

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: 31.12.2015³

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

Signaturanwendungskomponente „AuthentiDate SLM Base Component, Version 3.0.20“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

DSC.002.08.2009

Bremerhaven, den 02.09.2010

Dr. Sönke Maseberg
Geschäftsführer datenschutz cert GmbH

datenschutz cert

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.

Beschreibung des Produktes für qualifizierte elektronische Signaturen

1. Handelsbezeichnung des Produktes und Lieferumfang

1.1 Handelsbezeichnung

AuthentiDate SLM Base Component V3.0.20

1.2 Auslieferung

CD-ROM oder online per Download

1.3 Hersteller

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

1.4 Lieferumfang des Produktes

Das Produkt „AuthentiDate SLM Base Component V3.0.20“ besteht aus folgenden Dateien:

- ausgelieferte Dateien des Produktes als Signaturanwendungskomponente gemäß SigG (Windows):
 - AD_SLMBC_3.0.20_Win32.zip
 - AD_SLMBC_3.0.20_Win32.zip.cms
 - AD_DOC_3.0.20_Win32.zip
 - AD_DOC_3.0.20_Win32.zip.cms
 - AD_SF_CT_Tool_3.0.20_Win32.zip
 - AD_SF_CT_Tool_3.0.20_Win32.zip.cms

Zudem werden die folgenden Produktunterlagen mit ausgeliefert:

- „SAK Handbuch für Benutzer und Administratoren“, Version 1.4.16, 12.08.2009.
- „Handbuch zum sicheren Betrieb“, Version 1.4.7, 12.08.2009.
- „SAK Installationshandbuch Windows XP SP3 für Administratoren“, Version 1.1.12, 12.08.2009.

2. Funktionsbeschreibung

2.1 Übersicht

Die Signaturanwendungskomponente „AuthentiDate SLM Base Component V3.o.20“ kann benutzt werden, um qualifizierte elektronische Signaturen (Einfach- oder Mehrfach-Signaturen in den Ausprägungen Stapel- und Komfortsignatur) gemäß SigG zu erstellen und zu prüfen.

2.2 Begriffserklärungen

Die Begriffe Einfach-, Mehrfach-, Stapel- und Komfortsignatur orientieren sich an der Definition in der Technischen Richtlinie TR 03115 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [TR-03115]:

„Einfachsignatur: Die sichere Signaturerstellungseinheit (SSEE) erlaubt nach einmaliger erfolgreicher Authentisierung des Signaturschlüssel-Inhabers die Erzeugung höchstens 1 Signatur.

Mehrfachsignatur: Erstellung einer begrenzten Anzahl Signaturen nach der einmaligen Authentisierung des Signaturschlüssel-Inhabers gegenüber der SSEE.“

Dabei gibt es Mehrfachsignaturen in den Ausprägungen Stapel- und Komfortsignatur. Zitat [TR-03115]:

„Der Begriff ‚Komfortsignatur‘ ist für diese technische Richtlinie wie folgt definiert:

„Erstellung einer begrenzten Anzahl qualifizierter elektronischer Signaturen in einer gesicherten Einsatzumgebung, bei der

- die Authentisierung des Signaturschlüssel-Inhabers durch Wissen gegenüber der sicheren Signaturerstellungseinheit (SSEE) vor der Anzeige der zu signierenden Daten erfolgt,
- der Signaturschlüssel-Inhaber sich gegenüber der SSEE für die Auslösung eines Signaturstapels authentisiert,
- die berechtigt signierende Person der Signaturanwendungskomponente den Signaturvorgang innerhalb eines durch ihn selbst und die Signaturanwendungskomponente kontrollierten Zeitraums auslösen kann.“
[...]

Die Stapelsignatur ist definiert als [...]:

„Erstellung einer begrenzten Anzahl qualifizierter elektronischer Signaturen nach den zeitlich unmittelbar aufeinander folgenden Prozessen der Anzeige der zu signierenden Daten und der einmaligen Authentisierung des Signaturschlüssel-Inhabers gegenüber der SSEE“.

