Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: +43 1 503 19 63–0
Fax: +43 1 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

QSEE-BESCHEINIGUNG DER BESTÄTIGUNGSSTELLE GEM. § 7 ABS. 1 SVG[1] IVM ART. 30 ABS. 3 LIT. B EIDAS-VO[2]

Qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) PrimeSign Remote Signing Device/Core für qualifizierte Signaturen und Siegel (QRSD-C, Version 2.2)

Antragsteller:
PrimeSign GmbH
Wielandgasse 2
8010 Graz

Referenznummer A-SIT-VIG-23-072

QSEE-Bescheinigung gültig ab:
Siehe Datum der qualifizierten elektronischen Signatur

1. Beschreibung der zu bescheinigenden Komponente

Teilkomponenten:

Die qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) *PrimeSign Remote Signing Device/Core für qualifizierte Signaturen und Siegel (QRSD-C[3], Version 2.2)* besteht aus einer Hardware-Appliance (i.e., QRSD-C-Server)[4], in der die lokale Softwareapplikation QRSD-Core betrieben wird und in dem ein Hardware-Security-Modul (HSM) vom Typ *Thales Luna K7* zur Durchführung der kryptografischen Operationen installiert ist[5]. Durch die lokale Softwareapplikation *QRSD-Core* wird das Signature-Activation-Protocol (SAP) implementiert. Dieses steuert insbesondere die Kontrolle über die Auslösung der Signatur- sowie der Siegelerstellungsfunktion.

[1] Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016 vom 8. Juli 2016 idF BGBl. I Nr. 27/2019 vom 29. März 2019)

[2] 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

[3] QRSD-C – Qualified Remote Signing Device - Core

[4] Anmerkung – Die Hardware-Appliance stellt eine vor Manipulationen geschützte sichere Umgebung für das QRSD-C zur Verfügung, ist allerdings selbst nicht Teil der bescheinigten Komponente.

[5] Zertifizierte Hard- und Firmware-Versionen für die diese Bescheinigung gültig ist, sind in Abschnitt 6. angeführt.

© A-SIT, Partner für Sicherheitsfragen

Der Betrieb des QRSD-C erfolgt im geschützten Bereich des qualifizierten Vertrauensdiensteanbieters (VDA), der physische Zugang zum QRSD-C ist restriktiv auf autorisierte, privilegierte Benutzerinnen und Benutzer eingeschränkt.

Erzeugung der Signatur- und Siegelerstellungsdaten:

Die QSEE unterstützt „Einmalsignaturen“[6] und Signaturen bzw. Siegel mit persistenten Signatur- bzw. Siegelerstellungsdaten. Nach der Authentifizierung der Benutzerin bzw. des Benutzers[7] (die Anmeldung erfolgt entweder direkt über den VDA oder mittels delegierter Authentifizierung bei Identity-Providern bzw. Registration-Authorities) werden im HSM die Signatur- bzw. Siegelerstellungsdaten erzeugt und ein Zertifikatsrequest signiert. Das Zertifikat wird durch einen qualifizierten VDA ausgestellt[8] und den Signatur- bzw. Siegelerstellungsdaten zugeordnet. Bei Einmalsignaturen können anschließend in der aktiven Sitzung Signaturaufträge durchgeführt werden und die Signatur- bzw. Siegelerstellungsdaten werden anschließend zerstört. Sonst werden die Signatur- bzw. Siegelerstellungsdaten persistent gespeichert.

Speicherung der Signatur- und Siegelerstellungsdaten:

Die Signaturerstellungsdaten werden bei qualifizierten Signaturen nur temporär für die Dauer des Signaturvorgangs im HSM gehalten und sonst in verschlüsselter Form außerhalb gespeichert. Bei qualifizierten Siegeln ist auch eine persistente Speicherung der Siegelerstellungsdaten im HSM möglich. Zur persistenten Speicherung außerhalb des HSM werden die Signatur- bzw. Siegelerstellungsdaten mit einem Schlüssel des HSM verschlüsselt.

Signaturerstellung:

Zur Signaturerstellung müssen sich Benutzerinnen und Benutzer über einen vom VDA betriebenen Authentication Provider (nicht Teil der QSEE) nach SCAL2[9] gemäß EN 419 241-1 authentifizieren.

Allgemein sind zwei voneinander unabhängige[10] Faktoren für die Authentifizierung im Einsatz. Dabei handelt es sich um:

(1) Erster Authentifizierungsfaktor
- Persistierte Benutzerdaten (z.B. Benutzername und Passwort)
- One-time-tokens[11]
- Kryptografische Challenge-Response-Verfahren mit asymmetrischer Verschlüsselung (z.B. FIDO2[12])

(2) Zweiter Authentifizierungsfaktor
- SMS[13]-TAN[14] mit einer vorregistrierten Mobiltelefonnummer
- Kryptografische Challenge-Response-Verfahren mit shared-secret (z.B. TOTP[15])
- Kryptografische Challenge-Response-Verfahren mit asymmetrischer Verschlüsselung (z.B. FIDO2)

[6] D.h. die Signaturerstellungsdaten werden nur für die Signaturaufträge der aktiven Sitzung verwendet und anschließend gleich wieder zerstört.
[7] D.h. Signatorinnen und Signatoren (Unterzeichnerinnen und Unterzeichner iSd eIDAS-Verordnung) bzw. Siegelerstellerinnen und Siegelersteller
[8] Anmerkung: Die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser Bescheinigung
[9] SCAL2 – Sole Control Assurance Level 2
[10] Anmerkung: „unabhängig“ bedeutet, dass wenn für beide Faktoren gleiche Verfahren (z.B. kryptografische Challenge-Response-Verfahren mit asymmetrischer Verschlüsselung) zum Einsatz kommen, voneinander unabhängige Elemente (z.B. unterschiedliche Hardware-Token) und auch Elemente aus mindestens zwei unterschiedlichen Kategorien (Wissen, Besitz, Inhärenz) verwendet werden müssen.
[11] z.B. ein vom VDA ausgestelltes Artefakt (eine lange, nicht erratbare Zeichenfolge)
[12] FIDO – Fast IDentity Online
[13] SMS – Short Message Service
[14] TAN – Transaction Authentication Number
[15] TOTP - time-based one-time password über eine registrierte Smartphone-App

- Weitere Methoden, die den Anforderungen nach SCAL2 gemäß EN 419 241-1 genügen

Wenn – bei delegierter Authentifizierung – die SCAL2 Anforderungen bereits durch den delegierten Authentication Provider erfüllt werden, ist kein zweiter Authentifizierungsfaktor erforderlich.

Nach erfolgreicher Authentifizierung und Autorisierung der zu signierenden Daten generiert der Authentication Provider ein signiertes Token (die DTBS/R[16] gehen in dieses Token ein), das an die QSEE übermittelt und dort geprüft wird. Nach erfolgreicher Prüfung werden die Signaturerstellungsdaten im HSM entschlüsselt und eine qualifizierte elektronische Signatur erstellt. Nach der Signaturerstellung werden die entschlüsselten Signaturerstellungsdaten im HSM gelöscht.

Siegelerstellung:

Die Funktion zur Siegelerstellung ist nur dann durchführbar, wenn das korrespondierende Zertifikat für elektronische Siegel ausgestellt wurde. Bei der Siegelerstellung müssen die SCAL2 Anforderungen nicht zwingend erfüllt werden und es kommt somit wahlweise nur der erste Authentifizierungsfaktor zum Einsatz oder sowohl der erste als auch der zweite Authentifizierungsfaktor. Die zur Verfügung stehenden Verfahren für den ersten und zweiten Authentifizierungsfaktor sind ident mit jenen für die Signaturerstellung. Es ist eine persistente Speicherung der Siegelerstellungsdaten im HSM über die Sitzung zur Siegelerstellung hinaus möglich.

[16] Data to be signed / Representation

2. Erfüllung der Anforderungen der eIDAS-VO

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach Artikel 29 Abs. 1[17] eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1[18] eIDAS-VO,
- Anforderungen nach Anhang II eIDAS-VO (Abs. 1 lit. a[19],b[20],c[21],d[22], Abs. 2[23], Abs. 3[24], Abs. 4 lit a[25], b[26])

Die QSEE ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung von Signatur- und Siegelerstellungsdaten,
- Komponenten und Verfahren zum Speichern von Signatur- und Siegelerstellungsdaten,
- Komponenten und Verfahren zur Verarbeitung der Signatur- und Siegelerstellungsdaten

3. Gültigkeitsdauer der QSEE-Bescheinigung

Die Gültigkeit dieser QSEE-Bescheinigung ist bis auf Widerruf durch A-SIT aufrecht. A-SIT führt bei Beauftragung eine kontinuierliche Evidenthaltung und ein Monitoring hinsichtlich der Sicherheit der eingesetzten Produkte und Verfahren sowie der kryptografischen Algorithmen und Parameter durch. Mit der Ausstellung dieser QSEE-Bescheinigung ist ein Monitoring für zwei Jahre verbunden. Der Widerruf erfolgt sofern die Sicherheit der eingesetzten Produkte und Verfahren sowie der

---

[17] *Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.*

[18] *Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.*

[19] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass die Vertraulichkeit der zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten angemessen sichergestellt ist.*

[20] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten praktisch nur einmal vorkommen können.*

[21] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass 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.*

[22] *Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich geschützt werden können.*

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

[24] *Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.*

[25] *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.*

[26] *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: Es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.*

kryptografischen Algorithmen und Parameter nicht mehr dem Stand der Technik entsprechen bzw. kein weiteres Monitoring beauftragt wird.

4. Einsatzbedingungen

Die Gültigkeit dieser QSEE-Bescheinigung ist an die im Folgenden angeführten Einsatzbedingungen gebunden. Diesen ist in geeigneter Weise der Wirkung nach zu entsprechen und es sind die getroffenen Maßnahmen

- durch das Sicherheits- und Zertifizierungskonzept des Vertrauensdiensteanbieters sicherzustellen,
- in der Belehrung der Benutzerin bzw. des Benutzers entsprechend zu übernehmen
- und deren Wirkung im Wege der Beaufsichtigung (iSv Artikel 20 eIDAS-VO) sicherzustellen.

(1) Die eindeutige Zuordnung und die sichere Beendigung der Benutzer/innen-Session sowie die Vertraulichkeit und Integrität der Autorisierungscodes und die Integrität der zu signierenden bzw. zu besiegelnden Daten bei der Übertragung von der Benutzerin bzw. vom Benutzer zur QSEE im Zuge des Auslösevorgangs sind in der Systemumgebung der QSEE sicherzustellen und daher nicht Teil der QSEE-Bescheinigung[27]. Es ist sicherzustellen, dass die Benutzerin bzw. der Benutzer darüber informiert sind, dass ihre im Zuge der Auslösung der Signatur bzw. des Siegels verwendeten Komponenten (Mobilfunkgerät, OTP-Device, Webbrowser etc.) geeignet abgesichert sein müssen.

(2) Die QSEE darf nur von einem qualifizierten Vertrauensdiensteanbieter betrieben werden.

(3) Der qualifizierte Vertrauensdiensteanbieter muss die QSEE in einer geschützten Umgebung betreiben, dabei ist insbesondere zu gewährleisten:

- Beschränkung des physischen Zugangs zur QSEE auf privilegiertes und autorisiertes Personal
- Schutz vor Verlust und Diebstahl der QSEE und der außerhalb dieser gespeicherten Assets
- Maßnahmen zur Erkennung und zur Verhinderung von Manipulationsversuchen (einschließlich Zugriffe auf Seitenkanäle, Zugriffe auf Verbindungen zwischen physisch separierten Komponenten der QSEE oder Teile der Hardware-Appliance)
- Schutz gegen die Möglichkeit von Attacken beruhend auf kompromittierender elektromagnetischer Abstrahlung
- Schutz vor unautorisierten Änderungen an der Software und Konfiguration der QSEE sowie der Hardware-Appliance
- Äquivalentes hohes Schutzniveau für alle Teilkomponenten (einschließlich für zu Sicherungszwecken verwendete Komponenten)

(4) Das HSM muss unter Einhaltung des 4-Augen-Prinzips (dabei muss mindestens eine Person die Rolle „Security Officer“ innehaben) initialisiert und dabei in den „FIPS 140-2 approved mode“ geschalten werden.

(5) Elektronische Signatur- bzw. Siegelerstellungsdaten dürfen zu Sicherungszwecken nur soweit kopiert werden als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.

(6) Externe Authentifizierungsmechanismen, die zur Authentifizierung von Benutzerinnen und Benutzern verwendet werden, um eine qualifizierte elektronische Signatur zu erstellen, müssen einem Authentifizierungsmittel entsprechen, das der EU-Durchführungsverordnung 2015/1502 für ein substanzielles oder höheres Sicherheitsniveau entspricht.

(7) Es muss technisch und/oder organisatorisch verhindert werden, dass benutzerseitige Komponenten, die ausnutzbare Schwachstellen aufweisen und somit ungeeignet für die Authentifizierung sind, für die Signaturauslösung verwendet werden können.

[27] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

5. Algorithmen und zugehörige Parameter

Zur Erstellung von qualifizierten elektronischen Signaturen bzw. qualifizierten elektronischen Siegeln werden von der QSEE die kryptografischen Algorithmen

- RSASSA-PKCS1-v1_5 mit SHA-256 oder SHA-512 nach FIPS PUB 186-4 und RFC 8017 mit Schlüssellängen von 3072 und 4096 Bit,
- RSASSA-PSS nach FIPS PUB 186-4 und RFC 8017 mit Schlüssellängen von 3072 und 4096 Bit oder
- ECDSA mit SHA-256, SHA-384 oder SHA-512 nach FIPS PUB 186-4 und den Kurven P-256, P-384 und P-521 nach FIPS PUB 186-4 sowie brainpool_p256r1, brainpool_p384r1, brainpool_p512r1 nach RFC 5639 mit Schlüssellängen von 256, 384, 512 und 521 Bit

verwendet.

6. Prüfstufe und Mechanismenstärke

Zu dem von der QSEE verwendeten Hardware Security Modul vom Typ „Thales/SafeNet Luna K7“[28] (Modell-Nr.: A700, A750 und A790) liegt das von der US-Amerikanischen (National Institute of Standards and Technology) und Kanadischen (Communications Security Establishment) FIPS 140-2 Zertifizierungsstelle ausgestellte Zertifikat Nr. 4090[29] ausgestellt am 02.12.2021, zuletzt erneuert am 09.03.2023 für Thales Luna K7, Firmware Versionen: 7.7.0 und 7.7.1 oder 7.7.1-20, mit Boot-Loader Versionen 1.1.1, 1.1.2, 1.1.4 und 1.1.5, Hardware Versionen: 808-000048-002, 808-000048-003, 808-000066-001, 808-000073-001 und 808-000073-002

Das Zertifikat weist dem Hardware Security Modul eine erfolgreiche Evaluierung nach FIPS 140-2 level 3 nach.

Da keine Normen für die Sicherheitsbewertung vorliegen, die durch die Kommission im Wege von Durchführungsrechtsakten festgelegt wurden, wurde das QSEE-Bescheinigungsverfahren gemäß Art. 30 Abs. 3 lit. b eIDAS-VO durchgeführt und die Gleichwertigkeit des Sicherheitsniveaus wurde von der Bestätigungsstelle nach dem Stand der Technik beurteilt.

Die QSEE widersteht in ihrer vorgesehenen Einsatzumgebung Angreifern mit hohem Angriffspotenzial.

Die dieser QSEE-Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VIG-23-072 dokumentiert.

Unterschrift

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN	**Unterzeichner**	Herbert Leitold
	Datum/Zeit-UTC	2023-08-31T20:10:09+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at

DI Herbert Leitold, Gesamtleiter

[28] Hersteller: Thales (ehem. Gemalto bzw. SafeNet), 20 Colonnade Road, Suite 200, Ottawa, ON K2E 7M6, Canada

[29] https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4090