6c 19 bc 79 4d 1f 25 d8 ca 8d 7a c5 a3 99 31 83 5e f0 af c1 fc 7a 61 f0 71 a3 74 3b 3b 64 dc 44 21 f1 f3

85 e9 e1 d7 84 d5 06 70 23 cc ee 7a 28 ea ec 24 45 9a b7 bf 9d 1d 60 57 f4 59
e4 9a ce c6 be fb dd ec 45 d3 1e c8 8a a2 7c c0 b5 07 12 68 6f eb 4b cf f1 2c e5
7a a7 15 6d d9 d2 b2 8a a0 6b ee 59 dc 65 e7 de 77 e2 b1 3b 36 ee d2 64 06 41
d5 16 8c b6 17 36 79 37 5c 4c 41 a7 41

Exponent 01 00 01

Signatur des Ausstellers

Signaturalgorithmus	SHA512withRSA/PSS
Signatur	50 d7 78 cc 02 cd b5 81 f9 a2 12 ae f1 e6 69 1c 08 1d 1f 01 6f 1d fa 0a e5 98 7e 36 79 3a 73 f8 03 4a ab 56 bd 4d 68 b6 10 c8 9f f6 7b 2c c6 33 0e 1b e3 11 ff 16 6c f5 66 fe 6e d9 f1 12 39 4b 4c cb 8c 5c c5 29 df 32 0a 4c 52 46 c9 f1 8a 37 82 d7 5b b0 a8 74 0b bb 05 46 cf d1 15 b2 95 85 75 1b 11 7d 82 33 ca d7 7e 29 b9 bb 1a 99 39 34 2d e7 0d 93 ad ec 30 10 0f 35 90 69 ee 54 a0 05 aa 51 2e 77 ad 91 19 a9 6d 23 29 b5 3d 5b 09 db 4b 76 55 37 e4 b0 5c fb 90 c8 18 70 b2 14 36 04 a1 9f 9c b4 1a 06 73 59 84 f1 3e 19 33 9d 55 d2 b0 47 35 52 2e 2c 56 a6 ac 67 08 b8 f1 ad bd ba 88 39 c7 8d 89 5a 28 c7 ff 8f 8b 5a 29 f0 12 91 ec fc 81 14 6e 35 74 cf af 13 1e 87 f1 9a ef bc 3b 36 75 bc 52 a7 0b a8 55 c5 89 26 cf b0 70 4d 6a 8e 12 70 8a 63 1c 8d c6 cc 8d 54 e7 31 6e b1 2f e6 cb 38 9f b7 d7 12 82 80 27 3b d1 e6 fc a1 3f f8 e9 e9 28 01 6d fd 6d 47 09 f9 e1 d4 b8 c7 22 79 04 96 c6 2e 80 6b 84 a1 d0 d4 96 6d a2 ff fb f7 ba 83 8d a9 ca e7 b7 62 eb c7 e6 ea 8a 90 7d 68 01 32 97 8e 74 55 55 91 d8 4d 92 e0 89 eb bf 82 20 a7 4f 36 62 5b fb 77 6e d6 d1 c0 c6 76 0b 93 25 cc b0 99 06 4c f7 8d 7a 8f 3a de 01 8d 57 89 93 74 5f 9e 5b 1b b6 2a 8b 86 65 05 8f f9 cb d6 5d 9f 23 b8 62 49 2f ee a8 7e 6e 43 e5 33 28 74 ed 60 e4 ce a1 99 6c 27 d8 aa 6f 5d 6a ef 89 3b 0f 50 c2 33 c2 c8 bb ff 5c 51 fe 6c 49 16 97 61 70 a3 df 5d 8a 6a 77 34 eb 6a b2 8f d5 20 2e bc 93 a3 27 ab 3b 76 54 03 54 a2 e2 65 88 6d 02 a9 e9 10 f2 33 fc 3d cf d7 a1 d6 f8 5e fe ea 53 90 be fa 7e 4f 44 08 93 ce 74 cc 82 17 6c 40 53 7d 7b 45 1e ca 50 85 87 0e cb db ed 95 a9 8c

