Sicherheitsbestätigung

T-Systems.02245.TE.12.2013

FlexiTrust Version 3.6.1 Release 1111

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]

Gültig bis: 31.12.2014

Bestätigung
T-Systems.02245.TE.12.2013

T-Systems GEI GmbH
- Zertifizierungsstelle -

Vorgebirgsstr. 49, 53119 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 15 Abs. 2 und 4, § 11 Abs. 3 SigV,
dass die

technische Komponente für Zertifizierungsdienste

FlexiTrust Version 3.6.1 Release 1111

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02245.TE.12.2013

Bonn, den 20.12.2013

_____
Dr. Igor Furgel
Leiter der Zertifizierungsstelle

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 (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) (BGBl. Jahrgang 2009, Teil I S. 2091)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) (BGBl. I S. 1542)

Die Bestätigung zur Registriernummer T-Systems.02245.TE.12.2013 besteht aus 28 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Die technische Komponente für Zertifizierungsdienste „FlexiTrust Version 3.6.1 Release 1111“.

1.2 Auslieferung

Die Auslieferung des Produktes FlexiTrust Version 3.6.1 Release 1111 erfolgt durch persönliche Übergabe am Einsatzort durch den Hersteller an den Benutzer (Betreiber). Die Auslieferung erfolgt im Vier-Augen-Prinzip und wird durch zwei instruierte Mitarbeiter des Herstellers durchgeführt. Das Erstellen der Auslieferung erfolgt in der sicheren Umgebung des Herstellers. Der Evaluierungsgegenstand (als EVG oder TOE abgekürzt) wird vom Hersteller installiert, konfiguriert und im funktionsfähigem (betriebsbereiten) Zustand dem Benutzer übergeben, der einer sicheren Konfiguration des EVG entspricht. Neben den auszuliefernden Dateien werden Prüflisten erstellt und ausgeliefert, die den Namen, die Dateirechte der ausgelieferten Daten und den MD5-Hashwert dieser Daten enthält. Desweiteren erhält der Benutzer das Dokument „Auslieferungs-, Installations-, Generierungs- und Anlaufprozeduren“, um sich über seine Pflichten und Aufgaben zu informieren.

Die auszuliefernden Daten und Prüflisten werden auf einem einmal beschreibbaren Datenträger in einem versiegelten Umschlag persönlich von einem autorisierten Mitarbeiter des Herstellers an den Kunden übergeben. Die an der Übergabe beteiligten Personen werden von Hersteller und Kunde im Voraus mitgeteilt und müssen sich vor der Übergabe durch ein amtliches Dokument identifizieren. Die Auslieferung des einsatzbereiten EVG wird protokolliert und vom Benutzer dem Hersteller durch Unterschrift bestätigt (Übergabeprotokoll).

Der Benutzer identifiziert den EVG anhand der Begleitdokumente (siehe Tabelle 1 weiter unten) und während der Installation durch die Überprüfung der erzeugten Hashwerte mit den in den Lieferdokumenten aufgeführten Hashwerten. Auch dieser Vorgang wird protokolliert. Das Übergabeprotokoll wird nach der Überprüfung der Hashwerte der Dateien an den Hersteller ausgehändigt, sodass Ausfertigungen der Protokolle und Formulare sowohl beim Hersteller als auch beim Benutzer vorhanden sind.

1.3 Lieferumfang

Das Produkt besteht aus Software und Handbüchern. Der Lieferumfang umfasst:

Produktname	Gegenstand	Software Version / Release Dokumentation	Datum
FlexiTrust Version 3.6.1 Release 1111	Binärpakete der Systeme CA und IS	Siehe Tabelle 2	-
	Binärpakete Kartentreiber PKCS#11	Siehe Tabelle 2	-
	Vorkonfiguration und Konfigurationsskripte (werden im Rahmen der Initialisierung/Installation angepasst)	-	-
	Benutzerhandbuch	1.10	16.07.2013
	Administrationshandbuch	2.7	17.07.2013
	Auslieferungs-, Installations-, Generierungs- und Anlaufprozeduren	3.6	08.07.2013

Tabelle 1: Lieferumfang FlexiTrust Version 3.6.1 Release 1111

Der Anwender identifiziert die Lieferung des EVGs anhand der Begleitdokumente und während der Installation durch die Überprüfung der erzeugten MD5-Hashwerten der Binärpakete der Systeme CA und IS und der Binärpakete des Kartentreiber PKCS#11 mit den in den Lieferdokumenten aufgeführten Hashwerten (siehe Tabelle 2).

Dateiname	Version	Hashwert (MD5)
cardman.jar	1.1	5d254d1597e12e37949bfaac92af37ef
fs_codec.jar	1.1	0894a267481bec89cfb596059edd994b
fs_util.jar	1.1.2.1	c5eb0f2e147dfbbe7f513cdddee87f6e
is.jar	1.1.2.1	946ed24c5c6ab1734a5d463ec492c634
ka_init.jar	1.1.2.1	ffb80ed9523731676f04158785c66593
ldapclient.jar	1.1	409467612c60e95b55a8869f3ebd3ced
leanca.jar	1.1.2.2	0f3f3192b2faa694b4748b6277184956
libpkcs11bna.so	1.1	92f21077426fedd1c6f20478b7c76623
libnativepkcs11.so	1.1	799979d3541a4ca42a7302768179d205
lws.jar	1.1	c23f9956f2c916751b3de9920c90cb9c
p11.jar	1.1	db7a9a0fe8fd5a54a9dccef979f26f72
pass_sharing.jar	1.1	6331154a8b2b63a87e983dae2b452b99
pin_sharing.jar	1.1	f97aa671c2f31ab2b24720aeffdc0732
secret_sharing.jar	1.1	d30375029ecc6739e7c9e63f4c9764ed

Tabelle 2: Binärpakete von Teilsystemen CA/IS und Kartentreiber PKCS #11

Weitere Softwarepakete, die für den Betrieb des EVG erforderlich bzw. vom Hersteller für die Interaktion mit dem EVG vorgesehen sind, gehören optional zum Lieferumfang (Binärpaket der Komponente RA, Binärpakete andere Kartentreiber, MySQL Datenbank, OpenLDAP). Sie sind nicht Teil des EVG. Die für den Betrieb des Produktes erforderliche Einsatzumgebung und die erforderlichen bestätigten Komponenten anderer Hersteller sind in Abschnitt 3.2 angegeben.

1.4 Antragsteller dieser Bestätigung und Hersteller des Produkts

Der Antragsteller für das aktuelle Bestätigungsverfahren ist

FlexSecure GmbH
Industriestraße 12
64297 Darmstadt

2. Funktionsbeschreibung

Der EVG[3] FlexiTrust Version 3.6.1 Release 1111 ist teils eine technische Komponente für Zertifizierungsdienste teils eine Signaturanwendungskomponente gemäß §2 SigG:

„Im Sinne dieses Gesetzes sind [...]

11. „Signaturanwendungskomponenten“ Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

12. „Technische Komponenten für Zertifizierungsdienste“ Software- oder Hardwareprodukte, die dazu bestimmt sind, […] b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten […]“

2.1 Kurzbeschreibung

Der FlexiTrust Version 3.6.1 Release 1111 stellt Funktionen für den Betrieb eines **Zertifizierungs-** und **Revokationsdienstes** zur Verfügung. Aus diesen Diensten heraus werden Daten generiert, die für den Betrieb eines Verzeichnisdienstes notwendig sind.

FlexiTrust Version 3.6.1 Release 1111 ist mandantenfähig, daher können mehrere logisch voneinander getrennte (virtuelle) Trustcenter verwaltet werden. Es ist dabei sichergestellt, dass die Verarbeitung der Zertifikate strikt nach Mandanten getrennt erfolgt.

Der **Zertifizierungsdienst** ermöglicht die Erzeugung qualifizierter und nicht qualifizierter Zertifikate[4]. Die erstellten Zertifikate werden zum Zweck der Personalisierung einer SEE (Speicherung der Zertifikate auf der SEE, für die sie bestimmt sind) exportiert. Des Weiteren werden Zertifikate nach ihrer Aktivierung exportiert, um sie in einem Auskunfts- bzw. Verzeichnisdienst nachprüfbar und ggf. abrufbar zu halten. Der FlexiTrust Version 3.6.1 Release 1111 unterstützt aktiv die Trennung zwischen nur nachprüfbaren und abrufbaren Zertifikaten.

Der EVG kann folgende Zertifikate erstellen:

- selbst-signierte Root-Zertifikate
- Cross-Zertifikate

[3] Evaluierungsgegenstand (Engl.: TOE)

[4] Diese Bestätigung bezieht sich ausschließlich auf das Management von qualifizierten Zertifikaten

- Public-Key-Zertifikate
- Attribut-Zertifikate

Anträge auf Zertifizierung für die unterstützten Zertifikate können dem EVG im XML-Format über das Dateisystem zugeführt werden. Zu signierende Daten werden dann der dem jeweiligen Mandanten zugeordneten EVG-externen Signaturerstellungseinheit[5] zur Signierung zugeführt.

Nach dem Signaturprozess werden die Zertifikate der Prozessdatenbank zugeführt, aus der sie entnommen und zur Personalisierung der zugehörigen SEE ins Dateisystem exportiert werden[6]. Damit ist die Zertifizierung seitens des EVG abgeschlossen.

Die Aktivierung von Zertifikaten erfolgt über die Dateisystem-Schnittstelle. Die entsprechende EVG-Komponente wertet die Prozessdatenbank für das Zertifikat aus und entscheidet, ob das Zertifikat lediglich nachprüfbar oder auch abrufbar gehalten werden soll und führt es der Aktivierungsdatenbank zu. Im letzteren Fall wird das Zertifikat auch zusätzlich in einem separaten Bereich der Aktivierungsdatenbank gespeichert, in dem zwecks Unterscheidungsmöglichkeit nur die abrufbaren Zertifikate enthalten sind. Damit ist die Aktivierung des Zertifikats seitens des EVG abgeschlossen.

Durch den **Revokationsdienst** wird die vorzeitige Sperrung von Zertifikaten (vor Ablauf ihrer Gültigkeitsdauer) ermöglicht. Dazu werden Sperrinformationen generiert und exportiert, die für einen Auskunfts- bzw. Verzeichnisdienst verwendet werden können.

Die Sperrung von Zertifikaten ist ebenfalls antragsbasiert und kann über die bereits genannte Schnittstelle im XML-Format initiiert werden.

Die entsprechende EVG-Komponente prüft, ob das jeweilige Zertifikat existiert bzw. ob es bereits gesperrt wurde, und ordnet die Sperrung über die Mandantenkennung der entsprechenden Signaturerstellungseinheit zu. Die Sperrinformationen des Mandanten werden um die aktuelle Sperrung erweitert und mit der gültigen gesetzlichen Zeit versehen, wonach sie der EVG-externen Signaturerstellungseinheit[7] zur Signatur zugeführt werden. Nach deren Abschluss werden die signierten Sperrinformationen in die Prozessdatenbank geschrieben und an die entsprechende EVG-Komponente exportiert. Diese führt die Sperrinformationen dann der Aktivierungsdatenbank zwecks Veröffentlichung zu.

[5] Nicht Gegenstand der Bestätigung

[6] Dieser Informationsabfluss und die Weiterverarbeitung des exportierten Zertifikats gehört nicht zur Sicherheitsfunktionalität des EVG.

[7] Nicht Gegenstand der Bestätigung

Der FlexiTrust Version 3.6.1 Release 1111 beinhaltet keine Registrierungsfunktionalität. Diese Funktionalität wird durch die vorgelagerte Komponente FlexiTrust-RA[8] geleistet.

Der FlexiTrust Version 3.6.1 Release 1111 beinhaltet keine Funktionalität zur Erstellung von Zeitstempeln.

Die Beantwortung von Statusanfragen, die Datenhaltung im Zertifikatsverzeichnis sowie die öffentlichen Kommunikationsanbindung sind nicht Bestandteil des EVG.

Im Sinne des Signaturgesetzes umfasst FlexiTrust Version 3.6.1 Release 1111 folgende Einzelkomponenten:

1. Signaturanwendungskomponente im Zertifizierungsdienst:
   Diese Komponente führt im Sinne von SigG, § 2, Nr. 11 a) Zertifikate dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zu.

2. Signaturanwendungskomponente im Revokationsdienst:
   Diese Komponente führt im Sinne von SigG, § 2, Nr. 11 a) Sperrinformationen dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zu.

3. Technische Komponente für Zertifizierungsdienste:
   Diese Komponente führt qualifizierte Zertifikate und Sperrinformationen einer aus Sicht des EVG externen Komponente zu, um diese im Sinne von SigG, § 2, Nr. 12 b) nachprüfbar bzw. abrufbar zu halten. Nur nachprüfbare qualifizierte Zertifikate werden nicht für den Abruf exportiert. Rückwirkende oder mehrfache Sperrungen werden verhindert, um zu gewährleisten, dass Sperrungen nicht rückgängig gemacht werden.

2.2 Beschreibung der evaluierten Sicherheitsfunktionalität

Der EVG bietet die folgenden Sicherheitsfunktionen, die nachfolgend erläutert werden. Hierbei ist zu beachten, dass die vorliegende Bestätigung sich **ausschließlich auf qualifizierte** elektronische Signaturen bezieht; alle etwaigen Angaben zu anderen Arten von Signaturen als qualifizierte elektronische Signaturarten dienen ausschließlich Information des Lesers.

Die folgenden Sicherheitsfunktionen sind aus dem Security Target (ST) übernommen. Die verwendeten Rollen, Daten, Operationen und Subjekte sind im ST[9], Kap. 6.1 bis 6.4 erläutert.

Protokollierung AUDIT

[8] Nicht Gegenstand der Bestätigung

[9] Security Target: „Sicherheitsvorgaben für FlexiTrust Version 3.6.1 Release 1111“, Version 3.46, 18.12.2013

AUDIT*.1: Alle Anwendungen des EVG initiieren die Protokollierung unmittelbar nach dem Start. Der Betrieb der Software mit ausgeschalteter Protokollierung ist nicht möglich. Das Beenden einer Anwendung wird protokolliert. Start und Beendigung einer Anwendung sind gleichbedeutend mit Beginn und Ende der Protokollierung.

AUDIT*.2: Resultieren protokollierbare Ereignisse aus Aktionen, die von identifizierten Benutzern ausgelöst wurden, wird zusätzlich die Identität des Benutzers protokolliert.

AUDIT*.3: Folgende Informationen werden für Ereignisse protokolliert: Zeit, Datum und Art eines Ereignisses zusammen mit dem auslösenden Subjekt, der Typ des Ereignisses (Fatal, Critical, Warning, Info, usw.) und der Erfolg oder Misserfolg des Ereignisses.

AUDIT*.4: Die Ereignisse gemäß der Tabelle 6.3 im ST werden protokolliert. Zusätzlich wird die Überprüfung der mathematischen Korrektheit einer qualifizierten Signatur (korrekt, nicht korrekt) protokolliert.

AUDIT*.5: Bei dem Ereignis der Zuführung von SIGNED DATA zur Erzeugung einer elektronischen Signatur an eine SEE wird zusätzlich protokolliert: Identifikationsmerkmal der SEE, Stand des Fehlbedienungszählers der SEE, Mandantenzuordnung der SEE. Dies gilt insbesondere für die Erzeugung qualifizierter elektronischer Signaturen.

Identifikation IA

IA*.1: Das Subjekt CA-IMP importiert Anträge von Benutzern, die in der Rolle ANTRAGSTELLER agieren. Integrität der Antragsdaten sowie Identität der Benutzer werden mittels an den zu importierenden Daten angebrachten Signatur festgestellt. Die Signaturprüfung erfolgt unter Verwendung von in der IT-Umgebung des EVG gespeicherten Zertifikaten. Als Benutzer wird ausschließlich die vorgelagerte FlexiTrust-RA akzeptiert.

IA*.2: Benutzer, die in der Rolle UNTERZEICHNER agieren, um SEE zu aktivieren, werden durch das Subjekt CA-SIGN identifiziert. Dies geschieht, in dem geprüft wird, ob unter Verwendung der in der IT-Umgebung gespeicherten PIN-Shares und zwei Bedienerkarten die PIN der zu aktivierenden SEE entschlüsselt werden kann. Es wird geprüft, ob die notwendigen Schlüssel-Shares vorhanden sind. Um Shares zu entschlüsseln, muss sich der Benutzer durch PIN-Eingabe gegenüber seiner Bediener-Chipkarte identifizieren.

IA*.3: Das Subjekt IS importiert Anträge von Benutzern, die in der Rolle ANTRAGSTELLER agieren. Die Integrität der Antragsdaten sowie die Identität des Benutzers werden mittels an den zu importierenden Daten angebrachten Signatur

festgestellt. Die Signaturprüfung erfolgt unter Verwendung von in der IT-Umgebung des EVG gespeicherten Zertifikaten.

IA*.4: Nicht identifizierte Benutzer können mit dem System keine Interaktionen durchführen, für die eine Identifikation notwendig ist.

Durchsetzung von Sicherheitspolitiken ENF

ENF*.1: Die Aktivierung einer Signaturerstellungseinheit (SEE) erfolgt mittels ihrer PIN (IDENTIFICATION DATA). Diese werden nach dem Verfahren nach Shamir[10][11] rekonstruiert. Jedes Share einer PIN ist mit dem Schlüssel genau einer Bedienerkarte verschlüsselt und als verschlüsseltes Share im System abgelegt (CONFIGURATION DATA). Nur die Inhaber dieser Bedienerkarten können die Rolle UNTERZEICHNER annehmen.

Zum Berechnen der PIN einer SEE sind wenigstens zwei Bedienerkarten erforderlich. Die PIN wird nur im Speicher entschlüsselt und zusammengesetzt.

Vor der Zuführung der PIN wird der Fehlbedienungszähler der SEE ausgewertet. Wenn dieser anzeigt, dass eine Fehlbedienung stattgefunden hat, wird die Aktivierung der SEE nicht durchgeführt.

Die PIN wird nach dem Versuch der Aktivierung der SEE aus dem Speicher gelöscht.

Nachdem eine SEE aktiviert wurde, gilt mindestens eine von beiden Begrenzungen für die Erstellung von Signaturen durch diese SEE:

- es kann nur eine festgelegte Zahl von Signaturen erstellt werden
- es können nur für eine festgelegte Zeitdauer Signaturen erstellt werden

Welche dieser Begrenzungen tatsächlich gilt und welche begrenzende Zahl bzw. Zeitdauer gilt, wird vom EVG anhand von CONFIGURATION DATA ermittelt.

Das nach der Aktivierung an die SEE gebundene Subjekt CA-SIGN agiert im Auftrag eines Benutzers in der Rolle UNTERZEICHNER. Eine korrekt aktivierte SEE, d.h. die zugeführte PIN wurde von der SEE akzeptiert, wird anhand des zugehörigen öffentlichen Schlüssels per Konfiguration einem Mandanten zugeordnet. Die Mandantenkennung wird im Attribut SEEMANDANT des Subjekts CA-SIGN gespeichert. Die Rolle UNTERZEICHNER wird für einen Benutzer dadurch eingeschränkt, dass nur für bestimmte (an einen Mandanten gebundene)

[10] Shamir, Adi: „How to share a secret. Communications of the ACM“, 22(11):612-613, November 1979

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI): „Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, BSI TR-02102, Version 2013.02, 9. 01. 2013

SEE PIN-Shares konfiguriert werden können. Ob ein Benutzer in der Rolle UNTERZEICHNER für einen gegebenen Mandanten agieren darf, richtet sich danach, ob er in der Lage ist, entsprechende PIN-Shares zum Aktivieren einer SEE des Mandanten zu entschlüsseln.

ENF*.2: Der Importer der CA (Subjekt CA-IMP) agiert im Auftrag von Benutzern in der Rolle ANTRAGSTELLER. Der Importer überprüft regelmäßig (polling) die Import-Schnittstelle auf das Vorhandensein neuer, zu importierender Anträge. Sind Anträge vorhanden, werden sie importiert und verarbeitet. Es gibt keine andere Möglichkeit, Anträge in die CA zu importieren.

Die CA stellt anhand der importierten Daten fest, um welche Art von SIGNED DATA es sich handelt. Es werden nur Anträge auf Zertifizierung, das Attribut TYP erhält den Wert ZERT, und Anträge auf Sperrung, das Attribut TYP erhält den Wert SPL, verarbeitet.

Für alle importierten Anträge ist sichergestellt, dass der Mandant, in dessen Anwendungsbereich der Antrag bearbeitet werden soll, angegeben ist. Das Attribut ZIELMANDANT wird entsprechend initialisiert. Es wird sichergestellt, dass der im Antrag angegebene Mandant im EVG konfiguriert ist.

Für Zertifizierungsanträge (TYP hat den Wert ZERT) wird geprüft, dass im Antrag angegeben ist, ob das Zertifikat später im Rahmen der Aktivierung veröffentlicht werden soll oder nicht. Das Attribut PUBLIC wird entsprechend initialisiert. Für Sperranträge wird kein solches Attribut unterstützt.

ENF.2.1: Die CA kann durch die Schnittstelle zum Triggern von Antragsimporten benachrichtigt werden, dass neue, zu importierende Anträge vorhanden sind. Der Import erfolgt unverzüglich nach Erhalt der Benachrichtigung.

ENF*.3: Die Zuführung von SIGNED DATA zur SEE kann nur im Subjekt CA-SIGN erfolgen. Diese Zuführung erfolgt ohne Sicherheitsattribute. Das Subjekt CA-SIGN verarbeitet nur SIGNED DATA, die vom Subjekt CA-IMP zugeführt werden.

Die SIGNED DATA wird nur dann der SEE zugeführt, wenn der Wert des Attributs SEEMANDANT des Subjekts CA-SIGN mit dem Wert des Attributs ZIELMANDANT der SIGNED DATA übereinstimmt.

Die SIGNED DATA wird unmittelbar vor der Zuführung zur Signatur mit der gültigen gesetzlichen Zeit versehen.

Nach Zuführung der SIGNED DATA zur Signaturerstellung wird die mathematische Korrektheit der Signatur überprüft. Außerdem wird für qualifiziert agierende Mandanten überprüft, ob die qualifizierte elektronische Signatur, die von der SSEE erzeugt wurde, einem Zertifikat zugeordnet werden kann, welches für die Signatur des jeweiligen TYP der SIGNED DATA (ZERT, SPL) vorgesehen ist.

Im Folgenden sind die Unterschiede der Signaturerstellung für die unterschiedlichen Typen von SIGNED DATA aufgeführt:

ENF*.3.1: Signatur von SIGNED DATA mit TYP ZERT:

Die CA vergibt für SIGNED DATA des Typs ZERT eine eindeutige Zertifikats-ID vor der Zuführung zur Signaturerstellung. Die CA kann so konfiguriert werden, dass die SIGNED DATA des TYP ZERT unmittelbar vor der Übertragung an die Signaturkarte dem Benutzer in der Rolle UNTERZEICHNER gemäß der Normen Common PKI[12], Part1 eindeutig und frei von aktiven oder verdeckten Inhalten dargestellt und von ihm bestätigt werden muss. Nicht darstellbare Inhalte werden zeichenweise in einer anderen, darstellbaren Form angezeigt, und der Benutzer wird darüber informiert. Besteht der Bedarf, die Inhalte zu signierender Daten hinreichend erkennen zu lassen, muss die Konfiguration des EVG so gewählt werden, dass die Darstellung erfolgt.

Vor jedem Signaturvorgang wird geprüft, ob der Vorgang durch den UNTERZEICHNER autorisiert ist. Fällt die Prüfung negativ aus, wird dieser Vorgang nicht durchgeführt.

ENF*.3.2: Signatur von SIGNED DATA mit TYP SPL:

Der UNTERZEICHNER autorisiert alle Signaturvorgänge beim Aktivieren der SEE des Revokationsdienstes. Die CA prüft, ob das zu sperrende Zertifikat in der Aktivierungsdatenbank gespeichert ist. Existiert das Zertifikat in der Aktivierungsdatenbank nicht, wird die Sperrung mit einem Fehler abgebrochen. Die CA des Revokationsdienstes prüft die intern vorgehaltene Sperrliste gegen die in der Aktivierungsdatenbank gespeicherte Sperrliste, um festzustellen, ob die intern vorgehaltene Sperrliste aktuell ist. Hat die Sperrliste in der Aktivierungsdatenbank einen jüngeren Erstellungszeitpunkt, wird diese verwendet. Es wird in diesem Fall geprüft, dass die Sperrliste aus der Aktivierungsdatenbank mindestens alle Sperreinträge beinhaltet, die auch die lokal vorgehaltene Sperrliste beinhaltet hat.

Die Kommunikation mit der Aktivierungsdatenbank erfolgt über einen vertrauenswürdigen Kanal.

Die CA prüft, ob das zu sperrende Zertifikat bereits in die Sperrliste aufgenommen ist. Ist dies der Fall, wird die Sperrung mit einer Fehlermeldung abgebrochen. Alle in der aktuellen Sperrliste enthaltenen Sperrungen werden in die SIGNED DATA der neuen Sperrliste übernommen.

Die CA trägt direkt vor Zuführung zur SEE die gültige gesetzliche Zeit sowohl als Zeitpunkt der Sperrung des zu sperrenden Zertifikats als auch als Zeitpunkt der Erstellung der neuen Sperrliste ein.

12 Common PKI specifications for interoperable applications, version 2.0, T7 and TeleTrusT, 2009

Die Zuführung zur SEE erfolgt nach Bestehen aller Überprüfungen automatisch. Die SIGNED DATA wird nach Prüfung der Signatur zur aktuell in der CA vorgehaltenen Sperrliste.

ENF*.4: Das Subjekt IS agiert ausschließlich im Auftrag von Benutzern in der Rolle ANTRAGSTELLER.

Die IS überprüft regelmäßig (polling) die Schnittstelle für die Übermittlung von SIGNED DATA von der CA an die IS auf das Vorhandensein neuer, in diesem Sinne zu importierender SIGNED DATA. Ist SIGNED DATA vorhanden, werden diese importiert und verarbeitet. Beim Import stellt die IS anhand der importierten Daten fest, um welchen Typ von SIGNED DATA es sich handelt (TYP hat entweder den Wert ZERT oder SPL). Die Verarbeitung der beiden Typen von SIGNED DATA wird in den Abschnitten ENF*.4.2 und ENF*4.3 beschrieben.

Die IS nimmt nur SIGNED DATA an, welche von der CA stammen. Dies wird durch die Prüfung der Transportsignatur gewährleistet.

ENF.4.1: Die IS kann durch die Schnittstelle zum Triggern von Antragsimporten benachrichtigt werden, dass neue, zu importierende Anträge vorhanden sind. Der Import erfolgt unverzüglich nach Erhalt der Benachrichtigung.

ENF*.4.2: Die IS nimmt Sperrlisten (SIGNED DATA vom Typ SPL) von der CA entgegen.

In der Aktivierungsdatenbank existiert für jeden möglichen Mandanten (Attribut ZIELMANDANT) ein logisch von allen anderen Mandanten getrennter Bereich. Die Sperrliste wird umgehend in die Aktivierungsdatenbank exportiert, um sie für Statusauskünfte verfügbar zu machen. Die Speicherung erfolgt in den durch das Sicherheitsattribut ZIELMANDANT vorgegebenen logischen Bereich der Aktivierungsdatenbank. Dadurch wird die Sperrliste direkt mit dem Sicherheitsattribut verknüpft. Das Sicherheitsattribut TYP ergibt sich direkt aus der Struktur der SIGNED DATA.

Wird bei der Übermittlung der SIGNED DATA zur Aktivierungsdatenbank ein Fehler festgestellt, wird die Verarbeitung unterbrochen und eine Fehlermeldung erzeugt.

Vor der Übermittlung der SIGNED DATA wird die IT-Umgebung über die bevorstehende Veröffentlichung informiert. Die Veröffentlichung findet nur statt, wenn die IT-Umgebung die Bereitschaft der Aktivierungsdatenbank zum Empfang der SIGNED DATA meldet. Tritt ein Fehler auf oder meldet die IT-Umgebung, dass die Aktivierungsdatenbank nicht zum Empfang von SIGNED DATA bereit ist, so wird die Verarbeitung abgebrochen und eine Fehlermeldung erzeugt. Die IT-Umgebung wird außerdem über den Abschluss der Veröffentlichung und über bei der Übermittlung der SIGNED DATA zur Aktivierungsdatenbank aufgetretene Fehler informiert.

ENF*4.3: Die IS nimmt Zertifikate (SIGNED DATA vom Typ ZERT) von der CA entgegen. Die IS exportiert Zertifikate zum Zwecke der Personalisierung der SEE ohne Sicherheitsattribute in das Dateisystem und in die Prozessdatenbank.

ENF*.5: Das Subjekt IS agiert ausschließlich im Auftrag von Benutzern in der Rolle ANTRAGSTELLER.

Die IS überprüft regelmäßig (polling) die Schnittstelle für die Zuführung von Aktivierungsanträgen auf das Vorhandensein neuer, in diesem Sinne zu importierender Anträge. Sind Anträge vorhanden, werden sie importiert und verarbeitet.

Die IS stellt sicher, dass sich Aktivierungsanträge auf existierende Zertifikate (SIGNED DATA des Typs ZERT) beziehen und dass diese Zertifikate noch nicht aktiviert wurden.

In der Aktivierungsdatenbank existiert für jeden möglichen Mandanten (Attribut ZIELMANDANT) ein logisch von allen anderen Mandanten getrennter Bereich. Jeder solche Bereich ist in zwei logisch voneinander getrennte Teilbereiche, den Teilbereich “abrufbar” und den Teilbereich “nur nachprüfbar”, getrennt.

Die IS exportiert aktivierte Zertifikate in den gemäß Attribut ZIELMANDANT zugeordneten Bereich der Aktivierungsdatenbank. Dadurch sind die SIGNED DATA mit dem Sicherheitsattribut direkt verknüpft. Der Export findet in den Teilbereich “nur nachprüfbar” statt, um die Zertifikate nachprüfbar zu machen.

Hat das Attribut PUBLIC eines Zertifikats den Wert TRUE, wird es zudem als Kopie in den Teilbereich “abrufbar” exportiert, um es abrufbar zu machen. Die Verknüpfung eines Zertifikats mit dem Attribut PUBLIC resultiert aus der Tatsache, dass das Zertifikat im Teilbereich “abrufbar” gespeichert ist (PUBLIC hat den Wert TRUE) oder nicht (PUBLIC hat den Wert FALSE). Das Sicherheitsattribut TYP ergibt sich direkt aus der Struktur der SIGNED DATA.

Die IS kann so konfiguriert werden, dass die IT-Umgebung per Signal über eine bevorstehende Aktivierung informiert wird. Der Kommunikationskanal zur Aktivierungsdatenbank wird dann nur aufgebaut, wenn die IT-Umgebung das Signal positiv beantwortet und damit die Bereitschaft der Aktivierungsdatenbank zum Empfang der SIGNED DATA signalisiert. Tritt ein Fehler auf oder meldet die IT Umgebung einen negativen Status, so wird die Verarbeitung der Aktivierung abgebrochen und eine Fehlermeldung erzeugt. Die IS kann zudem so konfiguriert werden, dass sie die IT-Umgebung nach der Aktivierung per Signal über den Abschluss der Aktivierung informiert.

Wenn bei der Übermittlung der SIGNED DATA zur Aktivierungsdatenbank ein Fehler auftritt, wird die Verarbeitung unterbrochen und eine Fehlermeldung erzeugt.

Schutz von Benutzer-/TSF-Daten und der Kommunikation PROTECT

PROTECT*.1: Folgende CONFIGURATION DATA sind durch Verschlüsselung geschützt: Aktivierungsdatenbank -Passwörter, Datenbank-Passwörter, KeyStore-Passwörter für interne Signaturen (durch Verschlüsselung geschützte CONFIGURATION DATA). Sie werden beim Start der Komponenten IS und CA durch zwei Bediener-Karten entschlüsselt und folgendermaßen der Java-Virtual-Machine im RAM zur Verfügung gestellt, so dass ausschließlich die Applikationen des EVG darauf zugreifen können:

Auf die durch Verschlüsselung geschützten CONFIGURATION DATA kann über einen Methoden-Aufruf innerhalb der Java-Virtual-Machine zugegriffen werden.

Damit wird gewährleistet, dass sich nur die dafür autorisierten Applikationen mit der Datenbank einen Kommunikationskanal aufbauen können bzw. interne Signaturen zur Transportsicherung erzeugen können. Es wird auch gewährleistet, dass nur die dafür autorisierten Applikationen mit der Aktivierungsdatenbank einen Kommunikationskanal für Schreibzugriffe aufbauen können. Kein anderes Subjekt kann die Datenbank und die passwortgeschützten KeyStores benutzen. Kein anderes Subjekt kann einen Kommunikationskanal für den Schreibzugriff mit der Aktivierungsdatenbank aufbauen. Somit werden sichergestellt:

- Schutz vor Manipulation von Benutzer-Daten und TSF-Daten in der Datenbank und in der Aktivierungsdatenbank. Schutz vor Manipulation der damit verknüpften Sicherheitsattribute.

- Schutz der Prozesssteuerung. Der EVG kann für die Aktualisierung von PRODUCT DATA, Export und Publikation von SIGNED DATA, Änderung des Attributs PUBLIC von SIGNED DATA nicht umgangen werden.

- Authentizität des EVG gegenüber der Datenbank

- Authentizität des EVG bei Schreibzugriffen gegenüber der Aktivierungsdatenbank

- Schutz des Mechanismus der internen Signaturen und somit Sicherstellung der Integrität und Authentizität von PRODUCT DATA und SIGNED DATA (CA-IS).

PROTECT*.2: Die durch den Importer der CA importierten SIGNED DATA sind durch eine Signatur geschützt. Schlägt die Verifikation dieser Signatur fehl, nimmt der EVG eine Modifikation der zugeführten Daten an bricht die weitere Verarbeitung ab.

PROTECT*.3: Die durch die IS importierten Aktivierungs-Kommandos sind durch eine Signatur geschützt. Schlägt die Verifikation dieser Signatur fehl, nimmt der EVG eine Modifikation der zugeführten Daten an bricht die weitere Verarbeitung ab.

PROTECT*.4: Die PRODUCT DATA (Zertifikats- und Sperr-Anträge) und SIGNED DATA (Zertifikate und Sperrinformationen) werden beim Transport zwischen den Komponenten CA und IS (materiell getrennte Teile des EVG) durch eine interne Signatur geschützt. (Zum Schutz des Mechanismus selbst, siehe PROTECT.1). Dessen Authentizität und Integrität werden somit sichergestellt. Wurden während dem Transport Daten modifiziert, wird die Signatur ungültig. In diesem Fall wird eine Fehlermeldung ausgegeben und die Verarbeitung wird unterbrochen.

PROTECT*.5: Die SIGNED DATA (Zertifikate und Sperrinformationen) werden beim Transport zwischen dem EVG und der Aktivierungsdatenbank durch einen vertrauenswürdigen Kanal geschützt. Dieser Kanal wird durch den EVG aufgebaut. Wird die Integrität der Verbindung verletzt, indem Daten während des Transports eingefügt, manipuliert, gelöscht oder alte Daten erneut zugeführt werden, löst dies einen Protokollfehler aus. Ein solcher Fehler wird protokolliert und die Verarbeitung wird abgebrochen.

PROTECT*.6: Vor dem Übertragen der IDENTIFICATION DATA (PIN der Signaturkarten) wird ein sicherer Kommunikationskanal mittels Secure-Messaging aufgebaut. Im Rahmen des Secure-Messagings werden die übertragenen Daten durch Verschlüsselung und einen MAC-Code vor Preisgabe, Manipulation, Löschen, erneutem Zuführen und Einfügen geschützt. Die IDENTIFICATION DATA wird mittels dieses Verfahrens gesichert an die SEE übertragen. Der EVG wird durch diese PIN-Authentisierung gegenüber der SEE authentifiziert. Die SEE-Authentifikation wird implizit dadurch durchgeführt, dass die PIN zur SEE passt.

SIGNED DATA wird erst nach erfolgreicher Identifikation übertragen werden. Die Übertragung der SIGNED DATA erfolgt ebenfalls geschützt durch Secure-Messaging. Wird die Integrität der Verbindung bei der Übertragung der PIN oder von SIGNED DATA verletzt, indem Daten während des Transports eingefügt, manipuliert, gelöscht oder alte Daten erneut zugeführt werden, löst dies einen Protokollfehler aus. Ein solcher Fehler wird protokolliert und die Verarbeitung wird abgebrochen.

PROTECT*.7: Der SEE werden Hash-Werte zugeführt, die aus den zugehörigen SIGNED DATA berechnet werden. Für die Berechnung der Hash-Werte (full-length message digests) wird eines der Verfahren SHA-224, SHA-256, SHA-384 und SHA-512 gemäß „FIPS PUB 180-4 Secure Hash Standard (SHS)“, March 2012 und Kapitel 5.2.1 aus „Quynh Dang: NIST Special Publication 800-107 Recommendation for Applications Using Approved Hash Algorithms“, Revision 1, August 2012 verwendet. Einzelne Verfahren können durch Konfiguration von der Verwendung ausgeschlossen werden.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Produkt erfüllt die Anforderungen nach:

SigG

§ 8 Sperrung von qualifizierten Zertifikaten

§ 8 (1) und § 8 (2)

Der Zertifizierungsdiensteanbieter hat ein qualifiziertes Zertifikat unverzüglich zu sperren, […] Die Sperrung muss den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig. […]

Diese Anforderungen sind durch die Sicherheitsfunktionen ENF*.1, ENF*.2, ENF*.3, ENF*.4, ENF*.5, IA*.3, PROTECT*.2, PROTECT*.3, PROTECT*.4, PROTECT*.5, PROTECT*.6 und PROTECT*.7 umgesetzt und durch IA*.1 und PROTECT*.2 unterstützt (s. Abschn. 2.2 weiter oben).

Anmerkung: Der EVG unterstützt in diesem Zusammenhang u.a. die Verpflichtung zur unverzüglichen Sperrung.

§ 17 Produkte für qualifizierte elektronische Signaturen

§ 17 (1)

Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen […].

Diese Anforderungen sind durch die Sicherheitsfunktionen ENF*.1, ENF*.2, ENF*.3, ENF*.4, ENF*.5, IA*.1, IA*.2, IA*.3, PROTECT*.3, PROTECT*.6 und PROTECT*.7 umgesetzt und durch PROTECT*.2 unterstützt (s. Abschn. 2.2 weiter oben).

Anmerkung: Der EVG unterstützt in diesem Zusammenhang die Verwendung von TOE-externen SSEE zur Speicherung von Signaturschlüsseln sowie die Verwendung von TOE-externen SSEE zur Erzeugung qualifizierter elektronischer Signaturen und den Schutz der

Signaturschlüssel gegen unberechtigte Nutzung. Der EVG stellt sicher, dass Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar sind.

§17 (2)

Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht.

Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,
1. auf welche Daten sich die Signatur bezieht, […]
4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, […] aufweisen […].

Diese Anforderungen sind durch die Sicherheitsfunktion ENF*.1, ENF*.2, ENF*.3, ENF*.4, ENF*.5, IA*.3 und PROTECT*.3 umgesetzt und durch IA*.1 und PROTECT*.2 unterstützt (s. Abschn. 2.2 weiter oben).

§ 17 (3) Nr.2

Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um […]

2. qualifizierte Zertifikate, die gemäß § 5 Abs. 1 Satz 3 nachprüfbar oder abrufbar gehalten werden, vor unbefugter Veränderung und unbefugtem Abruf zu schützen

Diese Anforderungen sind durch die Sicherheitsfunktionen ENF*.1, ENF*.2, ENF*.3, ENF*.4, ENF*.5, IA*.1, IA*.3, PROTECT*.2, PROTECT*.3, PROTECT*.4, PROTECT*.5, PROTECT*.6, PROTECT*.7 umgesetzt (s. Abschn. 2.2 weiter oben).

SigV

§ 4 Führung eines Zertifikatsverzeichnisses

§ 4 (1) und § 4 (2)

Der Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens fünf weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates

endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 3 des Signaturgesetzes zu führen.

Ein akkreditierter Zertifizierungsdienstanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 3 des Signaturgesetzes zu führen.

Um diese Anforderungen technisch zu unterstützen, werden qualifizierte Zertifikate und Sperrinformationen durch den EVG nach ihrer Ausstellung im Rahmen ihrer Aktivierung für die Zuführung zu einem Verzeichnisdienst zur Verfügung gestellt:
Das ist durch die Sicherheitsfunktionen ENF*.1, ENF*.2, ENF*.3, ENF*.4, ENF*.5, IA*.3 und PROTECT*.3 umgesetzt und werden von IA*.1 und PROTECT*.2 unterstützt (s. Abschn. 2.2 weiter oben).

§ 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen

§ 15 (2), Nr. 1

Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

1. bei der Erzeugung einer qualifizierten elektronischen Signatur

a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,

b) eine Signatur nur durch die berechtigt signierende Person erfolgt,

c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird […]

Diese Anforderungen sind durch die Sicherheitsfunktionen ENF*.1, ENF*.2, ENF*.3, ENF*.4, ENF*.5, IA*.1, IA*.2, IA*.3, PROTECT*.6, PROTECT*.7 umgesetzt und durch IA*.4 unterstützt (s. Abschn. 2.2 weiter oben).

§ 15 (3)

Technische Komponenten nach § 17 Abs. 3 des Signaturgesetzes müssen gewährleisten, dass die Sperrung eines qualifizierten Zertifikates nicht unbemerkt rückgängig gemacht werden kann […].

Diese Anforderungen sind insbesondere durch die Sicherheitsfunktionen

ENF*.1, ENF*.2, ENF*.3, ENF*.4, ENF*.5, IA*.1, IA*.3, PROTECT*.3, PROTECT*.4, PROTECT*.5, PROTECT*.6 und PROTECT*.7 umgesetzt und durch PROTECT*.2 unterstützt (s. Abschn. 2.2 weiter oben).

Anmerkung: Der EVG unterstützt in diesem Zusammenhang u.a., dass nur nachprüfbare Zertifikate nicht öffentlich abgerufen werden können.

§ 15 (4)

Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

Diese Anforderung ist vor allem durch die Sicherheitsfunktion ENF*.1, IA*.1, IA*.2, IA*.3, PROTECT*.6, AUDIT*.1, AUDIT*.2, AUDIT*.3, AUDIT*.4 und AUDIT*.5 umgesetzt (s. Abschn. 2.2 weiter oben).

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen durch den Produktbetreiber / Produktbenutzer gewährleistet sind:

3.2.1 Anforderungen an die technische Einsatzumgebung

Der FlexiTrust Version 3.6.1 Release 1111 besteht nur aus Software, daher werden für den Betrieb folgende Komponenten benötigt, die nicht Teil des EVG sind:

Komponente	Software	Version
Betriebssystem	Oracle Solaris	Sparc Solaris 10 9/10
Laufzeitumgebung	Oracle Java SE Runtime Environment (JRE), incl. Unlimited Strength Java Cryptography Extension (JCE) Policy Files	Version 7, Update 21, Build 1.7.0_21
Prozessdatenbank	MySQL	5.1.63
Aktivierungsdatenbank	OpenLDAP	2.4.23
Verschlüsselung	OpenSSL	1.0.0d
Interne DB	BerkeleyDB	4.8.30
Kartenleser Treiber	Kobil CT-API (für Solaris)	2006-01-20

Tabelle 3: Technische Einsatzumgebung: Software

Komponente	Hardware / Version	Bestätigung nach SigG
SEE	„Signaturerstellungseinheit (SEE) TCOS 3.0 Signature Card, Version 1.1", Ausprägung „Signature Card 3.0M, Version 1.0"	TUVIT.93146.TE.12.2006 Gültig bis 31.12.2014
Kartenleser	Kartenterminal KOBIL Chipkartenterminal KAAN Advanced (USB/RS232), Hardware Version K104R3, Firmware Version 1.19	Bestätigungsnummer Nachtrag T-Systems.02207.TU.04.2008 zur Bestätigung BSI.02050.TE.12.2006 vom 20.12.2006 Kein Gültigkeitsdatum
Hardwareplattform	Oracle SPARC Server	-
Bediener Chipkarten	E4NetKey TCOS Version 2.03	-

Tabelle 4: Technische Einsatzumgebung: Hardware

Es sei angemerkt, dass das Chipkartenterminal im Rahmen seiner Verwendung durch den EVG nicht Teil einer Signaturanwendungskomponente ist. Die Kommunikation des EVGs mit der externen (sicheren) Signaturerstellungseinheit erfolgt unmittelbar über einen geschützten Kanal, der vom Chipkartenterminal unabhängig ist. Diese Ende-zu-Ende-Verbindung wird sowohl für den Transport der Identifikationsdaten als auch für die Zuführung von Daten zur elektronischen Signatur verwendet. Daher ist es im Rahmen der vorliegenden Bestätigung ohne Bedeutung, ob der in der Tabelle 4 aufgeführte Kartenleser SigG-bestätigt ist oder nicht.

Das Produkt ist ausschließlich für die Nutzung im geschützten Einsatzbereich mit geregelten Zugriffsmöglichkeiten vorgesehen.

Das Produkt FlexiTrust Version 3.6.1 Release 1111 benötigt für den Betrieb eine Hardwareplattform, ein Betriebssystem und eine Java-Laufzeitumgebung. Als Hardwareplattform dient *„Oracle SPACR (Server)“* mit Maus/Tastatur und Monitor, als Betriebssystem wird das Produkt „*Sparc Solaris 10 9/10“* verwendet. Als Laufzeitumgebung wird vom EVG *„Oracle Java“* eingesetzt und innerhalb der Laufzeitumgebung wird zusätzlich *„Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7“* verwendet. Als Aktivierungsdatenbank-Server wird *„OpenLDAP“* eingesetzt, welches zur Verschlüsselung *OpenSSL* und als interne DB die Komponenten *BerkeleyDB* verwendet. Für die Teilsysteme Zertifizierungs- und Revokationsdienst des EVG, wird die Prozessdatenbank *MySQL* verwendet.

Für die Erstellung qualifizierter elektronischer Signaturen werden ausschließlich bestätigte sichere Signaturerstellungseinheiten nach § 2 Nr. 10 SigG verwendet. FlexiTrust Version 3.6.1 Release 1111 unterstütz als SEE die *„Signaturerstellungseinheit (SEE) TCOS 3.0 Signature Card, Version 1.1"*,

Ausprägung *„Signature Card 3.0M, Version 1.0".* Für die Anwendung von Zeitstempeln durch FlexiTrust Version 3.6.1 Release 1111 (vgl. ENF*.3 in Abschn. 2.2) ist ein Zugang zu einem Zeitstempeldiensteanbieter erforderlich.

Der Betrieb des FlexiTrust Version 3.6.1 Release 1111 benötigt die Verfügbarkeit eines Kartenlesers. Die unterstürzten Kartenleser sind in Tabelle 4 aufgeführt.

Neben dem Kartenleser werden zum Betrieb des FlexiTrust Version 3.6.1 Release 1111 Bediener-Chipkarten benötigt. Für die Verschlüsselung der PIN- und Systempasswort-Shares werden *E4NetKey Karten* eingesetzt.

Für die Registrierung der Zertifikatsinhaber und der Erstellung und Verwaltung von Zertifikats-, Aktivierungs- und Sperr-Anträgen wird die Komponente FlexiTrust-RA verwendet (nicht Bestandteil der Bestätigung). Die Beantwortung von Statusanfragen, die Datenhaltung im Zertifikatsverzeichnis sowie die öffentlichen Kommunikationsanbindung sind nicht Bestandteil des EVG und, somit, nicht der Bestätigung.

Die genauen Versionen aller benötigten Komponenten sind in Tabelle 3 und Tabelle 4 aufgeführt.

3.2.2 Anforderungen an die organisatorische und administrative Einsatzumgebung

Grundsätzlich müssen Benutzer und Administratoren/Betreiber des Produkts vertrauenswürdig und qualifiziert sein und den Anweisungen der mit dem Produkt ausgelieferten Benutzerdokumentation folgen.

Insbesondere sind die folgenden Anforderungen zu beachten:

- Der Betreiber von FlexiTrust Version 3.6.1 Release 1111 muss dafür Sorge tragen, dass die Anforderungen an einen geschützten Einsatzbereich im Sinne von SigB[13] erfüllt und in einem Sicherheitskonzept entsprechend den Vorgaben von SigG/SigV dokumentiert sind, wenn der EVG in einem Zertifizierungs- oder Revokationsdienst für qualifizierte Zertifikate verwendet werden soll.

- Der Betreiber muss organisatorisch sicher stellen, dass öffentliche Schlüssel, die in qualifizierte Zertifikate aufgenommen werden sollen, im Sinne SigG/SigV geeignet sind.

- Der Betreiber von FlexiTrust Version 3.6.1 Release 1111 muss dafür Sorge tragen, dass der EVG nur von angemessen geschultem Personal benutzt wird. Die Schulung der Benutzer ist erforderlich, um eine

[13] Einheitliche Spezifizierung der Einsatzbedingung für Signaturanwendungskomponenten, Version 1.5, 11. Nov. 2011, Bundesnetzagentur (Hrsg.)

ausreichende Qualifikation für den sicheren Betrieb des EVG zu erwerben.

- Um zu gewährleisten, dass der Inhalt von qualifizierten Zertifikaten für den Benutzer hinreichend erkennbar wird, darf der Betreiber für die Darstellung am Monitor (sichere Anzeige) ausschließlich den folgenden Zeichensatz mit Serifen verwenden:
  - *Monotype Times New Roman*
  - True Type Font (TTF)
  - Zeichenkodierung: ISO 8859-1
  - Dateiname: TimesNewRoman.ttf
  - MD5 (Hashwert): 38019d8f82800beaced54dadbf8e77d8

- Um das Risiko der Preisgabe von Identifikationsdaten der verwendeten Signaturerstellungseinheiten zu reduzieren, darf auf dem Hostsystem (Server), auf dem der EVG ausgeführt wird, keinerlei installierte Debugger-Software verfügbar sein. Dies ist vom Betreiber sicherzustellen.

- Um das Risiko der Preisgabe von Identifikationsdaten der verwendeten Signaturerstellungseinheiten und anderer Geheimnisse zu reduzieren, muss das Betriebssystem, in dem der EVG ausgeführt wird, ausschließlich mit abgeschaltetem SWAP-Space konfiguriert sein. Dies ist vom Betreiber sicherzustellen.

- Um das Risiko der Preisgabe von Identifikationsdaten der verwendeten Signaturerstellungseinheiten zu reduzieren, muss das Hostsystem (Server) nach einem Ausfall/Absturz des EVG neu gestartet werden. Dies ist vom Betreiber sicherzustellen.

- Der Betreiber muss den EVG in exakter Übereinstimmung mit den Administrations- und Benutzerhandbüchern sowie mit dieser Bestätigung bertreiben.

3.2.3 Nutzung und Abgrenzung des Produkts

- Der FlexiTrust Version 3.6.1 Release 1111 bietet eine Import-Schnittstelle für Anträge (Dateisystem), eine Schnittstelle zum Triggern von Antragsimporten und ein zum Triggern von Statusaktualisierungen, je eine Schnittstelle zur Aktivierungsdatenbank und Prozessdatenbank. Desweiteren gibt es Schnittstellen zur Systemzeit des Betriebssystems, zum Dateisystem, zu Kartenleser, zur SEE und zu Monitor/Tastatur.

  Import-Schnittstelle für Anträge (Dateisystem)

  > Über diese Schnittstelle können Zertifikate, Aktivierungen und Sperrungen von Zertifikaten beantragt werden

  Schnittstelle zum Triggern von Antragsimporten

Schnittstelle, über welche die vorgelagerte RA-Komponente den EVG über das Vorhandensein neuer, zu importierender Anträge benachrichtigen kann. Die Schnittstelle unterstützt die Umsetzung der gesetzliche Unverzüglichkeitsanforderung. Sie setzt keine Sicherheitsanforderungen um.

Schnittstelle zur Aktivierungsdatenbank

Die Schnittstelle dient dazu produzierte Zertifikaten sowie Sperrinformationen zu exportieren, damit externe Anwendungen Statusauskünfte zu Zertifikaten erzeugen und Zertifikate abrufbar halten können. Der EVG benutzt diese Schnittstelle, um die IT-Umgebung über bevorstehende Exports und abgeschlossene Exports zu informieren. Dem EVG wird über diese Schnittstelle die Bereitschaft der Aktivierungsdatenbank zum Empfang von Zertifikaten und Sperrinformationen signalisiert.

Schnittstelle zum Triggern von Statusaktualisierungen

Diese Schnittstelle wird zum Benachrichtigen von externe Anwendungen, die Statusauskünfte ausliefern, bezüglich Änderungen von Statusinformationen zu benachrichtigen (“Triggern”). Technisch wird dazu eine Statusantwort zu einem Zertifikat von einem OCSP-Responder abgerufen. Die Schnittstelle kann zur Umsetzung der gesetzlichen Unverzüglichkeitsanforderung verwendet werden. Sie setzt keine Sicherheitsanforderungen um.

Schnittstelle zur Prozessdatenbank

Die Schnittstelle zur Prozessdatenbank wird von dem EVG verwendet um die Produkte und zugehörige Protokollinformationen während der Verarbeitung zwischenzuspeichern. Die Schnittstelle des EVG zur Prozessdatenbank setzt keinerlei Sicherheitsanforderungen.

Schnittstelle zu Monitor/Tastatur bzw. Maus

Über diese Schnittstelle können Signaturkarten als Schnittstelle zur SEE eingebunden werden. Diese Schnittstelle ist optional, da der EVG auch automatisch erkennen kann, wenn neue SEE angebunden werden. Diese werden dann aktiviert, wenn die entsprechenden Bedienerkarten zur Verfügung stehen (Hotplug). In diesem Anwendungsfall setzt die Schnittstelle keine Sicherheitsfunktionalität um. Über diese Schnittstelle werden außerdem die SIGNED DATA der Zertifikate vor dem Signaturvorgang angezeigt und die Absicht eine Signatur über die angezeigte SIGNED DATA zu erstellen bestätigt. In diesem Anwendungsfall setzt die Schnittstelle einen sicheren Pfad zum Benutzer um.

Schnittstelle zu Kartenleser

Über die Schnittstelle zum Kartenleser werden die Bedienerkarten an den FlexiTrust Version 3.6.1 Release 1111 angebunden.

Schnittstelle Systemzeit des Betriebssystems

Über diese Schnittstelle wird die Systemzeit des IT-Systems ausgelesen. Es muss durch die Umgebung sichergestellt sein, dass die Systemzeit der gültigen gesetzlichen Zeit entspricht. Diese Zeitangabe wird für die Erzeugung von Zertifikaten und Sperrinformationen, sowie für die Erzeugung von Protokolleinträgen verwendet.

Schnittstelle zur SEE

Über diese Schnittstelle werden Produkte des EVG einer SEE zugeführt, um diese mit einer elektronischen Signatur zu versehen, sowie die signierten Produkte von der SEE empfangen.

Schnittstelle zum Dateisystem

Über die Schnittstelle zum Dateisystem werden Konfigurationsdaten geladen und Protokollausgaben geschrieben. Desweiteren dient die Schnittstelle zur Kommunikation zwischen verschiedenen Teilsystemen des EVG und zum Export von Zertifikate, um sie der Personalisierung einer SEE zuführen zu können. Dieser Funktionalität des EVG stellt keinen Teil der Sicherheitsleistung dar.

Diese Schnittstellen stellen die logische Grenze des Produktes dar.

- Die funktionale Abgrenzung ist durch die evaluierte Sicherheitsfunktionalität (vgl. Abschn. 2.2) eindeutig gegeben.
  Insbesondere die folgende Funktionalität war **außerhalb** der Betrachtung der Sicherheitsevaluierung:

  - Bestandteile außerhalb dieser Grenzen wie das Betriebssystem selbst, die Hardware, auf dem das Betriebssystem ausgeführt wird, Kartenterminals und SSEE, die mit dem Produkt kommunizieren, sowie jegliche weitere Applikationen sind **nicht** Gegenstand dieser Bestätigung.

  - Der EVG beinhaltet **keine** Registrierungs-Funktionalität. Diese Funktionalität wird durch die vorgelagerte Komponente FlexiTrust-RA geleistet.

  - Der EVG beinhaltet **keine** Funktionalität zur Erstellung von Zeitstempeln.

- Die Beantwortung von Statusanfragen, die Datenhaltung im Zertifikatsverzeichnis sowie die öffentlichen Kommunikationsanbindung sind **nicht** Bestandteil des EVG.

- Die vorliegende Bestätigung bezieht sich **ausschließlich auf qualifizierte** elektronische Signaturen. Alle anderen Arten elektronischer Signaturen inkl. fortgeschrittener sind **nicht** Gegenstand dieser Bestätigung.

3.3 Algorithmen und zugehörige Parameter im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2

Die folgenden Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 werden vom Produkt FlexiTrust Version 3.6.1 Release 1111 für die Berechnung von Hashwerten bereitgestellt:

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[14]	Gültigkeit gem. aktuellen Festlegungen[14]
SHA-224	n.a.	n.a.	geeignet	bis Ende 2015
SHA-256	n.a.	n.a.	geeignet	bis Ende 2019
SHA-384	n.a.	n.a.	geeignet	bis Ende 2019
SHA-512	n.a.	n.a.	geeignet	bis Ende 2019

Alle Algorithmen der SHA-Familie werden nur im Modus „full-length message digest“ verwendet.

3.4 Prüfstufe und Mindeststärke der Sicherheitsfunktionen

Der EVG „FlexiTrust Version 3.6.1 Release 1111“ wurde nach der Prüfstufe EAL3 (augmentiert um ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, AVA_VAN.5) der Common Criteria v. 3.1 rev. 4 mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV erfolgreich evaluiert.

Die eingesetzten Sicherheitsfunktionen[15] erreichen die Stärke "hoch".

[14] vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 20.Februar 2013, veröffentlicht am 27.03.2013 im Bundesanzeiger.

[15] In Common Criteria 3.1: Teil der Schwachstellenbewertung (AVA_VAN); in Common Criteria 2.3: Strength of Functions (AVA_SOF)

3.5 Gültigkeit der Bestätigung

Die Gültigkeitsdauer der vorliegenden Bestätigung insgesamt ist auf das nächstliegende Gültigkeitsdatum beschränkt, das sich aus der Gültigkeit der Produktbestätigung und der maximalen Dauer eines bestätigungskonformen Betriebs des Produkts ergibt. So ist **die Gültigkeit dieser Bestätigung zeitlich beschränkt, und zwar bis 31.12.2014**. Für weitere Einzelheiten s. Abschn. 3.5.1 und 3.5.2 weiter unten.

Die Gültigkeit der Bestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

3.5.1 Gültigkeit der Produktbestätigung

Diese Produktbestätigung ist u.a. auf Grundlage

(i) der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung (s. Abschn. 0) und

(ii) der Angaben der aktuell gültigen „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 20.Februar 2013, veröffentlicht am 27.03.2013 im Bundesanzeiger“

zustande gekommen, woraus sich die Bestimmung ihrer Gültigkeit ergibt.

In Bezug auf die Gültigkeitsdauer der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung – unter Berücksichtigung der bei der Implementierung des EVG verwendeten Technologie und der beabsichtigten Einsatzumgebung (Software, die im geschützten Einsatzbereich ausgeführt wird) – agiert die Bestätigungsstelle auf der **Annahme**, dass diese Ergebnisse **7 Jahre** ab dem Zeitpunkt des Evaluierungsabschlusses (20.12.2013) gültig bleiben.

In Bezug auf Verwendung der Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 ergibt sich ihre Gültigkeitsdauer aus dem Abschnitt 3.3, wobei stets zu berücksichtigen ist, ob ein Algorithmus im Betrieb tatsächlich verwendet wird, und wenn Ja, für welche Dienste/Funktionen er verwendet wird.

Die Gültigkeitsdauer der vorliegenden Produktbestätigung ist dann auf das nächstliegende Gültigkeitsdatum beschränkt. So ist die Gültigkeit dieser Produktbestätigung zeitlich beschränkt, und zwar bis 31.12.2019.

Die Gültigkeit der Produktbestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

3.5.2 Maximale Dauer eines bestätigungskonformen Betriebs des bestätigten Produkts

Ein bestätigungskonformer Betrieb des EVG ist an Erfüllung aller Bedingungen aus Abschn. 3.2 „Einsatzbedingungen“ gebunden. Da der Betrieb des EVG die Verfügbarkeit mindestens einer SSEE benötigt (vgl. Abschn. 3.2.1), ist ihr bestätigungskonformer Betrieb an die Gültigkeit der Produktbestätigungen (bzw. Herstellererklärungen, solange SigG-konform) der eingesetzten SSEEs gebunden.

Daraus ergibt sich die maximal mögliche Dauer **eines bestätigungskonformen Betriebs** des EVG, und zwar wie folgt:

a) Das Gültigkeitsdatum der Bestätigungen der in Abschn. 3.2.1 aufgelisteten SSEEs ist 31.12.2014 (TUVIT.93146.TE.12.2006).

Die **maximal** mögliche **Dauer eines bestätigungskonformen Betriebs des EVG** ist auf das nächstliegende Gültigkeitsdatum beschränkt, nämlich auf 31.12.2014.

Die maximal mögliche Dauer eines bestätigungskonformen Betriebs des EVG kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

Ende der Bestätigung.

Bestätigung
T-Systems.02245.TE.12.2013

Hrsg.: T-Systems GEI GmbH
Adresse: Vorgebirgsstr. 49, 53119 Bonn
Telefon: +49-(0)228-9841-0
Fax: +49-(0)228-9841-6000
Web: www.t-systems.de/ict-security
www.t-systems-zert.com