

# 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>

Korrigendum 1 zur Bestätigung  
SRC.00021.TE.05.2013 vom 13.05.2013

SRC Security Research & Consulting GmbH  
Graurheindorfer Straße 149 A  
53117 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 korrigiert wird.**

Bonn, den 14.11.2013

\_\_\_\_\_  
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 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542)

## Korrekturen

Der fünfte Absatz auf Seite 7 (in Kapitel 2 Funktionsbeschreibung, Funktionalität und Architektur) wird durch den folgenden Absatz ersetzt:

„Die „GD-Signaturkarte“ unterstützt die optionale Verwendung von zwei Signaturschlüsseln (z.B. ein RSA-Signaturschlüssel und ein Signaturschlüssel für elliptische Kurven). Der Zugriff auf die Signaturschlüssel kann entweder durch eine gemeinsame Signatur-PIN geschützt werden oder jeder Signaturschlüssel verfügt über seine eigene Signatur-PIN. Im Falle eigener Signatur-PINs verfügt jede Signatur-PIN auch über eigene Sicherheitsattribute (z.B. Transport-PIN, Fehlbedienungszähler (FBZ)). Die „GD-Signaturkarte“ kann somit in den folgenden Varianten genutzt werden:“

Der letzte Absatz auf Seite 15 (in Kapitel 2 Funktionsbeschreibung, Sicherheitsfunktionen bzw. -eigenschaften der „GD-Signaturkarte“, „Prozesse der PIN-basierten Authentisierung (Signatur-PIN)“) wird durch den folgenden Absatz ersetzt:

Die „GD-Signaturkarte“ unterstützt die optionale Verwendung von zwei Signaturschlüsseln (z.B. ein RSA-Signaturschlüssel und ein Signaturschlüssel für elliptische Kurven). Der Zugriff auf die Signaturschlüssel kann entweder durch eine gemeinsame Signatur-PIN geschützt werden oder jeder Signaturschlüssel verfügt über seine eigene Signatur-PIN. Im Falle eigener Signatur-PINs verfügt jede Signatur-PIN auch über eigene Sicherheitsattribute (z.B. Transport-PIN, FBZ). Die beschriebenen Sicherheitseigenschaften gelten für jede Signatur-PIN.

**Ende des Korrigendums 1**