Sicherheitsbestätigung und Bericht

T-Systems. 02162.TE.01.2007

FlexiTrust-OCSP 3.5 – Release 0621

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-OCSP 3.5 – Release 0621“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems. 02162.TE.01.2007

Bonn, den 16.01.2007

(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. 02162.TE.01.2007 besteht aus 6 Seiten.

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:

FlexiTrust-OCSP 3.5 – Release 0621

Auslieferung:

Die Auslieferung der technischen Komponente kann in mehreren Varianten erfolgen:

- Persönliche Übergabe durch den Hersteller an den Benutzer (Standardverfahren),
- Versand durch Post oder Kurier an den Benutzer.

Die Übergabe erfolgt auf einem einmal beschreibbaren Datenträger in einem versiegelten Umschlag, die Hashwerte aller Dateien werden separat übermittelt.

- Elektronische Übermittlung an den Benutzer in Form einer Archiv-Datei mit separater Übermittlung der Hashwerte aller Dateien.

Die Einzelheiten der Auslieferung sind in "FlexiTRUST OCSP Version 3.5 Release 0621 ADO_DEL.2 – Auslieferungsprozeduren / ADO_IGS.1 – Installations-, Generierungs- und Anlaufprozeduren, Stand 12. Januar 2007" detailliert beschrieben.

Lieferumfang:

Der Lieferumfang umfasst

- die Binärpakete des OCSP-Systems, Skripte für die Bedienung des TOE (EVG), Vorkonfiguration (wird im Rahmen der Initialisierung / Installation angepasst), Benutzerhandbuch, Administrationshandbuch, Auslieferungshandbuch
- sowie optional (nicht zum Produkt gehörend) Binärpakete Kartentreiber und OpenLDAP.

Die ausgelieferten Dateien sind mit Angabe des Versionsstandes in "FlexiTRUST-OCSP Version 3.5 Release 0621 ACM SCP.1 – Konfigurationsliste", Stand: 12.01.2007, erfasst.

Für den Betrieb werden weiterhin benötigt

- die unter "Evaluierte Konfiguration" in Abschnitt 3.2 angegebene HW-/SW-Ausstattung,

- KOBIL Chipkartenterminal B1 Professional, HW-Version KCT-100, FW-Version 2.08 GK 1.04 oder/und KOBIL Chipkartenterminal KAAN Advanced RS232, HW-Version K104R3, FW-Version 1.02 und
- SSEE (Dienstekarten) vom Typ "STARCOS 3.0 with Electronic Signature Application V 3.0" der Fa. Giesecke & Devrient GmbH unter Verwendung der Initialisierungstabelle "dgn_z1".
- SSEE (Endbenutzerkarten) vom Typ "STARCOS 3.0 with Electronic Signature Application V 3.0" der Fa. Giesecke & Devrient GmbH unter Verwendung der Initialisierungstabelle "dgn_e2".

Hersteller:

FlexSecure GmbH,

Industriestraße 12, 64297 Darmstadt

2. Funktionsbeschreibung

Die Komponente FlexiTrust-OCSP 3.5 – Release 0621 ist eine technische Komponente für Zertifizierungsdienste. Sie stellt Funktionen für einen Dienst zur Verfügung, der qualifizierte Zertifikate nachprüfbar bzw. abrufbar hält.

Die Software realisiert dazu das OCSP-Protokoll. Über dieses Protokoll werden Zertifikate jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar gehalten. Für nachprüfbare Zertifikate liefert die technische Komponente eine Aussage darüber, ob ein angefragtes Zertifikat zum angegebenen Zeitpunkt existiert hat und ob es gesperrt ist (Statusauskunft).

Zusätzlich werden Zertifikate, für die der Eigentümer zuvor seine Einwilligung gegeben hat, über öffentlich erreichbare Kommunikationsverbindungen abrufbar gehalten. Die technische Komponente liefert in diesem Fall das angefragte Zertifikat in der Statusauskunft mit, falls dies in der Anfrage so gewünscht wurde.

Die Komponente FlexiTrust-OCSP 3.5 – Release 0621 generiert Statusauskünfte basierend auf einer Datenbank, die durch die Umgebung zur Verfügung gestellt werden muss. Die Umgebung muss insbesondere sicherstellen, dass die Datenbasis aktuell, konsistent und korrekt ist.

Die Komponente FlexiTrust-OCSP 3.5 – Release 0621 ist mandantenfähig und in der Lage, Statusauskünfte sowohl für qualifizierte als auch nicht qualifizierte Zertifikate parallel auszuliefern. Die Zuordnung einer Anfrage zu einem Mandanten erfolgt auf Basis der Informationen, die in der Anfrage enthalten sind. Es ist sichergestellt, dass Statusauskünfte für "qualifizierte" Mandanten mit einer qualifizierten elektronischen Signatur versehen werden.

Im Sinne des Signaturgesetzes umfasst FlexiTrust-OCSP 3.5 – Release 0621 folgende Einzelkomponenten:

1. Signaturanwendungskomponente im Auskunftsdienst: Diese Komponente führt im Sinne von §2 SigG Nr. 11 a) Statusauskünfte dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zu.
2. Unterstützende technische Komponente für Zertifizierungsdienste: Diese Komponente hält im Sinne von §2 SigG Nr. 12 b) qualifizierte Zertifikate öffentlich nachprüfbar und ggf. abrufbar[3]. Sie beantwortet Statusanfragen mit entsprechenden Auskünften.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ erfüllt insbesondere die folgenden Anforderungen:

§17 Abs. 3 Nr. 2 SigG

§15 Abs. 3 Satz 1, 2 und 3 SigV

§15 Abs. 4 SigV

Für die von der technischen Komponente ausgeübten Funktionen einer Signaturanwendungskomponente (s. Abschnitt 2) sind zusätzlich die Anforderungen von §15 Abs. 2 Nr. 1 SigV erfüllt.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ wurde evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration:

- Rechner mit Betriebssystem System SUN Solaris Solaris 9 Rel. 8/03
- Laufzeitumgebung SUN Java jdk 1.4.2 _13 + JCE

[3] Die Datenhaltung im Zertifikatsverzeichnis und die öffentliche Kommunikationsanbindung sind nicht Bestandteil der technischen Komponente.

- Applikationsserver JBoss 3.2.8.SP1
- Servlet-Container Apache Tomcat 5.0.30
- Aktivierungsdatenbank OpenLDAP 2.3.17
- Interne DB Berkeley DB 4.3.27
- Authentifizierung Cyrus SASL 2.1.19
- Verschlüsselung OpenSSL 0.9.8d

Diese Sicherheitsbestätigung für die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ gilt ausschließlich für den Einsatz zusammen mit der oben beschriebenen Hard- und Softwareausstattung sowie den zum Betrieb erforderlichen Komponenten (Chipkartenterminal, SSEE) aus Abschnitt 1 "Auslieferung".

Soll der Einsatz mit einer geänderten Hard- oder Softwareausstattung erfolgen, so ist die Bestätigungsstelle vorab zu informieren und einzubeziehen. Eine Übertragung der Evaluationsergebnisse auf eine andere Einsatzumgebung kann ggf. eine Reevaluation erforderlich machen.

b) Einbindung in die Hard- und Softwareumgebung

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ wird vom Hersteller gemäß Abschnitt 1 ausgeliefert. Das spezifizierte Auslieferungsverfahren ist einzuhalten.

Die Inbetriebnahme und jede Wiederinbetriebnahme, die eine Neuinstallation erfordert, müssen durch fachkundiges Personal des Herstellers erfolgen. Dabei sind alle Auflagen an den Hersteller aus dem Evaluationsbericht einzuhalten.

Die korrekte Einbindung der technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ in ein Trust Center eines ZDA ist von der Prüf- und Bestätigungsstelle zu überprüfen.

Anwendungen, die die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ nutzen, sind **nicht** Gegenstand dieser Bestätigung.

c) Nutzung des Produktes

Vor Installation der technischen Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ ist zu prüfen,

- ob das angegebene Auslieferungsverfahren eingehalten wurde,
- ob die ausgelieferten Dateien unverändert sind,
- ob die Bedingungen an die technische Einsatzumgebung erfüllt sind.

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

- Der Betrieb der technischen Komponente ist nur in einer vertrauenswürdigen Umgebung eines Trust Centers zulässig. Die für die Sicherheit relevanten Annahmen an die Einsatzumgebung sind der Beschreibung der Sicherheitsumgebung zu entnehmen (s. Kap. 3 im Security Target, Version 0621_1.2, Stand: 12.01.2007, separat beim Hersteller erhältlich).
- Für die Teile der technischen Komponente, die Signaturanwendungskomponenten darstellen, sind zusätzlich die Bedingungen für den geschützten Einsatzbereich gemäß "Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten"[4] einzuhalten.
- Der Schutz der Einsatzumgebung muss durch geeignete materielle, organisatorische und personelle Maßnahmen gewährleistet werden, die gemäß den gesetzlichen Vorgaben in einem Sicherheitskonzept dokumentiert sein müssen.
- Es ist sicherzustellen, dass auf den von FlexiTrust-OCSP 3.5 – Release 0621 benutzten Hardwareplattformen keine Viren oder Trojanischen Pferde eingespielt werden.
- Es ist vertrauenswürdiges Personal einzusetzen.
- Mit Identifikationsmerkmalen, die an Signaturerstellungseinheiten weitergereicht oder die im Zusammenhang mit Sperranträgen benutzt werden, ist vertraulich umzugehen, insbesondere seitens handelnder Personen und beteiligter Anwendungen.
- Von FlexiTrust-OCSP 3.5 – Release 0621 erzeugte Meldungen sind regelmäßig zu kontrollieren und auszuwerten.
- Versiegelungen von Karten und Systemen sind regelmäßig zu kontrollieren; durchgeführte Kontrollen sind zu protokollieren.
- Bei der Evaluierung wurde festgestellt, dass das Risiko der Speicherung von Identifikationsdaten für die Aktivierung von SSEE als Dienstekarten nicht vollständig ausgeschossen werden, wenn während der Verarbeitung vom Betriebssystem Speicherseiten in den SWAP-Bereich der Festplatte ausgelagert werden. Um die gesetzlichen Anforderungen hinsichtlich des Speicherverbots von Identifikationsdaten zu erfüllen, ist zu gewährleisten, dass während der Verarbeitung von Identifikationsdaten das Swapping deaktiviert ist.
- Durch Veränderungen der Einsatzumgebung dürfen die bekannten Schwachstellen in der Konstruktion und bei der operationalen Nutzung nicht ausnutzbar werden, und es dürfen keine neuen Schwachstellen entstehen.

---

[4] Dokument verfügbar auf der Web-Site der Bundesnetzagentur.

Mit Auslieferung der technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ ist der Betreiber auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ verwendet folgende Algorithmen:

- Hashfunktion RIPEMD-160. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht mindestens bis Ende 2010 (s. Bundesanzeiger Nr. 58, S. 1913-1915 vom 23. März 2006).
- Hashfunktion SHA-1[5]. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung bei Anwendung für qualifizierte Zertifikate reicht mindestens bis Ende 2010, bei anderen Anwendungen mindestens bis Ende 2009 (s. Bundesanzeiger Nr. 58, S. 1913-1915 vom 23. März 2006).

Diese Sicherheitsbestätigung ist somit - abhängig von der Nutzung der jeweiligen Hashfunktion - gültig bis mindestens 31.12.2009 bzw. 31.12.2010; sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

3.4 Prüfstufe und Mechanismenstärke

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP 3.5 – Release 0621“ wurde erfolgreich nach der Prüfstufe **EAL3** der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert.

Die eingesetzten Sicherheitsmechanismen erreichen die Stärke "**hoch**".

Die im Evaluationsbericht enthaltenen Auflagen an den Hersteller sind einzuhalten.

Ende der Bestätigung

[5] Aufgrund des Evaluationsergebnisses fällt ein Betrieb des Produktes mit dem vorhandenen SHA-256 nicht unter diese Sicherheitsbestätigung.

Sicherheitsbestätigung:
T-Systems. 02162.TE.01.2007

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