



## 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](mailto:office@a-sit.at)  
ZVR: 948166612

DVR: 1035461

UID: ATU60778947

# BESTÄTIGUNG DER BESTÄTIGUNGSSTELLE GEM SIGG UND SIGV

## Signaturerstellungseinheit des ZDA

### Hardware Security Module Baltimore Sureware Keyper Version 2, Release 1

Antragsteller:

A-Trust Gesellschaft für Sicherheitssysteme im el. Datenverkehr GmbH  
Landstraßer Hauptstraße 5  
1030 Wien

**Bestätigung ausgestellt am: 21.12.2011**  
**Referenznummer A-SIT-1.094**

### 1. Beschreibung der zu bestätigenden Komponente

Die Komponente „Baltimore Sureware Keyper Version 2 Release 1“ (nachstehend HSM genannt) ist ein Sicherheitsmodul bestehend aus Firmware und Hardware wie folgt:

- Firmware:
  - Application Boot Loader, Version 9, Revision 4;
  - Loader, Version 3, Revision 3; und
  - Host Security Module Server, Version 2, Revision 7.
- Hardware:
  - SureWare Keyper Professional, Baltimore part number 9620, Version 2 Release 1.

Der Hersteller ist Baltimore Technologies Ltd<sup>1</sup>, Innovation House, Mark Road, Hemel Hempstead, Hertfordshires HP2 7DN, United Kingdom.

Das HSM ist ein spezieller Rechner („Multi-Chip Embedded“), der kryptographische Funktionen einem HSM-Host-Rechner zur Verfügung stellt (z.B. Schlüsselgenerierung, Signaturerstellung, Authentifizierung in Form von Message Authentication Code). Die Verbindung zwischen dem HSM-Host und dem HSM wird über ein LAN (d.h. Ethernet) hergestellt. Das HSM verfügt über Schnittstellen für Import/Export von kryptographischen Schlüsseln über Chipkarten in Form von Token. Die Programmierschnittstelle basiert auf PKCS #11<sup>2</sup>. Die vom HSM zur Verfügung gestellten kryptographischen Funktionen werden vom HSM-Host aus verwendet, auf dem ein geeigneter HSM-Treiber installiert ist. Auf dem HSM gibt es keine ID-basierte Zugriffskontrolle auf kryptographische Funktionen.

Das HSM besteht aus folgenden Teilen:

- einer Einheit im Metallgehäuse mit separater Stromversorgung,

<sup>1</sup> mittlerweile AEP Networks, Focus 31 West Wing, Cleveland Road, Hemel Hempstead, Herts, HP2 7BW, United Kingdom

<sup>2</sup> Public-Key Cryptography Standard #11: Cryptographic Token Interface Standard

- einer kleinen faltbaren Tastatur (Keypad) für Eingabe von PINs und Konfigurationsdaten,
  - einem Chipkartenleser,
  - einem Schloss für einen physischen Schlüssel und
- einem kleinen hintergrundbeleuchteten Display.

## 2. Erfüllung der Anforderungen des SigG<sup>3</sup> und der SigV<sup>4</sup>

Das HSM erfüllt unter nachstehenden Einsatzbedingungen die in den jeweiligen Fußnoten angeführten

- Anforderungen nach § 18 Abs. 3<sup>5</sup> SigG,
- Anforderungen nach § 5 Abs. 1<sup>6</sup> SigV und
- Anforderungen nach § 6 Abs. 1<sup>7</sup> SigV.

Das HSM kann somit bei Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate anbieten, in folgenden Kategorien eingesetzt werden:

- Komponenten und Verfahren zur Erzeugung von Signaturerstellungsdaten des Zertifizierungsdiensteanbieters,
- Komponenten und Verfahren zur Speicherung der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters und
- Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters.

## 3. Gültigkeitsdauer der Bestätigung

Diese Bestätigung ist für die Dauer von zwei Jahren ab Datum der Ausstellung gültig.

