



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

Bescheinigung nach §18(5) SigG:

Sicherheitsmodul mit CP/Q++
von *IBM Corporation*
mit

Hardware: P/N 04K9036, EC CF75600M
Firmware: Miniboot 0 Version A, Miniboot 1 Version A
Kontrollprogramm CP/Q++ 2.41

Antragsteller:
Rundfunk und Telekom Regulierungs-GmbH
Mariahilferstraße 77-79
1060 Wien

1. Beschreibung der bescheinigten Komponente¹

Die bescheinigte Komponente (nachstehend Sicherheitsmodul genannt) ist eine Einschubkarte und besteht aus folgenden Teilen:

- Hardware:
 - P/N² 04K9036 und EC³ CF75600M.
- Firmware:
 - Miniboot 0 Version A, und
 - Miniboot 1 Version A.
- Software:
 - Kontrollprogramm CP/Q++ 2.41, und
 - 4758 Common Cryptographic Architecture (CCA) Support Version 2.41.

Die bescheinigte Funktionalität ist wie folgt :

- Initialisierung (Setup);
- Rollen- und Benutzerverwaltung;
- RSA-Schlüsselgenerierung;
- RSA-Schlüsselverwaltung;
- Schutz der RSA-Schlüssel;
- Anwendung von RSA-Schlüsseln und kryptographischen Hash-Funktionen für Erzeugung elektronischer Signaturen.

¹ Diese Bescheinigung stellt eine Verlängerung der Bescheinigung für die Komponente „IBM 4758-023 PCI Cryptographic Coprocessor mit Miniboot 0 und Miniboot 1 V2.41 und CP/Q++ V2.41 und Common Cryptographic Architecture V2.41“ vom 17.09.2002 dar.

² Security Module Part Number

³ Engineering Change Number

2. Erfüllung der Anforderungen des SigG und der SigV

Der Sicherheitsmodul erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach §18(1) SigG⁴,
- Anforderungen nach §18(2) SigG⁵,
- Anforderungen nach §3(3) SigV⁶,
- Anforderungen nach §3(4) SigV⁷,
- Anforderungen nach §3(5) SigV⁸,
- Anforderungen nach §4(1) SigV⁹,
- Anforderungen nach §7(3) SigV¹⁰,
- Anforderungen nach §9(2) SigV¹¹,
- Anforderungen gemäß Anhang 1 Punkt 2 SigV¹², und
- Anforderungen gemäß Anhang 2 Punkt 2 SigV¹³.

Der Sicherheitsmodul ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung und Speicherung von Signaturerstellungsdaten,
- Komponenten und Verfahren zum Erzeugen des Hashwertes aus dem Dokument,
- Komponenten und Verfahren zur Verwahrung der Signaturerstellungsdaten und zur Sicherstellung des autorisierten Zuganges und
- Komponenten und Verfahren zur Anwendung der Signaturerstellungsdaten.

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist ein Jahr nach der Ausstellung gültig. Die Bescheinigung endet jedenfalls, sofern die derzeit laufende Evaluierung bzw. Zertifizierung gemäß Common Criteria EAL4+ der bescheinigten Komponente mit einem negativen Ergebnis endet.

⁴ Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer 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 Signaturerstellungsdaten für sichere elektronische Signaturen der Signatoren müssen die im Anhang 1 Punkt 2. festgesetzte Mindestlänge aufweisen. (...) Die verwendeten Algorithmen müssen offengelegt sein. Die Signaturerstellungsdaten für sichere elektronische Signaturen dürfen mit an Sicherheit grenzender Wahrscheinlichkeit ausschließlich beim Signator vorkommen. Sie müssen nach dem jeweiligen Stand der Technik den eindeutigen Rückschluss auf den Signator ermöglichen. Die wiederholte Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen darf nicht dazu führen, dass sich die Schlüsselqualität unter das für das jeweilige Signaturverfahren maßgebliche Sicherheitsniveau vermindert.

⁷ Wiederholte Anwendungen der Signaturerstellungsdaten für sichere elektronische Signaturen dürfen nicht zu einer Verminderung der Schlüsselqualität führen (...).

⁸ Die Erzeugung der Signaturerstellungsdaten für sichere elektronische Signaturen muss auf einer tatsächlichen Zufälligkeit beruhen, der ein technischer Zufall oder ein Signator-bezogener Zufall zu Grunde liegt. Die Signaturerstellungsdaten müssen in der im Anhang 1 Punkt 3. festgelegten Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein (qualitätsvoller Zufall). Die Zufallselemente müssen auf ihre Eignung hin ausreichend geprüft sein. Pseudozufallszahlen dürfen nicht als Ausgangsbasis verwendet werden (...).

