

Herstellereklärung

Die

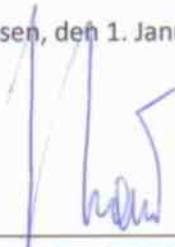
Infotech GmbH
Holthoffstraße 122a
D-45659 Recklinghausen
HRB 1912 AG Recklinghausen

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG¹
in Verbindung mit § 15 Abs. 5 der SigV²,
dass ihr Produkt

Infotech Signer³, Version 2.0 / Win32

die nachstehend genannten Anforderungen des SigG und der SigV erfüllt

Recklinghausen, den 1. Januar 2010



Rainer Hans, Geschäftsführer

Parallel läuft das Bestätigungsverfahren nach Signaturgesetz für Infotech Signer bei **TÜV Informationstechnik GmbH** unter der Nummer TUVIT.93165.TE nach Common Criteria EAL3+ / hoch (www.tuvit.de).

Diese Herstellereklärung ist bis zum Abschluss des Bestätigungsverfahrens gültig.
Sie trägt die Dokumentnummer he.infotech.2010.1 und besteht aus 6 Seiten.

¹ Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert am 17. Juli 2009 (BGBl. I S. 2091)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert am 18. Juni 2009 (BGBl. I S. 1346)

³ Infotech Signer ist ein eingetragenes Warenzeichen der Infotech GmbH, Recklinghausen. Es ist in allen Ländern der Europäischen Gemeinschaft geschützt.

Anlage zur Herstellererklärung vom 1. Januar 2010

1. Handelsbezeichnung und Lieferumfang

Die Handelsbezeichnung lautet Infotech Signer.

Die Auslieferung erfolgt in Form eines Setup gemeinsam mit den Fachapplikationen ZEDAL Forms und E-Form. Das Setup wird durch einen SSL-gesicherten Kanal vom Anwender heruntergeladen und enthält folgende signierte Dateien:

- ITsigner.exe
- ITsigner.cfg
- ITScard.dll

Authentizität und Integrität des Infotech Signer werden durch Prüfroutinen des Setup Programms und bei jedem Programmstart der Fachapplikationen sichergestellt.

Einsatz und Verwendung des Infotech Signers werden in den Handbüchern von ZEDAL Forms und E-Form beschrieben.

2. Funktionsbeschreibung

Infotech Signer ist eine Signatur Anwendungskomponente (SAK). Durch Einbindung dieser Komponente können Applikationen Daten signieren und die Signatur von signierten Daten verifizieren.

Infotech Signer ist das Nachfolgeprodukt von ZEDAL(SIG), das seit 2004 für die elektronische Nachweisführung in ZEDAL und E-Form eingesetzt wird (Herstellererklärung he.infotech.2004.1 vom 22.10.2004). Im Gegensatz zu ZEDAL(SIG) ermöglicht Infotech Signer Signaturen, die den Vorgaben der Anlage 3 der Nachweisverordnung gerecht werden. Auf der ZEDAL Plattform wird Infotech Signer in ZEDAL Forms, einem Formulareditor, eingesetzt.

Infotech Signer stellt im Einzelnen folgende Funktionalitäten zur Verfügung:

- Erstellung und Prüfung von Signaturen nach PKCS#7
- Erstellung und Prüfung von Signaturen nach XML-Signature mit XAdES Erweiterungen
- Zertifikatsprüfung
- OCSP-Prüfung
- Zeitstempelanforderung
- Bedienoberfläche zur Anzeige von Zuständen und Interaktion mit dem Benutzer (GUI)

Zur Kommunikation mit der Applikation stellt das Programm eine Schnittstelle bereit. Die Steuerung der Funktionen durch die Applikation erfolgt über ein spezielles Protokoll. Das Protokoll sieht eine Authentifizierung vor, so dass nur zugelassene Anwendungen die Funktionen nutzen können. Die Konnektivität mit dem Internet wird ebenfalls über dieses Protokoll hergestellt. Dazu leitet die

Applikation die Anfragen der SAK zum Internet weiter und liefert das Ergebnis der Anfragen zurück. Diese Funktion wird für die Zertifikatsprüfung nach OCSP und das Einholen von Zeitstempeln benötigt. Durch Schlüsselwerte in den Anfragen wird sichergestellt, dass die Antworten zu den Anfragen passen. Durch diese Vorgehensweise ist die SAK auch ohne eigene Netzwerk-Einstellungen in einem Browser-Plugin einsetzbar.