Die Gültigkeit dieser Bestätigung ist an die Erfüllung der Einsatzbedingungen gebunden, sie endet jedenfalls, wenn zumindest eines der zugrunde liegenden IT-Sicherheitszertifikate

- FIPS 140-1 Level 4 Zertifikat<sup>8</sup> No. 146
- Certification Report<sup>9</sup> No. 160 (ITSEC) gemäß UK IT Security Evaluation and Certification Scheme

seine Gültigkeit verliert.

## 4. Einsatzbedingungen

Folgende Einsatzbedingungen müssen beim Einsatz des HSM bei den Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate anbieten, erfüllt werden:

- (1) Bei der ersten Initialisierung des HSM beim Zertifizierungsdiensteanbieter („Controlled Initialisation“) muss ein neuer SMK (Storage Master Key) erzeugt werden und die Option

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> Bei der Erstellung und Speicherung von qualifizierten Zertifikaten sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung und Verfälschung von Zertifikaten verhindern.

<sup>6</sup> Bei der Ausstellung qualifizierter Zertifikate müssen die vom ZDA verwendeten Signaturerstellungsdaten in einer nach § 6 geprüften Signaturerstellungseinheit erzeugt sein und dürfen außerhalb dieser nicht zur Verfügung stehen. Die verwendeten Algorithmen und Parameter müssen dem Anhang entsprechen.

<sup>7</sup> Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Es können insbesondere Schutzprofile (Protection Profiles) herangezogen werden, die nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Security Evaluation – ISO/IEC 15408)“ oder nach den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (Information Technology Security Evaluation Criteria – ITSEC)“ erstellt wurden. Das Gleiche gilt für die Prüfung von vertrauenswürdigen Systemen, Produkten und Verfahren, die für die Erstellung von qualifizierten Zertifikaten, für die Speicherung von Signaturerstellungsdaten für qualifizierte Zertifikate oder für qualifizierte Zeitstempeldienste eingesetzt werden.

<sup>8</sup> Abgerufen unter <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt146.pdf> am 20.12.2011

<sup>9</sup> Abgerufen unter [http://www.cesg.gov.uk/products\\_services/iacs/cc\\_and\\_itsec/media/certreps/cr160.pdf](http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/certreps/cr160.pdf) am 20.12.2011

KeyExport anschließend auf „disabled“ gesetzt werden. Diese Vorgänge müssen nach dem Vier-Augen-Prinzip kontrolliert und protokolliert werden.

- (2) Die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters müssen im HSM erzeugt werden.
- (3) Physische und logische (inkl. Netzwerk-) Zugriffe auf das HSM und auf den HSM-Host dürfen nur berechtigten Personen und Prozessen gestattet werden.
- (4) Da es auf dem HSM keine ID-basierte Zugriffskontrolle auf kryptographische Funktionen gibt, muss die Zugriffskontrolle auf die Schlüsselerzeugungsfunktion und Signaturerstellungsfunktion durch geeignete technische Maßnahmen auf dem HSM-Host realisiert werden, so dass nur berechnete Personen und Prozesse auf diese Funktionen zugreifen können.
- (5) Die HSM-Host-Anwendung muss geeignete Mechanismen implementieren, die unautorisierte Änderungen der Daten bei der Übertragung zum HSM/vom HSM erkennen lassen.
- (6) Bei der Entsorgung eines HSM müssen die Signaturschlüssel nachweislich vernichtet werden. Das HSM muss auf eine sichere Weise entsorgt werden, so dass keine Informationen über den Signaturschlüssel ausgelesen werden können.
- (7) Alle Annahmen aus Abschnitt 3.5.1 des Dokumentes „010387 ITSEC Security Target, Version 3.3“, von Baltimore Technologies Ltd., müssen nachweislich erfüllt werden.

## 5. Algorithmen und zugehörige Parameter

Folgende Algorithmen werden vom HSM zur Erstellung von elektronischen Signaturen bereitgestellt:

- RSA-Algorithmus (entspricht SigV Anhang, Tabelle 4, Kennzahl 1.01) mit einer Schlüssellänge von 2048 Bit<sup>10</sup>
- SHA-1 Algorithmus (entspricht SigV Anhang, Tabelle 2, Kennzahl 2.01)
- Paddingverfahren gemäß EMSA-PKCS1-v1\_5 (entspricht SigV, Anhang, Tabelle 3, Kennzahl 3.01)

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV<sup>11</sup> erfüllt.

## 6. Prüfstufe und Mechanismenstärke

Es liegt das FIPS 140-1 Level 4 Zertifikat No. 146 für die „Advanced Configurable Crypto Environment (ACCE) SV and BE (Firmware Version v2.1, Hardware Version 2640-G3, „When operated in the FIPS mode““ vor, ausgestellt im April 2001 durch das U.S.-amerikanische National Institute of Standards and Technology. Die AACE wird in der SureWare Keyper-Produktfamilie verwendet. Im Rahmen dieser Evaluierung wurden die kryptographischen Mechanismen, die Widerstandsfähigkeit gegen Manipulieren (Tamper-Resistance) und der Zufallsgenerator geprüft.


Es liegt der Certification Report No. 160 nach dem UK IT Security Evaluation and Certification Schema für den „SureWare Keyper Professional Version 2 Release 1“ vor, ausgestellt durch „Certification Body, PO Box 152, Cheltenham, Glos GL52 5UF, United Kingdom“. Die zuständige Zertifizierungsstelle ist verwaltet durch die CESG (Communications-Electronics Security Group) und das Department of Trade and Industry. Die zuständige Prüfstelle war IBM Global Services CLEF (Commercial Evaluation Facility). Der Evaluationsgegenstand (HSM) erfüllt die Anforderungen der Vertrauenswürdigkeitsstufe E3 nach ITSEC. Die Zertifizierungsstelle war Zeuge des erfolgreichen Testens der RSA-Implementierung beim


<sup>10</sup> Da das RSA-Signaturschlüsselpaar des Zertifizierungsdiensteanbieters im HSM erzeugt werden muss, wird bei dieser Schlüssellänge das Chinese Remainder Theorem (CRT) verwendet; Angabe geprüft für „Baltimore SureWare PKCS#11 Adaptor“.

<sup>11</sup> 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.

Hersteller. Die Vertrauenswürdigkeit der RSA-Implementierung wurde im Rahmen dieser Evaluierung nicht geprüft.

### Unterschriften:

<b>Signaturwert</b>	TZ7G6Ht.05UdDg20cSVg48F30g1MX3SX81Q6F4UP5wZOhMzZ0RSP+WY5HikKe49z1CMvjfD YvvLlfg02d4r5CRg==	
	<b>Unterzeichner</b>	Prof. Reinhard Posch
	<b>Aussteller-Zertifikat</b>	CN=a-sign-premium-mobile-03,OU=a-sign-premium-mobile-03,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	<b>Serien-Nr.</b>	448413
	<b>Methode</b>	urn:pdfsigfilter:bka.gv.at:binaer:vl.1.0
	<b>Parameter</b>	etsi-bka-atrust-1.0:ecdsa-sha256:sha256:sha256:sha1
<b>Prüfinformation</b>	Signaturprüfung unter: <a href="http://www.signaturpruefung.gv.at">http://www.signaturpruefung.gv.at</a>	
<b>Datum/Zeit-UTC</b>	2011-12-21T19:53:11Z	

<b>Signaturwert</b>	68yokD+lcm1kbLlRYzRPF4cusSNxoRcIwVPf1ExNrVbq1g6FZC6SMTS/8FO0kJB3IuY69k s7bqy9MyWUnk6PmA==	
	<b>Unterzeichner</b>	Manfred Holzbach, gf. Vorstand
	<b>Aussteller-Zertifikat</b>	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	<b>Serien-Nr.</b>	523847
	<b>Methode</b>	urn:pdfsigfilter:bka.gv.at:binaer:vl.1.0
	<b>Parameter</b>	etsi-moc-1.1@9d9753ac
<b>Prüfinformation</b>	Signaturprüfung: <a href="http://www.signaturpruefung.gv.at">http://www.signaturpruefung.gv.at</a>	
<b>Datum/Zeit-UTC</b>	2011-12-22T11:45:58Z	