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

A-SIT

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

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) Swisscom All-in Signing Service (AIS), Version 3.2

Antragsteller:
Swisscom IT Services Finance S.E.,
Swisscom Trust Services
Mariahilfer Straße 123 / 3. Stock
1060 Wien

Referenznummer: A-SIT-VIG-24-035

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

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

[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, geändert durch Verordnung (EU) 2024/1183 des europäischen Parlaments und des Rates vom 11. April 2024

© A-SIT, Partner für Sicherheitsfragen

Operationen. Es werden HSM vom Typ Thales Luna Network HSM[3] verwendet. Der 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[4]) oder IDP-Broker 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“[5] 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.

[3] Zertifizierte Hard- und Firmware-Versionen für die diese Bescheinigung gültig ist, sind in Abschnitt 6. angeführt.
[4] IDP – Identity Provider
[5] D.h. die Signaturerstellungsdaten werden nur für die Signaturaufträge der aktiven Sitzung verwendet und anschließend gleich wieder zerstört.

Signatur- und Siegelerstellung:

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

Das vorliegende Produkt AIS 3.2 unterstützt zwei verschiedene Protokolle: AIS-2 und AIS-3. Der grundsätzliche Unterschied zwischen beiden Protokollen ist, dass die Überprüfung der Authentifizierungsfaktoren zur Auslösung der Signaturerstellung bei AIS-2 durch das AIS selbst durchgeführt wird und bei AIS-3 durch einen ausgelagerten IDP bzw. IDP-Broker. Weiters kann AIS-3 nur für Signaturen eingesetzt werden, wohingegen AIS-2 sowohl Signaturen als auch Siegel unterstützt.

Signatur:

- AIS-2 (OASIS): Für die Signaturerstellung muss der Unterzeichner eine Zwei-Faktor-Authentifizierung absolvieren. Diese kann entweder mittels SMS-TAN-Verfahren oder Mobile ID Service erfüllt werden:
    - Bei ersterem wird ein TAN[6] per SMS an die bei der Registrierung angegebene Mobilnummer (Besitz) versendet. Zusätzlich wird bei qualifizierten Signaturen das bei erstmaliger Verwendung angegebene Passwort (Wissen) abgefragt.
    - Für das zweite Verfahren wird ein Mobilgerät benötigt auf dem die *Mobile ID* (entweder als Mobilapplikation oder SIM[7]-Applet) installiert ist und das im Zuge der Registrierung über die Mobilfunknummer an den Unterzeichner gebunden wurde. Die Signaturauslösung erfolgt – je nach Einstellung – entweder durch Eingabe der Mobile ID[8] PIN[9] oder durch die betriebssystemeigenen Mechanismen zur Entsperrung, wie zum Beispiel PIN, Passwort (Wissen) oder biometrische Abfragen (Inhärenz). Die Abfrage dieses Faktors wird durch die Mobile ID durchgeführt, welche in weiterer Folge eine signierte Bestätigung an den AIS sendet und somit auch den Besitz des Mobilgerätes eindeutig nachweist.

  Nach positivem Abgleich der beiden Faktoren können anschließend Signaturaufträge in der aktiven Sitzung durchgeführt werden. Dieser Abgleich und die Signaturerstellung erfolgen remote im AIS. Die dafür benötigten Signaturerstellungsdaten werden anschließend zerstört.

- AIS-3 (basierend auf ETSI TS 119 432): Als zusätzliche Variante für die Signaturfreigabe kann die Authentifizierung nach SCAL2 auch an einen IDP bzw. IDP-Broker ausgelagert werden. Ersterer prüft die Faktoren und sendet eine Bestätigung für einen Signaturauftrag an die SSA. Der AIS prüft wiederum beim IDP, ob die Bestätigung mit dem von der SSA eingebrachten Signaturauftrag übereinstimmt und startet anschließend die Signaturerstellung. Statt der direkten Anbindung eines IDP kann auch ein IDP-Broker (MAB[10]) zwischengeschalten werden. Dieser registriert und verwaltet die angebundenen vertrauenswürdigen IDP und sendet Anfragen der SSA an den jeweiligen IDP weiter. Nach der Prüfung der Authentifizierungsfaktoren retourniert der IDP eine signierte Bestätigung zurück an den IDP-Broker, welcher die Bestätigung nach erfolgreicher Validierung ebenfalls signiert und an die SSA weiterleitet. Der AIS kann in weiterer Folge den von der SSA eingebrachten Signaturauftrag beim IDP-Broker prüfen. Der IDP-Broker kann auch selbst als IDP fungieren.

Siegel:

- AIS-2: Für die Ausstellung qualifizierter elektronischer Siegel wird eine beidseitig authentisierte TLS[11]-Verbindung zwischen SSA und AIS aufgebaut. Der AIS prüft dabei, ob

[6] TAN – Transaction Authentication Number
[7] SIM – Subscriber Identity Module
[8] ID – Identity
[9] PIN – Personal Identification Number
[10] MAB – Multiple Authentication Broker
[11] TLS – Transport Layer Security

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[12] eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1[13] eIDAS-VO,
- Anforderungen nach Anhang II eIDAS-VO (Abs. 1 lit. a[14],b[15],c[16],d[17], Abs. 2[18], Abs. 3[19], Abs. 4 lit a[20], b[21])

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

[12] *Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.*
[13] *Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.*
[14] *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.*
[15] *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.*
[16] *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.*
[17] *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.*
[18] *Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.*
[19] *Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.*
[20] *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.*
[21] *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 Gültigkeit dieser QSEE-Bescheinigung ist bis zu 5 Jahre aufrecht oder bis zu einem zwischenzeitlichen Widerruf durch A-SIT. 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. Zur Aufrechterhaltung der Bescheinigung muss der Antragsteller alle zwei Jahre eine Schwachstellenanalyse durchführen und aufgetretene Schwachstellen zeitnah beheben. 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, nicht alle zwei Jahre eine Schwachstellenanalyse durchgeführt wird, identifizierte Schwachstellen nicht zeitnah behoben werden oder 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[22]. 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 unter Berücksichtigung der für die Betriebsumgebung identifizierten Risiken
- 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)

[22] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

(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[23] 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[24], 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 „Substanziell“ oder höher entsprechen[25].

(8) Es muss verhindert werden, dass benutzerseitige Komponenten, die Schwachstellen aufweisen oder ungeeignet für die Authentifizierung sind, für die Signaturauslösung verwendet werden können.

(9) Nur die unter Punkt 5. dieser Bescheinigung aufgelisteten kryptografischen Algorithmen, Parameter und Hash-Funktionen dürfen für die Erstellung qualifizierter elektronischer Signaturen oder qualifizierter elektronischer Siegel verwendet werden.

5. Algorithmen und zugehörige Parameter

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

- RSASSA[26]-PSS[27] nach PKCS#1 v2.2 (RFC 8017) mit Schlüssellängen von 3072 Bit
- ECDSA[28] nach FIPS PUB 186-4 mit den Kurven aus der NIST-Familie P-256, P-384 und P-521 gemäß FIPS 186-4 und Länge der Parameter p, q von 256-Bit, 384-Bit und 521-Bit.

verwendet.

Zur Berechnung der Hashwerte kommen die Hashfunktionen SHA-256, SHA-384 und SHA-512 zur Anwendung[29].

6. Prüfstufe und Mechanismenstärke

[23] FIPS – Federal Information Processing Standard

[24] Vgl. dazu „SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms”, Version 1.3, Februar 2023

[25] 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

[26] RSASSA – RSA (Rivest Shamir Adleman) Signature Scheme with Appendix

[27] PSS – Probabilistic Signature Scheme

[28] ECDSA – Elliptic Curve Digital Signature Algorithm

[29] 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.

Zu dem von der QSEE verwendeten Hardware Security Module vom Typ „Thales Luna Network HSM“[30] liegt das folgende von der US-Amerikanischen (National Institute of Standards and Technology) und Kanadischen (Communications Security Establishment) FIPS 140-2 Zertifizierungsstelle ausgestellte Zertifikat vor:

- Nr. 3205[31] ausgestellt am 25.06.2018, zuletzt erneuert am 29.04.2022 für Thales Luna K7 Cryptographic Module, für die von der QSEE unterstützte Firmware Version: 7.0.3, mit Boot-Loader Versionen 1.1.1, 1.1.2 und 1.1.4, Hardware Versionen: 808-000048-002, 808-000048-003, 808-000066-001, 808-000073-001 und 808-000073-002

Das Zertifikat weist dem Hardware Security Module eine erfolgreiche Evaluierung nach FIPS 140-2 nach[32,33].

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-24-035 dokumentiert.

Unterschrift:

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN	**Unterzeichner**	Herbert Leitold
	Datum/Zeit-UTC	2024-12-12T21:39:32+01:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at

DI Herbert Leitold, Gesamtleiter

[30] Hersteller: Thales (ehemals Gemalto bzw. SafeNet), 20 Colonnade Road, Suite 200, Ottawa, ON K2E 7M6, Kanada

[31] https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3205

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

[33] Der Status des Zertifikats Nr. 3205 wurde vom NIST auf *historical* geändert. Der Grund für die Umstufung hat jedoch keine negativen sicherheitstechnischen Auswirkungen auf die Verwendung des HSM als Teil dieser QSEE.