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 Signaturerstellungseinheit (QSEE) der A-Trust für die Handy-Signatur bestehend aus HSM und HSM Server, Version 1.3

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

QSEE-Bescheinigung ausgestellt am: 03.07.2018
Referenznummer A-SIT-VIG-18-062

1. Beschreibung der zu bescheinigenden Komponente

Teilkomponenten:

Die Signaturerstellungseinheit besteht aus einem Rechner (HSM-Server), in dem sich ein Hardware Security Modul (HSM) vom Typ nShield 500e F3[3] befindet. Dieser Rechner wird im Hochsicherheitsbereich der Rechenzentren der A-Trust in einem Safe betrieben, zu dem nur Sicherheitspersonal der A-Trust Zugriff hat.
Die Funktionalität der Handy-Signatur (Bereitstellung der zu signierenden Daten, Kontrolle über die Auslösung der Signaturfunktion) ist in dem Programm HSMServerApplication.exe implementiert, welches auf dem HSM-Server läuft, und die Funktionen des HSM zur Erzeugung der Signaturerstellungsdaten, zur Erstellung von qualifizierten elektronischen Signaturen und zur Entschlüsselung der gespeicherten Signaturerstellungsdaten nutzt.

[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] 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

Erzeugung und Speicherung der Signaturerstellungsdaten:

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 Password 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[4].

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, Gesichtserkennung oder Password bzw. PIN-Eingabe 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.

[4] Anmerkung: Die Prozesse zur Identifikation, Registrierung und Zertifikatsausstellung sind nicht Gegenstand dieser QSEE-Bescheinigung

2. Erfüllung der Anforderungen der eIDAS-VO

Die QSEE erfüllt unter nachstehenden Einsatzbedingungen

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

Die QSEE ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung von Signaturerstellungsdaten,
- Komponenten und Verfahren zum Speichern von Signaturerstellungsdaten,
- Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten

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.

---

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

[6] *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.*

[7] *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.*

[8] *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.*

[9] *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.*

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

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

[12] *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.*

[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: 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 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 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[14]. Es ist sicherzustellen, dass die Benutzerinnen und Benutzer darüber informiert sind, dass im Zuge der Auslösung der Signatur 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, 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) Das HSM muss unter Einhaltung des 4-Augen-Prinzips im FIPS 140-2 level 3 mode initialisiert werden.

(5) Elektronische Signaturerstellungsdaten 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.

[14] Entsprechend Erwägungsgrund 56 der eIDAS-VO.

5. Algorithmen und zugehörige Parameter

Zur Erstellung von qualifizierten elektronischen Signaturen 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[15].

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 [Ref22] 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[16], 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 Angreifern mit hohem Angriffspotenzial.

Die dieser QSEE-Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VIG-18-062 dokumentiert.

Unterschrift:

A-SIT Zentrum für sichere Informationstechnologie – Austria

Wien, (Datum siehe el. Signatur)

SIGNATURINFORMATIONEN		
	Unterzeichner	Reinhard Posch
	Datum/Zeit-UTC	2018-07-03T13:24:05+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

[15] Die Berechnung des Hashwertes erfolgt in der Systemumgebung der Signaturerstellungseinheit.
[16] AVA_VAN.5 – Advanced methodical vulnerability analysis