

# HERSTELLERERKLÄRUNG

Der Hersteller

**struktur**<sup>®</sup>

struktur AG  
Friedrichstr. 14  
D-70174 Stuttgart

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

## ICOYA EDI Signature Server

eine „Signaturanwendungskomponente“ (Software) gemäß §2 Abs. 11 SigG ist, die es ermöglicht, qualifizierte elektronische Signaturen in PDF- und sonstige Dokumente im Batchbetrieb (Massensignatur) einzufügen und die die Anforderungen des Signaturgesetzes<sup>1</sup> bzw. der Signaturverordnung<sup>2</sup> erfüllt.

Ein Widerruf dieser Erklärung wird ggf. unter <http://www.struktur.de> veröffentlicht.

Stuttgart, den 16.02.2006

Niels Mache  
(CEO)

---

<sup>1</sup> Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22)

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59)

## 1. Handelsbezeichnung

Die Handelsbezeichnung lautet:

**ICOYA EDI Signature Server**

Hersteller ist:

**struktur AG  
Friedrichstr. 14  
D-70174 Stuttgart  
GERMANY**

Auslieferung:

Der ICOYA EDI Signature Server wird als Software auf CD-ROM sowie als Server-Appliance, d.h. als Signatur-Gerät, ausgeliefert. Auf der CD-ROM befinden sich Installationsprogramme und Archivdateien für den ICOYA EDI Signature Server sowie Handbücher (im PDF-Format) zur Installation und Administration. Zusätzlich zur Produkt CD-ROM wird ein zertifiziertes SmartCard Kartenlesegerät („Card Reader“) der Sicherheitsstufe Klasse 2 oder Klasse 3 für qualifizierte Signaturkarten mitgeliefert. Auf der Produkt CD-ROM sind die für den Betrieb des Kartenlesegeräts benötigten Treiberprogramme enthalten.

## 2. Funktionsbeschreibung

Der ICOYA EDI Signature Server ist eine Signaturanwendungskomponente gemäß §2 Nr. 11 SigG, die elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen durch eine SigG-konform personalisierte und ISIS-MTT konforme SmartCard zuführen kann. Insbesondere können PDF-, TIFF (Faxdokumente) und sonstige Dokumente sowie XML- und EDI Daten im Massenbetrieb mit einer qualifizierten elektronischen Signatur versehen werden.

