

## Herstellereklärung

Der Hersteller

### **Mentana-Claimsoft AG**

Spreenhagener Str. 16  
D-15528 Spreenhagen

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

### **Proof-It Version 4.1**

eine „Teil- Signaturanwendungskomponente“ (Software) im Sinne von § 2 Nr. 11 SigG ist, die es ermöglicht,

- qualifizierte Zeitstempel für Lokal gespeicherte Dateien von einem Zertifizierungsdienstanbieter anzufordern

und die den Anforderungen des Signaturgesetzes und der Signaturverordnung genügt.

**Diese Erklärung ersetzt die Herstellereklärung vom 10.12.2006 veröffentlicht im Amtsblatt der Bundesnetzagentur Nr. 2/2007 vom 24.01.2007, Mitteilung Nr. 87, Seite 2753.**

Unbeschadet der Veröffentlichung im Amtsblatt der Bundesnetzagentur (vormals Regulierungsbehörde für Post und Telekommunikation) gemäß §17 Abs.4 Satz 3 SigG wird ein Widerruf oder eine Erneuerung dieser Erklärung unter

<http://www.mentana-claimsoft.de> veröffentlicht.

Spreenhagen b. Berlin, 26.05.2008

Dr. Inf. Ralf Hesse  
Leiter Softwareentwicklung

Dipl. Ing. Axel Janhoff  
Vorstand

<sup>1</sup> Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. S. 876, Jahrgang 2001 Teil I Nr. 22) in der Fassung des 1.SigÄndG vom 04. Januar 2005 zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179).

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) in der Fassung des 1.SigÄndG vom 04. Januar 2005 (BGBl. I S. 2) zuletzt geändert durch Art. 9 Abs. 18 G v. 23.11.2007.

# Herstellereklärung



Teil-Signaturanwendungskomponente

**Proof-It Version 4.1**

Deckblatt/ Inhaltsverzeichnis

Seite 2 von 11

**HP.BK.10.06.002**

Deckblatt.....	1
<b>1. Handelsbezeichnung.....</b>	<b>3</b>
<b>2. Funktionsbeschreibung .....</b>	<b>3</b>
<b>2.1 Anfordern qualifizierter Zeitstempel.....</b>	<b>4</b>
<b>2.2 Verifikation qualifizierter Zeitstempel.....</b>	<b>5</b>
<b>2.2.1 Prüfungsablauf.....</b>	<b>5</b>
<b>2.2.2 Vertrauensanker.....</b>	<b>5</b>
<b>2.3 Unterstützte Ausführungsumgebung .....</b>	<b>6</b>
<b>3. Erfüllung der Anforderungen des SigG und der SigV.....</b>	<b>6</b>
<b>3.1 Erfüllte Anforderungen.....</b>	<b>6</b>
<b>3.2 Einsatzbedingungen.....</b>	<b>7</b>
<b>3.2.1 Einrichtung der Rechners zur Beweissicherung/ Archivierung .....</b>	<b>7</b>
<b>3.2.2 Betrieb/Nutzung .....</b>	<b>7</b>
<b>3.2.2.1 Potentielle Bedrohungen.....</b>	<b>7</b>
<b>3.2.2.2 Maßnahmen in der Einsatzumgebung.....</b>	<b>8</b>
<b>a) Auflagen zur Anbindung an das Internet .....</b>	<b>8</b>
<b>b) Auflagen zur Anbindung an ein Intranet.....</b>	<b>8</b>
<b>c) Auflagen zur Sicherheit der IT-Plattform und Applikationen.....</b>	<b>8</b>
<b>3.2.2.3 Schutz vor unbefugter Veränderung .....</b>	<b>9</b>
<b>3.2.3 Wartung/Reparatur .....</b>	<b>9</b>
<b>3.4 Auflagen zur Auslieferung und Installation des Produktes .....</b>	<b>9</b>
<b>4. Begleitende Dokumente.....</b>	<b>10</b>
<b>5. Gültigkeit der Herstellereklärung.....</b>	<b>11</b>

Dokumenten -Version	Bearbeiter	Inhalt	Datum
2.01	Raoul Kirmes	Übernahme Stand Amtsbaltt BNetzA	15.11.2007
2.02	Raoul Kirmes	Überarbeitung Algorithmen	30.03.2008
2.03	Raoul Kirmes	Ergänzung SSEE/Leser	15.05.2008
2.04	Raoul Kirmes	Umsetzung aktuelles Release	17.05.2008
2.05	Dr. Ralf Hesse	Prüfung	18.05.2008
2.06	Axel Janhoff	Autorisierung zur Veröffentlichung	25.05.2008

## 1. Handelsbezeichnung

Die Handelsbezeichnung lautet: **Proof-It® Version 4.1**

Auslieferung:

**Proof-It®** wird sowohl auf einer CD als auch als vorgefertigtes Installationspaket<sup>3</sup> ausgeliefert. Auf dieser CD bzw. in diesem Paket befinden sich eine Installationsroutine für **Proof-It®**, die erforderlichen Systemkomponenten, bestehend aus Microsoft® .NET Framework Software Development Kit (SDK), Version 1.1 und der Datenbank Microsoft® Data Access Components (MDAC) 2.8 sowie ein Handbuch zur Installation und Administration in elektronischer Form.

Hersteller: **Mentana-Claimsoft AG**  
Spreenhagener Str. 16  
15528 Spreenhagen b. Berlin  
Tel. : 033633/691188  
info@mentana.de

## 2. Funktionsbeschreibung

Die Software **Proof-It®** ist eine Teil-Signaturanwendungskomponente<sup>4</sup> im Sinne von § 2 Nr. 11 SigG, die elektronische Daten durch Anforderung „**qualifizierter Zeitstempel**“ nach § 2 Nr. 14 SigG in eine revisionssichere (§ 238ffHGB) wie auch rechtssichere (§126a BGB i.v.m. § 371a ZPO) elektronische Form bringt. Hauptanwendungsfall der Software **Proof-It®** ist die Beweissicherung von elektronischen Bildern und sonstigen Dokumenten oder Dateien für Gutachter, Architekten und Bauherren im Rahmen des Mängelmanagements.

<sup>3</sup> Im Rahmen des Vertriebes über Online-Shops

<sup>4</sup> „Teil“ einer Signaturanwendungskomponente da nur die ausdrücklich genannten Funktionen erbracht werden.

## 2.1 Anfordern qualifizierter Zeitstempel

Jegliche Dokumente (Dateien) können durch den Benutzer für Archivierungszwecke oder für Beweissicherungszwecke mit einem qualifizierten Zeitstempel (elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 des SigG und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 SigG erfüllt) gesichert werden.

Dazu wird über eine verschlüsselte Verbindung (HTTPS) auf einen passwortgeschützten Benutzeraccount, einer geschlossenen Benutzergruppe, bei [www.signaturportal.de](http://www.signaturportal.de) mittels eines Web-Service zugegriffen. Die Realisierung des Web-Service basiert auf den offenen Standards Simple Object Access Protocol - „SOAP“ (siehe <http://www.w3.org/TR/SOAP/>) sowie Web-Service- Description-Language – „WSDL“ (siehe <http://www.w3.org/TR/wsdl>)

Der Hash-Wert (SHA-256 oder SHA 512) der betreffenden Datei wird durch **Proof-It**<sup>®</sup> ermittelt und an [www.signaturportal.de](http://www.signaturportal.de) übermittelt. Das Portal [www.signaturportal.de](http://www.signaturportal.de) unterhält gesicherte Verbindungen zu den nachfolgend genannten Zertifizierungsdiensteanbietern, denen der übermittelte Hash-Wert der Datei eingeliefert wird. Die Zeitstempeldatei (Antwort des Zertifizierungsdiensteanbieters) wird zurück an den Benutzer der Software **Proof-It**<sup>®</sup> übermittelt und mit einem Referenzverweis zum Ursprungsdokument in die Anwendungsdatenbank geschrieben. Das Ursprungsdokument wird bei Anzeige in der Datenbank durch einen Symbol markiert, um anzuzeigen, dass ein Zeitstempel vorliegt. Durch eine interne Datenbankroutine wird verhindert, dass die Ursprungsdatei nach der Zeitstempelung überschrieben, vom Ursprungsdokument getrennt oder sonst verändert wird (Schreibschutz).

Per Stand 2008 werden Zeitstempel der folgenden Zertifizierungsdienste ausgeliefert.

a) **AuthentiDate International AG**<sup>5</sup>

Großenbaumer Weg 6

40472 Düsseldorf

---

<sup>5</sup> Gütezeichen RegTP Nr. Z0015, erteilt am 9. November 2001.

b) **Deutsche Post Com GmbH<sup>6</sup>**

Geschäftsfeld Signtrust

Tulpenfeld 9

53113 Bonn

## 2.2 Verifikation qualifizierter Zeitstempel

### 2.2.1 Prüfungsablauf

Nach Aufforderung durch den Benutzer überprüft **Proof-It<sup>®</sup>** die Zeitstempel auf folgende Punkte:

- Kann die Zertifikatskette zum ausstellenden ZDA<sup>7</sup> aufgebaut werden?
- Ist die ausstellende Organisation ein ZDA<sup>8</sup>?
- War das Zertifikat zum Zeitpunkt der Signaturerstellung gültig<sup>9</sup>?

Das Ergebnis der Zertifikatsprüfung wird dem Benutzer tabellarisch dargestellt.

### 2.2.2 Vertrauensanker

Das Vertrauens in ein Zertifikat bzw. eine Zertifikatskette basiert auf dem Vertrauen in die ausstellende oder oberste CA als sog. "Vertrauensanker" (trustanchor), welche Ausgangspunkt für die Validierung eines Zertifikats oder einer Zertifikatskette ist.

Für die vorbeschriebenen Zeitstempel gilt folgender Vertrauensanker:

1) qualifizierte Signaturen von ZDA´s nach § 15 Abs.1 SigG:

a) Hierarchisches Top-Down-Modell im Bereich qualifizierter Signaturen mit Anbieterakkreditierung des ausstellenden ZDA:

- Ebene 0: BNetzA (RegTP) als Wurzel (Top-Level-CA, Root-CA u.Ausstellerzertifikat)
- Ebene 1: ZDA (Unterzeichnerzertifikat)

b) Vertrauensmodus:

- "Single CA"

c) **Es kann nur dem öffentlichen Schlüssel („Public-Key RegTP“) der BNetzA, vormals RegTP, vertraut werden die im Bundesanzeiger veröffentlicht werden.**

Die Zertifikate können daneben elektronisch über <http://www.nrca-ds.de/> abgerufen werden.

<sup>6</sup> Gütezeichen RegTP Nr. Z0002, erteilt am 17. September 2004.

<sup>7</sup> „ZDA“ steht für Zertifizierungsdiensteanbieter gemäß SigG wie oben benannt.

<sup>8</sup> ist das ausstellende ZDA ein Anbieter gemäß § 4 Abs.3 SigG oder § 15 Abs.1 SigG..

<sup>9</sup> Die Prüfung erfolgt im Kettenmodell. Angezeigt wird „gültig/ ungültig/unbekannt“

## **2.3 Unterstützte Ausführungsumgebung**

Die Software **Proof-It**<sup>®</sup> kann unter den Betriebssystemen

- Windows 2000 Professional / Server
- Windows XP Home / Professional / MCE
- Windows 2003 Server / Advanced Server

eingesetzt werden.

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

### **3.1 Erfüllte Anforderungen**

Die Software **Proof-It**<sup>®</sup> erfüllt die Anforderungen nach § 17 Abs. 2 SigG i.v.m. § 17 Abs. 3 Nr. 3 SigG.

Es werden die folgenden Eigenschaften zugesichert:

1. eindeutige Anzeige und Feststellbarkeit der Daten, die der Sicherung durch Zeitstempel zugeführt werden sollen (vor Abruf der Zeitstempel),
2. eindeutige Anzeige und Feststellbarkeit der Daten die durch Zeitstempel gesichert wurden (nach Sicherung durch Zeitstempel bei jedem Abruf aus der Datenbank),
3. Feststellbarkeit der Ursprungsdaten zum Zeitstempel, des Unverändertseins der Daten seit Zeitstempelsicherung, der Zuordnung zum qualifizierten Zeitstempel sowie
4. bei Bedarf Anzeige des Inhalts der Zeitstempeldatei (Anzeige des Hash der Ursprungsdatei, der amtlichen Zeit, Zertifikatsinformationen des ZDA)

Im Sinne von §15 Abs.2 ff SigV insbesondere:

- eindeutige Anzeige der Zeitstempelsignatur und eindeutige Erkennbarkeit der Gültigkeit der Zertifikate welche dem Zeitstempel zu Grunde lagen sowie

Im Sinne von §15 Abs.4 SigV insbesondere

- Erkennbarkeit von sicherheitstechnischen Veränderungen an der Teilkomponente Proof-It.

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

## 3.2 Einsatzbedingungen

### 3.2.1 Einrichtung der Rechners zur Beweissicherung/ Archivierung

Die Installation des Rechners erfolgt durch den Kunden bzw. einen betreuenden Techniker. Es muss vorausgesetzt werden, dass diejenige Person, die das System installiert, die entsprechende Eignung zur Installation und Inbetriebnahme besitzt.

### 3.2.2 Betrieb/Nutzung

Der Betrieb des Rechners muss derart abgesichert sein, dass nur autorisierte Nutzer Zugang zum System erhalten. Insbesondere ist die Passwortgeschützte Nutzerverwaltung einzusetzen.

Ein Installations- und Administrationshandbuch, in dem entsprechende Maßnahmen dokumentiert werden, liegt der Software in elektronischer Form bei.

#### 3.2.2.1 Potentielle Bedrohungen

Die Sicherheit der Teil-Signaturanwendungskomponente **Proof-It**<sup>®</sup> ist potentiell bedroht durch

- Angriffe über Kommunikationsnetze<sup>10</sup>,
- Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger<sup>11</sup> und
- Fehler/Manipulationen bei Installation, Betrieb/Nutzung und Wartung/Reparatur.

Grundlage dieser Erklärung ist der Einsatz von **Proof-It**<sup>®</sup> in einem geschützten Einsatzbereich. Für den sicheren Einsatz von **Proof-It**<sup>®</sup> und zur Verhinderung von erfolgreichen Angriffen mit den Zielen, dass:

- Daten vom Zeitstempel getrennt werden
- Ein fehlerhafter/falscher Hashwert für ein Ursprugsdokument übermittelt wird mit der Folge, dass die gewünschte Beweis-/Revisionsicherheit nicht erreicht werden kann.

sind die folgenden Auflagen zu beachten:

<sup>10</sup> Spezifizierte Bedrohung gemäß Fußnote 15 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

<sup>11</sup> Spezifizierte Bedrohung gemäß Fußnote 16 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

### 3.2.2.2 Maßnahmen in der Einsatzumgebung

Der Rechner wird in einem geschützten Bereich<sup>12</sup> betrieben, der eine Kontrolle und Dokumentation des Zugangs zur Teil-Signaturanwendungskomponente beinhaltet.

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

Für die Internetanbindung des Systems muss sichergestellt sein, dass kein Zugriff auf dieses System aus ungesicherten Netzen möglich ist. Die Netzwerkverbindung muss durch den Einsatz einer konfigurierten Firewall gesichert werden. Durch den Benutzer ist zu gewährleisten, dass Angriffe aus dem Internet erkannt und soweit möglich unterbunden werden.

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

Wenn das eingesetzte System innerhalb eines Intranets 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 **Proof-It**<sup>®</sup> muss sich davon überzeugen, dass keine Angriffe auf das Anwendungssystem und die dort installierten Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf dem Rechner installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf dem Rechner keine Viren oder Trojanischen Pferde eingespielt werden können,
3. die Hardware des Rechners nicht unzulässig verändert werden kann oder
4. ein Direktzugriff auf die Datenbank ohne Nutzerauthentifizierung unterbleibt
5. Eine Benutzerauthentifizierung am Betriebssystem des Rechners ist notwendig. Bei Unterbrechung der Arbeiten ist eine Konsolensperrung notwendig, die eine erneute Authentifizierung beim nächsten Arbeiten erforderlich macht.

---

<sup>12</sup> Definierter Einsatzbereich gemäß Nr. 4.2 RegTP Dokument: Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten Version 1.1.

### 3.2.2.3 Schutz vor unbefugter Veränderung

Um eine Überprüfung der eingesetzten Teil-Signaturanwendungskomponente zu ermöglichen, veröffentlicht die Mentana-Claimsoft AG zu jeder Programmversion Referenz-Hashwerte der ausführbaren Dateien auf ihrer Webseite ([www.mentana-claimsoft.de](http://www.mentana-claimsoft.de)).

Die Versionsnummer und der Hashwert der eingesetzten **Proof-It**<sup>®</sup> Version lässt sich im Menü **Info** der Software anzeigen. Der SHA-256 Hashwert der aktuell ausgeführten Programmdatei wird zur Laufzeit berechnet und angezeigt. Dieser Hashwert kann vom Anwender mit dem veröffentlichten Referenz-Hashwert verglichen werden.

### 3.2.3 Wartung/Reparatur

Bei der Wartung und der Reparatur des Anwendungssystems gelten die Voraussetzungen der Erstinstallation (vergleiche Punkt 3.2.1). Bei Erkennen von Fehlern, die die Sicherheit der Teil-Signaturanwendungskomponente betreffen können, stellt die Mentana-Claimsoft AG umgehend aktualisierte Versionen der Programmkomponenten zur Verfügung. Die Anwender des Programms werden über die Webseite der Mentana-Claimsoft AG ([www.mentana-claimsoft.de](http://www.mentana-claimsoft.de)) über das Auftreten einer solchen Situation, unbeschadet einer ergänzenden Veröffentlichung, eines Widerruf oder einer Erneuerung der Herstellereklärung im Amtsblatt der Bundesnetzagentur (vormals Regulierungsbehörde für Post und Telekommunikation) gemäß §17 Abs.4 Satz 3 SigG informiert.

## 3.3 Algorithmen und zugehörige Parameter

Der verwendeten Hashalgorithmen SHA-256 und SHA-512 sind gemäß Anlage 1 Abs. I Nr. 2 SigV mindestens bis Ende 2014 geeignet (vgl. Bundesanzeiger Nr. 19, Seite 376 veröffentlicht am 05. Februar 2008). Der aktuell gültige sowie die jährlichen Aktualisierungen des Algorithmenkatalogs können auf der Website der Bundesnetzagentur unter:

[http://www.bundesnetzagentur.de/enid/65026a6ee5e22c71a33b5e7e1f6803d7.0/Veroeffentlichungen/Algorithmen\\_sw.html](http://www.bundesnetzagentur.de/enid/65026a6ee5e22c71a33b5e7e1f6803d7.0/Veroeffentlichungen/Algorithmen_sw.html)

eingesehen werden.

### **3.4 Auflagen zur Auslieferung und Installation des Produktes**

Die Teil-Signaturanwendungskomponente **Proof-It**<sup>®</sup> wird vom Hersteller als Produkt entweder auf CD oder als installationsfähiges Softwarepaket über das Internet ausgeliefert.

Die Teil-Signaturanwendungskomponente **Proof-It**<sup>®</sup> 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)
- Unterstützte Betriebssysteme sind Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server, Windows 2003 Enterprise Server, Windows XP.
- Laufzeitumgebung: Microsoft<sup>®</sup> .NET Framework Software Development Kit (SDK), Version 1.1
- Microsoft<sup>®</sup> Data Access Components (MDAC) 2.8 oder Microsoft<sup>®</sup> SQL Server 2000 Enterprise Edition

### **4. Begleitende Dokumente**

Für diese Herstellereklärung gelten folgende Begleitdokumente:

1. Sicherheitstechnische Produktvorgaben Proof-It (EVG) Version 4.1, Version 1.2, Stand 10.04.2008.
2. Spezifikation der Test- und Entwicklungsumgebung für Proof-It (EVG) Version 4.1, Version 1.2, Stand 10.04.2008.

### **5. Referenz**

Diese Erklärung ersetzt die Herstellereklärung vom 10.12.2006 veröffentlicht im Amtsblatt der Bundesnetzagentur Nr. 2/2007 vom 24.01.2007, Mitteilung Nr. 87, Seite 2753.

## **6. Gültigkeit der Herstellereklärung**

Diese Herstellereklärung ist bis zum Widerruf durch Mentana-Claimsoft AG bzw. bis zum Ablauf der Vertrauenswürdigkeit des Hashalgorithmen SHA-256 oder SHA 512 - angezeigt durch die Bundesnetzagentur (vormals Regulierungsbehörde für Telekommunikation und Post ([www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)) – gültig, längstens jedoch bis zum **31.12.2014**.

Dieses Dokument umfasst 11 Seiten.

Ende der Herstellereklärung.