TeleSec ServerPass

PKI Disclosure Statement (PDS)

T-Systems International GmbH
TC Solutions

öffentlich

Version:	1.0	Stand:	01.08.2017
Status:	freigegeben		

Mit Veröffentlichung wird dieses Dokument gültig. Alle bisherigen Versionen verlieren ihre Gültigkeit!

Impressum

Herausgeber	T-Systems International GmbH TC Solutions

Dateiname	**Stand**	**Titel**
PDS ServerPass v1 0_20170808.docx	01.08.2017	TeleSec ServerPass

Version	**Status**	**Freigegeben am**
1.0	freigegeben	08.08.2017 / M. Etrich

Ansprechpartner	**Telefon**	**E-Mail**
T-Systems – Trust Center Solutions	+49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)	telesec_support@t-systems.com

Kurzbeschreibung
PKI Disclosure Statement TeleSec ServerPass gemäß ETSI EN 319 411-1

Inhaltsverzeichnis

1 Einleitung

TeleSec ServerPass ist eine vom Vertrauensdiensteanbieter (VDA) T-Systems International GmbH im T-Systems Trust Center betriebene PKI-Dienstleistung zur Ausstellung von verschiedenen X.509v3 TLS/SSL Server-Zertifikaten.

Der Vertrauensdienst TeleSec ServerPass besteht aus mehreren Zertifizierungsstellen (CA) zur Ausstellung von qualifizierten und nicht-qualifizierten Website-Zertifikaten.

Die Sicherheitsleitlinien des Zertifizierungsdienstes sowie weitergehende Informationen über das Zertifikatsmanagement sind in der Zertifizierungsrichtlinie und Erklärung zum Zertifizierungsbetrieb TeleSec ServerPass (CP/CPS)“ beschrieben, siehe Kap. 8.

Dieses Dokument fasst die Kernpunkte des CP/CPS zusammen und dient als Übersicht für Antragsteller und vertrauende Dritte. Zur Gewährleistung der Vergleichbarkeit ist es gemäß ETSI EN 319-11-1 aufgebaut.

2 Kontaktadressen

Der VDA T-Systems ist über folgende Kontakte zu erreichen:

- Anschrift: T-Systems International GmbH, Trust Center Services,
  Untere Industriestraße 20, D-57250 Netphen
- Telefon: +49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)
- E-Mail: telesec_support@t-systems.com
- Internet: https://www.telesec.de

Der Sperrservice ist 7x24 Stunden
online: https://serverpass.telesec.de/serverpass/ts/ee/index.html

telefonisch: +49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)

erreichbar.

3 Zertifikatstypen, Validierung und Verwendung

Der Vertrauensdienst TeleSec ServerPass stellt ausschließlich organisations- und erweitert validierte Zertifikate unter öffentlichen Vertrauensankern (Root-Zertifikate) aus. Die Prozesse der Auftragsprüfung für die unterschiedlichen Zertifikatstypen werden im CP/CPS beschrieben. Es handelt sich ausschließlich um X.509 v3 Zertifikate.

3.1 TeleSec ServerPass Test

Ein nicht qualifiziertes X509-Website Zertifikat für Testzwecke unter einer nicht öffentlichen Testroot.

Registrierung
Registrierung im Kundenportal erforderlich
Gültigkeitsdauer
30 Tage
Validierungsverfahren
Online-Auftrag erforderlich
keine Auftragsprüfung

3.2 TeleSec ServerPass Standard, Wildcard und SAN UCC

Nicht qualifizierte X509v3 Zertifikate für Website-Authentifizierung unter einer öffentlichen Root mit Organisationvalidierung.

Root-Zertifikate

- CN=T-TeleSec GlobalRoot Class 2
- CN=TeleSec GlobalRoot Class 2 G2
- CN=Deutsche Telekom Root CA 2

Sub-CAs

- CN=TeleSec ServerPass Class 2 CA
- CN=TeleSec ServerPass CA 2 G2
- CN=TeleSec ServerPass DE-2

Registrierung
Registrierung im Kundenportal erforderlich
Gültigkeitsdauer
1 Jahr, 2 Jahre, 3 Jahre (plus 5 Tage Kulanzzeitraum)
Validierungsverfahren
Online-Auftrag erforderlich
Organisationsvalidierte Auftragsprüfung

3.3 TeleSec ServerPass EV

Qualifiziertes X509v3 Zertifikat für Website-Authentifizierung unter einer öffentlichen Root mit erweiterter Validierung und QC-Statement.

Root-Zertifikate

- CN=T-TeleSec GlobalRoot Class 3
- CN=TeleSec GlobalRoot Class 3 G2

Sub-CAs:

- CN = TeleSec ServerPass Extended Validation Class 3 CA
- CN = TeleSec ServerPass CA 3 G2

Registrierung
Registrierung im Kundenportal erforderlich
Gültigkeitsdauer
1 Jahr, 2 Jahre (plus 5 Tage Kulanzzeitraum)
Validierungsverfahren
Online-Auftrag erforderlich
Erweiterte Auftragsprüfung

Alle Zertifikate werden im Rahmen von definierten Auftragsprüf- und Ausgabeprozessen erstellt.

