TÜVIT

Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

SK ID Solutions AS
Pärnu avenue 141
11314 Tallinn, Estland

Zertifikatsgültigkeit:
26.09.2023 – 26.09.2028

für die qualifizierte elektronische Signaturerstellungseinheit

Smart-ID SecureZone, Version 11.5.23

die Erfüllung der Anforderungen gemäß

Anhang II der VO (EU) Nr. 910/2014 (eIDAS).

Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats mit der ID 9803.23 und besteht aus 6 Seiten.

Essen, 26.09.2023

Dr. Christoph Sutter, Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen
tuvit.de

Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH ist als Zertifizierungsstelle gemäß Artikel 30.2 der „VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG“ von der Bundesnetzagentur (Deutschland) notifiziert.

Die Zertifizierungsstelle führt ihre Zertifizierung für qualifizierte Signatur-/Siegelerstellungseinheiten (QSCD) auf der Grundlage des folgenden Zertifizierungsschemas durch:

- „Certification Process for eIDAS conformant QSCDs of the certification body of TÜV Informationstechnik GmbH“, Version 1.2 vom 27.10.2020; die aktuelle Version kann heruntergeladen werden von: www.tuvit.de/en/services/eid-trust-services/qscd/

Der Zertifizierungsprozess für eIDAS-konforme QSCDs macht von der alternativen Methode nach Artikel 30.3 (b) der eIDAS Gebrauch.

Evaluierungs- / Zertifizierungsbericht

- “Certification Report TUVIT-TSZ-CC-9265-2023 Smart-ID SecureZone, Version 11.5.23” vom 26.09.2023, TÜV Informationstechnik GmbH

Evaluierungsanforderungen

Die Evaluierungsanforderungen sind definiert in:

- Anhang II der VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Die Evaluierungsanforderungen sind am Ende zusammenfassend aufgeführt.

Evaluierungsgegenstand

Der Evaluierungsgegenstand ist die qualifizierte elektronische Signaturerstellungseinheit (QSCD) „Smart-ID SecureZone“, Version 11.5.23.

Beschreibung des Evaluierungsgegenstands

Die QSCD besteht aus einer Softwarekomponente (kurz EVG), einem mobilen Client (Benutzerschnittstelle zum Unterzeichner) und einem nach EN 419 221-5[1] zertifizierten kryptographischen Modul (HSM). Es handelt sich um eine Remote-QSCD, bei der der qualifizierte Vertrauensdiensteanbieter die elektronischen Signaturerstellungsdaten im Auftrag eines Unterzeichners verwaltet.

Der EVG ist das Softwareprodukt „Smart-ID SecureZone“. Es ist ein Java-Applikationsserver-Paket, das die serverseitigen Funktionen des Threshold Signature Scheme Protocol für den Unterzeichner und die Verwaltungsfunktionen für die Administratoren implementiert.

Das Threshold Signature Scheme Protocol besteht aus einem kryptographischen Protokoll und Algorithmen, die vom Unterzeichner und dem EVG befolgt werden, um das verteilte Schlüsselpaar des Unterzeichners zu erzeugen und später das Schlüsselpaar zu verwenden, um die Signatur des Unterzeichners zu erstellen.

Der Unterzeichner, der die clientseitigen Funktionen des TSSP nutzt, kann die Dienste des EVG in Anspruch nehmen, um neue Schlüsselpaare zu registrieren, digitale Signaturen zu erzeugen und die Schlüsselpaare zu zerstören. Der EVG allein erstellt nicht die gesamte digitale Signatur im Auftrag des Unterzeichners, sondern beide nehmen an dem kryptographischen Protokoll teil.

Der EVG wird in einer speziellen manipulationssicheren Umgebung eingesetzt, die über einen vertrauenswürdigen Kanal mit dem HSM verbunden ist. Er verwendet die Signaturaktivierungsdaten (SAD), die der Unterzeichner auf dem mobilen Client eingibt, um die Signaturberechnung mit dem HSM abzuschließen.

Auslieferung des Evaluierungsgegenstandes

Der EVG einschließlich der EVG-Dokumentation ist in einem Software-Zip-Archiv zusammengestellt, das über ein Auslieferungssystem ausgeliefert wird. Die Integrität des ausgelieferten EVG muss durch Vergleich der SHA-384-Hash-Werte des EVG überprüft werden.

Nr.	Typ	Artikel / SHA-384 Hash Wert	Form der Auslieferung
1.	SW	SecureZone binary package (file name: sz-11.5.23_RELEASE-all.jar) 5cfcafdd4ed4dfbd9c414b615985abbb7310bc74b47211c3b541389cbe7b1086eb146a41b39a541b92ed1efd500c94a7	Secure file transfer system
2.	SW	sz-boot-11.5.23_RELEASE-executable.jar (file name: sz-boot-11.5.23_RELEASE-executable.jar) a7fdb96566bad7be962f9095b5bc9d95c76d03e3781213139caa3bf01f4840026ef874de84b20f759801657d8471a924	Secure file transfer system
3.	SW	SecureZone Admin CLI binary package (file name: secure-zone-cli.jar)	Secure file transfer system

[1] Protection Profiles for TSP cryptographic modules – Part 5: cryptographic module for Trust Services. English version EN 419221-5:2018

Nr.	Typ	Artikel / SHA-384 Hash Wert	Form der Auslieferung
		2b46995d8fc7b05af99214dbf9a26be935ff6768ac5b5276124bb19b21fcf043f5ac0be1b4833886de73b4a9b84347aa	
4.	SW	Liquibase changesets and scripts for initializing and updating the database schema (file name: liquibase.tar) 619252e50b20900cc7e8295b13127903a21407cf98c37ab1b43bd9b4ce687b9fefd14e5c8bf1739672398e05afc96170	Secure file transfer system
5.	DOC	Installation Guide for SecureZone v2.32_v133 f817289ac42b9241b8d648924746d0b67f92a9deb96b5cab164fde02346518d6092a59acbdebeb8b649944006297988a	Secure file transfer system
6.	DOC	Administration Guide for SecureZone v2.15_v78 7e65d4d7a7b366a0b8f4a12958987161ab51e4e2bd6a0c073ab04e1c51e3277138ce70d1677a1fec6c9a2fd55fccfa7a	Secure file transfer system
7.	DOC	Smart-ID SecureZone monitoring guide v1.6_v19 2dac8a1f63952a00759febb0b868556218861857a1b28eda1172debfebcb4a0661da35e33a4d26e1121e71107f39e844	Secure file transfer system
8.	DOC	Signer User Guidance information for SecureZone and TSE library operators v2.8_v11 1850e329825b29918e538fd0181add2137021a085c7bd6764ee06fabc3d0e0d1ff7c7e58545097082043d8b01a31e66d	Secure file transfer system

Die Informationen für den Integritätsprüfungsprozess werden in einem digital signierten Zustellungsbericht im Asice-Format geliefert.

Nr.	Typ	Artikel / SHA-384 Hash Wert	Form der Auslieferung
9.	DOC	Release Notes document (file name: smartid-sz-release-notes-11.5.23.txt)	Secure file transfer system, delivered in digitally signed container containing overview of changes and checksums of all delivered components
10.	DOC	Checksums txt (file name: smartid-sz-checksums-11.5.23.txt)	Secure file transfer system, delivered in digitally signed container containing overview of changes and checksums of all delivered components

Die Lieferung des HSM und des mobilen Clients muss gemäß den Zertifizierungsanforderungen erfolgen.

Evaluierungsergebnis

- Der Evaluierungsgegenstand erfüllt alle anwendbaren Evaluierungsanforderungen.

- Die im Zertifizierungsschema definierten Zertifizierungsanforderungen sind erfüllt.
- Die Einsatzbedingungen im Zertifizierungsbericht sind zu beachten.

Zusammenfassung der Evaluierungsanforderungen

Der Anhang II der eIDAS enthält die folgenden Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten:

1. Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass

   (a) die Vertraulichkeit der zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten angemessen sichergestellt ist.

   (b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten praktisch nur einmal vorkommen können.

   (c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit nicht abgeleitet werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik verlässlich gegen Fälschung geschützt ist.

   (d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.

2. Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.

3. Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.

4. Unbeschadet des Absatzes 1 Buchstabe d dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich zu Sicherungszwecken kopieren, sofern folgende Anforderungen erfüllt sind:

   (a) Die kopierten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen.

   (b) Es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.

Betriebsbedingungen

Die folgenden Betriebsbedingungen müssen erfüllt sein:

- Der EVG muss in der Umgebung eines qualifizierten Vertrauensdiensteanbieters implementiert werden, der die in den eIDAS festgelegten Anforderungen erfüllt.
- Die Umgebung des EVG muss physisch gesichert sein.
- Für die kryptographische Schlüsselerzeugung und kryptographische Operationen muss eines der folgenden HSM-Modelle installiert, konfiguriert und als Zufallsquelle für die Secure Zone verwendet werden:
  - CC-zertifiziertes HSM Thales nShield HSM Family v11.72.02 (Zertifikat Nr. 1/16, Stand: 2016-03-10 von OCSI - Organismo di Certificazione della Sicurezza Informatica, via Viale America, 201, 00144 Roma, Italien)
  - CC-zertifiziertes HSM nCipher nShield Solo XC v12.60.15 (Bericht Nr. NSCIB-CC-163968-CR2, Stand: 17-03-2021 vom TÜV Rheinland Nederland B.V, Westervoortsedijk 73, 6827 CE Arnhem, Niederlande)
- Als Benutzerschnittstelle muss die mobile Anwendung mit einer zertifizierten TSE-Bibliothek, die von CC mit der Assurance mindestens Stufe EAL2 bewertet wurde, vom Unterzeichner verwendet werden.
- Die Administratoren dürfen nur sichere Verdauungsalgorithmen (SHA-256 oder besser) für die Erzeugung der zu signierenden Datendarstellung (DTBS/R) akzeptieren.
- Der Secure Zone Server muss mit einer vertrauenswürdigen Zeitquelle synchronisiert werden.
- Nur vertrauenswürdiges, gut geschultes Personal darf mit der Durchführung von Administrationsaufgaben betraut werden.
- Administrationsaufgaben müssen im Vier-Augen-Prinzip durchgeführt werden.
- Die netzwerk- und kanalbasierte Sicherheit muss so konfiguriert sein, dass die übertragenen DTBS/R vor der Offenlegung geschützt sind.

Algorithmen und zugehörige Parameter

Für die Erstellung von qualifizierten elektronischen Signaturen verwendet der EVG kryptographische Algorithmen:

- RSA PKCS1-v1_5, RSASSA-PSS mit 3071, 3072, 4095, 4096, 6143, 6144, 8191, 8192 Bit Schlüssellänge gemäß PKCS#1: RSA Cryptography Specifications, Version 2.2 vom November 2016 (RFC8017)

Evaluation Assurance Level

Der EVG, Version 11.5.23, wurde nach Common Criteria evaluiert und zertifiziert. Ein Zertifikat wurde unter der Nummer TUVIT-TSZ-CC-9265-2023 am 26.09.2023 von der Zertifizierungsstelle der TÜViT ausgestellt. In den Sicherheitsvorgaben wurden die Anforderungen aus den zertifizierten Schutzprofilen berücksichtigt:

- EN 419 221-5:2018, Protection profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

- EN 419 241-2019, Feb. 2019, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing

Der Zertifizierungsreport für den EVG, Version 11.5.23, der die Sicherheitsvorgaben enthält, kann von der TÜVIT-Website heruntergeladen werden:

- https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/en/9265BE.pdf

Die Anforderungen an die Vertrauenswürdigkeit des EVG basieren vollständig auf den Vertrauenswürdigkeitskomponenten und -klassen, die in Teil 3 der Common Criteria definiert sind (siehe Teil C dieses Berichts oder [CC] Teil 3 für weitere Einzelheiten). Der EVG erfüllt die Vertrauenswürdigkeitsanforderungen der Vertrauenswürdigkeitsstufe EAL 4 (Evaluation Assurance Level 4), ergänzt durch AVA_VAN.5 (Advanced methodical vulnerability analysis).

Gültigkeitsdauer des Zertifikats

Dieses Zertifikat ist nur in Verbindung mit dem Zertifikat TUVIT-TSZ-CC-9265-2023 und dem entsprechenden Zertifizierungsreport ab dem 26.09.2023 gültig.

Die Gültigkeitsdauer des QSCD-Zertifikats hängt von der Stärke der im Produkt implementierten Sicherheitsmechanismen und Algorithmen ab und ist maximal bis zum 26. September 2028 begrenzt.

Die Gültigkeitsdauer kann zu einem bestimmten Zeitpunkt verlängert oder verkürzt werden, wenn neue Erkenntnisse über die Eignung der Sicherheitsmechanismen oder Algorithmen vorliegen.