⁹ Die Speicherung der Signaturerstellungsdaten für sichere elektronische Signaturen hat so zu erfolgen, dass deren Bekanntwerden ausgeschlossen ist und ihre Verwendung unter der ausschließlichen Kontrolle des Signators steht. Das Duplizieren von Signaturerstellungsdaten nach deren Erzeugung ist nicht zulässig.

¹⁰ Die Signaturfunktion in der Signaturerstellungseinheit des Signators darf nur nach Verwendung von Autorisierungs-codes (z.B. PIN-Eingabe, Fingerabdruck) auslösbar sein. (...) Das unbefugte Erfahren der Autorisierungs-codes muss durch dessen Gestaltung und durch wirksame Sperrmechanismen praktisch ausgeschlossen sein. Derselbe Autorisierungscode darf nicht für unterschiedliche Anwendungen (z.B. Signatur- und Bankomatfunktion) verwendbar sein. Signaturerstellungseinheiten, die mehrere Anwendungen zulassen, wie z.B. Multiapplikationskarten oder Multiapplikationsterminals, dürfen nur verwendet werden, wenn die Maßnahmen und Methoden, die das Auslösen unterschiedlicher Anwendungen mit denselben Autorisierungs-codes verhindern, im Sicherheitskonzept beschrieben sind. (...).

¹¹ Die Prüfung der technischen Komponenten und Verfahren nach § 7 Abs. 2, § 10 und § 18 SigG kann auch (...), soweit anwendbar auch nach den Security Requirements for Cryptographic Modules (FIPS 140-1, level 2) (...), erfolgen.

¹² Die Schlüssellänge der Signaturerstellungsdaten für sichere elektronische Signaturen muss zumindest betragen: (...) - beim Verfahren RSA 1023 Bit (...). Führende Nullbit sind in die Schlüssellänge nicht einzurechnen. Die Schlüssellänge ist jedenfalls für den geheimen Teil der Signaturerstellungsdaten maßgeblich.

¹³ Folgende Hashverfahren werden als sicher anerkannt (...) b) Funktion SHA-1. Diese Hashverfahren sind bis 31.12.2005 für den Einsatz bei elektronischen Signaturen als sicher anzusehen. (...)

4. Einsatzbedingungen

- (1) Der Sicherheitsmodul ist ausschließlich zur Verwendung als Signaturerstellungseinheit in einer gesicherten Umgebung bescheinigt. Geeignete Zutritts- und Zugriffskontrollmaßnahmen zum Sicherheitsmodul und zum Host-Rechner müssen dokumentiert werden.
- (2) Das Auslösen der Signaturfunktion auf dem Sicherheitsmodul darf ohne Eingabe des Autorisierungscode nicht möglich sein.
- (3) Die Anzahl der Signaturen, die mit einer Autorisierung des Signators gegenüber dem Sicherheitsmodul ausgelöst wird, muss dem Signator bekannt gegeben werden. Sichere Signaturen dürfen nicht automatisch (z.B. durch den Aufruf eines Programms auf dem Host-Rechner und ohne willentliche Aktion des Signators) erstellt werden.
- (4) Durch geeignete und dokumentierte Maßnahmen muss das Nachladen böswilligen Codes verhindert werden.
- (5) Die wesentlichen Konfigurationsumstände und die organisatorischen Sicherheitsmaßnahmen sind in einem Audit (Setup Audit) unter Bezug auf die Signaturstellungsdaten und relevante Operationen zu dokumentieren. Sämtliche Veränderungen in diesem Zusammenhang bedürfen eines neuen Audits.
- (6) Der Sicherheitsmodul muss so konfiguriert sein, dass nach dem Setup (Initialisierung) keine Änderung der Rollen und ihrer Berechtigungen (d.h. bis zum nächsten Setup) erlaubt ist.
- (7) Falls der Sicherheitsmodul so konfiguriert ist, dass nach dem Setup (Initialisierung) weitere Erzeugung der Signaturstellungsdaten für sichere Signaturen erlaubt ist, muss durch geeignete Maßnahmen sichergestellt werden, dass die Sicherheit der Signaturfunktion des Sicherheitsmoduls nicht vermindert ist. Diese Maßnahmen und ihre Wirksamkeit müssen dokumentiert werden.
- (8) Am Ende des Lebenszyklus (Entsorgung) müssen dem Sicherheitsmodul die Batterien entnommen werden, um alle darauf gespeicherten Schlüssel zu zerstören. Der Sicherheitsmodul muss danach sicher aufbewahrt werden.
- (9) Der Sicherheitsmodul muss so konfiguriert sein, dass sichere Signaturstellungsdaten weder ausgelesen noch auf einen anderen Sicherheitsmodul kopiert werden können.
- (10) Durch geeignete und dokumentierte Maßnahmen muss sichergestellt werden, dass der Autorisierungscode für die Auslösung der Signaturfunktion auf dem Sicherheitsmodul für unterschiedliche Anwendungen nicht verwendbar ist.
- (11) Falls der Sicherheitsmodul so konfiguriert ist, dass andere Rollen bzw. Berechtigungen als Operational Default¹⁴, Auditor¹⁵ oder Signer¹⁶ in der operationalen Phase (d.h. nach dem Setup) erlaubt sind, muss durch geeignete Maßnahmen sichergestellt werden, dass die Sicherheit der Signaturfunktion des Sicherheitsmoduls nicht vermindert ist. Diese Maßnahmen und ihre Wirksamkeit müssen dokumentiert werden.
- (12) Eine geeignete Prozedur muss eingerichtet und dokumentiert werden, die sicherstellt, dass der technische Zufall in vollem Umfang in die Schlüsselerzeugung eingeht und dass dieser Zufall in keinen anderen Schlüsseln verwendet wird.
- (13) Das unbefugte Erfahren der Autorisierungscode muss durch deren Gestaltung und durch wirksame Sperrmechanismen praktisch ausgeschlossen sein.

5. Algorithmen und zugehörige Parameter

Zur Erstellung sicherer elektronischer Signaturen wird der RSA-Algorithmus mit einer Schlüssellänge von 1024 bis 2048 Bit bereitgestellt. Die RSA-Implementierung verwendet das Chinese Remainder Theorem ab einer RSA-Schlüssellänge über 1024 Bit. Zur Berechnung kryptographischer Hashwerte für sichere elektronische Signaturen wird das

¹⁴ Keine Authentifizierung erforderlich; erlaubte Operationen: Hashwertberechnung, Lesen von nicht-vertraulichen Zugriffskontrollinformationen.

¹⁵ Mit Authentifizierung; erlaubte Operationen: Re-initialisierung des Sicherheitsmoduls, Lesen von nicht-vertraulichen Zugriffskontrollinformationen, Lesen von „retained RSA keys labels“. „Retained RSA keys“ sind die RSA-Privatschlüssel, die im Sicherheitsmodul gespeichert sind und nicht ausgelesen werden können.

¹⁶ Mit Authentifizierung; erlaubte Operationen: Signaturerstellung mit „retained RSA keys“, Hashwertberechnung, Lesen von nicht-vertraulichen Zugriffskontrollinformationen, Lesen von „retained RSA keys labels“.

Verfahren SHA-1 bereitgestellt. Dadurch sind die Anforderungen gemäß Anhang 1 Punkt 2 SigV und gemäß Anhang 2 Punkt 2 SigV erfüllt.

6. Prüfstufe und Mechanismenstärke

Segmente 0 und 1 (Hardware, Firmware):

Es liegt die Information über die Ausstellung des Zertifikats #117 für „IBM 4758-023 PCI Cryptographic Coprocessor (Miniboot Layers 0 und 1¹⁷)“ vor¹⁸. Das Zertifikat wurde durch das U.S.-amerikanische *National Institute of Standards and Technology* in 2000 ausgestellt. Das Zertifikat weist der Komponente die Evaluationsstufe „Level 3“ nach FIPS PUB 140-1 aus.

Segmente 1 und 2 (Firmware, Kontrollprogramm):

Es liegt das „FIPS 140-1 Certificate No. 346 for the Cryptographic Module *Security Module with CP/Q++ by IBM Corporation (When operated in FIPS mode; Hardware: P/N 04K9036, EC CF75600M, Firmware: Miniboot 0 Version A, Miniboot 1 Version A, CP/Q++ 2.41)*“ vor¹⁹ [1039_02]. Das Zertifikat weist der Komponente die Evaluationsstufe „Level 3“ nach FIPS PUB 140-1 aus. Das Zertifikat wurde durch das U.S.-amerikanische *National Institute of Standards and Technology* am 25.09.2003 ausgestellt.

Segment 3:

Es liegt eine informelle Stellungnahme des Evaluators (Tele-Consulting GmbH, Deutschland) über den Evaluationsstatus für „IBM 4785 PCI Cryptographic Coprocessor“ (inkl. CP/Q++ und Common Cryptographic Architecture 2.41) nach den Common Criteria (Evaluationsstufe EAL4+, SoF high) vom 01.09.2003 vor. Dem Evaluator liegen keine Erkenntnisse über Sicherheitsprobleme vor.

Wien, 25.09.2003

A-SIT Zentrum für sichere Informationstechnologie – Austria



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



Manfred Holzbach
Geschäftsführender Vorstand

¹⁷ ID: PN 04K9036, EC C75600M, Miniboot 0 version A, Miniboot 1 version A

¹⁸ <http://csrc.ncsl.nist.gov/cryptval/140-1/1401val2000.htm>

¹⁹ <http://csrc.ncsl.nist.gov/cryptval/140-1/1401val2003.htm>