Die Zertifikate dürfen im Rahmen der vorgesehen Nutzung und der im jeweiligen Zertifikat festgelegten Schlüsselverwendung eingesetzt werden. Die Verwendung der Zertifikate als Zertifizierungsstelle (Sub-CA) oder Stammzertifizierungsstelle (Root-CA) ist nicht erlaubt. Die Details sind im CP/CPS (siehe Kap. 8) geregelt.

4 Haftungsbeschränkungen des VDA

T-Systems setzt keine Vertrauensgrenzen für die von ihr ausgestellten Zertifikate.

Es sind jedoch die Beschränkungen bzgl. der Haftung (siehe Kap. 7) sowie der Nutzung gemäß der vorgesehenen Zwecke (siehe Kap. 3) zu beachten.

In der Zertifikatshistorie werden alle relevanten Ereignisse von der Auftragstellung über die Registrierung, die Prüfungen durch den VDA, die Produktion und ggf. der Sperrung erfasst und integritätsgeschützt abgelegt.

Die Papierdokumente und elektronisch erfassten Auftrags- und Zertifikatsdaten sowie die Daten der Zertifikatshistorie werden über die Zertifikatsgültigkeit hinaus weitere zehn Jahre vorgehalten. Bei einer Zertifikatserneuerung verlängert sich die Aufbewahrungsfrist der ursprünglichen Dokumente und Daten entsprechend.

5 Pflichten des Zertifikatinhabers

Die Pflichten des Zertifikatsinhabers sind im CP/CPS und den Allgemeinen Geschäftsbedingungen aufgeführt. Die Dokumente sind im Internet unter https://www.telesec.de/de/serverpass/support/downloadbereich abrufbar.

6 Verpflichtungen vertrauender Dritter zur Zertifikatsstatusüberprüfung

Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

Jeder vertrauende Dritte sollte daher

- die Gültigkeit des Zertifikats überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie) sowie den Gültigkeitszeitraum und die Sperrinformationen (via CRLs oder OCSP) des Zertifikats überprüft,
- die technischen Verwendungszwecke prüfen, die durch die im Zertifikat angegebenen Attribute „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ festgelegt sind.

Vertrauende Dritte müssen geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

7 Ausschluss- und Haftungsbegrenzungsklauseln

Für Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie für Schäden, die auf eine vorsätzliche Pflichtverletzungen zurückzuführen sind, haftet die Zertifizierungsstelle. Im Übrigen wird die Haftung für Schäden, die auf einer fahrlässigen Pflichtverletzung beruhen in den Allgemeinen Geschäftsbedingungen (AGB) oder einzelvertraglich geregelt.

8 Anwendbare Vereinbarungen, CP/CPS, AGB

Dieses PDS, das CP/CPS sowie die Allgemeinen Geschäftsbedingungen sind im Internet unter https://www.telesec.de/de/serverpass/support/downloadbereich abrufbar.

9 Datenschutzrichtlinien

Zur Leistungserbringung muss T-Systems personenbezogene Daten elektronisch speichern und verarbeiten. T-Systems stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen zum Schutz der Daten gemäß der geltenden datenschutz-

rechtlichen Bestimmungen sicher. Bzgl. der Aufbewahrungsdauer der Daten gelten die Regelungen aus Kap. 4.

10 Rückerstattungsrichtlinien

Die Erstattung von Entgelten durch T-Systems erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts. Darüber hinaus gelten die Regelungen der jeweils gültigen AGB oder sonstige mit dem Kunden vereinbarte vertraglichen Regelungen

11 Anwendbares Recht und Streitbeilegungsklauseln

Es gilt deutsches Recht. Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei. Gerichtsstand ist der Sitz der T-Systems International GmbH in Frankfurt am Main.

12 Status als Vertrauensdiensteanbieter und Audit

Für die Ausgabe der qualifizierten Zertifikate gelten Anforderungen der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates („eIDAS“)

Zur Gewährleistung der Konformität erfüllt die Zertifizierungsstelle die Anforderungen aus

- [ETSI EN 319 401]: General Policy Requirements for TSPs
- [ETSI EN 319 411-1]: General Policy and security requirements for TSPs
- [ETSI EN 319 411-2]: Requirements for TSPs issuing EU qualified certificates
- [ETSI EN 319 412-5]: Certificate Profiles: QCStatements

Zur Prüfung der Konformität wird die Zertifizierungsstelle sowohl durch interne Auditoren als auch durch eine anerkannte Prüfstelle (gemäß [ETSI EN 319403]) auditiert. Im Rahmen der Audits wird neben der Dokumentation (Sicherheitskonzept, Betriebskonzept sowie weitere interne Dokumente) die Umsetzung der Prozesse und Einhaltung der Vorgaben überprüft.

Die deutsche Vertrauensliste ist auf den Internetseiten der Bundesnetzagentur veröffentlicht unter: www.nrca-ds.de.