



## 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](mailto:office@a-sit.at)

DVR: 1035461

ZVR: 948166612

### BESCHEINIGUNG NACH § 18 ABS. 5 SIGG

## Sichere Signaturerstellungseinheit STARCOS 3.4 Health AHC C1

Antragsteller:  
Giesecke & Devrient GmbH  
Prinzregentenstraße 159  
D-81677 München

**Bescheinigung ausgestellt am: 21.12.2009**  
**Referenznummer A-SIT-1.084**

### 1. Beschreibung der zu bescheinigenden Komponente

STARCOS 3.4 Health AHC C1 ist eine sichere Signaturerstellungseinheit (nachstehend Signaturkarte genannt) bestehend aus:

Hardware:

- Prozessorchip NXP P5CC052V0A<sup>1</sup>, Hersteller: NXP Semiconductors Germany GmbH, Stresemannallee 101, 22529 Hamburg

Eingebettete Software:

- Betriebssystem STARCOS 3.4, Hersteller: Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81677 München
- Applikation für die qualifizierte elektronische Signatur gemäß „Generic Application STARCOS 3.4 Health AHC C1“

Mit der Signaturkarte wird die folgende Dokumentation geliefert:

- Guidance Documentation STARCOS 3.4 Health AHC C1 - Main Document
- Guidance Documentation for the Initialisation Phase STARCOS 3.4 Health AHC C1
- Guidance Documentation for the Personalisation Phase STARCOS 3.4 Health AHC C1
- Guidance Documentation for the Usage Phase STARCOS 3.4 Health AHC C1
- Generic Application STARCOS 3.4 Health AHC C1
- STARCOS 3.4 SmartCard Operating System Reference Manual

Eine SW-Applikation zur Verifikation der Korrektheit des File-Systems („Smart Card Application Verifier“) ist ebenfalls Teil des Auslieferungsumfangs.

<sup>1</sup> Der Prozessorchip Phillips P5CC52V0A wurde vom BSI zertifiziert. Das Zertifikat BSI-DSZ-CC-0466-2008 vom 24.6.2008 weist der Komponente eine Konformität zum Schutzprofil BSI-PP-0002-2001, sowie die erfolgreiche Evaluierung nach der Prüfstufe EAL5+ (Erweiterungen: ALC\_DVS.2: Lebenszyklus-Unterstützung - Ausreichende Sicherheitsmaßnahmen, AVA\_MSU.3: Schwachstellenbewertung – Analysieren und Testen auf unsichere Zustände, AVA\_VLA.4: Schwachstellenbewertung – Hohe Widerstandsfähigkeit) aus. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke „hoch“.

STARCOS 3.4 ist ein zum ISO/IEC 7816 Standard konformes SmartCard Betriebssystem, das im ROM des zertifizierten<sup>1</sup> Prozessorchips NXP P5CC052V0A installiert ist. Die vom Prozessorchip bereit gestellte kryptographische Bibliothek (RSA 2048 Bit) wird von der bescheinigten Komponente nicht genutzt. Das Betriebssystem enthält eine eigene Bibliothek zur Berechnung von elektronischen Signaturen auf Basis von elliptischen Kurven (ECC) mit einer Schlüssellänge von 256 Bit.

Die Signaturkarte darf nur in einer vertrauenswürdigen Einsatzumgebung eingesetzt werden. Der Signator muss daher vor jedem Einsatz der Signaturkarte zur Erstellung von qualifizierten Signaturen entscheiden, ob die Einsatzumgebung vertrauenswürdig ist oder nicht. Zum Setzen der Signatur-PIN vor dem erstmaligen Einsatz der Signaturkarte ist ein Initialisierungs-Mechanismus implementiert, der gewährleistet, dass vor dem Setzen der Signatur-PIN keine Signaturen erzeugt werden können. Nach dem Setzen der Signatur-PIN ist dieser Mechanismus deaktiviert und kann nicht mehr aktiviert werden. Die Signatur-PIN hat eine Mindestlänge von 6, eine Maximallänge von 12 Stellen und besitzt einen Fehlbedienungs-Zähler, der im Zuge der Personalisierung vom Zertifizierungsdiensteanbieter bzw. Kartenherausgeber auf einen Wert von max. 10 Versuchen gesetzt werden kann. Bei abgelaufenem Fehlbedienungs-Zähler ist die Signaturfunktionalität permanent gesperrt. Die Signatur-PIN ist ausschließlich den Signaturerstellungsdaten zugeordnet, nach erfolgreicher Authentisierung mit der Signatur-PIN kann vom Signator genau eine Signatur erstellt werden. Ein Wechsel der Signatur-PIN durch den Signator ist möglich.