Einfach-, Mehrfach-, Stapel- und Komfortsignatur stellen qualifizierte elektronische Signaturen gemäß SigG dar.

2.3 Hinweis

Aufgrund der Beschränkung der Evaluierung bezieht sich diese Bestätigung ausschließlich auf das Produkt „AuthentiDate SLM Base Component V3.0.20“ in der Ausprägung

- für den Betrieb als Signaturanwendungskomponente (SAK) im einteiligen Betrieb,
- für das Betriebssystem Windows XP SP3,
- 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)
- sowie für die Kartenleser
 - Reiner SCT cyberJack e-com, Version 3.0, Bestätigungs-ID: TUVIT.93155.TE.09.2008,
 - SCM Microsystems Chipkartenleser SPR532, FW 5.10, Bestätigungs-ID: BSI.02080.TE.10.2006.

Weitere Funktionalitäten – insb. für den Betrieb als technische Komponente – und weitere zugelassene Betriebssysteme, Signaturerstellungseinheiten und Kartenleser sind nicht Bestandteil der vorliegenden Bestätigung.

2.4 Einsatzmodi

Das Produkt kann in zwei verschiedenen Einsatzmodi betrieben werden, den schwach prozessgebundenen (Einfach- und Stapelsignatur) und den stark prozessgebundenen (Komfortsignatur) Einsatzmodus.

Die Vorgänge zur Erstellung und zur Prüfung von Signaturen werden im Folgenden als Verarbeitung von Signaturen bezeichnet. Einer oder mehrere dieser Signatur-Verarbeitungsprozesse sind zu einer logischen Einheit zusammengefasst und werden Auftrag genannt, anhand dessen die Signaturanwendungskomponente diese Verarbeitungsprozesse abarbeitet.

Vorgänge zur Erstellung von Signaturen erfolgen mit Hilfe von sicheren Signaturerstellungseinheiten, von denen eine oder mehrere als Gruppe von sicheren Signaturerstellungseinheiten zusammengefasst werden.

Die Signaturanwendungskomponente kann für einen von zwei verschiedenen Einsatzmodi konfiguriert werden, den schwach prozessgebundenen und den stark prozessgebundenen.

2.4.1 Schwach prozessgebundener Einsatzmodus (Einfach- und Stapelsignatur)

Im schwach prozessgebundenen Einsatzmodus erfordert das Produkt für jeden Auftrag die Eingabe der Identifikationsdaten des Signaturschlüsselinhalters für die Signaturerstellungseinheiten und erlaubt nicht die Existenz mehr als eines Auftrages zur Erstellung von Signaturen für eine Menge von sicheren Signaturerstellungseinheiten. Vor dem Löschen eines Auftrages zur Erstellung von Signaturen werden alle sicheren Signaturerstellungseinheiten der zugeordneten Gruppe wieder deaktiviert.

2.4.2 Stark prozessgebundener Einsatzmodus (Komfortsignatur)

Im stark prozessgebundenen Einsatzmodus erlaubt das Produkt die gleichzeitige Nutzung einer jeden Gruppe von sicheren Signaturerstellungseinheiten durch eine beliebige Anzahl von Aufträgen. Entsprechend deaktiviert das Produkt die sicheren Signaturerstellungseinheiten einer Gruppe auch nicht vor dem Löschen eines Auftrages, sondern bleibt für einen vorgegebenen Zeitraum oder Anzahl von Signaturen aktiv.

Das Produkt muss im stark prozessgebundenen Einsatzmodus mindestens in einem besonders geschützten Einsatzbereich gemäß [BNetzA_Einsatz] eingesetzt werden.

2.5 Einsatzumgebungen

Für den Betrieb der Signaturanwendungskomponente werden drei Einsatzumgebungen klassifiziert:

--- einfache bzw. geschützte Einsatzumgebung

In der einfachen bzw. geschützten Einsatzumgebung dürfen durch das Produkt nur Einfachsignaturen in schwacher Prozessbindung erzeugt werden.

--- besonders geschützte Einsatzumgebung

In der besonders geschützten Einsatzumgebung sind Einfach- und Mehrfachsignaturen (als Stapel- und Komfortsignaturen) möglich. Das Produkt darf in starker und schwacher Prozessbindung betrieben werden.

--- isolierte Einsatzumgebung

In der isolierten Einsatzumgebung sind Einfach- und Mehrfachsignaturen (als Stapel- und Komfortsignaturen) möglich. Das Produkt darf in starker und schwacher Prozessbindung betrieben werden.

2.6 Interaktion mit Benutzern

Aufträge zur Erstellung von Signaturen oder deren Prüfung nimmt das Produkt nur von authentisierten und dazu autorisierten Benutzern entgegen. Dabei prüft das Produkt die Authentisierung mit Hilfe von Benutzererkennung und Kennwort. Die Autorisierung wird anhand der (vor unberechtigtem Zugriff geschützten) lokalen Konfiguration des Produktes, in der auch die Berechtigung von bekannten Benutzern zum Ausführen einer Funktion beschrieben ist, überprüft.

Die sicheren Signaturerstellungseinheiten sind in Gruppen organisiert. Jede Einheit ist genau einer Gruppe zugeordnet. Die Gruppierung der sicheren Signaturerstellungseinheiten und die Zuordnung der Gruppen zu Benutzern werden durch den

Administrator des Produktes gemäß dem Willen des Inhabers der sicheren Signaturerstellungseinheit vorgenommen und sind in einem speziellen Teil der Konfiguration des Produktes beschrieben.

Funktionsaufrufe werden über das Protokoll HTTPS in Form von XML-Strukturen übermittelt und Antworten werden ebenfalls als XML-Dokument bereitgestellt. Nur zum Herunterladen (Download) zu verifizierender Daten beziehungsweise zu prüfender Daten werden diese vom Produkt als binärer Datenstrom innerhalb von HTTPS bereitgestellt und vom Benutzer ausschließlich über Angabe eines URL angefordert.

Gegenüber den Benutzern, die Aufträge an das Produkt übermitteln, authentisiert sich das Produkt im Zuge des Aufbaus der HTTPS-Verbindung mit Hilfe eines Kommunikationszertifikates (SSL-Server-Zertifikat). In diesem Zertifikat wird der Rechnername aus dem Domain Name System (DNS) des Servers bestätigt, damit der Client-Prozess sicherstellen kann, dass auf dem benannten Rechner das Produkt unter einem bestimmten Netzwerk-Port erreichbar ist.

2.7 Funktionsumfang

Die Signaturanwendungskomponente eignet sich besonders für den unbeaufsichtigten Betrieb innerhalb eines besonders geschützten Einsatzbereichs gem. [BNetzA_Einsatz], ist aber auch für den Einsatz an speziell eingerichteten Arbeitsplatzrechnern geeignet.

Die Signaturanwendungskomponente erlaubt die Komfortsignatur und automatisch ablaufende Erstellung und Prüfung qualifizierter Signaturen in stark prozessgebundenen Einsatzumgebungen. Benutzer als Inhaber einer Menge von Signaturschlüsseln fordern vom Produkt die Erzeugung von qualifizierten elektronischen Signaturen mit diesen Schlüsseln an. Das Produkt zeigt dem Signaturschlüsselinhaber die aktuelle Verwendung seiner Signaturschlüssel.

Sowohl die zu prüfenden Daten als auch zu signierende Daten werden vom Produkt vor der Signaturerstellung beziehungsweise vor der Prüfung in einen sicheren Bereich, „Sicheres Verzeichnis“ genannt, verschoben. Die Zugriffsrechte auf die Daten werden so gesetzt, dass sie vor unbefugter Manipulation geschützt sind. Die Kontrolle über den sicheren Bereich und der Zugriffsschutz werden hierbei vom Betriebssystem geleistet. Das Produkt überprüft aktiv die Integrität der Daten im Sicheren Verzeichnis. Die Daten bleiben dort auch nach Bearbeitungsabschluss mitsamt den erstellten Signaturen beziehungsweise Ergebnissen solchermaßen geschützt, bis ihre Freigabe beauftragt wird.