### 2.1 Signatur von Dokumenten und Rechnungen

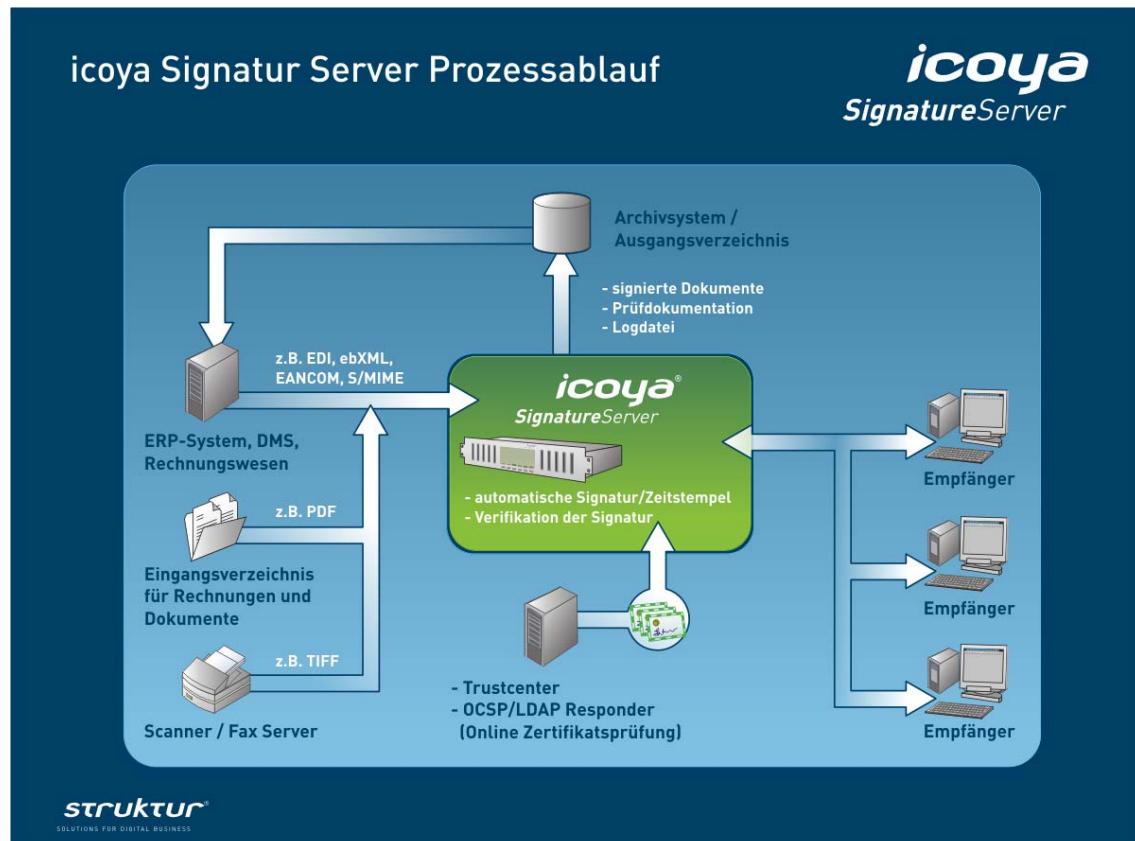
Für die Signatur von Rechnungen im PDF- oder TIFF-Format werden die Rechnungs- bzw. Buchungsdaten (Rechnungsempfänger/-ersteller, Rechnungsnummer, Artikelbezeichnung, Stückzahl, MwSt., usw.) der Rechnung signiert und maschinenlesbar (XML, ebXML, EDI, EDIFACT, u.a.) in Form eines 2-dimensionalen Barcodes (DataMatrix ECC200, standardisiert gemäß ISO/IEC 16022) auf die Rechnung aufgebracht. Dadurch ist gewährleistet, dass die Rechnungsinformation auf der Empfängerseite unabhängig vom verwendeten Übertragungsweg (elektronisch, Fax-Server/Telefon, Papier) maschinell gelesen und verifiziert werden kann. Für die Verifikation signierter Dokumente wird die frei verfügbare Software ICOYA Scan Processor eingesetzt. Die Anwendungssoftware ICOYA Scan Processor ist per Download auf dem Internetserver <http://dl.struktur.de> verfügbar. Zusätzlich kann mit PKCS#7-konformen Softwaretools die Gültigkeit der digitalen Signatur anhand der

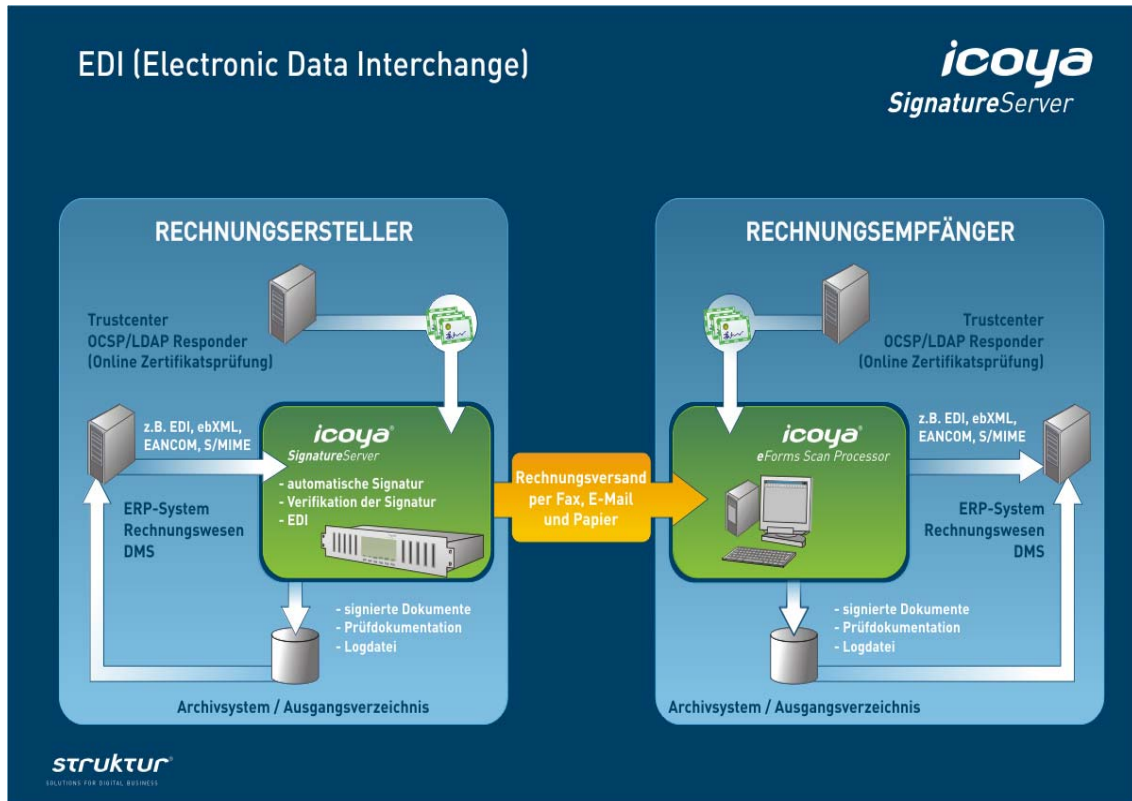
externen Signaturdatei (PKCS#7-konform) überprüft werden.

