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) der A-Trust bestehend aus HSM und HSM Server, Version 2.1, Update 1

Antragsteller:
A-Trust GmbH
Landstraßer Hauptstraße 1b, E02
1030 Wien

Referenznummer A-SIT-VIG-23-096

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

1. Beschreibung der zu bescheinigenden Komponente

Teilkomponenten:

Die qualifizierte Signatur- bzw. Siegelerstellungseinheit (QSEE) besteht aus einem Rechner (HSM-Server), in dem sich ein Hardware Security Modul (HSM)[3] für die Durchführung der kryptografischen Operationen befindet. Dieser Rechner wird im Hochsicherheitsbereich der Rechenzentren der A-Trust in einem Safe betrieben. Zugang zu diesem Safe hat nur autorisiertes Sicherheitspersonal in der Rolle des Security Officer des qualifizierten Vertrauensdiensteanbieters (VDA) A-Trust.

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

Die Funktionalität der „qualifizierten Fernsignatur“[4] (Bereitstellung der zu signierenden Daten, Kontrolle über die Auslösung der Signaturfunktion) ist in einem Programm auf dem HSM-Server implementiert, welches die Funktionen des HSM zur Erzeugung der Signaturerstellungsdaten, zur Erstellung von qualifizierten elektronischen Signaturen und zur Entschlüsselung der gespeicherten Signaturerstellungsdaten nutzt.

Die Funktionalität der Siegelerstellung (Bereitstellung der zu besiegelnden Daten, Kontrolle über die Auslösung der Siegelfunktion, Erstellung des Siegels) läuft ebenfalls auf dem HSM-Server und nützt die Funktionen des HSM zur Erzeugung der Siegelerstellungsdaten, zur Erstellung von qualifizierten elektronischen Siegeln und zur Entschlüsselung der gespeicherten Siegelerstellungsdaten.

Erzeugung und Speicherung der Signaturerstellungsdaten:

Die Anmeldung für den Signaturerstellungsdienst erfolgt entweder direkt über den VDA oder mittels delegierter Authentifizierung bei vertrauenswürdigen Dritten – z.B.: Identity-Providern, Registration-Authorities. Zur Aktivierung einer „qualifizierten Fernsignatur“ müssen nach der Identifikation der Signatorin bzw. des Signators von dieser bzw. diesem ihre bzw. seine Mobilfunknummer oder der Benutzername angegeben und ein Signaturpasswort (Faktor „Wissen“) festgelegt werden. Der Faktor „Besitz“ wird mittels eines Einmalpasswortes, das über eine Verifikations-SMS[5] an die Mobilfunknummer übermittelt wird, überprüft. Die Überprüfung des Faktors „Besitz“ kann auch über eine App (sog. „TAN[6]-App“)[7] erfolgen, welche von der Signatorin bzw. dem Signator auf dem Mobiltelefon installiert werden muss. Die „TAN-App“ tauscht ein Einmalpasswort über eine sichere Verbindung mit dem A-Trust Rechenzentrum aus, bzw. ist – sofern das Mobiltelefon den Einsatz eines Secure Elements unterstützt – der Besitz auch durch den Zugriff auf einen Schlüssel, der im Secure Element abgelegt ist, nachweisbar. Dieser Zugriff ist nur der Signatorin bzw. dem Signator mittels einer auf dem Mobiltelefon eingestellten Authentifizierungsmethode Fingerprint, Gesichtserkennung oder Passwort- bzw. PIN[8]-Eingabe möglich. Eine weitere Möglichkeit zur Überprüfung des Faktors „Besitz“ ist die Verwendung geeigneter FIDO[9] Authentifizierungstoken[10], dabei wird der Besitz des verwendeten Tokens durch die Signatur über eine Challenge mit einem im Token sicher gespeicherten geheimen Schlüssel nachgewiesen.

Dann werden die Signaturerstellungsdaten im HSM generiert. Die Signaturerstellungsdaten werden durch einen nur im HSM verfügbaren Schlüssel und durch einen vom Signaturpasswort und der Mobilfunknummer bzw. Benutzername abgeleiteten Schlüssel verschlüsselt abgespeichert, wodurch die Anwendung der Signaturerstellungsdaten nur innerhalb des HSM und nach Eingabe des Signaturpassworts durch die Signatorin bzw. den Signator möglich ist. Es wird ein Zertifikatsrequest erzeugt und das qualifizierte Zertifikat wird durch einen qualifizierten VDA ausgestellt[11].

Sonderfall ID Austria[12] - Erzeugung und Speicherung der Signaturerstellungsdaten:

Die QSEE wird auch für die Aktivierung der Funktionalität für die qualifizierte Fernsignatur im Rahmen der ID Austria herangezogen. Die Anmeldung für den Signaturerstellungsdienst erfolgt

[4] Anmerkung: Vormals als „Handy-Signatur“ bezeichnet und nach der Umstellung der Handy-Signatur auf die ID Austria vom 5.12.2023 im Zuge dieser Bescheinigung durch A-Trust umbenannt.
[5] SMS – Short Messaging Service
[6] TAN – Transaktionsnummer
[7] Die verwendete App muss die Komponente „VDA-Library“ der A-Trust implementiert haben. Zum Zeitpunkt der Ausstellung dieser QSEE-Bescheinigung sind die Apps „A-Trust Signatur App“ der A-Trust und „Digitales Amt“ des Bundesministeriums für Finanzen verfügbar.
[8] PIN – Personal Identification Number
[9] FIDO – Fast Identity Online
[10] Geeignet sind Token mit mindestens FIDO Zertifizierungslevel L2, Key Protection „hardware“ und „user verification“
[11] Anmerkung: Die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser QSEE-Bescheinigung
[12] Anmerkung: Auch als E-ID (Elektronischer Identitätsnachweis) bezeichnet (entsprechend E-Government-Gesetz § 2 Z. 10).

ausschließlich über die Involvierung einer Behörde (z.B.: Passbehörde, Botschaften, Landespolizeidirektion), derzeit entweder mittels einer Vorregistrierung, der App „Digitales Amt“, SMS oder über POST-TAN.

Die eigentliche Generierung der Signaturerstellungsdaten im HSM und die anschließende Speicherung erfolgen analog dem herkömmlichen und oben beschriebenen Ablauf.

Erzeugung und Speicherung der Siegelerstellungsdaten:

Die Anmeldung für den Siegelerstellungsdienst erfolgt entweder direkt bei einem Portal des VDA oder mittels delegierter Authentifizierung bei vertrauenswürdigen Dritten – z.B.: Identity-Providern, Registration-Authorities. Für die Aktivierung generiert der Kunde bzw. die Kundin nach der Identifizierung einen Authentifizierungsschlüssel (RSA-Schlüssel mit einer Mindestschlüssellänge von 2048-Bit oder einen ECC-Schlüssel mit einer Mindestschlüssellänge von 256-Bit) und übermittelt den öffentlichen Teil des Authentifizierungsschlüssels (als PKCS#10) gemeinsam mit den Antragsdaten:

- Antragsteller[13] – Vorname, Nachname, Telefonnummer, E-Mail
- Vertretungsbefugter – Vorname, Nachname, Telefonnummer, E-Mail
- Organisation – Firmenname, Adresse, Firmenbuchnummer, Steuernummer

über eine TLS[14]-geschützte Webseite[15] an die A-Trust. Der Antrag wird vom Vertretungsbefugten elektronisch signiert.

Für die Aktivierung eines qualifizierten elektronischen Siegels mittels delegierter Authentifizierung bei vertrauenswürdigen Dritten ruft der Antragsteller bzw. die Antragstellerin eine TLS-geschützte Webseite auf und übermittelt die vom vertrauenswürdigen Dritten erhaltenen Identifizierungsdaten (in der Regel Benutzername und Passwort). In weiterer Folge wird ein Authentifizierungsschlüssel durch A-Trust generiert und das zugehörige Authentifizierungszertifikat ausgestellt.

Bei beiden Varianten werden im Anschluss die Siegelerstellungsdaten im HSM generiert und verschlüsselt in einer Datenbank gespeichert. Der für die Verschlüsselung verwendete Schlüssel ist im HSM nicht exportierbar gespeichert. In dieser Datenbank werden die Siegelerstellungsdaten dem zuvor ausgestellten Authentifizierungszertifikat zugeordnet. Für die den Siegelerstellungsdaten entsprechenden Siegelvalidierungsdaten wird ein Zertifikatsrequest erstellt und das resultierende qualifizierte Zertifikat der Siegelerstellerin bzw. dem Siegelersteller ausgestellt[16].

Aktivierung mit Signatur:

Die QSEE unterstützt mit Hilfe eines eigenen Kommandos die Auslösung von qualifizierten elektronischen Signaturen bereits im Aktivierungsprozess. Dabei wird der Signatorin bzw. dem Signator über die Anzeige bei der Signaturpassworteingabe und in der Verifikations-SMS deutlich gemacht, dass neben der Aktivierung (Ausstellung eines qualifizierten Zertifikats) auch eine Signatur über das bzw. die im Zuge des Prozesses übermittelte(n) Dokument(e) ausgelöst wird. Die Auslösung der qualifizierten elektronischen Signatur(en) über das bzw. die übermittelte(n) Dokument(e) erfolgt dann direkt nach der Zertifikatsausstellung, ohne dass eine weitere Authentifizierung der Signatorin bzw. des Signators durch Signaturpasswort und Einmalpasswort notwendig ist.