Die SAK verfügt über eine Statusanzeige, in der der aktive Kartenleser, die benutzte Karte, Metadaten zu den bereitgestellten Datenblöcken und eine gerade durchgeführte Signatur angezeigt werden.

Neben der Statusanzeige können Daten, auf die sich eine Signatur bezieht, und die Zertifikatsdaten und Prüfergebnisse als Datei bereitgestellt werden (dies ist unabhängig von der übergeordneten Applikation immer möglich). Während der Durchführung einer Signatur oder Prüfung ist eine Veränderung der Daten nicht möglich.

Variable Programmkonfigurationen werden ebenfalls vom Hersteller signiert bereitgestellt. Das umfasst u.a. die Einstellungen zur Sicherheitseignung von Algorithmen und deren Parametern, wie die Gültigkeitsdauer der Algorithmen zur Hash-Erzeugung.

Neben einfachen Signaturkarten werden Multisignaturkarten unterstützt.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Infotech Signer erfüllt die folgenden Anforderungen des § 17 Abs. 2 SigG.

Hinsichtlich der Signaturerstellung zeigt Infotech Signer die Erzeugung einer qualifizierten Signatur vorher eindeutig an und lässt feststellen, auf welche Daten sich die Signatur bezieht (§ 17 Abs. 2 Satz1).

Hinsichtlich der Signaturprüfung lässt Infotech Signer feststellen

- auf welche Daten sich die Signatur bezieht (§ 17 Abs. 2 Nr.1 SigG)
- ob die signierten Daten unverändert sind (§ 17 Abs. 2 Nr.2 SigG)
- welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist (§ 17 Abs.2 Nr.3 SigG)
- welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen (§ 17 Abs. 2 Nr.4 SigG)
- zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs.1 S.3 geführt hat.

Infotech Signer erfüllt die folgenden Anforderungen des § 15 Abs. 2 SigV.

Es ist gewährleistet, dass bei der Erzeugung einer qualifizierten elektronischen Signatur

- die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden (§ 15 Abs. 2 Nr.1a SigV)
- eine Signatur nur durch die berechtigt signierende Person erfolgt (§ 15 Abs. 2 Nr.1b SigV)

- die Erzeugung einer Signatur vorher eindeutig angezeigt wird (§ 15 Abs. 2 Nr.1c SigV).

Es ist ferner gewährleistet, dass bei der Prüfung einer qualifizierten elektronischen Signatur

- die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird (§ 15 Abs.2 Nr.2a SigV)
- eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren (§ 15 Abs.2 Nr. 2b SigV).

3.2 Einsatzbedingungen

Die Erfüllung der vorstehend genannten Anforderungen werden nur in geschützten Einsatzbereichen bei Vorliegen der nachfolgend genannten Voraussetzungen gewährleistet.

3.2.1 Technische Einsatzumgebung

Folgende technische Einsatzumgebung ist auf den Clients vorausgesetzt:

- 32 Bit Betriebssystem Microsoft Windows XP, Vista, 7
- Microsoft Internet Explorer Version 7 oder Version 8
- Mozilla Firefox Version 3.x
- Infotech Program Integrity Checker (PIC)
- Kartenlesegeräte
 - Reiner SCT cyberJack e-com, Version 2.0 (TUVIT.09363.TE.06.2002)
 - Reiner SCT cyberJack pinpad, Version 3.0 (TUVIT.93107.TU.11.2004)
- Signaturkarten
 - D-Trust:
Chipkarte mit Prozessor SLE66CX322P, CardOS V4.3B Re_Cert mit Applikation für digitale Signatur (T-Systems.02182.TE.11. 2006)
 - S-Trust:
ZKA Banking Signature Card, Version 6.6; Giesecke & Devrient GmbH (TUVIT.93130.TU.05.2006)
 - Signtrust:
STARCOS 3.2 QES Version 1.1; Giesecke & Devrient GmbH (BSI.02102.TE.11.2008)
 - TeleSec:
TCOS 3.0 Signature Card, Version 1.1 (NetKey 3.0) or TCOS 3.0 Signature Card, Version 1.1 (NetKey 3.0M) (TUVIT.93146.TE.12.200615)

3.2.2 Einrichtung der Signatur-Station

Der Anwender hat sicherzustellen, dass die Signatur-Stationen nicht kompromittiert, d.h., frei von Viren, Trojanern und sonstigen Schadprogrammen sowie frei von böswilliger äußerer Beeinflussung sind. Unter „Signatur-Station“ werden die Rechner verstanden, auf denen Infotech Signer läuft.

Davon, dass die Signatur-Station nicht kompromittiert ist, hat sich der Anwender

- vor der Installation von Infotech Signer
- nach jeder späteren Inbetriebnahme der Signatur-Station
- regelmäßig während des Betriebes der Signatur-Station

zu überzeugen.

Hierzu hat der Anwender u.a. geeignete Software einzusetzen. Hierzu gehören

- geeignete Virens Scanner mit jeweils aktuellen Signaturen
- Infotech Programm Integrity Checker (Infotech PIC).

Die Virens Scanner sind nicht Teil der Auslieferung von Infotech Signer.

Mit Infotech PIC kann sich der Anwender davon überzeugen, dass die installierte Fachapplikation in dem vom Hersteller vorgesehenen Umfang korrekt installiert vorliegt und nicht verändert wurde.

3.2.3 Betrieb und Nutzung

Der Anwender hat folgendes für den sachgemäßen Betrieb von Infotech Signer zu beachten:

- Die Betriebsanweisungen von Infotech Signer, die mit den Fachapplikationen ausgeliefert werden, sind einzuhalten.
- Die Signaturkarte, das Kartenlesegerät und die Signatur-Station sind gegen unbefugte Benutzung sowie gegen die Beeinflussung signaturrelevanter Daten durch Unbefugte zu sichern.
- Die ordnungsgemäße Funktion der Signatur-Station ist regelmäßig zu überprüfen.
- Bei Benutzung der Signaturkarte ist dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet noch die PIN anderen Personen bekannt wird.
- Die PIN ist regelmäßig zu ändern.

3.2.4 Wartung und Reparatur

Mit der Wartung und Reparatur der Signatur-Station und der darauf installierten Software darf nur vertrauenswürdige Personal beauftragt werden. Der Anwender muß sich hiervon in geeigneter Weise überzeugen, bevor der betreffenden Person der Zugriff auf die Signatur-Station gewährt wird. Ggf. muss er den Wartungs- bzw. Reparaturvorgang selbst beobachten oder durch geeignete sonstige Personen beobachten lassen.

Dem Wartungs- bzw. Reparaturpersonal darf unter keinen Umständen die Signatur-PIN bekanntgemacht werden.

Unmittelbar nach jedem Wartungs- bzw. Reparaturvorgang muß sich der Anwender davon überzeugen, dass

- Infotech Signer nicht verändert wurde
- keine Schadprogramme eingeschleust sind.

Sollte es beim Signaturvorgang zu Fehlfunktionen kommen oder sollte der Anwender sonstige Auffälligkeiten beobachten, ist Infotech Signer gemeinsam mit der Fachapplikation neu zu installieren. Bei fortdauernder Fehlfunktion bietet der Hersteller telefonische Hilfestellung unter 02361-91300 an.

4. Algorithmen und zugehörige Parameter

Zur Erzeugung qualifizierter elektronischer Signaturen werden vom Infotech Signer die Hashfunktionen RIPE-MD 160, SHA-224, SHA-256, SHA-384, SHA-512 bereitgestellt.

Zur Prüfung qualifizierter elektronischer Signaturen werden vom Infotech Signer die Hashfunktionen SHA-1, RIPE-MD 160, SHA-224, SHA-256, SHA-384, SHA-512 sowie das Signaturverfahren nach RSA PKCS#1-v1.5 mit den Schlüssellängen 1024 bis 4096 Bit bereitgestellt

Die gemäß Anlage 1 Abs.1 Nr.2 SigV festgestellte Eignung für die verwendeten kryptographischen Algorithmen sind gemäß den Angaben der Bundesnetzagentur (letzte Veröffentlichung am 04. Februar 2010 im Bundesanzeiger Nr. 19, Seite 426) wie folgt als geeignet eingestuft:

Algorithmus	Schlüssellänge	Gültig bis
RSA	1024	31.3.2008
RSA	1280	Ende 2008
RSA	1536	Ende 2009
RSA	1728	Ende 2010
RSA	1976	Ende 2016
RSA	2048	Ende 2016
SHA1		31.03.2008 (nur zur Prüfung)
RIPEMD160		Ende 2010
SHA224		Ende 2015
SHA256		Ende 2016
SHA384		Ende 2016
SHA512		Ende 2016

Ende der Herstellererklärung