Bestätigung
für technische Komponenten
gemäß § 14 (4) Gesetz zur digitalen Signatur und §§ 16 und 17 Signaturverordnung

debis Systemhaus Information Security Services GmbH
- Zertifizierungsstelle debisZERT -

Rabinstraße 8
53111 Bonn

bestätigt hiermit gemäß §14 Abs. 4 Signaturgesetz[1] und §17 Abs. 3 Signaturverordnung[2], daß

STARCOS SPK2.3 with Digital Signature Application StarCert
(unlimited signature generation configuration)

den nachfolgend beschriebenen Anforderungen des Artikels 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Gesetz zur digitalen Signatur) vom 01. August 1997 bzw. der Signaturverordnung vom 01. November 1997 entsprechen und bei sachgemäßen Einsatz im Wirkungsbereich der genannten Rechtsvorschriften eingesetzt werden können.

Die Dokumentation zu dieser Bestätigung ist unter

debisZERT.02037.TE.03.2001

registriert.

Bonn, den 06.04.2001 **gez. Dr. Heinrich Kersten**
Zertifizierungsstelle

debis Systemhaus Information Security Services GmbH – Zertifizierungsstelle - ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für technische Komponenten gemäß § 14 Abs. 4 des Gesetzes zur digitalen Signatur ermächtigt.

---

1 Gesetz zur digitalen Signatur (Signaturgesetz – SigG) vom 22.07.1997 (BGBl. I., S. 1870, 1872)
2 Verordnung zur digitalen Signatur (Signaturverordnung – SigV) vom 08.10.1997 (BGBl. I., S. 2498 ff.)

Die Bestätigung zur Registrierungsnummer debisZERT.02037.TE.03.2001 besteht aus 8 Seiten.

Beschreibung der technischen Komponente:

1 Handelsbezeichnung der technischen Komponente und Lieferumfang

Gegenstand dieser Bestätigung ist die technische Komponente

- STARCOS SPK2.3 with Digital Signature Application StarCert
  (unlimited signature generation configuration)

Auslieferung:

- Prozessorchipkarte (Prozessor P8WE5032V0G)
  mit Betriebssystem STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration)

- Benutzerhandbuch für Trust Center

Hersteller:

- Giesecke & Devrient GmbH
  Prinzregentenstraße 159, D-81607 München

2 Funktionsbeschreibung

Die Komponente ist eine Prozessorchipkarte mit Betriebssystem und Signaturanwendung.

STARCOS ist ein komplettes Betriebssystem für Prozessorchipkarten (integrated circuit card, ICC). STARCOS steuert den Datenaustausch und die Speicherbereiche und verarbeitet Informationen im ICC. Als Ressourcenmanager stellt STARCOS die notwendigen Funktionen für Operation und Management einer jeden Anwendung bereit. STARCOS SPK2.3 ist eine Weiterentwicklung von STARCOS S2.1, die die gesamte Funktionalität von STARCOS S2.1 beinhaltet und die für asymmetrische Kryptographie benötigten Funktionen hinzufügt.

STARCOS SPK2.3 implementiert den symmetrischen Verschlüsselungsalgorithmus DEA (Data Encryption Algorithm) und seine Spezialform Triple-DES, sowie die asymmetrischen Krypto-algorithmen RSA und DSA. Die Algorithmen RSA und DSA können benutzt werden, um digitale Signaturen zu erzeugen. Das benutzte Padding-Verfahren entspricht PKCS 1.0 Version 1.5 und ISO/IEC 9796-2. STARCOS SPK2.3 unterstützt die gegenseitige Geräteauthentisierung und secure messaging gemäß ISO/IEC 7816-4.

In Verbindung mit der Signaturanwendung StarCert (Digital Signature Application StarCert) ermöglicht STARCOS SPK2.3 die Erzeugung und Prüfung digitaler Signaturen.

Der ICC kann als multifunktionale Chipkarte benutzt werden. In diesem Fall können andere Anwendungen während der Phase der operationellen Nutzung in den ICC geladen werden.

STARCOS SPK2.3 mit der Anwendung zur digitalen Signatur StarCert stellt Sicherheitsfunktionen zur Verfügung, die insbesondere die Authentisierung, die sichere Datenspeicherung (insbesondere von Signaturschlüsseln und Identifikationsdaten), die Sicherung der Kommunikation zwischen einer (externen) Anwendung und STARCOS SPK2.3 sowie kryptographische Funktionen zur Berechnung digitaler Signaturen und zur Verschlüsselung von Daten umfassen.

STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) kann ein bis maximal zehn Schlüsselpaare generieren und speichern. Die Schlüsselgenerierung basiert auf einem physikalischen Zufallszahlengenerator, dessen Zufallsfolgen softwaretechnisch bearbeitet werden. Anschließend werden die Primfaktoren ausgewählt, mit denen schließlich die RSA-Parameter berechnet werden. Diese Schlüsselgenerierung in drei Schritten erfüllt die gesetzlichen Anforderungen.

Die Verwendung dieser Schlüsselpaare zu anderen Zwecken als zur Erzeugung oder Prüfung digitaler Signaturen ist nicht Gegenstand dieser Sicherheitsbestätigung.

STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) unterstützt die gegenseitige Geräteauthentisierung und secure messaging.

Diese beiden Funktionalitäten sind nicht Gegenstand dieser Sicherheitsbestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllung der Anforderungen

Die Anforderungen an die hier betrachtete Komponente ergeben sich aus § 16 Abs. 1 und Abs. 2 Sätze 1, 2, 4 und 5 der Signaturverordnung:

„Die zur Erzeugung von Signaturschlüsseln erforderlichen technischen Komponenten müssen so beschaffen sein, daß ein Schlüssel mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommt und aus dem öffentlichen Schlüssel nicht der private Schlüssel errechnet werden kann. Die Geheimhaltung des privaten Schlüssels muß gewährleistet sein und er darf nicht dupliziert werden können. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.“

„Die zur Erzeugung oder Prüfung digitaler Signaturen erforderlichen technischen Komponenten müssen so beschaffen sein, daß aus der Signatur nicht der private Signaturschlüssel errechnet oder die Signatur auf andere Weise gefälscht werden kann.“

„Der private Signaturschlüssel darf erst nach Identifikation des Inhabers durch Besitz und Wissen angewendet werden können und bei der Anwendung nicht preisgegeben werden.“

„Die zum Erfassen von Identifikationsdaten erforderlichen technischen Komponenten müssen so beschaffen sein, daß sie die Identifikationsdaten nicht preisgeben und diese nur auf dem Datenträger mit dem privaten Signaturschlüssel gespeichert werden."

„Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden."

Diese Anforderungen werden durch STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) unter den angegeben Einsatzbedingungen erfüllt.

3.2 Einsatzbedingungen

3.2.1 Technische Einsatzumgebung

Die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) wird vor dem Beginn der Phase der operationellen Nutzung in die Prozessorchipkarte mit dem Prozessor P8WE5032V0G der Firma Philips Semiconductors Hamburg eingebracht. Dieser Prozeß endet mit der Initialisierung. Die bis zum Ende der Initialisierungsphase einzuhaltenden technischen und organisatorischen Sicherheitsbestimmungen sind dokumentiert und liegen dem Chiphersteller vor.

Während der Erstpersonalisierung werden die den späteren Signaturschlüsselinhaber (hier: die Zertifizierungsstelle) charakterisierenden Daten in die technische Komponente eingebracht. Wurde bisher kein Signaturschlüsselpaar erzeugt, so wird dies ebenfalls getan. Dabei wird die Erzeugung vollständig von der Prozessorchipkarte selbst vorgenommen. Das Problem der Erzeugung und Speicherung des privaten Signaturschlüssels in einer externen Komponente entsteht daher nicht.

Am Ende der Erstpersonalisierung ist die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) für die Zertifizierungsstelle (Trust Center) nutzbar.

Die Auslieferung der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) an einen Signaturschlüsselinhaber, der nicht Zertifizierungsstelle ist, ist aus Sicherheitsgründen bedenklich.

Diese Sicherheitsbestätigung gilt in einem solchen Fall ausdrücklich nicht.

An die zu verwendende Prozessorchipkarte bestehen folgende Anforderungen:

1. Die Prozessorchipkarte schützt die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) vor Veränderungen.

2. Die Prozessorchipkarte schützt die in der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) gespeicherten privaten Signaturschlüssel und den Authentisierungsschlüssel SK.ICC.AUT vor dem Verlust der Vertraulichkeit durch physikalische Angriffe.

3. Die Prozessorchipkarte implementiert Sicherheitsmechanismen, um den unerwünschten Informationsfluß durch Beobachtung physikalischer Größen bei der Anwendung des privaten Signaturschlüssels zu verhindern oder ausreichend zu reduzieren.

4. Die Prozessorchipkarte implementiert Sicherheitsmechanismen, um potentielle Sicherheitsverletzungen durch Betrieb außerhalb der zulässigen Grenzen der Taktfrequenz, der Versorgungsspannung oder der Temperatur zu erkennen. Wenn eine potentielle Sicherheitsverletzung erkannt ist, wird ein Reset der Prozessorchipkarte durchgeführt.

Die Prozessorchipkarte mit der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) verfügt nicht über eine benutzerlesbare Schnittstelle. Sie muss daher zusammen mit einem geeigneten IT-System und einem geeigneten Chipkartenlesegerät benutzt werden. Chipkartenleser und IT-System können in einem Gerät integriert sein.

