Bestätigung
von Produkten für qualifizierte elektronische Signaturen

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

Nachtrag zur Bestätigung

BSI.02124.TE.09.2010 vom 24. September 2010

Bundesamt für Sicherheit in der Informationstechnik[3]
Godesberger Allee 185-189
53175 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 11 Abs.3, 15 Abs. 2 und 4 SigV,
dass die o.g. Bestätigung für

CHERRY SmartTerminal ST-2xxx; Firmwareversion: 6.01

erweitert wurde.

Im Auftrag

Bundesamt
für Sicherheit in der
Informationstechnik

Bonn, den 02.11.2015

Matthias Intemann

Das Bundesamt für Sicherheit in der Informationstechnik ist, auf Grundlage des Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, erschienen im Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 54, ausgegeben zu Bonn am 19. August 2009, Geltung ab 20. August 2009, zuletzt geändert durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, ausgegeben am 24.07.2015, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

---

[1] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4, Absatz 111 des Gesetzes vom 07. August 2013 (BGBl. I S. 3154)
[2] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 4, Absatz 112 des Gesetzes vom 07. August 2013 (BGBl. I S. 3154)
[3] Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, Postfach 200363, 53133 Bonn, Tel: +49(0)228 99 9582-0, Fax: +49(0)3018 9582-5455, E-Mail: bsi@bsi.bund.de, Web: www.bsi.bund.de

---

Nachtrag für das Produkt für qualifizierte elektronische Signaturen:

1 Änderungen gegenüber der Bestätigung BSI.02124.TE.09.2010 vom 24. September 2010

1.1 Antragsteller dieser Bestätigung bzw. Nachtrags-Bestätigung:

Nach Angaben des Antragstellers gleichzeitig Herstellers des o.g. Produktes wird sich der Firmenname ab 01.01.2016 ändern. Gemäß der amtlichen „Mitteilung über die Eintragung im Handelsregister B Amberg“ vom 28.09.2015 wird der bisherige Firmenname

ZF Electronics GmbH, Cherrystraße, 91275 Auerbach

zum 01.01.2016 auf

Cherry GmbH, Cherrystraße, 91275 Auerbach

geändert.

1.2 Laufzeit der Bestätigung

Die Sicherheitsfunktion SF.SECDOWN stützt sich im wesentlichen auf die Algorithmen RSA-2048 und SHA-256 ab. Diese im o.g. Produkt implementierten Algorithmen sind gegenüber der o.g. Bestätigung nicht geändert worden. Gemäß der von der Bundesnetzagentur veröffentlichten derzeit aktuellen Übersicht über geeignete Algorithmen[4] sind die Gültigkeitslaufzeiten für den RSA-Algorithmus mit der Länge von 2048 Bit und der Hash-Algorithmus SHA-256 von Ende 2016 auf Ende 2021 geändert worden. Damit erhöht sich auch die Gültigkeit der o.g. Bestätigung vom 31. Dezember 2015 auf den 31. Dezember 2021.

Über den von der Bundesnetzagentur angegebenen Zeitpunkt hinaus kann hinsichtlich der Widerstandsfähigkeit der Sicherheitsfunktion SF.SECDOWN keine Aussage getroffen werden.

1.3 Weitere Änderungen

Zu den o.g. in Kap. 1.1 und 1.2 beschriebenen Änderungen in der Bestätigung gibt es keine weiteren Änderungen, weder in der o.g. Bestätigung noch im o.g. Produkt selbst.

Alle Angaben, ausgenommen die beiden hier genannten Änderungen, in der o.g. Bestätigung gelten weiterhin.

Diese Nachtrags-Bestätigung ist nur in Verbindung mit der o.g. Bestätigung BSI.02124.TE.09.2010 gültig.

[4] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 15.12.2014

2 Gültigkeitsdauer der verwendeten Algorithmen

Durch die oben aufgeführte neue Version des Algorithmenkatalogs sind für die von der Sicherheitsfunktion SF.SECDOWN genutzten kryptograghischen Algorithmen die zeitlichen Randbedingungen wie folgt erweitert worden:

Hashalgorithmus	Geeignet bis
SHA-256	Bis Ende 2021

Tabelle 1: Zulässige Hashfunktionen

Schlüssellänge (Mindestwert)	Einsetzbar bis
RSA 1976 Bit	Bis Ende 2021

Tabelle 2: Zulässige Schlüssellängen

3 Gültigkeit der o.g. Bestätigung einschließlich dieser Nachtrags-Bestätigung

Diese Nachtrags-Bestätigung weist aus, dass die Gültigkeit der o.g. Bestätigung BSI.02124.TE.09.2010 vom 24. September 2010 bis zum 31. Dezember 2021 befristet ist.

Diese Befristung ist bedingt durch die Begrenzung der Einsetzbarkeit der Algorithmen gemäß Algorithmenkatalog der Bundesnetzagentur.

Da keine Neubewertung des Produktes vorgenommen wurde, kann keine Aussage zur Gültigkeit der Bestätigung hinsichtlich der aktuellen Sicherheit des Produktes vorgenommen werden. Diese Aussage ist vom Risikomanagement des Anwenders zu treffen.

Ende der Nachtrags-Bestätigung