

Herstellererklärung

Version 1.0, Stand 15.10.2007

menten GmbH

Hauptstraße 136-140

51465 Bergisch Gladbach

erklärt hiermit gemäß §17(4) Satz 2 Signaturgesetz¹, in Verbindung mit §15(5) Signaturverordnung², dass das Produkt

**i-effect® *SIGG
Qualifizierte Elektronische Signatur - V1R3**

einer Teilkomponente einer Signaturanwendungskomponente basierend auf den nachstehend genannten Anforderungen des Signaturgesetzes bzw. der Signaturverordnung entspricht.

Ort, Datum

Bergisch Gladbach, 23.10.2007

gez. Ralph Menten

(Geschäftsführer)

¹ Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2).

² Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) geändert durch 1. SigÄndG.

Revisionshistorie des Handbuches

Datum	HE-Version	Beschreibung
20.11.2006	0.1	Erst-Version
27.09.2007	0.2	Überarbeitete Fassung der HE
15.10.2007	1.0	Geprüfte und freigegebene Fassung

1 Handelsbezeichnung des Produkts

Handelsbezeichnung:	i-effect® *SIGG Qualifizierte Elektronische Signatur - V1R3
Auslieferung:	Die Auslieferung durch den Hersteller erfolgt auf CD-R bzw. DVD-R und per Download.
Hersteller:	menten GmbH Hauptstraße 136-140 51465 Bergisch Gladbach Tel.: 0 22 02 - 23 99 0 Fax: 0 22 02 - 23 99 23 HRB 47762

2 Lieferumfang und Versionsinformationen

Nachfolgend ist der Lieferumfang, einschließlich der Versionsinformationen, aufgezählt:

Produktbestandteil	Bezeichnung	Version	Übergabeform
Software	i-effect® - „Die integrierte Lösung für IBM System i“	V1R3Mx	CD
Software	i-effect® *SIGG wird als Image-Datei auf DVD ausgeliefert und enthält ein vollwertiges, vorinstalliertes, vorkonfiguriertes MS Windows Server-System mit allen notwendigen Treibern, Softwarekomponenten und der eigentlichen Softwareanwendungskomponente. Alternative kann i-effect® *SIGG separat auf CD oder über die Webseite von www.i-effect.de in Form einer Passwortgeschützten ZIP-Datei heruntergeladen werden. Die separate Version auf CD bzw. die Download-Version ist digital signiert.	V1R3	DVD CD bzw. Passwortgeschütztes ZIP
Handbuch	i-effect® *SIGG – Installieren, Einrichten und Verwenden	1.0	PDF-Datei auf CD

Tabelle 1: Lieferumfang und Versionsinformationen

Das Produkt i-effect® *SIGG nutzt die folgenden nach SigG bestätigten Produkte, die von Dritten hergestellt werden und nicht Bestandteil dieser Erklärung sind:

Produktklasse	Bezeichnung	Beschreibung + Registriernummer der Bestätigung
SSEE	D-Trust, D-TRUST multiscard (D-Trust c-card V2.1) (2048-bit)	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 dem Nachtrag zur Nr. 1 zur Bestätigung vom 06.02.2007, Konfiguration A
Kartenleser	Chipkartenleser SCM SPR 532, Firmware Version 5.10	Kartenlesegerät mit Eingabe-Tastatur für PIN, Registrierungsnummer: BSI.02080.TE.10.2006

Tabelle 2: Zusätzliche Produkte

3 Funktionsbeschreibung

Das Produkt i-effect® *SIGG ist eine Teilkomponente einer Softwareanwendungskomponente entsprechend §2 Nr. 11 SigG, die elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zuführt. Das Produkt versetzt den Anwender vor allem in die Lage, beliebige Dateien sowie im Besonderen PDF-Dokumente und EDIFACT-Dateien im Massenbetrieb qualifiziert signieren zu lassen.

i-effect® *SIGG ist das Signaturserver-Modul von i-effect® - ,Die integrierte Lösung für IBM System i' :

- i-effect® - ,Die integrierte Lösung für IBM System i' - dient hier konzeptionell als Client zur Erstellung von Signatur-Aufträgen.
- i-effect® *SIGG (Server) ist die eigentliche Softwareanwendungskomponente zur Erzeugung von qualifizierten elektronischen Signaturen.

i-effect® ist aufgrund dessen nicht Gegenstand dieser Herstellererklärung.