An das Chipkartenlesegerät bestehen folgende Anforderungen:

1. Das Chipkartenlesegerät sendet nur solche Mitteilungen oder Hashwerte an die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) für die die Zertifizierungsstelle eine digitale Signatur generieren möchte. Derartige Mitteilungen oder Hashwerte werden vom Chipkartenlesegerät nicht verändert.

2. Das Chipkartenlesegerät enthält Sicherheitseinrichtungen, die die Vertraulichkeit der von der Zertifizierungsstelle als ihre Identifikationsdaten angegebenen Daten gewährleisten.

3. Das Chipkartenlesegerät nimmt alle Mitteilungen der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) entgegen und reicht diese unverändert an den Computer weiter. Soweit das Chipkartenlesegerät eine Interpretation der Mitteilungen vornimmt, ist diese korrekt.

Die dieser Bestätigung zugrunde liegende Prüfung der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) ist in Verbindung mit dem Prozessor P8WE5032V0G der Firma Philips Semiconductors Hamburg durchgeführt worden. Für diesen Secure 8-bit Smart Card Controller liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-ITSEC-0158-2001 vor.

Diese Bestätigung ist nur mit dem Prozessor P8WE5032V0G der Firma Philips Semiconductors Hamburg und die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) gültig.

Bevor eine Sicherheitsbestätigung für die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) in Verbindung mit einem anderen Prozessorchip ausgestellt werden kann, ist eine Reevaluierung notwendig.

3.2.2 Organisatorische Einsatzumgebung und sachgemäßer Einsatz

Die Prozessorchipkarte (Prozessor P8WE5032V0G) mit Betriebssystem STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) wird an die

Zertifizierungsstelle durch die Wurzelzertifizierungsstelle (hier: die zuständige Behörde im Sinne des § 3, SigG) ausgegeben. Die Abholung der oben genannten Prozessorchipkarten beim Hersteller erfolgt durch die Zertifizierungsstelle.

Anforderungen bei Abholung durch die Zertifizierungsstelle

Für Prozessorchipkarten (Prozessor P8WE5032V0G) mit Betriebssystem STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration), die beim Hersteller durch die Zertifizierungsstelle abgeholt wurden, bestehen folgende Anforderungen:

1. Die Zertifizierungsstelle hat Verbleib und Verwendung der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) von der direkten Abholung beim Hersteller bis zum Einsatz in der Produktion und die Art und Weise der Überprüfung der Tatsache, dass an dieser technischen Komponente keine sicherheitstechnischen Veränderungen vorgenommen worden sind, in ihrem Sicherheitskonzept zu beschreiben.

2. Die Erzeugung von Signaturschlüsselpaaren hat unter Aufsicht der Wurzelzertifizierungsstelle zu erfolgen.

3. Zum Abschluß der Erstpersonalisierung muss das Paßwort des Herstellers (PIN.GD.PERS) dauerhaft gesperrt werden.

4. In der Zeit nach der Erzeugung eines Signaturschlüsselpaares muss sich die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) solange im Gewahrsam der Wurzelzertifizierungsstelle befinden, bis das Signaturschlüsselzertifikat der Wurzelzertifizierungsstelle über den öffentlichen Schlüssel in die technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) eingebracht wurde. Es ist zulässig, mehrere Signaturschlüsselpaare unmittelbar nacheinander zu erzeugen.

An den Signaturschlüsselinhaber (hier: die Zertifizierungsstelle) bestehen folgende Anforderungen:

1. Der Signaturschlüsselinhaber muss die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) so benutzen und aufbewahren, dass Mißbrauch und Manipulation vorgebeugt wird.

2. Der Signaturschlüsselinhaber hat sicherzustellen, dass ihm die öffentlichen Signatur- oder Authentisierungsschlüssel der Wurzelzertifizierungsstelle und ihre Zertifikate sowie das Zertifikat der Wurzelzertifizierungsstelle über den öffentlichen Signaturschlüssel des Signaturschlüsselinhabers authentisch übergeben werden.

3. Der Signaturschlüsselinhaber benutzt die Signaturerzeugungsfunktion nur für solche Daten, deren Integrität oder Authentizität er sicherstellen will.

4. Der Signaturschlüsselinhaber hält seine Identifikationsdaten für die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) (PIN und PUK) vertraulich.

5. Der Signaturschlüsselinhaber ändert seine Identifikationsdaten (PIN) für die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) in regelmäßigen Abständen.

