



## 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](http://www.a-sit.at)  
E-Mail: [office@a-sit.at](mailto:office@a-sit.at)

### **Bestätigung**

für PC Card

### **Chrysalis-ITS® Luna® CA<sup>3</sup> Firmware Version 3.9**

Antragsteller:

Chrysalis ITS, Inc.  
One Chrysalis Way

Ottawa, Ontario, Canada, K2G 6P9

## **1. Beschreibung der bestätigten Komponente**

Die Komponente „Chrysalis-ITS® Luna® CA<sup>3</sup> Firmware Version 3.9“ (nachstehend Token genannt) ist eine Type II PC Card bestehend aus Firmware und Hardware.

Der Hersteller ist der Antragsteller.

Der Token ist eine spezielle PC-Karte („Multi-Chip Standalone Module“), die kryptographische Funktionen einem Host-Rechner zur Verfügung stellt. Die verfügbaren Funktionen sind Benutzeridentifikation und –authentifikation, Zugriffskontrolle, Datenschutz, Datenverschlüsselung, Message-Digest, elektronische Signatur, Verwaltung von kryptographischen Parametern und sicherer Backup (Sicherung) von kritischen kryptographischen Parametern.

Die Verbindung zwischen dem Host und dem Token wird über einen speziellen Kartenleser hergestellt. Die Programmierschnittstelle basiert auf PKCS #11. Die vom Token zur Verfügung gestellten kryptographischen Funktionen werden vom Host aus verwendet, auf dem ein geeigneter Treiber installiert ist.

Für eine sichere Anwendung des Tokens sind folgende Systemteile notwendig, die kein Gegenstand dieser Bestätigung sind:

- Chrysalis-ITS® dual-slot Luna® Dock PC Card Reader: ein spezieller Kartenleser mit zwei Schlitzen;
- Luna® Pin Entry Device (PED): ein PIN-Eingabegerät mit Tastatur, das eine gesicherte Verbindung (Trusted Path) zwischen dem PED und dem Token herstellt;
- PED Keys (Datakey® Device): serielle Speichergeräte für die Speicherung kritischer kryptographischer Parameter durch das PED;
- Enabler (Product Configuration) Software: eine Benutzerschnittstelle zum Konfigurieren und Testen; und
- Cryptographic API Software: eine kryptographische PKCS#11 Schnittstelle für die Host-Anwendung (Windows DLL oder Unix-type SO Programmibliothek).

## 2. Erfüllung der gesetzlichen Anforderungen

Hiermit wird bestätigt, dass der Token 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).

Der Token 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 Tokens bei den Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate anbieten, erfüllt werden:

- Für eine sichere Anwendung des Tokens sind die Systemteile aus Kapitel 1 dieser Bestätigung notwendig.
- Im Fixed Policy Vector (FPV) darf das Bit FPV\_ENABLE\_CLONING nicht gesetzt werden. Alle anderen FIPS 140-1 relevanten FPV-Bits müssen wie bei der FIPS 140-1 evaluierten Version von Luna CA<sup>3</sup> V3.9 gesetzt werden. Die Konfiguration des FPV muss vor der Inbetriebnahme des Tokens vom ZDA kontrolliert und nach dem Vieraugen-Prinzip protokolliert werden.

- Der Token Policy Vector muss vor der Inbetriebnahme des Tokens wie in Tabelle 1 gezeigt konfiguriert werden. Dieser Vorgang muss nach dem Vieraugen-Prinzip protokolliert werden.
- Für die Authentifizierung des Security Officers und aller Token Users muss zusätzlich zum PED Key eine mindestens 6-stellige PED PIN verlangt werden.
- Die M-von-N-Aktivierung (*M of N Activation*) muss sowohl für den Security Officer als auch für alle Token User verwendet werden, wobei  $M \geq 2$  und  $N \geq M$ .
- Der Token muss vor der ersten RSA-Schlüsselgenerierung und danach vor jeder zweiten Schlüsselgenerierung aus einem externen und für diesen Einsatzzweck evaluierten HRNG<sup>1</sup> mit neuem zufälligen Seed initialisiert werden. Dieser Vorgang muss unter Kontrolle des ZDA sein. Aus der HRNG-Evaluation hat insbesondere hervorzugehen, dass durch den Umstand „extern“ und durch die Art der Übertragung des Zufalls keine Minderung der Schlüsselqualität entsteht.
- Bei der Erstellung qualifizierter Zertifikate und relevanter Sperr- und Widerrufslisten muss der zu signierende kryptographische Hashwert dieser Daten im Token berechnet werden.
- Wenn die Signaturerstellungsdaten eines Tokens nicht mehr verwendet werden sollen, müssen sie gelöscht werden. Ein zu entsorgender Token muss physisch zerstört oder sicher aufbewahrt werden. Der Token darf nicht mehr für Zertifizierungsdienste (qualifizierte Zertifikate) verwendet werden.
- Physische und logische (inkl. Netzwerk-) Zugriffe auf den Token und auf den Host dürfen nur berechtigten Personen und Prozessen gestattet werden.
- Alle Zugriffe vom Host auf die Signaturfunktion des Tokens müssen protokolliert werden.
- Der Token darf nur in einem Raum verwendet werden, in dem keine Gefahr besteht, dass elektromagnetische Emanationen des Tokens von unberechtigten Personen empfangen werden oder dass durch starke elektromagnetische Strahlungen das korrekte Funktionieren des Tokens durch unberechtigte Personen gestört oder die Daten auf dem Token durch unberechtigte Personen modifiziert werden.
- Firmware-Updates (inkl. Patches, d.h. wenn sich die Versionsnummer der Firmware nicht ändert) sind nicht erlaubt.
- Bis spätestens 01.04.2003 muss ein unabhängiger Nachweis der Korrektheit der RSA-Implementierung für Luna CA<sup>3</sup> Version 3.9 vorgelegt werden. Ein solcher Nachweis für Luna CA<sup>3</sup> Version 3.97, der im Rahmen der derzeit laufenden Common Criteria-Evaluierung erstellt werden sollte, kann auch akzeptiert werden.

Token Policy Vector Bit	Wert
TPV_USER_ZEROIZE	1
TPV_USER_FW_UPDATE	0
TPV_M_OF_N_ACTIVATION	<b>1</b>
TPV_KEY_ATTRIB_LOCK	1
TPV_KEY_SINGLE_FUNCTION	0
TPV_SIGNING_KEY_LOCAL	<b>1</b>
TPV_DISABLE_CLONING_BY_USER	<b>1</b>

Tabelle 1: Konfiguration des Token Policy Vector für Luna CA<sup>3</sup> (**fett** gedruckte Werte sind unterschiedlich von den Default-Werten für die FIPS 140-1 evaluierte Version von Luna CA<sup>3</sup> V3.9)

## 5. Algorithmen und zugehörige Parameter

Zur Erstellung einer fortgeschrittenen elektronischen Signatur wird vom Token der RSA-Algorithmus mit einer Schlüssellänge von 2048 Bit bereitgestellt. Das Chinese Remainder Theorem (CRT) wird verwendet.

Zur Berechnung des Hashwertes bei der Erstellung einer fortgeschrittenen elektronischen Signatur wird vom Token der SHA-1 Algorithmus bereitgestellt. Der Hashwert wird gemäß PKCS #1 Block Type 01 v1\_5 auf die Signaturblocklänge verlängert („Padding“).

<sup>1</sup> Hardware Random Number Generator

## 6. Prüfstufe und Mechanismenstärke

Es liegt das FIPS 140-1 Level 3 Zertifikat No. 58 für Luna CA<sup>3</sup> (Firmware-Versionen 3.2, 3.9 und 3.93) „For services provided by the listed FIPS-approved algorithms, and Triple DES“ vor, ausgestellt durch das U.S.-amerikanische National Institute of Standards and Technology (NIST). Das Zertifikat wurde ursprünglich für Luna CA<sup>3</sup> Firmware-Version 3.2 im August 1999 ausgestellt und 2001 für Firmware-Versionen 3.9 und 3.93 auf Antrag des Evaluators<sup>2</sup> aktualisiert. Das Zertifikat bestätigt die Evaluationsstufe „Level 3“ für das Krypto-Modul-Design, Rollen und Dienste, physische Sicherheit, EMI/EMC<sup>3</sup>, Schlüsselverwaltung, Token-Schnittstellen, Finite State Machine-Model, SW-Sicherheit und Self-Tests.

Das FIPS 140-1 Zertifikat No. 58 gilt u.a. für SHA-1 und RSA. RSA ist nur als „vendor affirmed“ im Zertifikat bezeichnet, da NIST über keine genehmigten („approved“) Testsätze für RSA verfügt. Die derzeit laufende Common Criteria-Evaluierung gemäß EAL4<sup>4</sup> wird voraussichtlich auch einen Nachweis der Korrektheit der RSA-Implementierung liefern. Die zuständige Zertifizierungsstelle ist Communication Security Establishment<sup>5</sup> (Canadian Common Criteria Scheme). Der Hersteller hat bestätigt, dass es zwischen Luna CA<sup>3</sup> V3.9 und V3.97 keine Unterschiede auf dem HW-Architektur-Level gibt und dass die Unterschiede in der Funktions- und Schnittstellen-Spezifikation sowie in den verfügbaren Konfigurationsoptionen für die bestätigte Sicherheitsfunktionalität nicht relevant sind.

Wien, 20.03.2002

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach  
Geschäftsführender Vorstand

<sup>2</sup> DOMUS IT Security Laboratory, 2220 Walkley Road, Ottawa, Ontario, Canada, K1G 5L2

<sup>3</sup> Electromagnetic Interference/Electromagnetic Compatibility

<sup>4</sup> SoF high for the authentication mechanisms and random number generation mechanism

<sup>5</sup> <http://www.cse-cst.gc.ca>