T · · Systems ·

Sicherheitsbestätigung

T-Systems.02216.TE.11.2008

FlexiTrust-OCSP Version 3.5 Release 0847

FlexSecure GmbH

Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 3 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 Version 3.5 Release 0847“

der

FlexSecure GmbH

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02216.TE.11.2008

Bonn, den 20.11.2008

(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 Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Technische Komponente für Zertifizierungsdienste
„FlexiTrust-OCSP Version 3.5 Release 0847“

Hinweis:

Das Produkt stellt eine Weiterentwicklung des Produktes „FlexiTrust-OCSP 3.5 – Release 0621“ dar (Bestätigungsnummer T-Systems.02162.TE.01.2007 vom 16.01.2007).

1.2 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 0847 ADO DEL.2 – Auslieferungsprozeduren, ADO IGS.1 – Installations-, Generierungs- und Anlaufprozeduren“ vom 10.10.2008 detailliert beschrieben.

1.3 Lieferumfang

Der Lieferumfang umfasst

- die Binärpakete des OCSP-Systems, Binärpakete Kartentreiber PKCS#11, Skripte für die Bedienung von „FlexiTrust-OCSP Version 3.5 Release 0847“, Vorkonfiguration (wird im Rahmen der Initialisierung / Installation angepasst), Benutzerhandbuch, Administrationshandbuch, Auslieferungshandbuch

- sowie optional (nicht zum Produkt gehörend) Binärpakete anderer Kartentreiber und OpenLDAP.

Die ausgelieferten Dateien sind mit Angabe des Versionsstandes in „FlexiTrust-OCSP Version 3.5 Release 0847 ACM SCP.1 – Konfigurationsliste“ vom 16.10.2008 erfasst.

Die für den Betrieb des Produktes erforderliche Einsatzumgebung und die erforderlichen bestätigten Komponenten anderer Hersteller sind in Abschnitt 3.2 angegeben.

1.4 Hersteller

FlexSecure GmbH
Industriestraße 12
64297 Darmstadt

2. Funktionsbeschreibung

Die Komponente FlexiTrust-OCSP Version 3.5 Release 0847 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 Version 3.5 Release 0847 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 Version 3.5 Release 0847 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 Version 3.5 Release 0847 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.

Hinweis:

Gegenüber dem Release 0621 sind am Produkt folgende Änderungen vorgenommen worden:

1. Integration der Hashfunktionen SHA-224, SHA-256, SHA-384 und SHA-512.
2. Einbindung der SSEE „TCOS 3.0 Signature Card, Version 1.1“, Konfigurationsvariante “Signature Card 3.0M, Version 1.0” (Bestätigungsnummer TUVIT.93146.TE.12.2006) als mögliche Dienste-SSEE.
3. Software-Wartung, insbesondere Anpassungen bzgl. der Kodierung von Zertifikaten.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ 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:

---

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

a) Technische Einsatzumgebung

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ wurde auf der Basis der folgenden Hard- und Softwarekonfiguration evaluiert:

- Rechner mit Betriebssystem SUN Solaris Sparc Solaris 9 Rel. 8/03
- Laufzeitumgebung SUN Java jre 1.6.0_07 +JCE
- Applikationsserver JBoss 3.2.8 SP1
- Servlet-Container Apache Tomcat 5.0.30
- Aktivierungsdatenbank OpenLDAP 2.3.43
- Verschlüsselung OpenSSL 0.9.8h
- Interne DB BerkeleyDB 4.4.20
- Authentifizierung Cyrus SASL 2.1.21

Für den Betrieb von „FlexiTrust-OCSP Version 3.5 Release 0847“ sind weiterhin folgende bestätigte Komponenten anderer Hersteller einsetzbar[4]:

