

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

**T-Systems International GmbH**  
**Untere Industriestraße 20**  
**57250 Netphen, Germany**

to confirm that its trust service

**TeleSec ServerPass OV CA**

fulfils all requirements defined in the standard (EN)

**ETSI EN 319 411-1 V1.1.1 (2016-02),  
policy OVCP.**

The appendix to the certificate is part of the certificate and consists of 3 pages.

The certificate is valid only in conjunction with the evaluation report.



20  
Certificate valid until  
2020-06-15

Certificate ID: 67109.18  
© TÜVIT - TÜV NORD GROUP - www.tuvt.de

Essen, 2018-06-15

Dr. Christoph Sutter  
Head of Certification Body

**TÜV Informationstechnik GmbH**  
TÜV NORD GROUP  
Langemarckstr. 20  
45141 Essen, Germany  
www.tuvt.de



**Certificate**

## **Certification System**

The certification body of TÜV Informationstechnik GmbH is accredited by “DAkkS Deutsche Akkreditierungsstelle GmbH” according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- “Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH”, version 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

## **Evaluation Report**

- “Evaluation Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67109, TeleSec ServerPass OV CA”, version 2.0 as of 2018-06-14, TÜV Informationstechnik GmbH

## **Evaluation Requirements**

The evaluation requirements are defined in the standard ETSI EN 319 411-1:

- ETSI EN 319 411-1 V1.1.1 (2016-02): “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements”, Version 1.1.1, 2016-02, European Telecommunications Standards Institute

The applicable ETSI Certificate Policy is:

- OVCP: Organizational Validation Certificate Policy

## Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

### TeleSec ServerPass OV CA:

<b>Issuer of CA certificate (Root CA or intermediate CA): CN = T-TeleSec GlobalRoot Class 2 Certificate Serial Number: 01</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass Class 2 CA	7e 39 c7 ad 1d d9 f0 43

<b>Issuer of CA certificate (Root CA or intermediate CA): CN = Baltimore CyberTrust Root Certificate Serial Number: 02 00 00 b9</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass CA 2	07 27 b2 16

<b>Issuer of CA certificate (Root CA or intermediate CA): CN = Deutsche Telekom Root CA 2 Certificate Serial Number: 26</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass DE-2	00 c7 5e 01 58 2a c3 be e7

<b>Issuer of CA certificate (Root CA or intermediate CA): CN = TeleSec GlobalRoot Class 2 G2 Certificate Serial Number: 00 a8 0a 76 8d f7 b2 75 37</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass CA 2 G2	1f 6b ab e8 71 0e e7 e1

together with the Certification Practice Statement (CPS) of the operator:

- „CP/CPS TeleSec Server Pass“, version 7.0 as of 2018-04-13, T-Systems International GmbH

### **Evaluation Result**

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

### **Summary of the Evaluation Requirements**

ETSI EN 319 411-1 contains requirements for Trust Service Providers practice under the following headlines:

- 1 Publication and repository responsibilities**
- 2 Identification and authentication**
- 3 Certificate Life-Cycle operational requirements**
- 4 Facility, management, and operational controls**
- 5 Technical security controls**
- 6 Certificate, CRL, and OCSP profiles**
- 7 Compliance audit and other assessment**
- 8 Other business and legal matters**
- 9 Other provisions**

## Scope of the Amendment

This amendment as of 2019-07-26 supplements the certificate with certificate ID: 67109.18 as of 2018-06-15 because of the conducted surveillance audit.

## Certification System

The certification body of TÜV Informationstechnik GmbH is accredited by “DAkkS Deutsche Akkreditierungsstelle GmbH” according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- “Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH”, version 2.0 as of 2016-06-06, TÜV Informationstechnik GmbH

## Evaluation Report

- “Evaluation Report – Surveillance Audit – ETSI EN 319 411-1, TUVIT-CA67109 A1, TeleSec ServerPass OV CA”, Version 2.0 as of 2019-07-26, TÜV Informationstechnik GmbH

## Evaluation Requirements

The evaluation requirements are defined in the standard ETSI EN 319 411-1 V1.2.2:

- ETSI EN 319 411-1 V1.2.2 (2018-04): “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”, Version 1.2.2, 2018-04, European Telecommunications Standards Institute

Additionally the following criteria were considered in the audit:

- “Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates”, Version 1.6.3 as of 2019-02-01, CA/Browser Forum

The applicable ETSI Certificate Policy is:

- OVCP: Organizational Validation Certificate Policy

### Evaluation Target

The target of evaluation is characterized by the certificate information of the inspected trust service:

#### TeleSec ServerPass OV CA:

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = T-TeleSec GlobalRoot Class 2</b> <b>Certificate Serial Number: 01</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass Class 2 CA	7E 39 C7 AD 1D D9 F0 43

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = Deutsche Telekom Root CA 2</b> <b>Certificate Serial Number: 26</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass DE-2	00 C7 5E 01 58 2A C3 BE E7

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = TeleSec GlobalRoot Class 2 G2</b> <b>Certificate Serial Number: 00 A8 0A 76 8D F7 B2 75 37</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass CA 2 G2	1F 6B AB E8 71 0E E7 E1

<b>Issuer of CA certificate (Root CA or intermediate CA):</b> <b>CN = Baltimore CyberTrust Root</b> <b>Certificate Serial Number: 02 00 00 B9</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass CA 2	07 27 B2 16

together with the documentation of the operator:

- “CP/CPS TeleSec ServerPass Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb (CP/CPS)“, version 10.00 as of 2018-10-16, T-Systems International GmbH
- “TeleSec ServerPass PKI Disclosure Statement (PDS)”, version 2.4 as of 2019-02-27, T-Systems International GmbH
- “Allgemeine Geschäftsbedingungen TeleSec-Produkte” as of 2018-08-01, T-Systems International GmbH

### Evaluation Result

- The target of evaluation fulfills all applicable evaluation requirements.
- The certification requirements defined in the certification system are fulfilled.

## **Summary of the Evaluation Requirements**

ETSI EN 319 411-1 enthält Anforderungen für Vertrauensdiensteanbieter (VDA) bzgl. der Tätigkeit des VDAs unter folgenden Überschriften:

- 1 Verantwortlichkeiten bzgl. Veröffentlichung und öffentlichem Verzeichnis**
- 2 Identifizierung und Authentifizierung**
- 3 Betriebsanforderungen an den Zertifikatslebenszyklus**
- 4 Anforderungen an Einrichtung, Verwaltung und Betrieb**
- 5 Technische Sicherheitsanforderungen**
- 6 Zertifikats-, Sperrlisten- (CRL-) und OCSP-Profile**
- 7 Compliance-Audit und andere Bewertungen**
- 8 Sonstige geschäftliche und rechtliche Angelegenheiten**
- 9 Sonstige Maßnahmen**