Neben der Signaturapplikation mit den Signaturerstellungsdaten für qualifizierte elektronische Signaturen können auf der Signaturkarte weitere Applikationen mit weiteren Schlüsselpaaren und Daten vorhanden sein. Diese zusätzlichen Applikationen sind nicht Gegenstand dieser Bescheinigung.

## 2. Erfüllung der Anforderungen des SigG<sup>2</sup> und der SigV<sup>3</sup>

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach § 18 Abs. 1<sup>4</sup> und § 18 Abs. 2 zweiter Satz<sup>5</sup> SigG,
- Anforderungen nach § 3 Abs. 1<sup>6</sup> und § 3 Abs. 2<sup>7</sup> SigV und
- Anforderungen nach § 6 Abs. 1<sup>8</sup> und § 6 Abs. 2<sup>9</sup> SigV.

Die Signaturkarte ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung von Signaturerstellungsdaten,
- Komponenten und Verfahren zum Speichern von Signaturerstellungsdaten und
- Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten

<sup>2</sup> Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008 vom 22. April 2008.

<sup>3</sup> Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008)

<sup>4</sup> Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter 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

<sup>5</sup> 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.

<sup>6</sup> Die technischen Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten müssen in Hinblick auf das Erfordernis der Prüfung nach § 18 Abs. 5 SigG den Anforderungen des § 6 entsprechen.

<sup>7</sup> Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

<sup>8</sup> Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Es 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. (...)

<sup>9</sup> Bei den Prüfungen nach Abs. 1 sind insbesondere Referenznummern zu beachten, die im Amtsblatt der Europäischen Gemeinschaften nach Art. 3 Abs. 5 der Signaturrichtlinie 1999/93/EG für sichere Signaturerstellungseinheiten (Secure Signature-Creation Devices – SSCD) oder vertrauenswürdige Systeme oder Produkte des ZDA veröffentlicht wurden.

### 3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist für die Dauer von zwei Jahren ab Datum der Ausstellung gültig.

### 4. Einsatzbedingungen

Die Gültigkeit dieser Bescheinigung ist an die im Folgenden angeführten Einsatzbedingungen gebunden:

- (1) Die mit der Signaturkarte ausgelieferte Dokumentation (siehe Kapitel 1 dieser Bescheinigung) enthält die notwendigen Anweisungen für den sicheren Gebrauch der Signaturkarte. Zusätzlich sind für den sicheren Gebrauch der Signaturkarte die Annahmen über die Einsatzumgebung im Security Target, sowie das Security Target als Ganzes in Betracht zu ziehen. Diesen Anweisungen und Annahmen sowie den Einsatzbedingungen dieser Bescheinigung ist in geeigneter Weise der Wirkung nach zu entsprechen und es sind die getroffenen Maßnahmen
  - durch das Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters entsprechend § 12 SigV sicherzustellen,
  - in der Belehrung des Signators entsprechend zu übernehmen
  - und deren Wirkung im Wege der Aufsicht sicherzustellen.
- (2) Die Gültigkeit der Bescheinigung ist auf die in der Evaluierung berücksichtigten Initialisierungstabellen beschränkt. Der Hersteller der Signaturkarte muss eine Möglichkeit<sup>10</sup> bereitstellen, durch die überprüft werden kann, ob die Signaturkarte mit evaluierten Initialisierungstabellen verwendet wird.
- (3) Die Signaturerstellungsdaten sind vor ihrer ersten Anwendung mit einem Initialisierungs-Mechanismus geschützt. Vor Benutzung der Karte zur Erstellung von qualifizierten Signaturen bzw. vor Ausstellung eines qualifizierten Zertifikats über die Signaturprüfdaten müssen sich Signator bzw. ZDA mit Hilfe dieses Mechanismus vergewissern, dass die Signaturerstellungsdaten noch nicht verwendet worden sind.
- (4) Die Signaturkarte darf zur Erstellung von qualifizierten Signaturen nur in einer vertrauenswürdigen Einsatzumgebung verwendet werden. Diese Einsatzumgebung muss die Vertraulichkeit und Integrität der vom Signator eingegebenen Autorisierungs-codes sowie die Integrität der zu signierenden Daten bei deren Übermittlung an die Signaturkarte schützen.

