



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

A-1040 Wien, Weyringergasse 35
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

Homepage: www.a-sit.at
E-Mail: office@a-sit.at

Bestätigung für Hardware Security Module **Baltimore SureWare Keyper Professional** **Version 2 Release 1**

Antragsteller:

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

1. Beschreibung der bestätigten 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., Innovation House, Mark Road, Hemel Hempstead, Herts 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. 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,
- einer kleinen faltbaren Tastatur (Keypad) für Eingabe von PINs und Konfigurationsdaten,
- einem Chipkartenleser,
- einem Schloss für einen physischen Schlüssel und
- einem kleinen Display.

2. Erfüllung der gesetzlichen Anforderungen

Hiermit wird bestätigt, dass das HSM folgende Anforderungen erfüllt:

- Anforderungen nach Artikel 2 Pkt. 2 Lit. c und Lit. d der EU-RL („fortgeschrittene elektronische Signatur“) und
- Anforderungen nach Anhang 2f der EU-RL (Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate anbieten).

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

- Komponenten und Verfahren zur Erzeugung und Speicherung von Signaturerstellungsdaten des Zertifizierungsdiensteanbieters,
- Komponenten und Verfahren zur Erzeugung des Hashwertes aus dem Dokument,
- Komponenten und Verfahren zur sicheren Verwahrung der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters und
- Komponenten und Verfahren zur Anwendung der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters.

Erklärung

Die EU-RL ist die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

„Fortgeschrittene elektronische Signatur“ ist eine Signatur, die unter anderem folgende Anforderungen erfüllt (Artikel 2 Pkt. 2 Lit. c und Lit. d der EU-RL):

- Sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;
- sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Die relevante Anforderung an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate anbieten, ist wie folgt (Anhang 2f der EU-RL):

- Zertifizierungsdiensteanbieter müssen vertrauenswürdige Systeme und Produkte einsetzen, die vor Veränderungen geschützt sind und die die technische und kryptographische Sicherheit der von ihnen unterstützten Verfahren gewährleisten.

3. Gültigkeitsdauer der Bestätigung

Diese Bestätigung ist bis 31.12.2005 gültig. Die Gültigkeit dieser Bestätigung ist an die Erfüllung der Einsatzbedingungen gebunden.

4. Einsatzbedingungen

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

- Bei der ersten Initialisierung des HSM beim Zertifizierungsdiensteanbieter („Controlled Initialisation“) muss ein neuer SMK (Storage Master Key) erzeugt werden und die Option KeyExport anschließend auf „disabled“ gesetzt werden. Diese Vorgänge müssen nach dem Vier-Augen-Prinzip kontrolliert und protokolliert werden.
- Die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters müssen im HSM erzeugt werden.
- Physische und logische (inkl. Netzwerk-) Zugriffe auf das HSM und auf den HSM-Host dürfen nur berechtigten Personen und Prozessen gestattet werden.

- 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.
- Die HSM-Host-Anwendung muss geeignete Mechanismen implementieren, die unautorisierte Änderungen der Daten bei der Übertragung zum HSM/vom HSM erkennen lassen.
- 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.
- Bei der Erstellung qualifizierter Zertifikate und relevanter Sperr- und Widerruflisten muss der zu signierende kryptographische Hashwert dieser Daten auf dem HSM berechnet werden.
- 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

Zur Erstellung einer fortgeschrittenen elektronischen Signatur wird vom HSM der RSA-Algorithmus mit einer Schlüssellänge von 2048 Bit bereitgestellt. Da das RSA-Signaturschlüsselpaar des Zertifizierungsdiensteanbieters im HSM erzeugt werden muss, wird bei dieser Schlüssellänge das Chinese Remainder Theorem (CRT) verwendet.¹

Zur Berechnung des Hashwertes bei der Erstellung einer fortgeschrittenen elektronischen Signatur wird vom HSM der SHA-1 Algorithmus bereitgestellt. Der Hashwert wird gemäß EMSA-PKCS1-v1_5 auf die Signaturblocklänge verlängert („Padding“).

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 (z.B. SHA-1), 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 für den „SureWare Keyper Professional Version 2 Release 1“ vor, ausgestellt durch das Certification Body, PO Box 152, Cheltenham, Glos GL52 5UF, United Kingdom. Die zuständige Zertifizierungsstelle ist verwaltet durch die CESA (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 Hersteller. Die Vertrauenswürdigkeit der RSA-Implementierung wurde im Rahmen dieser Evaluierung nicht geprüft.

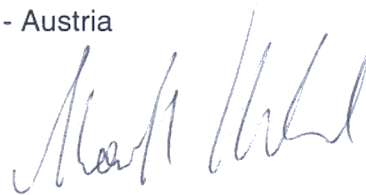
¹ Angabe geprüft für Baltimore SureWare PKCS#11 Adaptor

Wien, 23.01.2002

A-SIT Zentrum für sichere Informationstechnologie - Austria



o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch
Wissenschaftlicher Gesamtleiter



Manfred Holzbach
Geschäftsführender Vorstand