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) des Swisscom All-in Signing Service (AIS), Version 3.0

Antragsteller:
Swisscom IT Services Finance S.E.
Modecenterstraße 17 / Unit 2
1110 Wien

QSEE-Bescheinigung ausgestellt am: 04.10.2019
Referenznummer A-SIT-VIG-18-089

1. Beschreibung der zu bescheinigenden Komponente

Das *Swisscom All-in Signing Service* (AIS) ist ein Dienst zur Erstellung von qualifizierten und fortgeschrittenen Signaturen, qualifizierten und fortgeschrittenen Siegeln sowie qualifizierten Zeitstempeln und zur Ausstellung und Verwaltung der zugehörigen Zertifikate. Der Dienst verwendet dazu eine qualifizierte Signatur- und Siegelerstellungseinheit (QSEE bzw. qualified remote electronic signature/seal creation device - QRSCD), welche in einer sicheren Umgebung des Antragstellers betrieben wird.

Teilkomponenten:

Die QSEE des AIS besteht aus dem Signatur-Aktivierungsmodul (SAM), welches per Signaturaktivierungsprotokoll (SAP) die Auslösung der Signatur- und Siegelerstellungsfunktion steuert und den Hardware-Security-Modulen (HSM) zur Durchführung von kryptografischen Operationen. Es werden HSM vom Typ Gemalto SafeNet Luna Network HSM[3] verwendet. Der

[1] Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016 vom 08.Juli 2016 idF BGBl. I Nr. 32/2018 vom 17. Mai 2018)

[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] Geräte-Software: 6.2.2 bzw. 7.3, Firmware-Version: 6.10.9 bzw. 7.0.2, Hardware-Versionen: VBD-05-0100, VBD-05-0101, VBD-05-0103, 808-000048-002, 808-000066-001, 808-000073-001. Hersteller: Safenet Inc. heute integriert in Gemalto N.V. Barbara Strozzilaan 382, 1083 HN Amsterdam, Niederlande

Zugriff des AIS auf den HSM erfolgt über eine PKCS#11-Schnittstelle. Diese beiden Komponenten (SAM und HSM) bilden den zu bescheinigenden Bereich.

Der Betrieb all dieser Teilkomponenten erfolgt im geschützten Bereich des qualifizierten Vertrauensdiensteanbieters, darin ist einerseits der physische Zugang eingeschränkt und andererseits auch kein direkter Internetzugriff von außen möglich.

Alle restlichen Komponenten des AIS,

- die Certificate Authority (CA), zum Ausstellen bzw. Verwalten der Zertifikate,
- der Time Stamping Service (TSS), zum Erstellen von Zeitstempeln und
- das Datenbank-Management System (DBMS),

sowie die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser Bescheinigung. Auch die Serversignaturanwendung (SSA) und eventuelle Identitätsanbieter (IDP) als weitere remote Umgebungen zwischen dem Signator und dem AIS sind nicht Teil der Bescheinigung.

Erzeugung der Signatur- und Siegelerstellungsdaten:

Die QSEE unterstützt sowohl sog. „Einmalsignaturen“[4] als auch die Verwendung von statischen Siegelerstellungsdaten. Die zur Erstellung einer Signatur bzw. eines Siegels benötigten Erstellungsdaten werden im HSM generiert bzw. verwaltet und verlassen dieses nicht. Nach erfolgter Sicherstellung der Willenserklärung eines Unterzeichners, wird im Falle einer „Einmalsignatur“ ein einmaliger Unterzeichnungsschlüssel im HSM generiert, sowie ein kurzzeitig gültiges Zertifikat bei der CA beantragt. Mit Hilfe dieser Daten wird im Anschluss eine Signatur erstellt. Bei der Verwendung von statischen Siegelerstellungsdaten zur Erstellung qualifizierter elektronischer Siegel werden diese ebenfalls im HSM generiert und auch dauerhaft darin gespeichert.

Speicherung der Signatur- und Siegelerstellungsdaten

Signaturerstellungsdaten werden im HSM nur temporär gespeichert bis die Signatur generiert worden ist und danach gleich wieder zerstört. Für die Erstellung von Siegeln werden statische Siegelerstellungsdaten verwendet, die im HSM dauerhaft gespeichert bleiben. Signatur- und Siegelerstellungsdaten können nicht aus dem HSM exportiert werden.

Signatur- und Siegelerstellung:

Um eine qualifizierte Signatur- oder Siegelerstellung zu beantragen, müssen Unterzeichner zuerst durch die Registration-Authority (RA) authentifiziert und registriert werden. Die RA ist Teil der SSA oder eines IDP und somit nicht Gegenstand dieser Bescheinigung.

AIS liegt derzeit in zwei Produktvarianten vor. Das bisherige Produkt im Versionsnummernbereich 2.x unterstützt nur das Protokoll AIS-2. Das mit dieser Bescheinigung neu hinzugekommene Produkt mit der Versionsnummer 3.0 unterstützt zusätzlich zum Protokoll AIS-2 auch noch das Protokoll AIS-3. Die vorrangigste Änderung des neuen Protokolls ist ein zusätzlicher Auslösevorgang für den Signaturprozess.

AIS-2: Für die Signaturerstellung muss der Unterzeichner eine Zwei-Faktor-Authentifizierung absolvieren. Dabei wird ein SMS-TAN an die bei der Registrierung angegebene Mobilnummer (Besitz) versendet. Zusätzlich wird bei qualifizierten Signaturen das bei erstmaliger Verwendung angegebene Passwort (Wissen) abgefragt. Nach positivem Abgleich der beiden Faktoren können anschließend Signaturaufträge in der aktiven Sitzung durchgeführt werden. Dieser Abgleich und

[4] D.h. die Signaturerstellungsdaten werden nur für die Signaturaufträge der aktiven Sitzung verwendet und anschließend gleich wieder zerstört.

die Signaturerstellung erfolgen remote im AIS. Die dafür benötigten Signaturerstellungsdaten werden anschließend zerstört.

AIS-3: Als zusätzliche Variante für die Signaturfreigabe kann die Authentifizierung nach SCAL2 auch an einen IDP ausgelagert werden. Dieser prüft die Faktoren und sendet eine Bestätigung für einen Signaturauftrag an den AIS. Der AIS prüft wiederum, ob die Bestätigung mit dem von der SSA eingebrachten Signaturauftrag übereinstimmt und startet anschließend die Signaturerstellung.

AIS-2: Für die Ausstellung qualifizierter elektronischer Siegel wird eine beidseitig authentisierte TLS-Verbindung zwischen SSA und AIS aufgebaut. Der AIS prüft dabei, ob die Verbindung mit dem der SSA zugehörigen privaten Schlüssel aufgebaut wurde. Nach positiver Überprüfung übermittelt die SSA die Schlüssel-ID des Unterzeichners. Der AIS verwendet die unter dieser ID im HSM gespeicherten Siegelerstellungsdaten um ein Siegel zu erstellen.

2. Erfüllung der Anforderungen der eIDAS-VO

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach Artikel 29 Abs. 1[5] eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1[6] eIDAS-VO,
- Anforderungen nach Anhang II eIDAS-VO (Abs. 1 lit. a[7],b[8],c[9],d[10], Abs. 2[11], Abs. 3[12], Abs. 4 lit a[13], b[14])

[5] *Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.*
[6] *Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.*
[7] *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.*
[8] *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.*
[9] *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.*
[10] *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.*
[11] *Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.*
[12] *Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.*
[13] *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.*
[14] *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.*

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 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[15]. 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, 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

[15] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

- 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) Der durch die QSEE technisch unterstützte Hashalgorithmus SHA-1 eignet sich nicht für den Einsatz bei der Erstellung von qualifizierten elektronischen Signaturen[16], und darf daher in diesem Zusammenhang auch nicht mehr eingesetzt werden.

(7) Wird die Authentifizierung der Benutzerin oder des Benutzers zur Erstellung von qualifizierten Signaturen ausgelagert, so müssen die eingesetzten Methoden den Anforderungen an einen Authentifizierungsmechanismus nach EU Durchführungsverordnung 2015/1502 für das Sicherheitsniveau „Substantiell“ oder höher entsprechen[17].

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 und RSASSA-PSS nach PKCS#1 v2.2 (RFC 8017) mit Schlüssellängen von 2048 oder 3072 Bit

Zur Berechnung der Hashwerte wird SHA-256, SHA-384, SHA-512 verwendet[18].

6. Prüfstufe und Mechanismenstärke

Zu den von der QSEE verwendeten Hardware Security Modulen vom Typ Gemalto „SafeNet Luna Network HSM“ 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. 2489 ausgestellt am 15.12.2015, zuletzt erneuert am 27.03.2018 für Safenet Luna PCI-E Cryptographic Module, Firmware Versionen: 6.10.7, 6.10.9 und 6.11.2, Hardware Versionen: VBD-05-0100, VBD-05-0101 und VBD-05-0103

[16] Vgl. dazu „SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms”, Version 1.1, Juni 2018

[17] DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt; gemäß ANHANG Abschnitte 2.1, 2.2.1 und 2.3.1

[18] Die Berechnung der Hashwerte erfolgt außerhalb der QSEE in der aufrufenden Applikation. SHA-1 wird zur Rückwärtskompatibilität technisch unterstützt, darf allerdings bei qualifizierten Signaturen bzw. Siegeln nicht eingesetzt werden (siehe Einsatzbedingung 6). Die Dokumentation weist auf diesen Umstand hin.

- Nr. 3205 ausgestellt am 25.06.2018, zuletzt erneuert am 23.06.2019 für Safenet Luna K7 Cryptographic Module, Firmware Versionen: 7.0.1, 7.0.2, 7.0.3 und 7.3.3, Hardware Versionen: 808-000048-002, 808-000066-001 und 808-000073-001

Die Zertifikate weisen den Hardware Security Modulen eine erfolgreiche Evaluierung nach FIPS 140-2 nach[19].

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-18-089 dokumentiert.

Unterschrift:

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2019-10-04T16:03:37+02:00
	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

[19] Die Module werden in der gesicherten Umgebung des VDA im FIPS 140-2 level 3 Modus betrieben.