Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 2 und 15 Signaturverordnung[2]

T-Systems ISS GmbH
- Zertifizierungsstelle -

Rabinstr.8, 53111 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 1 SigG sowie §§ 15 Abs. 1 und 4, § 11 Abs. 3 SigV,
daß die

Signaturerstellungseinheit „Prozessorchipkarte mit Prozessor P8WE5032V0G und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems. 02078.TE.12.2001

Bonn, den 14.12.2001 _____
(Dr. Heinrich Kersten)

T-Systems ISS GmbH - Zertifizierungsstelle - ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

---

1 Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22)

2 Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59)

Die Bestätigung zur Registrierungsnummer T-Systems. 02078.TE.12.2001 besteht aus 9 Seiten.

Beschreibung der technischen Komponente:

1 Handelsbezeichnung der technischen Komponente und Lieferumfang:

Signaturerstellungseinheit „Prozessorchipkarte mit Prozessor P8WE5032V0G und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“

Auslieferung:
Prozessorchipkarte mit Prozessor P8WE5032V0G, Betriebssystem STARCOS SPK 2.3 v 7.0 und Signaturanwendung StarCert v 2.2

Umfang der Dokumentation:

a. Wenn der Kunde ein Systemhaus ist:

Dokumentation STARCOS SPK 2.3 v 7.0:

Reference Manual Smart Card Operating System STARCOS S 2.1, Giesecke & Devrient München, Edition August 2001, ID No 186467051

Reference Manual Smart Card Operating System STARCOS SPK 2.3 v 7.0, Supplement to the STARCOS S 2.1 Reference Manual, Giesecke & Devrient München, Edition Juli 2001, ID No. Z18899981

Release Notes for STARCOS SPK 2.3 v 7.0, Giesecke & Devrient München, 11.09.2001

Configuration Sheet STARCOS SPK 2.3 v 7.0, Giesecke & Devrient München, 11.09.2001

Dokumentation StarCert v 2.2:

Specification Signature Application StarCert version 2.2 for STARCOS SPK 2.3 v 7.0; Dokumentenversion 2.7, Giesecke & Devrient München, Datum 06.12.2001

User Documentation for the Cardholder, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v2.2; Dokumentenversion 1.5.6, Giesecke & Devrient München, Datum 16.11.2001

User Documentation for Terminal Developers, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v 2.2; Dokumentenversion 1.5.4, Giesecke & Devrient München, Datum 16.11.2001

b. Wenn der Kunde ein Zertifizierungsdiensteanbieter ist, zusätzlich:

Documentation for the Trust Center, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v 2.2; Dokumentenversion 1.7.5, Giesecke & Devrient München, Datum 19.11.2001

Specification, Card Life Cycle of STARCOS SPK 2.3 v.7.0 with the Signature Application StarCert v 2.2; Dokumentenversion 1.8, Giesecke & Devrient München, Datum 16.11.01

Delivery, generation, and configuration, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v2.2; Dokumentenversion 1.4.5, Giesecke & Devrient München, Datum 18.10.2001

STARCOS SPK 2.3 v.7.0 and StarCert v.2.2, Start-up and operation; Dokumentenversion 1.4.3, Giesecke & Devrient München, Datum 18.10.2001

Hersteller:
Giesecke & Devrient GmbH
Prinzregentenstraße 159
D-81607 München

2 Funktionsbeschreibung

Die Komponente ist eine Signaturerstellungseinheit. Sie besteht aus einer Prozessorchipkarte mit dem Prozessor P8WE5032V0G, dem Betriebssystem STARCOS SPK 2.3 v 7.0 und der Signaturanwendung StarCert v 2.2.[3]

STARCOS ist ein komplettes Betriebssystem für Prozessorchipkarten. STARCOS steuert den Datenaustausch und die Speicherbereiche und verarbeitet Informationen in der Prozessorchipkarte. Als Ressourcenmanager stellt STARCOS die notwendigen Funktionen für Betrieb und Management einer jeden Anwendung bereit. **STARCOS SPK 2.3 v 7.0** ist eine Weiterentwicklung des Betriebssystems STARCOS S 2.1, welche die gesamte Funktionalität von STARCOS S 2.1 beinhaltet und die für asymmetrische Kryptographie benötigten Funktionen hinzufügt.

STARCOS SPK 2.3 v 7.0 implementiert den symmetrischen Verschlüsselungsalgorithmus DEA (Data Encryption Algorithm) und seine Spezialform Triple-DES, sowie die asymmetrischen Kryptoalgorithmen RSA und DSA. Die Algorithmen RSA und DSA können benutzt werden, um elektronische Signaturen zu erzeugen. In Verbindung mit der Signaturanwendung StarCert v 2.2 ermöglicht STARCOS SPK 2.3 v 7.0 die sichere Erzeugung und Prüfung elektronischer Signaturen.

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 stellt Sicherheitsfunktionen zur Verfügung, die insbesondere die symmetrische und asymmetrische Authentisierung, die sichere Datenspeicherung (insbesondere von Signaturschlüsseln und Identifikationsdaten), die Sicherung der Kommunikation zwischen einer (externen) Anwendung und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 sowie kryptographische Funktionen zur Berechnung elektronischer Signaturen und zur Verschlüsselung von Daten umfassen.

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 kann ein bis maximal drei Signaturschlüsselpaare auf der Prozessorchipkarte generieren und speichern. Die sichere Erzeugung von Signaturschlüsselpaaren wurde mit einem Hardwarezufallszahlengenerator auf der Prozessorchipkarte realisiert. Die so erzeugten Zufallszahlen werden zusätzlich durch eine kryptographische Software-Nachbehandlung weiterbearbeitet.

[3] Die folgende Funktionsbeschreibung wurde vom Hersteller vorgelegt und durch die Bestätigungsstelle nur geringfügig in der Terminologie angepaßt.

Abhängig vom verfügbaren Speicherplatz können weitere Datenobjekte wie X.509 v 3-Zertifikate und PKCS#15-Dateien gespeichert und über die Kartenschnittstelle ausgelesen werden.

StarCert v 2.2 ist eine Weiterentwicklung von StarCert, die insbesondere um die Funktionalität der SSL-Authentisierung ergänzt wurde. Für SSL-Authentisierung und Entschlüsselung ist jeweils ein eigenes Schlüsselpaar vorgesehen, das von außen in StarCert v 2.2 eingebracht wird. In Sonderfällen können diese beiden Schlüsselpaare identisch sein. Unabhängig von der Signaturanwendung schützt StarCert v 2.2 den Zugriff auf die SSL-Authentisierungs- und Entschlüsselungsfunktionalität durch Nutzerauthentisierung mittels eines optionalen Global-PIN-Mechanismus. Die Global-PIN-Funktionalität wird während der Initialisierung aktiviert und kann nicht nachträglich gesetzt werden. Die Global-PIN kann entweder ausschließlich für SSL-Authentisierung oder für Entschlüsselung bzw. alternativ zum gleichzeitigen Freischalten beider Anwendungen aktiviert werden; die Global-PIN schaltet jedoch niemals die Signaturfunktionalität frei. Ist die Global-PIN nicht aktiviert, erfolgt der Zugriff auf SSL-Authentisierung oder Entschlüsselung ungeschützt.

Während der Auslieferung an den Nutzer ist die Signaturanwendung selbst mit einem Transport-PIN-Mechanismus versehen. Die Transport-PIN muß vom Nutzer vor der ersten Signatur zur Signatur-PIN geändert werden. In der Nutzungsphase ist die Signaturanwendung mit einer nur dem Nutzer bekannten Signatur-PIN geschützt, die von der Transport-PIN und der Global-PIN verschieden ist. Eine nach mehrmaliger Fehleingabe der Signatur-PIN gesperrte Signaturanwendung kann durch einen optional implementierbaren PUK-Mechanismus wieder entsperrt werden. Die Aktivierung des PUK-Mechanismus erfolgt während der Initialisierung und kann nicht nachträglich stattfinden.

Die Signaturanwendung StarCert v 2.2 kann durch den Hersteller in zwei Grundkonfigurationen ausgeliefert werden, je nachdem ob nach erfolgter Nutzerauthentisierung durch die Signatur-PIN

K1. nur genau eine einzige Signatur oder

K2. eine unbegrenzte Menge von Signaturen

erstellt werden kann. Im Fall K2 kann eine Beschränkung der Anzahl von Signaturen ohne erneute Authentisierung des Nutzers durch eine geeignete Signaturanwendungskomponente über die Zeit (Zeitvorgabe oder manuelles Entfernen der Prozessorchipkarte aus dem Kartenleser) oder über die Anzahl (Zählen von Signaturen) gesteuert werden.

Während der Nutzungsphase können einzelne Signaturschlüsselpaare dauerhaft gesperrt werden oder die gesamte Signaturanwendung StarCert v 2.2 über ein Kommando irreversibel unbrauchbar gemacht werden (beispielsweise am Ende der Nutzungsphase).

Es werden die Hashfunktionen SHA-1 und RIPEMD-160 sowie drei verschiedene Verfahrensweisen bei der Hashwertberechnung unterstützt. Bei dem Hashverfahren SHA-1 wird der Hashwert entweder vollständig auf der Prozessorchipkarte berechnet oder es wird in einem alternativen Verfahren ein Zwischenwert an die Prozessorchipkarte übergeben und die letzte Hashrunde auf der Prozessorchipkarte selbst ausge-

führt. Außerdem ist es möglich, einen komplett extern berechneten Hashwert zu übergeben und nur das Padding auf der Prozessorchipkarte mit StarCert v 2.2 auszuführen. Bei dem Hashverfahren RIPEMD 160 muss der Hashwert stets komplett extern berechnet und an StarCert v 2.2 übergeben werden. Das Padding und die Berechnung der Signatur erfolgen in jedem Fall durch StarCert v 2.2 auf der Prozessorchipkarte.

Als Padding-Verfahren kann der Benutzer alternativ Padding nach PKCS#1 v 1.5 oder ISO/IEC 9796 Teil 2 unter Verwendung von Zufallszahlen auswählen. STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 unterstützt die gegenseitige Geräteauthentisierung und Secure Messaging gemäß ISO/IEC 7816 Teil 4. Es werden die Transportprotokolle T=0 und T=1 unterstützt.

Die Prozessorchipkarte kann als multifunktionale Chipkarte benutzt werden. In diesem Fall können andere Anwendungen während der Phase der operationellen Nutzung in die Prozessorchipkarte geladen werden.

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 unterstützt verschiedene Personalisierungsmodelle, wobei die Personalisierung entweder zentral, also unter direkter, lokaler Kontrolle eines Zertifizierungsdiensteanbieters, oder dezentral, d.h. beim Nutzer oder einem externen Personalisierungsdienstleister, durchgeführt werden kann. Während der Erstpersonalisierung wird STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 durch eine Personalisierungs-PIN geschützt, so dass der Personalisierungsvorgang bei Bedarf sicher unterbrochen, fortgeführt und beendet werden kann.

StarCert v 2.2 ermöglicht den sicheren Export des (öffentlichen) Signaturprüfschlüssels. Mit dem CV-Kartenzertifikatmechanismus und dem Kartenauthentisierungsschlüsselpaar kann über eine Zertifikatskette der technische Nachweis erbracht werden, dass ein bestimmter (öffentlicher) Signaturprüfschlüssel zu einer ganz bestimmten Prozessorchipkarte gehört, und dass dieses Signaturschlüsselpaar insbesondere auch in dieser bestimmten Karte generiert worden ist.

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 wurde gemäß den Standards ISO/IEC 7816 Teile 1-8, den Deutschen DIN Vornormen DIN - V 66291 v 1.0 Teile 1-4, der Health Professional Card Spezifikation HPC v 1.0 und der Office Identity Card Spezifikation OIC v 1.0 implementiert. Außerdem sind die Standards PKCS#1 v 2.0 basierend auf v 1.5 und ISO/IEC 9796 Teil 2 berücksichtigt.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturerstellungseinheit „Prozessorchipkarte mit Prozessor P8WE5032V0G und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“ erfüllt die folgenden Anforderungen:

- §15 Abs. 1 S. 1 SigV
- §15 Abs. 1 S. 2 SigV
- §15 Abs. 1 S. 4 SigV
- §15 Abs. 4 SigV

Diese Anforderungen werden durch die Signaturerstellungseinheit unter den angegebenen Einsatzbedingungen 3.2 und unter Beachtung folgender Restriktionen erfüllt:

- Die Erzeugung von elektronischen Signaturen mit dem Algorithmus DSA ist **nicht** Gegenstand dieser Sicherheitsbestätigung.
- Die SSL-Authentisierungs- und Entschlüsselungsfunktionalität ist **nicht** Gegenstand dieser Sicherheitsbestätigung.
- Eine dezentrale Personalisierung der Signaturerstellungseinheit fällt nur dann unter diese Sicherheitsbestätigung, wenn sie unter der Kontrolle eines Zertifizierungsdiensteanbieters (hier: ggf. durch eine Registrierung als ausgelagerter Teildienst des Zertifizierungsdienstes) durchgeführt wird.
- Die mit dem CV-Kartenzertifikatmechanismus[4] realisierte Funktionalität ist **nicht** Gegenstand dieser Sicherheitsbestätigung.
- Die Konfiguration K2 (s. Kapitel 2) darf nur in besonders gesicherten Einsatzumgebungen betrieben werden, in denen ein Mißbrauch der Signaturerstellungsfunktion sicher auszuschließen ist. Eine solche Einsatzumgebung liegt typischerweise bei einem akkreditierten Zertifizierungsdiensteanbieter vor.
- In der Konfiguration K2 (s. Kapitel 2) kann eine Begrenzung der Parameter „Zeit“ oder „Anzahl“ durch eine geeignete gesetzeskonforme Signaturanwendungskomponente erfolgen, sofern sichergestellt ist, daß eine erneute Authentisierung stets durch den Signaturschlüsselinhaber (und nicht automatisiert durch die Anwendung) erfolgt. Dabei muss eindeutig die willentliche Erklärung des Signaturschlüsselinhabers zur Signaturerzeugung erkennbar sein.
- Der PUK-Mechanismus darf weder für den Zertifizierungsdiensteanbieter noch für den Signaturschlüsselinhaber aktiviert werden.

[4] Diese Funktionalität ist im Rahmen der Evaluierung geprüft worden; hinsichtlich der ITSEC-Konformität vgl. man das Deutsche IT-Sicherheitszertifikat / den Zertifizierungsreport T-Systems-DSZ-ITSEC-04075-2001. Die mögliche Verwendung dieser Funktionalität im Zusammenhang mit der Personalisierung der Karten muß im Sicherheitskonzept des ZDA beschrieben werden; die Vereinbarkeit des Personalisierungsverfahrens mit den Anforderungen des Signaturgesetzes ist dabei zu prüfen.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, daß folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 wird vor dem Beginn der Phase der operationellen Nutzung in die Prozessorchipkarte mit dem Prozessor P8WE5032V0G der Firma Philips[5] eingebracht. Dieser Prozeß endet mit der Initialisierung. Die bis zum Ende der Initialisierungsphase einzuhaltenden technischen und organisatorischen Sicherheitsbestimmungen sind dokumentiert und liegen dem Chipkartenhersteller vor.

Anmerkung: Die dieser Bestätigung zugrunde liegende Prüfung von STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 ist in Verbindung mit dem Prozessor P8WE5032V0G der Firma Philips durchgeführt worden. Diese Bestätigung ist deshalb zunächst nur mit dem Prozessor P8WE5032V0G der Firma Philips gültig. Bevor diese Sicherheitsbestätigung auf einen anderen Prozessorchip erweitert werden kann, ist eine Re-Evaluierung notwendig. An die Prozessorchipkarte bestehen dabei folgende Anforderungen:

1. Die Prozessorchipkarte schützt STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 vor Veränderungen.
2. Die Prozessorchipkarte schützt die 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 den 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.

Während der Erstpersonalisierung werden die den späteren Signaturschlüsselinhaber charakterisierenden Daten in die Signaturerstellungseinheit eingebracht. Wurde bisher kein Signaturschlüsselpaar erzeugt, so kann dies ebenfalls getan werden. In diesem Fall ist die Signaturerstellungseinheit für den Signaturschlüsselinhaber bereits unmittelbar nach Abschluß der Erstpersonalisierung nutzbar. Die Erzeugung des Signaturschlüsselpaares wird vollständig von der Prozessorchipkarte selbst vorgenommen. Das Problem der Erzeugung und Speicherung des (privaten) Signaturschlüssels in einer externen Komponente entsteht daher nicht.

Wird bei der Erstpersonalisierung kein Schlüsselpaar erzeugt, so kann dies später auch durch den Signaturschlüsselinhaber veranlaßt werden. Diese dezentrale Schlüsselerzeugung fällt nur dann unter diese Sicherheitsbestätigung, wenn sie unter der Kontrolle eines Zertifizierungsdiensteanbieters durchgeführt wird (hier: ggf. eine Registrierung als ausgelagerter Teildienst des Zertifizierungsdienstes, s. hierzu auch Abschnitt 3.1).

Die Signaturerstellungseinheit verfügt nicht über eine benutzerlesbare Schnittstelle. Sie muss daher zusammen mit einer geeigneten gesetzeskonformen Signaturanwendungskomponente genutzt werden.

