Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass die

Signaturanwendungskomponente
Signtrust Signaturserver, Version 4.1

der

Deutsche Post Com GmbH

den nachstehend genannten Anforderungen des Signaturgesetzes bzw. der Signaturverordnung entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93178.TU.03.2011

registriert.

Essen, 30.03.2011

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 17.07.2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch die Verordnung vom 15.11.2010 (BGBl. I S. 1542)

Die Bestätigung zur Registrierungsnummer TUVIT.93178.TU.03.2011 besteht aus 18 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang

Signaturanwendungskomponente Signtrust Signaturserver, Version 4.1[3] in den beiden Varianten

- Variante 1: Server-Plattform mit Client-API
- Variante 2: Signaturbox mit Client-API

Die Client-API stellt eine Funktionsbibliothek zur Einbindung in eine Applikation dar.

Auslieferung:

auf einer einmal beschreibbaren CD-ROM durch persönliche Übergabe des Produkts und der Dokumentation mit den in den nachfolgenden Tabellen aufgelisteten Bestandteilen

Das Produkt wird hergestellt im Auftrag der

Deutsche Post Com GmbH
Geschäftsfeld Signtrust
Tulpenfeld 9
53113 Bonn

Hersteller des Produkts ist die
secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

1.1 Variante 1: Server-Plattform mit Client-API

Der serverseitige und clientseitige Signtrust Signaturserver wird auf einer Single-Session-CD-ROM ausgeliefert. Zusammen mit der Konfigurationsliste in Papierform, welche die Bestandteile des Signtrust Signaturservers eindeutig identifiziert, wird die CD-ROM und die Betriebsdokumentation (auf Datenträger oder in Papierform) von einer vertrauenswürdigen Person der secunet Security Networks AG dem Verantwortlichen des Auftraggebers persönlich übergeben.

Auf der Auslieferungs-CD finden sich die nachfolgend aufgelisteten Dateien in eindeutigen Unterverzeichnissen:

Bezeichnung	Beschreibung	Version, Datum SHA-1 Hashwert
signaturserver	Ausführbares Programm des Signaturservers unter Linux	4.1, 14.12.2009 0acea793039975afb8e3d2ab76d2261d6ebb56a3

[3] Im Folgenden kurz mit Signaturserver bezeichnet.

Bezeichnung	Beschreibung	Version, Datum SHA-1 Hashwert
Signaturserver	Ausführbares Programm des Signaturservers unter Sun Solaris	4.1, 14.12.2009 c5ca5c7d35b7766b9a40 a42266011d43ccabd36b
CertificateDatabase.dat	Zertifikatsdatenbank des Signaturservers	Exemplarische Datei ohne definierte Version
signaturserver.conf	Konfigurationsdatei des Signaturservers	Exemplarische Datei ohne definierte Version
configmodule.ini	Konfigurationsdatei für die vom Signaturserver genutzte Funktions-bibliothek	Exemplarische Datei ohne definierte Version

Tabelle 1: ***Auslieferungsbestandteile (serverseitig) des Signaturservers in der Variante 1 (Server-Plattform)***

Bezeichnung	Beschreibung	Version, Datum SHA-1 Hashwert
libSignServer ClientApi.a	Statische Client-API-Bibliothek für Linux, 32-Bit-Variante	4.1, 14.12.2009 09a89b8c4ff3281b4561 817fcc17520a697bdde6
libSignServer ClientApi.so	Dynamische Client-API-Bibliothek für Linux, 32-Bit-Variante	4.1, 14.12.2009 426797e1cd4a34a2b360 108abb8252e0adb18cf7
libSignServer ClientApi.a	Statische Client-API-Bibliothek für Solaris, 32-Bit-Variante	4.1, 14.12.2009 3ecdbae1e562da34b69a a94256901942c018273c
libSignServer ClientApi.so	Dynamische Client-API-Bibliothek für Solaris, 32-Bit-Variante	4.1, 14.12.2009 a469f49e2e16dbbd1c05 1d5bc14312387c7e1df6
libSignServer ClientApi.a	Statische Client-API-Bibliothek für Linux, 64-Bit-Variante	4.1, 14.12.2009 c8733e3daec58c162314 1e102f0bd3ea580c6673
libSignServer ClientApi.so	Dynamische Client-API-Bibliothek für Linux, 64-Bit-Variante	4.1, 14.12.2009 be86402666a456f63ce2 176111c6a6445df44733
ClientApi.dll	Client-API-Bibliothek für Windows, 32-Bit-Variante	4.1, 14.12.2009 af96edeb2c273b4d8fcd 6cb935e9508d7b78dbc5
ClientApi.lib	Exportdefinition des Interfaces der ClientApi.dll für Windows	4.1, 14.12.2009 b3277777e3e2bf985df2 50298e1517aa66d6d891

Bezeichnung	Beschreibung	Version, Datum SHA-1 Hashwert
ClientCAPI.h	Headerdatei zu den Client-API-Funktionsbibliotheken	4.1, 14.12.2009 90ea8c87be4b4e90732d d879a627cf013a69a63b
ClientAPITypes.h	Headerdatei zu den Client-API-Funktionsbibliotheken	4.1, 14.12.2009 a7201edefd7ce7e2d2b6 e58c0b832dd53f0a76f9
SharedClientApiTypes.h	Headerdatei zu den Client-API-Funktionsbibliotheken	4.1, 14.12.2009 3e6cac69edd8df54649f e1e8990edc16492de2fe

Tabelle 2: ***Auslieferungsbestandteile (clientseitig) des Signaturservers***

Der Client-Anteil des Signtrust Signaturservers ist für beide Varianten, Variante 1 und Variante 2, identisch.