Bei Einzel- oder Stapelsignaturen kann und soll sich der Anwender davon überzeugen, welche Daten signiert werden sollen.

Bei Komfortsignaturen muss die auf das Produkt zugreifende Anwendung (der Benutzer) sicherstellen, dass die zu signierenden Daten plausibilisiert werden und nur gleichartige Dokumente signiert werden.

Wenn eine sichere Signaturerstellungseinheit aus dem Kartenleser entfernt wird oder nicht mehr zur Verfügung steht (durch Defekt der sicheren Signaturerstellung-

einheit oder den Kartenleser), wird diese sichere Signaturerstellungseinheit deaktiviert.

2.8 Sicherheitsfunktionen

In den Sicherheitsvorgaben werden die folgenden Sicherheitsfunktionen definiert:

- SF.Authentication;
- SF.Task Management;
- SF.Card Management;
- SF.SigCreation;
- SF.SigVerification;
- SF.Integrity.

2.8.1 SF.Authentication

Die Sicherheitsfunktion SF.Authentication realisiert die Identifikation und Authentifikation des Benutzers des Produktes und weist ihm je nach Konfiguration die Rolle des Benutzers oder des Administrators zu.

2.8.2 SF.Task Management

Durch die Sicherheitsfunktion SF.Task Management wird die Vorgangsteuerung der Signatur- resp. Prüfvorgänge in Form eines endlichen Automaten mit definierten Übergängen erreicht und der korrekte Ablauf dieser Vorgänge bewirkt.

2.8.3 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 Produkt stellt im schwach prozessgebundenen Einsatzmodus nach Abarbeitung eines Auftrags sicher, dass die SSEE unmittelbar nach Auftragsende deaktiviert wird.

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.

2.8.4 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.

2.8.5 SF.SigVerification

Durch die Sicherheitsfunktion SF.SigVerification wird die korrekte Prüfung einer Signatur erreicht: inkl. mathematischer Überprüfung (Verifikation) und Prüfung der Gültigkeit des zugehörigen Zertifikats (Validierung).

Das Ergebnis der Prüfung einer Signatur beschreibt

- auf welche Daten sich die Signatur bezieht,
- ob die Daten unverändert sind,
- welchem Signaturschlüsselinhaber die Signatur zuzuordnen ist,
- welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, aufweist,
- welche Inhalte zugehörige Attribut-Zertifikate aufweisen und
- zu welchem Ergebnis die Nachprüfung von Zertifikaten führte, durch die die Zuordnung eines Signaturprüfchlüssels zu einer identifizierten Person durch ein qualifiziertes Zertifikat zu bestätigen und dieses jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten ist.

2.8.6 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 (SAK)

Anforderung aus SigV	Umsetzung durch das Produkt
<p>§ 15 Abs. 2 Nr. 1 a SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Erzeugung einer qualifizierten elektronischen Signatur die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden.“</p>	<p>Diese Anforderung wird im Wesentlichen durch die zugelassenen, nach SigG bestätigten sicheren Signaturerstellungseinheiten und Chipkartenleser gewährleistet. Das Produkt kommt mit Identifikationsmerkmalen nicht in Berührung.</p>
<p>§ 15 Abs. 2 Nr. 1 b) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Erzeugung einer qualifizierten elektronischen Signatur eine Signatur nur durch die berechtigt signierende Person erfolgt.“</p>	<p>Grundsätzlich ist aus Sicht der Bestätigungsstelle zunächst zu berücksichtigen, dass eine Signatur nur durch den Signaturschlüsselinhaber erfolgt, der seine PIN am Chipkartenleser eingibt.</p> <p>Dies gilt im einfachsten Fall der Einfachsignaturen, und auch für das Szenario der Stapelsignaturen (Mehrfachsignaturen), wo ein definierter Stapel nach Eingabe der PIN am Chipkartenleser signiert wird. Bei Stapelsignaturen wird eine besonders geschützte Einsatzumgebung vorausgesetzt.</p> <p>Im Szenario der Mehrfachsignaturen in der Ausprägung der Komfortsignatur sind weitere Sicherheitsaspekte durch das Produkt realisiert – etwa die Authentisierung des Benutzers sowie die Steuerung der angeschlossenen Signaturkarten – sowie eine besonders geschützte Einsatzumgebung vorausgesetzt, durch die insb. gewährleistet wird, dass der Signaturschlüssel-Inhaber die „alleinige Kontrolle“ über seine sichere Signaturerstellungseinheit ausüben kann.</p>

Anforderung aus SigV	Umsetzung durch das Produkt
<p>§ 15 Abs. 2 Nr. 1 c) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Erzeugung einer qualifizierten elektronischen Signatur die Erzeugung einer Signatur vorher eindeutig angezeigt wird.“</p>	<p>Die Erzeugung einer qual. elektr. Signatur wird vor der Erzeugung eindeutig angezeigt; zudem muss der Benutzer den Vorgang der Signaturerzeugung durch ein Passwort anstoßen.</p>
<p>§ 15 Abs. 2 Nr. 2 a) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Prüfung einer qualifizierten elektronischen Signatur die Korrektheit der Signatur</p> <ul style="list-style-type: none"> ▪ zuverlässig geprüft und ▪ zutreffend angezeigt wird.“ 	<p>Das Produkt realisiert die inhaltlichen Aspekte zur Prüfung einer qualifizierten elektronischen Signatur via SF.SigVerification und stellt die Prüfergebnisse einer Applikation in der Einsatzumgebung zur Anzeige bereit.</p>
<p>§ 15 Abs. 2 Nr. 2 b) SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Prüfung einer qualifizierten elektronischen Signatur eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“</p>	<p>Das Produkt realisiert die inhaltlichen Aspekte zur Prüfung, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt, und stellt die Prüfergebnisse einer Applikation in der Einsatzumgebung zur Anzeige bereit.</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 Einsatzumgebung zu berücksichtigen:</p> <ul style="list-style-type: none"> ▪ Für die Erzeugung von Einzel- und Stapelsignaturen steht direkt am Arbeitsplatz der Chipkartenleser und der Signaturschlüsselinhaber hat seine sichere Signaturerstellungseinheit direkt unter Kontrolle. ▪ Für die Erzeugung von Stapelsignaturen sind Auflagen an die Ein-

Anforderung aus SigV	Umsetzung durch das Produkt
	<p>satzumgebung abgegeben: Gefordert ist eine besonders geschützte Einsatzumgebung.</p> <ul style="list-style-type: none"> Für die Erzeugung von Komfortsignaturen sind Auflagen an den Betrieb formuliert: Gefordert ist eine besonders geschützte Einsatzumgebung. <p>Die Hinweise an den Benutzer sowie die organisatorischen Aspekte werden in den Handbüchern adäquat dargestellt.</p>

Tabelle 2: Umsetzung der Anforderungen aus SigG (SAK)

Anforderung aus SigG	Umsetzung des Produktes
<p>§ 17 Abs. 2 Satz 1 SigG: „Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur</p> <ul style="list-style-type: none"> vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht.“ 	<p>Die Erzeugung einer qual. elektr. Signatur wird vor der Erzeugung eindeutig angezeigt; zudem muss der Benutzer den Vorgang der Signaturerzeugung durch ein Passwort anstoßen. Auf welche Daten sich die Signatur bezieht, lässt sich durch einen Download anzeigen.</p>
<p>§ 17 Abs. 2 Satz 2 Nr. 1 - 5 SigG: „Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,</p> <ol style="list-style-type: none"> auf welche Daten sich die Signatur bezieht, ob die signierten Daten unverändert sind, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und zu welchem Ergebnis die Nachprüfung 	<p>Das Produkt realisiert die inhaltlichen Aspekte zur mathematischen Prüfung der Signatur sowie zur Prüfung, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt, und stellt die Prüfergebnisse einer Applikation in der Einsatzumgebung zur Anzeige bereit.</p>

Anforderung aus SigG	Umsetzung des Produktes
von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.“	

3.2 Explizit nicht erfüllte Anforderungen

Für das Produkt werden mit Ausnahme der nachfolgenden Anforderungen aus SigG und SigV alle Anforderungen durch das Produkt bzw. seine Einsatzumgebung umgesetzt:

--- bzgl. Anzeige des Inhalts zu signierender oder signierter Daten gem. SigG § 17 Abs. 2 Satz 3.

3.3 Ergänzungen bzgl. 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.

Die Umsetzung der präzisierenden Anforderungen zu schwachwerdenden Algorithmen und qualifizierten Zeitstempeln werden nachfolgend im Überblick dargestellt:

Norm	Anforderung	Umsetzung
a) Abgelaufene Algorithmen	<p>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>Unspezifische Aussagen zu abgelaufene Algorithmen sind nicht</p>	<p>Bei der Verifikation wird bei jedem Vorkommen eines Signatur- oder Hashing-Algorithmus geprüft, ob er zum Zeitpunkt der Erstellung der zugehörigen Signatur einerseits und zum aktuellen Zeitpunkt andererseits noch stark genug war bzw. ist. Bei fehlenden Bewertungsdaten oder Schwäche zum ersten Zeitpunkt wird eine entsprechende Fehlermeldung in den Bericht eingearbeitet. Bei Schwäche lediglich zum jetzigen Zeitpunkt oder gar nur drohender Schwäche in naher Zukunft wird eine entsprechende Warnung in den Bericht eingearbeitet. Die Fehler- bzw. Warnmeldung und begleitende Bewertungsbe-</p>

Norm	Anforderung	Umsetzung
	zulässig.	richtsausgaben weisen auf den betroffenen Algorithmus und das Datum des Schwachwerdens hin. Die zugreifende Anwendung spezifiziert dabei den Prüfzeitpunkt, also den Zeitpunkt der Erstellung der Signatur.
b) Nicht implementierte Algorithmen	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. Unspezifische Aussagen zu nicht implementierten Algorithmen sind nicht zulässig.	Bezüglich nicht implementierter Algorithmen wird bei der Verifikation ein Fehlerbericht zurückgegeben, der darauf hinweist, dass die Signatur auf Grund des bezeichneten unbekanntem Algorithmus nicht dekodiert werden konnte. In der Dokumentation der Fehlerberichte wird beim entsprechenden Fehlercode explizit hierauf hingewiesen.
c) Qualifizierte Zeitstempel	Tragen Daten einer qualifizierten Signatur, bei deren Verifikation zu erkennen ist, dass der Signaturprüfchlüssel 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. Solange kein standardisiertes Verfahren für die Einbindung von qualifizierten Zeitstempeln 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.	Zeitstempel werden bei der Verifikation einer Signatur als solche erkannt und bei entsprechender Konfiguration geprüft und einer Algorithmenbewertung unterzogen. In der Rückgabe ist insb. der Zeitpunkt aufgeführt.

Norm	Anforderung	Umsetzung
	Unspezifische Aussagen zu qualifizierten Zeitstempeln sind nicht zulässig	

3.4 Einsatzbedingungen

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

3.4.1 Anforderungen an die technischen Einsatzbedingungen

Das Produkt „AuthentiDate SLM Base Component V3.0.20“ 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: Microsoft Windows XP SP3;
- Java Runtime Environment (JRE): Version 1.4.2_19 zusammen mit den unlimitierten Sicherheitsvorgabedateien von Sun in der Version 1.4.2 („Unlimited Strength Jurisdiction Policy Files 1.4.2“ unter <http://java.sun.com/j2se/1.4.2/download.html> zum Download verfügbar);

Software-Konfiguration:

- Betrieb als Signaturanwendungskomponente (SAK) im einteiligen Betrieb;

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.

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

Produktart	Bezeichnung	Version	Bestätigungs-ID
			Application for Digital Signature, Bestätigungs-ID: T-Systems.02182.TE.11.2006
Kartenleser	Reiner SCT cyberJack e-com	3.0	TUVIT.93155.TU.09.2008
Kartenleser	SCM Microsystems SPR532	FW 5.10	BSI.02080.TE.10.2006

Die Produkte der Einsatzumgebung sind nicht Bestandteil dieser Bestätigung.

3.4.2 Auslieferung und Inbetriebnahme

Die Auslieferung erfolgt per CD-ROM oder Online per Download.

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.

3.4.3 Anforderungen an die organisatorische und administrative Einsatzumgebung

Wie in Abschnitt 2.5 beschrieben, werden für das Produkt drei Einsatzumgebungen klassifiziert, an die die folgenden Anforderungen gestellt werden.

An die einfache bzw. geschützte Einsatzumgebung werden folgende Auflagen gestellt:

- ordnungsgemäß installierter Firewall;
- aktuelle Malware und Virens Scanner;
- ordnungsgemäß installiertes Betriebssystem;
- 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.

An die besonders geschützte 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.

An die isolierte Einsatzumgebung werden folgende Auflagen gestellt:

- alle Maßnahmen aus besonders geschützter Einsatzumgebung;
- zzgl. der folgenden Maßnahmen:
 - Durch Sicherheitskonzepte wird sichergestellt, dass ein potentieller Zugriff Unbefugter zuverlässig erkennbar wird.
 - Im Falle eines potentiellen Zugriffs Unbefugter wird vor einer weiteren Nutzung der Signaturanwendungskomponente eine entsprechende sicherheitstechnische Überprüfung durch geeignetes und geschultes Personal durchgeführt.
- zzgl. der folgenden Anforderungen an das Personal, das für die Administration, Wartung und Reparatur der Server verantwortlich ist, auf denen das Produkt installiert wurde:
 - 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.

3.5 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.

Zur Prüfung qualifizierter elektronischer Signaturen werden vom Produkt die Hashfunktionen RIPEMD-160 sowie SHA-256, SHA-384, und SHA-512 sowie der RSA-Algorithmus mit einer Schlüssellänge von mindestens 1024 Bit 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 2015 als geeignet eingestuft.
- RSA wird in Abhängigkeit von der Schlüssellänge wie folgt eingestuft:
 - Bis Ende des Jahres 2009 wird eine Schlüssellänge von 1536 Bit, bis Ende des Jahres 2010 von 1728 Bit und bis Ende des Jahres 2015 Länge von 1976 Bit vorausgesetzt.
 - Für die Gewährleistung eines langfristigen Sicherheitsniveaus wird grundsätzlich die Erhöhung auf 2048 Bit empfohlen.

Durch die Unterstützung von RSA-Schlüssellängen mit mind. 1024 Bit kann das Produkt auch Signaturen überprüfen, bei denen eine notwendige Übersignatur aufgrund ungültiger Algorithmen nicht vorhanden ist

3.6 Prüfstufe und Mechanismenstärke

Das Produkt „AuthentiDate SLM Base Component V3.0.20“ wurde in der Ausprägung für den Betrieb als Signaturanwendungskomponente (SAK) im einteiligen Betrieb, für das Betriebssystem „Windows XP SP3“, 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: TU-VIT.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 die Kartenleser „Reiner SCT cyberJack e-com, Version 3.0, Bestätigungs-ID: TU-VIT.93155.TE.09.2008“ und „SCM Microsystems Chipkartenleser SPR532, FW 5.10, Bestätigungs-ID: BSI.02080.TE.10.2006“ 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 die Stärke hoch erreichen.

3.7 Gültigkeit

Die Bestätigung ist gültig bis 31.12.2015, da abgelaufene Algorithmen vom Produkt entsprechend interpretiert werden, vgl. Ausführungen in Abs. 3.3.

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.

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

- [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 17. November 2008, veröffentlicht am 27. Januar 2009 im Bundesanzeiger Nr. 13, S. 346.
- [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).
- [TR-03115] Bundesamt für Sicherheit in der Informatik, Technische Richtlinie Komfortsignatur mit dem Heilberufsausweis, Version 2.0 vom 19.10.2007.

Ende der Bestätigung