Nachtrag Nr. 3 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. 3 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 folgt erweitert wurde:

- Einbeziehung der Komponente FlexiTrust TSS zur Erzeugung von „Übersignaturen“.

Bonn, den 07.12.2007

(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. 3 bezieht sich auf den Patch-Level "20070910".

1.2 Auslieferung

Keine Änderung gegenüber dem bisherigen Auslieferungsverfahren.

1.3 Lieferumfang

Keine Änderung: Die Komponente FlexiTrust TSS zur Erzeugung von Übersignaturen war bereits im bisherigen Lieferumfang enthalten (jedoch nicht in die Sicherheitsbestätigung einbezogen worden).

Folgende Dokumentation ist maßgebend:

- Benutzerhandbuch Übersignatur der Zertifizierungsinstanz der Regulierungsbehörde für Telekommunikation und Post (RegTP), Version 1.4, 15.02.2004

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 sowie der Nachtragsbestätigung Nr. 1 vom 10.05.2007 und der Nachtragsbestätigung Nr. 2 vom 14.08.2007, haben sich beim Patch 20070910 folgende Änderungen ergeben:

In die Sicherheitsbestätigung wird die Komponente FlexiTrust TSS einbezogen, die der Erzeugung qualifizierter Zeitstempel von Daten dient, deren Beweiswert langfristig gesichert werden soll („Übersignatur“ gemäß §17 SigV).

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 und 2 sind einzuhalten.

Die Einträge in der Konfigurationsdatei FlexTSS.ini sind auf Korrektheit zu prüfen.

Nach der Installation von FlexiTrust TSS müssen folgende Verzeichnisse und Dateien vorhanden sein, bei den Dateien ist die Übereinstimmung mit den angegebenen Hashwerten zu überprüfen:

Bezeichnung	Hashwert
/usr/local/FlexiTRUST-TSS drwxr-xr-x secadmin flexi directory	-
/usr/local/FlexiTRUST-TSS/certs drwxr-x--- secadmin flexi directory	-
/usr/local/FlexiTRUST-TSS/FlexTSS.ini -rwxr-x--- secadmin flexi	a52eafa17cba8c09185583fe8575d73e
/usr/local/FlexiTRUST-TSS/initTssPinShares.sh -rwxr-x--- secadmin flexi	3f61a202e6dffd0bbe8834b42ff8bd5e
/usr/local/FlexiTRUST-TSS/keystore drwxr-x--- secadmin flexi directory	–
/usr/local/FlexiTRUST-TSS/lib drwxr-x--- secadmin flexi directory	–
/usr/local/FlexiTRUST-TSS/lib/admin.jar -rwxr-xr-x secadmin flexi	5f11a395d4447e3038478a623015f6cd

/usr/local/FlexiTRUST-TSS/lib/codec.jar -rwxr-xr-x secadmin flexi	417345485e12067ce9ed47922f989561
/usr/local/FlexiTRUST-TSS/lib/FlexiProvider.jar -rwxr-xr-x secadmin flexi	45faad51c0499eb3c584244c09a26e5f
/usr/local/FlexiTRUST-TSS/lib/fs_util.jar -rwxr-xr-x secadmin flexi	adc309da982a7a1d10684b412f7f08ef
/usr/local/FlexiTRUST-TSS/lib/p11.jar -rwxr-xr-x secadmin flexi	09783a33ffd09e0c977aebc291f2523c
/usr/local/FlexiTRUST-TSS/lib/pinsharing.jar -rwxr-xr-x secadmin flexi	9926c7c0a5fa1b138210ad1eb830c3fe
/usr/local/FlexiTRUST-TSS/lib/tss.jar -rwxr-xr-x secadmin flexi	abbc8757aedc751b10700d12bdf40aea
/usr/local/FlexiTRUST-TSS/reshareTssPinShares.sh -rwxr-x--- secadmin flexi	64fcf479483248965edb217c0a7ade57
/usr/local/FlexiTRUST-TSS/startTSS.sh -rwxr-x--- secadmin flexi	e503aebd3b3ec985de09df100403c239
/usr/local/FlexiTRUST-TSS/Test.txt -rw-r--r-- secadmin flexi	18e21ced7204992b60306d7a53b28401
/usr/local/FlexiTRUST-TSS/tssIn drwxr-x--- secadmin flexi directory	-
/usr/local/FlexiTRUST-TSS/tssOut drwxr-x--- secadmin flexi directory	-

Die Übersignaturkomponente FlexiTrust TSS benötigt eine Zeitquelle, die die gültige gesetzliche Zeit bereitstellt, eine sicherheitsbestätigte SSEE sowie einen entsprechenden Kartenleser.

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 und 2 sind einzuhalten.
- Um ein Verlust der im Ausgabeverzeichnis befindlichen Zeitstempel durch Überschreiben zu verhindern, sind nach jeder Ausführung der Übersignatur-Komponente alle Dateien im Ausgabeverzeichnis TSS_OUT zu sichern; das Verzeichnis ist anschließend zu leeren.

Mit Auslieferung von FlexiTrust 3.0 - Release 0650 Patch 20070910 ist der Betreiber auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Es gelten die Aussagen der früheren Bestätigungen mit folgender Ergänzung: Bei der Erzeugung der Zeitstempel durch FlexiTrust TSS werden folgende Hashfunktionen bereitgestellt: SHA-1, RIPEMD-160, SHA-224, SHA-256, SHA-384 und SHA-512.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht mindestens (s. Bundesanzeiger Nr. 69, S. 3759 vom 12. April 2007) bis:

- RIPEMD-160: Ende 2010
- SHA-1: (Anwendung nur bei qualifizierten Zertifikaten:) Ende 2010, (sonst:) Ende 2009
- SHA-224, SHA-256, SHA-384, SHA-512: Ende 2011.

3.4 Prüfstufe und Mechanismenstärke

Die Übersignaturkomponente FlexiTrust TSS von FlexiTrust 3.0 - Release 0650 Patch 20070910 wurde gemäß §15 (7) SigG hinreichend geprüft: Die Prüfung umfasste nach Vorgaben der Bundesnetzagentur Tests zur korrekten Funktion, um festzustellen, ob der Untersuchungsgegenstand seiner Spezifikation entspricht, sowie Missbrauchstests auf Grundlage der Benutzerdokumentation, um festzustellen, ob ein sicherer Betrieb des Untersuchungsgegenstands in seiner Einsatzumgebung möglich ist.

Die Prüfung ist im Bericht „Prüfung FlexiTrust-TSS V3.0 R0650 Patch20070910, Test Report #01, Unabhängige Tests“ vom 29.11.2007 (und mitgeltenden Anlagen) dokumentiert.

Ende des Nachtrags Nr. 3

Nachtrag Nr. 3 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