

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

**Deutsche Telekom Security 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 V1.2.2 (2018-04),**  
**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.



**Certificate ID: 67128.20**

© TÜVIT - TÜV NORD GROUP - [www.tuvit.de](http://www.tuvit.de)

Certificate validity:  
2020-07-01 – 2022-07-01

Essen, 2020-07-01

Dr. Christoph Sutter  
Head of Certification Body

**TÜV Informationstechnik GmbH**

TÜV NORD GROUP  
Langemarckstr. 20  
45141 Essen, Germany  
[www.tuvit.de](http://www.tuvit.de)



**Certificate**

## Certification Scheme

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 2.1 as of 2020-03-01, TÜV Informationstechnik GmbH

## Evaluation Report

- „Audit Report – Re-Certification – ETSI EN 319 411-1, TUVIT-CA67128, TeleSec ServerPass OV CA“, version 2.0 as of 2020-06-29, TÜV Informationstechnik GmbH

## Evaluation Requirements

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

- 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

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 = TeleSec GlobalRoot Class 2 G3</b> <b>Certificate Serial Number:</b> <b>08227067E116F69056EF0BFEBBDD991</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass CA 2 G3	285F5310C2D97C 336D1AE724E56C 1C52

<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	7E39C7AD1DD9F0 43

<b>Issuer of CA certificate (Root CA or Intermediate CA):</b> <b>CN = CN = Baltimore CyberTrust Root</b> <b>Zertifikatsseriennummer: 020000B9</b>	
<b>Name of CA (as in certificate)</b>	<b>serial number of certificate</b>
CN = TeleSec ServerPass CA 2	0727B216

together with the documentation of the operator:

- “CP/CPS TeleSec ServerPass, Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb (CP/CPS)“, Version 13.00 as of 2020-06-04, Deutsche Telekom Security GmbH
- “TeleSec ServerPass, PKI Disclosure Statement (PDS)“, version 2.4 as of 2019-02-27, T-Systems International GmbH

- “Allgemeine Geschäftsbedingungen TeleSec-Produkte”,  
version 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 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**