Die Signatur von Dateien/Dokumenten erfolgt PKCS#7-bzw. PKCS#1-konform und wird je nach Auswahl

- in einer separaten Signaturdatei des Typs P7S gespeichert,
- zusammen mit den signierten Daten in einer Datei des Typs P7M gespeichert,
- in ein PDF-Dokument der Version 1.3 bis 1.6 integriert,
(Die integrierte Signatur ist kompatibel mit Adobe Acrobat Reader Version 6.x. Die Software Adobe Acrobat Reader Version 6.x ist nicht Gegenstand dieser Herstellererklärung.)
- gemäß den Vorgaben der ISO-Norm 9735, Second Edition 2002-07-01 (Part 5 und 6) in die entsprechende EDIFACT-Struktur integriert (Zur Zeit werden noch nicht alle Varianten von signierten EDIFACT-Dateien unterstützt).

An i-effect® *SIGG werden Signatur-Aufträge von i-effect® übergeben, die die zu signierende/n Datei/en, das Zielverzeichnis samt Ausgabedateiname/n, die Art der Signatur und im Falle einer zu integrierenden Signatur in ein PDF-Dokument die Darstellungsweise der Signatur (Sichtbarkeit der Signatur, Anzeige einer firmenspezifischen Grafik) enthalten.

Signiert wird mit Hilfe einer konfigurierten PKCS#11-Bibliothek, die die zu signierenden Daten der Softwareanwendungskomponente an die sichere Signaturerstellungseinheit übergibt. Die erzeugte Signatur wird gemäß des Signatur-Auftrages unter dem angegebenen Ausgabepfad separat bzw. zusammen mit den signierten Daten gespeichert oder in die PDF- bzw. EDIFACT-Datei integriert. Die verwendete PKCS#11-Bibliothek sowie die sichere Signaturerstellungseinheit ist nicht Gegenstand dieser Herstellererklärung.

Eine durch eine autorisierte Person aktivierte Signatur-Sitzung für die Durchführung von Signatur-Aufträgen ist entweder bis zum Erreichen eines definierten Zeitpunkts oder bis zum Erreichen einer definierten Anzahl an durchgeführten Signaturen gültig.

Die Aktivierung einer Sitzung erfolgt durch die PIN-Eingabe einer autorisierten Person am Kartenlesegerät der sicheren Signaturerstellungseinheit. Das erneute Aktivieren einer Sitzung kann nur durch die wiederholte PIN-Eingabe der autorisierten Person erfolgen. Ein Zwischenspeichern der PIN durch die Softwareanwendungskomponente ist nicht möglich. Das Kartenlesegerät ist nicht Gegenstand dieser Herstellererklärung.

Für die Erzeugung einer qualifizierten elektronischen Signatur wird der Einsatz einer für die Massensignatur geeigneten, sicheren Signaturerstellungseinheit und eines Kartenlesegerätes

vorausgesetzt, die den Vorgaben des Signaturgesetzes entsprechen und von der Bundesnetzagentur zugelassen sind.

Während des gesamten Signaturvorgangs werden die einzelnen Verarbeitungsschritte seitens i-effect® protokolliert. Diese einzelnen Verarbeitungsschritte eines Auftrages können jederzeit eingesehen werden. Im Erfolgsfall wird ein Auftrag mit einem OK-Status abgeschlossen. Im Fehlerfall wird der Auftrag mit einem ERROR-Status beendet.

4 Erfüllung des Signaturgesetzes und der Signaturverordnung

Im Folgenden werden die Anforderungen, die i-effect *SIGG als Teilkomponente einer Signaturanwendungskomponenten entspricht, dargestellt. Durch den Charakter einer Teilkomponente werden im Folgenden nur die Passagen des SigG bzw. SigV angeführt, die durch die Teilkomponente umgesetzt werden.

Die Anforderungen für die Erzeugung einer qualifizierten elektronischen Signatur nach §17 Absatz 2 Satz 1 Signaturgesetz

„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.“

wird durch das Logging von i-effect *SIGG erfüllt. Der Werdegang eines Signatur-Auftrags wird von dessen Eingang bis zur Beendigung der Verarbeitung protokolliert. Dieses Log kann jederzeit in i-effect *SIGG zur Anzeige gebracht werden. Ein Pausierungs-Mechanismus gewährleistet, dass Aufträge vor der eigentlichen Signatur angehalten werden können, um den Auftrag zu überprüfen (zu signierende Daten, Art der durchzuführenden Signatur).

Das Log zeigt sowohl die Erzeugung einer qualifizierten Signatur eindeutig an als auch auf welche Dateien sich die Erstellung der Signatur bezieht.

Abweichend von §17 Absatz 2 Satz 1 erfolgt die Anzeige der zu signierenden Daten nach einem eingestellten Wahrscheinlichkeitsprinzip.

Die Wahrscheinlichkeit, dass ein Dokument zur Anzeige gebracht wird, kann durch den Benutzer eingestellt werden (Bereich: 5 – 100%).

i-effect® *SIGG erfüllt die Anforderungen des § 15 Absatz 2 Nr. 1 Signaturverordnung:

„(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

- 1. bei der Erzeugung einer qualifizierten elektronischen Signatur*
 - a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,*
 - b) eine Signatur nur durch die berechtigt signierende Person erfolgt,*
 - c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und“*

Die Authentifizierung gegenüber der sicheren Signaturerstellungseinheit kann nur durch die PIN(Identifikationsdaten)-Eingabe des Signaturschlüsselinhabers direkt über die Tastatur des Kartenlesegerätes erfolgen. Eine Eingabe der PIN über die Computertastatur ist nicht möglich. Eine Weitergabe des PIN an andere Personen als den Signaturschlüsselinhaber ist nicht zulässig. Durch die im Folgenden definierten Einsatzbedingungen/-umgebung haben nur berechtigte Personen Zugang zu der Teilsignaturanwendungskomponente. Aufgrund dessen können auch nur berechtigte Personen die Erzeugung von Signaturen veranlassen.

Die Auflage bei Massensignaturen die Signaturvorgänge zeitlich bzw. in der Anzahl zu begrenzen wird durch die Teilsignaturanwendungskomponente erfüllt. Die berechtigte Person muss vor der eigentlichen Freigabe der Erzeugung von Signaturen bestätigen, dass die eingestellt Zeit bzw. Anzahl für Signaturen den eigenen Vorstellungen entspricht.

Die Anforderung des §15 Absatz 4 der Signaturverordnung

„(4) Sicherheitstechnische Veränderungen an technischen Komponenten nach den Ab-sätzen 1 bis 3 müssen für den Nutzer erkennbar werden.“)

sind durch den Einsatz der Softwareanwendungskomponente in einer sicheren Systemumgebung erfüllt.

Sicherheitstechnische Veränderungen an der Software können erkannt werden, da sich das System (IBM System i5 mit IXS für i-effect® *SIGG) in einer zugriffssicheren Betriebsumgebung befindet und der Netzwerkzugang durch Virens Scanner und Firewalls abgesichert ist.

Darüber hinaus ist die Software digital signiert. Eine Prüfung während des Startvorgangs von i-effect® *SIGG überprüft die Unversehrtheit der Softwareanwendungskomponente. Eine erkannte Veränderung an i-effect® *SIGG wird umgehend durch einen Warnhinweis angezeigt.

Voraussetzung für die Erfüllung der Anforderungen ist die Einhaltung der unter 5 ff spezifizierten Einsatzbedingungen.

5 Einsatzbedingungen

Diese Erklärung gilt für den Einsatz von i-effect® *SIGG innerhalb der im Folgenden erläuterten sicheren, geschlossenen Systemumgebung innerhalb einer IBM System i. Die unter Punkt 3 und 4 genannten Funktionen bzw. Anforderungen sind nur dann erfüllt, wenn die folgenden Einsatzbedingungen gewährleistet sind.

5.1 Auslieferungszustand

Das Produkt i-effect® *SIGG V1R3 wird für eine Kombination aus IBM System i mit IXS (Integrated xSeries Server for System i) angeboten.

5.1.1 Hardware

- IXS PCI-Karte, Typ: 481x oder Typ: 2892
- Eines oder mehrere Kartenlesegeräte vom Typ SCM SPR 532

5.1.2 Software

i-effect® - ,Die integrierte Lösung für IBM System i':

i-effect® wird auf einer nur einmal beschreibbaren CD mit einer Installationsroutine für IBM System i, Betriebssystem V5R3 oder höher ausgeliefert.

i-effect® *SIGG:

i-effect *SIGG wird als vorkonfiguriertes Image für den Einsatz auf einem IXS für IBM System i auf einer nur einmal beschreibbaren DVD ausgeliefert.

Das Image beinhaltet eine MS Windows 2003 Server-Installation inklusive vorinstallierten Treibern für den Kartenleser SCM SPR 532, PKCS#11-Bibliothek, installierter Java-Runtime Edition Version 5.x, Adobe Acrobat Reader 8.x und der Softwareanwendungskomponente i-effect® *SIGG.

Existiert bereits ein IXS mit installiertem MS Windows Server-Betriebssystem, kann i-effect *SIGG von der Webseite <http://www.i-effect.de> aus dem Downloadbereich eine Passwort-geschützte ZIP-Datei heruntergeladen oder in Form einer CD zugesandt werden (sowohl das ZIP als auch die CD enthalten die Setup-Datei, die Signaturdatei sowie das Integritäts-Prüf tool). In diesen beiden zuletzt genannten Fällen (Download bzw. Zusendung per CD) ist eine Integritäts-Prüfung erforderlich.

Da die Installationsdatei von i-effect *SIGG vor der Auslieferung signiert wurde, ist die Gültigkeit der Signatur zunächst zu prüfen. Eine Anleitung zur Überprüfung der Integrität von i-effect *SIGG wird im Handbuch beschrieben.

5.2 Installation

Die Installation von i-effect® *SIGG erfolgt in der Regel durch einen Mitarbeiter der menten GmbH oder einen autorisierten Partner.

Im Vorfeld der Installation werden die Gegebenheiten der Einsatzumgebung anhand der Anforderungen, die in der Herstellererklärung festgelegt sind, geprüft.

Die Software kann auch nach Zusendung einer Original-CD oder dem Download der Software von der firmeneigenen Webseite direkt von dem Benutzer installiert werden. Die Installation darf erst erfolgen, wenn die Gegebenheiten der Einsatzumgebung und des Einsatzbereiches erfüllt sind und eine vorherige Integritätsprüfung der Installations-Datei erfolgt ist.

Weiterführende Informationen bezüglich der Installation können dem Handbuch entnommen werden.

5.3 Technische Einsatzumgebung

i-effect® - ,Die integrierte Lösung für IBM System i' :

Die Basisvoraussetzung ist das Vorhandensein einer IBM System i mit einem installierten i5/OS Betriebssystem ab Version V5R3.

Die Voraussetzung für die Erzeugung von Signatur-Aufträgen wird durch die Installation von i-effect® - ,Die integrierte Lösung für IBM System i' ab Version V1R3 geschaffen.

i-effect® *SIGG:

Als Einsatzumgebung für i-effect® *SIGG ist ein IXS (Integrated xSeries Server for System i) vom Typ 481x (Intel Pentium M-basierend) oder vom Typ 2892 (Intel Xeon-basierend) in Form einer PCI-Karte vorgesehen. Diese Karte wird in die IBM System i eingesetzt. Auf diese Weise wird bereits konzeptionell eine sichere Systemumgebung geschaffen.

Als Betriebssystem des IXS ist MS Windows 2003 Server vorgesehen. Weitere Softwarevoraussetzungen werden durch die vorinstallierte PKCS#11-Bibliothek für den Zugriff auf die sichere Signaturerstellungseinheit sowie die Java Runtime Edition Version 5.x geschaffen.

