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 3 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 17.03.2017

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

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 / Dezember 2016	Dokument in elektronischer Form

1.4 Hersteller

Keine Änderung gegenüber der Bezugsbestätigung.

2. Funktionsbeschreibung

Die *SSCD-Anwendung* kann durch den Signaturschlüsselinhaber administriert werden. Hierzu wird die folgende Funktion ergänzt (vgl. Seite 8 der Bezugsbestätigung):

- Setzen einer neuen Signatur-PIN nach erfolgreicher Benutzerauthentisierung mit der PUK (nur für internationale Konfigurationen)

Angegebene Regeln der Zugriffskontrolle in der Nutzungsphase werden wie folgt ergänzt (vgl. Seite 11/12 der Bezugsbestätigung):

- Sofern in der Kartenkonfiguration die Verwendung einer PUK vorgesehen ist, kann eine neue Signatur-PIN nach einer erfolgreichen Benutzerauthentisierung mit der PUK gesetzt werden. Dies ist jedoch nur für internationale Konfigurationen möglich (vgl. [UG_GenApp]).

„Prozesse der PIN-basierten Authentisierung (Signatur-PIN)“

Der vierte Absatz wird wie folgt ergänzt:

Bei internationalen Konfigurationen (vgl. [UG_GenApp]) kann der Fehlbedienungszähler während der Initialisierung auf maximal zehn gesetzt werden. Sofern ein maximaler Fehlbedienungszähler zwischen vier und zehn gewählt wird, ist die zusätzliche Einsatzbedingung an die Initialisierung hinsichtlich der Mindestlänge der PIN sicherzustellen.

Der sechste Absatz wird wie folgt ersetzt:

Zum Zurücksetzen des FBZ ist das Kommando RESET RETRY COUNTER zu verwenden. Ein Wechsel einer Signatur-PIN ist bei nationalen Konfigurationen nicht möglich. Nur bei internationalen Konfigurationen (vgl. [UG_GenApp]) kann das Setzen einer neuen Signatur-PIN nach einer erfolgreichen Benutzerauthentisierung mit der PUK vorgenommen werden. In beiden Fällen erfolgt jedoch kein Setzen des Sicherheitszustandes einer Signatur-PIN, d.h. das Zurücksetzen einer blockierten Signatur-PIN ermöglicht nicht die Erzeugung einer qualifizierten Signatur.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Keine Änderung gegenüber der Bezugsbestätigung.

3.2 Einsatzbedingungen

Die Einsatzbedingungen an den Initialisierer werden wie folgt ergänzt:

- Bei internationalen Konfigurationen sind der Maximalwert f_{max} des Fehlbedienungszählers und die Minimallänge der PIN m so zu wählen, dass der Wert für f_{max} höchstens m/2 (abgerundet) beträgt und den Wert 10 nicht übersteigt.

Die Einsatzbedingungen an den Zertifizierungsdiensteanbieter werden wie folgt ergänzt:

- Wenn bei Anwendung internationaler Konfigurationen der ZDA dem Signaturschlüsselinhaber eine PUK übergeben muss, mit der das Setzen einer neuen Signatur-PIN möglich ist, so muss die Übergabe dieser PUK so erfolgen, dass

  1. sie zu keinem Zeitpunkt nach Einbringen in die SSEE bzw. Erzeugen in der SSEE außerhalb der SSEE gespeichert ist und

  2. der ZDA dem Signaturschlüsselinhaber ein abgeleitetes Datum (bzgl. PUK) auf einem geeigneten Datenträger übergibt. Hierbei muss ein unberechtigter Versuch, Kenntnis vom abgeleiteten Datum zu nehmen, leicht durch Inaugenscheinnahme des Datenträgers erkannt werden können.

  Das dedizierte Verfahren zur Übergabe der PUK bedarf weiterer Konkretisierung und ist im Sicherheitskonzept des ZDA detailliert darzulegen.

