Sicherheitsbestätigung

T-Systems.02247.TE.12.2013

FlexiTrust-OCSP 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.02247.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-OCSP 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.02247.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.02247.TE.12.2013 besteht aus 22 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

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

1.2 Auslieferung

Die Auslieferung des Produktes FlexiTrust-OCSP 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 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-OCSP Version 3.6.1 Release 1111	Binärpakete des Systems OCSP	Siehe Tabelle 2	-
	Binärpakete Kartentreiber PKCS#11	Siehe Tabelle 2	-
	Vorkonfiguration und Konfigurationsskripte (werden im Rahmen der Initialisierung/Installation angepasst)	-	-
	Benutzerhandbuch	1.6	22.10.2013
	Administrationshandbuch	2.5	22.10.2013
	Auslieferungs-, Installations-, Generierungs- und Anlaufprozeduren	3.6	08.07.2013

Tabelle 1: Lieferumfang FlexiTrust-OCSP 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 OCSP und der Binärpakete des Kartentreiber PKCS# mit den in den Lieferdokumenten aufgeführten Hashwerten (siehe Tabelle 2).

Dateiname	Version	Hashwert (MD5)
auth.jar	1.1	11d00d2cd074efa2d24d32de6d982321
cardman.jar	1.1	5d254d1597e12e37949bfaac92af37ef
fs_codec.jar	1.1	0894a267481bec89cfb596059edd994b
fs_util.jar	1.1.2.1	c5eb0f2e147dfbbe7f513cdddee87f6e
ka_init.jar	1.1.2.1	ffb80ed9523731676f04158785c66593
ldapclient.jar	1.1	409467612c60e95b55a8869f3ebd3ced
leanca.jar	1.1.2.1	a8cc0f3b073c3dc9516d9548f0bc86ae
libpkcs11bna.so	1.1.2.1	743e23daaf4aa19bdfaae4543bfe0f74
libnativepkcs11.so	1.1	799979d3541a4ca42a7302768179d205
ocsp-responder.ear	1.1.2.3	a82ed1d0ab6ddbdeb2f033dc96010b43
p11.jar	1.1	db7a9a0fe8fd5a54a9dccef979f26f72
pass_sharing.jar	1.1	6331154a8b2b63a87e983dae2b452b99
pin_sharing.jar	1.1	f97aa671c2f31ab2b24720aeffdc0732

Dateiname	Version	Hashwert (MD5)
secret_sharing.jar	1.1	d30375029ecc6739e7c9e63f4c9764ed

Tabelle 2: Binärpakete des Systems OCSP und des Kartentreibers PKCS#11

Weitere Softwarepakete, die für den Betrieb des EVGs erforderlich bzw. vom Hersteller für die Interaktion mit dem EVG vorgesehen sind, gehören optional zum Lieferumfang (Binärpakete andere Kartentreiber und OpenLDAP). Sie sind nicht Teil des EVGs. 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 FlexiTrust-OCSP Version 3.6.1 Release 1111 ist teils eine technische Komponente für Zertifizierungsdienste und 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 […]

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-OCSP Version 3.6.1 Release 1111 stellt Funktionen für den Betrieb eines **Auskunfts- und Verzeichnisdienstes** zur Verfügung, der qualifizierte Zertifikate nachprüfbar bzw. abrufbar hält. Der EVG realisiert dazu das Online Certificate Status Protocol (OCSP).

Zertifikate werden jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar gehalten. Für qualifizierte Zertifikate liefert die technische Komponente qualifiziert signierte Auskünfte ob ein angefragtes Zertifikat zum angegebenen Zeitpunkt existiert hat und ob es gesperrt ist (Statusauskunft). Unter dem „angegebenen Zeitpunkt“ ist dabei das in der Statusauskunft angegebene Erstellungsdatum der als Informationsgrundlage dienenden Sperrliste zu verstehen. Für nicht qualifizierte Zertifikate[3] liefert die technische Komponente nicht qualifiziert signierte Auskünfte zum Status.

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

Der FlexiTrust-OCSP Version 3.6.1 Release 1111 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.

[3] Diese Bestätigung bezieht sich ausschließlich auf qualifizierte Zertifikate

FlexiTrust-OCSP Version 3.6.1 Release 1111 ist mandantenfähig. Das bedeutet, dass der EVG ohne Replikation parallel Statusauskünfte für mehrere Trustcenter ausliefern kann. Der EVG ist insbesondere in der Lage, Statusauskünfte sowohl für qualifizierte als auch nicht qualifizierte Trustcenter parallel auszuliefern. Dabei kann ein Mandant entweder für den qualifizierten oder für den nicht qualifizierten Betrieb konfiguriert werden. 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 3.6.1 Release 1111 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. Technische Komponente für Zertifizierungsdienste:
   Diese Komponente hält im Sinne von §2 SigG Nr. 12 b) qualifizierte Zertifikate öffentlich nachprüfbar und ggf. abrufbar[4]. Sie beantwortet Statusanfragen mit entsprechenden Statusauskünften.

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[5], Kap. 6.1 bis 6.4 erläutert.

Protokollierung AUDIT

AUDIT.1: Alle Komponenten des EVGs initiieren die Protokollierung unmittelbar nach dem Start. Der Betrieb der Software mit ausgeschalteter Log-Funktion ist nicht möglich.

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

[5] Security Target: „Sicherheitsvorgaben für FlexiTrust-OCSP Version 3.6.1 Release 1111“, Version 3.32, 18.12.2013

AUDIT.2: Die Identifikation des Bedieners wird protokolliert. Sowohl erfolgreiche als auch erfolglose Versuche zur Identifikation werden protokolliert.

AUDIT.3: Für jedes Ereignis werden folgende Daten protokolliert: Uhrzeit und Datum des Auftretens, Art, Verursacher, Schweregrad und Erfolg oder Misserfolg der betroffenen Funktion.

AUDIT.4: Die Ereignisse gemäß der Tabelle 6.3 im ST werden protokolliert.

Identifikation IA

IA.1: Vor der Zuweisung der Rolle UNTERZEICHNER wird geprüft, ob unter Verwendung der in der IT-Umgebung gespeicherten PIN-Shares und den zwei Bedienerkarten die PIN (IDENTIFICATION DATA) der Signaturkarte entschlüsselt werden kann. Dabei wird eine Identifizierung der Benutzer gegenüber ihren Bedienerkarten durchgeführt (PIN).

Den Benutzern werden im Vier-Augen-Prinzip die Rolle UNTERZEICHNER und entsprechend der Mandantenzuordnung der SEE das Attribut SEEMANDANT zugeordnet. Nur solche Benutzer können die Rolle UNTERZEICHNER annehmen.

IA.2: Nicht identifizierte Benutzer können mit dem System keine Interaktionen durchführen, für die eine Identifikation notwendig ist.

IA.3: Wird über die OCSP-Anfrage-Schnittstelle eine Statusauskunft (SIGNED DATA des Typs STA) oder ein Zertifikat (SIGNED DATA des Typs ZERT) angefragt, so geschieht dies ohne die Identifizierung eines Benutzers.

Durchsetzung der Sicherheitsfunktionen ENF

ENF.1: Die Aktivierung einer SEE erfolgt mittels ihrer PIN (IDENTIFICATION DATA). Diese ist mit dem Verfahren nach Shamir in Shares aufgeteilt. Jedes Share ist mit dem Schlüssel genau einer Bedienerkarte verschlüsselt und als verschlüsselt im System abgelegt (CONFIGURATION DATA).

Der nach der Aktivierung der SEE an die SEE gebundene funktionale Teil des OCSP Responder agiert im Auftrag des Benutzers in der Rolle UNTERZEICHNER. Entsprechend wird das Attribut SEEMANDANT an dieses Subjekt gebunden.

Zur Berechnung der PIN einer SEE müssen wenigstens zwei zuvor entschlüsselte Shares kombiniert werden. Die PIN wird nur im Speicher entschlüsselt und

zusammengesetzt. Dies geschieht entsprechend dem Secret-Sharing-Verfahren nach Adi Shamir[6][7].

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 wieder aus dem Speicher gelöscht.

Das nach der Aktivierung an die SEE gebundene Subjekt OCSP-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 OCSP-SIGN gespeichert. Die Rolle UNTERZEICHNER wird für einen Benutzer dadurch eingeschränkt, dass nur für bestimmte (an einen Mandanten gebundene) 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: Zertifikate und Sperrlisten (SIGNED DATA des Typs ZERT und SPL) werden aus der Aktivierungsdatenbank zusammen mit dem Sicherheitsattribut ZIELMANDANT importiert und dienen als Grundlage für die Berechnung von Statusauskünften.

In der Aktivierungsdatenbank existiert bezüglich der SIGNED DATA Typen ZERT und SPL für jeden möglichen Mandanten (Attribut ZIELMANDANT) ein Bereich der logisch von den Bereichen aller anderen Mandanten getrennt ist. Bezüglich der Zertifikate (SIGNED DATA des Typs ZERT) ist jeder solche Bereich in zwei logisch voneinander getrennte Teilbereiche aufgeteilt: den Teilbereich “abrufbar” und den Teilbereich “nur nachprüfbar”.

Für importierte Zertifikate wird das Attribut PUBLIC importiert. Ist ein Zertifikat im Teilbereich “abrufbar” enthalten, erhält das Attribut den Wert TRUE. Ist dies nicht der Fall, erhält das Attribut den Wert FALSE.

ENF.3: Statusauskünfte (SIGNED DATA des Typs STA) werden gemäß ihrer Mandantenzuordnung (ZIELMANDANT) der entsprechenden SEE zur Erzeugung einer elektronischen Signatur zugeführt. Dies wird dadurch sichergestellt, dass das die Statusauskunft demjenigen aktiven Teil des OCSP zugeführt wird, dessen

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

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI): „Technische Richtlinie - Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, BSI TR-02102, Version 2013.02, 09. 01. 2013

Attribut SEEMANDANT denselben Wert hat wie das Attribut ZIELMANDANT der Statusauskunft.

Wurde in der Statusanfrage der Auslieferung des angefragten Zertifikats gewünscht, wird dieses ausgeliefert, wenn das Attribut PUBLIC des Zertifikats den Wert TRUE hat.

Als Erstellungszeitpunkt von Statusauskünften (SIGNED DATA des TYP STA) wird die Systemzeit eingetragen. Diese entspricht der gültigen gesetzlichen Zeit.

Nach der Erzeugung der Signatur wird die mathematische Korrektheit der Signatur geprüft. Dazu wird ein Zertifikat verwendet das für den spezifischen Verwendungszweck und den jeweiligen Mandanten (SEEMANDANT) in der CONFIGURATION DATA hinterlegt ist. Dadurch wird sichergestellt, dass die Statusauskunft mit einer elektronischen Signatur versehen ist, deren Eignung auf einem Zertifikat beruht, dass die Art und Nutzung des Signaturschlüssels auf diesen Typ der SIGNED DATA beschränkt. Darüber hinaus wird dadurch sichergestellt, dass Statusauskünfte zu qualifizierten Zertifikaten ausschließlich mit qualifizierten elektronischen Signaturen versehen werden und dass Statusauskünfte zu nicht qualifizierten Zertifikaten nicht mit qualifizierten elektronischen Signaturen versehen werden.

War die Signaturerstellung im Rahmen der Operation AUSLIEFERN VON SIGNED DATA erfolgreich, werden die signierte Statusauskunft und das darin ggf. enthaltene Zertifikat an den Benutzer exportiert. Dieser Export erfolgt ohne weitere Sicherheitsattribute.

ENF.4: Der OCSP nimmt Statusanfragen entgegen. Es wird sichergestellt, dass es sich um eine gültige Statusanfrage handelt. Es wird nur dann eine Statusauskunft (SIGNED DATA) erstellt, wenn eine gültige OCSP-Statusanfrage an den OCSPResponder erfolgt. Das Attribut TYP erhält den Wert STA.

Das Attribut ZIELMANDANT der Statusauskunft erhält zunächst den in der CONFIGURATION DATA hinterlegten Wert des Default-Mandanten.

Anhand der aus der Aktivierungsdatenbank importierten Zertifikate (SIGNED DATA des Typs ZERT) wird bestimmt, ob das angefragte Zertifikat existiert. Dabei wird zudem sichergestellt, dass die Attribute ZIELMANDANT des Zertifikats und der Statusauskunft übereinstimmen.

Der OCSP wertet Sperrinformationen (SIGNED DATA des Typs SPL) aus der Aktivierungsdatenbank aus, und bestimmt anhand dieser, ob das angefragte Zertifikat gesperrt ist. Dabei wird zudem sichergestellt, dass die Attribute ZIELMANDANT der Sperrinformation und der Statusauskunft übereinstimmen. Als Zeitpunkt, auf den sich eine Statusauskunft bezieht, wird der Zeitpunkt der

Erzeugung der Sperrinformation (SIGNED DATA des Typs SPL) eingetragen. Dieser Zeitpunkt ist in der Sperrinformation enthalten. Der Wert der Statusauskunft wird wie folgt gebildet:

1. Wenn der Aussteller nicht konfiguriert ist, bekommt die Statusauskunft den Wert UNKNOWN.

2. Wenn das Zertifikat nicht existiert, bekommt die Statusauskunft den Wert UNKNOWN.

3. Wenn das Zertifikat existiert aber nicht in der Sperrliste enthalten ist, bekommt die Statusauskunft den Wert GOOD.

4. Wenn das Zertifikat existiert und in der Sperrliste enthalten ist, bekommt die Statusauskunft den Wert REVOKED.

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

PROTECT.1: Es ist sichergestellt, dass die Kommunikation mit der Aktivierungsdatenbank über einen vertrauenswürdigen Kanal erfolgt, da der Aufbau des sicheren Kanals durch den EVG initiiert wird. Hierbei wird die Authentizität der Aktivierungsdatenbank anhand des verwendeten Kommunikationsprotokolls sichergestellt. Der Referenzwert für die Überprüfung der Authentizität wird der CONFIGURATIONDATA entnommen. Der EVG greift ausschließlich lesend auf die Aktivierungsdatenbank zu.

PROTECT.2: 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 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 des Typs STA 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 des Typs STA verletzt, indem Daten während des Transports eingefügt, manipuliert oder gelöscht werden, löst dies einen Protokollfehler aus. Ein solcher Fehler wird protokolliert und die Verarbeitung wird abgebrochen.

PROTECT.3: Den 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-256, SHA-224, 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 per Konfiguration abgeschaltet werden.

PROTECT.4: Die SIGNED DATA (Zertifikate und Sperrinformationen) werden beim Import aus der Aktivierungsdatenbank durch einen vertrauenswürdigen Kanal geschützt. Der Aufbau dieses Kanals wird vom EVG initiiert, wobei der Kanal selbst durch die Umgebung bereitgestellt wird.

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.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Produkt erfüllt die Anforderungen nach:

SigG

§ 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 PROTECT.2, PROTECT.3, PROTECT.4, ENF.1, ENF.3 und ENF.4 umgesetzt und durch IA.1 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.

§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,[…]

Diese Anforderungen sind durch die Sicherheitsfunktionen ENF.3, ENF.4, IA.1, IA.2 und IA.3 umgesetzt (s. Abschn. 2.2 weiter oben).

§17 (3), Satz 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 Anforderung ist durch die Sicherheitsfunktion PROTECT.1, PROTECT.2, PROTECT.3, PROTECT.4, ENF.1, ENF.2, ENF.3, ENF.4, IA.1, IA.2 und IA.3 umgesetzt (s. Abschn. 2.2 weiter oben).

SigV

§ 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen

§ 15 (2), Satz 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 Anforderung ist durch die Sicherheitsfunktionen PROTECT.2, PROTECT.3, PROTECT.4, ENF.1, ENF.2, ENF.3, ENF.4, IA.1, IA.2 und IA.3 umgesetzt (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 und die Auskünfte auf ihre Echtheit überprüft werden können. Die Auskünfte nach Satz 1 müssen beinhalten, ob die nachgeprüften qualifizierten Zertifikate im Verzeichnis der qualifizierten Zertifikate zum angegebenen Zeitpunkt vorhanden und ob sie nicht gesperrt waren. Nur nachprüfbar gehaltene qualifizierte Zertifikate dürfen nicht öffentlich abrufbar sein. […]

Diese Anforderung ist durch die Sicherheitsfunktionen PROTECT.1, PROTECT.2, PROTECT.3, PROTECT.4, ENF.2, ENF.3 und ENF.4 umgesetzt (s. Abschn. 2.2 weiter oben).

§ 15 (4)

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

Diese Anforderung ist durch die Sicherheitsfunktionen ENF.1, AUDIT.1, AUDIT.2, AUDIT.3 und AUDIT.4 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-OCSP Version 3.6.1 Release 1111 besteht nur aus Software, daher werden für den Betrieb folgende Komponenten benötigt die nicht Teil des EVGs 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
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 Chipkarte	E4NetKey TCOS Version 2.03	-

Tabelle 4: Technisch 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-OCSP Version 3.6.1 Release 1111 benötigt für den Betrieb eine Hardwareplattform, ein Betriebssystem und eine 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 Erstellung qualifizierter elektronischer Signaturen werden ausschließlich bestätigte sichere Signaturerstellungseinheiten nach § 2 Nr. 10 SigG. FlexiTrust-OCSP 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-OCSP Version 3.6.1 Release 1111 (vgl. ENF.3 und

ENF.4 in Abschn. 2.2) ist ein Zugang zu einem Zeitstempeldiensteanbieter erforderlich.

Der Betrieb des FlexiTrust-OCSP Version 3.6.1 Release 1111 benötigt die Verfügbarkeit eines Kartenlesers. Die unterstürzten Kartenleser sind in Tabelle 4 aufgeführt, wobei mindestens eines dieser aufgeführten Terminals für Anwendung von Zeitstempeln (vgl. ENF.3 und ENF.4 in Abschn. 2.2) einzusetzen ist.

Die Datenhaltung im Zertifikatsverzeichnis und die öffentliche 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-OCSP Version 3.6.1 Release 1111 muss dafür Sorge tragen, dass die Anforderungen an einen geschützten Einsatzbereich im Sinne von SigB[8] 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 von FlexiTrust-OCSP 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 ausreichende Qualifikation für den sicheren Betrieb des EVG zu erwerben.

- Der Startvorgang gewährleistet, dass der EVG nur einmal gestartet werden kann. Damit erfolgt die Verarbeitung exklusiv von einer einzigen Instanz des EVG. Allerdings wirkt der Mechanismus erst unmittelbar vor dem letzten Schritt des Startvorgangs und somit nach dem Start der Protokollierung und der Aktivierung der SEE. Um mögliche Konflikte beim Zugriff auf die Protokolldatei oder beim Verbindungsaufbau mit den

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

SEE auszuschließen, muss der Betreiber mit einer organisatorischen Maßnahme dafür Sorge tragen, dass der EVG nur einmal gestartet wird.

- 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-OCSP Version 3.6.1 Release 1111 bietet eine Schnittstelle zur Aktivierungsdatenbank, zur Systemzeit des Betriebssystems, zum Dateisystem, zu Kartenleser, zur SEE und zu Monitor/Tastatur.

  OCSP-Anfragen

  Ein Anfrager hat über diese Schnittstelle die Möglichkeit Statusabfragen zu Zertifikaten abzuschicken und erhält dabei vom EVG Statusauskünfte. Außerdem hat der Anfrager die Möglichkeit sich ein Zertifikat, dass sich auf die Anfrage bezieht, ausliefern zu lassen. Das Zertifikat wird jedoch nur dann ausgeliefert, wenn der Besitzer des Zertifikats der Auslieferung zuvor zugestimmt hatte. Die Abrufbarkeit eines Zertifikats wird anhand der Daten in der Aktivierungsdatenbank bestimmt.

  Schnittstelle zur Aktivierungsdatenbank

  Die Aktivierungsdatenbank wird dafür verwendet, produzierte Zertifikate und Sperrinformationen für die Statusauskünfte zu Zertifikaten abzufragen sowie abrufbare Zertifikate öffentlich verfügbar zu machen. Um eine wirksame Unterscheidung zwischen abrufbaren und nur nachprüfbaren Zertifikaten auf Basis der Informationsflusskontrolle der Aktivierungsdatenbank zu

ermöglichen, werden abrufbare Zertifikate zusätzlich zu allen (nachprüfbaren) Zertifikaten in Kopie in einem getrennten Bereich der Aktivierungsdatenbank abgelegt.

Schnittstelle zu Monitor/Tastatur

Der EVG benutzt die Schnittstelle zu Monitor und Tastatur, um Signaturkarten (Schnittstelle SEE), die während des Betriebs der Schnittstelle “Kartenleser´´ zugeführt werden, einzubinden. 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). Die Schnittstelle
setzt keine Sicherheitsfunktionen um, da die eigentliche Aktivierung der SEE (Zuführen der IDENTIFICATION DATA) nur dann erfolgt, wenn die Bediener des Systems sich gegenüber ihren Bedienerkarten identifizieren und damit die IDENTIFICATION DATA verfügbar machen. Die Schnittstelle wird außerdem dazu verwendet, um für die Bediener des Systems Benutzungshinweise auszugeben.

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 Statusauskünften verwendet.

Schnittstelle zu Kartenleser

Über diese Schnittstelle sind Bedienerkarten an den EVG angebunden. Mit den Bedienerkarten werden Passwörter für die Benutzung der Ressourcen des EVG bzw. die IDENTIFICATION DATA für die SEE freigeschaltet und dem System zur Verfügung gestellt. Dies geschieht dadurch, dass sich mindestens zwei Bediener gegenüber ihrer Bedienerkarte durch Eingabe einer PIN am Kartenleser identifizieren. Der Zugriff auf die Bedienerkarten erfolgt über entsprechende Treibersoftware. Der EVG verfügt über eine Schnittstelle zu Treibern gemäß PKCS#11 Standard.

Schnittstelle zur SEE

Über diese Schnittstelle werden zu signierende Statusauskünfte des EVG der entsprechenden SEE zugeführt, um diese mit einer elektronischen Signatur zu versehen, sowie die signierten Auskünfte von dieser zu empfangen. Des Weiteren wird der SEE über diese Schnittstelle die IDENTIFICATION DATA zugeführt, um diese zu aktivieren. Die Identifikation der jeweiligen SEE basiert auf SEE eigenen Mechanismen. Die Absicherung erfolgt durch den EVG in Zusammenarbeit mit der SEE (Secure Messaging). Der Zugriff auf

die SEE erfolgt über entsprechende Treibersoftware. Ein PKCS#11-Treiber zur Anbindung von SEE des Typs TCOS Signature Card 3.0M ist im EVG enthalten.

Schnittstelle zum Dateisystem

Die Schnittstelle zum Dateisystem wird für verschiedene Aufgaben verwendet. Erstens werden darüber Konfigurationsdaten geladen und zweitens werden darüber Protokollausgaben geschrieben.

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.

  - Die Datenhaltung im Zertifikatsverzeichnis und die öffentliche Kommunikationsanbindung sind nicht Bestandteil des EVG, und somit **nicht** Gegenstand dieser Bestätigung.

- 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-OCSP Version 3.6.1 Release 1111“ für die Berechnung von Hashwerten bereitgestellt:

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[9]	Gültigkeit gem. aktuellen Festlegungen[9]
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-OCSP 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 und 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[10] erreichen die Stärke "hoch".

[9] 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.

[10] 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. 3.4) 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 EVGs ist an Erfüllung aller Bedingungen aus Abschn. 3.2 „Einsatzbedingungen“ gebunden. Da der Betrieb des EVGs die Verfügbarkeit mindestens einer SigG-bestätigten 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 EVGs, und zwar wie folgt:

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

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

Die maximal mögliche Dauer eines bestätigungskonformen Betriebs des EVGs 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.02247.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