

## Herstellereklärung

Der Hersteller

**PixelPlanet GmbH**

**Schwachhauser Heerstr. 122**

**28209 Bremen**

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG<sup>1</sup>

in Verbindung mit § 15 Abs. 5 SigV<sup>2</sup>,

dass sein Produkt

**WinSigner, Version 2.0**

die Anforderungen des Signaturgesetzes<sup>1</sup> bzw. der Signaturverordnung<sup>2</sup> an eine  
Signaturanwendungskomponente als Teil einer Signaturanwendungskomponente erfüllt.

Bremen, den 20.05.2010

gez. Dirk Carstensen

Dirk Carstensen

---

Geschäftsführung

Diese Herstellereklärung mit der Dokumentennummer PixelPlanet20100220 besteht aus 15 Seiten.

---

<sup>1</sup> Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932)

## Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	20.05.2010	PixelPlanet GmbH	Initialversion

### Hinweis:

Das Produkt „WinSigner, Version 2.0“ stellt eine Weiterentwicklung des Produktes „WinSigner 1.0“ dar. Hierzu sind mit den Dokumentennummern PixelPlanet2008001 und PixelPlanet2008001\_N1 bereits Herstellerklärungen bei der Bundesnetzagentur eingereicht und veröffentlicht.

Zur Wahrung der Übersichtlichkeit werden im Folgenden sämtliche Änderungen bis zum Dokument PixelPlanet2008001 angeführt, so dass nachstehend eine benutzerorientierte, kumulierte Fassung entsteht.

### Zusammenfassende Änderungsübersicht:

Eine Übersicht aller Änderungen gegenüber der Herstellerklärung mit der Dokumentennummer PixelPlanet2008001 stellt sich wie folgt dar:

- Kapitel 1, Handelsbezeichnung und Hersteller:  
Im Rahmen kontinuierlicher Weiterentwicklung hat das Produkt „WinSigner“ inzwischen die Version 2.0 erreicht.
- Kapitel 2, Lieferumfang und Versionsinformationen:  
Ebenfalls begründet durch die stetige Weiterentwicklung beschränken sich die Änderungen auf die Aktualisierung der Versionsnummern und Anpassung der Konfigurationsliste. Aufgrund einer neu unterstützten Signaturkarte, ist in der vorliegenden Fassung die Liste zusätzlicher, nach SigG bestätigter Produkte ergänzt worden. Detaillierte Informationen Tabelle 3.
- Kapitel 3, Funktionsbeschreibung:  
Ergänzend zum bisherigen Funktionsumfang, unterstützt die aktuelle Version 2.0 des Produktes „WinSigner“ neben einer zuvor festgelegten Anzahl von Signaturen nun auch die Erzeugung von Signaturen innerhalb eines geeigneten, zuvor festgelegten Zeitraumes.
- Kapitel 4, Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung:  
Um den erweiterten Anforderungen hinsichtlich schwachwerdender und nicht implementierten Algorithmen sowie qualifizierten elektronischen Zeitstempeln künftig vollumfassend zu entsprechen, hat die Software „WinSigner“ hinsichtlich ihres Prüfberichts in Version 2.0 einige Änderungen erhalten.
- Kapitel 5, Maßnahmen der Einsatzumgebung:  
Aus Gründen der Übersicht erfolgt eine vollständige Wiedergabe samt Präzisierung für die Nutzung von Stapelsignaturen, basierend auf Zeitfenstern.
- Kapitel 6, Algorithmen und zugehörige Parameter:  
Zur Wahrung der Übersichtlichkeit wird das Kapitel vollständig wiedergegeben.

- Kapitel 7, Gültigkeit der Herstellerklärung:  
Zur Wahrung der Übersichtlichkeit wird das Kapitel vollständig wiedergegeben.

## Beschreibung des Produkts

### 1. Handelsbezeichnung und Hersteller

Die Handelsbezeichnung lautet: WinSigner, Version 2.0  
 Auslieferung: online oder per CD-ROM  
 Hersteller: PixelPlanet GmbH, Schwachhauser Heerstraße 122, 28209 Bremen  
 Handelsregisterauszug: HRB 21447, Amtsgericht Bremen

### 2. Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

**Tabelle 1: Lieferumfang der Software „WinSigner, Version 2.0“**

Produktart	Bezeichnung	Version	Datum	Übergabeform
Software	WinSigner (SHA-256: be8f853247bdd082bcad7bed bfc736c83a89707359d257be 7af58b020608017c)	2.0	20.05.2010	per Download oder alternativ auf CD-ROM
Handbuch	Dokumentation	2.0	20.05.2010	per Download oder alternativ auf CD-ROM

Die Software „WinSigner, Version 2.0“ besteht aus den in der folgenden Tabelle aufgeführten Dateien:

**Tabelle 2: Auflistung der Dateien**

Bibliothek	Beschreibung	Version
WinSigner.exe	Ausführungsdatei, Hauptanwendung	2.0
WinSignerCore.dll	Core-Objekt	2.0
PPpkcs11.dll	Kartenansteuerung	2.0
Elevation.dll	Windows Vista Elevation	1.0
PdfView.wlx	Pdf-Anzeige Plugin	1.0
TiffView.wlx	Tiff-Anzeige Plugin	1.0
WinSignerOutlookAddin.dll	Outlook Addin	2.0
WinSignerShellExt.dll	Windows Explorer Addin	2.0
WinSigner.chm	Programmhilfe	2.0

Das Produkt „WinSigner, Version 2.0“ nutzt die folgenden nach SigG bestätigten Produkte, die von Dritten hergestellt werden und nicht Bestandteil dieser Erklärung sind (z.B. Kartenleser oder sichere Signaturerstellungseinheit (SSEE)):

**Tabelle 3: Zusätzliche Produkte**

Produkt-klasse	Bezeichnung, Hersteller	Registriernummer der Bestätigung
SSEE	TCOS 3.0 Signature Card, Version 1.0 der Firma T-Systems Enterprises GmbH	TUVIT.93119.TE.09.2006
SSSE	„Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“ der Firma Siemens AG	T-Systems.02122.TE.05.2005
SSEE	ZKA Banking Signature Card, Version 6.31 NP, Type 3 der Firma Giesecke & Devrient GmbH	TUVIT.09397.TU.03.2005
SSEE	ZKA Banking Signature Card, Version 6.32 NP, Type 3 der Firma Giesecke & Devrient GmbH	TUVIT.93125.TU.12.2005
SSEE	ZKA Banking Signature Card, Version 6.6 der Firma Giesecke & Devrient GmbH	TUVIT.93130.TU.05.2006
SSEE	STARCOS 3.0 with Electronic Signature Application V3.0 der Firma Giesecke & Devrient GmbH	TUVIT.93100.TE.09.2005
SSEE	STARCOS 3.2 QES, Version 2.04 der Firma Giesecke & Devrient GmbH	BSI.02114.TE.12.2008
Kartenleser	KAAN Professional und B1 Professional, Firma KOBIL Systems GmbH	TUVIT.09331.TE.03.2002
Kartenleser	SmartBoard ST-2xxx, Firma Cherry GmbH	BSI.02059.TE.02.2006
Kartenleser	CardMan Trust CM3621 / CM3821, Firma OMNIKEY GmbH	BSI.02057.TE.12.2005
Kartenleser	CyberJack® pinpad, Version 3.0 der Firma Reiner Kartengeräte GmbH & Co KG	TUVIT.93107.TU.11.2004
Kartenleser	CyberJack® e-com, Version 2.0 der Firma Reiner Kartengeräte GmbH & Co KG	TUVIT.09363.TE.06.2002
Kartenleser	SPR 132, SPR 332, SPR 532 der Firma SCM Microsystems GmbH	TUVIT.09370.TE.03.2003

### 3. Funktionsbeschreibung

Die Software „WinSigner“ ist Teil einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG; die auf geeigneter Hardware mit geeigneten Betriebsmitteln – insbesondere mit SigG-konformen Chipkartenlesern und sicheren Signaturerstellungseinheiten (in diesen Fall Signaturkarten) in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ (vgl. „Einheitliche Spezifizierung der Einsatzkomponenten für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen“, Version 1.4, 19.07.2005) betrieben und über eine Oberfläche (Graphical User Interface – GUI) von einem Nutzer konfiguriert und genutzt wird. Die Software ‚WinSigner‘ kann im privaten, privatwirtschaftlichem oder behördlichem Umfeld auf einem handelsüblichen Rechner betrieben werden.

Die Software „WinSigner“ erfüllt alle Anforderungen gemäß § 17 Abs. 2 SigG, umfasst allerdings keine Chipkartenleser oder sichere Signaturerstellungseinheiten.

#### **Beschreibung des Signaturproduktes**

Die Software „WinSigner“ stellt Funktionen zur Erzeugung und zur Prüfung qualifizierter elektronischer Signaturen zur Verfügung:

- Die Software „WinSigner“ unterstützt den Signaturschlüssel-Inhaber bei der Erzeugung von qualifizierten elektronischen Signaturen, die lokal von einer sicheren Signaturerstellungseinheit erzeugt werden.

Voraussetzung hierfür ist, dass der Signaturschlüssel-Inhaber an seinem Arbeitsplatz unmittelbar zur Signaturerzeugung Zugriff auf seine Signaturkarte und den Chipkartenleser hat.

Signaturgegenstand können Dokumente des Eingangsformates Portable Document Format (PDF) oder sämtliche anderen Dateiformate sein. Für PDF-Dokumente wird die Signatur in die Datei integriert, für alle anderen Formate wird eine Datei mit der Dateierdung ‚.pkcs7‘ als externe Signaturdatei oder mit eingebettetem Dokumentinhalt erzeugt.

Zum Signieren steckt der Nutzer seine Signaturkarte in den Chipkartenleser, betätigt den Signier-Button – woraufhin die zu signierenden Daten der sicheren Signaturerstellungseinheit zugeführt werden, in der sein privater Signaturschlüssel vorgehalten wird – und autorisiert das Signieren durch Eingabe seiner PIN am PIN-Pad des Kartenlesegeräts.

Sofern die eingesetzten Signaturkarten die Erzeugung mehrerer Signaturen mit einer einzigen PIN-Eingabe unterstützen, kann die Software für einen definierten Stapel von Dokumenten Signaturen erzeugen lassen.

Die Erzeugung von Stapelsignaturen unterstützt die Software „WinSigner“ in folgender Weise:

- Der Nutzer kann einen Stapel von Dokumenten definieren und die Erzeugung von qualifizierten elektronischen Signaturen für diesen definierten Stapel von Dokumenten autorisieren.
- Dem Signaturschlüssel-Inhaber wird eindeutig angezeigt, dass eine solche Stapelsignatur erzeugt wird (Warnhinweis vor der Erzeugung).
- Der Signaturschlüssel-Inhaber kann sich dabei jedes Dokument dieses Stapels ansehen.
- Die Software „WinSigner“ lässt die Konfiguration eines maximalen Stapels zu, der die maximal zu signierenden Dateien definiert.

- Die Begrenzung kann durch vorheriges Festlegen einer bestimmten Anzahl von Signaturen oder der Dauer eines Zeitfensters zur Signaturerstellung, welches maximal 8 Stunden beträgt, erfolgen. Die Signatur-Sitzung wird dabei automatisch geschlossen, sobald eine der beiden Begrenzungen (Anzahl oder Zeit) tangiert wird.
- Es erfolgt keine Zwischenspeicherung der PIN (kein PIN-Caching).
- Bei dieser Stapelsignatur handelt es sich um eine sogenannte „Lokalsignatur“ (vgl. dazu FAQ 18a der Bundesnetzagentur), bei der Signaturschlüssel-Inhaber die Signaturkarte an seinem Arbeitsplatz nutzt.

Es findet kein automatisierter Prozess statt, der nach Eingabe der PIN diese für das System vorhält, zum Signieren automatisch abrufen und an die SSEE sendet.

- Die Software „WinSigner“ führt für qualifizierte elektronische Signaturen eine Signaturprüfung (Verifikation) sowie die Zertifikatsprüfung (Validierung) durch.

Für die Zertifikatskettenbildung ist ein Schlüssel-/Zertifikatsmanagement enthalten, in dem die vertrauenswürdigen Zertifikate abgelegt sind. Weiterhin ist ein Zugriff auf den Windows-Zertifikatsspeicher durch den Benutzer einstellbar. Für die Online-Validierung greift die Software auf Verzeichnisdienste zu.

Die Software „WinSigner“

- prüft lokal die mathematische Korrektheit der qualifizierten elektronischen Signatur des Absenders (Verifikation) und
- validiert online das Zertifikat (Validierung).

Die Software „WinSigner“ unterstützt für die Zertifikatsprüfung als Gültigkeitsmodell das Kettenmodell. Daneben sind als weitere Gültigkeitsmodelle das Schalen- sowie das Hybridmodell durch den Benutzer einstellbar, als nicht SigG/SigV-konforme Gültigkeitsmodelle jedoch nicht in dieser Dokumentation beschrieben.

Das Ergebnis der Prüfung wird dem Benutzer in einem Fenster der Software angezeigt. Zusätzlich wird ein Prüfbericht als PDF-Dokument erzeugt, in dieser Datei wird auch das jeweilige Gültigkeitsmodell angezeigt. Insbesondere umfasst das Ergebnis der Prüfung:

- Prüfungsergebnis: Zeigt an, ob die Signatur gültig ist.
- Integritätsprüfung: Zeigt an, ob das Dokument seit Aufbringung der Signatur verändert wurde.
- Zertifikatskettenprüfung: Zeigt an, ob die Kette der übergeordneten Zertifikate gültig (d.h. vorhanden und nicht gesperrt) ist.
- Online-Sperrprüfung: Zeigt an, ob das Signaturzertifikat zum Zeitpunkt der Signatur gültig (d.h. vorhanden und nicht gesperrt) war.

Dem Benutzer wird der Dateiname sowie der Speicherort des zu prüfenden Dokumentes angezeigt; zudem kann sich der Benutzer über den „Ansicht“-Button das Dokument anzeigen lassen. Des Weiteren lässt sich das verwendete Signaturzertifikat anzeigen, aus dem insbesondere der Signaturschlüssel-Inhaber hervorgeht.

Prüfgegenstand können Dokumente des Eingangsformates Portable Document Format (PDF) oder sämtliche anderen Dateiformate sein. Die Signaturprüfung kann dabei auch für den Fall erfolgen, dass die Signaturerzeugung in Form einer angehängten Signaturdatei mit der Dateiendung ‚.pkcs7‘ erfolgt ist. Sofern es sich bei dem Prüfgegenstand um das signierte Dokument handelt, wird dann die angehängte Signaturdatei,

anderenfalls das signierte Dokument während der Signaturprüfung ermittelt. Die Software kann sowohl ein einzelnes Dokument wie auch einen definierten Stapel von Dokumenten prüfen.

- Während der Erzeugung qualifizierter elektronischer Signaturen können qualifizierte Zeitstempel angebracht, während der Signatur- und Zertifikatsprüfung von qualifizierten elektronischen Signaturen können qualifizierte Zeitstempel geprüft werden. Für die Anforderung qualifizierter Zeitstempel im Rahmen der Signaturerzeugung sind dabei Zeitstempelservers von entsprechenden Anbietern vorkonfiguriert und aktivierbar.
- Die Software „WinSigner“ interagiert in einem Assistentenmodus mit dem Benutzer und begleitet ihn durch den Signatur- und Prüfprozess. Nach dem Start der Software wird der Benutzer in einer festen Abfolge über mehrere Programmfenster von der Erstellung bis zur Durchführung des Signatur- oder Prüfauftrages geleitet. Der Start der Software kann neben einem direkten Aufruf über das Startmenü auch durch das Windows Explorer Kontextmenu, Dateiverknüpfung, Microsoft Outlook oder über den mitgelieferten PDF Drucker erfolgen.
- Die Software „WinSigner“ beinhaltet Funktionen für die Dokument- und Zertifikatsansicht.

Der Benutzer kann sich jedes Dokument anzeigen lassen – auch bei einem definierten Stapel von zu signierenden bzw. zu prüfenden Dokumenten. Für die Betrachtung von Dokumentinhalten der Datenformate Text, Bild (insbesondere TIFF) und PDF steht eine integrierte Dokumentansicht („Sichere Anzeige“) zur Verfügung. Innerhalb der ‚Sicheren Anzeige‘ werden kritische Dokumentinhalte (z.B. JavaScript) erkannt und angezeigt. Bei nicht über die ‚Sichere Anzeige‘ dargestellten Dokumenten enthalten sowohl die Applikation als auch das Benutzerhandbuch und die Online-Hilfe der Software „WinSigner“ entsprechende Hinweise zur Darstellungsproblematik – insb. von Word-Dokumenten –, dass sich der Benutzer durch einen entsprechenden Betrachter davon zu überzeugen hat, dass er exakt das signiert, was er signieren möchte, und bei der Prüfung alle Inhalte hat sehen können. Unabhängig von der Art der Anzeige wird zunächst durch Abgleich der Hashwerte gewährleistet, dass ausgewähltes und dargestelltes Dokument übereinstimmen.

Die Zertifikatsansicht erfolgt ausschließlich über das programminterne Anzeigemodul. Sofern die entsprechenden Informationen verfügbar sind, umfasst die Darstellung – neben dem ausgewählten Zertifikat bei der Signaturerzeugung bzw. dem für die Dokumentunterschrift verwendeten Zertifikat bei der Signaturprüfung – die Zertifikatskette sowie Attributzertifikate.

- Die Software „WinSigner“ verfügt zum Schutz vor Manipulation über Selbstprüfungsmechanismen und die Möglichkeit einer manuellen Prüfung.

#### 4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt „WinSigner, Version 2.0“ erfüllt die nachfolgenden Anforderungen des SigG:

**Tabelle 4: Erfüllung der Anforderungen des SigG**

Referenz	Gesetzestext	Beschreibung
§ 17 Abs. 2 Satz 1	Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die	Zur Umsetzung dieser gesetzlichen Anforderungen ist in der Software „WinSigner“ eine entsprechende Anzeige implementiert.

Referenz	Gesetzestext	Beschreibung
	Signatur bezieht.	
§ 17 Abs. 2 Satz 2	<p>Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,</p> <ol style="list-style-type: none"> <li>1. auf welche Daten sich die Signatur bezieht,</li> <li>2. ob die signierten Daten unverändert sind,</li> <li>3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,</li> <li>4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und</li> <li>5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat.</li> </ol>	Zur Umsetzung dieser gesetzlichen Anforderungen ist in der Software „WinSigner“ eine entsprechende Anzeige implementiert.
§ 17 Abs. 2 Satz 3	Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.	Zur Umsetzung dieser gesetzlichen Anforderungen ist in der Software „WinSigner“ eine entsprechende Anzeige implementiert.

Das Produkt „WinSigner, Version 2.0“ erfüllt die nachfolgenden Anforderungen der SigV:

**Tabelle 5: Erfüllung der Anforderungen der SigV**

Referenz	Gesetzestext	Beschreibung
§ 15 Abs. 2 Nr. 1	<p>Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Erzeugung einer qualifizierten elektronischen Signatur</p> <ol style="list-style-type: none"> <li>a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,</li> <li>b) eine Signatur nur durch die berechtigt</li> </ol>	<p>Zur Umsetzung dieser Anforderungen ist in der Software „WinSigner“ implementiert,</p> <ul style="list-style-type: none"> <li>• dass die Signaturerzeugung auf einer sicheren Signaturerstellungseinheit erfolgt, die über einen Chipkartenleser angesprochen wird,</li> <li>• dass die PIN-Eingabe ausschließlich über Chipkartenleser erfolgt – damit werden die Identifikationsdaten nicht in der Software „WinSigner“ verarbeitet –,</li> <li>• dass die Erzeugung einer Signatur</li> </ul>

Referenz	Gesetzestext	Beschreibung
	<p>signierende Person erfolgt,</p> <p>c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird [...].</p>	<p>vorher eindeutig angezeigt wird, wobei die Erzeugung einer Stapelsignatur als solche gekennzeichnet wird,</p>
§ 15 Abs. 2 Nr. 2	<p>Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass [...] bei der Prüfung einer qualifizierten elektronischen Signatur</p> <p>a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und</p> <p>b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.</p>	<p>Zur Umsetzung dieser Anforderungen ist in der Software „WinSigner“ implementiert,</p> <ul style="list-style-type: none"> <li>• dass die Verifikation der Signatur (lokale mathematische Prüfung) und</li> <li>• dass die Validierung des Zertifikats (online Überprüfung, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren) korrekt ausgeführt und zutreffend angezeigt werden.</li> </ul>
§ 15 Abs. 4	<p>Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.</p>	<p>Die Anforderungen zur Erkennung sicherheitstechnischer Veränderungen werden durch die Auflagen zum Betrieb sowie die im Produkt „WinSigner, Version 2.0“ implementierten Selbstprüfungsmechanismen und manuellen Prüfmöglichkeiten realisiert.</p>

Seitens der Bundesnetzagentur wurden jedoch die Anforderungen an Signaturanwendungskomponenten in Bezug des Umgangs mit schwachwerdenden Algorithmen und qualifizierten Zeitstempeln weiter präzisiert. Signaturanwendungskomponenten i. S. v. § 2 Nr. 11 b SigG müssen demnach auch dann eine zuverlässige Prüfung und zutreffende Anzeige des Ergebnisses gem. § 15 Abs. 2 Nr. 2a SigV gewährleisten, wenn die geprüfte Signatur auf einem Algorithmus oder Parameter beruht, der als nicht mehr geeignet und damit als nicht mehr hinreichend zuverlässig eingestuft ist, oder wenn ein qualifizierter Zeitstempel vorliegt.

In Tabelle 6 wird nachstehend dargelegt, inwiefern die Software „WinSigner, Version 2.0“ aktuell die Anforderungen erfüllt:

**Tabelle 6: Erfüllung und Verhalten der Software WinSigner, Version 2.0 hinsichtlich erweiterter Anforderungen an Signaturanwendungskomponenten**

Anforderung	Erfüllung und Verhalten der Software „WinSigner, Version 2.0“
<p>a) Abgelaufene Algorithmen:</p> <p>Die Prüfung einer Signatur durch eine</p>	<p>Das Produkt „WinSigner, Version 2.0“ informiert den Benutzer bei der Verifikation von Signaturen deren</p>

<p>Signaturanwendungskomponente (SAK) für qualifizierte elektronische Signaturen i.S.v. § 2 Nr. 11b SigG muss bei abgelaufenen Algorithmen für den Nutzer deutlich anzeigen, dass die geprüfte Signatur mit einem Algorithmus erzeugt wurde, der nicht mehr dem Stand der Wissenschaft und Technik entspricht, und sie somit einen verminderten Beweiswert hinsichtlich der Authentizität und Integrität des verbundenen Dokuments gegenüber dem Signaturzeitpunkt besitzt. Weiter sollte der Zeitpunkt, zu dem der Algorithmus seine Eignung verloren hat, zutreffend angezeigt werden.</p> <p>Unspezifische Aussagen zu abgelaufene Algorithmen sind nicht zulässig.</p>	<p>Algorithmen nicht mehr dem Stand der Wissenschaft und Technik entsprechen darüber, dass die Signatur einschließlich ihrer verbundenen Daten einen verminderten Beweiswert hinsichtlich Authentizität und Integrität gegenüber dem Signaturzeitpunkt besitzt. Des Weiteren wird dem Benutzer der Zeitpunkt, zu dem der Algorithmus seine Eignung verloren hat, zutreffend angezeigt.</p>
<p>b) Nicht implementierte Algorithmen:</p> <p>Ist bei der Prüfung einer Signatur ein Algorithmus zu verwenden, der in der Verifikationskomponente der SAK nicht implementiert ist, so muss dies dem Nutzer zutreffend angezeigt werden.</p> <p>Unspezifische Aussagen zu nicht implementierten Algorithmen sind nicht zulässig.</p>	<p>Dem Benutzer wird unter Angabe des entsprechenden Algorithmus zutreffend angezeigt, dass die Signatur, mangels nicht implementierten Algorithmus, nicht geprüft werden konnte.</p>
<p>c) Qualifizierte Zeitstempel:</p> <p>Tragen Daten einer qualifizierten Signatur, bei deren Verifikation zu erkennen ist, dass der Signaturprüfchlüssel zu einem Zeitstempel-Zertifikat gehört, so ist dies dem Nutzer zutreffend anzuzeigen. Der Zeitpunkt, der im qualifizierten Zeitstempel enthalten ist, ist dem Nutzer ebenfalls darzulegen.</p> <p>Solange kein standardisiertes Verfahren für die Einbindung von qualifizierten Zeitstempeln existiert, ist es ausreichend, wenn das Produkt seine selbst integrierten qualifizierten Zeitstempel auswerten kann. Qualifizierte Zeitstempel, die aus Fremdprodukten und damit in einer ev. proprietären Datenstruktur vorliegen, müssen nicht zwingend durch das Produkt ausgewertet werden.</p> <p>Unspezifische Aussagen zu qualifizierten Zeitstempeln sind nicht zulässig.</p>	<p>Das Produkt „WinSigner, Version 2.0“ kann selbst integrierte qualifizierte Zeitstempel korrekt auswerten.</p> <p>Der enthaltene Zeitpunkt wird dem Benutzer hierbei zutreffend angezeigt.</p>

## 5. Maßnahmen in der Einsatzumgebung

### 5.1 Einrichtung der IT-Komponenten

Für den Betrieb der Software „WinSigner, Version 2.0“ wird folgende Einsatzumgebung vorausgesetzt:

- Personal Computer: Die folgenden Mindestvoraussetzungen müssen erfüllt sein, um WinSigner einzusetzen:
  - IBM-kompatibler Personalcomputer ab Pentium 2 (Empfehlung: Pentium 4 / 2 GHz)
  - mindestens 128 Megabyte Arbeitsspeicher (RAM)
  - mindestens 50 Megabyte freier Festplattenspeicher - abhängig vom Speicherort der zu signierenden und signierten Daten
  - CD-ROM-Laufwerk für die Installation
- Betriebssystem: Als Betriebssystem können verwendet werden:
  - Windows NT4.0 SP 6a
  - Windows 2000 SP4
  - Windows XP Home Edition SP2 und Windows XP Professional Edition SP2
  - Windows Vista
  - Windows 7
- Chipkartenlesegeräte: Für die Gewährleistung der sicheren PIN-Eingabe muss einer der in Tabelle 3 aufgeführten, durch die Bundesnetzagentur bestätigten und im Einsatz mit der Software „WinSigner“ erfolgreich getesteten Chipkartenleser verwendet werden.
- Sichere Signaturerstellungseinheiten (SSEE): Es muss eine der in Tabelle 3 aufgeführten, von einem ZDA ausgegebenen, durch die Bundesnetzagentur bestätigten und im Einsatz mit der Software „WinSigner“ erfolgreich getesteten Sicheren Signaturerstellungseinheiten (SSEE) verwendet werden.
- Internet: Für die Durchführung einer Signaturprüfung muss eine Netzverbindung bestehen, um einen Zugriff auf den OCSP-/CRL- bzw. auf den LDAP-Verzeichnisdienst des Trustcenters zu gewährleisten.

Weiterhin wird der Einsatz der nachfolgend aufgelisteten Software empfohlen:

- MSOutlook 2000 bis 2007 für WinSigner Outlook-Integration

Das Produkt „WinSigner, Version 2.0“ darf ausschließlich innerhalb der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden.

### 5.2 Anbindung an ein Netzwerk

Der Rechner ist durch entsprechende Software vor Angriffen aus öffentlichen Netzwerken und vor Angriffen durch schädliche Software zu schützen. „WinSigner, Version 2.0“ muss in einer geschützten Einsatzumgebung ausgeführt werden: Sofern der Computer, auf dem eine Signatur oder Signaturprüfung erfolgen soll, mit dem Internet oder einem Intranet verbunden ist, muss sowohl eine intakte und aktualisierte Firewall als auch ein intakter und aktualisierter Virenschanner installiert und aktiv sein.

### 5.3 Auslieferung und Installation

Die Auslieferung des auf den Microsoft Installer basierenden, mit InstallShield erzeugten Installationspakets (Setup-Datei) für die Signaturanwendungskomponente „WinSigner“ erfolgt per Datenträger (Original-CD-Rom) oder Download der Software von der firmeneigenen Produktseite <http://www.winsigner.de>.

Sämtliche Setups der Software sind bei Auslieferung mit einer elektronischen Signatur versehen (Code Signing). Die Installation darf nur erfolgen, sofern sich das Setup auf einem Originaldatenträger befindet oder von der firmeneigenen Produktseite heruntergeladen wurde. Bei Installation vom Originaldatenträger ist die ausgelieferte CD vor Installation der Software auf Unversehrtheit zu überprüfen. Unabhängig von der Art der Auslieferung ist weiterhin aus Sicherheitsgründen das Setup auf Authentizität und Integrität zu prüfen.

Um die Authentizität und Integrität der Setup-Datei zu prüfen, kann über die Ansicht der Eigenschaften der Setup-Datei die elektronische Signatur eingesehen werden. Fingerabdruck und öffentlicher Schlüssel des Zertifikates, mit dem die elektronische Signatur der Datei erstellt wurde, sind dann mit den auf der Produktseite der Software unter <http://www.winsigner.de> veröffentlichten Daten zu vergleichen. Eine genaue Anleitung zur Prüfung befindet sich im Handbuch oder auf der Produktseite.

Das für das Code Signing verwendete Zertifikat der PixelPlanet GmbH ist von der Firma GlobalSign ausgestellt, vgl. <http://globalsign.de>. GlobalSign ist ein Zertifizierungsdiensteanbieter (TrustCenter) und vergibt ausschließlich Zertifikate, die der EU-Richtlinie für die digitale Signatur entsprechen.

Vor der Installation der Software sowie im laufenden Betrieb ist sicherzustellen, dass die Sicherheit des Rechners und des installierten Betriebssystems nicht kompromittiert ist bzw. wird. Das auf dem Rechner installierte Betriebssystem ist bzgl. verfügbarer Sicherheits-Patches und Updates auf dem aktuellsten Stand zu halten.

Weitere Voraussetzung für die Installation ist, dass die nachfolgend aufgeführten Auflagen für die Gegebenheiten der Einsatzumgebung und des Einsatzbereiches erfüllt sind. Für die Installation der Software sind Administratorenrechte erforderlich. Weiterführende Informationen bezüglich der Installation können dem Handbuch entnommen werden.

Im Anschluss an die Installation ist die Integrität der Bibliotheks- (.DLL) und Anwendungsdateien (.EXE) im Installationsverzeichnis der Software „WinSigner, Version 2.0“ zu überprüfen. Diese Dateien sind ebenfalls mit einer elektronischen Signatur versehen. Die Prüfung erfolgt analog zur Beschreibung in diesem Abschnitt.

Updates für die Signaturanwendungskomponente sind möglich. Neue Versionen stehen – wie zuvor beschrieben – ausschließlich über einen Download von den Produktseiten des Herstellers zur Verfügung. Die Durchführung von Updates darf weiterhin nur über die entsprechende programminterne Funktion erfolgen.

### 5.4 Auflagen für den Betrieb des Produktes

Die Software „WinSigner, Version 2.0“ wird in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“ (vgl. „Einheitliche Spezifizierung der Einsatzkomponenten für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen“, Version 1.4, 19.07.2005) betrieben.

Es wird vorausgesetzt, dass nur autorisierte Personen Zugriff auf den Rechner haben, auf dem der WinSigner betrieben wird.

Der Zugang zum Client muss restriktiv organisiert werden, so dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird.

Es ist sicherzustellen, dass die verwendeten Freigaben/Ordner und zu signierenden Daten nur unter der Kontrolle von autorisierten Personen liegen.

Die Eingabe der PIN am Kartenlesegerät darf nur durch den Zertifikatinhaber erfolgen. Bei PIN-Eingabe ist sicherzustellen, dass dieser weder visuell noch mechanisch oder elektronisch ausgelesen werden kann.

Beim Verlassen des Computerstandortes durch den Anwender muss sichergestellt sein, dass der Computer vor einem Zugriff Dritter geschützt ist.

Der Bildschirmschoner mit Passwort-Eingabe zur Deaktivierung muss aktiviert sein, mit Sperrung nach maximal 5 Minuten.

Die PIN für die zu verwendende Signaturkarte muss für Dritte unzugänglich aufbewahrt werden.

Es wird vorausgesetzt, dass sämtliche Datenträger vor dem Auslesen von Daten mit geeigneter Sicherheitssoftware (z.B. AntiVirus, AntiSpy) auf schädliche Software überprüft werden.

Im laufenden Betrieb ist sicherzustellen, dass die Sicherheit des Rechners und des installierten Betriebssystems nicht kompromittiert ist bzw. wird. Das auf dem Rechner installierte Betriebssystem ist bzgl. verfügbarer Sicherheits-Patches und Updates auf dem aktuellsten Stand zu halten.

Es ist sicherzustellen, dass einer der in Tabelle 3 dieser Dokumentation aufgeführten, durch die Bundesnetzagentur bestätigten und im Einsatz mit der Software ‚WinSigner, Version 2.0‘ erfolgreich getesteten Chipkartenleser verwendet wird.

Es ist sicherzustellen, dass eine der in Tabelle 3 dieser Dokumentation aufgeführten, von einem ZDA ausgegebenen, durch die Bundesnetzagentur bestätigten und im Einsatz mit der Software „WinSigner, Version 2.0“ erfolgreich getesteten Sicheren Signaturerstellungseinheiten (SSEE) verwendet wird.

Für die Durchführung einer Signaturprüfung muss eine Netzverbindung bestehen, um einen Zugriff auf den OCSP-/ CRL- bzw. auf den LDAP-Verzeichnisdienst des Trustcenters zu gewährleisten.

Es ist die korrekte Systemzeit einzustellen.

Zum Schutz vor Manipulation der Software verfügt die Signaturanwendungskomponente „WinSigner, Version 2.0“ über Selbstprüfungsmechanismen entsprechend § 15 Abs. 4 SigV und die Möglichkeit einer manuellen Prüfung. Die Software „WinSigner, Version 2.0“ besteht aus mehreren Programmbestandteilen in Form von Bibliotheks- (.DLL) und Anwendungsdateien (.EXE) im Installationsverzeichnis. Diese Programmbestandteile von „WinSigner, Version 2.0“ sind mit einer elektronischen Signatur versehen. Die Signaturen werden bei jedem Programmstart selbständig mit der Microsoft Authenticode-Technologie verifiziert. Dafür werden die in der Signatur enthaltenen Daten für den Fingerabdruck des verwendeten Zertifikats mit den entsprechenden Daten des Herstellers verglichen und geprüft, ob die Identität des Herstellers mit der Signatur übereinstimmt. Eine nicht erfolgreich durchgeführte Selbstprüfung wird dem Anwender bei Programmstart eindeutig angezeigt und die weitere Programmausführung unterbunden. Voraussetzung für die Selbstprüfung ist, dass der Überprüfungsmechanismus nicht manipuliert wurde. Um eine manuelle Prüfung durchzuführen, sind die Programmbestandteile einer Prüfung gemäß der Erläuterung in Abschnitt 2.4.2 zu unterziehen. Im Falle einer Manipulation ist die Software „WinSigner, Version 2.0“ zu deinstallieren und der Rechner auf Viren und Trojaner zu prüfen. Im Anschluss ist „WinSigner, Version 2.0“ neu von dem Originaldatenträger (CD-ROM) oder den per Download geladenen Originalprogrammdateien zur Installation der Signaturanwendungskomponente gem. Abschnitt 2.4.2 zu installieren.

## **6. Algorithmen und zugehörige Parameter**

Die folgenden kryptographischen Verfahren werden von der Software „WinSigner“ eingesetzt:

- Hashfunktionen:
  - RIPEMD-160; gültig bis 31.12.2010
  - SHA-2 Familie (SHA-224, SHA-256, SHA-384, SHA-512); gültig bis 31.12.2015
- Verifikationsalgorithmus:
  - RSA mit Schlüssellängen von 2048 Bit und PKCS#1-Padding; gültig bis 31.12.2015.

Die gemäß Anlage I Abs. 1 Nr. 2 SigV festgelegte Eignung reicht mindestens bis zum 31.12.2010 (vgl. „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“ der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn 17. November 2008, veröffentlicht am 27. Januar 2009 im Bundesanzeiger Nr. 13, S. 343.

## **7. Gültigkeit der Herstellererklärung**

Diese Herstellererklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2010 (aufgrund der Gültigkeit der eingesetzten kryptographischen Verfahren) gültig. Der aktuelle Status der Gültigkeit der Erklärung ist bei der zuständigen Behörde (Bundesnetzagentur, Referat Elektronische Signatur) zu erfragen.

## **8. Zusatzdokumentation**

- PixelPlanet GmbH, „Unterlagen zur Herstellererklärung gemäß § 17 Abs. 4 SigG für die Software , WinSigner, Version 2.0' – Sicherheitstechnische Produktbeschreibung und Spezifikation“, Dokumentenversion 1.0, Stand 20.05.2010, 16 Seiten
- PixelPlanet GmbH, „Unterlagen zur Herstellererklärung gemäß § 17 Abs. 4 SigG für die Software, WinSigner, Version 2.0' – Testdokumentation“, Dokumentenversion 1.0, Stand 20.05.2010, 11 Seiten
- PixelPlanet GmbH, „Benutzerhandbuch“, Dokumentenversion 1.0, Stand 20.05.2010, 93 Seiten

**Ende des Nachtrages**