## 2.2 Signaturvorgang

Der Signaturvorgang des ICOYA EDI Signature Servers erfolgt entweder kontinuierlich oder zeitgesteuert. Die Anzahl der Signaturen, die nach einer erfolgreichen PIN-Eingabe möglich sind, sind durch Angabe einer maximalen Anzahl von Signaturen oder durch Angabe eines Enddatums bzw. eines Zeitraums einschränkbar. Der ICOYA EDI Signature Server unterstützt zusätzlich auch Mehrfachsignaturen pro Dokument. Die digitale Signatur von elektronischen Dokumenten kann mit dem ICOYA EDI Signature Server entsprechend den Erfordernissen konfiguriert werden. Das Format der erzeugten digitalen Signatur ist in Abhängigkeit des Dokumententyps und des Verwendungszwecks einstellbar. Für die Signatur von PDF-Dokumenten wird die Signatur standardmäßig in das PDF-Dokument integriert. Die Signatur von PDF-Dateien ist konform zur PDF (Portable Document Format) Spezifikation der Adobe Inc. Für sonstige Dokumente (z.B. TIFF, XML) wird eine PKCS#7-konforme, externe Signaturdatei erstellt. Optional kann auch für die Signatur von PDF-Dokumenten eine PKCS#7-konforme, externe Signaturdatei erzeugt werden. XML Dateien können gemäß des internationalen Signaturstandards XMLSig des W3C digital signiert werden.

Für den Betrieb des ICOYA EDI Signature Servers werden keine weiteren Produkte von Drittanbietern benötigt. Die Funktionsweise und Schnittstellen des ICOYA EDI Signature Servers und des icoya Scan Processors sind in den folgenden Schaubildern dargestellt.





Der ICOYA EDI Signature Server ist unter einer Vielzahl von Betriebssystemen lauffähig. Siehe hierzu Abschnitt 6. Zur Erzeugung einer qualifizierten elektronischen Signatur muss ein zertifiziertes SmartCard Lesegerät angeschlossen sein und eine qualifizierte Signaturkarte (SmartCard) von einem akkreditierten Trustcenter zum Einsatz kommen. Für Anwendungen bei denen eine sehr hohe Anzahl von Signaturen pro Zeiteinheit benötigt wird, kommen zertifizierte (FIPS-140 Level 3) Cryptokarten wie z.B. die Rainbow CryptoSwift HSM PCI Karte für einen Durchsatz von 720.000 Signaturen pro Stunde, zum Einsatz. Für weitergehende Informationen kontaktieren Sie bitte die struktur AG unter der folgenden Adresse:

**struktur AG**  
**Friedrichstr. 14**  
**D-70174 Stuttgart**  
**GERMANY**  
**Telefon: +49 711 896656 0**  
**Fax: +49 711 896656 10**  
**email: info@struktur.de**  
**Web: www.struktur.de**

Neben den oben beschriebenen Funktionen zum Signieren im Sinne des Signaturgesetzes bietet ICOYA EDI Signature Server weitere Funktionen zum Ver- bzw. Entschlüsseln und Signieren mit nicht SigG-konformen Signatortokens oder Software-Zertifikaten. Zusätzlich existiert eine Anbindung an einen Zertifikatsdienst (<http://www.certificate24.de>) zum Zwecke der Verifikation Digitaler Zertifikate durch den Unterzeichner oder Rechnungsersteller und den Empfänger. Zusätzlichen Funktionalitäten sind **nicht**

Gegenstand dieser Bestätigung.

