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.00007.TE.10.2010 vom 29.10.2010

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
„TCOS Identity Card Version 1.0 Release 1/P5CD128/145“

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

Bonn, den 13.12.2016

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

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 Einsatzsatzbedingungen 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 $E(F_p)$ zur Erstellung von elektronischen Signaturen gemäß [TR-03111] bereit. Es werden Schlüssellängen von 224, 256, 320, 384 und 512 Bit unterstützt. Dabei erfolgt die Signaturerzeugung mit einer ausschließlich externen Hashwertberechnung.

Zur Erzeugung von Zufallszahlen wird in der „nPA-Signaturkarte“ der durch die Hardware von NXP zur Verfügung gestellte Zufallszahlengenerator verwendet. 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 2016] wie folgt 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 2022
p	Keine Einschränkung	Keine Einschränkung
q	224 Bit	250 Bit

Die Schlüssellänge von 224 Bit darf nicht mehr verwendet werden.

Für die Erzeugung von Zufallszahlen gilt für hoheitliche Ausweisdokumente eine Bestandswahrung (vgl. [Alg_Kat 2016], 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.

Diese Bestätigung der „nPA-Signaturkarte“ ist somit maximal gültig bis **31.12.2022**. Die Gültigkeit kann jedoch verkürzt werden, wenn zu diesem Zeitpunkt Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen und Parameter vorliegen, oder 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 2016] 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, 9. Dezember 2015, Veröffentlicht auf den Internetseiten des Bundesanzeigers (www.bundesanzeiger.de) unter "BAnz AT 01.02.2016 B5".

Ende des Nachtrags 2