Nachtrag Nr. 1 zur Sicherheitsbestätigung

T-Systems.02247.TE.12.2013

Kobil-Trust OCSP Version 3.6.1 Release 1111

KOBIL Systems GmbH

Bestätigung
von Produkten für qualifizierte elektronische Signaturen

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

Gültig bis: 30.06.2016

Nachtrag Nr. 1 zur Sicherheitsbestätigung T-Systems.02247.TE.12.2013 vom 20.12.2013

T-Systems GEI GmbH
- Zertifizierungsstelle -

Vorgebirgsstr. 49, 53119 Bonn

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

technische Komponente für Zertifizierungsdienste

Kobil-Trust OCSP Version 3.6.1 Release 1111

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02247.TU.12.2014

Bonn, den 18.12.2014

_____

Dr. Igor Furgel
Leiter der Zertifizierungsstelle

Die T-Systems GEI GmbH – Zertifizierungsstelle – ist gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

---

1 Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), vom 16. Mai 2001 (BGBl. I S. 876), das durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist (BGBl. Jahrgang 2009, Teil I S. 2091)

2 Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16. November 2001 (BGBl. I S. 3074), die durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist (BGBl. I S. 1542)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Die technische Komponente für Zertifizierungsdienste „Kobil-Trust OCSP Version 3.6.1 Release 1111“.

Die Bezugsbestätigung T-Systems.02247.TE.12.2013 vom 20.12.2013 wurde für das Produkt „FlexiTrust OCSP Version 3.6.1 Release 1111“ ausgestellt. Die Produktbezeichnung hat sich wegen der Umfirmierung des Herstellers (s. Abschn. 1.4 weiter unten) ohne jegliche technische Änderungen am Produkt geändert.

1.2 Auslieferung

Es gelten alle relevanten Angaben der Bezugsbestätigung.

1.3 Lieferumfang

Es gelten alle relevanten Angaben der Bezugsbestätigung unter der Berücksichtigung der aktuellen Produktbezeichnung Kobil-Trust OCSP Version 3.6.1 Release 1111.

1.4 Antragsteller dieser Bestätigung und Hersteller des Produkts

Der Antragsteller für das aktuelle Bestätigungsverfahren und der Hersteller des Produkts ist

KOBIL Systems GmbH
Pfortenring 11
67547 Worms

Die Bezugsbestätigung T-Systems.02247.TE.12.2013 vom 20.12.2013 wurde für den Antragsteller, der auch der Hersteller des Produkts war, ausgestellt:

FlexSecure GmbH
Industriestraße 12
64297 Darmstadt

2. Funktionsbeschreibung

Der EVG[3] Kobil-Trust OCSP Version 3.6.1 Release 1111 ist teils eine technische Komponente für Zertifizierungsdienste und teils eine Signaturanwendungskomponente gemäß §2 SigG:

„Im Sinne dieses Gesetzes sind [...]

11. „Signaturanwendungskomponenten“ Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen […]

12. „Technische Komponenten für Zertifizierungsdienste“ Software- oder Hardwareprodukte, die dazu bestimmt sind, […] b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten […]“

2.1 Kurzbeschreibung

Es gelten alle relevanten Angaben der Bezugsbestätigung unter der Berücksichtigung der aktuellen Produktbezeichnung Kobil-Trust OCSP Version 3.6.1 Release 1111.

2.2 Beschreibung der evaluierten Sicherheitsfunktionalität

Es gelten alle relevanten Angaben der Bezugsbestätigung unter der Berücksichtigung der aktuellen Produktbezeichnung Kobil-Trust OCSP Version 3.6.1 Release 1111.

[3] Evaluierungsgegenstand (Engl.: TOE)

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Es gelten alle relevanten Angaben der Bezugsbestätigung.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen durch den Produktbetreiber / Produktbenutzer gewährleistet sind:

3.2.1 Anforderungen an die technische Einsatzumgebung

Es gelten alle relevanten Angaben der Bezugsbestätigung.

Für die folgende Komponente der Einsatzumgebung wurde eine Nachtragsbestätigung ausgestellt:

Komponente	Hardware / Version	Bestätigung nach SigG
SEE	„Signaturerstellungseinheit (SEE) TCOS 3.0 Signature Card, Version 1.1", Ausprägung „Signature Card 3.0M, Version 1.0"	Nachtrag #2 vom 20.03.2014 zur Bestätigung TUVIT.93146.TE.12.2006 Gültig bis 30.06.2016 (abhängig vom im Betrieb verwendeten Hash-Verfahren)

3.2.2 Anforderungen an die organisatorische und administrative Einsatzumgebung

Es gelten alle relevanten Angaben der Bezugsbestätigung.

3.2.3 Nutzung und Abgrenzung des Produkts

Es gelten alle relevanten Angaben der Bezugsbestätigung.

3.3 Algorithmen und zugehörige Parameter im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2

Die folgenden Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 werden vom Produkt „Kobil-Trust OCSP Version 3.6.1 Release 1111“ für die Berechnung von Hashwerten bereitgestellt:

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[4]	Gültigkeit gem. aktuellen Festlegungen[4]
SHA-224	n.a.	n.a.	geeignet	bis Ende 2015
SHA-256	n.a.	n.a.	geeignet	bis Ende 2020
SHA-384	n.a.	n.a.	geeignet	bis Ende 2020
SHA-512	n.a.	n.a.	geeignet	bis Ende 2020

Alle Algorithmen der SHA-Familie werden nur im Modus „full-length message digest“ verwendet.

3.4 Prüfstufe und Mindeststärke der Sicherheitsfunktionen

Es gelten alle relevanten Angaben der Bezugsbestätigung.

[4] vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 13./21. Januar 2014, veröffentlicht am 20.02.2014 im Bundesanzeiger.

3.5 Gültigkeit der Bestätigung

Die Gültigkeitsdauer der vorliegenden Bestätigung insgesamt ist auf das nächstliegende Gültigkeitsdatum beschränkt, das sich aus der Gültigkeit der Produktbestätigung und der maximalen Dauer eines bestätigungskonformen Betriebs des Produkts ergibt. So ist **die Gültigkeit dieser Bestätigung zeitlich beschränkt, und zwar bis 30.06.2016**. Für weitere Einzelheiten s. Abschn. 3.5.1 und 3.5.2 weiter unten.

Die Gültigkeit der Bestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

3.5.1 Gültigkeit der Produktbestätigung

Diese Produktbestätigung ist u.a. auf Grundlage

(i) der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung (s. Abschn. 3.4) und

(ii) der Angaben der aktuell gültigen „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 13./21. Januar 2014, veröffentlicht am 20.02.2014 im Bundesanzeiger“

zustande gekommen, woraus sich die Bestimmung ihrer Gültigkeit ergibt.

In Bezug auf die Gültigkeitsdauer der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung – unter Berücksichtigung der bei der Implementierung des EVG verwendeten Technologie und der beabsichtigten Einsatzumgebung (Software, die im geschützten Einsatzbereich ausgeführt wird) – agiert die Bestätigungsstelle auf der **Annahme**, dass diese Ergebnisse **7 Jahre** ab dem Zeitpunkt des Evaluierungsabschlusses (20.12.2013) gültig bleiben.

In Bezug auf Verwendung der Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 ergibt sich ihre Gültigkeitsdauer aus dem Abschnitt 3.3, wobei stets zu berücksichtigen ist, ob ein Algorithmus im Betrieb tatsächlich verwendet wird, und wenn Ja, für welche Dienste/Funktionen er verwendet wird.

Die Gültigkeitsdauer der vorliegenden Produktbestätigung ist dann auf das nächstliegende Gültigkeitsdatum beschränkt. So ist die Gültigkeit dieser Produktbestätigung zeitlich beschränkt, und zwar bis 20.12.2020.

Die Gültigkeit der Produktbestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

3.5.2 Maximale Dauer eines bestätigungskonformen Betriebs des bestätigten Produkts

Ein bestätigungskonformer Betrieb des EVGs ist an Erfüllung aller Bedingungen aus Abschn. 3.2 „Einsatzbedingungen“ gebunden. Da der Betrieb des EVGs die Verfügbarkeit mindestens einer SigG-bestätigten SSEE benötigt (vgl. Abschn. 3.2.1), ist ihr bestätigungskonformer Betrieb an die Gültigkeit der Produktbestätigungen (bzw. Herstellererklärungen, solange SigG-konform) der eingesetzten SSEEs gebunden.

Daraus ergibt sich die maximal mögliche Dauer **eines bestätigungskonformen Betriebs** des EVGs, und zwar wie folgt:

a) Das Gültigkeitsdatum der Bestätigungen des in Abschn. 3.2.1 aufgelisteten SSEEs ist 30.06.2016 (Nachtrag #2 vom 20.03.2014 zu TUVIT.93146.TE.12.2006).

Die **maximal** mögliche **Dauer eines bestätigungskonformen Betriebs des EVGs** ist auf das nächstliegende Gültigkeitsdatum beschränkt, nämlich auf 30.06.2016.

Die maximal mögliche Dauer eines bestätigungskonformen Betriebs des EVGs kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

Ende der Bestätigung.

Nachtrag Nr. 1 zu T-Systems.02247.TE.12.2013

Hrsg.: T-Systems GEI GmbH
Adresse: Vorgebirgsstr. 49, 53119 Bonn
Telefon: +49-(0)228-9841-0
Fax: +49-(0)228-9841-6000
Web: www.t-systems-zert.com
security.t-systems.com/