Bestätigung

von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 S. 1 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und § 11 Abs. 3 Signaturverordnung[2]

Nachtrag 5 zur Bestätigung
SRC.00021.TE.05.2013 vom 13.05.2013

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 ECC C1R“

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

Bonn, den 28.11.2017

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.

---

1 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)

2 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

Keine Änderung gegenüber der Bezugsbestätigung.

2. Funktionsbeschreibung

Die Beschreibung zur Sicherheitsfunktion „Password Authenticated Connection Establishment (PACE) Protokoll“ wird wie folgt ergänzt:

Für die Signaturerzeugung über die kontaktlose Schnittstelle muss PACE mit der PCAN, AdminCAN (abgeleiteter AES-Schlüssel) oder der CAN durchgeführt worden sein. In Abhängigkeit der Konfiguration der „GD-Signaturkarte“ können die öffentlichen Schlüsselwerte nach PACE mit der PCAN, AdminCAN oder der CAN gesichert ausgelesen und PIN- und PUK-Werte müssen immer vertraulich an die Karte übertragen werden.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Keine Änderung gegenüber der Bezugsbestätigung.

3.2 Einsatzbedingungen

Keine Änderung gegenüber der Bezugsbestätigung.

3.3 Algorithmen und zugehörige Parameter

Keine Änderung gegenüber der Bezugsbestätigung.

3.4 Prüfstufe und Mechanismenstärke

Keine Änderung gegenüber der Bezugsbestätigung.

Referenzen

In der Referenz [UG_GenApp] zu den generischen Applikationen wird der Eintrag zur Application Specification PACE international 1PIN ersetzt durch:

- STARCOS 3.5 ID ECC C1R Application Specification PACE international 1PIN, Version 0.30, 02.11.2017

Ende des Nachtrags 5