1 EINLEITUNG

Dieses Dokument informiert den Anwender über den Dienst Server.ID (TeleSec ServerPass) und enthält ergänzend zur Allgemeinen Geschäftsbedingung Server.ID (TeleSec ServerPass) die Verpflichtungen des Unterzeichners.

Durch das Akzeptieren dieses Dokuments, erklärt sich der Unterzeichner mit diesen Nutzungsbedingungen einverstanden.

2 LEISTUNGSBESTANDTEILE

Die Server.ID (TeleSec ServerPass) (inkl. SAN/UCC (Multidomain)) Standard-Varianten erfüllen die Anforderungen von ETSI 319 411-1 policy OVCP.

Alle EV-Varianten (EVCP) (inkl. SAN) erfüllen die ETSI EN 319 411-1 policy.

ServerPass EV (inkl. SAN (Multidomain)) QCP-w erfüllt zusätzlich die Anforderungen an qualifizierte Vertrauensdiensteanbieter (TSP) bzw. qualifizierte Vertrauensdienste für Website-Authentisierung gemäß eIDAS-Verordnung (EU) No 910/2014.

Die Erfüllung dieser Anforderungen wird jährlich durch eine DIN EN ISO/IEC 17065 akkreditierte Zertifizierungsstelle bescheinigt. Darüber hinaus wir jährlich ein internes Audit nach DIN EN ISO/IEC 19011 durchgeführt.

Für alle hier beschriebenen Varianten gilt die Erklärung zum Zertifizierungsbetrieb (CPS Server.ID (TeleSec ServerPass)).

2.1 Kontaktdaten

Adresse:

T-Systems International GmbH
vertreten durch Deutsche Telekom Security GmbH
Trust Center & ID Security
Untere Industriestraße 20
57250 Netphen, Deutschland

Telefon:

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

WWW: https://www.telesec.de

E-Mail: telesec_support@t-systems.com

2.2 Erreichbarkeit des Sperrservices (24x7)

WWW: https://serverpass.telesec.de/serverpass/ts/ee/login/displayLogin.html

Auswählbare Sperrgründe sind:

- nicht spezifiziert
- Schlüssel kompromittiert
- Angaben im Zertifikat nicht mehr aktuell oder falsch
- Zertifikat wird nicht mehr benötigt

- Geschäftsaufgabe

Telefon:

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

2.3 Erreichbarkeit sonstiger Services

- Das Serviceportal und der Webserver stehen im monatlichen Mittel zu 98,0% zur Verfügung.
- Der LDAP-Verzeichnisdienst (CRL, ARL) steht im monatlichen Mittel zu 98,0% zur Verfügung.
- Der Online-Validierungsdienst (OCSP) steht im monatlichen Mittel zu 98,0% zur Verfügung.
- Der E-Mailserver steht im monatlichen Mittel zu 98,0% zur Verfügung.

2.4 Protokollereignisse

Im Loggingkonzept ist festgelegt, welche Daten und Ereignisse in welchen Abständen und von wem aufgezeichnet werden. Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden (aktuell 6 Wochen) und wie sie vor Verlust und unbefugtem Zugriff geschützt werden. Es werden dabei die Anforderungen aus ETSI EN 319 401 umgesetzt.

2.5 Aufbewahrungszeitraum für archivierte Daten

Folgende Aufzeichnungen und Aufbewahrungszeiträume werden festgelegt:

- Auftragsunterlagen, insbesondere Informationen zu Zertifikatsanträgen, deren Validierung, sowie die daraus resultierenden Zertifikate und vorgenommene Sperrungen, werden 7 Jahre nach Ablauf der Zertifikatsgültigkeit vorgehalten,
- bei Server.ID EV / EV SAN mit QWAC (TeleSec ServerPass EV / EV SAN mit QWAC) bis zur Betriebsbeendigung,
- Audit- und Event Logging Daten werden entsprechend den aktuellen gesetzlichen Bestimmungen archiviert.

2.6 Bestimmungen zur Beilegung von Streitigkeiten

Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei.

3 VERPFLICHTUNGEN

Der Unterzeichner (Auftraggeber, der Zertifikatsnehmer oder die autorisierte Person), der ein oder mehrere Zertifikate für einen Endteilnehmer oder ein Gerät beantragt, verwaltet oder betreibt, verpflichtet sich:

- Bei Bedarf einen Nachweis zu liefern, dass er Zertifikatsanforderungen im Namen des Kunden (juristische Person) beauftragen darf.
- Einen Nachweis über den Besitz oder die Kontrolle der Domain(s) aus dem Zertifikatsauftrag zu liefern.
- Die Angaben im Zertifikatsantrag vollständig und korrekt anzugeben.
- Umgehend nach der Ausstellung zu überprüfen, dass der Zertifikatsinhalt den zugrundeliegenden Auftragsdaten entspricht.
- Das ausgestellte Zertifikat ausschließlich bestimmungsgemäß und für autorisierte und legale Zwecke zu verwenden.
- Keinen Zertifikatsmissbrauch zu betreiben und nicht der Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) des Dienstes Server.ID (TeleSec ServerPass) zu widersprechen und Festlegungen zu Themenpunkt Zertifikatssperrung beachten.
- Die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der im o.g. CPS beschriebenen Pflichten entstehen.
- Die Schlüssel und Zertifikate nur in den zulässigen Anwendungen einzusetzen. Die Anwendung muss dabei den im Zertifikat eingetragenen Schlüsselverwendungen genügen.
- Das Zertifikat nicht mit Anwendungen oder Maschinen zu nutzen, deren Funktionen unbekannt, verdächtig oder unzuverlässig erscheint.
- Den privaten Schlüssel angemessen und vor unberechtigtem Zugriff durch Dritte zu schützen.
- Tatsächlich als Endteilnehmer zu agieren und mit seinem privaten Schlüssel keine CA-Funktionalitäten durchzuführen, wie z.B. Signatur von Zertifikaten oder Sperrlisten.
- Bei Verlust, Verdacht der Kompromittierung oder Manipulation des privaten Schlüssels, wesentlichen Änderungen der Zertifikatsangaben, Einstellung der Zertifikatsnutzung oder Missbrauchsvermutung eine Sperrung des entsprechenden Endteilnehmer-Zertifikats unverzüglich zu veranlassen bzw. selbst durchzuführen.
- Bei Kompromittierung des privaten Schlüssels ist dessen Verwendung unmittelbar und dauerhaft einzustellen.
- Das Zertifikat nicht mehr zu nutzen, wenn bekannt wird, dass das Zertifikat der Zertifizierungsstelle kompromittiert wurde.

Die aktuelle Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS) des Dienstes Server.ID (TeleSec ServerPass) als auch Vorgängerversionen dieses Dokuments sind öffentlich abgelegt unter:

https://www.telesec.de/de/service/downloads/pki-repository/

4 EMPFEHLUNGEN AN VERTRAUENDE DRITTPARTEIEN (RELYING PARTIES)

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 zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

Jeder Vertrauende Dritte sollte daher

- vor der Nutzung des Zertifikats die darin angegebenen Informationen auf Richtigkeit überprüfen,
- die Gültigkeit des Zertifikats überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie) sowie den Gültigkeitszeitraum und die Sperrinformationen (CRLs oder OCSP) des Zertifikats überprüft,
- das Zertifikat ausschließlich für autorisierte und legale Zwecke in Übereinstimmung mit der vorliegenden CPS einsetzen. T-Systems ist nicht für die Bewertung der Eignung eines Zertifikats für einen bestimmten Zweck verantwortlich,
- 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.