[13] Anmerkung: Gemeint sind in diesem Anwendungsfall die Antragstellerin bzw. der Antragsteller für das qualifizierte elektronische Siegel.
[14] TLS – Transport Layer Security
[15] Abrufbar unter: https://www.a-trust.at/Bestellungen/asignsealqualified/
[16] Anmerkung: Die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser Bescheinigung

Signaturerstellung:

Zum Auslösen einer qualifizierten elektronischen Signatur müssen von der Signatorin bzw. vom Signator zuerst Benutzername bzw. Mobilfunknummer sowie Signaturpasswort (Faktor „Wissen“) an einem Webportal eingegeben werden, worauf an die Mobilfunknummer eine SMS (sog. „SMS-TAN“) mit einem vom HSM generierten, zeitlich begrenzt gültigen Einmalpasswort und einem aus dem Hashwert der zu signierenden Daten erstellten Verifikationswert gesendet wird (Faktor „Besitz“).

Alternativ kann das Einmalpasswort auch mit der „TAN-App“ über eine gesicherte Verbindung ausgetauscht werden. Sofern das Mobiltelefon den Einsatz eines Secure Elements unterstützt, kann mithilfe der „TAN-App“ die Signaturvariante „One Device“ durchgeführt werden. Die Mobilfunknummer bzw. der Benutzername werden bei der ersten Verwendung hinterlegt. Zur Auslösung einer qualifizierten elektronischen Signatur wird das Signaturpasswort in der App abgefragt (Faktor „Wissen“) und die Signatorin bzw. der Signator muss mittels einer vom jeweiligen Smartphone unterstützten geeigneten Methode[17] nachweisen, dass sie bzw. er Zugriff auf den Schlüssel im Secure Element hat (Faktor „Besitz“). Diese Variante kann nur von registrierten Applikationen ausgelöst werden. Der Hashwert der zu signierenden Daten geht in die Prüfung des Faktors „Besitz“ ein, sodass der Verifikationsvorgang nur auf eine Signatur über diese Daten anwendbar ist. Bei der Authentifizierung mittels FIDO wird der Faktor „Besitz“ durch eine Assertion gemäß der FIDO WebAuthn Spezifikation nachgewiesen, dabei wird eine vom HSM-Server generierte Challenge mit einem sicher im Authentifizierungstoken gespeicherten geheimen Schlüssel signiert. Der Hashwert der zu signierenden Daten und die Challenge werden mit der WebAuthn Session verknüpft und gehen somit in die Prüfung des Faktors „Besitz“ ein. Nach erfolgreicher Prüfung des Faktors „Besitz“ (Einmalpasswort bzw. Zugriff auf Schlüssel im Secure Element oder FIDO Authentifizierungstoken) werden im HSM die Signaturerstellungsdaten entschlüsselt und eine qualifizierte elektronische Signatur erstellt.

Eine weitere alternative Art der Signaturauslösung wird mittels qualifizierter Signaturkarte unterstützt. Dabei handelt es sich um ein kombiniertes Authentifizierungsservice, wobei die beiden Faktoren Wissen und Besitz gemeinsam in einer Operation geprüft werden. Im Aktivierungsvorgang wird ein Schlüssel durch ein Kommando der QSEE auf der Signaturkarte generiert und dessen Public-Key mit einer bestehenden qualifizierten Fernsignatur sowie dem qualifizierten Zertifikat der Signaturkarte verknüpft. Anschließend können Signaturoperationen durchgeführt werden, indem eine Signatorin bzw. ein Signator eine qualifizierte Signatur mittels Signaturkarte erstellt. Diese Signatur wird vom HSM mit dem hinterlegten Public-Key überprüft und die eigentliche qualifizierte elektronische Signatur mit der verknüpften qualifizierten Fernsignatur erstellt.

Siegelerstellung:

Zum Auslösen eines qualifizierten elektronischen Siegels muss vom Siegelersteller bzw. von der Siegelerstellerin eine Anfrage – über eine TLS-geschützte Verbindung – an den A-Trust-Webserver gestellt werden. Diese Anfrage muss enthalten:

- Seal-Identifikation (Zertifikatsseriennummer des Authentifizierungszertifikats)
- zu besiegelnden Hashwert[18]
- Signatur des zu besiegelnden Hashwerts mittels Authentifizierungszertifikat
- den dabei verwendeten Signaturerstellungsmechanismus

Die Siegelerstellung ist nur dann durchführbar, wenn das korrespondierende Zertifikat zur Verwendung für elektronische Siegel ausgestellt wurde.

2. Erfüllung der Anforderungen der eIDAS-VO

[17] z.B.: Biometrie (Fingerprint, Gesichtserkennung etc.), Geräte-PIN, Geräte-Passwort
[18] Anmerkung: A-Trust überprüft diesen Hashwert auf eine Mindestlänge von 32 Byte.

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach Artikel 29 Abs. 1[19] eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1[20] eIDAS-VO,
- Anforderungen nach Anhang II eIDAS-VO (Abs. 1 lit. a[21],b[22],c[23],d[24], Abs. 2[25], Abs. 3[26], Abs. 4 lit a[27], b[28])

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

---

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

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

[21] *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.*

[22] *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.*

[23] *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.*

[24] *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.*

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

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

[27] *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.*

[28] *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.*

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[29]. 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 (Mobiltelefon, 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 autorisiertes, vertrauenswürdiges und geprüftes 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)
- Schutz gegen die Möglichkeit von Attacken beruhend auf kompromittierender elektromagnetischer Abstrahlung
- Schutz vor unautorisierten Änderungen an der Software und Konfiguration der QSEE
- Äquivalentes hohes Schutzniveau für alle Teilkomponenten (einschließlich für zu Sicherungszwecken verwendete Komponenten)

(4) Komponenten der Signatorin bzw. des Signators, die Schwachstellen oder ungeeignete Methoden zur Benutzer/innen-Authentifizierung aufweisen, dürfen bei der Signaturauslösung nicht verwendet werden können.

(5) Die HSMs müssen gemäß ihrer Common Criteria-Zertifizierung unter Einhaltung des 4-Augen-Prinzips initialisiert und betrieben werden.

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

(7) Sofern die Funktion *Aktivierung mit Signatur* verwendet wird, muss unmissverständlich sichergestellt werden, dass der Signatorin bzw. dem Signator bewusst ist, dass im Zuge der Aktivierung auch eine Signaturoperation durchgeführt wird.

5. Algorithmen und zugehörige Parameter

Zur Erstellung von qualifizierten elektronischen Signaturen bzw. qualifizierten elektronischen Siegeln wird von der QSEE der kryptografische Algorithmus

[29] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

- ECDSA[30] nach FIPS PUB 186-4 mit der Kurve P-256 und Länge der Parameter p, q von 256-Bit verwendet.

Zur Berechnung des Hashwertes wird der Algorithmus SHA[31]-256, SHA-384 bzw. SHA-512 nach ISO/IEC 10118-3.

6. Prüfstufe und Mechanismenstärke

Die QSEE unterstützt die folgenden beiden HSM-Typen:

- nCipher[32] nShield HSM-Familie v11.72.02
- Entrust nShield Solo XC HSM-Familie v12.60.15

Zu den verwendeten Hardware Security Modulen nCipher nShield F3 500e und nCipher nShield F3 6000+ (Modell-Nr.: nC4033E-500 und nC4433E-6K0, Firmware Version: 2.55.1 level 3) liegt das Common Criteria Zertifikat Nr. 1/16 vor, ausgestellt am 10.03.2016 von der italienischen Common Criteria Zertifizierungsstelle OCSI (Organismo di Certificazione della Sicurezza Informatica). Das Zertifikat weist den Hardware Security Modulen eine erfolgreiche Evaluierung nach Common Criteria Version 3.1, Evaluation Assurance Level EAL4+ (erweitert um AVA_VAN.5[33]) nach.

Zu den verwendeten Hardware Security Modulen nShield Solo XC F2, nShield Solo XC F3 und nShield Solo XC for nShield Connect XC (Modell-Nr.: nC3025E-000 rev 06, nC4035E-000 rev 06 und nC4335N-000 rev 06, Firmware Version: v12.60.15) liegt das Common Criteria Zertifikat CC-21-0368256 vor, ausgestellt am 17.03.2021 von TÜV Rheinland Nederland B.V. und gültig bis 17.03.2026. Das Zertifikat weist den Hardware Security Modulen eine erfolgreiche Evaluierung gemäß Common Criteria Version 3.1, Revision 5 auf Evaluation Assurance Level EAL4+ (erweitert um AVA_VAN.5 und ALC_FLR.2[34]) nach, sowie Konformität zum Schutzprofil CEN EN 419 221-5.

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-23-096 dokumentiert.

Unterschrift

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN	**Unterzeichner**	DI Herbert Leitold
	Datum/Zeit-UTC	2024-02-14T16:34:32+01:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at

DI Herbert Leitold, Gesamtleiter

[30] ECDSA – Elliptic Curve Digital Signature Algorithm
[31] SHA – Secure Hash Algorithm
[32] nCipher Security Limited (ein Entrust-Unternehmen) - One Station Square, Cambridge CB1 2GA, United Kingdom
[33] AVA_VAN.5 – Advanced methodical vulnerability analysis
[34] ALC_FLR.2 – Flaw reporting procedures