Entscheidend für die Sicherheit der Anwendung ist die zweifelsfreie Identifikation einer vertrauenswürdigen Herkunft des Codes. Daher sind die Systemsoftware und alle sicherheitsrelevanten Funktionen und Module des ICOYA EDI Signature Servers zum Schutz der Datenintegrität seitens der struktur AG mit Zertifikaten signiert und dadurch vor Manipulation geschützt. Wird die Software bzw. Firmware des ICOYA EDI Signature Servers oder Teile hiervon verändert, ist der ICOYA Signatur Server dadurch als ganzes nicht mehr lauffähig. Diese Sicherheitsmechanismen garantieren den fehlerfreien Betrieb und schützen den Anwender vor einer Kompromittierung der Sicherheit durch Manipulation oder Einschleusen von Programmcode („Würmern“, „Trojaner“, „Viren“, etc.).

### **3. Erfüllung der Anforderungen des SigG und der SigV**

#### **3.1 Erfüllte Anforderungen**

ICOYA EDI Signature Server und die Verifikationsoftware icoya Scan Processor erfüllt die Anforderungen nach § 17 Abs. 2 Satz 1,2,3 SigG. Insbesondere gelten die folgenden Zusicherungen:

1. eindeutige Anzeige und Feststellbarkeit der Daten bei Signaturerzeugung,
2. auf welche Daten sich die Signatur bezieht,
3. Feststellbarkeit der Daten, Vollständigkeit der Rechnungsdaten, des Unverändertseins der Daten,
4. der Zuordnung zum Signaturschlüsselinhaber und welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht und zugehörige qualifizierte Attribut-Zertifikate aufweisen, sowie
3. bei Bedarf Anzeige des Inhalts der zu signierenden oder signierten Daten.

Der icoya EDI Signature Server gewährleistet, wie nach §15 Abs. 2 ff SigV gefordert, dass bei der Erzeugung einer qualifizierten elektronischen Signatur

1. keine Preisgabe der Identifikationsdaten,
2. Signatur nur durch berechtigt signierende Person,
3. die Korrektheit der Signatur zuverlässig geprüft (serverseitige Signaturprüfung) und zutreffend angezeigt wird,
4. eine eindeutige Anzeige der Signatur vor Erzeugung und eindeutige Erkennbarkeit der Gültigkeit der Zertifikate sowie
5. die Erkennbarkeit von sicherheitstechnischen Veränderungen gewährleistet ist.

Voraussetzung dafür ist, dass die unter 3.2 ff spezifizierten Einsatzbedingungen eingehalten werden. Es wird ein Betrieb in einem geschützten Einsatzbereich vorausgesetzt.

## **4. Einsatzbedingungen**

### **4.1 Einrichtung des Signaturrechners**

Die Installation des Signaturrechners erfolgt durch einen Mitarbeiter der struktur AG oder einen Consultant eines Partnerunternehmens. Die Eignung zur Installation und Inbetriebnahme des ICOYA EDI Signature Servers muss der Consultant durch eine schriftliche Bestätigung der struktur AG vorweisen.

Es darf nur ein zertifizierter Klasse2 oder Klasse3 SmartCard-Leser verwendet werden, der über einen CT-API Treiber angesteuert wird. Dadurch ist die PIN-Eingabe nur am SmartCard-Leser selbst möglich. Es muss eine qualifizierte Massensignaturkarte eines akkreditierten Trustcenters verwendet werden.

Zur Beachtung:

Es darf keine weitere Software und keine weiteren Dienste auf dem Signaturrechner aktiv sein. Es wird eine, über die Standardkonfiguration hinausgehende, Absicherung des Signaturrechners durchgeführt, so dass nur die für den Betrieb notwendigen Protokolle und Ports zur Verfügung stehen.

### **4.2 Betrieb/Nutzung**

Der Signaturrechner wird in einer gesicherten Umgebung betrieben, die eine Zugangskontrolle zur Konsole des Signaturservers beinhaltet.

Ein Installations- und Administrationshandbuch wird in elektronischer Form mitgeliefert.

### **4.3 Potentielle Bedrohungen**

Die Sicherheit der Anwendungskomponenten des ICOYA EDI Signature Servers ist potentiell bedroht durch

- Angriffe über Kommunikationsnetze,
- Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger und
- Fehler/Manipulationen bei Installation, Betrieb/Nutzung und Wartung/Reparatur.

Grundlage dieser Erklärung ist der Einsatz von ICOYA EDI Signature Server in einem geschützten Einsatzbereich. Für den sicheren Einsatz des ICOYA EDI Signature Servers und zur Verhinderung von erfolgreichen Angriffen mit den Zielen, dass:

- Daten signiert werden, die nicht signiert werden sollen und
- die Geheimhaltung des Identifikationsmerkmals (PIN) nicht gewährleistet ist,

sind die Auflagen einer gesicherten technischen Einsatzumgebung zu beachten.

### **4.4 Voraussetzungen an die technische Einsatzumgebung**

Vor Verwendung des ICOYA EDI Signature Servers muss jeder Benutzer sicherstellen, dass er in einer technischen Einsatzumgebung arbeitet, die zum Zeitpunkt der Ausführung der elektronischen Signatur nicht kompromittiert ist. Hierbei ist vom Benutzer sicherzustellen, dass an seinem PC-Arbeitsplatz keine „Viren“ oder „trojanische Pferde“ eine

Kompromittierung herbeigeführt haben. Schutz hierzu kann durch die Installation und Verwendung von aktueller Virenschutzsoftware erreicht werden.

Zusätzlich ist die technische Einsatzumgebung durch unberechtigte Zugriffe auf Systemressourcen aus dem Internet oder Intranet zu schützen. Dies kann durch die fachgerechte Installation und Verwendung einer „Firewall“ sichergestellt werden. Insbesondere ist zu gewährleisten, dass die verwendeten Internet Browser sowie deren Komponenten aus zuverlässigen Quellen (z.B. direkt vom Hersteller) bezogen werden und dass die von den Herstellern regelmäßig zur Verfügung gestellten Sicherheits-Updates installiert werden.

#### **a) Auflagen zur Anbindung an das Internet**

Eine Internetanbindung kann zum Einspielen oder Abholen von unsignierten bzw. signierten Dokumenten notwendig sein. Dabei darf der Signaturrechner nicht direkt an das Internet angeschlossen sein, sondern eine solche Netzverbindung muss durch eine geeignet konfigurierte „Firewall“ abgesichert sein, so dass Online-Angriffe aus dem Internet auf den eingesetzten Server erkannt bzw. unterbunden werden.

#### **b) Auflagen zur Anbindung an ein Intranet**

Wenn der eingesetzte Server 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.

#### **c) Auflagen zur Sicherheit der IT-Plattform und Applikationen**

Der Benutzer von ICOYA EDI Signature Server muss sich davon überzeugen, dass keine Angriffe auf den Server und die dort vorhandenen Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf dem Signaturrechner installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf dem Signaturrechner keine Viren oder Trojanischen Pferde eingespielt werden können,
3. die Hardware des Signaturrechners oder Server Appliances nicht unzulässig verändert werden kann oder
4. der verwendete Chipkarten-Leser weder manipuliert noch in irgendeiner 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.

Durch den Betrieb des icoya EDI Signature Servers in einer gesicherten Umgebung ist sicherzustellen, dass

1. eine Benutzerauthentifizierung am Signaturrechner unumgänglich ist,
2. installierte Zertifikate benutzerabhängig eingerichtet sind, so dass Zertifikate, die

unter einer anderen Benutzerkennung installiert werden, nicht bei der Auswahl eines Zertifikats für einen anderen - etwa den berechtigten Benutzer - zur Verfügung stehen. So wird verhindert, dass ein irrtümlicherweise ein fremdes Zertifikat ausgewählt und verwendet werden kann.

3. Für die Arbeitsverzeichnisse des ICOYA EDI Signature Servers müssen geeignete Benutzerberechtigungen vergeben werden, um einen unautorisierten Zugriff auf Dokumente zu verhindern.

Empfehlungen über die, für den sicheren Betrieb des ICOYA EDI Signature Servers erforderlichen Sicherheitsmassnahmen und Einstellungen werden auf der ICOYA Homepage ([www.ICOYA.de](http://www.ICOYA.de)) bereitgestellt.

#### **4.5 Administrative Einsatzumgebung**

Der Benutzer des ICOYA EDI Signature Servers hat durch geeignete Sicherheitsmassnahmen sicherzustellen, dass Manipulationen oder auch physische Zugriffe auf die Einsatzumgebung durch Dritte nicht möglich sind. Dies muss aufgrund von personellen, materiellen und organisatorischen Maßnahmen erfolgen. Geeignete Maßnahmen zur Sicherung des Servers und PC Arbeitsplatzes werden vom BSI im BSI Grundschriftbuch zur Verfügung gestellt.

#### **4.6 Schutz vor unbefugter Veränderung**

Zum Schutz vor unbefugter Veränderung der Systemsoftware bzw. Firmware des icoya EDI Signature Servers wurden alle sicherheitsrelevanten Softwaremodule verschlüsselt und von Mitarbeitern der struktur AG digital signiert. Im Falle der Modifikation eines oder mehrerer Softwarekomponenten ist der icoya EDI Signature Server nicht mehr lauffähig. Die Kompromittierung des Servers ist für den Anwender dadurch unmittelbar erkennbar.

#### **4.7 Wartung/Reparatur**

Der Signaturrechner wird in einer gesicherten Umgebung betrieben, die eine Zugangskontrolle zur Konsole des Signaturservers beinhaltet.

Es findet entweder eine Einweisung der Administratoren durch Struktur oder eine direkte Wartung durch Struktur statt. Die Einweisung der Administratoren wird schriftlich durch Struktur bestätigt.

### **5. Algorithmen und zugehörige Parameter**

Das verwendete Hash-Verfahren ist der SHA-1 Algorithmus, implementiert und ausgeführt auf der gesicherten CPU der SmartCard. Die gemäß Anlage 1 Abs. 1 Nr. 2 SigV festgestellte Eignung gilt mindestens bis Ende des Jahres 2008 (siehe BAnz. Nr. 48 vom 11.03.2003, Seite 4.202).

### **6. Auflagen zur Auslieferung und Installation des Produktes**

Die Anwenderkomponente ICOYA EDI Signature Server wird vom Hersteller als

- Stand-Alone Server Appliance Produkt ausgeliefert.
- Alternativ ist das Produkt auf einer CD-ROM für die Installation auf einem Rechnersystem verfügbar.

Die Anwenderkomponente ICOYA EDI Signature Server ist für die folgende technische Einsatzumgebung vorgesehen:

IBM-kompatibler PC/ Server lauffähig mit einem der unten genannten Betriebssysteme, mit Anschlussmöglichkeiten für ein Read-Only-Memory-Laufwerk (z.B. ein DVD-ROM oder CD-ROM) sowie für einen SmartCard-Leser (serielle Schnittstelle oder USB).

Unterstützte Betriebssysteme sind Windows 2000 Professional, Windows 2000 Server, Windows 2003 Advanced Server, Windows 2003 Enterprise Server, Red Hat Linux Enterprise Linux Version 4 (zertifiziert nach Common Criteria EAL4+).

Klasse2 oder Klasse3 SmartCard-Leser mit PIN-Eingabefeld, der die sichere Eingabe der PIN unterstützt. Die Struktur GmbH empfiehlt den Leser Chipdrive SCM SPR 532 Pinpad. Es werden funktional jedoch auch andere SmartCard-Leser mit CT-API Treiber an der seriellen oder USB-Schnittstelle unterstützt. Vor dem Echtbetrieb sind aber Sicherheitstests durch Struktur durchzuführen.

Wir empfehlen die Verwendung des icoya EDI Signature Server Appliance oder den Einsatz von Red Hat Linux Enterprise Linux, Version 4 in Verwendung mit standardisierten (nicht-proprietären), qualifizierten Signaturkarten (SmartCards) von einem akkreditierten Trustcenter.

## **7. Gültigkeit der Herstellereklärung**

Diese Herstellereklärung ist bis zum Widerruf durch struktur (Veröffentlichung auf [www.struktur.de](http://www.struktur.de)) bzw. bis zum Ablauf der Vertrauenswürdigkeit des Hashalgorithmus SHA-1, der verwendeten asymmetrischen Verschlüsselungsverfahren (RSA/DAS) - angezeigt durch das Bundesamt für Sicherheit in der Informationstechnik ([www.BSI.de](http://www.BSI.de)) bzw. die Regulierungsbehörde für Telekommunikation und Post ([www.RegTP.de](http://www.RegTP.de)) - gültig.

## **Ende der Herstellereklärung**