



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

<http://www.a-sit.at>
E-Mail: office@a-sit.at

BESTÄTIGUNG
DER BESTÄTIGUNGSSTELLE GEM SIGG¹ UND SIGV²

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

| | |
|---------------------------------------|--|
| Projektnummer | A-SIT 1.059 |
| Auftraggeber | A-Trust Gesellschaft für Sicherheitssysteme im el. Datenverkehr GmbH Landstraßer Hauptstraße 5 1030 Wien |
| Ansprechperson | Friedrich Hirschbügl, Romana Stangl |
| Antrag gestellt am | 01.10.2005 |
| Typenbezeichnung | Hardware Security Module „Baltimore Sureware Keyper Version 2 Release 1“, Hersteller Baltimore plc |
| Bestätigung ausgestellt am | 22.12.2005 |

¹ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 152/2001 vom 21. Dezember 2001.

² Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV, BGBl. II Nr. 30/2000 vom 2. Februar 2000) in der Fassung BGBl. II Nr. 527/2004 vom 30. Dezember 2004.

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 plc ³, 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 #11⁴. 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 hintergrundbeleuchteten Display.

2. Erfüllung der Anforderungen des SigG⁵ und der SigV⁶

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

- Anforderungen nach §18(3)⁷ SigG,
- Anforderungen nach §5(1)⁸ SigV und
- Anforderungen nach §9(1)⁹ SigV.

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

³ Früher Baltimore Technologies Ltd.

⁴ Public-Key Cryptography Standard #11: Cryptographic Token Interface Standard

⁵ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 152/2001 vom 21. Dezember 2001.

⁶ Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV, BGBl. II Nr. 30/2000 vom 2. Februar 2000) in der Fassung BGBl. II Nr. 527/2004 vom 30. Dezember 2004.

⁷ „Bei der Erstellung und Speicherung von qualifizierten Zertifikaten sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung und Verfälschung von Zertifikaten verhindern.“

⁸ „Signaturerstellungsdienste, die Zertifizierungsdiensteanbieter bei der Ausstellung qualifizierter Zertifikate verwenden, müssen in einer nach § 9 geprüften Signaturerstellungseinheit erzeugt sein. Sie dürfen außerhalb dieser Signaturerstellungseinheit nicht zur Verfügung stehen. Die verwendeten Algorithmen und Parameter müssen dem Anhang entsprechen.“

⁹ „Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Hierbei 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 Signaturerstellungsdiensten für qualifizierte Zertifikate oder für sichere Zeitstempeldienste 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.

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 Zertifikat¹⁰ No. 146
- Certification Report¹¹ No. 160 (ITSEC) gemäß UK IT Security Evaluation and Certification Schema

seine Gültigkeit verliert.

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 Widerrufslisten 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

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 Bit¹²
- 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)

¹⁰ Abgerufen unter <http://csrc.nist.gov/cryptval/140-1/140crt/140crt146.pdf>, am 19.12.2005

¹¹ Abgerufen unter <http://www.cesg.gov.uk/site/iacs/itsec/media/certreps/cr160.pdf>, am 19.12.2005

¹² 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“.

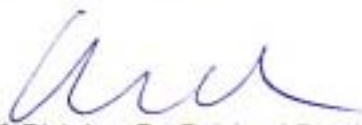
6. Prüfstufe und Mechanismenstärke

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

Wien, 22.12.2005

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand