Nachtrag Nr. 4 zur Sicherheitsbestätigung

T-Systems.02186.TU.03.2007

FlexiTrust 3.0 - Release 0650

FlexSecure GmbH

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. 2 und 15 Signaturverordnung[2]

Nachtrag Nr. 4 zur Bestätigung
T-Systems.02186.TU.03.2007 vom 05.04.2007

T-Systems GEI GmbH
- Zertifizierungsstelle -

Rabinstr.8, 53111 Bonn

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

technische Komponente für Zertifizierungsdienste
„FlexiTrust 3.0 - Release 0650“

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

Bonn, den 04.03.2008

(Dr. Heinrich Kersten)

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 Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. Jahrgang 2007, Teil I S. 179)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Art. 2 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 04. Januar 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 1)

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

1.1 Handelsbezeichnung

Technische Komponente für Zertifizierungsdienste „FlexiTrust 3.0 - Release 0650“

Dieser Nachtrag Nr. 4 bezieht sich auf den Patch-Level "20070911".

1.2 Auslieferung

Keine Änderung gegenüber dem bisherigen Auslieferungsverfahren.

1.3 Lieferumfang

Keine Änderung gegenüber dem bisherigen Lieferumfang. Das Dokument „FlexiTRUST Version 3.0 Release 0650 – Konfigurationsliste“, Version 1.9 vom 04.03.2008 beschreibt die aktuellen Versionsstände der ausgelieferten Komponenten.

1.4 Hersteller

FlexSecure GmbH

Industriestraße 12

64297 Darmstadt

2. Beschreibung der Änderungen

Gegenüber der

- Bestätigung T-Systems.02186.TU.03.2007 vom 05.04.2007,
- der Nachtragsbestätigung Nr. 1 vom 10.05.2007,
- der Nachtragsbestätigung Nr. 2 vom 14.08.2007 und
- der Nachtragsbestätigung Nr. 3 vom 07.12.2007

wurden beim aktuellen Patch 20070911 zwei Verhaltensweisen der Software geändert:

1. Die Verhaltensweise, dass bei einer Sperrung mit einer gewissen Wahrscheinlichkeit das Datum thisUpdate der Sperrliste eine Sekunde älter ist, als das neuste Sperrdatum (revocationDate) eines gesperrten Zertifikats.
2. Die Verhaltensweise, dass vorbefüllte Anträge an der Eingabeschnittstelle der RA nicht gelöscht werden können, obwohl diese Funktionalität so vorgesehen ist.

Hinsichtlich der Übersignatur-Komponente FlexiTrust TSS, die der Erzeugung qualifizierter Zeitstempel von Daten dient, deren Beweiswert langfristig gesichert werden soll („Übersignatur“ gemäß §17 SigV), sind folgende Anpassungen vorgenommen worden:

3. Änderung der Policy-OID im TimeStampInfo der Übersignatur, Verwendung des SigningCertifcateV2-Attribut gemäß RFC5035 in der SignerInfo der Übersignatur (mit Angabe des SHA512), Anpassungen im Workflow (nur einmaliges Einlesen des Signaturzertifikats von der SSEE).

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Siehe Bezugsbestätigung T-Systems.02186.TU.03.2007 vom 05.04.2007.

Zusätzlich erfüllt die Übersignatur-Komponente die Vorgaben des §17 SigV.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Keine Änderung an der technischen Einsatzumgebung.

b) Einbindung in die Hard- und Softwareumgebung

Alle Vorgaben hinsichtlich der Installation der Komponente aus der Sicherheitsbestätigung T-Systems.02186.TU.03.2007 sowie den dazu gehörenden Nachträgen 1, 2 und 3 sind einzuhalten.

c) Nutzung des Produktes

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

- Alle Bedingungen aus der Sicherheitsbestätigung T-Systems.02186.TU.03.2007 sowie den dazu gehörenden Nachträgen 1, 2 und 3 sind einzuhalten.

Mit Auslieferung von FlexiTrust 3.0 - Release 0650 Patch 20070911 ist der Betreiber auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Hinsichtlich der verwendeten Algorithmen gelten die Aussagen der ursprünglichen Bestätigung und der Nachtragsbestätigungen 1, 2 und 3. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht bei Verwendung der angegebenen Hash-Algorithmen mindestens (s. Bundesanzeiger Nr. 19, S. 376 vom 05. Februar 2008) bis:

RIPEMD-160: Ende 2010;
ausschließlich zur Prüfung qualifizierter Zertifikate: Ende 2014

SHA-1: 30.06.2008,
Erzeugung qualifizierter Zertifikate: Ende 2009;
Erzeugung qualifizierter Zertifikate bei ≥20 Bit Entropie der Seriennummer: Ende 2010;
ausschließlich zur Prüfung qualifizierter Zertifikate: Ende 2014

SHA-224, SHA-256, SHA-384, SHA-512: Ende 2014.

3.4 Prüfstufe und Mechanismenstärke

Die technische Komponente für Zertifizierungsdienste FlexiTrust 3.0 - Release 0650 Patch 20070911 wurde gemäß §15 (7) SigG hinreichend geprüft:

- Die Änderungen 1 und 2 (s. Kapitel 2) wurden gemäß der Vorgaben der Common Criteria nach der Prüfstufe EAL3 mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV behandelt. Die eingesetzten Sicherheitsmechanismen wurden unverändert mit „hoch“ bewertet.
  Diese Prüfung ist im Bericht „Evaluierung FlexiTrust V3.0 R0650 Patch 20070911: Observation Report #01: Bewertung des Impact Analysis Reports“, Version 1.0 vom 04.03.2008 dokumentiert.
- Für die Änderung 3 (s. Kapitel 2) wurden nach Vorgaben der Bundesnetzagentur die gemäß Nachtrag Nr. 3 durchgeführten Prüfungen wiederholt.
  Diese Prüfung ist im Bericht „Prüfung FlexiTrust-TSS V3.0 R0650 Patch 20070911, Test Report #01, Unabhängige Tests“, Version 1.1 vom 29.02.2008 dokumentiert.

Ende des Nachtrags Nr. 4

Nachtrag Nr. 4 zur Bestätigung
T-Systems.02186.TU.03.2007

Hrsg.:	T-Systems GEI GmbH
Adresse:	Rabinstr.8, 53111 Bonn
Telefon:	+49-(0)228-9841-0
Fax:	+49-(0)228-9841-60
Web:	www.t-systems.com/ict-security
	www.t-systems-zert.com