- KOBIL Chipkartenterminal KAAN Advanced (USB/RS232) Hardware Version K104R3, Firmware Version 1.19, der Fa. Kobil Systems GmbH (Bestätigungsnummer T-Systems.02207.TU.04.2008, hier: Nachtragsbestätigung vom 07.04.2008 zu BSI.02050.TE.12.2006).
- SSEE als Dienste-Karte vom Typ "TCOS 3.0 Signature Card, Version 1.1" der Fa. T-Systems Enterprise Services GmbH, und zwar unter Verwendung der Ausprägung "Signature Card 3.0M, Version 1.0" (Bestätigungsnummer TUVIT.93146.TE.12.2006).
- SSEE als Dienste-Karte vom Typ "STARCOS 3.0 with Electronic Signature Application V 3.0" der Fa. Giesecke & Devrient GmbH unter Verwendung der Initialisierungstabelle "dgn_z1" (Bestätigungsnummer TUVIT.93100.TE.09.2005)[5].

Die Auflagen und Hinweise aus den Sicherheitsbestätigungen dieser Produkte sind einzuhalten.

Die vorliegende Sicherheitsbestätigung für die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ gilt ausschließlich für den Einsatz zusammen mit der oben beschriebenen Hard- und Softwareausstattung. Soll ihr Einsatz zusammen 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.

---

4 Die beiden als Dienstekarte angegebenen SSEE können alternativ verwendet werden.

5 Bei dieser SSEE sind als Hashfunktionen nur SHA-1 und RIPEMD-160 zulässig.

b) Einbindung in die Hard- und Softwareumgebung

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ wird vom Hersteller gemäß Abschnitt 1 ausgeliefert. Das spezifizierte Auslieferungsverfahren ist einzuhalten.

Die technische Komponente „FlexiTrust-OCSP Version 3.5 Release 0847“ ist so zu installieren und zu konfigurieren, dass die vorhandene Hashfunktion SHA-1 nicht für die qualifizierte Signatur von Statusauskünften verwendet werden kann.

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 Version 3.5 Release 0847“ in ein Trust Center eines ZDA ist von der Prüf- und Bestätigungsstelle zu überprüfen.

Anwendungen, die die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ nutzen, sind nicht Gegenstand dieser Bestätigung.

c) Nutzung des Produktes

Vor Installation der technischen Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ 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 der „FlexiTrust-OCSP Version 3.5 Release 0847“, Version 1.6 vom 14.11.2008, 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"[6] einzuhalten.

---

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

- 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 Version 3.5 Release 0847 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 Version 3.5 Release 0847 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.

Mit Auslieferung der technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ ist der Betreiber auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Die technische Komponente für Zertifizierungsdienste „FlexiTrust-OCSP Version 3.5 Release 0847“ verwendet folgende Algorithmen, deren Eignung gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV[7] festgestellt wird:

- Hashfunktion RIPEMD-160, geeignet bis mindestens Ende 2010, für die Prüfung qualifizierter Zertifikate mindestens bis Ende 2015.

[7] i. V. mit: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. November 2008

- Hashfunktion SHA-1, geeignet für die Erzeugung qualifizierter Zertifikate mindestens bis Ende 2009, zur Erzeugung qualifizierter Zertifikate bei ≥20 Bit Entropie der Seriennummer mindestens bis Ende 2010, für die Prüfung qualifizierter Zertifikate mindestens bis Ende 2015.[8]
- Hashfunktionen SHA-224, SHA-256, SHA-384, SHA-512, geeignet mindestens bis Ende 2015.

Die vorliegende Sicherheitsbestätigung ist somit in Abhängigkeit von der verwendeten Hashfunktion gültig bis zum jeweils angegebenen Datum; 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 Version 3.5 Release 0847“ wurde nach der Prüfstufe EAL3 der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV auf der Basis der früheren Evaluierung (Bestätigungsnummer T-Systems.02162.TE.01.2007) erfolgreich re-evaluiert.

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

Ende der Bestätigung.

[8] Für die Erzeugung und Prüfung anderer qualifiziert signierter Daten darf diese Hashfunktion nicht eingesetzt werden.

Sicherheitsbestätigung
T-Systems.02216.TE.11.2008

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.de/ict-security
	www.t-systems-zert.com