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 2 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 20.10.2016

Gerd Cimiotti 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

Der letzte Absatz auf Seite 2 wird durch den folgenden Absatz ersetzt:

Die Personalisierung der Karte erfolgt ebenfalls beim Zertifizierungsdiensteanbieter (bzw. bei einem beauftragten Dritten), der die spezifischen Daten in die Karte einbringt und sie anschließend an den Endkunden ausliefert. Als Transport-Schutz bei der Auslieferung zum Kunden wird eine spezifische Transport-PIN eingebracht oder das Leer-PIN-Verfahren verwendet. Weiterhin kann ein Resetting-Code (im Folgenden auch als PUK bezeichnet) entweder als echte PUK personalisiert werden oder die PUK wird durch den Kunden gesetzt, wobei eine Transport-PUK zum Einsatz kommen kann. Die Verwendung einer PUK ist optional. Die karteninterne Generierung des Signaturschlüsselpaars kann bereits mit der Personalisierung oder nach der Auslieferung durch den Kunden erfolgen. Möglich ist auch eine Kombination der beiden Verfahren, wobei das erste Schlüsselpaar während der Personalisierung und alle weiteren nach der Auslieferung durch den Kunden erzeugt werden.

1.3 Lieferumfang

Tabelle 1, Lieferumfang, Zeile 9 wird ersetzt durch:

9	Dokumentation	Generic Application of STARCOS 3.5 ID ECC C1R [UG_GenApp], Spezifikation des Filesystems		Januar 2013 / Oktober 2016	Dokument in elektronischer Form

1.4 Hersteller

Keine Änderung gegenüber der Bezugsbestätigung.

2. Funktionsbeschreibung

Der zweite und dritte Absatz auf Seite 7 (in Kapitel 2 Funktionsbeschreibung, Funktionalität und Architektur) werden durch die folgenden Absätze ersetzt:

Optional kann das erstellte Zertifikat auch auf der „GD-Signaturkarte“ abgespeichert werden. Im Rahmen dieser Komplettierung der *SSCD-Anwendung* muss, soweit nicht bereits vorhanden, noch die Transport-PIN und ggf. die Transport-PUK bzw. eine echte PUK in der Karte gesetzt werden.

Um mit der komplettierten *SSCD-Anwendung* eine Signatur erzeugen zu können, muss der designierte Signaturschlüsselinhaber die „GD-Signaturkarte“ als sichere Signaturerstellungseinheit (SSEE) aktivieren. Dazu muss er die voreingestellte und maximal fünfstellige Transport-PIN durch eine gültige Signatur-PIN ersetzen. Weiterhin setzt der designierte Signaturschlüsselinhaber die PUK sofern in der Kartenkonfiguration die Verwendung einer PUK vorgesehen ist, keine echte PUK personalisiert und an den Signaturschlüsselinhaber ausgehändigt wurde. Zum Setzen der PUK kann zusätzlich eine Transport-PUK verwendet werden. Das Setzen der PUK erfolgt einmalig.

Der dritte Absatz auf Seite 8 (in Kapitel 2 Funktionsbeschreibung, Funktionalität und Architektur) wird durch den folgenden Absatz ersetzt:

Nach einer Außerbetriebnahme kann eine erneute Aktivierung erfolgen, d.h. es kann eine neue Signatur-PIN nach dem nur in diesem Kartenzustand möglichen Leer-PIN-Verfahren gesetzt werden. Danach kann auch ein neuer Signaturschlüssel in der Karte generiert sowie ein qualifiziertes Zertifikat erzeugt und optional dieses in die Karte eingebracht werden.

Der sechste Punkt der Spiegelstrichliste auf Seite 11 (in Kapitel 2 Funktionsbeschreibung, Sicherheitsfunktionen bzw. –eigenschaften der „GD-Signaturkarte“, „Zugriffskontrolle“) wird durch die folgenden Punkte ersetzt:

- Sofern in der Kartenkonfiguration die Verwendung einer PUK vorgesehen ist und keine echte PUK personalisiert wurde, kann die PUK durch den designierten Signaturschlüsselinhaber bei einer ersten Aktivierung des Signaturschlüssels gesetzt werden. Dies kann abhängig von der Konfiguration der „GD-Signaturkarte“ unter Anwendung einer Transport-PUK erfolgen. Nach Setzen der PUK ist die PUK im Status "activated". Ein Rücksetzen des Status ist dann nicht mehr möglich, d.h. die PUK kann nur einmal gesetzt werden.
- Das Wechseln einer aktiven PUK in eine neue PUK durch den Signaturschlüsselinhaber kann nur nach einer erfolgreichen Benutzerauthentisierung mit der alten PUK erfolgen. Die Möglichkeit zum Wechseln der PUK ist optional und abhängig von der Kartenkonfiguration.

Im ersten Abschnitt auf Seite 15 (in Kapitel 2 Funktionsbeschreibung, Sicherheitsfunktionen bzw. –eigenschaften der „GD-Signaturkarte“, „Prozesse der PIN-basierten Authentisierung (Signatur-PIN)“) werden die letzten fünf Sätze wie folgt ersetzt:

Sofern in der Kartenkonfiguration die Verwendung einer PUK vorgesehen ist und keine echte PUK personalisiert wurde, ist der Resetting-Code mit einer Mindestlänge von sechs Stellen vor der Aktivierung der *SSCD-Anwendung* durch den designierten Signaturschlüsselinhaber zu setzen. Das Setzen der PUK kann nur einmalig bei der ersten Aktivierung des

Signaturschlüssels erfolgen. Bei Verwendung einer Transport-PUK muss sich der Benutzer durch eine erfolgreiche Eingabe der Transport-PUK gegenüber der „GD-Signaturkarte“ authentisieren. Die Verwendung der PUK sowie die Möglichkeit zum Wechsel einer aktiven in eine neue PUK sind optional und abhängig von der Konfiguration der „GD-Signaturkarte“.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Keine Änderung gegenüber der Bezugsbestätigung.

3.2 Einsatzbedingungen

Der zweite Punkt der Spiegelstrichliste im Kapitel 3.2 Einsatzbedingungen, Anforderungen an den Signaturschlüssel- bzw. Karteninhaber wird wie folgt ersetzt:

- Der Signaturschlüsselinhaber muss verifizieren, dass eine maximal fünfstellige Transport-PIN noch gültig ist, indem er mit dieser eine neue, von ihm selbst gewählte Signatur-PIN setzt, die über mindestens eine Länge von sechs Stellen verfügt. Ist die Transport-PIN nicht gültig, so muss sich der Signaturschlüsselinhaber mit dem ausgebenden ZDA in Verbindung setzen.

3.3 Algorithmen und zugehörige Parameter

Keine Änderung gegenüber der Bezugsbestätigung.

3.4 Prüfstufe und Mechanismenstärke

Keine Änderung gegenüber der Bezugsbestätigung.

Referenzen

Die Referenz zu [UG_GenApp] wird wie folgt geändert:

Generic Application of STARCOS 3.5 ID ECC C1R:

- STARCOS 3.5 ID ECC C1R Application Specification ESignK national, Version 0.18, 07.10.2016
- STARCOS 3.5 ID ECC C1R Application Specification ESignK national 1PIN, Version 0.10, 09.01.2013
- STARCOS 3.5 ID ECC C1R Application Specification EACv2 national, Version 0.20, 09.01.2013
- STARCOS 3.5 ID ECC C1R Application Specification EACv2 national 1PIN, Version 0.10, 09.01.2013
- STARCOS 3.5 ID ECC C1R Application Specification PACE national, Version 0.20, 09.01.2013
- STARCOS 3.5 ID ECC C1R Application Specification PACE national 1PIN, Version 0.10, 09.01.2013

Ende des Nachtrags 2