Prüfprotokoll: 19.08.2025, 18:00:04 MESZ

Fachliche Prüfung:

Fachliche Prüfrichtlinie:	Kumuliertes 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.	132595a0-54d2-43c3-9828-e1a03820a12d.pdf	Hellenthal, Peter	EU-qualifizierte elektronische Signatur (EUMS-TL)	**gültig**

Dokument bzw. Containerstruktur:

CAdES-Dokument: Urschrift Protokoll (Diktat).pdf.pkcs7

Signierte Datei oder Inhalt:	132595a0-54d2-43c3-9828-e1a03820a12d.pdf
Signatur durch:	Hellenthal, Peter
Signaturtyp:	Detached
Ergebnis der Signaturprüfung:	**gültig**

PDF-Dokument: 132595a0-54d2-43c3-9828-e1a03820a12d.pdf

1. Revision

Übersicht Prüfung der Signaturen:

CAdES: Urschrift Protokoll (Diktat).pdf.pkcs7

Zeitpunkt der Durchführung der Prüfung:	19.08.2025, 18:00:04 MESZ
Signierte Datei oder Inhalt:	132595a0-54d2-43c3-9828-e1a03820a12d.pdf
Signatur durch:	Hellenthal, Peter
Niveau und Typ der Signatur:	EU-qualifizierte elektronische Signatur (EUMS-TL)
Behaupteter Signaturzeitpunkt:	19.08.2025, 17:59:50 MESZ
Prüfzeitpunkt der Signatur:	Behaupteter Signaturzeitpunkt
Ergebnis der Signaturprüfung:	**gültig**

Prüfung der Signaturen im Detail:

CAdES-Signatur B: Urschrift Protokoll (Diktat).pdf.pkcs7

Zeitpunkt der Durchführung der Prüfung:	19.08.2025, 18:00:04 MESZ
Signierte Datei oder Inhalt:	132595a0-54d2-43c3-9828-e1a03820a12d.pdf
Signatur durch:	Hellenthal, Peter
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:	Deutsche Telekom AG
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:	09.04.2024, 11:56:13 MESZ
Startdatum des Dienstestatus:	11.08.2022, 16:00:00 MESZ
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

- 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
- Qualifizierte Zertifikatsrichtlinie
- Qualifizierte Zertifikatsrichtlinie für natürliche Personen mit Schlüssel auf QSCD gemäß eIDAS-Verordnung

Behaupteter Signaturzeitpunkt:	19.08.2025, 17:59:50 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 ECDSA (p = 256) (q = 256)
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 Hellenthal, Peter:	**gültig**

Angaben aus dem Zertifikat

Name des Inhabers:	Hellenthal, Peter

Inhaber

Name	Hellenthal, Peter
Vorname	Peter
Land	DE
Familienname	Hellenthal
Seriennummer	1

Aussteller

Organisation	Deutsche Telekom AG
Name	TeleSec PKS eIDAS QES CA 5
Land	DE
Organisationskennung	USt-IdNr. DE 123475223

Allgemeines

Typ	X.509
Version	3
Gültig ab	09.04.2024, 11:56:13 MESZ
Gültig bis	13.04.2026, 01:59:00 MESZ
Seriennummer	143241857602408905492947016528370881730a c6 bc e2 53 77 6a 8f d8 5b 9c 2d 65 c7 3b ad

Öffentlicher Schlüssel

Algorithmus	EC
Kurven-OID	1.2.840.10045.3.1.7
Kurven-OID	1.2.840.10045.3.1.7
Parameter W	00 04 c4 58 b5 9a 69 d0 53 a7 29 ad 13 60 ef 03 a3 cd 22 1e 83 95 13 44 52 64 f0 42 c0 f4 67 2e a4 c7 d3 fc 1a 47 ba 00 fd 96 c4 d8 8f bc 38 13 b9 48 ae 4b 76 9d e7 0d e7 41 6a 2d 9f 25 ea 7e cc ef

Signatur des Ausstellers

Signaturalgorithmus	SHA256withECDSA
Signatur	30 45 02 20 46 de 2e 75 0a 04 38 c5 5d 5b ff 55 a7 1f f7 29 0e e9 80 e4 56 f9 8d a1 d9 b1 e1 23 3c 0a 9a 9e 02 21 00 e2 21 a7 46 fc 25 62 ab 91 34 80 78 2d c3 ef 0a 96 c0 bd 86 be 94 6a b1 47 31 fd 8b da f9 3f 8b

Fingerabdruck

SHA-1	9e e8 12 f0 49 c8 9f d2 55 d5 d8 6e 19 81 be 70 de 0a 5c 76
MD5	7c 46 0b 10 50 cc 68 af f1 d7 e4 8e b2 81 28 ef

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 http://tqrca1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_5.crt
Zugriff auf	Online-Zertifikat-Status-Protokoll (OCSP) http://pks.telesec.de/ocspr
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://www.telesec.de/signaturkarte/agb
Erweiterung	Zertifizierungsrichtlinien (2.5.29.32)
Kritisch	Nein
Zertifikatsrichtlinie	Qualifizierte Zertifikatsrichtlinie für natürliche Personen mit Schlüssel auf QSCD gemäß eIDAS-Verordnung (OID 0.4.0.194112.1.2) Certificate Practice Statement http://pks.telesec.de/cps
Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	a1 a6 51 60 2b c0 9b e9 d8 32 66 a9 4e 30 a9 1e 69 3f 8b 5d
Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	34 b6 7f 22 c3 5c 6b f2 12 c4 e0 9f bd 05 ca d5 14 ad 17 d8
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	01000000 Nichtabstreitbarkeit

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	143241857602408905492947016528370881 73
Gültigkeitszeitraum:	09.04.2024, 11:56:13 MESZ bis 13.04.2026, 01:59:00 MESZ
Angaben zur Zertifikatsqualität:	EU-qualifiziertes Zertifikat Signaturschlüssel auf qualifizierter sicherer Signaturerstellungseinheit (QSCD)

Zertifikatsprüfung

Zertifikatsherkunft:	Mit der Prüfanfrage übermittelt
Mathematische Prüfung der Zertifikatsignatur:	**gültig**
Signaturalgorithmus:	SHA256 ECDSA (p = 256) (q = 256)
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:	OCSP-Signer TeleSec PKS eIDAS QES CA 5
Ermittelter Status mindestens korrekt bis:	19.08.2025, 18:00:04 MESZ
Neuere Statusinformationen spätestens verfügbar ab:	nicht vorhanden
Signaturzeitpunkt der OCSP-Antwort bzw. CRL:	19.08.2025, 18:00:04 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 ECDSA (p = 256) (q = 256)
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 OCSP-Signer TeleSec PKS eIDAS QES CA 5:	**gültig**

Angaben aus dem Zertifikat

Name des Inhabers:	OCSP-Signer TeleSec PKS eIDAS QES CA 5

Inhaber

Organisation	Deutsche Telekom AG
Name	OCSP-Signer TeleSec PKS eIDAS QES CA 5
Land	DE
Organisationskennung	USt-IdNr. DE 123475223

Aussteller

Organisation	Deutsche Telekom AG
Name	TeleSec PKS eIDAS QES CA 5
Land	DE
Organisationskennung	USt-IdNr. DE 123475223

Allgemeines

Typ	X.509
Version	3
Gültig ab	23.05.2025, 10:33:42 MESZ
Gültig bis	01.12.2025, 00:59:00 MEZ

Seriennummer	428972789267588196159038987284572063982045 b7 24 92 26 72 2d ac fe 3b ae 7f ba 7a 7e

Öffentlicher Schlüssel

Algorithmus	EC
Kurven-OID	1.2.840.10045.3.1.7
Kurven-OID	1.2.840.10045.3.1.7
Parameter W	00 04 9a bc 97 fc 48 65 94 92 29 5a 24 f3 22 86 7e a9 02 3f 3a 71 41 41 c5 5b 78 df 94 78 c2 86 77 91 3e 36 0d 08 73 52 89 33 6e b4 95 36 2a 55 41 15 bb 4d 54 f7 f9 93 bc 7a 5b 58 72 df 38 0d 38 d0