### 5. Algorithmen und zugehörige Parameter

Zur Erstellung einer qualifizierten elektronischen Signatur wird von der Signaturkarte der ECDSA<sup>11</sup> Algorithmus nach ANSI X9.62 mit Längen der Parameter  $p$ ,  $q$  von 256 Bit bereitgestellt.

Zur Berechnung des Hashwertes wird von der Signaturkarte der Algorithmus SHA-256 nach ISO/IEC 10118-3 bereitgestellt.

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV<sup>12</sup> erfüllt.

---

<sup>10</sup> Laut Prüfbericht des Evaluators werden gültige Initialisierungstabellen vom Hersteller auf der Webseite <https://certificates.gi-de.com> veröffentlicht.

<sup>11</sup> DSA basierend auf einer Gruppe  $E(F_p)$


<sup>12</sup> Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.


## 6. Prüfstufe und Mechanismenstärke

Es liegt der Prüfbericht des Evaluators TÜV Informationstechnik GmbH<sup>13</sup> aus dem Zertifizierungsverfahren BSI-DSZ-CC-0601 vor. Der Prüfbericht weist der Signaturkarte die erfolgreiche Evaluierung nach der Prüfstufe EAL4+ (EAL4 mit Zusatz: AVA\_VAN.5<sup>14</sup>) der Common Criteria (CC, Version 3.1) aus. Die Signaturkarte ist nicht nach einem bestehenden Schutzprofil evaluiert worden. Die Evaluierung erfolgte auf Basis von Hersteller-spezifischen Sicherheitsvorgaben, die basierend auf dem Schutzprofil BSI-PP-0006-2002<sup>15</sup> erstellt wurden.

Die Signaturkarte widersteht in ihrer vorgesehenen Einsatzumgebung einem hohen Angriffspotential.

### Unterschriften:

Signaturwert	BOXMtOJAwQkj3CF5CnZkST4AIbquZmjuyd9n+5Ru2gS6P0rK5fndGK/UeTeHnqFY	
	Unterzeichner	Manfred Holzbach, Geschäftsführender Vorstand
	Datum/Zeit-UTC	2009-12-21T14:33:41Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	261828
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1261406021-18018406@30942-2746-0-18433-17653
Prüfhinweis	Prüfservice: <a href="http://www.signaturpruefung.gv.at">http://www.signaturpruefung.gv.at</a>	

Signaturwert	BIZsBnrVqZ0l3su+fXr2IPVYrR5QUFCizKtIOWeGsBq+K90/TZqga/RLSx8u4FpF	
	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2009-12-21T21:43:30Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	322009
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1261431810-1218161@29668-10739-0-11454-27462
Prüfhinweis	Prüfservice: <a href="https://www.signaturpruefung.gv.at/">https://www.signaturpruefung.gv.at/</a>	

<sup>13</sup> TÜV Informationstechnik GmbH, Langemarckstr. 20, 45141 Essen

<sup>14</sup> Vulnerability Assessment – Advanced methodical vulnerability analysis

<sup>15</sup> Es wurde das Protection Profile „Secure Signature-Creation Device Type 3“, Version 0.93 CC-V3.1, eine CC Version 3.1 entsprechende Weiterentwicklung des Schutzprofils BSI-PP-0006-2002 herangezogen. Dieses Schutzprofil entspricht dem CWA 14169 (Protection Profile for the SSCD Type 3) im „Verzeichnis allgemein anerkannter Normen für Produkte für elektronische Signaturen, die von den Mitgliedsstaaten angenommen werden sollen in Übereinstimmung mit den Anforderungen des Anhangs III der Richtlinie 1999/93/EG.“, veröffentlicht im Amtsblatt der Europäischen Union L 175/45 vom 15.7.2003.