Als Chipkartenterminals zur Authentifizierung an der eingesetzten sicheren Signaturerstellungseinheit kommen Geräte des Typs SCM SPR 532 zum Einsatz, die durch die Bundesnetzagentur nach den Vorgaben des Signaturgesetzes und der Signaturverordnung geprüft und bestätigt wurden.

Als sichere Signaturerstellungseinheiten können nur personalisierte Signaturkarten eingesetzt werden, die für Massensignatur geeignet sind und den Vorgaben des Signaturgesetzes und der Signaturverordnung (geprüft und bestätigt durch die Bundesnetzagentur) entsprechen. Daraus ergibt sich zur Zeit nur der Einsatz von Signaturkarten der Firma D-Trust vom Typ D-TRUST multiscard (D-Trust c-card V2.1) mit 2048-bit.

Autorisierte Benutzer von i-effect® *SIGG müssen dafür Sorge tragen, dass die technische Einsatzumgebung (wie hier unter Punkt 5.3 beschrieben) erhalten bleibt.

5.4 Administrative Einsatzumgebung

Die MS Windows 2003 Server-Installation darf für keine anderen Dienste oder Programme außer den Signaturdienst verwendet werden.

Die Installation von Software, die nicht Teil des Auslieferungszustandes ist bzw. nicht der Wartung der Softwareanwendungskomponente dient, bedeutet den Verlust der Gewährleistung der gesetzeskonformen Funktion von i-effect® *SIGG.

Auf der IXS dürfen nur die für den Betrieb notwendigen Benutzerkonten angelegt sein, um autorisierten Benutzern die Kontrolle und Wartung des Systems zu ermöglichen.

Die IXS darf nicht direkt mit dem Internet verbunden werden. Zugriffe bzw. Angriffe aus dem Internet müssen praktisch unmöglich sein und durch geeignete Schutzmechanismen wie den Einsatz von Virenschaltern und einer Firewall verhindert werden.

Ist die IXS an ein Intranet angebunden, muss diese Verbindung durch geeignete Schutzmechanismen wie den Einsatz von Virenschaltern und einer Firewall abgesichert werden, so dass man mögliche Angriffe auf das System erkennen und unterbinden kann.

Die Systemzeit muss korrekt sein.

Für die Kommunikation zwischen i-effect® auf IBM System i und i-effect® *SIGG auf IXS wird die Verwendung des virtuellen Netzwerkadapters empfohlen, um eine abgeschirmte, sichere Verbindung für die Übertragung der Signaturaufträge zu gewährleisten. Eine Manipulation von außerhalb der IBM System i wird mit dieser Methode verhindert.

(Der virtuelle Netzwerkadapter wird von IBM System i einem IXS zur Verfügung gestellt. Eine entsprechende Konfiguration vorausgesetzt, werden Datenströme nur innerhalb des Systems übertragen und können nicht in ein externes Netz [z.B. Intranet] gelangen.)

Bei Verwendung der physischen Netzwerkadapter sind die Einsatzbedingungen für den Anschluss an das Intranet bzw. Internet zu beachten, die einen Schutz durch einen Virenschalter und einer Firewall voraussetzen.

5.5 Organisatorische Einsatzumgebung

Die Eingabe der PIN am Kartenlesegerät darf nur durch den Schlüsselinhaber erfolgen.

Die IBM System i mitsamt der IXS befindet sich in einem Raum, zu dem nur autorisierte Personen Zugang haben.

5.6 Einsatzbereich

Die im Vorfeld beschriebene Einsatzumgebung definiert grundlegend den Einsatz von i-effect *SIGG in einem **geschützten Einsatzbereich**.

Es wird vorausgesetzt, dass während des Betriebes von i-effect *SIGG nur autorisierte Personen Zugriff auf alle signaturprozess-relevanten Aspekte haben.

Für einen sicheren Einsatz von i-effect *SIGG gilt es folgendes zu beachten:

- Die Installation von i-effect *SIGG darf nur von dem Originaldatenträger aus erfolgen, sofern es sich bei der Installationsdatei von i-effect *SIGG nicht um eine Download-Version handelt. Aus Sicherheitsgründen sollte die Setup-Datei auf ihre Integrität geprüft werden (eine Anleitung für die Integritätsprüfung finden Sie im Handbuch).
- Bei der Verwendung der Download-Version der Installationsdatei von i-effect *SIGG hat eine Prüfung der Integrität dieser Datei vor der Installation zu erfolgen (eine Anleitung für die Integritätsprüfung finden Sie im Handbuch).
- Das ein durch die Bundesnetzagentur bestätigtes Kartenlesegerät eingesetzt wird.
- Das eine durch die Bundesnetzagentur bestätigte sichere Signaturerstellungseinheit verwendet wird.
- Sicherstellung, dass nur autorisierte Personen Zugriff auf der IXS und das dort installierte Windows 2003 Server-System und dessen Dienste besitzen.
- Sicherstellung, dass die verwendeten Freigaben/Ordner und zu signierenden Daten nur unter der Kontrolle von autorisierten Personen liegen.
- Sollte der IXS Zugriff auf das Intranet und/oder Internat Zugriff haben, dass das System durch einen Virenschalter und eine Firewall geschützt ist.
- Das i-effect *SIGG für das Einsatzland „Deutschland“ konfiguriert ist.

6 Updates

Mögliche Updates für die Teilsignaturkomponente i-effect *SIGG können über die Internetseite per Download oder per Datenträger (eine nur einmal beschreibbare CD) bezogen werden. Updates

beeinflussen keine der Funktionalitäten, die Gegenstand dieser Herstellererklärung sind. Eine Installation eines Updates setzt die vorherige Deinstallation der älteren i-effect *SIGG - Installation voraus.

Enthalten Updates Funktionalitäten, die Gegenstand der Herstellererklärung sind, werden diese in einer neuen, überarbeiteten Version der Herstellererklärung aufgeführt und erläutert.

7 Algorithmen und zugehörige Parameter

Der Hashwert der zu signierenden Daten einer Datei bzw. der Datenbereiche eines PDF-Dokuments wird mit der Hashfunktion SHA-1 berechnet.

Für die Erzeugung der Signatur auf Basis von SHA-1 wird das RSA Signaturverfahren der sicheren Signaturerstellungseinheit mit Schlüssellängen von 2048 Bit verwendet.

Die Länge des Schlüssel hängt von dem auf der Signaturkarte gespeicherten qualifizierten Zertifikat ab.

Nach Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung vom 22. Februar 2007, veröffentlicht am 12. April 2007 im Bundesanzeiger Nr. 69, S. 3759 durch die Bundesnetzagentur ist:

- die Verwendung von SHA-1 nach heutigem Kenntnisstand bis auf weiteres bis Ende 2009 für qualifizierte elektronische Signaturen geeignet.
- die Verwendung des Signaturverfahrens RSA mit Schlüssellängen von 2048 Bit über das Jahr 2012 hinaus bis auf weiteres geeignet.

8 Gültigkeit der Herstellererklärung

Die vorliegende Herstellererklärung ist bis zum Widerruf durch die menten GmbH oder der nach §3 SigG zuständigen Behörde bzw. bis zum Ablauf der Vertrauenswürdigkeit des Hash-Algorithmus SHA-1 gültig, längstens jedoch bis zum 31.12.2009.

9 Zusatzdokumentation

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

- Sicherheitstechnische Produktvorgabe und Testdokumentation – Version 1.0
- Handbuch i-effect® *SIGG – Version 1.0

10 Inhalt der Erklärung

Diese Herstellererklärung dient ausschließlich dazu, die Erfüllung der im Signaturgesetz und der in der Signaturverordnung festgeschriebenen Anforderungen zu bestätigen. Eine Übernahme weiterer Garantien und Zusicherungen in Hinblick auf die Produkteigenschaften ist damit nicht verbunden. Vor allem sei darauf hingewiesen, dass die genannten Anforderungen nur unter Einhaltung der Einsatzbedingungen unter Punkt 5 durch den Nutzer erfüllt sind.

- Ende der Herstellererklärung -