Fingerabdruck

SHA-1	b3 ee 22 ed 72 8c 2c 15 c4 6c 77 2b b6 89 67 8b e8 7c 3c 77
MD5	49 b4 2d 64 ee 59 4a 3c ce ba d2 9d c7 da d0 ff

Erweiterungen

Erweiterung	Allgemeine Einschränkungen (2.5.29.19)
Kritisch	Ja
Erweiterung	Keine OCSP-Prüfung (1.3.6.1.5.5.7.48.1.5)
Kritisch	Nein
Erweiterung	Angaben zum qualifizierten Zertifikat (1.3.6.1.5.5.7.1.3)
Kritisch	Nein
	Qualifiziertes Zertifikat gemäß Signaturdirektive oder eIDAS-Verordnung (OID 0.4.0.1862.1.1)
	Privater Schlüssel und öffentlicher Schlüssel im qualifizierten Zertifikat auf SSCD gemäß Signaturdirektive oder auf QSCD gemäß eIDAS-Verordnung (OID 0.4.0.1862.1.4)
Typ des qualifizierten Zertifikats	Zertifikat für elektronische Signaturen gemäß eIDAS-Verordnung (OID 0.4.0.1862.1.6.1)
PKI Offenlegungserklärung (en)	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
PKI Offenlegungserklärung (de)	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	8b cb 83 86 29 8d f8 61 13 1d 4a 62 e9 89 8e 1f 01 e5 5a 7a

Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	52 47 f9 0c 66 cf 48 1f ca e9 ef 7a 96 7a 70 e7 70 af 16 ae
Erweiterung	Erweiterte Schlüsselverwendung (2.5.29.37)
Kritisch	Nein
	OCSP-Signierung
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	10000000
	digitale Signatur

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	4370895103649344012
Gültigkeitszeitraum:	27.12.2024, 15:41:13 MEZ bis 26.09.2034, 16:41:13 MESZ
Angaben zur Zertifikatsqualität:	EU-qualifiziertes Zertifikat Signaturschlüssel auf qualifizierter sicherer Signaturerstellungseinheit (QSCD) Zertifikat für elektronische Signaturen gemäß eIDAS-Verordnung

Zertifikatsprüfung

Zertifikatsherkunft:	Aus der Inhaltsdatensignatur
Mathematische Prüfung der Zertifikatssignatur:	gültig
Signaturalgorithmus:	SHA512 RSA (n = 4096) (e = 65537) PSS
Signaturalgorithmus für QES geeignet bis:	ohne Ablaufdatum
Ausgewählter Eignungszeitpunkt:	Zeitpunkt der Durchführung der Prüfung
Eignung zu diesem Zeitpunkt:	gültig
Prüfzeitpunkt des Zertifikats:	Behaupteter Signaturzeitpunkt
Prüfzeitpunkt der Signatur innerhalb Gültigkeitsintervall des Zertifikats:	gültig
Sperrstatus des Zertifikats:	nicht geprüft
Meldungen:	Der Sperrstatus des OCSP-Signer-Zertifikats wurde nicht ermittelt. Gemäß Angabe im Zertifikat wird das Zertifikat innerhalb seines Gültigkeitsintervalls nicht gesperrt.

Prüfung des Zertifikats von BNotK rqSigt CA 2020:

Meldungen:

nicht geprüft

Das Zertifikat ist ein digitaler Dienste-Identifier (SDI) aus einer gültigen hoheitlichen Vertrauensliste (EUMS-TL). Gemäß verwendeter Prüfrichtlinie ist es damit ein Vertrauensanker und wird nicht geprüft.

Angaben aus dem Zertifikat

Name des Inhabers: BNotK rqSigt CA 2020

Inhaber

Organisation	Bundesnotarkammer
Organisationseinheit	Zertifizierungsstelle

Name	BNotK rqSigt CA 2020
Organisationskennung	DE122788238
Land	DE

Aussteller

Organisation	Bundesnotarkammer
Organisationseinheit	Zertifizierungsstelle
Name	BNotK Root CA 2017
Organisationskennung	DE122788238
Land	DE

Allgemeines

Typ	X.509
Version	3
Gültig ab	15.09.2020, 11:00:09 MESZ
Gültig bis	08.10.2037, 09:48:49 MESZ
Seriennummer	2482885588456368880
	22 74 fb 49 ad e0 ea f0

Öffentlicher Schlüssel

Algorithmus	RSA/PKCS#1 v1.5
Schlüssellänge	4096 Bit
Modulus	00 bf b0 06 00 dc 54 c0 6d b6 05 3b 1e 9e 1a 65 ed 78 00 1d 96 4d 1e 4b 03 1f 21 89 fd 4e 57 32 66 f5 91 b4 59 0e e5 85 ee 2b 60 bb 1a 22 c4 fd 9e de 3a a5 27 69 ca 56 b4 e7 f2 ba d1 28 fd 1c 74 8d 86 2e f0 aa ae dd 04 5d fe 94 15 98 5a fe ca 68 5f 2a bf 06 eb b5 5d 2e ca 65 40 81 62 6b d5 71 95 5c 66 fd e8 51 f5 37 c0 b8 d7 e8 58 5d a2 ab b3 16 34 1f c6 e3 e8 56 80 39 4d 12 ab 1f 53 5f 63 e5 93 64 d9 5d c2 d2 5a 96 98 33 81 89 0c 6a c5 d4 3e 70 48 14 8f 1c 47 a4 b2 8c c6 4d 40 a9 a3 03 6b d1 e3 27 39 7c d2 07 f7 c3 0d bd 7a 84 b0 14 35 b3 4b 63 1c 82 64 eb 90 e7 90 2b c2 bf 21 9a 63 f5 3d ef ca 96 09 0d 82 39 41 56 48 ae 9a 41 43 93 25 22 17 81 7a ed 5a 43 45 77 9f 11 61 6a f0 7f 5e cb 14 a0 b0 1b 0d e5 b8 f9 99 e7 2f 5a c6 79 61 ad 6c d5 60 36 10 7b 46 64 26 9c 69 4a e9 83 8a 52 69 d4 a6 ef d7 3c 51 5c 22 77 44 75 3b 16 ae 20 ae e1 09 7e 3d 8d 99 b7 28 6f 21 99 3e 2e ce 69 50 b8 1d 14 f3 c3 4a 1a 83 0e bf 64 78 f7 e5 6a de 1b 93 88 d2 77 d3 52 c0 c6 91 bc 8f f1 27 f6 81 7a 83 92 db ea ff 04 df 47 66 ea 4f 88 5e 49 3a 9c b7 0a c9 c7 49 a2 af cc 7b 53 35 f3 80 77 4c 66 44 64 8b a4 15 eb 5b d8 c2 48 bc 18 d7 0a 53 88 7a 20 04 8f c7 e2 f9 96 e9 15 da f8 59 65 75 7a 55 a5 a8 4a 23 ff dc e1 cb d2 eb 89 0a bf 94 64 0d 2d 42 66 ae 3d d7 a0 c8 bd 70 f0 83 92 fc 6f ec 32 36 cc ec c0 f3 ea 56 90 43 c5 20 e0 fd c6 46 55 a6 cf d1 16 52 1a 18 16 87 5b 0f f7 0a 73 f7 94 2e 02 51 d7 c6 b7 65 01 7c 23 04 db 11 62 db 8d 22 d1 76 7d 47 14 34 4c ba 9a d0 c0 9f 1f 8c e6 ba 18 3a f1 22 fd 08 0e c0 af 73 05 c2 3e f7 89 84 76 a0 33 9b
Exponent	01 00 01

Signatur des Ausstellers

Signaturalgorithmus	SHA512withRSA/PSS
Signatur	6d c4 b5 0f 7a 83 34 56 ce a2 00 9f 7d bc 89 18 05 f8 7a 46 ef 17 27 1a e8 d0 7b 4b bc 50 c3 d5 13 a7 d1 41 67 dc 46 e2 33 84 91 88 55 57 62 35 80 e1 eb 57 f8 8c 22 34 86 38 01 b8 0e 04 7c b9 f1 3e c2 d3 04 1f 63 b4 dd f1 7e 4c 67 16 8f 95 eb 81 a8 5d 22 b1 6e 9f c2 f4 fa 30 50 d3 10 05 d7 bb cb 17 9a 63 70 09 3f ab 2a 2a 3c 26 58 03 c5 4f 56 32 94 a4 98 c0 9c ec fc c6 86 88 d0 6f b2 b0 82 e8 f9 fa 88 7e bd 27 90 6f 8d 8d 00 4e 5c 09 8c e9 a1 02 17 0a 38 de ce d4 f9 d1 ff 66

69 a4 24 ff 25 e3 6f be 42 ff c4 35 dd fa 5e 3d 76 5f 44 f3 e4 f8 e6 b5 ca 4d 0d
 29 91 3f 5c bf 01 a5 7a 32 3a 13 2c 06 d8 e1 5a 83 1f 9b 05 a3 2a 38 06 7d 61
 3b bf 9d f1 96 87 a8 65 29 61 aa 80 a6 2c b1 12 66 9a 08 4f c2 c8 ad 44 1a ef f9
 21 bd 12 83 97 bf 26 9e 73 c2 fe f8 08 d5 9c 45 d3 db df 53 2f 6c e2 cf fb 69 7f
 30 b2 39 06 83 e7 74 8a 62 50 c4 28 20 30 8e dd 07 87 47 7a 3d b6 3a 51 ab 3f
 2e f7 12 53 ac 6f e7 6d 11 46 b0 79 8e 5a 66 1e 6b 81 7c ee c0 5f 21 f0 f0 79 42
 bd de 95 70 3a b2 8b 03 2c 8e f8 42 0c 56 4c 18 a6 75 74 f6 a1 11 33 48 7e bf c0
 57 ba cd 50 c7 f2 f3 72 f5 62 14 12 92 3e 7e 71 48 8c ae 22 ec f2 bb 62 53 ad 1b
 a7 57 49 67 09 ef 96 38 2f 44 05 86 30 37 ed bc 7b a0 3e 2a 32 fc e3 2e 22 7e
 9e ec 8f 54 4a 99 ab d2 a4 4a fb ed 84 16 a1 be af b5 81 27 a2 30 73 6d 98 84
 f0 a0 16 ac ee 9e 6f ab 31 ad 89 72 6a 7f a5 25 47 66 59 79 36 c3 9f 00 c8 15 fe
 51 93 3a d7 bf 3c 06 5b b7 81 e5 a0 72 f3 e0 37 fb 7a 41 bf 7f b5 e5 92 62 e5 a6
 04 93 7f aa 9f 85 fc c1 87 2d 6e 8c 55 46 e0 27 bf 18 b4 13 5a a0 ad f4 b8 52 a9
 c2 1d 93 34 ba

Fingerabdruck

SHA-1	16 d7 3d 28 49 e8 c2 1d 0b a0 cd fc b5 a5 6b 20 8d ba d2 da
MD5	50 b1 33 66 34 2f 94 13 17 4f 6a 83 92 8d 0c b0

Erweiterungen

Erweiterung	Allgemeine Einschränkungen (2.5.29.19)
Kritisch	Ja
	CA-Zertifikat
Erweiterung	Zugangsinformationen des Ausstellers (1.3.6.1.5.5.7.1.1)
Kritisch	Nein
Zugriff auf	Ausstellerzertifikat
	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Zugriff auf	Online-Zertifikat-Status-Protokoll (OCSP)
	http://ocsp.zs.bnotk.de/eqsig
Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	c5 30 47 07 a2 49 c7 4f 16 43 49 24 76 43 80 4a 7b 6d 8a 00
Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	8b cb 83 86 29 8d f8 61 13 1d 4a 62 e9 89 8e 1f 01 e5 5a 7a
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	00000110
	Zertifikatssignierung, CRL-Signaturverifizierung

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	2482885588456368880
Gültigkeitszeitraum:	15.09.2020, 11:00:09 MESZ bis 08.10.2037, 09:48:49 MESZ

Prüfung der verwendeten Vertrauensliste

Ergebnis der Prüfung der Signatur der verwendeten Vertrauensliste und LOTL:	gültig
Ergebnis der Prüfung der zeitlichen Gültigkeit der Vertrauensliste:	gültig

Link zu Details zur Vertrauensliste:	Vertrauensliste #1
Prüfung des Zertifikats von BNotK rqSigt CA 2020:	nicht geprüft
Meldungen:	Das Zertifikat ist ein digitaler Dienste-Identifier (SDI) aus einer gültigen hoheitlichen Vertrauensliste (EUMS-TL). Gemäß verwendeter Prüfrichtlinie ist es damit ein Vertrauensanker und wird nicht geprüft.
Angaben aus dem Zertifikat	
Name des Inhabers:	BNotK rqSigt CA 2020
Inhaber	
Organisation	Bundesnotarkammer
Organisationseinheit	Zertifizierungsstelle
Name	BNotK rqSigt CA 2020
Organisationskennung	DE122788238
Land	DE
Aussteller	
Organisation	Bundesnotarkammer
Organisationseinheit	Zertifizierungsstelle
Name	BNotK Root CA 2017
Organisationskennung	DE122788238
Land	DE
Allgemeines	
Typ	X.509
Version	3
Gültig ab	15.09.2020, 11:00:09 MESZ
Gültig bis	08.10.2037, 09:48:49 MESZ
Seriенnummer	2482885588456368880
	22 74 fb 49 ad e0 ea f0
Öffentlicher Schlüssel	
Algorithmus	RSA/PKCS#1 v1.5
Schlüssellänge	4096 Bit
Modulus	00 bf b0 06 00 dc 54 c0 6d b6 05 3b 1e 9e 1a 65 ed 78 00 1d 96 4d 1e 4b 03 1f 21 89 fd 4e 57 32 66 f5 91 b4 59 0e e5 85 ee 2b 60 bb 1a 22 c4 fd 9e de 3a a5 27 69 ca 56 b4 e7 f2 ba d1 28 fd 1c 74 8d 86 2e f0 aa ae dd 04 5d fe 94 15 98 5a fe ca 68 5f 2a bf 06 eb b5 5d 2e ca 65 40 81 62 6b d5 71 95 5c 66 fd e8 51 f5 37 c0 b8 d7 e8 58 5d a2 ab b3 16 34 1f c6 e3 e8 56 80 39 4d 12 ab 1f 53 5f 63 e5 93 64 d9 5d c2 d2 5a 96 98 33 81 89 0c 6a c5 d4 3e 70 48 14 8f 1c 47 a4 b2 8c c6 4d 40 a9 a3 03 6b d1 e3 27 39 7c d2 07 f7 c3 0d bd 7a 84 b0 14 35 b3 4b 63 1c 82 64 eb 90 e7 90 2b c2 bf 21 9a 63 f5 3d ef ca 96 09 0d 82 39 41 56 48 ae 9a 41 43 93 25 22 17 81 7a ed 5a 43 45 77 9f 11 61 6a f0 7f 5e cb 14 a0 b0 1b 0d e5 b8 f9 99 e7 2f 5a c6 79 61 ad 6c d5 60 36 10 7b 46 64 26 9c 69 4a e9 83 8a 52 69 d4 a6 ef d7 3c 51 5c 22 77 44 75 3b 16 ae 20 ae e1 09 7e 3d 8d 99 b7 28 6f 21 99 3e 2e ce 69 50 b8 1d 14 f3 c3 4a 1a 83 0e bf 64 78 f7 e5 6a de 1b 93 88 d2 77 d3 52 c0 c6 91 bc 8f f1 27 f6 81 7a 83 92 db ea ff 04 df 47 66 ea 4f 88 5e 49 3a 9c b7 0a c9 c7 49 a2 af cc 7b 53 35 f3 80 77 4c 66 44 64 8b a4 15 eb 5b d8 c2 48 bc 18 d7 0a 53 88 7a 20 04 8f c7 e2 f9 96 e9 15 da f8 59 65 75 7a 55 a5 a8 4a 23 ff dc e1 cb d2 eb 89 0a bf 94 64

Exponent	0d 2d 42 66 ae 3d d7 a0 c8 bd 70 f0 83 92 fc 6f ec 32 36 cc ec c0 f3 ea 56 90 43 c5 20 e0 fd c6 46 55 a6 cf d1 16 52 1a 18 16 87 5b 0f f7 0a 73 f7 94 2e 02 51 d7 c6 b7 65 01 7c 23 04 db 11 62 db 8d 22 d1 76 7d 47 14 34 4c ba 9a d0 c0 9f 1f 8c e6 ba 18 3a f1 22 fd 08 0e c0 af 73 05 c2 3e f7 89 84 76 a0 33 9b
	01 00 01

Signatur des Ausstellers

Signaturalgorithmus	SHA512withRSA/PSS
Signatur	6d c4 b5 0f 7a 83 34 56 ce a2 00 9f 7d bc 89 18 05 f8 7a 46 ef 17 27 1a e8 d0 7b 4b bc 50 c3 d5 13 a7 d1 41 67 dc 46 e2 33 84 91 88 55 57 62 35 80 e1 eb 57 f8 8c 22 34 86 38 01 b8 0e 04 7c b9 f1 3e c2 d3 04 1f 63 b4 dd f1 7e 4c 67 16 8f 95 eb 81 a8 5d 22 b1 6e 9f c2 f4 fa 30 50 d3 10 05 d7 bb cb 17 9a 63 70 09 3f ab 2a 2a 3c 26 58 03 c5 4f 56 32 94 a4 98 c0 9c ec fc c6 86 88 d0 6f b2 b0 82 e8 f9 fa 88 7e bd 27 90 6f 8d 8d 00 4e 5c 09 8c e9 a1 02 17 0a 38 de ce d4 f9 d1 ff 66 69 a4 24 ff 25 e3 6f be 42 ff c4 35 dd fa 5e 3d 76 5f 44 f3 e4 f8 e6 b5 ca 4d 0d 29 91 3f 5c bf 01 a5 7a 32 3a 13 2c 06 d8 e1 5a 83 1f 9b 05 a3 2a 38 06 7d 61 3b bf 9d f1 96 87 a8 65 29 61 aa 80 a6 2c b1 12 66 9a 08 4f c2 c8 ad 44 1a ef f9 21 bd 12 83 97 bf 26 9e 73 c2 fe f8 08 d5 9c 45 d3 db df 53 2f 6c e2 cf fb 69 7f 30 b2 39 06 83 e7 74 8a 62 50 c4 28 20 30 8e dd 07 87 47 7a 3d b6 3a 51 ab 3f 2e f7 12 53 ac 6f e7 6d 11 46 b0 79 8e 5a 66 1e 6b 81 7c ee c0 5f 21 f0 f0 79 42 bd de 95 70 3a b2 8b 03 2c 8e f8 42 0c 56 4c 18 a6 75 74 f6 a1 11 33 48 7e bf c0 57 ba cd 50 c7 f2 f3 72 f5 62 14 12 92 3e 7e 71 48 8c ae 22 ec f2 bb 62 53 ad 1b a7 57 49 67 09 ef 96 38 2f 44 05 86 30 37 ed bc 7b a0 3e 2a 32 fc e3 2e 22 7e 9e ec 8f 54 4a 99 ab d2 a4 4a fb ed 84 16 a1 be af b5 81 27 a2 30 73 6d 98 84 f0 a0 16 ac ee 9e 6f ab 31 ad 89 72 6a 7f a5 25 47 66 59 79 36 c3 9f 00 c8 15 fe 51 93 3a d7 bf 3c 06 5b b7 81 e5 a0 72 f3 e0 37 fb 7a 41 bf 7f b5 e5 92 62 e5 a6 04 93 7f aa 9f 85 fc c1 87 2d 6e 8c 55 46 e0 27 bf 18 b4 13 5a a0 ad f4 b8 52 a9 c2 1d 93 34 ba

Fingerabdruck

SHA-1	16 d7 3d 28 49 e8 c2 1d 0b a0 cd fc b5 a5 6b 20 8d ba d2 da
MD5	50 b1 33 66 34 2f 94 13 17 4f 6a 83 92 8d 0c b0

Erweiterungen

Erweiterung	Allgemeine Einschränkungen (2.5.29.19)
Kritisch	Ja
	CA-Zertifikat
Erweiterung	Zugangsinformationen des Ausstellers (1.3.6.1.5.5.7.1.1)
Kritisch	Nein
Zugriff auf	Ausstellerzertifikat
	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Zugriff auf	Online-Zertifikat-Status-Protokoll (OCSP)
	http://ocsp.zs.bnotk.de/eqsig
Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	c5 30 47 07 a2 49 c7 4f 16 43 49 24 76 43 80 4a 7b 6d 8a 00
Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	8b cb 83 86 29 8d f8 61 13 1d 4a 62 e9 89 8e 1f 01 e5 5a 7a
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	00000110

Zertifikatssignierung, CRL-Signaturverifizierung

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	2482885588456368880
Gültigkeitszeitraum:	15.09.2020, 11:00:09 MESZ bis 08.10.2037, 09:48:49 MESZ

Prüfung der verwendeten Vertrauensliste

Ergebnis der Prüfung der Signatur der verwendeten Vertrauensliste und LOTL:

gültig

Ergebnis der Prüfung der zeitlichen Gültigkeit der Vertrauensliste:

gültig

Link zu Details zur Vertrauensliste:

[Vertrauensliste #1](#)

Technischer Anhang

Prüfrichtlinien

Prüfrichtlinie #1

Herausgeber:	Governikus KG
Version:	1.3.0
Name:	Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO)
Bewertung der Prüfrichtlinie:	entspricht Governikus Prüfrichtlinie
Herkunft der Prüfrichtlinie:	automatisch bestimmt
Zertifikatsketten-Prüfmethode:	Schale
Prüfung der Eignung der Schlüsselverwendung für:	Signaturzertifikate (EE) Zwischenzertifikate (CA) Zeitstempelzertifikate OCSP-Signer-Zertifikate bzw. CRL-Signer-Zertifikate
Aktualität des Sperrstatuswertes berücksichtigen:	Zum in der Prüfrichtlinie festgelegten Vertrauensniveau des Prüfzeitpunktes (POE)
Maximales Alter des Sperrstatusantwort bei Prüfzeitpunkt	60 s
"Zeitpunkt der Durchführung der Prüfung":	
Eignung des Signaturalgorithmus zum behaupteten Signaturzeitpunkt ermitteln:	nein
Eignung des Signaturalgorithmus zum Zeitpunkt der Durchführung der Prüfung ermitteln:	nein
Wenn möglich, Eignung des Signaturalgorithmus zum abgesicherten Zeitpunkt in der Vergangenheit ermitteln:	ja
Verwendung von Vertrauensankern zulässig bei:	bestimmte SDI aus EUMS-TL (Zertifikate, OCSP, CRL, TST)
Notwendige Prüftiefe der Zertifikatsketten:	Normal
Maximal zulässige Cache-Zeit von OCSP-Antworten für CA-Zertifikate:	60 s
Maximal zulässige Cache-Zeit von OCSP-Antworten für EE-Zertifikate:	60 s
Alle Signaturprüfungen werden zu den behaupteten Signaturzeitpunkten durchgeführt:	ja
Zertifikat-Hashwert in OCSP-Antwort muss vorhanden sein:	nein
Sperrstatusermittlung nur über OCSP erlaubt:	ja
Minimal notwendiges Vertrauensniveau des Prüfzeitpunktes:	Behaupteter Signaturzeitpunkt