6. Vor Benutzung eines Chipkartenlesegerätes überzeugt sich der Signaturschlüsselinhaber davon, dass das Chipkartenlesegerät sicherheitsbestätigt im Sinne des Artikels 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Gesetz zur digitalen Signatur) vom 01. August 1997 ist. Mit nicht sicherheitsbestätigten Chipkartenlesegeräten nutzt er Signaturanwendung StarCert **nicht**.

7. Vor Benutzung eines Chipkartenlesegerätes stellt der Signaturschlüsselinhaber fest, ob es sich um ein von Dritten zur Nutzung bereitgestelltes Chipkartenlesegerät handelt. Ist dies der Fall, so nutzt er die Signaturerzeugungsfunktion der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) **nicht**.

8. Nutzt der Signaturschlüsselinhaber die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) als multifunktionale Karte, so darf er die Identifikationsdaten (PIN und PUK) für die Signaturanwendung StarCert nicht für andere Anwendungen ebenfalls vereinbaren.

9. Generiert und nutzt der Signaturschlüsselinhaber mehr als ein signaturgesetzkonformes Signaturschlüsselpaar, so hat er unmittelbar vor der Signaturerzeugung den gewünschten privaten Signaturschlüssel, mit dem er die digitale Signatur erzeugen will, auszuwählen.

10. Nach erfolgreicher Authentisierung ist die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) in der Lage, eine unbegrenzte Anzahl digitaler Signaturen zu erzeugen, wobei ein Wechsel des privaten Signaturschlüssels, mit dem eine digitale Signatur erzeugt wird, möglich ist. Die Zertifizierungsstelle hat daher dafür Sorge zu tragen, dass das geeignete IT-System, mit dem zusammen die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) benutzt wird, die Anzahl der ohne erneute Authentisierung generierbaren digitalen Signaturen begrenzt. Zulässig ist eine Begrenzung dieser Anzahl durch Überwachung der seit einer erfolgreichen Authentisierung abgelaufenen Zeit oder der Anzahl der erzeugten digitalen Signaturen. Ist die vorgegebene Zeit abgelaufen oder die vorgegebene Anzahl von digitalen Signaturen erzeugt worden, so muss das IT-System eine erneute Authentisierung erzwingen, bevor eine weitere digitale Signatur erzeugt würde.

11. Die Benutzung der Ver- und Entschlüsselungsmöglichkeiten der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) setzt die Authentisierung des Signaturschlüsselinhabers mittels seiner Identifikationsdaten (PIN oder PUK) voraus. Daher dürfen auch in diesem Fall nur signaturgesetzkonforme technische Komponenten verwendet werden.

Es bestehen weitere Anforderungen, die jedoch nicht in **unmittelbarem** Zusammenhang mit der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) stehen. Sie werden daher hier nicht aufgeführt, sondern können dem Zertifizierungsreport debisZERT-DSZ-ITSEC-04020-2001 (Kapitel 3, Security Target) entnommen werden.

3.3 Eingesetzte Algorithmen und Parameter mit Gültigkeit

Die folgenden von der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) verwendeten Algorithmen und Parameter sind für Verwendung bei gesetzeskonformen digitalen Signaturen durch die Regulierungsbehörde für Telekommunikation und Post freigegeben:

- Hashalgorithmus SHA-1 bis 31.12.2005,
- asymmetrischer Verschlüsselungsalgorithmus (Signaturalgorithmus) RSA 1024-Bit bis 30.06.2005.

Die Algorithmen SHA-1 und RSA 1024-Bit werden von der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) selbst ausgeführt.

Die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) erzeugt eine digitale Signatur auch auf der Basis von Hashwerten nach den Algorithmen MD-5 und RIPEMD-160, wenn die entsprechenden Hashwerte übergeben werden.

Die Verwendung der Hashfunktion MD-5 führt zu digitalen Signaturen, die nicht signaturgesetzkonform sind. Sie ist von dieser Sicherheitsbestätigung ausdrücklich ausgeschlossen.

Diese Sicherheitsbestätigung ist gültig bis zum 30.06.2005; sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

3.4 Prüfstufe und Mechanismenstärke

Die technische Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) wurde auf dem Prozessor P8WE5032V0G erfolgreich nach der Prüfstufe E4 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichten dabei die Mindeststärke „hoch“. Hierfür liegt das Deutsche IT-Sicherheitszertifikat debisZERT-DSZ-ITSEC-04020-2001 vom 21. März 2001 vor.

Der Prozessor P8WE5032V0G wurde erfolgreich nach der Prüfstufe E4 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichten dabei die Mindeststärke „hoch“. Hierfür liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-ITSEC-0158-2001 vom 17. Januar 2001 vor.

Die sicherheitstechnisch korrekte Integration der technischen Komponente STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) und des Prozessors P8WE5032V0G wurde überprüft.

Ende der Sicherheitsbestätigung zur Registrierungsnummer debisZERT.02037.TE.03.2001