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

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

A-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

BESCHEINIGUNG NACH § 18 ABS. 5 SIGG

Sichere Signaturerstellungseinheit der A-Trust für die Handy-Signatur bestehend aus HSM und HSM Server

Antragsteller:
A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 5
1030 Wien

Bescheinigung ausgestellt am: 14.12.2015
Referenznummer A-SIT-VI-15-050

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[1] befindet. Dieser Rechner wird im Hochsicherheitsbereich des Rechenzentrums 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.

Erzeugung und Speicherung der Signaturerstellungsdaten:

Nach der Identifikation der Signatorin bzw. des Signators müssen von dieser bzw. diesem ihre bzw. seine Mobilfunknummer angegeben und ein Signaturpasswort festgelegt werden. Der Besitz der Mobilfunknummer wird mittels eines Einmalpasswortes, das über eine Verifikations-SMS übermittelt wird, überprüft. Die Überprüfung des Besitzes kann auch über eine „Handy-Signatur App“ erfolgen, welche von der Signatorin bzw. dem Signator auf dem Mobiltelefon installiert werden muss und das Einmalpasswort über eine sichere Verbindung mit dem A-Trust Rechenzentrum austauscht.
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.

Signaturerstellung:

Zum Auslösen einer qualifizierten elektronischen Signatur müssen von der Signatorin bzw. vom Signator zuerst Mobilfunknummer und Signaturpasswort 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

[1] Modell-Nr.: nC4033E-500, Firmware Version: 2.38.4 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

erstellten Verifikationswert gesendet wird. Alternativ kann das Einmalpasswort auch mit der „Handy-Signatur App“ über eine gesicherte Verbindung ausgetauscht werden. Das Einmalpasswort ist über eine Signatur des HSM mit dem Hashwert der zu signierenden Daten verknüpft. Nach erfolgreicher Prüfung des Einmalpasswortes werden im HSM die Signaturerstellungsdaten entschlüsselt und eine qualifizierte elektronische Signatur erstellt.

2. Erfüllung der Anforderungen des SigG[2] und der SigV[3]

Die Signaturerstellungseinheit erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach § 18 Abs. 1[4] und § 18 Abs. 2 zweiter Satz[5] SigG,
- Anforderungen nach § 3 Abs. 1[6] und § 3 Abs. 2[7] SigV und
- Anforderungen nach § 6 Abs. 3[8] SigV.

Die Signaturerstellungseinheit ist daher in folgenden Kategorien bescheinigt:

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

3. Gültigkeitsdauer der Bescheinigung

Die Gültigkeit dieser Bescheinigung gilt bis auf Widerruf durch A-SIT. 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 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 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 Zertifizierungsdiensteanbieters entsprechend § 12 SigV sicherzustellen,
- in der Belehrung der Signatorin bzw. des Signators 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 Signatorin bzw. vom Signator zur

[2] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19.August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 75/2010 vom 18. August 2010.

[3] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008)) in der Fassung BGBl. II Nr. 401/2010 vom 9. Dezember 2010.

[4] Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verlässlich verhindern

[5] Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muss sichergestellt sein.

[6] Die technischen Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten müssen in Hinblick auf das Erfordernis der Prüfung nach § 18 Abs. 5 SigG den Anforderungen des § 6 entsprechen.

[7] Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

[8] Wenn technische Komponenten und Verfahren in einer kontrollierten Umgebung eingesetzt werden, können Sicherheitsanforderungen, die nach Abs. 1 technisch sichergestellt werden müssen, auch organisatorisch durch Einsatz qualifizierten und vertrauenswürdigen Personals oder technischorganisatorisch durch Einsatz geeigneter Zugriffs- und Zutrittskontrollmaßnahmen erfüllt werden. Die Erfüllung dieser Sicherheitsanforderungen ist durch eine Bestätigungsstelle zu prüfen.

Signaturerstellungseinheit im Zuge des Auslösevorgangs sind in der Systemumgebung der Signaturerstellungseinheit (§ 4 SigV) sicherzustellen und daher nicht Teil der Bescheinigung[9]. Es ist sicherzustellen, dass die Signatorinnen und Signatoren darüber informiert sind, dass ihre im Zuge der Auslösung der Signatur verwendeten Komponenten (Mobilfunkgerät, Webbrowser) geeignet abgesichert[10] sein müssen.

(2) Die Einhaltung der vom Betreiber der Signaturerstellungseinheit entsprechend § 6 Abs. 3[8] SigV getroffenen Sicherheitsmaßnahmen ist einer regelmäßigen Überprüfung zu unterziehen.

5. Algorithmen und zugehörige Parameter

Zur Erstellung einer qualifizierten elektronischen Signatur wird von der Signaturerstellungseinheit der ECDSA[11] Algorithmus nach ANSI X9.62-2005 bereitgestellt. Es wird die in FIPS PUB 186-3 definierte Kurve P-256 mit Länge der Parameter p, q von 256 Bit verwendet.

Zur Berechnung des Hashwertes wird der Algorithmus SHA-256 nach ISO/IEC 10118-3 verwendet[12].

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV[13] erfüllt.

6. Prüfstufe und Mechanismenstärke

Zum verwendeten Hardware Security Modul nShield 500e F3 (Modell-Nr.: nC4033E-500, Firmware Version: 2.38.4 level 3) liegt das Zertifikat Nr. 1197 vor, ausgestellt am 6.10.2009 von der US-Amerikanischen (National Institute of Standards and Technology) und Kanadischen (Communications Security Establishment) FIPS 140-2 Zertifizierungsstelle. Das Zertifikat weist dem Hardware Security Modul eine erfolgreiche Evaluierung nach FIPS 140-2 level 3 nach.

Da keine Zertifizierung nach einem Schutzprofil, das als Referenznummer im Amtsblatt der Europäischen Gemeinschaften nach Art. 3 Abs. 5 der Signaturrichtlinie 1999/93/EG für sichere Signaturerstellungseinheiten (Secure Signature-Creation Devices – SSCD) veröffentlicht wurde vorliegt, wurde die Erfüllung der organisatorischen und technischorganisatorischen Sicherheitsanforderungen gemäß § 6 Abs. 3[8] SigV von der Bestätigungsstelle überprüft.

Die dieser Bescheinigung zu Grunde liegenden Prüfungsergebnisse sind im Prüfbericht unter der Referenznummer A-SIT-VI-15-050 dokumentiert.

Unterschrift:

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2015-12-14T17:20:50+01:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	

[9] Entsprechend Anzeigesoftware, Kartenleser, PIN-Eingabe bei der Verwendung von Signaturkarten.
[10] D.h. die Komponenten müssen insbesondere frei von Viren und anderer Schadsoftware sein.
[11] DSA basierend auf einer Gruppe $E(F_p)$
[12] Die Berechnung des Hashwertes erfolgt in der Systemumgebung der Signaturerstellungseinheit.
[13] Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.