1.2 Variante 2: Signaturbox mit Client-API

Der serverseitige Signtrust Signaturserver wird vorinstalliert auf einer CompactFlash-Karte, die fest innerhalb der Signaturbox eingebaut ist, ausgeliefert. Das Gehäuse der Signaturbox ist vom Hersteller versiegelt. Der clientseitige Signtrust Signaturserver wird auf einer Single-Session CD-ROM ausgeliefert.

Zusammen mit der Konfigurationsliste des Signtrust Signaturservers in Papierform, die dessen Bestandteile eindeutig identifiziert, wird die Signaturbox, die CD-ROM und die Betriebsdokumentation (auf Datenträger oder in Papierform) von einer vertrauenswürdigen Person der secunet Security Networks AG dem Verantwortlichen der Deutsche Post Com GmbH persönlich übergeben.

Bezeichnung	Beschreibung	Version, Datum SHA-1 Hashwert
signaturserver	Ausführbares Programm des Signaturservers unter Linux	4.1, 14.12.2009 0acea793039975afb8e3 d2ab76d2261d6ebb56a3
CertificateDatabase.dat	Zertifikatsdatenbank des Signaturservers	Exemplarische Datei ohne definierte Version
signaturserver.conf	Konfigurationsdatei des Signaturservers	Exemplarische Datei ohne definierte Version
Configmodule.ini	Konfigurationsdatei für die vom Signaturserver genutzte Funktionsbibliothek LibSigG	Exemplarische Datei ohne definierte Version

Bezeichnung	Beschreibung	Version, Datum SHA-1 Hashwert
signaturserver.sh	Skript, das zum Starten des Signaturservers im Rahmen von Variante 2 (Signaturbox) benötigt wird	Wird nicht einzeln sondern als Teil des Box-Images ausgeliefert

Tabelle 3: ***Auslieferungsbestandteile (serverseitig) des Signaturservers in der Variante 2 (Signaturbox)***

Der Client-Anteil des Signtrust Signaturservers ist für beide Varianten, Variante 1 und Variante 2, identisch und in Tabelle 2: *Auslieferungsbestandteile (clientseitig) des Signaturservers* aufgelistet.

Zusätzlich werden folgende Tools (nicht Signaturserver-Bestandteil) im Rahmen von Variante 2 (Signaturbox) ausgeliefert:

- Tool `boxconfigurator` zur Konfiguration der Signaturbox (Auslieferung auf einer separaten CD-ROM),
- Tool `signaturecheck` (Signaturprüfung) zur Absicherung der externen USB-Schnittstelle (vor der Auslieferung vom Hersteller auf der CompactFlash-Karte installiert).

1.3 Weitere Auslieferungsbestandteile

Darüber hinaus wird folgende Dokumentation ebenso persönlich übergeben:

- Benutzerdokumentation – Signtrust Signaturserver, Version 4.1, Version 2.4 vom 26.11.2010 (elektronisch oder in Papierform ausgeliefert)
- Systemverwalterdokumentation – Signtrust Signaturserver, Version 4.1, Version 2.8 vom 26.11.2010 (elektronisch oder in Papierform ausgeliefert)
- Konfigurationsliste – Signtrust Signaturserver, Version 4.1, Version 1.4 vom 26.11.2010 ausgeliefert in Papierform

2 Funktionsbeschreibung

Das Produkt „Signtrust Signaturserver“ in der Version 4.1, stellt eine Lösung im Bereich der qualifizierten elektronischen Signatur (insbesondere im Szenario Batchsignaturen) zur Verfügung.

Der „Signtrust Signaturserver“ liegt in zwei möglichen Varianten vor, die sich in der Einsatzumgebung unterscheiden (unterschiedliche Hardware-Plattformen).

- Variante 1: Server-Plattform

  Der serverseitige Signtrust Signaturserver wird auf x86 kompatibler Hardware unter Linux (Kernel 2.6) oder Sun Solaris (Version 9) betrieben.

- Variante 2: Signaturbox

  Der serverseitige Signtrust Signaturserver wird auf einer speziellen Plattform, der Signaturbox, betrieben. Darin befindet sich die Software vorinstalliert auf einer fest eingebauten CompactFlash-Karte.

Beiden Varianten liegt derselbe Signtrust Signaturserver zugrunde.

Die folgenden Funktionen werden durch den Signtrust Signaturserver grundsätzlich bereitgestellt:

- Anstoßen einer qualifizierten Signaturerzeugung
- Signaturprüfung
- Zertifikatsprüfung
- Mandantenfähigkeit[4], d. h. es können für unterschiedliche Mandanten verschiedene Szenarien zur Signaturerstellung und unterschiedliche Schnittstellen konfiguriert werden.

Der Signtrust Signaturserver besteht aus einer serverseitigen und einer clientseitigen Komponente. Die clientseitige Komponente ist als Funktionsbibliothek realisiert und repräsentiert die clientseitige Netzwerk-Schnittstelle zur Nutzung der vom Server bereitgestellten Sicherheitsfunktionalität. Des Weiteren wird von der clientseitigen Komponente die Initialisierung eines sicheren Kanals zur serverseitigen Komponente zur Verfügung gestellt.

Die Funktionen des Signtrust Signaturservers können über verschiedene Schnittstellen angesprochen werden: Bei Nutzung der Dateischnittstelle muss dem Anwender Zugriff auf definierte Verzeichnisse auf dem Signaturen-Server-Rechner (Variante 1) bzw. auf definierte, gemountete Verzeichnisse auf einem dedizierten Rechner (Variante 2) eingerichtet werden. Wird die Netzwerk-Schnittstelle verwendet, so muss auf Seite des Clients die zum Signtrust Signaturserver gehörende Client-API verwendet werden. Der Signtrust Signaturserver nutzt die Sicherheitsfunktionen der eingebetteten Komponente K1–LibSigG (Bestätigung: TUVIT.93177.TU.01.2011 vom 20.01.2011) in vorgeschriebener Art und Weise. Jegliche Kommunikation mit der sicheren Signaturerstellungseinheit wird durch die LibSigG realisiert.

Die unterstützten Signaturformate sind von der verwendeten Schnittstelle abhängig:

	Signaturerzeugung	***Signatur- und Zertifikats-prüfung***
Datei-schnitt-stelle	PKCS#7 (detached, embedded) XML-DSig PDF (integrierte Signatur)	PKCS#7 (detached, embedded) XML-DSig PDF (integrierte Signatur)

[4] In der Signaturbox (Variante 2) ist die Anzahl der Mandanten auf eins beschränkt.

	Signaturerzeugung	***Signatur- und Zertifikats-prüfung***
Netzwerk-schnitt-stelle	PKCS#1 PKCS#7 (detached, embedded) XML-DSig PDF (integrierte Signatur)	PKCS#1 PKCS#7 (detached, embedded) XML-DSig PDF (integrierte Signatur)

Tabelle 4: ***Vom Signtrust Signaturserver unterstützte Signaturformate***

Das Softwareprodukt Signtrust Signaturserver, Version 4.1 ist eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, für die automatisierte Erzeugung von qualifizierten elektronischen Signaturen für einen bestimmten Zweck, wie z. B. die Signatur von elektronischen Rechnungen gemäß § 14 Abs. 3 Nr. 1 UStG. Dazu muss das verwendete qualifizierte Zertifikat eine entsprechende Beschränkung gemäß § 7 Nr. 7 SigG für diesen Anwendungszweck aufweisen, sowie die zugehörige Anwendung (nicht Gegenstand der Bestätigung) hinreichend geprüft und abgenommen sein. Bei der automatisierten Signaturerzeugung durch Multisignatur-SSEE wird mittels eines Zeitfensters die Dauer der SSEE Freischaltung nach PIN-Eingabe begrenzt. Ferner können mit dem Signtrust Signaturserver automatisiert qualifizierte elektronische Signaturen geprüft sowie zugehörige qualifizierte Zertifikate online bei einem OCSP-Verzeichnisdienst nachgeprüft werden.

Der Signtrust Signaturserver bietet hierzu zwei Schnittstellen an:

1. Dateischnittstelle

   Bei der Dateischnittstelle muss die zu signierende Datei bzw. die zu überprüfende signierte Datei in ein Eingangsverzeichnis abgelegt werden. Nach Erzeugung bzw. Prüfung der qualifizierten elektronischen Signatur durch den Signtrust Signaturserver werden die signierte Datei bzw. das Prüfergebnis als Datei in einem Ausgangsverzeichnis abgelegt. Es werden die Signaturformate PKCS#7, XML-DSig und PDF (integrierte Signatur) unterstützt. Es wird jeweils die aktuelle Systemzeit als Signaturerstellungszeitpunkt in die Signatur mit eingebunden.

2. Netzwerkschnittstelle

   Die Netzwerkschnittstelle wird über eine zusätzliche Funktionsbibliothek (Client-API – siehe Kapitel 1) zur Verfügung gestellt, welche eine abgesicherte Verbindung zur zentralen Komponente des Signtrust Signaturservers aufbaut. Die Funktionsbibliothek ist alleine nicht lauffähig und muss vertrauenswürdig in eine Anwendung (nicht Gegenstand der Bestätigung) eingebunden werden. Sie stellt der Anwendung, nach erfolgreicher Authentifizierung an der zentralen Serverkomponente, die notwendigen Server-Funktionen zur Erzeugung bzw. Prüfung von qualifizierten elektronischen Signaturen und Zertifikaten zur Verfügung, indem sie die Daten an den Signtrust Signaturserver gesichert übermittelt und die Antworten gesichert entgegennimmt. Es werden die Signaturformate PKCS#1, PKCS#7 (*detached* oder *embedded signature*), XML-DSig und PDF (integrierte Signatur) unterstützt. Bis auf das

Signaturformat PKCS#1, wird jeweils die aktuelle Systemzeit des Servers als Signaturerstellungszeitpunkt in die Signatur mit eingebunden.

