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
Member of TÜV NORD GROUP
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

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

Signaturanwendungskomponente
Infotech Signer
Version V3.0/Win32

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93189.TE.05.2013

registriert.

Essen, 31.05.2013

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.93189.TE.05.2013 besteht aus 11 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturanwendungskomponente Infotech Signer Version V3.0/Win32[3] bestehend aus einer zentralen Serverkomponente und drei Client-Bibliotheken für Mobilgeräte mit Android-Betriebssystem, für Mobilgeräte mit iOS Betriebssystem von Apple und für Arbeitsstationen mit Betriebssystem Windows 7 von Microsoft.

Auslieferung:

Die Auslieferungsbestandteile des Infotech Signer umfassen die Setup-Datei „ITSigner30.Setup_20130524.exe“ (Serverkomponente) und drei NetSignerService Client-Bibliotheken zur Anbindung an die Serverkomponente.

Die Auslieferung der Setup-Datei „ITSigner30.Setup_20130524.exe“ erfolgt per Webdownload von der Firmenhomepage (https://www.infotech.de/cc/) des Unternehmens. Der Download findet über einen SSL geschützten Kanal statt. Über das Serverzertifikat kann der Anwender die Identität des Servers überprüfen. Alternativ kann die Auslieferung der Serverkomponente auch per CD-ROM erfolgen.

Die Auslieferung der NetSignerService Bibliotheken erfolgt auf Anfrage per CD-ROM.

Der Lieferumfang des Produktes ist in der folgenden Tabelle zusammengefasst:

Produktart	**Bezeichnung (Typ)** **SHA-256-Hashwert**	**Version**	**Übergabeform**
Software	ITSigner.exe (TOE) mit Signatur ITSigner.exe.p7s d6 f1 f0 89 86 7e 66 18 c7 b3 73 e0 a4 26 e3 a3 50 fd d0 ee 0a db d3 97 32 4d 9e db db e7 9d f1	V3.0 / WIN32	In Setup-Datei
Konfigura-tionsdatei	ITSigner.cfg mit Signatur ITSigner.cfg.p7s 68 5c dc 18 ea 2e a3 a1 27 41 86 be 2e 57 8d c8 cb 5b 7d 7f 09 00 ec 44 51 3f 18 08 e8 26 54 21	24.05.2013	In Setup-Datei
Kartenleser-treiber	ITScard.dll mit Signatur ITScard.dll.p7s 59 cf ea 1a fc 1a c2 e6 f9 58 28 0f 90 5e ba 8c 66 85 98 cb 5c a3 4c 6d 50 fe 1f cf 06 24 b6 ac	24.05.2013	In Setup-Datei
Handbuch	ZEDAL30_AGD.pdf 11 a9 01 c9 87 ee ab f0 2c 7b 38 67 3f 25 59 e2 3e b0 ac 1e 2e 81 bb 69 64 8e 2e 2b 3d 5f 60 12	1.4	In Setup-Datei

[3] Im Folgenden kurz mit Infotech Signer bezeichnet.

Produktart	Bezeichnung (Typ) SHA-256-Hashwert	Version	Übergabeform
Prüftool	ITSigner.Check.exe 41 da 83 44 ba a9 ce bc 85 53 99 11 4a 41 b6 1a c7 97 1c 8c eb 08 b5 0e 12 6d c2 ff 7c 37 f5 87	1.3	In Setup-Datei
Android Bibliothek	Libsignerservice.so (TOE) ff 06 14 c3 15 6c 1e 59 39 c9 ea 7a e0 1b 49 2d 4c 84 60 68 bf 7a 72 b5 c7 41 48 f2 70 64 47 5d	1.0 12.04.2013	Auslieferung an Entwickler auf Anfrage per CD-ROM
Windows 7 (32bit) Bibliothek	NetSignerService.dll (TOE) 3f f8 59 19 c3 3a ea a5 c8 9c 4b 41 29 2d 0d 81 b5 22 6f 3e 42 b1 a7 d5 8c 1a 87 07 ca 74 74 60	1.0 12.04.2013	Auslieferung an Entwickler auf Anfrage per CD-ROM
iOS Bibliothek	SignerService.o (TOE) 92 7d bd 4b 8c 3f 05 d9 d7 67 97 a0 8c 22 e3 79 4b ad a1 d7 e0 fc 3f 22 1d 76 2d 14 bd da b3 e8	1.0 10.04.2013	Auslieferung an Entwickler auf Anfrage per CD-ROM

Tabelle 1: Auslieferungsbestandteile

Hersteller:

Infotech Gesellschaft für Informations- und Datentechnik mbH
Holthoffstraße 122a
45659 Recklinghausen

2 Funktionsbeschreibung

Infotech Signer ist eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, zum Erstellen und Verifizieren von qualifizierten elektronischen Signaturen und Anbringen und Prüfen von qualifizierten Zeitstempeln.

Die Serverkomponente von Infotech Signer wurde als ausführbare Datei für Windows-Systeme entwickelt. Das Produkt stellt folgende Funktionalitäten zur Verfügung:

- Erstellung und Prüfung von Signaturen nach PKCS#7, pdf und XML-Signature optional mit XAdES Erweiterungen
- Hashen mittels SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und RIPEMD-160 (SHA-1 und RIPEMD-160 nur zur Signaturprüfung)
- Formatierungsverfahren (Padding) RSASSA-PKCS1-V1_5 nach PKCS#1 v2.1: RSA Cryptographic Standard, 14.06.2002 zur Prüfung von qualifizierten elektronischen Signaturen mit den oben angegebenen Hashverfahren und Schlüssellängen von 1024 bis 2048 Bit in Schritten von 8 Bit. Darüber hinaus werden Schlüssellängen bis 8192 Bit bei der Prüfung von Signaturen unterstützt.

- ECDSA-Verfahren basierend auf Gruppen E(F_{2m}) und den Schlüssellängen 256 Bit zur Prüfung von qualifizierten elektronischen Signaturen mit den oben angegebenen Hashverfahren. Darüber hinaus werden Schlüssellängen von 224, 384 und 512 Bit bei der Prüfung von Signaturen unterstützt.
- Anbringen und Prüfen von qualifizierten Zeitstempeln
- Überprüfung der Gültigkeit von qualifizierten Zertifikaten beim Zertifizierungsdiensteanbieter unter Verwendung des Online Certificate Status Protocol (OCSP)
- Unterstützung bestätigter Chipkartenleser mit sicherer PIN-Eingabe
- Unterstützung von sicheren Signaturerstellungseinheiten (SSEE) in den Ausprägungen Einfach- und Multisignatur
- Bei Multisignatur-SSEE, Möglichkeit der Begrenzung des Signaturvorgangs auf eine maximale Anzahl von Signaturen und/oder Vorgabe des Endes des Zeitintervalls, in dem die SSEE nutzbar bleibt
- Unterstützung von externen Viewern durch Export von signierten Daten oder Daten die signiert werden sollen in einer vom Benutzer kontrollierten Umgebung. Ferner zeigt der EVG Metadaten an, die Rückschlüsse auf die signierten Daten oder Daten, die signiert werden sollen, zulassen.
- Unterstützung der qualifizierten Zertifikate und Attribut-Zertifikate der ZDA D-TRUST, DSV (S-TRUST), DP Signtrust und DTAG (Telesec)
- Optische Visualisierung von SSEE- und Kartenleser-Zuständen sowie von Prüfergebnissen (Signatur und Zertifikate) mittels eindeutiger Symbole. Infotech Signer lässt sich in mehreren Sprachen benutzen, die Bestätigung umfasst jedoch lediglich die deutsche Sprache.
- Schutz des Installationsprozesses gegen Manipulation durch den Download signierter Dateien über einen geschützten Kanal
- Möglichkeit zum Signieren von Dokumenten von entfernten Arbeitsplätzen

Mittels der NetSignerService Client-Bibliothek kann Infotech Signer auch von entfernten Arbeitsplätzen oder Mobilgeräten verwendet werden. Die Bibliothek ist für Mobilgeräte mit Android-Betriebssystem von Open Handset Alliance, für Mobilgeräte mit iOS Betriebssystem von Apple und Arbeitsstationen mit Betriebssystem Windows 7 (32bit) von Microsoft verfügbar. Sie baut eine abgesicherte Verbindung zur zentralen Serverkomponente auf. Die Bibliothek muss vertrauenswürdig in eine Anwendung (nicht Gegenstand der Bestätigung) eingebunden werden. Sie stellt der Anwendung, nach erfolgreicher Authentifizierung des Benutzers an der zentralen Serverkomponente, die oben genannten Server-Funktionen zur Erzeugung bzw. Prüfung von qualifizierten elektronischen Signaturen und Zertifikaten zur Verfügung, indem sie die Daten an die zentrale Serverkomponente gesichert übermittelt und die Antworten gesichert entgegennimmt.

Infotech Signer ist eine Signaturanwendungskomponente § 2 Nr. 11 SigG, die elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen durch eine sichere Signaturerstellungseinheit zuführen kann. Qualifiziert signierte elektronische Dokumente können via Timestamp Protocol mit einem qualifizierten Zeitstempel versehen werden.

Zusätzlich können mit Infotech Signer erzeugte qualifizierte elektronische Signaturen und qualifizierte Zertifikate auf ihre Gültigkeit hin überprüft und die Ergebnisse der Überprüfung angezeigt werden. Infotech Signer bietet hierzu die Möglichkeit, den Zertifikatstatus online bei einem OCSP-Verzeichnisdienst abzufragen.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Infotech Signer erfüllt die Anforderungen nach § 17 Abs. 2 Satz 1 (eindeutige Anzeige und Feststellbarkeit der Daten bei Signaturerzeugung), 2 (Feststellbarkeit der Daten, des Unverändertseins der Daten, der Zuordnung zum Signaturschlüsselinhaber, des Inhalts des qualifizierten Zertifikats und des Ergebnisses der Nachprüfung von Zertifikaten bei Signaturprüfung) sowie 3 (bei Bedarf Anzeige des Inhalts der zu signierenden oder signierten Daten) SigG und nach § 15 Abs. 2 Satz 1 (keine Preisgabe der Identifikationsdaten, Signatur nur durch berechtigt signierende Person, eindeutige Anzeige der Signatur vor Erzeugung) und 2 (korrekte Prüfung der Signatur und eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) sowie Abs. 4 (Erkennbarkeit von sicherheitstechnischen Veränderungen) SigV.

3.2 Einsatzbedingungen

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

Grundlage dieser Bestätigung ist der Einsatz von Infotech Signer in einem ***geschützten Einsatzbereich***. Für den sicheren Einsatz von Infotech Signer 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 von der Serverkomponente zum Verzeichnisdienst des Zertifizierungsdienstes ist für die Prüfung der Gültigkeit von Zertifikaten notwendig. Ferner wird auch zwischen der zentralen Serverkomponente und der Applikation mit der NetSignerService Client-Bibliothek eine Netzwerkverbindung benötigt. Beide Netzverbindungen müssen so abgesichert sein, z. B. durch geeignet konfigurierte Firewalls, dass online Angriffe aus dem Internet auf die jeweilige Rechner-Plattform erkannt bzw. unterbunden werden.

3.2.2 Auflagen zur Anbindung an ein Intranet

Wenn die zentrale Serverkomponente oder die NetSignerService Client-Bibliotheken in einem Intranet betrieben werden, 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 Benutzer von Infotech Signer muss sich davon überzeugen, dass keine Angriffe von den Rechner-Plattformen und den dort vorhandenen Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf den Rechner-Plattformen installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf den Rechner-Plattformen keine Viren oder Trojanischen Pferde eingespielt werden können,
3. die Rechner-Plattformen nicht unzulässig verändert werden können,
4. beim Einsatz von Mobilgeräten der Betrieb nur mit den originalen Betriebssystemkomponenten (ohne Jailbreak) erfolgt,
5. auf Mobilgeräten zum Aufbau des sicheren Kanals zusätzliche Zufallsdaten (Entropie) benötigt werden, die aus dem vorausgesetzten Lagesensor bezogen werden, und
6. 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 Infotech Signer Installation ist auf den IT-Plattformen regelmäßig zu überprüfen.

3.2.4 Auflagen zur Auslieferung und Installation des Produktes

Die Auslieferungsbestandteile des Infotech Signer umfassen die Setup-Datei „ITSigner30.Setup_20130524.exe“ (Serverkomponente) und drei NetSignerService Client-Bibliotheken zur Anbindung an die Serverkomponente.

Die Auslieferung der Setup-Datei „ITSigner30.Setup_20130524.exe“ erfolgt per Webdownload von der Firmenhomepage (https://www.infotech.de/cc/) des Unternehmens. Der Download findet über einen SSL geschützten Kanal statt. Über das Serverzertifikat kann der Anwender die Identität des Servers kontrollieren. Alternativ kann die Auslieferung der Serverkomponente auch per CD-ROM erfolgen.

Die Auslieferung der NetSignerService Bibliotheken erfolgt auf Anfrage per CD-ROM.

Die Serverkomponente von Infotech Signer ist für die folgende technische Einsatzumgebung vorgesehen:

- Rechner lauffähig mit Windows 7 (32bit) von Microsoft
- Infotech Program Integrity Checker (Prüftool ITSigner.Check.exe)
- bestätigte Kartenleser
  - Cherry GmbH Smartboard xx44, Firmware 1.04
    (Bestätigung: BSI.02048.TE.12.2004 vom 10.12.2004, kein Ablaufdatum gemäß Bestätigung)
  - Reiner Kartengeräte GmbH & Co. KG cyberJack pinpad, Version 3.0
    (Bestätigung: TUVIT.93107.TU.11.2004 vom 26.11.2004, kein Ablaufdatum gemäß Bestätigung)

  - Reiner Kartengeräte GmbH & Co. KG cyberJack e-com Version 3.0 (Bestätigung: TUVIT.93155.TE.09.2008 vom 16.09.2008, kein Ablaufdatum gemäß Bestätigung)
  - Reiner Kartengeräte GmbH & Co. KG cyberJack e-com plus Version 3.0 (Bestätigung: TUVIT.93156.TE.09.2008 vom 16.09.2008, kein Ablaufdatum gemäß Bestätigung)
  - Reiner Kartengeräte GmbH & Co. KG cyberJack RFID komfort, Version 2.0 (Bestätigung: TUVIT.93180.TU.12.2011, Ablaufdatum gemäß Bestätigung 31.12.2017)

- Sichere Signaturerstellungseinheiten
  - Giesecke & Devrient GmbH: STARCOS 3.4 Health QES C1 (auf QES C2 erweitert) (Bestätigung: BSI.02120.TE.05.2009 vom 19.05.2009 mit Nachtrag vom 15.11.2010, Ablaufdatum gemäß Bestätigung 31.12.2015)
  - Gemalto GmbH: ZKA-Signaturkarte, Version 6.32 (Bestätigung: TUVIT.93184.TU.11.2010 vom 12.11.2010 mit Nachtrag 1 vom 19.05.2011, Ablaufdatum gemäß Bestätigung 31.12.2017)
  - Gemalto GmbH: ZKA-Signaturkarte, Version 6.32 M (Bestätigung: TUVIT.93176.TU.05.2011 vom 19.05.2011, Ablaufdatum gemäß Bestätigung 31.12.2017)
  - Giesecke & Devrient GmbH: STARCOS 3.2 QES, Version 2.0 (Bestätigung: BSI.02114.TE.12.2008 vom 19.12.2008 mit Nachtrag 1 vom 08.03.2010, Ablaufdatum gemäß Bestätigung 31.12.2014)
  - T-Systems Enterprise Services GmbH: TCOS 3.0 Signature Card, Version 1.1 (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006 mit Nachtrag 1 vom 07.05.2010, Ablaufdatum gemäß Bestätigung 31.12.2014)
  - T-Systems International GmbH: TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P (Bestätigung: SRC.00016.TE.11.2012 vom 28.11.2012, Ablaufdatum gemäß Bestätigung 31.12.2018)

  mit gültigem qualifizierten Zertifikat, das bei Multisignatur-SSEE eine Beschränkung gemäß § 7 Nr. 7 SigG für den geplanten Anwendungszweck (z. B. für eine Rechnungssignatur gemäß § 14 Abs. 3 Nr. 1 UStG) enthalten sollte,

