T · · Systems ·

Sicherheitsbestätigung und Bericht

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]

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 die

technische Komponente für Zertifizierungsdienste
„FlexiTrust 3.0 - Release 0650“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02186.TU.03.2007

Bonn, den 05.04.2007

(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. 3 (9) des Zweiten Gesetzes zur Neuregelung des Energiewirtschaftsgesetzes (EnWG) vom 07. Juli 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 42)

[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)

Die Bestätigung zur Registrierungsnummer 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“

Kurzform: "FlexiTrust V3.0 R0650"

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 V3.0 R0650 – Auslieferungsprozeduren", Version 1.2, 27.03.2007 beschrieben.

1.3 Lieferumfang

Ausgelieferte Software-Komponenten von FlexiTrust V3.0 R0650:

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 / P11-Komponente
7. PKCS#10-Request Generator[3]

Ausgelieferte Handbücher für FlexiTrust V3.0 R0650:

1. FlexiTrust V3.0 R0650 – Administrationshandbuch CA für FlexiTrust 3.0 - Release 0650, Version 3.0, 21.03.2007
2. FlexiTrust V3.0 R0650 – Administrationshandbuch PIN-Sharing für FlexiTrust 3.0 - Release 0650, Version 2.3, 27.03.2007

---

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

3. FlexiTrust V3.0 R0650 – Administrationshandbuch PASS-Sharing für FlexiTrust 3.0 - Release 0650, Version 2.1, 27.03.2007
4. FlexiTrust V3.0 R0650 – Administrationshandbuch OCSP Responder für FlexiTrust 3.0 - Release 0650, Version 1.8, 27.03.2007
5. FlexiTrust V3.0 R0650 – Administrationshandbuch des Teilsystems RA für FlexiTrust 3.0 - Release 0650, Version 1.2, 27.03.2007
6. FlexiTrust V3.0 R0650 – Administratoren Handbuch – Infrastructure Services (IS) für FlexiTrust 3.0 - Release 0650, Version 1.6, 27.03.2007
7. FlexiTrust V3.0 R0650 – Konfigurationsdateien – Infrastructure Services (IS) für FlexiTrust 3.0 - Release 0650, Version 1.5, 27.03.2007
8. FlexiTrust V3.0 R0650 – Administrator-Handbuch – ImpEx für FlexiTrust 3.0 - Release 0650, Version 2.5, 27.03.2007
9. FlexiTrust V3.0 R0650 – Benutzerhandbuch des Teilsystems RA für FlexiTrust 3.0 - Release 0650, Version 2.0, 27.03.2007
10. FlexiTrust V3.0 R0650 – Benutzerhandbuch Produktions CA für FlexiTrust 3.0 - Release 0650, Version 2.0, 27.03.2007
11. FlexiTrust V3.0 R0650 – Benutzerhandbuch Revokations CA für FlexiTrust 3.0 - Release 0650, Version 1.9, 27.03.2007
12. FlexiTrust V3.0 R0650 – Benutzerhandbuch – ImpEx für FlexiTrust 3.0 - Release 0650, Version 2.6, 27.03.2007
13. FlexiTrust V3.0 R0650 – Benutzerhandbuch – OCSP Responder für FlexiTrust 3.0 - Release 0650, Version 2.2, 27.03.2007
14. FlexiTrust V3.0 R0650 – Benutzerhandbuch – Infrastructure Services (IS) für FlexiTrust 3.0 - Release 0650, Version 1.6, 27.03.2007
15. FlexiTrust V3.0 R0650 – Korrekturen und Ergänzungen zu den Administrationshandbüchern, Version 0.2, 06.03.2007
16. KOBIL Smart Key SigG-PKCS#11 Modul – Benutzerdokumentation, Version 1.1, 19.02.2007.
17. Dokumentation für das von der KOBIL Systems GmbH entwickelte Werkzeug PKCS#10-Request Generator[4].

1.4 Hersteller

FlexSecure GmbH

Industriestraße 12

64297 Darmstadt

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

2. Funktionsbeschreibung

Die Komponente ist eine technische Komponente für Zertifizierungsdienste.

Die Komponente FlexiTrust V3.0 R0650 ist eine Software zum Einsatz im Trust Center der Bundesnetzagentur und beinhaltet einen Zertifizierungsdienst, einen Revokationsdienst und einen Auskunftsdienst. Diese Dienste werden durch die unter Lieferumgang angegebenen Teilkomponenten erbracht.

RA-Komponente Zertifizierungsdienst: Diese Komponente dient der Annahme, Überprüfung und Verarbeitung von Anträgen für qualifizierte Zertifikate.

CA-Komponente Zertifizierungsdienst: Diese Komponente sorgt dafür, dass Zertifikate mit qualifizierten elektronischen Signaturen versehen werden.

IS-Komponente Zertifizierungsdienst: Diese Komponente hat die Aufgabe, mit qualifizierten elektronischen Signaturen versehene Zertifikate an den MasterLDAP- bzw. an den PublicLDAP-Server zu übertragen und den Erfolg dieser Aktionen zu überwachen.

RA-Komponente Revokationsdienst: Diese Komponente dient der Annahme, Überprüfung und Verarbeitung von Anträgen auf Sperrung von qualifizierten Zertifikaten.

CA-Komponente Revokationsdienst: Diese Komponente sorgt dafür, dass Sperrlisten mit qualifizierten elektronischen Signaturen versehen werden.

IS-Komponente Revokationsdienst: Diese Komponente hat die Aufgabe, mit qualifizierten elektronischen Signaturen versehene Sperrlisten an den MasterLDAP- und an den PublicLDAP-Server zu übertragen und den Erfolg dieser Aktionen zu überwachen.

OCSP-Komponente: Diese Komponente dient dazu, Anfragen über den Status von Zertifikaten zu bearbeiten. Die generierten Auskünfte werden von der OCSP-Komponente mit qualifizierten elektronischen Signaturen versehen. Die OCSP-Komponente dient sowohl der Beantwortung von externen als auch von internen Anfragen (Anfragen der IS-Komponente Zertifizierungs- bzw. Revokationsdienst).

ImpEx-Komponente: Diese Komponente stellt Dienstleistungen für die RA-, CA- und IS-Komponente Zertifizierungsdienst zur Verfügung. Sie automatisiert den Austausch von Daten zwischen der RA-Komponente Zertifizierungsdienst und der CA-Komponente Zertifizierungsdienst sowie zwischen der CA-Komponente Zertifizierungsdienst und der IS-Komponente Zertifizierungsdienst. Hierbei kommen jeweils externe Datenträger (Disketten) zum Einsatz.

PIN-/PASS-Sharing: Es handelt sich um Administrationswerkzeuge zur Erzeugung und Verschlüsselung von PIN-Shares für die Signaturkarten-PINs und die Passwort-Shares für MasterLDAP-, PublicLDAP- und Datenbank-Servers bzw. Key-Stores für den Transportschutzmechanismus.

P11-Komponente: Der PKCS#11-Treiber realisiert die Zuführung von Daten zur Erstellung qualifizierter Signaturen. Der PKCS#11-Treiber wird durch die Teilsysteme TS_CA und TS_OCSP verwendet.

PKCS#10-Request Generator: Die Aufgaben dieser Komponente bestehen in der Erzeugung von PKCS#10-Requests für Signaturkarten im Eigenbedarf des Betreibers.

Die einzelnen Dienste sind im Dokument "Sicherheitsvorgaben für FlexiTrust 3.0 – Release 0650", Version 1.16 detailliert beschrieben.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die technische Komponente für Zertifizierungsdienste „FlexiTrust V3.0 R0650“ erfüllt die folgenden Anforderungen:

- §17 Abs. 3 Nr. 2 SigG
- §15 Abs. 3 S. 1 SigV
- §15 Abs. 3 S. 2 SigV
- §15 Abs. 3 S. 3 SigV
- §15 Abs. 4 SigV

Des Weiteren sind die Anforderungen von §15 Abs. 2 Nr.1 SigV bei der Signierung von Zertifikaten erfüllt. Bei der Signierung von Auskünften des Verzeichnisdienstes (OCSP-Auskünfte und Sperrlisten) sind §15 Abs. 2 Nr.1 a) und b) SigV erfüllt.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die technische Komponente für Zertifizierungsdienste „FlexiTrust V3.0 R0650“ 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
- 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
- Prozessdatenbank MySQL 3.23.57
- Aktivierungsdatenbank OpenLDAP 2.0.27
- Verschlüsselung OpenSSL 0.9.8d
- Interne DB BerkeleyDB 3.1.17
- Hashwerte OpenSSL 0.9.8d
- SigG-konform personalisierte Signaturkarten vom Typ TCOS 3.0 SignatureCard Version 1.1
- SigG-konformes Chipkartenterminal KAAN Advanced, Firmware Version 1.02, Hardware Version K104R3

Diese Sicherheitsbestätigung für „FlexiTrust V3.0 R0650“ 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 „FlexiTrust V3.0 R0650“ wird vom Hersteller gemäß Abschnitt 1 ausgeliefert.

Vor Installation von „FlexiTrust V3.0 R0650“ ist zu prüfen, ob

- die vorgesehene Einbindung von „FlexiTrust V3.0 R0650“ 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 V3.0 R0650 eingehalten worden ist,
- die Originaldatenträger korrekt beschriftet sind,

- die Hashwerte der auf dem Originaldatenträger enthaltenen Dateien korrekt sind[5],
- die Integrität der SigG-PKCS#11 Funktionsbibliothek der KOBIL Systems GmbH gegeben ist, falls diese bereits installiert sein sollte.

Diese Prüfungen und ihre Ergebnisse sind aufzuzeichnen.

Die Inbetriebnahme von FlexiTrust V3.0 R0650 und jede Wiederinbetriebnahme, die eine Neuinstallation erfordert, müssen durch fachkundiges Personal des Herstellers erfolgen.

Die technische Komponente für Zertifizierungsdienste „FlexiTrust V3.0 R0650“ 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 V3.0 R0650“ 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 V3.0 R0650“ wurde für den geschützten Einsatzbereich[6] 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 V3.0 R0650“ und der beteiligten Systeme hat im Vier-Augen-Prinzip zu erfolgen.
- Es ist sicherzustellen, dass auf der von „FlexiTrust V3.0 R0650“ benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Bei der Konfiguration von „FlexiTrust V3.0 R0650“ 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.

---

5 Ein Werkzeug zur Prüfung der Integrität der ausgelieferten Dateien gehört nicht zum Lieferumfang von„FlexiTrust V3.0 R0650“.

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

- Von „FlexiTrust V3.0 R0650“ 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 V3.0 R0650“ 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.

Mit Auslieferung von „FlexiTrust V3.0 R0650“ ist der Betreiber auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Die technische Komponente für Zertifizierungsdienste „FlexiTrust V3.0 R0650“ 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. 58, S. 1913-1915 vom 23. März 2006) 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[7] und reicht jeweils mindestens bis zu den oben Zeitpunkten.

Eine Verlängerung der Gültigkeit kann erfolgen, wenn zu diesen Zeitpunkten keine Hinderungsgründe hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

[7] „FlexiTrust V3.0 R0650“ erlaubt es, per Konfiguration einzelne Algorithmen zu aktivieren bzw. zu deaktivieren und damit jeweils nur aktuell gültige Algorithmen zur verwenden.

3.4 Prüfstufe und Mechanismenstärke

Die technische Komponente für Zertifizierungsdienste „FlexiTrust V3.0 R0650“ 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, und zwar auf der Basis der unter

- T-Systems.02096.TE.12.2003 (Erst-Evaluierung) und
- T-Systems.02126.TE.11.2004 (1. Re-Evaluierung)

dokumentierten Verfahren .

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

Ende der Bestätigung

Sicherheitsbestätigung:
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-itc.de
	www.t-systems-zert.com