[5] hier und im folgenden stets: Philips Semiconductors Hamburg

b) Nutzung des Produktes

Die Signaturerstellungseinheit „Prozessorchipkarte mit Prozessor P8WE5032V0G und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“ wird vom Hersteller gemäß Abschnitt 1 ausgeliefert. Der spezifizierte Auslieferungsumfang ist einzuhalten.

Anwendungen, die diese Signaturerstellungseinheit nutzen, sind **nicht** Gegenstand dieser Bestätigung.

Folgende Bedingungen für den sachgemäßen Einsatz sind zu beachten:

Zertifizierungsdiensteanbieter:

1. Der Zertifizierungsdiensteanbieter muss die Signaturerstellungseinheit beim Hersteller direkt abholen. Abweichungen hiervon sind nur dann zulässig, wenn ein sicherheitstechnisch gleichwertiges Verfahren angewendet wird, das vom BSI zur Erfüllung der ITSEC-Anforderungen mindestens für die Stufe E3 zugelassen und die Signaturerstellungseinheit mit dem geänderten Auslieferungsverfahren erneut als konform zum Signaturgesetz bestätigt worden ist.
2. Bevor der Zertifizierungsdiensteanbieter für ein vom Signaturschlüsselinhaber generiertes Schlüsselpaar ein Zertifikat ausstellt, muss er sich davon überzeugen, dass an der Signaturerstellungseinheit keine sicherheitstechnischen Veränderungen vorgenommen worden sind.
3. Die Signaturprüf- oder Authentisierungsschlüssel und die Zertifikate des Zertifizierungsdiensteanbieters und der Wurzelzertifizierungsstelle sowie das Zertifikat des Zertifizierungsdiensteanbieters über den (öffentlichen) Signaturprüfschlüssel des Signaturschlüsselinhabers müssen authentisch und unverändert in die Signaturerstellungseinheit eingebracht werden.
4. Zum Abschluß der Erstpersonalisierung muss das Paßwort des Herstellers (PIN.GD.PERS) dauerhaft gesperrt werden.

Signaturschlüsselinhaber:

- Nutzt der Signaturschlüsselinhaber die Signaturerstellungseinheit als multifunktionale Karte, so darf er die Identifikationsdaten für die Signaturanwendung StarCert v 2.2 nicht für andere Anwendungen ebenfalls vereinbaren.

An den Signaturschlüsselinhaber bestehen folgende allgemeine Anforderungen:

1. Der Signaturschlüsselinhaber muss die Signaturerstellungseinheit so benutzen und aufbewahren, daß Mißbrauch und Manipulation vorgebeugt wird.
2. Der Signaturschlüsselinhaber benutzt die Signaturerzeugungsfunktion nur für solche Daten, deren Integrität oder Authentizität er sicherstellen will.
3. Der Signaturschlüsselinhaber hält seine Identifikationsdaten für die Signaturerstellungseinheit vertraulich.
4. Der Signaturschlüsselinhaber ändert seine Identifikationsdaten für die Signaturerstellungseinheit in regelmäßigen Abständen.
5. Der Signaturschlüsselinhaber verwendet die Signaturerstellungseinheit nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.

6. 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 elektronische Signatur erzeugen will, auszuwählen.

Mit Auslieferung der Signaturerstellungseinheit „Prozessorchipkarte mit Prozessor P8WE5032V0G und STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“ sind die Anwender auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Für die folgenden von der Signaturerstellungseinheit verwendeten Algorithmen und Parameter ist gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV die Eignung festgestellt worden (s. Bundesanzeiger Nr. 158 – Seite 18 562 vom 24. August 2001):

- Hashalgorithmus SHA-1 bis 31.12.2006,
- Signaturalgorithmus RSA 1024-Bit bis 31.12.2006.

Diese Sicherheitsbestätigung ist somit gültig bis zum 31.12.2006; 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

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 wurde auf dem Prozessor P8WE5032V0G erfolgreich nach der Prüfstufe **E4** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichten dabei die Mindeststärke „**hoch**“.

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 von STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 und des Prozessors P8WE5032V0G wurde überprüft.

Die für die Signaturerstellungseinheit nach SigV maßgebende Evaluierungsstufe **E3** und die Mechanismenstärke „**hoch**“ sind damit erreicht (bzw. übertroffen).

Ende der Bestätigung