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 3.1.1.3

der

Deutsche Post Com GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93128.TE.11.2006

registriert.

Essen, 21.11.2006

gez. Dr. Sutter
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) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch 1. SigÄndG

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturanwendungskomponente Signtrust Signaturserver, Version 3.1.1.3[3] bestehend aus einer zentralen Serverkomponente und einer Client-API zum Entwickeln von Anwendungen (siehe folgende Tabelle Zeilen 1-2 bzw. 3-8)

Auslieferung:
Als Produkt zusammen mit der Betriebsdokumentation durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM mit den folgenden Bestandteilen:

Bezeichnung	Beschreibung	Version, Datum
signaturserver-3.1.1.3	Ausführbares Programm für Linux	3.1.1.3, 22.09.2006
signaturserver-3.1.1.3	Ausführbares Programm für Solaris	3.1.1.3, 22.09.2006
libSignServerClientApi.a	Client-APIBibliothek für Linux	3.1.1.2, 13.04.2006
libSignServerClientApi.a	Client-APIBibliothek für Solaris	3.1.1.2, 13.04.2006
ClientApi.dll	Client-APIBibliothek für Windows	3.1.1.2, 13.04.2006
ClientApi.lib	Statische Stublib zum Export des Interfaces der ClientApi.dll	3.1.1.2, 13.04.2006
ClientApi.h	Headerdatei 1 zu ClientAPI.dll sowie libSignServerClientApi.a	3.1.1.2, 13.04.2006
ClientApiTypes.h	Headerdatei 2 zu ClientAPI.dll sowie libSignServerClientApi.a	3.1.1.2, 13.04.2006
CertificateDatabase.dat	Zertifikatsdatenbank	Exemplarische Datei ohne Version
signaturserver.conf	1. Konfigurationsdatei	Exemplarische Datei ohne Version
configmodule.ini	2. Konfigurationsdatei	Exemplarische Datei ohne Version
SignTrust-Server_BD.doc	Benutzerdokumentation – Signtrust Signaturserver, Version 3.1	1.6, 09.10.2006
SignTrust-Server_SD.doc	Systemverwalterdokumentation – Signtrust Signaturserver, Version 3.1	1.8, 09.10.2006

Ferner wird das Dokument „Konfigurationsliste – Signtrust Signaturserver, Version 3.1 (Dokument-Version 1.1 vom 10.10.2006) in Papierform persönlich übergeben.

[3] Im Folgenden kurz mit Signtrust Signaturserver bezeichnet.

Hersteller:
Deutsche Post Com GmbH
Geschäftsfeld Signtrust
Tulpenfeld 9, 53113 Bonn

2 Funktionsbeschreibung

Das Softwareprodukt Signtrust Signaturserver, Version 3.1.1.3 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. 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 bei der Signaturerzeugung die Signaturformate PKCS#1, PKCS#7, XML-DSig und PDF (integrierte Signatur) und bei der Signaturprüfung die Formate PKCS#1 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 SHA-1 zum Hashen sowie RSA mit 1024 Bit zur Signaturprüfung.

Die unterstützten SSEE (siehe Abschnitt 3.2.4) verwenden bei der Signaturerzeugung den Algorithmus RSA mit 1024 Bit. Nach erfolgreicher PIN-Authentifizierung können sie eine unbegrenzte Anzahl von Signaturen erzeugen (Multisignatur-SSEE). Der Signtrust Signaturserver begrenzt die Anzahl der Signaturen mittels eines Zeitfensters, das die Dauer der Freischaltung der SSEE nach PIN-Authentifizierung begrenzt. 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 benötigte Anwendung ist **nicht** Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturanwendungskomponente Signtrust Signaturserver erfüllt 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. 1 (keine Preisgabe oder Speicherung der Identifikationsdaten, Signatur nur durch berechtigt signierende Person, eindeutige Anzeige der Signatur vor Erzeugung) 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. Beide Netzverbindungen müssen so abgesichert sein, z. B. durch geeignet konfigurierte Firewalls, dass online Angriffe aus dem Internet auf sowohl auf die Rechner-Plattform des Servers als auch auf die der 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 Netzverbindungen 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. Insbesondere kann das Ausforschen der PIN auf der Rechner-Plattform nur bei einem Chipkartenleser mit sicherer PIN-Eingabe ausgeschlossen werden.

3.2.4 Auflagen zur Auslieferung und Installation des Produktes

Die Signaturanwendungskomponente Signtrust Signaturserver, Version 3.1.1.3 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:

1. zentrale Serverkomponente 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 2.4) oder Sun Solaris Version 9,
   - mind. B1 kompatibler Kartenleser, welcher die PC/SC- bzw. CT-API-Schnittstelle unterstützt, mit passendem Treiber, insbesondere der bestätigte Chipkartenleser mit PIN-Pad mit dem die Bestätigungstests durchgeführt wurden:
     - Kobil B1 Professional (HW-Version KCT100, FW-Version 2.08 GK 1.04) (Bestätigung: TUVIT.09331.TE.03.2002 vom 15.03.2002),
   - mind. eine sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
     - SEA-Card, Version 2.0
       (Bestätigung: TUVIT.09346.TE.02.2001 vom 25.03.2001),
     - PKS-Card, E4KeyCard und E4NetKeyCard jeweils Versionen 3.0 und 3.01
       (Bestätigung: TUVIT.09339.TE.12.2000 vom 15.12.2000 mit Nachträgen vom 22.02.2002 und 07.12.2004),

     mit gültigem qualifiziertem Zertifikat, das ein Beschränkung gemäß § 7 Nr. 7 SigG für den geplanten Anwendungszweck (z. B.: für Rechnungssignatur gemäß § 14 Abs. 3 Nr. 1 UStG) enthält,
   - abgesicherte Netzwerkverbindung zum Verzeichnisdienst sowie ggf. zur Client-API,

- verschlossener Elektroschrank mit der Rechner-Plattform und den Kartenlesern.

2. 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 Windows 2000/XP, Linux (Kernel 2.4), 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.

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 oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

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).

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 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 am EVG sind die Bestandteile der Signtrust Signaturserver durch Binärvergleich mit den Bestandteilen der ausgelieferten CD-ROM zu prüfen.

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

Eine Wartung bzw. Reparatur des Signtrust Signaturservers ist nicht vorgesehen. Eine Wartung bzw. Reparatur der Rechner-Plattform ist nur von vertrauenswürdigen Personen durchzuführen. Nach den durchgeführten Arbeiten ist die Integrität der Rechner-Plattform und aller Applikationen einschließlich der Integrität des Signtrust Signaturservers zu überprüfen.

3.2.10 Authentisierung des Wartungs-/Reparaturpersonals

Eine Wartung bzw. Reparatur des Signtrust Signaturservers ist nicht vorgesehen. 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 3.1.1.3 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.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch den Signtrust Signaturserver der Algorithmus SHA-1 und durch die unterstützten SSEE der Algorithmus RSA mit 1024 Bit verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch die Signtrust Signaturserver die Algorithmen SHA-1 und RSA mit 1024 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende des Jahres 2009 (bei Anwendung bei qualifizierten Zertifikaten bis Ende des Jahres 2010) (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA reicht für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Diese Bestätigung des Signtrust Signaturservers ist somit, abhängig vom Hash-Algorithmus und der RSA-Schlüssellänge, maximal gültig bis 31.12.2007; 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 3.1.1.3 wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung