

# Prüfprotokoll: 12.09.2025, 13:07:41 MESZ

## Fachliche Prüfung:

|                                  |   |
|----------------------------------|---|
| Fachliche Prüfrichtlinie:        | Kumuliertes Ergebnis der einzelnen Signaturprüfungen ohne Berücksichtigung des Signaturniveaus. |
| Ergebnis der fachlichen Prüfung: | <b>gültig</b>   |
| Meldungen:                       | Alle geprüften elektronischen Signaturen sind gültig.   |

## Zusammenfassung Dokumente und Signaturprüfungen:

| Nr. | Dokument   | Signiert durch    | Signaturniveau                                    | Signaturprüfung |
|-----|--|-------------------|---|-----------------|
| 1.  | <a href="#">Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.pdf</a> | Hellenthal, Peter | EU-qualifizierte elektronische Signatur (EUMS-TL) | <b>gültig</b>   |

## Dokument bzw. Containerstruktur:

| CADES-Dokument: Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.pdf.pkcs7 |  |
|--|--|
| Signierte Datei oder Inhalt:   | Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.pdf |
| Signatur durch:  | Hellenthal, Peter  |
| Signaturtyp:   | Detached   |
| Ergebnis der Signaturprüfung:  | <b>gültig</b>  |
| PDF-Dokument: Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.pdf         |  |
| 1. Revision  |  |

## Übersicht Prüfung der Signaturen:

| CADES: Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.pdf.pkcs7 |  |
|---|--|
| Zeitpunkt der Durchführung der Prüfung:   | 12.09.2025, 13:07:41 MESZ  |
| Signierte Datei oder Inhalt:  | Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.pdf |
| Signatur durch:   | Hellenthal, Peter  |
| Niveau und Typ der Signatur:  | EU-qualifizierte elektronische Signatur (EUMS-TL)                            |
| Behaupteter Signaturzeitpunkt:  | 12.09.2025, 13:07:34 MESZ  |
| Prüfzeitpunkt der Signatur:   | Behaupteter Signaturzeitpunkt  |
| Ergebnis der Signaturprüfung:   | <b>gültig</b>  |

## Prüfung der Signaturen im Detail:

| CADES-Signatur B: Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.pdf.pkcs7 |  |
|--|--|
| Zeitpunkt der Durchführung der Prüfung:  | 12.09.2025, 13:07:41 MESZ  |
| Signierte Datei oder Inhalt:   | Dienstliche Stellungnahme zum Befangenheitsantrag des Mark Jäckel vom 29.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 ( <a href="http://uri.etsi.org/TrstSvc/Svctype/CA/QC">http://uri.etsi.org/TrstSvc/Svctype/CA/QC</a> )         |
| Dienstestatus:                                   | Gewährt ( <a href="http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</a> )   |
| 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 ( <a href="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</a> ) |
| Link zu Details der verwendeten Vertrauensliste: | <a href="#">Vertrauensliste #1</a>  |

**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: | 12.09.2025, 13:07:34 MESZ     |
| Prüfzeitpunkt der Signatur:    | Behaupteter Signaturzeitpunkt |
| Ergebnis der Signaturprüfung:  | <b>gültig</b>                 |

|                                     |  |
|-------------------------------------|--|
| Verwendete Prüfrichtlinie mit Link: | <a href="#">Qualifizierte elektronische Signatur (qVDA aus DE eIDAS-VO) #1</a>                           |
| Verwendeter Algorithmenkatalog:     | <a href="#">Katalog Anwendung Governikus (SOG-IS Agreed Cryptographic Mechanisms v1.2 / BNetzA 2017)</a> |

**Integritätsprüfung**

|   |  |
|---|--|
| Strukturspezifische Prüfung:              | <b>gültig</b>                          |
| Mathematische Signaturprüfung:            | <b>gültig</b>                          |
| 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:              | <b>gültig</b>                          |

**Zertifikatprüfungen**

|  |                           |
|--|---------------------------|
| Gültigkeitsmodell für die Zertifikatskette:    | Schale                    |
| Gültigkeitsmodell definiert in:                | Verwendete Prüfrichtlinie |
| Prüfung des Zertifikats von Hellenthal, Peter: | <b>gültig</b>             |

**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 | 14324185760240890549294701652837088173<br>0a 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<br>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<br>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<br>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<br>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<br><a href="http://tqrca1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_5.crt">http://tqrca1.pki.telesec.de/crt/TeleSec_PKS_eIDAS_QES_CA_5.crt</a>   |
| Zugriff auf                    | Online-Zertifikat-Status-Protokoll (OCSP)<br><a href="http://pks.telesec.de/ocspr">http://pks.telesec.de/ocspr</a>  |
| Erweiterung                    | Angaben zum qualifizierten Zertifikat (1.3.6.1.5.5.7.1.3)   |
| Kritisch                       | Nein<br>Qualifiziertes Zertifikat gemäß Signaturdirektive oder eIDAS-Verordnung (OID 0.4.0.1862.1.1)<br>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) | <a href="https://www.telesec.de/signaturkarte/agb">https://www.telesec.de/signaturkarte/agb</a>   |
| 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)<br>Certificate Practice Statement<br><a href="http://pks.telesec.de/cps">http://pks.telesec.de/cps</a>                                       |
| 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<br>01000000<br>Nichtabstreitbarkeit  |

|   |   |
|---|---|
| Staat in dem der Aussteller ansässig ist: | Deutschland   |
| Seriennummer:                             | 14324185760240890549294701652837088173  |
| Gültigkeitszeitraum:                      | 09.04.2024, 11:56:13 MESZ bis 13.04.2026, 01:59:00 MESZ   |
| Angaben zur Zertifikatsqualität:          | EU-qualifiziertes Zertifikat<br>Signatur Schlüssel auf qualifizierter sicherer Signaturer-<br>stellungseinheit (QSCD) |

### Zertifikatsprüfung

|  |  |
|--|--|
| Zertifikatsherkunft:   | Mit der Prüfanfrage übermittelt        |
| Mathematische Prüfung der Zertifikatsignatur:                              | <b>gültig</b>                          |
| 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:   | <b>gültig</b>                          |
| Prüfzeitpunkt des Zertifikats:   | Behaupteter Signaturzeitpunkt          |
| Prüfzeitpunkt der Signatur innerhalb Gültigkeitsintervall des Zertifikats: | <b>gültig</b>                          |
| Sperrstatus des Zertifikats:   | <b>gültig</b>                          |

**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:              | 12.09.2025, 13:07:41 MESZ                    |
| Neuere Statusinformationen spätestens verfügbar ab:     | nicht vorhanden                              |
| Signaturzeitpunkt der OCSP-Antwort bzw. CRL:            | 12.09.2025, 13:07:41 MESZ                    |
| Prüfzeitpunkt der Signatur der OCSP-Antwort bzw. CRL:   | Behaupteter Signaturzeitpunkt                |
| Ergebnis der Signaturprüfung der OCSP-Antwort bzw. CRL: | <b>gültig</b>                                |

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

**Integritätsprüfung**

|   |  |
|---|--|
| Mathematische Signaturprüfung:            | <b>gültig</b>                          |
| 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:              | <b>gültig</b>                          |

**Zertifikatprüfungen**

|   |                           |
|---|---------------------------|
| Gültigkeitsmodell für die Zertifikatskette:                         | Schale                    |
| Gültigkeitsmodell definiert in:                                     | Verwendete Prüfrichtlinie |
| Prüfung des Zertifikats von OCSP-Signer TeleSec PKS eIDAS QES CA 5: | <b>gültig</b>             |

**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 42897278926758819615903898728457206398  
20 45 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: 42897278926758819615903898728457206398  
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:   | <b>gültig</b>  |
| Prüfzeitpunkt des Zertifikats:   | Behaupteter Signaturzeitpunkt  |
| Prüfzeitpunkt der Signatur innerhalb Gültigkeitsintervall des Zertifikats: | <b>gültig</b>  |
| Sperrstatus des Zertifikats:   | <b>nicht geprüft</b>   |
| 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: | <b>nicht geprüft</b>   |
| Meldungen:  | Das Zertifikat ist ein digitaler Dienste-Identifizier (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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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)<br><a href="http://tqrc1.ocsp.telesec.de/ocspr">http://tqrc1.ocsp.telesec.de/ocspr</a>                                      |
| Zugriff auf           | Ausstellerzertifikat<br><a href="http://tqrc1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt">http://tqrc1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt</a> |
| Erweiterung           | Distributionspunkt für CRL (2.5.29.31)  |
| Kritisch              | Nein  |
|                       | <a href="http://tqrc1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl">http://tqrc1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl</a>                           |
| Erweiterung           | Zertifizierungsrichtlinien (2.5.29.32)  |
| Kritisch              | Nein  |
| Zertifikatsrichtlinie | 1.3.6.1.4.1.7879.13.27<br>Certificate Practice Statement<br><a href="http://pks.telesec.de/cps">http://pks.telesec.de/cps</a>   |
| 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<br>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-Identifizierer (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)<br><a href="http://tqrca1.ocsp.telesec.de/ocspr">http://tqrca1.ocsp.telesec.de/ocspr</a>                                      |
| Zugriff auf           | Ausstellerzertifikat<br><a href="http://tqrca1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt">http://tqrca1.pki.telesec.de/crt/TeleSec_qualified_Root_CA_1.crt</a> |
| Erweiterung           | Distributionspunkt für CRL (2.5.29.31)  |
| Kritisch              | Nein  |
|                       | <a href="http://tqrca1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl">http://tqrca1.pki.telesec.de/rl/TeleSec_qualified_Root_CA_1.crl</a>                           |
| Erweiterung           | Zertifizierungsrichtlinien (2.5.29.32)  |
| Kritisch              | Nein  |
| Zertifikatsrichtlinie | 1.3.6.1.4.1.7879.13.27<br>Certificate Practice Statement<br><a href="http://pks.telesec.de/cps">http://pks.telesec.de/cps</a>   |
| 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**

**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 Schlüsselerwendung für:   | Signaturzertifikate (EE)<br>Zwischenzertifikate (CA)<br>Zeitstempelzertifikate<br>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:                                   | 147   |
| Download-URL:                              | <a href="https://localhost:8443/Filemanager/rest/resources/OFFICIAL_TL_DE/SHA-256_ca737675d935094055053b9b91ee2c0afda5f-cb1e77629a70679d1fea401f307">https://localhost:8443/Filemanager/rest/resources/OFFICIAL_TL_DE/SHA-256_ca737675d935094055053b9b91ee2c0afda5f-cb1e77629a70679d1fea401f307</a> |
| Ausgegeben am:                             | 10.09.2025, 15:00:00 MESZ   |
| Nächste Aktualisierung spätestens am:      | 10.03.2026, 15:00:00 MEZ  |

**Erweiterung zur Vertrauensliste #1**

|  |   |
|--|---|
| EU-Mitgliedsstaat:                         | Deutschland   |
| Ausstellende Aufsichtsbehörde oder Stelle: | Governikus KG   |
| Version:                                   | 127   |
| Download-URL:                              | <a href="https://localhost:8443/Filemanager/rest/resources/OFFICIAL_TL_DE_EXTENSION/SHA-256_9f48b535f290ae-f73505282e0c635069a429198f9673de1502dfe58bf6d1f1d6">https://localhost:8443/Filemanager/rest/resources/OFFICIAL_TL_DE_EXTENSION/SHA-256_9f48b535f290ae-f73505282e0c635069a429198f9673de1502dfe58bf6d1f1d6</a> |
| 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:                                   | 371   |
| Download-URL:                              | <a href="https://localhost:8443/Filemanager/rest/resources/LOTL_SHA-256_bb231cec463aa19f353b2de88fafc37f1312622a5e-d973a626628eb73368d440">https://localhost:8443/Filemanager/rest/resources/LOTL_SHA-256_bb231cec463aa19f353b2de88fafc37f1312622a5e-d973a626628eb73368d440</a> |
| Ausgegeben am:                             | 19.08.2025, 09:09:01 MESZ   |
| Nächste Aktualisierung spätestens am:      | 10.02.2026, 09:09:01 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:       | <a href="https://localhost:8443/Filemanager/rest/resources/ALGORITHM_CATALOG_SOGIS_PLUS/SHA-256_9996bba3d8bec32350544f7c7b147093cd3d7393d91e9234908b8ccd8a3cb3cf">https://localhost:8443/Filemanager/rest/resources/ALGORITHM_CATALOG_SOGIS_PLUS/SHA-256_9996bba3d8bec32350544f7c7b147093cd3d7393d91e9234908b8ccd8a3cb3cf</a> |

|          |  |
|----------|--|
| 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-sign-d.xml |

#### Prüfinstanz

|   |   |
|---|---|
| URL des Certificate Validation Servers:     | <a href="https://cvs.governikus-asp.de:443/CertificateValidationServer/cvs">https://cvs.governikus-asp.de:443/CertificateValidationServer/cvs</a> |
| Kumulierte Wartezeit auf externe Antworten: | 15 ms   |
| Version des Certificate Validation Servers: | 11.5.4  |
| Version der Crypto Service Library:         | 3.2.3   |