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 Infotech Signer, Version V2.0/Win32

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93165.TE.12.2010

registriert.

Essen, 17.12.2010

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.93165.TE.12.2010 besteht aus 9 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang

Signaturanwendungskomponente Infotech Signer Version V2.0/Win32[3]

Auslieferung:

Die Auslieferung des Produktes erfolgt mittels der Setup-Datei „ITSigner.Setup_20100701.exe“ per Webdownload von der Homepage des Unternehmens (https://www.infotech.de/cc/). Der Download findet über einen SSL geschützten Kanal statt. Über das Serverzertifikat kann der Anwender die Identität des Servers kontrollieren.

Alternativ kann die Auslieferung des Produktes auch per CD-ROM erfolgen.

Nach Ausführung der Setup-Datei werden die folgenden Dateien in das gewählte Verzeichnis kopiert:

Produktart	Bezeichnung (Typ)	SHA-256 - Hashwert	Datum
Software	ITSigner.exe mit Signatur ITSigner.exe.p7s	b3 ec 96 60 6c de 63 e1 61 f3 e8 d6 64 a3 8f 93 60 b6 60 72 fb 45 7a a9 6d 82 77 1b 3b 07 ba ed	01.07.2010
Prüftool	ITSigner.Check.exe	f1 65 9e d4 31 4a 82 c4 22 56 e4 8f ef 8e 0d 21 75 06 41 c0 1d 35 f3 2a 14 83 e3 77 d3 6a 64 59	01.07.2010
Konfigura-tionsdatei	ITSigner.cfg mit Signatur ITSigner.cfg.p7s	56 c8 82 8a c8 14 d0 8c 97 53 4e 75 55 85 f1 22 9b 61 ba 71 49 46 57 f7 50 fc 6a 3f 92 4f 9c 4c	01.07.2010
Treiber	ITScard.dll mit Signatur ITScard.dll.p7s	54 1c 56 22 3e 8e c4 7d c3 57 7f a0 0e 9b 79 08 ff be 18 0d 23 47 7c a3 1f e7 b0 61 ef 83 a8 d0	01.07.2010
Handbuch	ZEDAL_AGD_0.5.pdf	52 f5 c9 f1 6c a0 98 72 e6 fa 06 6c 06 46 08 26 fb 7a 67 dd b6 e0 b2 00 b7 6f 46 88 92 22 4e 08	13.12.2010

Tabelle 1: Auslieferungsbestandteile

Hersteller:

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

[3] Im Folgenden kurz mit Infotech Signer bezeichnet.

2 Funktionsbeschreibung

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

Infotech Signer wurde als ausführbare Datei für Windows-Systeme entwickelt. Unter Kontrolle einer Windows Applikation (z. B. als Browser Plug-In) stellt das Produkt folgende Funktionalitäten zur Verfügung:

- Erstellung und Prüfung von qualifizierten Signaturen nach PKCS#7 und XML-Signature mit XAdES Erweiterungen
- Hashen mittels SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und RIPE-MD 160
- RSASSA-PKCS1-V1_5 nach PKCS#1 zur Signaturprüfung mit den oben angegebenen Hashverfahren und Schlüssellängen von 1024 bis 4096 Bit in Schritten von 16 Bit
- 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 oder eine maximale Zeit zwischen zwei Signaturausführungen
- Unterstützung der qualifizierten Zertifikate und Attribut-Zertifikate der ZDA D-TRUST, DSV (S-TRUST), DP Com (Signtrust), und DTAG (Telesec)
- Unterstützung von externen Viewern durch Export von signierten Daten oder Daten die signiert werden sollen in einer vom Benutzer kontrollierten Umgebung. Ferner zeigt das Produkt Metadaten an, die Rückschlüsse auf die signierten Daten oder Daten die signiert werden sollen zulassen.
- 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 vor unbemerkter Veränderung der Programmkomponenten. Bei Systemstart prüft Infotech Signer mittels der mitgelieferten Signaturdateien die Integrität der Programmkomponenten. Bei Integritätsverletzungen werden diese angezeigt und Infotech Signer wird beendet.
- Schutz des Installationsprozesses gegen Manipulation durch eine signierte Zustellung.

Infotech Signer ist eine Signaturanwendungskomponente gemäß § 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) sowie 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 (z. B. mittels Modem, ISDN oder LAN-Anschluss) zum Verzeichnisdienst des Zertifizierungsdienstes ist für die Prüfung der Gültigkeit von Zertifikaten notwendig. Diese Netzverbindung muss so abgesichert sein, z. B.

durch eine geeignet konfigurierte Firewall, dass online Angriffe aus dem Internet auf den eingesetzten Personalcomputer erkannt bzw. unterbunden werden.

3.2.2 Auflagen zur Anbindung an ein Intranet

Wenn der eingesetzte Personalcomputer in einem Intranet betrieben wird, so muss diese Netzverbindung geeignet abgesichert sein, so dass online Angriffe aus dem Intranet auf den Computer 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 dem Personalcomputer und den dort vorhandenen Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf dem Personalcomputer und ggf. dem Server installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,

2. auf dem Personalcomputer und ggf. dem Server keine Viren oder Trojanischen Pferde eingespielt werden können,

3. die Hardware des Personalcomputers und ggf. des Servers nicht unzulässig verändert werden kann oder

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.

Die Integrität der Infotech Signer Installation auf dem Personalcomputer und ggf. auf dem Server ist regelmäßig zu überprüfen.

3.2.4 Auflagen zur Auslieferung und Installation des Produktes

Die Auslieferung von Infotech Signer erfolgt zusammen mit der Fachanwendung per Webdownload von der Firmenhomepage des Unternehmens. Der Download findet über einen SSL geschützten Kanal statt. Über das Serverzertifikat kann der Anwender die Identität des Servers kontrollieren.

Infotech Signer ist auch als Entwicklerversion zur Verwendung in weiteren Fachanwendungen verfügbar. Die Entwicklerversion wird auf Anfrage mit weiteren Dokumentationen und Klassen zur Integration in Anwendungen auf einem Installationsmedium (CD-ROM) ausgeliefert.

Die Signaturanwendungskomponente Infotech Signer ist für die folgende technische Einsatzumgebung vorgesehen:

- Betriebssysteme 32 Bit Windows XP, Windows Vista und Windows 7

- bestätigter Chipkartenleser mit PIN-Pad und auf dem Rechner installiertem passenden Kartenlesertreiber, z. B. der im Rahmen der Bestätigung verwendete Treiber cyberJack Base Components, V 6.8.0:

  - Reiner cyberJack pinpad, Version 3.0
    (Bestätigung: TUVIT.93107.TU.11.2004 vom 26.11.2004),

- Reiner cyberJack e-com, Version 2.0
  (Bestätigung: TUVIT.09363.TE.06.2002 vom 03.06.2002)

- mind. eine sichere Signaturerstellungseinheiten gemäß § 2 Nr. 10 SigG:

  - D-TRUST:
    Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature
    (Bestätigung T-Systems.02182.TE.11. 2006 vom 30.11.2006 mit Nachträgen vom 06.02.2007 und 06.05.2008)

  - DSV (S-TRUST):
    ZKA Banking Signature Card, Version 6.6; Giesecke & Devrient GmbH
    (Bestätigung: TUVIT.93130.TU.05.2006 vom 19.05.2006 mit Nachträgen vom 28.08.2006 und 18.10.2006)

  - DP-COM (Signtrust):
    STARCOS 3.2 QES Version 1.1; Giesecke & Devrient GmbH
    (Bestätigung: BSI.02102.TE.11.2008 vom 24.11.2008)

  - DTAG (Telesec):
    TCOS 3.0 Signature Card, Version 1.1 (NetKey 3.0) or TCOS 3.0 Signature Card, Version 1.1 (NetKey 3.0M)
    (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006 mit Nachtrag vom 07.05.2010)

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

- Netzwerkverbindung zu einem Zertifizierungsdiensteanbieter (Verzeichnisdienst und Zeitstempeldienst).

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Signaturanwendungskomponente Infotech Signer darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden. Nach der Installation muss die Integritätsprüfung, so wie in Abschnitt 2.5 des Handbuchs beschrieben, vorgenommen werden.

3.2.5 Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Der Personalcomputer, auf dem Infotech Signer verwendet wird, sowie der verwendete Chipkartenleser müssen gegen eine unberechtigte Benutzung gesichert sein, damit:

1. die auf dem Personalcomputer und ggf. auf dem Server installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,

2. auf dem Personalcomputer und ggf. auf dem Server keine Viren oder Trojanischen Pferde eingespielt werden können,

3. die Hardware des Personalcomputers und ggf. die des Servers nicht unzulässig verändert werden kann oder

4. 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 Signaturkarte 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 des Personalcomputers sowie der Internet- bzw. Intranetanbindung muss jedoch 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 des Personalcomputers und ggf. des Servers muss korrekt sein.

- Die Integritätsprüfung ist, so wie in Abschnitt 2.5 des Handbuchs beschrieben, regelmäßig vorzunehmen.

- 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,

3.2.9 Anforderungen an das Wartungs-/Reparaturpersonal

Eine Wartung bzw. Reparatur von Infotech Signer ist nicht vorgesehen. Eine Wartung bzw. Reparatur des Personalcomputers ist nur von vertrauenswürdigen Personen durchzuführen. Nach den durchgeführten Arbeiten ist die Integrität des Personalcomputers und aller Applikationen einschließlich der Integrität von Infotech Signer zu überprüfen.

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 ITSigner.Setup_20100701.exe und das Prüftool ITSigner.Check.exe geschützt aufbewahrt werden.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt die Hashfunktionen RIPE-MD 160, SHA-224, SHA-256, SHA-384, SHA-512 sowie durch die unterstützten SSEE der Algorithmus RSA mit 1728 bis 2048 Bit verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden vom Produkt die Hashfunktionen SHA-1, RIPE-MD 160, SHA-224, SHA-256, SHA-384, SHA-512 und RSA PKCS#1-v1.5 mit den Schlüssellängen 1024 bis 4096 Bit in Schritten von 16 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hashfunktion RIPEMD-160 bis Ende des Jahres 2010, 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 2016 (siehe BAnz. Nr. 19 vom 04.02.2010, Seite 426).

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. Nr. 19 vom 04.02.2010, Seite 426).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSASSA-PKCS1-V1_5 reicht für Mindestschlüssellängen von 1728 Bit bis Ende des Jahres 2010 und für Mindestschlüssellängen von 1976 Bit bis Ende des Jahres 2014 (siehe BAnz. Nr. 19 vom 04.02.2010, Seite 426).

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

Hash-Algorithmus / Schlüssellänge, Padding-Verfahren	RIPEMD-160, SHA-1 bei Erzeugung qualifizierter Zertifikate und mindestens 20 Bit Entropie der Seriennummer	SHA-224	SHA-256, SHA-384, SHA-512
1728, alle Padding-Verfahren	2010	2010	2010
1976 – 4096, RSASSA-PKCS1-V1_5	2010	2014	2014

Diese Bestätigung des Produktes 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 Infotech Signer Version V2.0/Win32 wurde erfolgreich nach der Prüfstufe EAL3+ mit Zusatz ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 und AVA_VAN.5 (hohes Angriffspotenzial einschließlich Missbrauchsanalyse) der Common Criteria, Version 3.1 R3 (CC) evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung