

Herstellereklärung



Die

Dictao Deutschland GmbH

c/o Taylor Wessing - Senckenberganlage 20-22 – 60325 Frankfurt am Main

erklärt hiermit gemäß § 17 Abs. 4 Satz 2 SigG ¹

in Verbindung mit § 15 Abs. 5 Satz 1 SigV ²,

dass sein Produkt

Dictao Signature & Validation Server (DxS)

Qualifizierte Elektronische Signatur – v4.8

Teil einer Signaturanwendungskomponente

die nachstehend genannten Anforderungen des SigG und der SigV erfüllt.

Frankfurt am Main, den 01.09.2010

gez. FLORENT LATOUR

Geschäftsführer

Diese Herstellereklärung in Version 1.0 mit der Dokumentennummer Dictao_DE_2010_01 besteht aus 14 Seiten.

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 17.12.2009 (BGBl. I S. 3932) § 17 Abs. 4 Satz 2 SigG1

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	01.09.2010	Christian KUHN	Endfassung

1. Handelsbezeichnung

Die Handelsbezeichnung lautet:

Teil-Signaturanwendungskomponente
Dictao Signature & Validation Server (DxS)
Qualifizierte Elektronische Signatur – v4.8³

Auslieferung:

Die Auslieferung durch den Hersteller erfolgt auf CD und per Download.

Hersteller:

Dictao Deutschland GmbH
c/o Taylor Wessing - Senckenberganlage 20-22 – 60325 Frankfurt am Main

Handelsregisterauszug: HRB 88222

³ Das Produkt „Dictao Signature & Validation Server Qualifizierte Elektronische Signatur – v4.8“, wird im Folgenden auch als „**DxS v4.8**“ verkürzt bezeichnet.

2. Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

Produktart	Bezeichnung	Version	Datum	Übergabeform
Software	Dictao Signature & Validation Server (DxS)	4.8	26.08.2010	Installationsfiles auf CD oder per Download
Handbuch	Dictao Signature & Validation Server (DxS) Anwenderdokumentation	1.3	21.07.2010	PDF-Datei auf CD oder per Download
Handbuch	Dictao Signature & Validation Server (DxS) Administrationshandbuch	9.7	26.08.2010	PDF-Datei auf CD oder per Download
Hashwert	Hash.txt		26.08.2010	Textdatei, separat über-mittelt, z.B. per E-Mail.

Tabelle 1: Lieferumfang und Versionsinformationen

Das Produkt **DxS v4.8** nutzt bzw. enthält die folgenden nach SigG bestätigten Produkte, die nicht Bestandteil dieser Erklärung sind:

Produktklasse	Bezeichnung	Beschreibung + Registrierungsnummer der Bestätigung (ggf. mit Nachträgen)
SSEE	Qualifizierte D-TRUST Multicard 2048 Bit, SHA 256	Für den Massensignaturbetrieb geeignete Karte basierend auf „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“, Registrierungsnummer: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit den Nachträgen vom 06.02.2007 und 06.05.2008
Kartenleser	Reiner SCT Kartenlesegeräte GmbH CyberJack e-com Version 3.0	Klasse 3 Chipkartenleser, TUVIT.93155.TE.09.2008

Tabelle 2: Zusätzliche Produkte, nach SigG bestätigt

3. Funktionsbeschreibung

Die Software **Dictao Signature & Validation Server (DxS) v4.8** ist Teil einer Signaturanwendungskomponente für die Erzeugung qualifizierter elektronischer Signaturen und für die Prüfung qualifizierter elektronischer Signaturen und erfüllt die im Signaturgesetz (SigG) und der Signaturverordnung (SigV) definierten Anforderungen an eine Signaturanwendungskomponente, die im Abschnitt 4 spezifiziert sind.

3.1 Funktionsumfang

Mit dem **DxS v4.8** können:

- in Verbindung mit geeigneten Chipkartenlesern und sicheren Signaturerstellungseinheiten (Signaturkarten) qualifizierte Signaturen serverseitig im Massensignaturverfahren erzeugt werden ;
- qualifizierte Signaturen serverseitig im Massensignaturprüfverfahren validiert werden.

Bei der serverseitigen Signaturerzeugung muss durch die Einsatzumgebung sichergestellt werden, dass gleichwertige Dokumente zur Signaturerzeugung übergeben werden. Die vorgesehene Einsatzumgebung ist durch einen Server mit Standard-Betriebssystem und Standard-Hardware gekennzeichnet, der in einem geschützten Einsatzbereich gemäß Definition der Bundesnetzagentur (vgl. Abschnitt 5) eingesetzt wird.

DxS v4.8 benötigt einen Direktzugriff auf eine Datenbank. Diese Datenbank enthält:

- Die generierten Nachweise zur Signaturerstellung und Signaturprüfung mit den zugehörigen Zertifikaten
- Die Konfiguration des Servers und die Historie der älteren Versionen
- Den Audit-Trail (log Veränderung)

Das Audit-Trail protokolliert die durchgeführten Änderungen der Konfiguration.

Hinweis: Alle diese Elemente sind in Integrität und Authentizität mittels elektronischer Signaturen geschützt.

3.2 Sichere PIN-Eingabe

Die Freigabe der PIN am Kartenleser wird durch die Konfiguration des **DxS v4.8** auf einen festen Zeitraum oder auf eine feste Signaturzahl beschränkt. Es gibt keine Voreinstellung. Ohne Konfiguration des DxS in Zeitraum und Signaturzahl ist eine Freischaltung nicht möglich. Vor der Eingabe der PIN am Kartenleser erscheint auf dem Display des Kartenlesers eine entsprechende Meldung.

Wenn die Signaturkarte nicht für Massensignaturverfahren sondern für Einzelsignaturverfahren geeignet ist, wird die Freischaltung auf eine Signatur beschränkt.

Es gibt keinen Prozess, der nach Eingabe der PIN diese für die Anwendung vorhält, zum Signieren automatisch abrufen und an die SSEE sendet.

3.3 Signaturgesetzlich relevanten Funktionen

DxS v4.8 stellt im Einzelnen die folgenden signaturgesetzlich relevanten Funktionen zur Verfügung:

- Die Zuführung der zu signierenden Daten an eine sichere Signaturerstellungseinheit ;
- Die Erzeugung von Signaturdatenobjekten nach dem folgenden Signatur-Standard :
 - XML-DSig wie von www.w3.org/2000/09/xmldsig definiert
 - XAdES 1.3.2
 - PKCS#7 /CMS
 - PDF 1.4, PDF 1.5, PDF 1.6, PDF 1.7
 - PDF/A

- Alle obengenannte Signaturen können in folgenden Format erzeugt werden :
 - *Detached* (losgelöste) Signature
 - *Enveloped* Signature
 - *Enveloping* Signature
- Die Berechnung von Hashwerten nach den Standards SHA-256, SHA-384, SHA-512 ;
- Die Unterstützung der sicheren PIN-Eingabe durch Verwendung eines geeigneten Kartenlesers durch den Benutzer ;
- Die Verifikation der Authentizität signierter Daten durch eine mathematische Prüfung der Zertifikatskette beginnend vom Signaturzertifikat bis zu einem vertrauenswürdigen Wurzelzertifikat ;
- eine Prüfung, ob das Signaturzertifikat aktuell gesperrt ist mithilfe einer Online-Abfrage beim herausgebenden Trustcenter ;
- Die Verifikation qualifizierter Signaturzertifikate.

DxS v4.8 ermöglicht das gleichzeitige Handling von einem oder mehreren Kartenlesern und Signaturkarten (Array).

3.4 Prozessorientierte Arbeitsweise

Der Ablauf der Prozesse im **DxS v4.8** kann nicht von außen beeinflusst werden. **DxS v4.8** gibt die Kontrolle erst nach erfolgreichem Abschluss der entsprechenden Operation (Erzeugen einer Signatur mithilfe einer SSEE und/oder prüfen einer Signatur) an das externe Anwendungsprogramm zurück, ansonsten erfolgt eine Fehlermeldung.

Die dem **DxS v4.8** übergebenen Daten werden durch dafür definierte Prozesse verarbeitet. Zur Definition solcher Prozesse sind im Wesentlichen die folgenden Prozesskonfigurationen zu tätigen:

- Festlegung der durchzuführenden Prozessschritte (Signieren, Verifizieren)
- Festlegung der Schnittstelle zur Übergabe der Daten (Web-Service Schnittstelle)

Die zu signierenden bzw. die signierten Daten können mit den jeweilig zuständigen externen Programmen vor bzw. nach dem Signaturprozess eingesehen werden, da der **DxS v4.8** keine Komponente in Form eines „secure viewer“ enthält.

3.5 Beschreibung der externen Schnittstellen

Über diese Schnittstelle können alle Funktionen der Signaturanwendungskomponente genutzt werden.

Die folgenden Funktionalitäten stehen zur Verfügung:

- Signierprozess: Dokument beliebigen Typs und Signatur beliebigen Standards
- Verifikationsprozess: Signatur
- Zertifikatprüfung: OCSP-Schnittstelle (Die zu verwendende URL wird jeweils dem Signaturzertifikat entnommen)

Der Ablauf des Verifikationsprozesses kann von der aufrufenden Anwendung nicht beeinflusst werden; erst nach vollständigem Durchlaufen des Verifikationsprozesses erhält die aufrufende Anwendung das Ergebnis zurück. Die Ergebniswerte werden an die aufrufende Anwendung zurückgeliefert. Der Nutzer hat auch die Möglichkeit direkt, durch ein versicherte Web-Portal von **DxS v4.8** die Prüfdokumentation anzusehen und/oder unterzuladen.

3.6 Prüfung qualifizierter Zertifikate aus Deutschland

Bei qualifizierten Zertifikaten aus Deutschland erfolgt die Prüfung der Zertifikatskette gemäß Common-PKI SigG Profile (Kettenmodell).

3.7 Integritätsprüfung

Die Teil-Signaturanwendungskomponente **DxS v4.8** verfügt entsprechend § 15 Abs. 4 SigV über Selbstprüfungsmechanismen zum Schutz vor der Manipulation der Software.

Ein **Integrity Checking Tool (ICT)** wird mit dem **DxS v4.8** ausgeliefert. Der Anwender hat die Möglichkeit, jeder Zeit die Authentizität und Integrität der Komponenten zu prüfen. Das ICT berechnet die Hashwerte der Komponenten und vergleicht sie mit den hinterlegten Hashwerten der Programmbestandteile des **DxS v4.8**.

Im Falle einer Manipulation wird dies dem Anwender eindeutig angezeigt.

3.8 Absicherung des Signaturprozesses

Zur Absicherung des Signaturprozesses ist vor der Signaturerzeugung der Signaturauftrag durch den Zertifikatsinhaber genau zu definieren. Nach Bestätigung des Signaturauftrages erfolgt durch den Zertifikatsinhaber die Eingabe der PIN.

Der Signaturauftrag wird in einem gesonderten Fenster zusammengefasst und dem Nutzer als eine Art Warnhinweis angezeigt.

In diesem Signaturauftrag wird u.a. aufgeführt, welcher Person der Signaturschlüssel zugeordnet ist und welches Zertifikat verwendet wird. Dabei lassen sich auf Wunsch auch die Zertifikatsinhalte anzeigen.

Vor dem Signaturprozess wird dem Signaturschlüsselinhaber in einem Konsolenfenster angezeigt, für welche Datei eine qualifizierte Signatur erzeugt werden soll.

Dabei ist zu beachten, dass der **DxS v4.8** in dem Szenario der Massensignatur nur für das Signieren von gleichwertigen Dokumenten innerhalb eines Prozesses bestimmt ist. Der Anwender muss technisch oder organisatorisch sicherstellen, dass nur gleichwertige Dokumente in einem einzelnen Prozess signiert werden, bzw. bei parallel ablaufenden Prozessen mit unterschiedlichen Konfigurationen, die Schnittstellen jeweils pro Prozess nur mit gleichwertigen Dokumenten befüllt werden.

3.9 Typische Anwendungsszenarien

Als Anwendungsbereich ist die Nutzung in größeren Infrastrukturen, z.B. im privatwirtschaftlichen und behördlichen Umfeld, in einem geschützten Einsatzbereich anzusehen.

DxS v4.8 wird typischerweise in folgenden Anwendungsszenarien eingesetzt:

- Signatur und Signaturprüfung von Auftrag- und Bestellscheinen
- Signatur und Signaturprüfung von Ausgangsrechnungen
- Signatur und Signaturprüfung von Versicherungsanträgen
- Signatur und Signaturprüfung von Steuererklärungen
- Signatur und Signaturprüfung von Verträgen

- Signatur und Signaturprüfung von Beweisen für gesetzlichen Archivierungen und Langzeitspeicherungen

4. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

Das Produkt **DxS v4.8** erfüllt die nachfolgend aufgeführten Anforderungen des SigG:

Referenz	Gesetzestext	Beschreibung
§ 17 Abs. 2 Satz 1 SigG	<i>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 Signatur bezieht.</i>	<p>Wird durch die Einsatzumgebung des Nutzers bzw. die aufrufende Softwareanwendung erfüllt.</p> <p>Siehe hierzu auch Kapitel 3.4 und 3.5 und 3.8</p> <p>Die Feststellung der zu signierenden Daten hat durch die aufrufende Signaturanwendung zu erfolgen. Durch DxS v4.8 wird vor Initialisierung der SSEE mittels der Signatur-PIN dem Nutzer ein Warnhinweis zu dem konfigurierten Signaturauftrag angezeigt (siehe auch 3.8). Ferner wird im Multisignaturbetrieb die Erzeugung einer Signatur vor dem eigentlichen Signaturprozess dem Signaturschlüssel-Inhaber im Management Interface des DxS v4.8 laufend angezeigt.</p> <p>Nach Bestätigung des Signaturauftrages erfolgt der Nachweis der PIN über ein Kartenlesegerät mit sicherer PIN-Eingabemöglichkeit gegenüber der SSEE.</p>
§ 17 Abs. 2 Satz 2 SigG	<i>Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,</i> <ol style="list-style-type: none"> 1. auf welche Daten sich die Signatur bezieht, 2. ob die signierten Daten unverändert sind, 3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist, 4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, (... und zugehörige qualifizierte Attribut-Zertifikate-...) aufweisen und 5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 	<p>Wird durch DxS v4.8 erfüllt.</p> <p>Zu jeder geprüften Datei wird vom DxS v4.8 eine Prüfdokumentation erstellt, aus der alle geforderten Daten ersichtlich sind.</p> <p>Darüber hinaus bietet das DxS v4.8 eine Schnittstelle, die es dem Unterzeichner und/oder Anwender ermöglicht, die bei der Signaturprüfung gesammelten Nachweise zu überprüfen. Zugehörige qualifizierte Attribut-Zertifikate werden nicht überprüft.</p>

	<i>5 Abs. 1 Satz 3 geführt hat.</i>	
§ 17 Abs. 2 Satz 3 SigG	<i>Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.</i>	Wird durch die Einsatzumgebung des Nutzers erfüllt. Der Nutzer muss durch technische und organisatorische Maßnahmen sicherstellen, dass Inhalte bei Bedarf mit externen Programmen angezeigt werden können.

Das Produkt **DxS v4.8** erfüllt die nachfolgend aufgeführten Anforderungen der SigV:

Referenz	Gesetzestext	Beschreibung
§ 15 Abs. 2 Nr. 1 SigV	<i>Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass</i> <i>1. bei der Erzeugung einer qualifizierten elektronischen Signatur</i> <i>a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,</i> <i>b) eine Signatur nur durch die berechtigt signierende Person erfolgt,</i> <i>c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und (...)</i>	zu a) Die Identifikationsdaten (PIN) werden nur auf der SSEE verwendet. Die Übergabe der PIN gegenüber der SSEE erfolgt mittels Kartenlesegerät mit sicherer PIN-Eingabemöglichkeit. zu b) Die Aktivierung der SSEE kann nur durch den Signaturschlüsselinhaber erfolgen, da nur dieser im Besitz der PIN ist. zu c) Die Erzeugung einer Signatur wird vor dem eigentlichen Signaturprozess dem Signaturschlüsselinhaber im Management Interface des DxS v4.8 laufend angezeigt.
§ 15 Abs. 2 Nr. 2 SigV	<i>(...) 2. bei der Prüfung einer qualifizierten elektronischen Signatur</i> <i>a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und</i> <i>b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.</i>	Wird durch DxS v4.8 erfüllt. Die aufrufende Softwareanwendung zeigt dem Nutzer das Prüfergebnis an. Der Nutzer hat auch die Möglichkeit, über ein gesichertes Web-Interface die Prüfdokumentation anzusehen und/oder herunterzuladen
§ 15 Abs. 4 SigV	<i>Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass (...)</i> <i>3. Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.</i>	Wird durch DxS v4.8 erfüllt. Die Überprüfung von sicherheitstechnischen Veränderungen am DxS v4.8 erfolgt wie im Kapitel 3.7 beschrieben.

Hinweis zu schwachwerdenden Algorithmen und qualifizierten Zeitstempeln

Signaturanwendungskomponenten i. S. v. § 2 Nr. 11 b SigG müssen 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.

Das Produkt „**DxS, Version 4.8**“ erfüllt die Anforderungen an schwach werdende Algorithmen und qualifizierte Zeitstempel wie folgt:

Anforderung	Erfüllung und Verhalten der Software „DxS, Version 4.8“
<p><i>a) Abgelaufene Algorithmen:</i> Die Prüfung einer Signatur durch eine 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><i>Unspezifische Aussagen zu abgelaufene Algorithmen sind nicht zulässig.</i></p>	<p>Bei der Prüfung einer Signatur prüft das Produkt DxS v 4.8, ob die verwendeten kryptographischen Algorithmen – sowohl zum Zeitpunkt der Prüfung (Prüfzeitpunkt) als auch zum Signierzeitpunkt – als geeignet anzusehen sind. Bzgl. der Eignung kryptographischer Algorithmen werden die Angaben des offiziellen Algorithmenkatalogs der Bundesnetzagentur genutzt.</p> <p>Das Prüfprotokoll, in dem die Ergebnisse der Prüfung zusammenfassend dem Benutzer dargestellt werden, hebt Signaturen, deren zugehörige kryptographische Algorithmen zum Prüf- oder zum Signierzeitpunkt als nicht mehr geeignet anzusehen sind, weist den Benutzer darauf hin, dass ein verwendeter Algorithmus zum Zeitpunkt der Prüfung oder zum Signierzeitpunkt gemäß Algorithmenkatalog nicht mehr für eine qualifizierte elektronische Signatur geeignet ist oder war.</p>
<p><i>b) Nicht implementierte Algorithmen:</i> 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><i>Unspezifische Aussagen zu nicht implementierten Algorithmen sind nicht zulässig.</i></p>	<p>Sofern die Software DxS v 4.8 eine Prüfung einer Signatur nicht (vollständig) durchführen kann, da ein benötigter kryptographischer Algorithmus nicht implementiert ist, wird dies dem Benutzer entsprechend angezeigt:</p> <p>Das Prüfprotokoll, in dem die Ergebnisse der Prüfung zusammenfassend dem Benutzer dargestellt werden, hebt Signaturen, deren zugehörige kryptographische Algorithmen nicht implementiert sind, entsprechend hervor und weist den Benutzer darauf hin, dass die Signatur nicht geprüft werden konnte, da ein Algorithmus nicht implementiert ist.</p>
<p><i>c) Qualifizierte Zeitstempel:</i> Tragen Daten einer qualifizierten Signatur, bei deren Verifikation zu erkennen ist, dass der Signaturprüf Schlüssel 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><i>Solange kein standardisiertes Verfahren für die Einbindung von qualifizierten Zeitstempeln</i></p>	<p>Die Software DxS v 4.8 bringt keine Zeitstempel an.</p> <p>Mangels standardisiertem Verfahren für die Einbindung von qualifizierten Zeitstempeln, werden qualifizierte Zeitstempel aus Fremdprodukten nicht interpretiert. Gleichwohl ergibt sich ein qualifizierter Zeitstempel aus dem zugehörigen, angezeigten Zertifikat.</p>

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.

Unspezifische Aussagen zu qualifizierten Zeitstempeln sind nicht zulässig.

5. Maßnahmen in der Einsatzumgebung

5.1 Einrichtung der IT-Komponenten

Das Produkt **DxS v4.8** benötigt als Voraussetzung Serverhardware mit:

Betriebssystem:

- SuSE Linux Enterprise Server 10

Chipkartenterminals:

- gemäß Signaturgesetz und –verordnung geprüfte und bestätigte Chipkarten-Terminals. Im Kapitel 2 beschrieben.

Personalisierte Signaturkarten:

- gemäß Signaturgesetz und –verordnung geprüfte und bestätigte sichere Signaturerstellungseinheiten. Im Kapitel 2 (Tabelle 2) beschrieben.

Treiber und Middleware:

- die zugehörigen Treiber für die Signaturkarten und die Signaturkartenleser und die zugehörige Middleware gemäß Handbuch.

Datenbank:

- Oracle 11g oder Postgre SQL 8

5.2 Anbindung an ein Netzwerk

Für den Betrieb des Produktes **DxS v4.8** ist ein Netzwerk notwendig.

Bei Anbindung des Produktes an ein Netzwerk müssen die folgenden Maßnahmen zum Schutz beachtet werden: Netzwerkverbindungen müssen so abgesichert sein, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall und durch die Verwendung geeigneter Anti-Viren-Programme.

Für den Betrieb der Software **DxS v4.8** in einer Terminalserver-Umgebung ist die Verbindung zwischen Client und Server über SSL bzw. TLS zu realisieren. Der Verbindungsaufbau ist durch gegenseitige Authentisierung über ausgetauschte Zertifikate zu schützen. Der Betrieb in einer Terminalserver-Umgebung ist nur innerhalb eines Intranets erlaubt.

Die in diesem Abschnitt gemachten Auflagen müssen eingehalten werden.

5.3 Auslieferung und Installation

Die Auslieferung des Produkts an den Kunden erfolgt per Post auf einer Software-CD, per Download von einem Webserver von Dictao oder durch persönliche Übergabe der Software-CD, welche den unter Abschnitt 2 Tabelle 1 beschriebenen Inhalt hat.

Die Installation darf nur von geschultem Personal durchgeführt werden. Das spezifizierte Auslieferungs- und Installationsverfahren ist einzuhalten. Dabei ist insbesondere zu prüfen, dass die Software im Vergleich zum Auslieferungszeitpunkt unverändert ist, in dem der SHA2-Hashwert durch das Installationspersonal mit dem Hashwert des ausgelieferten Produktes verglichen wird.

Der Hashwert wird von Dictao separat dem Kunden mitgeteilt.

5.4 Auflagen für den Betrieb des Produktes

Das Produkt **DxS v4.8** ist in einem geschützten Einsatzbereich gemäß Abschnitt 4.2 des Dokuments „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten - Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen, Version 1.4, Stand: 19.07.2005“ der Bundesnetzagentur zu betreiben.

Während des Betriebs sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

- Der Betrieb erfolgt in einer vertrauenswürdigen Umgebung und mit vertrauenswürdigen Personal.
- Das System wird nach dem Prinzip „Reduktion auf geringste benötigte Benutzer, Dienste und Berechtigungen“ betrieben.
- Es wird sichergestellt, dass auf der von dem Produkt **DxS v4.8** und der Anwendung benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Änderungen am produktiven System unterliegen dem Vieraugen-Prinzip und werden dokumentiert. Sie werden auf Risiken bzgl. der Signaturerstellung evaluiert.
- Kritische Daten (wie PIN der Signaturkarte, Benutzerpassworte) werden verantwortungsvoll und vertraulich behandelt.
- Benutzer / Anwender von **DxS v4.8** sind darüber informiert, dass sie die PIN zu ihrem Schlüssel auf keinen Fall und zu keiner Zeit weitergeben dürfen.
- Benutzer / Anwender von **DxS v4.8** sind mit dessen Handbuch und Voraussetzungen vertraut.
- Benutzer bzw. Anwender von **DxS v4.8** sind darüber informiert und sorgen dafür, dass in einem Signaturdurchlauf nur gleichwertige Dokumente (z.B. nur Rechnungen) dem Prozess der Massenerzeugung qualifizierter elektronischer Signaturen zugeführt werden.

6. Algorithmen und zugehörige Parameter

Zur Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt **DxS v4.8**

- die Hashfunktionen SHA-256, SHA-384, SHA-512

bereitgestellt.

Zur Prüfung qualifizierter elektronischer Signaturen und Zertifikate werden vom Produkt **DxS v4.8**

- die Hashfunktionen SHA-256, SHA-384, SHA-512

sowie die Signaturverfahren RSA mit einer

- Schlüssellänge von 1024 Bit, 2048 Bit, 4096 Bit

bereitgestellt.

Das Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002

Die gemäß Anlage I Abs. 1 Nr. 2 SigV festgelegte Eignung für die verwendeten kryptographischen Algorithmen sind gemäß den Angaben der Bundesnetzagentur vgl. „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) – Vom 06. Januar 2010 Veröffentlicht am 04. Februar 2010 im Bundesanzeiger Nr. 19, Seite 426 wie folgt als geeignet eingestuft:

Hash-Algorithmus	Gültig bis
SHA-1	bis Ende 2015 ausschließlich zur Prüfung qualifizierter Zertifikate
SHA-256	31.12.2016
SHA-384	31.12.2016
SHA-512	31.12.2016

Signatur-Algorithmus	Gültig bis
RSA 1280 bit	nicht mehr geeignet
RSA 1536 bit	nicht mehr geeignet
RSA 1728 bit	31.12.2010
RSA 1976 bit	31.12.2014
RSA 2048 bit	31.12.2014

7. Gültigkeit der Herstellereklärung

Diese Erklärung ist bis zu ihrem Widerruf, längstens jedoch bis zum 31.12.2015 gültig. Die Gültigkeit der Herstellereklärung ist weiter beschränkt durch die in Kapitel 6 aufgeführten Gültigkeiten der Algorithmen;

Die Gültigkeit kann sich verkürzen, wenn z.B. neue Feststellungen hinsichtlich der Sicherheit des Produktes oder der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

Der aktuelle Status der Gültigkeit der Erklärung ist bei der zuständigen Behörde (Bundesnetzagentur, Referat Qualifizierte Elektronische Signatur – Technischer Betrieb) zu erfragen.

8. Zusatzdokumentation

Folgende Bestandteile der Herstellereklärung wurden aus dem Veröffentlichungstext ausgegliedert und bei der zuständigen Behörde hinterlegt:

1. Security target, Dictao Signature & Validation Server (DxS), Version 1.0, 30.08.2010, 32 Seiten
2. Test plan, Dictao Signature & Validation Server (DxS), Version 1.0, 30.08.2010, 206 Seiten

Ende der Herstellereklärung