Signatur des Ausstellers

Signaturalgorithmus	SHA256withECDSA
Signatur	30 44 02 20 51 89 6a 44 2c 7e 1a 90 67 a4 d2 79 85 4f 90 94 7d 63 92 52 88 2b 6e 7b 36 92 75 98 e1 ed 27 d7 02 20 2b 06 2d 6d 44 59 03 d8 2f 9f 3a cf 1d 5b 0c 05 94 8e fe 0d 48 b7 92 8f 77 00 24 d4 95 c7 10 f7

Fingerabdruck

SHA-1	e7 fc ff a1 f1 8f f5 1a 0b 70 9a df 9b 89 b3 29 1e f0 22 2f
MD5	c4 79 21 83 d1 38 10 14 f7 f4 34 1e 9d 57 0b 7b

Erweiterungen

Erweiterung	Keine OCSP-Prüfung (1.3.6.1.5.5.7.48.1.5)
Kritisch	Nein
Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	a1 a6 51 60 2b c0 9b e9 d8 32 66 a9 4e 30 a9 1e 69 3f 8b 5d
Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	72 bd 0d b8 ff dc 7b 02 14 57 25 46 05 15 fc c3 c9 c0 1a 5a
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	10000000
	digitale Signatur
Erweiterung	Erweiterte Schlüsselverwendung (2.5.29.37)
Kritisch	Nein
	OCSP-Signierung

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	428972789267588196159038987284572063982045
Gültigkeitszeitraum:	23.05.2025, 10:33:42 MESZ bis 01.12.2025, 00:59:00 MEZ

Zertifikatsprüfung

Zertifikatsherkunft:	Aus der Inhaltsdatensignatur
Mathematische Prüfung der Zertifikatsignatur:	**gültig**
Signaturalgorithmus:	SHA256 ECDSA (p = 256) (q = 256)
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 TeleSec PKS eIDAS QES CA 5:	**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:	TeleSec PKS eIDAS QES CA 5

Inhaber

Organisation	Deutsche Telekom AG
Name	TeleSec PKS eIDAS QES CA 5
Land	DE
Organisationskennung	USt-IdNr. DE 123475223

Aussteller

Organisation	Deutsche Telekom AG
Name	TeleSec qualified Root CA 1
Land	DE
Organisationskennung	USt-IdNr. DE 123475223

Allgemeines

Typ	X.509
Version	3
Gültig ab	03.12.2019, 10:34:01 MEZ
Gültig bis	04.12.2034, 00:59:59 MEZ
Seriennummer	9584896279410215094
	00 85 04 64 62 17 35 88 b6

Öffentlicher Schlüssel

Algorithmus	EC
Kurven-OID	1.2.840.10045.3.1.7
Kurven-OID	1.2.840.10045.3.1.7
Parameter W	00 04 22 3b 09 ee 57 b2 b3 bb 8f f0 19 45 dd 25 a1 2e 67 16 cc 62 f7 77 18 cb 1d f6 d1 ca 9e a3 69 0f 60 77 38 4f 75 5c 5f 7b 1d 08 96 72 77 64 c1 59 a9 f3 3f 7d 12 6f 13 81 07 65 96 53 de d2 75 be

Signatur des Ausstellers

Signaturalgorithmus	SHA512withECDSA
Signatur	30 81 88 02 42 01 3d 3f 49 b8 a9 a3 3d 94 0d a0 91 c2 00 18 62 e9 88 cb 65 bd 48 c5 bc 06 be c1 f1 2e 1e 47 b0 cb ee 63 7d c5 51 9c b0 d1 58 05 90 be 19 0b b1 93 1b 3e bb 2b 17 9e b9 6d a6 c7 c3 5d 73 c1 c8 b6 89 02 42 00 c7 07 c2 21 e9 7a 7c eb 6a 15 ab 8a 2d 4c b4 ac 7b 63 f9 ac ad 5e 22 0e 04 b9 77 e8 51 7d 0a df 25 91 db 17 2d e1 72 ec 31 98 48 e0 c3 05 d8 45 26 14 12 8f ab 7c b5 f4 00 25 46 b0 6c 3d 9c ee 2c

Fingerabdruck

SHA-1	55 51 6f c0 9e bb 22 bc 4f 1b 50 cb 6a bf 57 35 d2 0e 49 e2
MD5	4e 76 5b 8b bb 54 b0 2e fa e8 79 65 bd aa 7a db

Erweiterungen

Erweiterung	Allgemeine Einschränkungen (2.5.29.19)
Kritisch	Ja
	CA-Zertifikat
Pfadlängenbegrenzung	0
Erweiterung	Zugangsinformationen des Ausstellers (1.3.6.1.5.5.7.1.1)
Kritisch	Nein
Zugriff auf	Online-Zertifikat-Status-Protokoll (OCSP)
	http://tqrca1.ocsp.telesec.de/ocspr
Zugriff auf	Ausstellerzertifikat
	http://tqrca1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt
Erweiterung	Distributionspunkt für CRL (2.5.29.31)
Kritisch	Nein
	http://tqrca1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl
Erweiterung	Zertifizierungsrichtlinien (2.5.29.32)
Kritisch	Nein
Zertifikatsrichtlinie	1.3.6.1.4.1.7879.13.27
	Certificate Practice Statement
	http://pks.telesec.de/cps
Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f
Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	a1 a6 51 60 2b c0 9b e9 d8 32 66 a9 4e 30 a9 1e 69 3f 8b 5d
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	00000110
	Zertifikatssignierung, CRL-Signaturverifizierung

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	9584896279410215094
Gültigkeitszeitraum:	03.12.2019, 10:34:01 MEZ bis 04.12.2034, 00:59:59 MEZ

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 TeleSec PKS eIDAS QES CA 5:	**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:	TeleSec PKS eIDAS QES CA 5

Inhaber

Organisation	Deutsche Telekom AG
Name	TeleSec PKS eIDAS QES CA 5
Land	DE
Organisationskennung	USt-IdNr. DE 123475223

Aussteller

Organisation	Deutsche Telekom AG
Name	TeleSec qualified Root CA 1
Land	DE
Organisationskennung	USt-IdNr. DE 123475223

Allgemeines

Typ	X.509
Version	3
Gültig ab	03.12.2019, 10:34:01 MEZ
Gültig bis	04.12.2034, 00:59:59 MEZ
Seriennummer	9584896279410215094
	00 85 04 64 62 17 35 88 b6

Öffentlicher Schlüssel

Algorithmus	EC
Kurven-OID	1.2.840.10045.3.1.7
Kurven-OID	1.2.840.10045.3.1.7
Parameter W	00 04 22 3b 09 ee 57 b2 b3 bb 8f f0 19 45 dd 25 a1 2e 67 16 cc 62 f7 77 18 cb 1d f6 d1 ca 9e a3 69 0f 60 77 38 4f 75 5c 5f 7b 1d 08 96 72 77 64 c1 59 a9 f3 3f 7d 12 6f 13 81 07 65 96 53 de d2 75 be

Signatur des Ausstellers

Signaturalgorithmus	SHA512withECDSA
Signatur	30 81 88 02 42 01 3d 3f 49 b8 a9 a3 3d 94 0d a0 91 c2 00 18 62 e9 88 cb 65 bd 48 c5 bc 06 be c1 f1 2e 1e 47 b0 cb ee 63 7d c5 51 9c b0 d1 58 05 90 be 19 0b b1 93

	1b 3e bb 2b 17 9e b9 6d a6 c7 c3 5d 73 c1 c8 b6 89 02 42 00 c7 07 c2 21 e9 7a 7c eb 6a 15 ab 8a 2d 4c b4 ac 7b 63 f9 ac ad 5e 22 0e 04 b9 77 e8 51 7d 0a df 25 91 db 17 2d e1 72 ec 31 98 48 e0 c3 05 d8 45 26 14 12 8f ab 7c b5 f4 00 25 46 b0 6c 3d 9c ee 2c

Fingerabdruck

SHA-1	55 51 6f c0 9e bb 22 bc 4f 1b 50 cb 6a bf 57 35 d2 0e 49 e2
MD5	4e 76 5b 8b bb 54 b0 2e fa e8 79 65 bd aa 7a db

Erweiterungen

Erweiterung	Allgemeine Einschränkungen (2.5.29.19)
Kritisch	Ja
	CA-Zertifikat
Pfadlängenbegrenzung	0
Erweiterung	Zugangsinformationen des Ausstellers (1.3.6.1.5.5.7.1.1)
Kritisch	Nein
Zugriff auf	Online-Zertifikat-Status-Protokoll (OCSP)
	http://tqrca1.ocsp.telesec.de/ocspr
Zugriff auf	Ausstellerzertifikat
	http://tqrca1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt
Erweiterung	Distributionspunkt für CRL (2.5.29.31)
Kritisch	Nein
	http://tqrca1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl
Erweiterung	Zertifizierungsrichtlinien (2.5.29.32)
Kritisch	Nein
Zertifikatsrichtlinie	1.3.6.1.4.1.7879.13.27
	Certificate Practice Statement
	http://pks.telesec.de/cps
Erweiterung	Ausstellerschlüssel-ID (2.5.29.35)
Kritisch	Nein
Schlüssel-ID	25 8d 2c 22 b8 92 1a 99 f9 34 cb f9 d4 35 ea af c6 b0 1d 0f
Erweiterung	Inhaberschlüssel-ID (2.5.29.14)
Kritisch	Nein
Schlüssel-ID	a1 a6 51 60 2b c0 9b e9 d8 32 66 a9 4e 30 a9 1e 69 3f 8b 5d
Erweiterung	Schlüsselverwendung (2.5.29.15)
Kritisch	Ja
	00000110
	Zertifikatssignierung, CRL-Signaturverifizierung

Staat in dem der Aussteller ansässig ist:	Deutschland
Seriennummer:	9584896279410215094
Gültigkeitszeitraum:	03.12.2019, 10:34:01 MEZ bis 04.12.2034, 00:59:59 MEZ

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 "Zeitpunkt der Durchführung der Prüfung":	60 s
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 Gültigkeitsintervalls:	Unbestimmt
Verwendeter Algorithmenkatalog mit Link:	SOG-IS Agreed Cryptographic Mechanisms / BNetzA 2017
Prüfung der Vertrauensstellungen für Sperrstatus-Antworten:	ja
Sperrstatusermittlung für Kurzzeit-Zertifikate erforderlich:	nein

Vertrauenslisten (mit Erweiterungen)

Vertrauensliste #1

EU-Mitgliedsstaat:	Deutschland
Ausstellende Aufsichtsbehörde oder Stelle:	Bundesnetzagentur
Version:	145
Download-URL:	https://localhost:8443/Filemanager/rest/resources/OFFICIAL_TL_DE/SHA-256_36958c460be81620f3d-af1e24d6819feead372b5b1e55d0e904cd526e3a36c6c
Ausgegeben am:	12.08.2025, 12:15:00 MESZ
Nächste Aktualisierung spätestens am:	12.02.2026, 12:15:00 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:	370
Download-URL:	https://localhost:8443/Filemanager/rest/resources/LOTL/SHA-256_464a345e6dc87091c21b4c0daf-a66b8f7e25c80336ebf1322aa7630baf6e5839
Ausgegeben am:	08.08.2025, 12:06:48 MESZ
Nächste Aktualisierung spätestens am:	04.02.2026, 12:06:48 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-c32350544f7c7b147093cd3d7393d91e9234908b8ccd8a3cb3cf

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:	31 ms
Version des Certificate Validation Servers:	11.5.4
Version der Crypto Service Library:	3.2.3