Nachtrag Nr. 2 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. 2 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:

1. Hashverfahren für die CertificateHash-Extension sind konfigurierbar.
2. Nutzung von SSEE des Typs TCOS 2.0.
3. Einführung eines Patch-Levels.

Bonn, den 14.08.2007

(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] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG), zuletzt geändert durch Art. 1 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 04. Januar 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 1)

[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)

Der Nachtrag Nr. 2 zur Bestätigung T-Systems.02186.TU.03.2007 besteht aus 9 Seiten.

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. 2 bezieht sich auf den Patch-Level "Patch20070724".

Die bisherigen Fassungen der technischen Komponente sind *nicht* mit einem Patch-Level gekennzeichnet.

1.2 Auslieferung

Die technische Komponente wird vom Hersteller durch persönliche Übergabe an den Betreiber ausgeliefert. Die Software-Komponenten werden auf einmal beschreibbaren Medien (finalisiert) gespeichert, die in versiegelten Umschlägen bereit gestellt werden. Diese Umschläge werden in der Einsatzumgebung des Betreibers im Beisein des Herstellers geöffnet; anhand der in einer Liste mitgelieferten Hashwerte kann die Integrität der Code-Dateien festgestellt werden.

Die genauen Auslieferungsprozeduren sind in "FlexiTrust 3.0 R0650 – Auslieferungsprozeduren“, Version 1.3 vom 31. 07. 2007 beschrieben.

1.3 Lieferumfang

Folgende Software-Komponenten von FlexiTrust V3.0 R0650 (Patch20070724) werden ausgeliefert:

1. RA-/CA-/IS-Komponente Zertifizierungsdienst
2. RA-/CA-/IS-Komponente Revokationsdienst
3. OCSP-Komponente
4. ImpEx-Komponente
5. Administrationswerkzeuge PIN-/PASS-Sharing
6. SigG-PKCS#11 Funktionsbibliothek[3]
   (Betrieb-1024: libkpkcs11regtp.so; Betrieb-2048: libkpkcs11bna.so)
7. PKCS#10-Request Generator[4]

---

[3] Diese Komponente wird in zwei Varianten ausgeliefert, und zwar je eine Bibliothek für die Konfigurationen „Betrieb-1024“ und „Betrieb-2048“, vgl. Abschnitt 2, Nr. 2 dieser Bestätigung.

[4] Diese Komponente wird nur benötigt, falls TCOS2.0-Karten zum Einsatz kommen.

Die einzelnen Software-Bestandteile und die genauen Versionsstände sind im Dokument „FlexSecure GmbH: FlexiTrust 3.0 R0650 – Konfigurationsliste, Version 1.7, 13. 08. 2007, enthalten.

Folgende Handbücher werden für FlexiTrust V3.0 R0650 (Patch20070724) ausgeliefert:

1. FlexiTrust 3.0 R0650 – Administrationshandbuch CA für FlexiTrust 3.0 - Release 0650, Version 3.0, 21.03.2007
2. FlexiTrust 3.0 R0650 – Administrationshandbuch PIN-Sharing für FlexiTrust 3.0 - Release 0650, Version 2.3, 27.03.2007
3. FlexiTrust 3.0 R0650 – Administrationshandbuch PASS-Sharing für FlexiTrust 3.0 - Release 0650, Version 2.1, 27.03.2007
4. FlexiTrust 3.0 R0650 – Administrationshandbuch OCSP Responder für FlexiTrust 3.0 - Release 0650, Version 1.8, 27.03.2007
5. FlexiTrust 3.0 R0650 – Administrationshandbuch des Teilsystems RA für FlexiTrust 3.0 - Release 0650, Version 1.2, 27.03.2007
6. FlexiTrust 3.0 R0650 – Administratoren Handbuch – Infrastructure Services (IS) für FlexiTrust 3.0 - Release 0650, Version 1.6, 27.03.2007
7. FlexiTrust 3.0 R0650 – Konfigurationsdateien – Infrastructure Services (IS) für FlexiTrust 3.0 - Release 0650, Version 1.5, 27.03.2007
8. FlexiTrust 3.0 R0650 – Administrator-Handbuch – ImpEx für FlexiTrust 3.0 - Release 0650, Version 2.5, 27.03.2007
9. FlexiTrust 3.0 R0650 – Benutzerhandbuch des Teilsystems RA für FlexiTrust 3.0 - Release 0650, Version 2.0, 27.03.2007
10. FlexiTrust 3.0 R0650 – Benutzerhandbuch Produktions CA für FlexiTrust 3.0 - Release 0650, Version 2.0, 27.03.2007
11. FlexiTrust 3.0 R0650 – Benutzerhandbuch Revokations CA für FlexiTrust 3.0 - Release 0650, Version 1.9, 27.03.2007
12. FlexiTrust 3.0 R0650 – Benutzerhandbuch – ImpEx für FlexiTrust 3.0 - Release 0650, Version 2.6, 27.03.2007
13. FlexiTrust 3.0 R0650 – Benutzerhandbuch – OCSP Responder für FlexiTrust 3.0 - Release 0650, Version 2.2, 27.03.2007
14. FlexiTrust 3.0 R0650 – Benutzerhandbuch – Infrastructure Services (IS) für FlexiTrust 3.0 - Release 0650, Version 1.6, 27.03.2007
15. FlexiTrust 3.0 R0650 – Korrekturen und Ergänzungen zu den Administrationshandbüchern, Version 1.0, 27.03.2007
16. FlexiTrust 3.0 R0650 Patch 20070724 Ergänzungsblatt zu den Administrationshandbüchern bzgl. CertificateHashExtension und Betriebsmodus, Version 1.3, 03.08.2007
17. FlexiTrust 3.0 R0650 Patch 20070724 Ergänzungsblatt zu den Benutzerhandbüchern bzgl. CertificateHashExtension und Betriebsmodus, Version 1.1, 10.08.2007

18. KOBIL Smart Key SigG-PKCS#11 Modul – Benutzerdokumentation, Version 1.1, 19.02.2007[5].
19. Dokumentation für das von der KOBIL Systems GmbH entwickelte Werkzeug PKCS#10-Request Generator[6].

1.4 Hersteller

FlexSecure GmbH

Industriestraße 12

64297 Darmstadt

2. Beschreibung der Änderungen

Gegenüber dem Leistungsumfang der Komponente, beschrieben in der Bestätigung T-Systems.02186.TU.03.2007 vom 05.04.2007 sowie der Nachtragsbestätigung Nr. 1 vom 10.05.2007, haben sich beim Patch-Level "Patch20070724" folgende Änderungen ergeben:

1) Der OCSP-Responder von FlexiTrust 3.0 Release 0650 liefert bei einer Auskunft zu einem ihm bekannten Zertifikat eine CertificateHash-Extension mit. Diese beinhaltet den über das angefragte Zertifikat gebildeten Hashwert als Beweis der Existenz.
   Im früheren Versionen von FlexiTrust 3.0 Release 0650 wurde als Hashverfahren SHA-512 verwendet. Mit dem neuen Patch-Level ist eine Konfigurationsmöglichkeit gegeben, d. h. in Abhängigkeit eines Eintrags in der Konfigurationsdatei des OCSP-Responders kann das Hashverfahren aus SHA-1, RIPEMD-160, SHA-224, SHA-256, SHA-384 und SHA-512 gewählt werden. Der Konfigurationseintrag wird bei einem Neustart des OCSP-Responders wirksam.

2) In der Bestätigung T-Systems.02186.TU.03.2007 vom 05.04.2007 wurden als zulässige SSEE ausschließlich SigG-konform personalisierte Signaturkarten vom Typ TCOS 3.0 SignatureCard Version 1.1 angegeben; diese werden von einer dedizierten PKCS#11-Bibliothek angesteuert. Bei dem hier beschriebenen Patch-Level wird diese Konfiguration als "Betrieb2048" bezeichnet.
   Durch Austausch der PKCS#11-Bibliothek gegen eine andere[7] evaluierte Biblio-

---

[5] Es handelt sich hier um die Dokumentation der PKCS#11-Bibliothek für die Konfiguration „Betrieb2048“. Für die beim „Betrieb1024“ zur Anwendung kommende PKCS#11-Bibliothek wird keine Benutzer-Dokumentation zur Verfügung gestellt.

[6] Diese Dokumentation wird nur benötigt, falls TCOS2.0-Karten zum Einsatz kommen.

[7] Gemäß dem maßgebenden Security Target Version 1.1.6 vom 22.02.2007 zu "FlexiTrust 3.0 - Release 0650", Abschnitt 2.4, ist ein solcher Austausch zulässig.

thek[8] des gleichen Herstellers können mit dem hier beschriebenen Patch-Level für die Sperr-CA und den OCSP-Dienst auch SSEE vom Typ TCOS 2.0 zur Anwendung kommen. Diese Konfiguration wird als "Betrieb1024" bezeichnet.

Die Auswahl der beiden alternativen Betriebsarten erfolgt durch Setzen eines Links auf die gewünschte PKCS#11-Bibliothek.

Die mit dem System ausgelieferte Dokumentation wurde hinsichtlich der dargestellten Änderungen und deren Handhabung um zusätzliche Blätter zu den Administrationshandbüchern und Benutzerhandbüchern ergänzt.

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.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die technische Komponente für Zertifizierungsdienste FlexiTrust 3.0 - Release 0650 (Patch20070724) wurde auf der Basis der folgenden Konfiguration evaluiert:

- Workstations SunFire 280R (Verzeichnisdienst) und SunBlade 150 (alle anderen Dienste) mit Betriebssystem SUN Solaris, Solaris 8 Rel. 2/02, installierter Patch 112438
- Laufzeitumgebung SUN Java JDK/JRE 1.4.2_13
- Applikationsserver / Servlet-Container Apache Tomcat 4.1.27
- Applikationsserver CA JBoss 3.0.6
  - WebServer Jetty 4.2.26
- Applikationsserver OCSP JBoss 3.2.8
  - Applikationsserver / Servlet-Container Tomcat 5.0.30

[8] PKCS#11-Bibliothek von FlexiTrust 3.0 Release 0421, bestätigt am 03.11.2004 unter der Bestätigungsnummer T-Systems.02126.TE.11.2004.

- Prozessdatenbank MySQL 3.23.57
- Aktivierungsdatenbank OpenLDAP 2.0.27
  - Verschlüsselung OpenSSL 0.9.8d
  - Interne DB BerkeleyDB 3.1.17
- Hashwerte – Prüfung der Installation OpenSSL 0.9.7b
- SigG-konform personalisierte und bestätigte Signaturkarten vom Typ TCOS 3.0 SignatureCard Version 1.1[9]
- Telesec Signaturkarte PKS Card 3.0 (mit TCOS 2.0 Release 3)[10] (nur im Zusammenhang mit der Konfiguration "Betrieb1024"),
- SigG-konformes Chipkartenterminal KAAN Advanced, Firmware Version 1.02, Hardware Version K104R3

Diese Sicherheitsbestätigung für FlexiTrust 3.0 - Release 0650 (Patch20070724) gilt deshalb ausschließlich für den Einsatz im Rahmen der oben beschriebenen Konfiguration. Soll ihr Einsatz mit einer geänderten Konfiguration erfolgen, so ist die Bestätigungsstelle vorab zu informieren und einzubeziehen.

b) Einbindung in die Hard- und Softwareumgebung

Die technische Komponente für Zertifizierungsdienste wird vom Hersteller gemäß Abschnitt 1.2 ausgeliefert.

Vor Installation von FlexiTrust 3.0 - Release 0650 (Patch20070724) ist zu prüfen, ob

- die vorgesehene Einbindung von FlexiTrust 3.0 - Release 0650 (Patch20070724) in das Trust Center der Bundesnetzagentur mit deren Sicherheitskonzept übereinstimmt,
- die Einhaltung der oben genannten Konfiguration bzw. technischen Einsatzumgebung gewährleistet ist,
- das spezifizierte Auslieferungsverfahren für FlexiTrust 3.0 - Release 0650 (Patch20070724) eingehalten worden ist,
- die Originaldatenträger korrekt (mit Patch-Level) beschriftet sind,
- die Hashwerte der auf dem Originaldatenträger enthaltenen Dateien korrekt sind[11],
- die Integrität jeder der beiden möglicherweise bereits installierten PKCS#11-Bibliotheken (Nr. 6 aus Abschnitt 1.3 auf der Seite 2) gegeben ist.

---

9 Bestätigung TÜVIT.93146.TE.12.2006

10 Bestätigung TÜVIT.09339.TE.12.2000 (Nachtrag 2).

11 Ein Werkzeug zur Prüfung der Integrität der ausgelieferten Dateien gehört nicht zum Lieferumfang von FlexiTrust 3.0 - Release 0650 (Patch20070724).

Diese Prüfungen und ihre Ergebnisse sind aufzuzeichnen.

Die Inbetriebnahme von FlexiTrust 3.0 - Release 0650 (Patch20070724) und jede Wiederinbetriebnahme, die eine Neuinstallation erfordert, müssen durch fachkundiges Personal des Herstellers erfolgen.

Jeder Konfigurationswechsel zwischen „Betrieb1024“ und „Betrieb2048“ muss durch fachkundiges Personal des Herstellers erfolgen, ebenso die dauerhafte Deaktivierung von „Betrieb1024“.

Die technische Komponente für Zertifizierungsdienste FlexiTrust 3.0 - Release 0650 (Patch20070724) darf nur in Verbindung mit vertrauenswürdigen, diese nutzende Anwendungen eingesetzt werden. Dies beinhaltet obligatorische und umfassende Tests dieser Anwendungen und eine Spezifikation der Sicherheitsziele, die diese Anwendungen abdecken.

Anwendungen, die die technische Komponente für Zertifizierungsdienste „FlexiTrust 3.0 - Release 0650“ nutzen, sind nicht Gegenstand dieser Bestätigung.

c) Nutzung des Produktes

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

- Die technische Komponente für Zertifizierungsdienste FlexiTrust 3.0 - Release 0650 (Patch20070724) wurde für den geschützten Einsatzbereich[12] des Trust Centers der Bundesnetzagentur evaluiert. Eine Übertragung der Evaluationsergebnisse auf einen anderen Einsatzbereich macht eine Re-Evaluation erforderlich.
- Es ist insbesondere vertrauenswürdiges und fachkundiges Personal einzusetzen. Die Administration von FlexiTrust 3.0 - Release 0650 (Patch20070724) und der beteiligten Systeme hat im Vier-Augen-Prinzip zu erfolgen.
- Es ist sicherzustellen, dass auf der von FlexiTrust 3.0 - Release 0650 (Patch20070724) benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Bei der Konfiguration von FlexiTrust 3.0 - Release 0650 (Patch20070724) mit mehr als einem aktiven Revokationssystem müssen organisatorische Maßnahmen getroffen und im Sicherheitskonzept dargelegt werden, die eine ausreichende Umschaltzeit zwischen den Revokationssystemen gewährleisten. Die Untergrenze für die Umschaltzeit ist bei der Konfiguration durch Messung zu bestimmen.

---

12 "Geschützter Einsatzbereich" im Sinne von "Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten", Version 1.4, 19.07.2005.

- Von FlexiTrust 3.0 - Release 0650 (Patch20070724) erzeugte Meldungen sind regelmäßig und zeitnah zu kontrollieren und auszuwerten, um insbesondere die Einhaltung der gesetzlichen Verfügbarkeitsanforderungen sicherzustellen.
- Die Systemzeiten der Systeme, auf denen FlexiTrust 3.0 - Release 0650 (Patch20070724) installiert ist, soll wöchentlich mit der gesetzlichen Zeit abgeglichen werden.
- Mit Identifikationsmerkmalen, die an Signaturerstellungseinheiten weitergereicht oder die im Zusammenhang mit Sperranträgen benutzt werden, ist vertraulich umzugehen, insbesondere seitens handelnder Personen und beteiligter Anwendungen.
- Um eine Speicherung von Identifikationsdaten bei der Aktivierung von sicheren Signaturerstellungseinheiten zu vermeiden, ist zu gewährleisten, dass während der Verarbeitung von Identifikationsdaten das Swapping auf den betreffenden Systemen deaktiviert ist.
- Die Konfiguration "Betrieb1024" ist in Anbetracht der Beschränkungen bei RSA-1024 nur bis zum 31.12.2007 gültig und muss dann dauerhaft deaktiviert werden.
- In das Sicherheitskonzept sind Maßnahmen aufzunehmen, die sicherstellen, dass im „Betrieb2048“ ausschließlich die genannten TCOS 3.0 Karten und im „Betrieb1024“ ausschließlich die genannten TCOS 2.0 Karten zum Einsatz kommen, und somit einer Verwechslung vorgebeugt wird. Dabei sind die in den Ergänzungsblättern zum Administrations- und Benutzerhandbuch dargelegten Informationen über Fehlerzustände und deren Behebung einzubeziehen.

Mit Auslieferung von FlexiTrust 3.0 - Release 0650 (Patch20070724) ist der Betreiber auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Die technische Komponente für Zertifizierungsdienste „FlexiTrust 3.0 - Release 0650“ verwendet folgende Algorithmen:

- Für die Erzeugung und Prüfung elektronischer Signaturen werden folgende Hashfunktionen bereitgestellt: RIPEMD-160, SHA-1, SHA-224, SHA-256, SHA-384, 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.

Die Gültigkeit der vorliegenden Sicherheitsbestätigung ist somit abhängig von den genutzten Hash-Algorithmen[13] und reicht für die Konfiguration „**Betrieb2048**“ jeweils mindestens bis zu den oben genannten Zeitpunkten. Eine Verlängerung der Gültigkeit kann erfolgen, wenn zu diesen Zeitpunkten keine Hinderungsgründe hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

Bei Nutzung der Konfiguration "**Betrieb1024**" ist die vorliegende Sicherheitsbestätigung nur bis zum 31.12.2007 gültig.

3.4 Prüfstufe und Mechanismenstärke

Die technische Komponente für Zertifizierungsdienste FlexiTrust 3.0 - Release 0650 (Patch20070724) wurde erfolgreich nach der Prüfstufe EAL3 der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert. Die Evaluierung erfolgte in Form einer Re-Evaluierung.

Für die eingesetzten Sicherheitsmechanismen wurde die Stärke "hoch" bestätigt.

Ende des Nachtrags Nr. 2

[13] „FlexiTrust 3.0 - Release 0650“ erlaubt es in der Konfiguration „Betrieb-2048“, einzelne Algorithmen zu aktivieren bzw. zu deaktivieren und damit jeweils nur aktuell gültige Algorithmen zur verwenden.

Nachtrag Nr. 2 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