3.3 Algorithmen und zugehörige Parameter

Die „GD-Signaturkarte“ stellt zur Erstellung von elektronischen Signaturen sowohl das ECDSA- als auch das RSA-Verfahren bereit. Das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ mit einer Länge von 256 Bit, 320 Bit, 384 Bit, 512 Bit oder 521 Bit für die Parameter p und q. Auf der Grundlage dieser Berechnungen können mit der „GD-Signaturkarte“ ECDSA Signaturen gemäß [EN 14890-1] erzeugt werden. Das RSA-Verfahren basiert auf dem RSA-Algorithmus mit einer Schlüssellänge von 2048 Bit bis zu 4096 Bit. Die konkrete Schlüssellänge wird durch die berücksichtigten Initialisierungsskripte während der Initialisierung gesetzt und kann nachträglich nicht mehr geändert werden. Der öffentliche Exponent wird bei der RSA-Schlüsselgenerierung durch die Konfiguration fest vorgegeben und erfüllt somit die Anforderungen gemäß [Alg_Kat 2017]. Als Formatierungsverfahren zur Erzeugung qualifizierter elektronischer Signaturen werden RSASSA-PSS und PKCS#1-v1_5 gemäß [PKCS#1] unterstützt.

Zur Erzeugung von elektronischen Signaturen kann eine karteninterne bzw. eine teilweise karteninterne Hashwertberechnung mit der Hashfunktion SHA-2 (224, 256, 384 oder 512 Bit) gemäß [FIPS 180-2] oder eine ausschließlich externe Hashwertberechnung genutzt werden. Für die Anwendung von Hashfunktionen sind insbesondere die Einsatzbedingungen an die Hersteller von Signaturanwendungskomponenten zu berücksichtigen.

Es wird eine Zufallszahlenerzeugung auf Basis eines deterministischen Zufallszahlengenerators (DRNG) und eines Zufallszahlengenerators (TRNG) der zugrundeliegenden Hardware unterstützt. Der DRNG wurde im Rahmen der Evaluierung als DRG.4-Generator mit Resistenz gegen hohes Angriffspotenzial gemäß [AIS 20] bewertet. Die Seed des Generators wird durch die zugrundeliegende Hardware generiert. Die Anforderungen gemäß [Alg_Kat 2017] an die erforderliche Entropie der Seed werden erfüllt.

Der TRNG der zugrundeliegenden Hardware von Infineon Technologies ist ein Zufallszahlengenerator mit einer PTG.2-Klassifizierung gemäß [AIS 31]. Die Zufallszahlen werden im laufenden Betrieb statistischen Tests unterzogen („Onlinetests“). Diese Eigenschaften wurden im Rahmen der CC Evaluierung der Hardware von Infineon nachgewiesen (vgl. [STHW] und [IFX_Cert]).

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

Für die Hashfunktion SHA-2 gelten die folgenden Hashwert-Längen als geeignet für die Anwendung bei qualifizierten elektronischen Signaturen:

Tabelle 4: Mindest-Hashwert-Längen für SHA-2 Hashfunktionen

Geeignet bis Ende 2023
SHA-256, SHA-384, SHA-512

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

Tabelle 5: 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 den RSA-Algorithmus gelten die folgenden Mindest-Schlüssellängen als geeignet:

Tabelle 6: Mindest-Schlüssellängen für den RSA Algorithmus

Parameter \ Zeitraum	Bis Ende 2022	Bis Ende 2023
Schlüssellänge	1976 (Mindestwert) 2048 (Empfehlung)	3000

Für das Formatierungsverfahren RSASSA-PSS sind keine zeitlichen Restriktionen hinsichtlich dessen Eignung festgelegt. Das Formatierungsverfahren PKCS#1-v1_5 ist noch bis Ende 2017 geeignet.

Diese Bestätigung der „GD-Signaturkarte“ ist somit maximal gültig bis **31.12.2023**.

Die durch die Karte zur Verfügung gestellte Hashfunktion SHA-224 darf gemäß [Alg_Kat 2017] zur Erzeugung von qualifizierten Signaturen nicht mehr verwendet werden. Dies muss durch die Signaturanwendungskomponente sichergestellt werden. Weiterhin dürfen ab Anfang 2023 nur noch RSA-Schlüssel mit einer Mindestlänge von 3000 Bit zum Einsatz kommen. Dies muss bei der Erzeugung der Signaturschlüssel berücksichtigt werden.

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) unter „BAnz AT 30.12.2016 B5“.

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 international, Version 0.18, 05.12.2016
- STARCOS 3.5 ID ECC C1R Application Specification ESignK international 1PIN, Version 0.10, 09.01.2013
- 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 international, Version 0.20, 09.01.2013
- STARCOS 3.5 ID ECC C1R Application Specification EACv2 international 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 international, Version 0.20, 09.01.2013
- STARCOS 3.5 ID ECC C1R Application Specification PACE international 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 3