- Netzwerkverbindung zu einem Zertifizierungsdiensteanbieter (Verzeichnisdienst und Zeitstempeldienst) sowie ggf. zur Client-Bibliothek

Die NetSignerService Client-Bibliotheken sind für die folgende technische Einsatzumgebungen vorgesehen:

- Mobilgeräte mit Android-Betriebssystem von Open Handset Alliance
- Mobilgeräte mit iOS Betriebssystem von Apple
- Arbeitsstationen mit Betriebssystem Windows 7 (32bit) von Microsoft
- abgesicherte Netzwerkverbindung zur zentralen Serverkomponente

Eine Übertragung der Evaluationsergebnisse auf andere Einsatzumgebungen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Signaturanwendungskomponente Infotech Signer darf deshalb ausschließlich in der oben beschriebenen Einsatzumgebung eingesetzt werden. Nach der Installation muss

die Integritätsprüfung mit dem Infotech Signer Integrity Tool (ITSigner.Check.exe) vorgenommen werden.

Ferner ist zu beachten: Die NetSignerService Client-Bibliotheken werden vom Anwendungsprogrammierer zur Erstellung von Anwendungen verwendet. Dabei dürfen die Client-Bibliotheken nur in Verbindung mit vertrauenswürdigen Anwendungen eingesetzt werden, welche die bereitgestellten Sicherheitsfunktionen sachgerecht nutzen und auf Fehlermeldungen korrekt reagieren und diesbezüglich hinreichend geprüft sind. Ferner müssen sicherheitstechnische Veränderungen an der Anwendung für den Nutzer erkennbar werden. Die mit den Client-Bibliotheken entwickelten Anwendungen sind nicht Gegenstand der 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-Bibliothek, sowie der verwendete Chipkartenleser müssen gegen eine unberechtigte Benutzung gesichert sein, damit:

1. die auf den jeweiligen Rechner-Plattformen installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf den jeweiligen Rechner-Plattformen keine Viren oder Trojanischen Pferde eingespielt werden können,
3. die jeweiligen Rechner-Plattformen nicht unzulässig verändert werden können,
4. beim Einsatz von Mobilgeräten der Betrieb nur mit den originalen Betriebssystemkomponenten (ohne Jailbreak) erfolgt und
5. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wird, 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 Sicherheitsadministration des Betriebes von Infotech Signer ist nicht vorgesehen. Eine vertrauenswürdige Administration der jeweiligen Rechner-Plattformen sowie der Internet- bzw. Intranetanbindung muss sichergestellt werden.

3.2.8 Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz von Infotech Signer zu beachten:

- Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Benutzer hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet wird noch dass die PIN anderen Personen bekannt gemacht wird.
- Die Einstellung der Systemzeit auf den jeweiligen Rechner-Plattformen muss korrekt sein.
- Die Integritätsprüfung ist, so wie in Abschnitt 2.5 des Handbuchs beschrieben, regelmäßig vorzunehmen.
- Die qualifizierten Zertifikate der verwendeten SSEE müssen gültig sein im Sinnes des Signaturgesetzes.
- Wird das Produkt zum Erzeugen von sog. Massensignaturen (vgl. amtliche Begründung zu § 15 Abs. 2 SigV) eingesetzt, dann dürfen ausschließlich Signaturen zu gleichwertigen Dokumenten vorgenommen werden, d. h., die qualifizierten Signaturen dürfen nur anlässlich eines voreingestellten Zweckes erfolgen.
- Die Verwendung eines nicht mehr sicherheitsgeeigneten Algorithmus oder abgelaufener Zertifikate wird nicht unterbunden, jedoch dem Benutzer angezeigt. Der Benutzer muss den Vorgang abbrechen. Die Verwendung nicht mehr sicherheitsgeeigneter Algorithmen ist nicht Gegenstand der Bestätigung.
- Die Anwendung stellt der Client-Bibliothek die zu signierenden Daten integer zur Verfügung.
- Die Authentifizierungsdaten für die Anmeldung an der zentralen Serverkomponente sind vertraulich zu behandeln.
- Der Anwendungsentwickler hat den Anwender darauf hinzuweisen, wie er die Integrität der Anwendung überprüfen kann.

3.2.9 Anforderungen an das Wartungs-/Reparaturpersonal

Eine Wartung bzw. Reparatur von Infotech Signer ist nicht vorgesehen. Eine Wartung bzw. Reparatur der jeweiligen Rechner-Plattformen ist nur von vertrauenswürdigen Personen durchzuführen. Nach den durchgeführten Arbeiten ist die Integrität der jeweiligen Rechner-Plattformen und aller Applikationen einschließlich der Integrität von Infotech Signer zu überprüfen (Infotech Signer Integrity Tool (ITSigner.Check.exe).

3.2.10 Authentisierung des Wartungs-/Reparaturpersonals

Eine Wartung bzw. Reparatur von Infotech Signer ist nicht vorgesehen.

3.2.11 Aufbewahrung/Transport der Produkte

Es ist darauf zu achten, dass die Setup-Datei ITSigner30.Setup_20130524.exe und das Prüftool ITSigner.Check.exe sowie die Client-Bibliotheken geschützt aufbewahrt werden.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt die Hashfunktionen SHA-224, SHA-256, SHA-384, SHA-512 sowie durch die unterstützten SSEE der Algorithmus RSA mit 1976 bis 2048 Bit oder ECDSA mit 256 Bit verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden vom Produkt die Hashfunktionen SHA-1, RIPEMD-160, SHA-224, SHA-256, SHA-384, SHA-512 und RSA mit RSASSA-PKCS1-V1_5 Padding und den Schlüssellängen 1024 bis 8192 Bit sowie das ECDSA-Verfahren basierend auf Gruppen $E(F_{2m})$ und den Schlüssellängen 224, 256, 384 und 512 Bit 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 2019 (siehe BAnz. AT 27.03.2013 B4).

Zur Prüfung qualifizierter Zertifikate 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. AT 27.03.2013 B4).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA mit RSASSA-PKCS1-V1_5 Padding reicht für die Mindestschlüssellänge von 1976 Bit bis Ende des Jahres 2015 (siehe BAnz. AT 27.03.2013 B4).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren ECDSA basierend auf Gruppen $E(F_{2m})$ reicht für die Mindestschlüssellänge (Parameter q) von 224 Bit bis Ende des Jahres 2015 und für die Mindestschlüssellänge (Parameter q) von 250 Bit bis Ende des Jahres 2019 (siehe BAnz. AT 27.03.2013 B4).

Die Gültigkeit der Bestätigung des Produkts in Abhängigkeit von Hash-Algorithmus, RSA- und ECDSA-Mindestschlüssellänge sowie Padding-Verfahren kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / Schlüssellänge, Padding-Verfahren	RIPEMD-160, SHA-1 zur Prüfung von qualifizierten Zertifikaten	SHA-224	SHA-256, SHA-384, SHA-512
RSA: 1976 – 8192, RSASSA-PKCS1-V1_5	2015	2015	2015
ECDSA: q = 224 Bit	2015	2015	2015
ECDSA: q = 250 Bit	2015	2015	2019

Diese Bestätigung des Produktes ist somit, abhängig vom Hash-Verfahren, dem Signaturverfahren, der Mindestschlüssellänge, dem Padding-Verfahren und den Gültigkeiten der Bestätigungen der eingesetzten Produkte maximal gültig bis 31.12.2019; 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 Infotech Signer Version V3.0/Win32 wurde erfolgreich nach der Prüfstufe EAL3+ mit ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, und AVA_VAN.5 (vollständige Missbrauchsanalyse und hohes Angriffspotential) der Common Criteria (CC) V3.1 Revision 4 evaluiert.

Die für die Signaturanwendungskomponenten nach SigV maßgebende Prüfstufe EAL3+ mit ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1, und AVA_VAN.5 (vollständige Missbrauchsanalyse und hohes Angriffspotential) wird damit erreicht.

Ende der Bestätigung