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

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

A-8010 Graz, Inffeldgasse 16a
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 1.0)

Antragsteller:
PrimeSign GmbH
Wielandgasse 2
8010 Graz, Österreich

QSEE-Bescheinigung ausgestellt am: 20.11.2017
Referenznummer A-SIT-VIG-17-067

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 1.0)* 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 *SafeNet Luna PCI-E*[5] zur Durchführung der kryptografischen Operationen installiert ist. 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. Der Betrieb des QRSD-C erfolgt im geschützten Bereich des qualifizierten Vertrauensdiensteanbieters, der physische Zugang zum QRSD-C ist restriktiv auf autorisierte, privilegierte Benutzerinnen und Benutzer eingeschränkt.

---

[1] Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016 vom 08.Juli 2016)
[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] Modell-Nr.: 1700 und 7000, Firmware-Versionen: 6.2.1, 6.2.5, 6.3.1, 6.10.4, 6.10.7 und 6.10.9, Hardware-Versionen: VBD-05 Version Code 0100, VBD-05 Version Code 0101, VBD-05 Version Code 0103. Hersteller: Safenet Inc. heute integriert in Gemalto N.V. Strozzilaan 382, 1083 HN Amsterdam, Niederlande

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 sowie mit einem von den Authentifizierungsdaten der Benutzerin bzw. des Benutzers abgeleiteten Schlüssel verschlüsselt.

Signaturerstellung:

Allgemein sind zwei Faktoren für die Authentifizierung von Benutzerinnen und Benutzern im Einsatz. Dabei handelt es sich um:

(1) Erster Authentifizierungsfaktor
- Persistierte Benutzerdaten (i.e. Benutzername und Passwort).
- Delegierte Authentifizierung mit einer signierten Assertion.
- One-time-token[9]

(2) Zweiter Authentifizierungsfaktor (zur Aktivierung der Signaturerstellungsdaten)
- SMS-TAN als Einmalkennwort.
- Kryptografischer Challenge-Response-Mechanismus[10].
- One-time-token[11,12]

Beim Starten einer Signatursitzung wird zuerst der erste Authentifizierungsfaktor überprüft und mit Hilfe der Authentifizierungsdaten wird die erste Verschlüsselungsschicht über Signaturerstellungsdaten entschlüsselt. Zur Überprüfung des zweiten Authentifizierungsfaktors wird eine zeitlich begrenzt gültige Challenge erzeugt, in die der Hashwert der zu signierenden Daten eingeht. Nur nach Übermittlung der Challenge[13] an die Benutzerin bzw. den Benutzer und erfolgreicher Prüfung der Antwort innerhalb des vorgesehenen Zeitlimits werden die Signaturerstellungsdaten im HSM entschlüsselt und eine qualifizierte elektronische Signatur erstellt. Nach der Signaturerstellung werden die Signaturerstellungsdaten im HSM zerstört.

Siegelerstellung:

Die Funktion zur Siegelerstellung ist nur dann durchführbar, wenn das korrespondierende Zertifikat für elektronische Siegel ausgestellt wurde. Bei der Siegelerstellung kommt nur der erste Authentifizierungsfaktor zum Einsatz und es ist eine persistente Speicherung der Siegelerstellungsdaten im HSM über die Sitzung zur Siegelerstellung hinaus möglich.

[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] z.B. ein vom VDA ausgestelltes Einmalpasswort
[10] Mit shared-secret oder asymmetrischer Verschlüsselung; z.B. über eine registrierte Smartphone-App
[11] z.B. durch den Identity-Provider bzw. die Registration-Authority ausgegebene Einmalpasswörter, Authentifizierungs-Apps etc.
[12] es sind auch weitere Methoden möglich, die der Anforderung einer starken Authentifizierung für qualifizierte Fernsignaturen (SCAL2 nach EN 419 241-1) genügen.
[13] Z.B. als SMS-TAN oder über eine Smartphone-App

2. Erfüllung der Anforderungen der eIDAS-VO

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach Artikel 29 Abs. 1[14] eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1[15] eIDAS-VO,
- Anforderungen nach Anhang II eIDAS-VO (Abs. 1 lit. a[16],b[17],c[18],d[19], Abs. 2[20], Abs. 3[21], Abs. 4 lit a[22], b[23])

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 laufende 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 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 Aufsicht 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

[14] *Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.*
[15] *Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.*
[16] *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.*
[17] *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.*
[18] *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.*
[19] *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.*
[20] *Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.*
[21] *Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.*
[22] *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.*
[23] *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.*

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[24]. 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.

5. Algorithmen und zugehörige Parameter

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

- 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 mit Schlüssellängen von 256, 384 und 512 Bit

verwendet.

6. Prüfstufe und Mechanismenstärke

Zu den von der QSEE verwendeten Hardware Security Modulen vom Typ „SafeNet Luna PCI-E“ (Modell-Nr.: 1700 und 7000) liegen die folgenden von der US-Amerikanischen (National Institute of Standards and Technology) und Kanadischen (Communications Security Establishment) FIPS 140-2 Zertifizierungsstelle ausgestellten Zertifikate vor:

- Nr. 2488 ausgestellt am 15.12.2015 für Safenet Luna PCI-E Modell-Nr.:1700 und 7000, Firmware Versionen: 6.10.7 und 6.10.9, Hardware Versionen: VBD-05-0100, VBD-05-0101 und VBD-05-0103

[24] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

- Nr. 2480 ausgestellt am 12.2.2015, zuletzt erneuert am 23.06.2017 für Safenet Luna PCI-E Modell-Nr.: 1700 und 7000, Firmware Versionen: 6.2.1 und 6.2.5, Hardware Versionen: VBD-05-0100, VBD-05-0101 und VBD-05-0103
- Nr. 2427 ausgestellt am 11.08.2015, zuletzt erneuert am 23.06.2017 für Safenet Luna PCI-E (Modell-Nr.: 1700 und 7000, Firmware Versionen: 6.10.4, 6.10.7 und 6.10.9, Hardware Versionen: VBD-05-0100, VBD-05-0101, VDB-05-102 und VBD-05-0103
- Nr. 2036 ausgestellt am 13.11.2013, zuletzt erneuert am 23.06.2017 für Safenet Luna PCI-E Modell-Nr.: 1700 und 7000, Firmware Version: 6.3.1, Hardware Version: VBD-05-0103
- Nr. 1693 ausgestellt am 23.06.2017, zuletzt erneuert am 23.06.2017 für Safenet Luna PCI-E Modell-Nr.: 1700 und 7000, Firmware Version: 6.2.1, Hardware Versionen: VBD-05-0100, VBD-05- 0101 und VBD-05-0103

Die Zertifikate weisen dem Hardware Security Modul eine erfolgreiche Evaluierung nach FIPS 140-2 nach[25].

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 dieser QSEE-Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VIG-17-067 dokumentiert.

Unterschrift:

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2017-11-21T07:23:32+01:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	

Prof. DI Dr. Reinhard Posch, Gesamtleiter

[25] Die Module werden in der gesicherten Umgebung des qualifizierten VDA mit passwort-basierter Authentifizierung im FIPS 140-2 level 2 mode betrieben. Für die Punkte „Physical Security“, „EMI/EMC“ und „Design Assurance“ wird FIPS 140-2 level 3 erreicht.