Prüfergebnis bei gesperrten Zertifikaten:	Ungültig
Prüfergebnis bei Prüfzeitpunkt ausserhalb des Gültigkeits- intervalls:	Unbestimmt
Verwendeter Algorithmenkatalog mit Link:	SOG-IS Agreed Cryptographic Mechanisms / BNetzA 2017
Prüfung der Vertrauensstellungen für Sperrstatus-Antworten:	ja

Vertrauenslisten (mit Erweiterungen)

Vertrauensliste #1

EU-Mitgliedsstaat:	Deutschland
Ausstellende Aufsichtsbehörde oder Stelle:	Bundesnetzagentur
Version:	143
Download-URL:	https://localhost:8443/Filemanager/rest/resources/OFFICIAL_TL_DE/SHA-256_e4dabbfeffc6c6d5562603ff25071364cb656fab0f6dc0a2e99e0691566211bf
Ausgegeben am:	23.07.2025, 15:30:15 MESZ
Nächste Aktualisierung spätestens am:	23.01.2026, 15:30:15 MEZ

Erweiterung zur Vertrauensliste #1

EU-Mitgliedsstaat:	Deutschland
Ausstellende Aufsichtsbehörde oder Stelle:	Governikus KG
Version:	127
Download-URL:	https://localhost:8443/Filemanager/rest/resources/OFFICIAL_TL_DE_EXTENSION/SHA-256_9f48b535f290ae-f73505282e0c635069a429198f9673de1502dfe58bf6d1f1d6
Ausgegeben am:	07.03.2024, 14:00:01 MEZ
Nächste Aktualisierung spätestens am:	07.09.2028, 00:00:00 MESZ

List of Trusted Lists (LOTL)

EU-Mitgliedsstaat:	Europäische Union
Ausstellende Aufsichtsbehörde oder Stelle:	Europäische Kommission
Version:	368
Download-URL:	https://localhost:8443/Filemanager/rest/resources/LOTL_SHA-256_9b01dfe2918acfccfc624e41fb142c40ad8df0e97e100d49164d8c4ec63f8ca
Ausgegeben am:	15.07.2025, 13:30:15 MESZ
Nächste Aktualisierung spätestens am:	13.01.2026, 13:30:15 MEZ

Algorithmenkataloge

Name:	Katalog Anwendung Governikus (SOG-IS V1.3/BNetzA 2017)
Version:	ALKAT_7_0_0
Land:	Deutschland
Veröffentlicht von:	Governikus KG im Auftrag des Lenkungsausschusses der Anwendung Governikus des IT-Planungsrates

Veröffentlicht am:	27.06.2023, 00:00:00 MESZ
Download-URL:	https://localhost:8443/Filemanager/rest/resources/ALGORITHM_CATALOG_SOGIS_PLUS/SHA-256_9996bba3d8be-c32350544f7c7b147093cd3d7393d91e9234908b8ccd8a3cb3c

Name:	Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms v1.2 / BNetzA 2017)
Version:	ALKAT_6_0_0
Land:	Deutschland
Veröffentlicht von:	Governikus KG im Auftrag des Lenkungsausschusses der Anwendung Governikus des IT-Planungsrates
Veröffentlicht am:	19.10.2020, 00:00:00 MESZ
Download-URL:	file:/C:/Program%20Files/Apache%20Software%20Foundation/Tomcat%209.0/webapps/PavonisService/WEB-INF/lib/cs_l_algo_catalog_files-3.2.0.jar!/algo_cat_sogis_plus.xml-signed.xml

Prüfinstanz

URL des Certificate Validation Servers:	https://cvs.governikus-asp.de:443/CertificateValidationServer/cvs
Kumulierte Wartezeit auf externe Antworten:	35 ms
Version des Certificate Validation Servers:	11.5.4
Version der Crypto Service Library:	3.2.3