Neben der Unterstützung beider Schnittstellen, ist der Signtrust Signaturserver mandantenfähig. Jedem Mandanten werden logisch eine Schnittstelle und ein Pool aus einer oder mehreren sicheren Signaturerstellungseinheiten (SSEE) zugeordnet. Dabei ist gewährleistet, dass jeder Mandant nur auf dem ihm zugeordneten Pool zugreifen kann.

Die vom Signtrust Signaturserver zur Verfügung gestellten Algorithmen sind in Abschnitt 3.3 aufgelistet. Der Systemverwalter muss sich über die Eignung und Gültigkeit der verwendeten Algorithmen auf der Web-Seite der Bundesnetzagentur informieren und den Zeitpunkt, bis zu dem die Verwendung des jeweiligen Algorithmus erlaubt ist, in der Konfiguration des Signtrust Signaturserver eintragen. Falls ein Hashalgorithmus ungültig ist oder nicht unterstützt wird, erfolgt eine Fehlermeldung.

Die unterstützten SSEE (siehe Abschnitt 3.2.4) verwenden bei der Signaturerzeugung den Algorithmus RSA mit 2048 Bit. Nach erfolgreicher PIN-Authentifizierung können die SSEE grundsätzlich eine unbegrenzte Anzahl von Signaturen erzeugen (Multisignatur-SSEE). Der Signtrust Signaturserver begrenzt mittels eines Zeitfensters die Dauer der Freischaltung der SSEE nach PIN-Authentifizierung. Das Zeitfenster muss durch den Signaturschlüssel-Inhaber vor der PIN-Eingabe definiert werden. Vor Freischaltung der SSEE mittels PIN-Authentifizierung wird vom Signtrust Signaturserver geprüft, dass das zur SSEE gehörige qualifizierte Zertifikat im gewählten Zeitfenster gültig ist. Wenn nicht, wird die SSEE nicht zur Signaturerzeugung freigeschaltet. Nach Ablauf des Zeitfensters einer freigeschaltenen SSEE wird der Authentifizierungsstatus der SSEE zurückgesetzt und es können ohne erneute PIN-Eingabe keine Signaturen mehr erzeugt werden.

Der Signtrust Signaturserver ist somit geeignet als Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, Daten dem Prozess der Erzeugung oder Prüfung elektronischer Signaturen zuzuführen sowie qualifizierte elektronische Signaturen zu prüfen und qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

Die vom Signtrust Signaturserver je nach Einsatzzweck clientseitig benötigte Anwendung basierend auf der Client-API ist nicht Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturanwendungskomponente Signtrust Signaturserver erfüllt in ihrer Ausprägung als Signaturanwendungskomponente die Anforderungen nach § 17 Abs. 2 Satz 1 (eindeutige Anzeige und Feststellbarkeit der Daten bei Signaturerzeugung) und nach Satz 2 (Feststellbarkeit der signierten Daten, des

Unverändertseins der Daten, der Zuordnung zum Signaturschlüssel-Inhaber, des Inhalts des qualifizierten Zertifikats und des Ergebnisses der Nachprüfung von Zertifikaten) SigG sowie § 15 Abs. 2 Nr. 1a (keine Preisgabe oder Speicherung der Identifikationsdaten), Nr. 1b (Signatur nur durch berechtigt signierende Person) und Nr. 2 (korrekte Prüfung der Signatur und Anzeige, eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Grundlage dieser Bestätigung ist der Einsatz des Signtrust Signaturservers in einem *geschützten Einsatzbereich*. Für den sicheren Einsatz des Signtrust Signaturservers und zur Verhinderung von erfolgreichen Angriffen mit den Zielen, dass:

- Daten signiert werden, die nicht signiert werden sollen,
- das Prüfergebnis der Signatur- bzw. Zertifikatprüfung falsch angezeigt wird,
- die Geheimhaltung des Identifikationsmerkmals (PIN) nicht gewährleistet ist,

sind die folgenden Auflagen zu beachten:

3.2.1 Auflagen zur Anbindung an das Internet

Eine Netzverbindung der zentralen Serverkomponente (z. B. mittels Modem, ISDN oder LAN-Anschluss) zum Verzeichnisdienst des Zertifizierungsdiensteanbieters ist für die Prüfung der Gültigkeit von Zertifikaten notwendig. Ferner wird auch zwischen der zentralen Serverkomponente und der Applikation mit der Client-API eine Netzwerkverbindung benötigt. Falls die Signaturbox mit Dateischnittstelle eingesetzt wird, ist auch eine dedizierte Netzwerkverbindung zwischen der Signaturbox und dem dediziertem Rechner erforderlich.

Die Netzverbindungen müssen so abgesichert sein, z. B. durch geeignet konfigurierte Firewalls, dass online Angriffe aus dem Internet sowohl auf die Server-Plattform (Variante 1) bzw. die Signaturbox (Variante 2) und ggf. dediziertem Rechner (Dateischnittstelle) als auch auf die Applikation erkannt bzw. unterbunden werden.

3.2.2 Auflagen zur Anbindung an ein Intranet

Wenn die zentrale Serverkomponente oder die Applikation mit der Client-API in einem Intranet betrieben wird, so muss die jeweilige Netzverbindung geeignet abgesichert sein, so dass online Angriffe aus dem Intranet auf die jeweilige Rechner-Plattform erkannt bzw. unterbunden werden.

3.2.3 Auflagen zur Sicherheit der IT-Plattform und Applikationen

Der Nutzer des Signtrust Signaturservers muss sich davon überzeugen, dass keine Angriffe von der Rechner-Plattform und den dort vorhandenen Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf der Rechner-Plattform installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,

2. auf der Rechner-Plattform keine Viren oder Trojanischen Pferde eingespielt werden können,

3. die Rechner-Plattform nicht unzulässig verändert werden kann und

4. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. Dieses kann die in Abschnitt 3.2 angegeben Folgen haben.

Die Integrität der zentralen Serverkomponente und der Applikation mit der Client-API ist regelmäßig zu überprüfen. Bei Variante 1 (Server-Plattform) kann der Systemverwalter die Integrität des serverseitigen Signtrust Signaturservers im Betrieb durch Vergleich mit den Original-Dateien auf der Auslieferungs-CD vergleichen. Bei Variante 2 (Signaturbox) befindet sich der Signtrust Signaturserver auf einer fest eingebauten CompactFlash-Karte im Gehäuse, das vom Hersteller versiegelt wurde, so dass eine Integritätsüberprüfung im Betrieb anhand der Versiegelung erfolgen kann. Darüber hinaus können nur elektronisch signierte neue Versionen auf die CompactFlash-Karte über die externe USB-Schnittstelle eingespielt werden.

Insbesondere wird das Ausforschen der PIN auf der Rechner-Plattform durch die Verwendung von einem bestätigten Chipkartenleser mit sicherer PIN-Eingabe ausgeschlossen.

Weitere Hinweise zum Schutz im Betrieb finden sich in Abschnitt 3.2.8.

3.2.4 Auflagen zur Auslieferung und Installation des Produktes

Die Signaturanwendungskomponente Signtrust Signaturserver, Version 4.1 bestehend aus einer zentralen Serverkomponente und einer Client-API zum Entwickeln von Anwendungen wird vom Hersteller als Produkt zusammen mit der Betriebsdokumentation auf einer einmal beschreibbaren CD-ROM ausgeliefert.

Die Signaturanwendungskomponente Signtrust Signaturserver ist, abhängig ob es sich um die zentrale Serverkomponente oder die Client-API handelt, für die folgende technische Einsatzumgebung vorgesehen:

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen oder die Nutzung andere Compiler ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Signaturanwendungskomponente Signtrust Signaturserver darf deshalb ausschließlich in der nachfolgend beschriebenen Hard- und Softwareumgebung eingesetzt werden.

3.2.4.1 Technische Einsatzbedingung der Variante 1 (Server-Plattform)

Server-Plattform als zentrale Serverkomponente des Signtrust Signaturservers

- x86 kompatibler oder SPARC-Prozessor mit mind. 450 MHz Taktfrequenz, mind. 128 MByte RAM, mind. einer Schnittstelle zum Anschluss des Chipkartenlesers und ein Netzwerkanschluss,
- Betriebssysteme Linux (Kernel 2.6) oder Sun Solaris (Version 9),
- bestätigter Chipkartenleser mit PIN-Pad:
  - Kobil Kaan Advanced (FW-Version 1.02, HW-Version K104R3) (Bestätigung: BSI.02050.TE.12.2006 vom 20.12.2006),
  - Kobil Kaan Advanced (FW-Version 1.19, HW-Version K104R3) (Bestätigung: BSI.02050.TE.12.2006 vom 20.12.2006 mit Nachtrag zur Bestätigung: T-Systems.02207.TU.04.2008 vom 07.04.2008),
  - Reiner cyberJack pinpad, Version 3.0 (Bestätigung: TUVIT.93107.TU.11.2004 vom 26.11.2004),
  - Reiner cyberJack e-com, Version 3.0 (Bestätigung: TUVIT.93155.TE.09.2008 vom 16.09.2008),
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
  - G&D StarCOS 3.2 QES Version 2.0 (Bestätigung: BSI.02114.TE.12.2008 vom 19.12.2008 mit Nachtrag zur Bestätigung: T-Systems.02243.TU.03.2010 vom 08.03.2010),

  mit gültigem qualifiziertem Zertifikat, das eine Beschränkung gemäß § 7 Nr. 7 SigG für den geplanten Anwendungszweck (z. B.: für Rechnungssignatur gemäß § 14 Abs. 3 Nr. 1 UStG) enthält,
- verschlossener Elektroschrank mit der Rechner-Plattform und den Kartenlesern,

3.2.4.2 Technische Einsatzbedingung der Variante 2 (Signaturbox)

Signaturbox als zentrale Serverkomponente des Signtrust Signaturservers

- x86 kompatibler Prozessor mit mind. 256 MByte RAM, mind. 4 GB CompactFlash-Karte, einer internen USB-Schnittstelle zum Anschluss des Chipkartenlesers, einer externen USB-Schnittstelle und ein Netzwerkanschluss, keine Festplatte und kein optisches Laufwerk,
- Betriebssystem Linux (Kernel 2.6),
- ein eingebauter bestätigter USB-Chipkartenleser mit PIN-Pad:
  - Reiner cyberJack e-com, Version 3.0 (Bestätigung: TUVIT.93155.TE.09.2008 vom 16.09.2008),
- ein handelsüblicher USB-Stick zur Hinterlegung der frei konfigurierbaren Konfigurationswerte,

- eine sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:

  - G&D StarCOS 3.2 QES Version 2.0
    (Bestätigung: BSI.02114.TE.12.2008 vom 19.12.2008 mit Nachtrag zur Bestätigung: T-Systems.02243.TU.03.2010 vom 08.03.2010),

  mit gültigem qualifiziertem Zertifikat, das eine Beschränkung gemäß § 7 Nr. 7 SigG für den geplanten Anwendungszweck (z. B.: für Rechnungssignatur gemäß § 14 Abs. 3 Nr. 1 UStG) enthält,

- verschlossener Elektroschrank mit der Signaturbox und dem Kartenleser.

Dedizierter Rechner für die Dateischnittstelle des Signtrust Signaturservers

- Betriebssysteme mit Zugriffskontrollmechanismen (einschl. einer zugrunde liegenden Benutzeridentifikation und –authentisierung): Linux (Kernel 2.6), Microsoft Windows XP oder Sun Solaris Version 9,
- Festplatte für die Eingangs- und Ausgangsverzeichnisse der Dateischnittstelle
- Netzwerkanschluss und dedizierte Netzwerkverbindung zur Signaturbox
- SMB-Dienst zur Bereitstellung eines Netzwerkdateisystems,
- Aufstellung mit den zugehörigen Netzwerkverbindungen im verschlossenen Elektroschrank zusammen mit der Signaturbox.
- Integere und authentische Datenübertragung zu den Eingangs- und Ausgangsverzeichnissen der Dateischnittstelle (z. B. mittels IPSEC-VPN: RSA 2048 und AES 256)

3.2.4.3 Weitere serverseitige technische Einsatzbedingungen

Die folgenden technischen Einsatzbedingungen gelten gleichermaßen für beide Server-Varianten 1 und 2:

- abgesicherte Netzwerkverbindung zum Verzeichnisdienst sowie ggf. zur Client-API und zum dedizierten Rechner,
- Beim Einsatz von Batch-Signaturen muss die Prozessorchipkarte nach einer einmaligen Übergabe der PIN in einem Zustand bleiben, der kontinuierlich Zugriff auf die Sicherheitsdienstleistungen der Karte bietet. Die PIN braucht hierbei nicht vor jeder Nutzung einer Sicherheitsdienstleistung der Karte übergeben werden.
- sichere Einsatzumgebung der Dateischnittstelle zur Absicherung der Authentizität und Integrität zu signierender Dokumente und des Veriikationsergebnisses. Die Übertragungssicherung kann beispielsweise über ein IPSEC-VPN (RSA 2048, AES 256) erfolgen. (Bei Verwendung der Netzwerkschnittstelle sichert der Signtrust Signaturserver selbst die Kommunikation über das TLS-Protokoll ab.

3.2.4.4 Technische Einsatzbedingung der Client-API

Client-API des Signtrust Signaturservers

- x86 kompatibler oder SPARC-Prozessor mit mind. 450 MHz Taktfrequenz, mind. 128 MByte RAM, mind. eine Schnittstelle zum Anschluss des Chipkartenlesers und ein Netzwerkanschluss,
- Betriebssysteme Linux (Kernel 2.6), Microsoft Windows XP oder Sun Solaris Version 9.
- abgesicherte Netzwerkverbindung zur zentralen Serverkomponente,
- Compiler Microsoft Visual C++, Version 7.0 (Windows-Variante) bzw. gcc 3.4 (Unix-Variante) zur Einbindung der Client-API in eine Anwendung.

Ferner ist zu beachten: Die Client-API ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer zur Erstellung von Anwendungen verwendet. Dabei darf die Client-API nur in Verbindung mit vertrauenswürdigen Anwendungen eingesetzt werden, welche die vom Signtrust Signaturserver bereitgestellten Sicherheitsfunktionen sachgerecht nutzen, auf Fehlermeldungen korrekt reagieren und diesbezüglich hinreichend geprüft sind. Ferner müssen sicherheitstechnische Veränderungen an der Anwendung für den Nutzer erkennbar werden. Die mit Client-API entwickelten Anwendungen sind nicht Gegenstand dieser Bestätigung.

Entwickler und Administratoren von Anwendungen müssen die oben genannten Bedingungen einhalten.

3.2.5 Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Die Rechner-Plattformen für die zentrale Komponente und die Applikation mit der Client-API sowie der verwendete Chipkartenleser müssen gegen eine unberechtigte Benutzung gesichert sein, damit:

1. die auf der jeweiligen Rechner-Plattform installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf der jeweiligen Rechner-Plattform keine Viren oder Trojanischen Pferde eingespielt werden können,
3. die jeweilige Rechner-Plattform nicht unzulässig verändert werden kann oder

4. die verwendeten Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. (siehe auch Abschnitt 3.2.3).

5. Der Rechner, auf dem der Signaturserver betrieben wird, sowie die eingesetzten Chipkarten und Chipkartenleser (Variante 1) bzw. die Signaturbox (Variante 2) müssen in einem verriegelten Elektroschrank eingesetzt werden. Bei Verwendung der Dateischnittstelle gilt dies auch für den dedizierten Rechner und die dedizierte Netzwerkverbindung zwischen diesem und der Signaturbox.

6. Zugang zu dem Elektroschrank hat der Systemverwalter. Der Elektroschrank muss nach jeder Administrationsarbeit wieder verschlossen werden.

Die Unterrichtung durch den Zertifizierungsdiensteanbieter zur Handhabung der SSEE ist zu beachten.

3.2.6 Auflagen zum Schutz vor Angriffen über Datenaustausch per Datenträger

Bei Einspielung von Daten über Datenträger muss gewährleistet werden, dass

1. die installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann und

2. keine Viren oder Trojanischen Pferde eingespielt werden können,

um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. (siehe auch Abschnitt 3.2.3)

3.2.7 Auflagen zur Sicherheitsadministration des Betriebes

Eine vertrauenswürdige Administration des Signtrust Signaturservers, der Rechner-Plattform sowie der Internet- bzw. Intranetanbindung muss sichergestellt werden.

3.2.8 Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Während des Betriebes sind, abhängig ob es sich um die zentrale Server-komponente oder die Client-API handelt die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

1. zentrale Serverkomponente des Signtrust Signaturservers

   - Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Signaturschlüssel-Inhaber hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet wird noch dass die PIN anderen Personen bekannt gemacht wird.

- Die Anwendung stellt dem Signtrust Signaturserver die zu signierende Datei integer zur Verfügung.
- Die zu signierenden Daten werden dem Signtrust Signaturserver integer über eine Netzwerk-Schnittstelle oder eine Dateischnittstelle zur Verfügung gestellt. Die dabei eingesetzten privaten TLS-Schlüssel bzw. VPN-Zugangsdaten sind vertraulich zu behandeln.
- Die qualifizierten Zertifikate der verwendeten Signaturerstellungseinheiten müssen gültig sein im Sinne des Signaturgesetzes.
- Die authentischen Root-CA- und CA-Zertifikate müssen durch den Signaturschlüssel-Inhaber bereitgestellt sein.
- Die von der Rechner-Plattform bereitgestellte Systemzeit muss korrekt sein und ist regelmäßig durch den Signaturschlüssel-Inhaber zu überprüfen.
- Die Authentifizierungsdaten der einzelnen Mandanten für die Anmeldung des Clients an der zentralen Serverkomponente sind vertrauenswürdig zu verwalten. Ferner muss bei Benutzung der Dateischnittstelle für jeden Mandanten ein eigenes Eingangs- und Ausgangsverzeichnis angelegt sei, auf welches nur er zugriffsberechtigt ist.
- Zum Erkennen von sicherheitstechnischen Veränderungen sind für Variante 1 die Bestandteile der Signtrust Signaturserver durch Binärvergleich mit den Bestandteilen der ausgelieferten CD-ROM und für Variante 2 die Integrität der Herstellersiegel regelmäßig zu überprüfen.
- Für den Fall, dass das Root-Zertifikat in der Zertifikatsdatenbank hinterlegt wird, muss dafür Sorge getragen werden, dass die Zertifikatsdatenbank nur im 4-AP geändert werden kann.
- Ein Austauschen von Chipkarten oder Chipkartenlesern muss eindeutig erkennbar sein (z. B. durch Versiegelung).
- In Batchsignatur-Szenarien sollte im Hauptzertifikat zusätzlich eine entsprechende Beschränkung (z. B. „Nur für Rechnungssignatur“) vorhanden sein, um die qualifizierte Signaturerzeugung auf einen bestimmten Zweck zu beschränken.
- Bei Verwendung von PDF-Prüfberichten ist es für Variante 1 (Serverplattform) möglich, ein vom Systemverwalter hinterlegtes Logo in den Prüfbericht einzubinden. Das korrekte Ablegen des Logos obliegt dem Systemverwalter. Das Logo für den PDF-Prüfbericht darf nicht den Anschein einer Prüfaussage (z. B. „Signaturprüfung erfolgreich“) darstellen.
- Der Systemverwalter muss sich über die Eignung und Gültigkeit der verwendeten Algorithmen auf der Web-Seite der Bundesnetzagentur informieren und den Zeitpunkt, bis zu dem die Verwendung des jeweiligenAlgorithmus erlaubt ist, in der Konfiguration des Signtrust Signaturservers eintragen.

2. Client-API des Signtrust Signaturservers

   - Die Anwendung stellt der Client-API die zu signierende Datei integer zur Verfügung.
   - Die Authentifizierungsdaten für die Anmeldung an der zentralen Serverkomponente sind vertraulich zu behandeln.
   - Der Anwendungsentwickler hat dem Endanwender ein Verfahren zur Integritätsprüfung der entwickelten Anwendung bereitzustellen und diese darauf hinzuweisen, wie er die Integrität der Anwendung überprüfen kann.

3.2.9 Anforderungen an das Wartungs-/Reparaturpersonal

Die vorgesehene Wartung des Signtrust Signaturservers umfasst den Austausch von defekten Chipkartenlesern und den Austausch von Chipkarten. Eine Wartung bzw. Reparatur der Rechner-Plattform ist nur von vertrauenswürdigen Personen durchzuführen.

Der Systemverwalter des Signtrust Signaturservers muss dafür Sorge tragen, dass anfallende Wartungsarbeiten für die Serverplattform (Variante 1) ordnungsgemäß durchgeführt werden. Nach Durchführung der Wartungsarbeiten hat der Systemverwalter sich davon zu überzeugen, dass die Hardware bzw. auf dem Rechner installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um Daten (insbesondere die PIN) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern.

Zur Wartung der Hardwarekomponenten der Signaturbox (Variante 2) muss diese persönlich an den Hersteller übergeben werden. Nach abgeschlossener Wartung wird das Auslieferungsverfahren der Signaturbox erneut durchlaufen.

3.2.10 Authentisierung des Wartungs-/Reparaturpersonals

Eine Authentisierung des Personals für die Wartung bzw. Reparatur der Rechner-Plattform muss geeignet erfolgen.

3.2.11 Aufbewahrung/Transport der Produkte

Die Signaturanwendungskomponente Signtrust Signaturserver, Version 4.1 in den beiden Varianten Serverplattform und Signaturbox bestehend aus einer zentralen Serverkomponente und einer Client-API zum Entwickeln von Anwendungen wird vom Hersteller als Produkt zusammen mit der Betriebsdokumentation auf einer einmal beschreibbaren CD-ROM ausgeliefert.

Es ist darauf zu achten, dass die CD-ROM geschützt aufbewahrt wird.

Die serverseitigen und clientseitigen Bestandteile der Variante 1 (Serverplattform) werden auf einer Single-Session CD-ROM ausgeliefert.

In Variante 2 wird der serverseitige Signtrust Signaturserver vorinstalliert auf einer CompactFlash-Karte, die fest innerhalb der Signaturbox eingebaut ist, ausgeliefert. Das Gehäuse der Box ist vom Hersteller versiegelt. Die externe USB-Schnittstelle wird mit Hilfe eines Prüftools (Signaturprüfung) abgesichert, das vom Hersteller vor

der Auslieferung der Signaturbox auf der CF-Karte installiert wurde. Hierbei können ausschließlich vom Hersteller elektronisch signierte Produktversionen über die externe USB-Schnittstelle eingespielt werden. Der clientseitige Signtrust Signaturserver wird auf einer Single-Session CD-ROM ausgeliefert.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch den Signtrust Signaturserver die Hashalgorithmen RIPEMD-160, SHA-224, SHA-256, SHA-384 und SHA-512, sowie durch die unterstützte SSEE der Algorithmus RSA mit 2048 Bit (PKCS1-V1_5 Padding) verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch den Signtrust Signaturserver zusätzlich die Algorithmen SHA-1 und RSA mit 1024, 1280, 1536, 1728, 1976 und 2048 Bit (PKCS1-V1_5 Padding) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hashfunktion SHA-224 bis Ende des Jahres 2015 und für die Hashfunktionen SHA-256, SHA-384 und SHA-512 bis Ende des Jahres 2017 (siehe BAnz. Nr. 17 vom 01.02.2011, Seite 383).

Ausschließlich zur Prüfung qualifizierter Zertifikate (aber nicht zu deren Erstellung oder zur Erzeugung und Prüfung anderer qualifiziert signierter Daten) reicht die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen SHA-1 und RIPEMD-160 bis Ende des Jahres 2015 (siehe BAnz. Nr. 17 vom 01.02.2011, Seite 383).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA reicht für die Schlüssellänge von 1728 Bit bis Ende des Jahres 2010, für Schlüssellängen von mindestens 1976 bis 2048 Bit bis Ende des Jahres 2017 und die Eignung des PKCS1-V1_5 Paddingverfahrens bis Ende des Jahres 2014 (siehe BAnz. Nr. 17 vom 01.02.2011, Seite 383).

Die Gültigkeit der Bestätigung der Signtrust Signaturserver in Abhängigkeit von Hash-Algorithmus, RSA-Mindestschlüssellänge und Padding-Verfahren kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / RSA-Schlüssellänge Padding-Verfahren	RIPEMD-160, SHA-1 (auschließlich zur Prüfung qualifizierter Zertifikate)	SHA-224	SHA-256, SHA-384, SHA-512
1728 RSASSA-PKCS1-V1_5	2015	2010	2010
1976 – 2048 RSASSA-PKCS1-V1_5	2015	2014	2014

Die Verwendung weiterer Hash-Verfahren zur Signaturerzeugung fällt nicht unter diese Bestätigung.

Diese Bestätigung des Signtrust Signaturserver ist somit, abhängig vom Hash-Verfahren, der Mindestschlüssellänge und dem Padding-Verfahren maximal gültig bis 31.12.2014; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

3.4 Prüfstufe und Mechanismenstärke

Die Signaturanwendungskomponente Signtrust Signaturserver, Version 4.1 wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung