

# QSEE-BESCHEINIGUNG DER BESTÄTIGUNGSSTELLE GEM. § 7 ABS. 1 SVG<sup>1</sup> I/M ART. 30 ABS. 3 LIT. B EIDAS-VO<sup>2</sup>

## Qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) der A-Trust für die Handy-Signatur und Siegel bestehend aus HSM und HSM Server, Version 1.4

Antragsteller:

A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH  
Landstraßer Hauptstraße 1b, E02  
1030 Wien

**QSEE-Bescheinigung ausgestellt am: 22.07.2019**  
**Referenznummer A-SIT VIG-19-058**

### 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) vom Typ nShield 500e F3<sup>3</sup> für die Durchführung der kryptografischen Operationen befindet. Dieser Rechner wird im Hochsicherheitsbereich der Rechenzentren der A-Trust in einem Safe betrieben, zu dem nur autorisiertes Sicherheitspersonal des qualifizierten Vertrauensdiensteanbieters (VDA) A-Trust Zugriff hat.

Die Funktionalität der Handy-Signatur (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

<sup>1</sup> 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)

<sup>2</sup> 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

<sup>3</sup> Modell-Nr.: nC4033E-500, Firmware Version: 2.55.1 level 3 (das Modul wird im strikten FIPS 140-2 level 3 Modus betrieben). Hersteller: Thales e-Security Inc., 900 South Pine Island Road, Suite 710 Plantation, Florida, 33324, USA

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 „Handy-Signatur“ müssen nach der Identifikation der Signatorin bzw. des Signators von dieser bzw. diesem ihre bzw. seine Mobilfunknummer angegeben und ein Signaturpasswort (Faktor „Wissen“) festgelegt werden. Der Faktor „Besitz“ wird mittels eines Einmalpasswortes, das über eine Verifikations-SMS an die Mobilfunknummer übermittelt wird, überprüft. Die Überprüfung des Besitzes kann auch über eine App („Handy-Signatur App“) erfolgen, welche von der Signatorin bzw. dem Signator auf dem Mobiltelefon installiert werden muss. Die „Handy-Signatur App“ tauscht ein Einmalpasswort über eine sichere Verbindung mit dem A-Trust Rechenzentrum aus, bzw. kann – sofern das Mobiltelefon den Einsatz eines Secure Elements unterstützt – der Besitz auch durch den Zugriff auf einen Schlüssel im Secure Element nachgewiesen werden. Dieser Zugriff ist nur der Signatorin bzw. dem Signator mittels Fingerprint, Gesichtserkennung oder Passwort- bzw. PIN-Eingabe möglich.

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 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<sup>4</sup>.

#### 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<sup>5</sup> – Vorname, Nachname, Telefonnummer, E-Mail
- Vertretungsbefugter – Vorname, Nachname, Telefonnummer, E-Mail
- Organisation – Firmenname, Adresse, Firmenbuchnummer, Steuernummer

über eine TLS-geschützte Webseite<sup>6</sup> 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

---

<sup>4</sup> Anmerkung: Die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser QSEE-Bescheinigung

<sup>5</sup> Anmerkung: Gemeint ist in diesem Anwendungsfall die Antragstellerin bzw. der Antragsteller für das qualifizierte elektronische Siegel.

<sup>6</sup> Abrufbar unter: <https://www.a-trust.at/Bestellungen/asignsealqualified/>

(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<sup>7</sup>.

#### 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.

#### Signaturerstellung:

Zum Auslösen einer qualifizierten elektronischen Signatur müssen von der Signatorin bzw. vom Signator zuerst Mobilfunknummer und Signaturpasswort (Faktor „Wissen“) an einem Webportal eingegeben werden, worauf an die Mobilfunknummer eine SMS 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 „Handy-Signatur App“ über eine gesicherte Verbindung ausgetauscht werden. Sofern das Mobiltelefon den Einsatz eines Secure Elements unterstützt, kann mithilfe der „Handy-Signatur App“ die Signaturvariante „One Device“ durchgeführt werden. Die Mobilfunknummer wird 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 Fingerprint oder Gesichtserkennung<sup>8</sup> 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. Nach erfolgreicher Prüfung des Faktors „Besitz“ (Einmalpasswort bzw. Zugriff auf Schlüssel im Secure Element) werden im HSM die Signaturerstellungsdaten entschlüsselt und eine qualifizierte elektronische Signatur 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<sup>9</sup>
- Signatur des zu besiegelnden Hashwerts mittels Authentifizierungszertifikat
- den dabei verwendeten Signaturerstellungsmechanismus

<sup>7</sup> Anmerkung: Die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser Bescheinigung

<sup>8</sup> Anmerkung: Bei iOS-Smartphones ist als Fallback auch eine Aktivierung mit Eingabe der Smartphone-PIN bzw. des Smartphone-Passworts möglich.

<sup>9</sup> Anmerkung: A-Trust überprüft diesen Hashwert auf eine Mindestlänge von 32 Byte.

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

## 2. Erfüllung der Anforderungen der eIDAS-VO

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach Artikel 29 Abs. 1<sup>10</sup> eIDAS-VO,
- Anforderungen nach Artikel 39 Abs. 1<sup>11</sup> eIDAS-VO,
- Anforderungen nach Anhang II eIDAS-VO (Abs. 1 lit. a<sup>12</sup>, b<sup>13</sup>, c<sup>14</sup>, d<sup>15</sup>, Abs. 2<sup>16</sup>, Abs. 3<sup>17</sup>, Abs. 4 lit a<sup>18</sup>, b<sup>19</sup>)

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

---

<sup>10</sup> *Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des Anhangs II erfüllen.*

<sup>11</sup> *Artikel 29 gilt sinngemäß für die Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten.*

<sup>12</sup> *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.*

<sup>13</sup> *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.*

<sup>14</sup> *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.*

<sup>15</sup> *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.*

<sup>16</sup> *Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese Daten vor dem Unterzeichnen angezeigt werden.*

<sup>17</sup> *Das Erzeugen oder Verwalten von elektronischen Signaturerstellungsdaten im Namen eines Unterzeichners darf nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt werden.*

<sup>18</sup> *Unbeschadet des Absatzes 1 Buchstabe d dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich zu Sicherheitszwecken kopieren, sofern folgende Anforderungen erfüllt sind: a) Die kopierten Datensätze müssen das gleiche Sicherheitsniveau wie die Original-Datensätze aufweisen.*

<sup>19</sup> *Unbeschadet des Absatzes 1 Buchstabe d dürfen qualifizierte Vertrauensdiensteanbieter, die elektronische Signaturerstellungsdaten im Namen des Unterzeichners verwalten, die elektronischen Signaturerstellungsdaten ausschließlich zu Sicherheitszwecken kopieren, sofern folgende Anforderungen erfüllt sind: Es dürfen nicht mehr kopierte Datensätze vorhanden sein als zur Gewährleistung der Dienstleistungskontinuität unbedingt nötig.*

### 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 Evidenzhaltung 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 Autorisierungs-codes und die Integrität der zu signierenden 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<sup>20</sup>. Es ist sicherzustellen, dass die Benutzerinnen und Benutzer darüber informiert sind, dass im Zuge der Auslösung der Signatur oder des Siegels nur die vom qualifizierten Vertrauensdiensteanbieter als geeignet definierten Apps verwendet werden dürfen und die dabei 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, vertrauenswürdige und geprüfte 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) Das HSM muss unter Einhaltung des 4-Augen-Prinzips im FIPS 140-2 level 3 mode initialisiert werden.

---

<sup>20</sup> Entsprechend Erwägungsgrund 56 der eIDAS-VO.

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

- ECDSA 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-256 nach ISO/IEC 10118-3 verwendet<sup>21</sup>.

## 6. Prüfstufe und Mechanismenstärke

Zum verwendeten Hardware Security Modul nShield 500e F3 (Modell-Nr.: nC4033E-500, Firmware Version: 2.55.1 level 3) liegt das Common Criteria Zertifikat Nr. 1/16 vor, ausgestellt am 10.3.2016 von der italienischen Common Criteria Zertifizierungsstelle OCSI (Organismo di Certificazione della Sicurezza Informatica). Das Zertifikat weist dem Hardware Security Modul eine erfolgreiche Evaluierung nach Common Criteria Version 3.1, Evaluation Assurance Level EAL4+, erweitert um AVA\_VAN.5<sup>22</sup>, 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 Angriffen mit hohem Angriffspotenzial.

Die dieser QSEE-Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VIG-19-058 dokumentiert.

### Unterschrift:

A-SIT Zentrum für sichere Informationstechnologie – Austria  
Wien, (Datum siehe el. Signatur)

Prof. DI Dr. Reinhard Posch, Gesamtleiter

---

<sup>21</sup> Die Berechnung des Hashwertes erfolgt in der Systemumgebung der Signaturerstellungseinheit.

<sup>22</sup> AVA\_VAN.5 – Advanced methodical vulnerability analysis