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

- 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 Zertifizierungsdiensteanbieter
„FlexiTrust 3.0 Release 0421“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02126.TE.11.2004

Bonn, den 03.11.2004 _____
(Dr. Heinrich Kersten)

Die T-Systems - 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 die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22)

2 Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59)

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Bezeichnung:
technische Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“

Auslieferung:
Der EVG und die zugehörigen Handbücher werden auf einem nicht wiederbeschreibbaren Datenträger (CD-ROM) durch den Hersteller direkt ausgeliefert. Zusätzlich werden die Handbücher und eine Prüfsummenliste in gedruckter Form ausgeliefert. Mit der Prüfsummenliste kann die Integrität der ausgelieferten technischen Komponente für Zertifizierungsdiensteanbieter überprüft werden.[3]

Lieferumfang:
An den Anwender werden die nachfolgend aufgelisteten Komponenten und Handbücher auf einem nicht wiederbeschreibbaren Datenträger (CD-ROM) ausgeliefert. Die Handbücher werden zusätzlich in gedruckter Form ausgeliefert.

Komponenten:

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
7. PKCS#10-Request Generator

Handbücher:

1. Administrationshandbuch OCSP Responder für FlexiTrust 3.0 – Release 0421. Version 1.7, 9 Seiten, 30.07.2004.
2. Administrationshandbuch des Teilsystems RA für FlexiTrust 3.0 – Release 0421. Version 1.1.6, 48 Seiten, 17.09.2004.
3. Administrationshandbuch CA für FlexiTrust 3.0 – Release 0421. Version 2.1, 20 Seiten, 30.07.2004.
4. Administratoren Handbuch – Infrastructure Services (IS) für FlexiTrust 3.0 – Release 0421. Version 1.5, 11 Seiten, 17.09.2004.
5. Konfigurationsdateien – Infrastructure Services (IS) für FlexiTrust 3.0 – Release 0421. Version 1.4, 18 Seiten, 17.09.2004.
6. Administrator-Handbuch – ImpEx für FlexiTrust 3.0 – Release 0421. Version 2.4, 6 Seiten, 30.07.2004.
7. Administrationshandbuch PIN-Sharing für FlexiTrust 3.0 – Release 0421. Version 2.2, 9 Seiten, 17.09.2004.
8. Administrationshandbuch PASS-Sharing für FlexiTrust 3.0 – Release 0421. Version 2.0, 13 Seiten, 27.07.2004.
9. Benutzerhandbuch OCSP Responder für FlexiTrust 3.0 – Release 0421. Version 2.1, 6 Seiten, 30.07.2004.
10. Benutzerhandbuch des Teilsystems RA für FlexiTrust 3.0 – Release 0421. Version 1.9.6, 52 Seiten, 17.09.2004.

---

[3] Ein Tool zur Integritätsprüfung (Korrektheit der Prüfsummen) wird vom Hersteller nicht mitgeliefert.

11. Benutzerhandbuch Revokations CA für FlexiTrust 3.0 – Release 0421. Version 1.8, 5 Seiten, 30.07.2004.
12. Benutzerhandbuch Produktions CA für FlexiTrust 3.0 – Release 0421. Version 1.9, 7 Seiten, 30.07.2004.
13. Benutzerhandbuch – Infrastructure Services (IS) für FlexiTrust 3.0 – Release 0421. Version 1.5, 7 Seiten, 17.09.2004.
14. Benutzerhandbuch – ImpEx für FlexiTrust 3.0 – Release 0421. Version 2.5, 7 Seiten, 30.07.2004.

Hersteller:
FlexSecure GmbH
Thüringer Straße 1, 64297 Darmstadt

2. Funktionsbeschreibung

Die Komponente ist eine technische Komponente für Zertifizierungsdiensteanbieter.

Die Komponente FlexiTrust 3.0 ist eine Software zum Einsatz bei Zertifizierungsdiensteanbietern, die folgende drei Dienste erbringt:

- Zertifizierung,
- Revokation und
- Auskunftserteilung.

Die FlexiTrust 3.0 Software beinhaltet folgende Teilkomponenten:

- RA-/CA-/IS-Komponente Zertifizierungsdienst
- RA-/CA-/IS-Komponente Revokationsdienst
- OCSP-Komponente
- ImpEx-Komponente
- Administrationswerkzeuge PIN-/PASS-Sharing
- SigG-PKCS#11 Funktionsbibliothek
- PKCS#10-Request Generator

Die RA-Teilkomponente dient der Erfassung und Bearbeitung der Antragsdaten. Die Antragsdaten können über ein Web-Frontend direkt eingegeben oder als XML-Antrag importiert werden. Vor der weiteren Verarbeitung können alle Daten geprüft und ggf. geändert werden. Die RA-Teilkomponente muss sicher in den Betrieb des Zertifizierungsdiensteanbieters eingebunden werden.

Die CA-Teilkomponente führt die zu signierenden Zertifikatsrohdaten nach Anzeige einer sicheren Signaturerstellungseinheit zu und veranlasst die Eintragung der erzeugten Zertifikate in eine Datenbank. Die CA-Teilkomponente realisiert ferner die Sperrung von Zertifikaten, wenn ein zulässiger Sperrantrag vorliegt, das zu sperrende Zertifikat im Zertifikatsverzeichnis des Zertifizierungsdiensteanbieters vorhanden und nicht bereits gesperrt ist. Die CA-Teilkomponente muss sicher in den Betrieb des Zertifizierungsdiensteanbieters eingebunden werden.

Die OCSP-Responder-Teilkomponente hält qualifizierte Zertifikate öffentlich nachprüfbar. Dazu nimmt sie Anfragen nach dem Status eines Zertifikates (OCSP-Anfragen) an und generiert eine signierte OCSP-Auskunft. Die OCSP-Responder-Teilkomponente muss sicher in den Betrieb des Zertifizierungsdiensteanbieters eingebunden werden.

Die Teilkomponenten IS und ImpEx übernehmen Serviceaufgaben für die oben genannten drei Teilkomponenten.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die technische Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ 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 Erstellung von Zertifikaten erfüllt. Bei der Signierung von Auskünften des Verzeichnisdienstes 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 Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ wurde für die spezielle Einsatzumgebung des Trust Centers der Regulierungsbehörde für Telekommunikation und Post (RegTP), der Root-CA, evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration:

- Workstations mit Betriebssystem Sun Solaris 8 2/02, Java Laufzeitumgebung (Bytecode-interpreter JDK 1.4.1, J2SE; Enterprise Application Server JBoss 3.0.6) und Datenbank MySQL 4.0.14
- SigG-konform personalisierte Signaturkarten mit Betriebssystem TCOS 2.0
- Chipkartenleser KOBIL Kaan Professional für Bediener- oder Signaturkarten
- SigG-Bibliothek KOBIL SigG-PKCS#11 Funktionsbibliothek für die vertrauenswürdige Kommunikation mit Signaturkarten
- KOBIL PKCS#10-Request Generator
- Apache Ant 1.5.4
- Tomcat 4.1.27

Eine Übertragung der Evaluationsergebnisse auf eine andere Umgebung und / oder andere Plattformen (z.B. anderes Betriebssystem, andere Laufzeitumgebung, andere Chipkarte, andere Personalisierung, andere Rechnerarchitektur, anderer Chipkartenleser) ist nicht möglich, sondern erfordert ggf. eine Reevaluation.

Diese Sicherheitsbestätigung für die technische Komponente für Zertifizierungsdienste-anbieter „FlexiTrust 3.0 Release 0421“ gilt deshalb 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 dies der Bestätigungsstelle anzuzeigen.

b) Einbindung in die Hard- und Softwareumgebung

Die technische Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ 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.

Wird der Zertifizierungsdienst bei entsprechender Konfiguration von „FlexiTrust 3.0 Release 0421“ mit mehr als einem aktiven Revokationssystem betrieben, so hat der Zertifizierungsdiensteanbieter durch organisatorische Maßnahmen dafür zu sorgen, dass eine ausreichende Umschaltzeit zwischen den Revokationssystemen gewährleistet ist. Die organisatorischen Maßnahmen sollen Bestandteil des Sicherheitskonzeptes des Zertifizierungsdiensteanbieters sein. Nach Messungen des Herstellers ist für den Betrieb im Trust Center der RegTP eine Umschaltzeit von 5 Minuten ausreichend.

Die korrekte Einbindung der technischen Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ in das Trust Center der RegTP ist zu prüfen.

Anwendungen, die die technische Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ nutzen, sind **nicht** Gegenstand dieser Bestätigung.

c) Nutzung des Produktes

Um die technische Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ in Betrieb zu nehmen und ihren Betrieb aufrecht zu erhalten, sind die im Sicherheitskonzept der RegTP genannten Rollen zu besetzen. Dabei ist insbesondere die ebenfalls im Sicherheitskonzept der RegTP beschriebene Rollentrennung zu beachten. Die den einzelnen Rollen zugeordneten Aufgaben sind so zu bestimmen, dass

- begleitende Aufgaben, die den technischen Betrieb und dessen Sicherheit überwachen, von operativen Aufgaben getrennt sind,
- Aufgaben, die Interessenskonflikte hervorrufen können (z.B. Revision und Leitung), getrennt sind,
- externe Aufgaben und Funktionen (z. B. Reinigung, Wartung und Antragsteller) von allen im regulären Zertifizierungsbetrieb auszuführenden Aufgaben getrennt sind, und
- Aufgaben der Systemadministration von allen anderen operativen Aufgaben getrennt sind.

Vor Installation der technischen Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ ist zu prüfen,

- ob der Originaldatenträger (CD-ROM) korrekt mit „FlexiTrust 3.0 Release 0421“ beschriftet ist,
- ob die Prüfsummen der auf dem Originaldatenträger „FlexiTrust 3.0 Release 0421“ enthaltenen Dateien korrekt sind,
- falls die SigG-PKCS#11 Funktionsbibliothek bereits auf dem System installiert ist, ob diese integer ist.

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

- Die technische Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ soll nur in der vertrauenswürdigen Umgebung des Trust Centers der RegTP betrieben werden.
- Es ist insbesondere vertrauenswürdiges und fachkundiges Personal einzusetzen.
- Es ist sicherzustellen, dass auf der von der technischen Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt 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.
- Von der technischen Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ erzeugte Meldungen sind regelmäßig zu kontrollieren und auszuwerten.
- Die Versiegelungen sind regelmäßig zu kontrollieren; durchgeführte Kontrollen sind zu protokollieren.
- Die Systemzeiten der Systeme, auf denen die technische Komponente für Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ installiert ist, soll wöchentlich mit der gesetzlichen Zeit abgeglichen werden.
- 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 Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ ist der Betreiber auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Der Verzeichnisdienst verwendet zur Signierung der Auskünfte den RSA-Algorithmus mit 1024 bit. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht daher mindestens bis Ende des Jahres 2007 (s. Bundesanzeiger Nr. 30 – S. 2537-2538 vom 13. Februar 2004).

Diese Sicherheitsbestätigung ist somit gültig bis zum 31.12.2007; 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 Zertifizierungsdiensteanbieter „FlexiTrust 3.0 Release 0421“ wurde erfolgreich nach der Prüfstufe **EAL3 mit Zusatz** der **CC** in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung

Sicherheitsbestätigung T-Systems. 02126.TE.11.2004
© T-Systems GEI GmbH, 2004

Adresse: Rabinstr.8, 53111 Bonn
Telefon: 0228/9841-0
Fax: 0228/9841-60
Web: www.t-systems-ict-security.de
www.t-systems-zert.com