

# Bestätigung

## von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 S. 1 Gesetz über Rahmenbedingungen für elektronische Signaturen<sup>1</sup> und § 11 Abs. 3 Signaturverordnung<sup>2</sup>

Nachtrag 2 zur Bestätigung  
SRC.00014.TE.02.2012 vom 01.02.2012

SRC Security Research & Consulting GmbH  
Emil-Nolde-Straße 7  
53113 Bonn

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

**Signaturerstellungseinheit  
„STARCOS 3.5 ID GCC C1R“**

**die o.g. Bestätigung wie nachstehend beschrieben erweitert wurde.**

Bonn, den 29.05.2017

\_\_\_\_\_  
Detlef Kraus Thomas Hueske



Die SRC Security Research & Consulting GmbH ist gemäß der Veröffentlichung im Amtsblatt der Bundesnetzagentur Nr. 19 unter der Mitteilung Nr. 605/2008 zur Erteilung von Bestätigungen für Produkte gemäß §§ 17 Abs. 4 S. 1, 15 Abs. 7 S. 1 SigG ermächtigt.

<sup>1</sup> Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

## **Beschreibung des Produktes für qualifizierte elektronische Signaturen:**

### **1. Handelsbezeichnung des Produktes und Lieferumfang**

#### **1.1 Handelsbezeichnung**

Keine Änderung gegenüber der Bezugsbestätigung.

#### **1.2 Auslieferung**

Keine Änderung gegenüber der Bezugsbestätigung.

#### **1.3 Lieferumfang**

Keine Änderung gegenüber der Bezugsbestätigung.

#### **1.4 Hersteller**

Die Angaben zum Hersteller werden durch folgenden Hinweis ergänzt:

**Hinweis:** Aufgrund einer Änderung der Organisationsstruktur, die zum Zeitpunkt der Ausstellung dieser Nachtragsbestätigung rechtlich noch nicht wirksam ist, ist der zukünftige Hersteller die Giesecke+Devrient Mobile Security GmbH, Prinzregentenstraße 159, 81677 München, Deutschland.

### **2. Funktionsbeschreibung**

Keine Änderung gegenüber der Bezugsbestätigung.

### 3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

#### 3.1 Erfüllte Anforderungen

Keine Änderung gegenüber der Bezugsbestätigung.

#### 3.2 Einsatzbedingungen

Die Einsatzbedingungen für die „nPA-Signaturkarte“ werden wie folgt ergänzt.

Aufgrund der Laufzeit der „nPA Signaturkarte“ von 10 Jahren und ständig verbesserter Angriffsmethoden ist auch durch das Risikomanagement des Anwenders, insbesondere dem Kartenherausgeber, zu bewerten, ob die Karte im Kontext fortgeschrittener Angriffsmethoden im Einsatz bleiben kann bis das hoheitliche Dokument seine Gültigkeit verliert.

#### 3.3 Algorithmen und zugehörige Parameter

Die „nPA-Signaturkarte“ stellt das ECDSA-Verfahren basierend auf Gruppen  $E(F_p)$  mit einer Länge von 256 Bit für die Parameter  $p$  und  $q$  zur Erstellung von elektronischen Signaturen bereit. Auf der Grundlage dieser Berechnungen können mit der „nPA-Signaturkarte“ ECDSA Signaturen gemäß EN 14890 erzeugt werden [EN 14890-1]. Dabei erfolgt die Signaturerzeugung mit einer ausschließlich externen Hashwertberechnung. Eine karteninterne Hashwertberechnung mit dem SHA-256 gemäß [FIPS 180-2] stellt die „nPA-Signaturkarte“ zwar zur Verfügung, zur Erzeugung qualifizierter Signaturen wird sie jedoch nicht genutzt.

Zur Erzeugung von Zufallszahlen wird in der „nPA-Signaturkarte“ ein deterministischer Zufallszahlengenerator verwendet. Der Zufallszahlengenerator ist ein K4-Generator mit Resistenz gegen Angriffe mit hohem Angriffspotenzial im Sinne der [AIS 20]. Der Parameter „Seed“ wird durch die zugrundeliegende Hardware mit einer Entropie von mindestens 120 Bit erzeugt. Der Zufallszahlengenerator der zugrundeliegenden Hardware ist ein P2-Generator mit SOF „hoch“ im Sinne der [AIS 31]. Die Zufallszahlen werden im laufenden Betrieb statistischen Tests unterzogen („Onlinetests“).

Die verwendeten kryptographischen Algorithmen sind gemäß dem Algorithmenkatalog der Bundesnetzagentur [Alg\_Kat 2017] als geeignet eingestuft.

Für das ECDSA-Verfahren basierend auf Gruppen  $E(F_p)$  gelten die folgenden Mindest-Schlüssellängen als geeignet:

**Tabelle 4: Mindest-Schlüssellängen für das ECDSA-Verfahren basierend auf Gruppen  $E(F_p)$**

Parameter \ Zeitraum	Bis Ende 2015	Bis Ende 2023
$p$	Keine Einschränkung	Keine Einschränkung
$q$	224 Bit	250 Bit

Für die Erzeugung von Zufallszahlen gilt für hoheitliche Ausweisdokumente eine Bestandswahrung (vgl. [Alg\_Kat 2017], Kapitel 4.3), die die Verwendung von Generatoren unter einer Zertifizierung alter Funktionalitätsklassen zulässt, bis das hoheitliche Dokument seine Gültigkeit verliert oder bis die Eignung des verwendeten Signaturverfahrens (bzw. Verfahren zur Erzeugung von Zufallszahlen) aus anderen Gründen erlischt.

Weiterhin wurde gemäß [Alg\_Kat 2017], Kapitel 3.2a) die ECC Brainpool Kurve P256r1 (brainpoolP256r1) bis Ende 2023 als geeignet eingestuft.

Diese Bestätigung der „nPA-Signaturkarte“ ist somit maximal gültig bis **31.12.2023**. Die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen und Parameter vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

### 3.4 Prüfstufe und Mechanismenstärke

Keine Änderung gegenüber der Bezugsbestätigung.

### Referenzen

Die angegebenen Referenzen werden wie folgt ergänzt.

[Alg\_Kat 2017] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001, 7. Dezember 2016, Veröffentlicht auf den Internetseiten des Bundesanzeigers ([www.bundesanzeiger.de](http://www.bundesanzeiger.de)) unter „BAnz AT 30.12.2016 B5“.

### Ende des Nachtrags 2