

Bestätigung von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen¹
und §§ 11 Abs. 3 und 15 Signaturverordnung²

gültig bis: 31.12.2016³

Die
datenschutz cert GmbH⁴
Barkhausenstraße 2
27568 Bremerhaven

bestätigt hiermit gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 11 Abs. 3, 15 SigV, dass die

Technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component, Version 3.0.21“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

DSC.063.09.2010

Bremerhaven, den 19.11.2010

Dr. Sönke Maseberg
Geschäftsführer datenschutz cert GmbH



¹Gesetz 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).

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

³ Die Gültigkeit der Bestätigung kann sich verkürzen, wenn z. B. neue Feststellungen hinsichtlich der Sicherheit des Produktes oder der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

⁴ Die datenschutz cert GmbH ist von der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle, vgl. Amtsblatt Nr. 19 der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen vom 08.10.2008 unter der Mitteilung Nr. 605/2008.

Inhaltsverzeichnis

1.	Handelsbezeichnung des Produktes und Lieferumfang	4
1.1	Handelsbezeichnung	4
1.2	Auslieferung	4
1.3	Hersteller	4
1.4	Lieferumfang des Produktes	4
2.	Funktionsbeschreibung	4
2.1	Übersicht	4
2.2	Hinweis	5
2.3	Einsatzumgebung	5
2.4	Funktionsumfang	6
2.5	Sicherheitsfunktionen	6
2.5.1	SF.Time Stamps	6
2.5.2	SF.Card Management	8
2.5.3	SF.SigCreation	8
2.5.4	SF.Integrity	8
3.	Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung	8
3.1	Erfüllte Anforderungen	8
3.2	Explizit nicht erfüllte Anforderungen	9
3.3	Einsatzbedingungen	9
3.3.1	Anforderungen an die technischen Einsatzbedingungen	10
3.3.2	Auslieferung und Inbetriebnahme	11
3.3.3	Anforderungen an die organisatorische und administrative Einsatzumgebung	11
3.3.4	Anforderungen an die Konfiguration	12
3.4	Algorithmen und zugehörige Parameter	12
3.5	Prüfstufe und Mechanismenstärke	13
3.6	Gültigkeit	13
4.	Referenzen	13

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
0.9	10.09.2010		Erstellung	Dr. Maseberg Dr. Karper
0.91	15.11.2010		Überarbeitung aufgrund von Anmerkungen der BNetzA	Dr. Maseberg
1.0	19.11.2010		Finalisierung auf Version 1.0 nach Abnahme durch BNetzA	Dr. Maseberg

Dokumenten-Überwachungsverfahren

Status: Final	Prozess-/Dokumentbesitzer: Dr. Maseberg	Version: 1.0

Beschreibung des Produktes für qualifizierte elektronische Signaturen

1. Handelsbezeichnung des Produktes und Lieferumfang

1.1 Handelsbezeichnung

Technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component V3.0.21“

1.2 Auslieferung

CD-ROM

1.3 Hersteller

AuthentiDate Deutschland GmbH
Rethelstraße 47
40237 Düsseldorf / Germany
Handelsregisterauszug: HRB 41892

1.4 Lieferumfang des Produktes

Die technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component V3.0.21“ besteht aus folgenden Dateien:

- AD_TIMESTAMPER_3.0.21_Linux.zip
- AD_TIMESTAMPER_3.0.21_Linux.zip.cms
- AD_DOC_3.0.21_Linux.zip
- AD_DOC_3.0.21_Linux.zip.cms
- AD_SF_CT_Tool_3.0.21_Linux.zip
- AD_SF_CT_Tool_3.0.21_Linux.zip.cms

Zudem werden die folgenden Produktunterlagen mit ausgeliefert:

- „Handbuch zum sicheren Betrieb für Benutzer und Administratoren“, Version 1.6.2, 09.09.2010.
- „TSA Installation and Usage Handbook for Users and Administrators“, Version 1.4.2, 09.09.2010.

2. Funktionsbeschreibung

2.1 Übersicht

Im Betrieb als technische Komponente für Zertifizierungsdienste (TK) nimmt SLMBC 3.0.21 bei der Erstellung qualifizierter Zeitstempel Anforderungen zur Erstellung eines qualifizierten Zeitstempels entgegen und gibt einen qualifizierten Zeitstempel zurück, wobei der betreffende Hashwert und die gültige gesetzliche Zeit mitsamt der erforderlichen Genauigkeit unverfälscht in den qualifizierten Zeitstempel aufge-

nommen werden. Die hierzu notwendige Zeitinformation wird dabei von einer vertrauenswürdigen Zeitquelle aus der Umgebung der technischen Komponente für Zertifizierungsdienste geliefert. Der qualifizierte Zeitstempel wird in Form einer qualifizierten elektronischen Signatur ausgestellt, indem das zeitzustempelnde Datum samt der zugehörigen Zeitinformation und ihrer Genauigkeit mit Hilfe der sicheren Signaturerstellungseinheiten des den Zeitstempeldienst betreibenden Zertifizierungsdiensts signiert wird.

2.2 Hinweis

Aufgrund der Beschränkung der Evaluierung bezieht sich diese Bestätigung ausschließlich auf die technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component V3.0.21“

- für das Betriebssystem „Red Hat Enterprise Linux 5.1“ (Red Hat Enterprise Linux ist nach Common Criteria zertifiziert; Reportnummer CCEVS-VR-VID10286-2008),
- für die sicheren Signaturerstellungseinheiten
 - Telesec TCOS 3.0 Signature Card, Version 1.1, in der Ausprägung „Signature Card 3.0M, Version 1.0 & NetKey 3.0M, Version 1.0“, Bestätigungs-ID: TUVIT.93146.TE.12.2006,
 - D-Trust c-card, Version 2.3, bestätigt als Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature, Bestätigungs-ID: T-Systems.02182.TE.11.2006,
- für den Kartenleser⁵
 - „Reiner SCT cyberJack e-com, Version 3.0, Bestätigungs-ID: TUVIT.93155.TE.09.2008“.

Weitere Funktionalitäten – insb. für den Betrieb als Signaturanwendungskomponente – sind Gegenstand der Bestätigung DSC.002.08.2009.

2.3 Einsatzumgebung

Die technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component V3.0.21“ muss in einer isolierten Einsatzumgebung eingesetzt werden, vgl. Abs. 3.3.3.

⁵ Für den Betrieb der Kartenterminals wird ein Treiber benötigt. Der folgende Treiber (kein Teil des Produktes) wird als Bestandteil des Binärpakets ausgeliefert:

Kartenterminal:	Reiner SCT cyberJack® e-com V3.0
Treiber:	CT API cyberJack®
Version:	V3.3.5
Dateiname:	libctapicyberjack.so
Hashwert (SHA-256):	e7 7b 8c 90 f0 83 45 59 e5 ae 44 44 4c aa 16 37 f2 2b fd c6 c5 05 82 87 95 ca 0f 1f 2c 4a 7c cc

2.4 Funktionsumfang

Die technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component V3.0.21“ erstellt auf Anforderung qualifizierte Zeitstempel konform zum Format gemäß RFC3161.

Der anfordernde Benutzer übermittelt den Hashwert der ursprünglichen Daten. Die technische Komponente für Zertifizierungsdienste übernimmt diesen Hashwert samt der gesetzlich gültigen Zeit und der Genauigkeit der Zeitangabe in die Datenstruktur des Zeitstempels gem. RFC3161. Die gesetzlich gültige Zeit wird von einer sicheren Zeitquelle angefordert, die nicht Teil des Produktes ist. Der Zeitstempel wird mit Hilfe einer ausschließlich für diesen Einsatzzweck bestimmten sicheren Signaturerstellungseinheit signiert. Dies erfolgt ausschließlich unter Verwendung bestätigter Klasse-2- oder Klasse-3-Kartenleser. Diese Zeitquelle, die Kartenleser, die sicheren Signaturerstellungseinheiten als auch die technische Komponente für Zertifizierungsdienste müssen sich dabei in einer isolierten Einsatzumgebung (z. B. einem Trustcenter) befinden.

Das Produkt erlaubt die Vorgabe eines Signaturalgorithmus für den qualifizierten Zeitstempel durch Anforderung. Die Vorgabe muss aus einer Menge als hinreichend stark eingestufte Algorithmen stammen und von einer verfügbaren sicheren Signaturerstellungseinheit unterstützt werden. Das Produkt wählt selbständig die nächst verfügbare Signaturerstellungseinheit, um die Anfrage möglichst schnell zu bedienen.

Das Produkt ist darauf ausgelegt, mit einer großen Menge von sicheren Signaturerstellungseinheiten zu arbeiten.

Die Protokollierung der Erzeugung von qualifizierten Zeitstempeln obliegt der Einsatzumgebung und ist nicht Bestandteil des Produktes.

2.5 Sicherheitsfunktionen

In den Sicherheitsvorgaben werden die folgenden Sicherheitsfunktionen definiert:

- SF.Time Stamps;
- SF.Card Management;
- SF.SigCreation;
- SF.Integrity.

2.5.1 SF.Time Stamps

Durch die Sicherheitsfunktion SF.Time Stamps wird die Zeitstempelerzeugung in Form einer qualifizierten elektronischen Signatur unter Einbettung der gesetzlich gültigen Zeit samt Genauigkeit für einen übergebenen Hashwert erreicht.

Der Benutzer stellt an das Produkt eine Anforderung zur Erzeugung eines qualifizierten Zeitstempels. Eine Identifikation oder gar Authentisierung des Benutzers ist nicht erforderlich, wird also vom Produkt nicht verlangt.

Da ein qualifizierter Zeitstempel in Form einer qualifizierten elektronischen Signatur ausgestellt wird, bedient sich die Sicherheitsfunktion zur Ausstellung der Signatur

zur Erfüllung der Zeitstempelanforderung der Sicherheitsfunktion „SF.Card Management“. Die in die Signatur aufzunehmende aktuelle gesetzlich gültige Zeit und ihre Genauigkeit gibt die Sicherheitsfunktion SF.Time Stamps dabei der Sicherheitsfunktion SF.Card Management vor.

Zusätzlich überprüft das Produkt, dass der bei einer solchen Zeitstempelanfrage übermittelte Hashwert auf einem geeigneten Algorithmus basiert (RIPEMD-160, SHA-256, SHA-384 oder SHA-512), und der betreffende Hashwert unverfälscht mit dem gegebenen Zeitwert (Zeitstempel), der aus einer vertrauenswürdigen Quelle stammt, in einen qualifizierten Zeitstempel aufgenommen wird. Er verifiziert den erstellten qualifizierten Zeitstempel gemäß RFC2313.

Die Sicherheitsfunktion SF.Time Stamps wird dabei insb. durch ein Teilsystem realisiert, welches die folgenden Funktionalitäten unterstützt:

- Aufgabe des Teilsystems ist es, auf Anforderung eines Benutzers qualifizierte Zeitstempel in dem in RFC3161 festgelegten Format zu erzeugen.
- Die Anfrage wird vom Benutzer an das Teilsystem gestellt, das über eine weitere Schnittstelle die zum Zeitpunkt der Erzeugung des qualifizierten Zeitstempels gültige gesetzliche Zeit mittels des Netzwerk-Zeitprotokolls (Simple Network Time Protocol SNTP – RFC2030) einholt, um diese unverfälscht in den Zeitstempel aufzunehmen.
- Als Beispiel kann das Netzwerk-Zeitprotokoll in einem isolierten Einsatzbereich durch einen RFC2030-konformen NTP-Server mit integrierter DCF77-Empfangseinheit zur Verfügung gestellt werden. Über die DCF77-Empfangseinheit wird bei diesem Beispiel das von der Physikalisch-Technischen Bundesanstalt erzeugte Zeitsignal des Rufzeichens des DCF77-Senders zwecks unverfälschter Aufnahme in die zu erzeugenden Zeitstempel empfangen und über den NTP-Server zur Verfügung gestellt. Ein weiteres Beispiel für die Bereitstellung der Primärzeitquelle ist der Einsatz eines NTP-Servers mit integrierter GPS Empfangseinheit.
- Zur Kontrolle dieser Primärzeitquelle führt dieses Teilsystem einen Vergleich mit einer Sekundärzeitquelle durch, die ihr Zeitsignal aus einer bewerteten Liste vertrauenswürdiger Zeitwerte ermittelt, die per SNTP empfangen wurden. Auf diese Weise wird sichergestellt, dass für die Zeitstempel-Erzeugung stets und ausschließlich die gültige gesetzliche Zeit verwendet wird.
- Die angeforderten Zeitstempel werden in Form eines qualifizierten Zeitstempels erzeugt. Hierzu erstellt das Teilsystem eine Anfrage zur Erstellung einer Signatur an die Sicherheitsfunktion „SF.Card Management“, indem es aus der Zeitstempelanforderung zusammen mit der Zeitinformation die Datenstruktur TSTInfo gemäß RFC3161 erzeugt und in Form eines Requests übergibt. Hierbei wird der übergebene, zeitstempelnde Hashwert unverändert in das Request weitergereicht.

2.5.2 SF.Card Management

Durch die Sicherheitsfunktion SF.Card Management wird die ausschließliche Aktivierung der sicheren Signaturerstellungseinheit (SSEE) durch die signierende Person mittels PIN-Eingabe erreicht.

Das Herausziehen einer SSEE führt unmittelbar zur Deaktivierung dieser SSEE. Gleiches gilt für den Fall, dass die SSEE oder der zugehörige Kartenleser als defekt erkannt wird. Die Fähigkeiten des Produktes werden dadurch nicht beeinträchtigt.

2.5.3 SF.SigCreation

Durch die Sicherheitsfunktion SF.SigCreation wird die korrekte Erzeugung einer Signatur erreicht. In jedem Vorgang werden entweder alle oder keine Daten eines Auftrags signiert.

Signaturen werden erstellt, indem ein Hashwert für das zu signierende Datum berechnet wird. Alle erstellten Signaturen werden nach ihrer Erzeugung auf ihre Korrektheit überprüft (verifiziert). Hierzu wird ausschließlich überprüft, ob die Signatur mit Hilfe des zugehörigen Signaturzertifikates kryptographisch geprüft werden kann und ob die kryptographische Bindung zu dem Hashwert der zu signierenden Daten besteht.

2.5.4 SF.Integrity

Das Produkt wird durch den Selbstschutz Mechanismus regelmäßig (alle 10 Minuten) auf Integrität geprüft.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Im Einzelnen sind die Anforderungen aus SigG und SigV wie folgt von den Sicherheitsfunktionen des Produktes abgedeckt:

Tabelle 1: Umsetzung der Anforderungen aus SigV (TK)

Anforderung aus SigV	Umsetzung durch das Produkt
<p>§ 15 Abs. 3 Satz 4 SigV: „Im Falle des § 17 Abs. 3 Nr. 3 des Signaturgesetzes muss gewährleistet sein, dass die zum Zeitpunkt der Erzeugung des qualifizierten Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird.“</p>	<p>Über die Einsatzumgebung wird eine verlässliche Zeitquelle mit der gesetzlich gültigen Zeit zur Verfügung gestellt.</p> <p>Das Produkt stellt sicher, dass die gültige gesetzliche Zeit aus der Einsatzumgebung unverfälscht in den Zeitstempel aufgenommen wird.</p> <p>Zudem werden nur bestätigte Sichere Signaturerstellungseinheiten samt Chipkartenlesern verwendet.</p> <p>Durch die verwendeten SSEE wird sicher-</p>

	<p>gestellt, dass die qualifizierten Zeitstempel eine qualifizierte elektronische Signatur aufweisen.</p> <p>Die Hinweise an den Benutzer sowie die organisatorischen Aspekte werden in den Handbüchern adäquat dargestellt.</p>
<p>§ 15 Abs. 4 SigV: „Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.“</p>	<p>Das Produkt kann Integritätsverletzungen am Code und die Entnahme von Sicheren Signaturerstellungseinheiten feststellen</p> <p>Zudem ist die Sicherheitsleistung der Einsatzumgebung zu berücksichtigen: das Produkt darf nur in einer isolierten Einsatzumgebung, also in der vertrauenswürdigen und zugangsbeschränkten Umgebung eines Trustcenters betrieben werden, die in ein gemäß SigG und SigV bestätigtes Sicherheitskonzept für Zertifizierungsdiensteanbieter eingebettet ist. Die Hinweise an den Benutzer sowie die organisatorischen Aspekte werden in den Handbüchern adäquat dargestellt.</p>

Tabelle 2: Umsetzung der Anforderungen aus SigG (TK)

Anforderung aus SigG	Umsetzung des Produktes
<p>§ 17 Abs. 3 Nr. 3 SigG: „Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um bei Erzeugung qualifizierter Zeitstempel Fälschungen und Verfälschungen auszuschließen.“</p>	<p>vgl. Anmerkungen in Tabelle 1 zu § 15 Abs. 3 Satz 4 SigV</p>

3.2 Explizit nicht erfüllte Anforderungen

Es gibt keine nicht erfüllten Anforderungen, da für das Produkt als technische Komponente alle Anforderungen aus SigG und SigV durch das Produkt und seine Einsatzumgebung umgesetzt werden.

3.3 Einsatzbedingungen

Diese Bestätigung gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

3.3.1 Anforderungen an die technischen Einsatzbedingungen

Die technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component V3.0.21“ wird in folgender Einsatzumgebung betrieben:

Hardware-Anforderungen:

- PC oder Server mit mind. 2 GHz, mind. 256 MB Hauptspeicher und mind. 10 GB freiem Festplattenplatz;

Software-Anforderungen:

- Betriebssystem: Red Hat Enterprise Linux 5.1;
- Java Runtime Environment (JRE): Version 1.4.2_26 for business von Oracle zusammen mit der Java Cryptography Extension (JCE) in der Ausprägung „Unlimited Strength Jurisdiction Policy Files“ in der Version 1.4.2;

Software-Konfiguration:

- Betrieb als technische Komponente für Zertifizierungsdienste (TK);

Peripheriegeräte:

- sichere Signaturerstellungseinheiten (SSEE): die zugelassenen, nach SigG bestätigten SSEEs sind in Tabelle 3 aufgeführt;
- Chipkartenleser: die zugelassenen, nach SigG bestätigten Chipkartenleser sind in Tabelle 3 aufgeführt;
- Zeitquelle (für den Betrieb als technische Komponente), die die gesetzlich gültige Zeit zuverlässig zur Verfügung stellt.

Tabelle 3: Zusätzliche, nach SigG bestätigte Produkte

Produktart	Bezeichnung	Version	Bestätigungs-ID
SSEE	Telesec TCOS 3.0 Signature Card in der Ausprägung „Signature Card 3.0M, Version 1.0 & NetKey 3.0M, Version 1.0“	1.1	TUVIT.93146.TE.12.2006
SSEE	D-Trust c-card	2.3	bestätigt als Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature, Bestätigungs-ID: T-Systems.02182.TE.11.2006
Kartenleser	Reiner SCT cyberJack e-com ⁵	3.0	TUVIT.93155.TE.09.2008

Die Produkte der Einsatzumgebung sind nicht Bestandteil dieser Bestätigung.

3.3.2 Auslieferung und Inbetriebnahme

Die Auslieferung erfolgt per CD-ROM.

Die ausgelieferten Dateien sind durch eine qualifizierte elektronische Signatur vor Veränderung geschützt.

Vor der Installation des Produktes ist es notwendig sämtliche Signaturen zu prüfen, um sicherzugehen, dass das Produkt während der Auslieferung nicht verändert wurde. Zur Verifikation der Dateien wird folgende Webseite aufgerufen: <http://www.signature-check.de>. Durch Klick auf die Schaltfläche Start wird die eigentliche Seite zur Signaturprüfung aufgerufen; diese Seite ist per SSL gesichert. Das Zertifikat kann im Webbrowser verifiziert werden. Da die Programmdateien größer sind als 350 KB, muss das Java-Applet heruntergeladen werden. Dieses Applet heißt `com.authentidate.verifyapplet.VerifyApplet`; es ist selbst digital signiert und stammt von der AuthentiDate International AG.

3.3.3 Anforderungen an die organisatorische und administrative Einsatzumgebung

An die technische Komponente für Zertifizierungsdienste in der isolierten Einsatzumgebung werden folgende Auflagen gestellt:

- ordnungsgemäß installierter Firewall,
- aktuelle Malware und Virens Scanner sowie
- ordnungsgemäß installiertes Betriebssystem,
- welches von IT-Personal gewartet und gepflegt wird;
- System- und Administratoren sind vertrauenswürdig, zuverlässig und adäquat ausgebildet, um die ihnen zugetragenen administrativen Aufgaben zu erfüllen;
- die System- und Administratoren haben in hinreichenden Zeitabständen dafür Sorge zu tragen, dass die Systemzeit korrekt eingestellt ist, oder es werden geeignete technische Maßnahmen ergriffen, die Systemzeit korrekt einzustellen;
- an das Produkt gerichtete Funktionsaufrufe eines erfolgreich authentisierten Benutzers werden durch ausreichend starke SSL- / TLS-Verschlüsselung im Transportprotokoll HTTPS geschützt;
- der Benutzer des Produktes gibt seine Authentisierungsinformationen nicht Preis, sodass deren Vertraulichkeit gewährleistet ist;
- Schutz vor manuellem Zugriff Unbefugter;
- Schutz vor digitalem Zugriff Unbefugter;
- Schutz vor Datenaustausch per Datenträger;
- Schutz der Signaturfunktion der SSEE vor Missbrauch (Besitz und Wissen) durch direkte Kontrolle des Karteninhabers;

- durch Sicherheitskonzepte sowie die Umsetzung der Sicherheitskonzepte in der Praxis wird sichergestellt, dass ein potentieller Zugriff Unbefugter zuverlässig erkennbar wird;
- im Falle eines potentiellen Zugriffs Unbefugter wird vor einer weiteren Nutzung des Produktes eine entsprechende sicherheitstechnische Überprüfung durch geeignetes und geschultes Personal durchgeführt, um sicherzustellen, dass die Integrität des Produktes gewährleistet ist;
- für das Personal, das für die Administration, Wartung und Reparatur der Server verantwortlich ist, auf denen SLMBC installiert wurde, gilt zusätzlich:
 - Das für diese Aufgaben eingesetzte Personal muss vertrauenswürdig sein.
 - Das Personal muss für die Durchführung der Wartungs- und Reparaturaufgaben durch den Hersteller geschult, qualifiziert und autorisiert worden sein.
 - Das Personal muss auf die sich aus dem Sicherheitshandbuch ergebenden Auflagen für ihren Tätigkeitsbereich hingewiesen und auf die Einhaltung der entsprechenden Vorgaben verpflichtet werden.

Weitere Hinweise finden sich im „Handbuch zum sicheren Betrieb für Benutzer und Administratoren“.

3.3.4 Anforderungen an die Konfiguration

Der Hash-Algorithmus RIPEMD-160 darf nur vor dem 01.01.2011 verwendet werden. Nach dem 31.12.2010 dürfen nur noch die Hash-Algorithmen SHA-256, SHA-384 und SHA-512 verwendet werden. Die technische Komponente für Zertifizierungsdienste ist dementsprechend zu konfigurieren, vgl. [Auth_HB], Abs. 4.2.

Die technische Komponente für Zertifizierungsdienste muss so konfiguriert werden, dass die gültige gesetzliche Zeit von einem NTP-Server in der Betriebsumgebung als primäre Zeitquelle bezogen wird, wobei der Anwender die technische Komponente zur Kontrolle der Güte des Zeitsignals (Dispersion, Synchronisation, Stratum) in Übereinstimmung mit regulativen Vorgaben konfigurieren muss.

3.4 Algorithmen und zugehörige Parameter

Zur Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt die Hashfunktionen RIPEMD-160 sowie SHA-256, SHA-384, und SHA-512 bereitgestellt.

Die verwendeten kryptographischen Algorithmen sind gemäß den Angaben der Bundesnetzagentur [BNetzA_Algo] als geeignet eingestuft:

- Der verwendete Hashalgorithmus RIPEMD-160 ist bis Ende 2010 als geeignet eingestuft.
- Die verwendeten Hashalgorithmen SHA-256, SHA-384 und SHA-512 werden bis Ende 2016 als geeignet eingestuft.

Aufgrund der Auflage, dass der Hash-Algorithmus RIPEMD-160 nur bis zum 31.12.2010 verwendet werden darf und die technische Komponente für Zertifizierungsdienste dementsprechend zu konfigurieren ist, sowie der weiteren implementierten Hash-funktionen ergibt sich die in Abs. 3.6 angegebene Gültigkeit der Bestätigung.

3.5 Prüfstufe und Mechanismenstärke

Die technische Komponente für Zertifizierungsdienste „AuthentiDate SLM Base Component V3.0.21“ für das Betriebssystem „Red Hat Enterprise Linux 5.1“, für die sicheren Signaturerstellungseinheiten „Telesec TCOS 3.0 Signature Card, Version 1.1, in der Ausprägung „Signature Card 3.0M, Version 1.0 & NetKey 3.0M, Version 1.0“, Bestätigungs-ID: TUVIT.93146.TE.12.2006“ und „D-Trust c-card, Version 2.3, bestätigt als Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature, Bestätigungs-ID: T-Systems.02182.TE.11.2006“ sowie für den Kartenleser „Reiner SCT cyberJack e-com, Version 3.0, Bestätigungs-ID: TUVIT.93155.TE.09.2008“ wurde erfolgreich nach den Common Criteria (CC) mit der Prüfstufe EAL3+ (EAL3 mit Zusatz ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4) evaluiert.

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke hoch.

3.6 Gültigkeit

Die Bestätigung ist gültig bis 31.12.2016.

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

Die Gültigkeit kann mittels eines Nachtrages verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit des Produktes oder der Algorithmen vorliegen.

4. Referenzen

[Auth_HB]	AuthentiDate Deutschland GmbH, „Handbuch zum sicheren Betrieb für Benutzer und Administratoren“, Version 1.6.2, 09.09.2010.
[BNetzA_Algo]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn vom 06. Januar 2010, veröffentlicht am 04. Februar 2010 im Bundesanzeiger Nr. 19, S. 426.
[BNetzA_Einsatz]	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), „Einheitliche Spezifizierung der Einsatzkomponenten für Signaturanwendungskomponenten – Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen“, Version 1.4, 19. Juli 2005.

[SigG]

Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG), vom 16.05.2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091).

[SigV]

Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), vom 16.11.2001 (BGBl. I S. 3074), zuletzt geändert durch Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932).

Ende der Bestätigung