Sicherheitsbestätigung

T-Systems.02249.TE.01.2012

OpenLimit Signature Kernel V.3.0

OpenLimit SignCubes GmbH

Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 3 und 15 Signaturverordnung[2]

Gültig bis: 31.12.2017

Bestätigung
T-Systems.02249.TE.01.2012

T-Systems GEI GmbH
- Zertifizierungsstelle -

Vorgebirgsstr. 49, 53119 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 15 Abs. 2 und 4, § 11 Abs. 3 SigV,
dass die

Signaturanwendungskomponente

OpenLimit Signature Kernel V.3.0

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02249.TE.01.2012

Bonn, den 31.01.2012

Dr. Igor Furgel
Leiter der Zertifizierungsstelle

Die T-Systems GEI GmbH – Zertifizierungsstelle – ist gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

---

1 Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) (BGBl. Jahrgang 2009, Teil I S. 2091)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) (BGBl. I S. 1542)

Die Bestätigung zur Registriernummer T-Systems.02249.TE.01.2012 besteht aus 26 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Signaturanwendungskomponente „OpenLimit Signature Kernel V.3.0“, im Folgenden auch **SAK** genannt.

1.2 Auslieferung

Der Hersteller (s. Abschn. 1.4 weiter unten) liefert das Produkt „OpenLimit Signature Kernel V.3.0“ ausschließlich durch persönliche Übergabe an den Vertreiber des Produktes, die OpenLimit SignCubes AG, in Form einer Kopie der Master-CD aus.

Bei der Auslieferung vom Vertreiber an die Endkunden wird zwischen physischer (materieller) und elektronischer Auslieferung unterschieden.

a) Materielle Auslieferung

Die materielle Auslieferung erfolgt auf nicht-wiederbeschreibbaren Speichermedien (z.B. CD-ROM) im Versand durch die OpenLimit SignCubes AG (Vertreiber).

b) Elektronische Auslieferung

Die elektronische (online) Auslieferung erfolgt über die Webseite des Vertreibers OpenLimit SignCubes AG (https://www.openlimit.com/olscv3/download.html). Es wird ein Installationswerkzeug (Installationsdateien *.msi) bereitgestellt, in welches die Software des Produkts „OpenLimit Signature Kernel V.3.0“ integriert ist. Die Installationsanleitungen im PDF-Format, die zum Lieferumfang des Produkts gehören, sind von derselben Webseite des Vertreibers auch herunterzuladen. Die Bedienungsanleitung (OpenLimit Middleware Version 3, Version 3.2.0, Benutzerhandbuch, Dokumentversion 1.4, OpenLimit SignCubes AG, 16.11.2011) wird zusammen mit dem Produkt installiert (als Teil des OpenLimit_3_2_0_Client.msi Pakets, s. Abschn. 1.3).

In der Benutzerdokumentation wird der Anwender darauf hingewiesen, das *Integrity Tool* auszuführen und somit sicherzustellen, dass er eine integere und bestätigte Version installiert hat. Der Anwender kann nach Installation der Setup-Datei „OpenLimit_3_2_0_IT.msi“ auf das *Integrity Tool* zugreifen.

Die SDK Schnittstelle für die Integration des OpenLimit Signature Kernel V.3.0 in eine Drittanwendung ist im separaten Handbuch (SDK Documentation, OpenLimit

Middleware Version 3, Dokumentenversion 0.9.7, OpenLimit SignCubes AG, 15.10.2011) beschrieben. Dieses Handbuch gehört nicht zum Standardlieferumfang der SAK und wird auf Anfrage vom Vertreiber der SAK dediziert zur Verfügung gestellt.

1.3 Lieferumfang

a) Die Bestandteile der physischen (materiellen) Auslieferung sind:

Produktname	Artikel-Nr.	Gegenstand	Software Version / Release Dokumentation	Datum
OpenLimit Signature Kernel V.3.0	0208090	OpenLimit_3_2_0_Client.msi	3.2.0	14.12.2011
		OpenLimit_3_2_0_IT.msi	3.2.0	14.12.2011
		OpenLimit_3_2_0_Installationshandbuch_Client.pdf	1.6	04.01.2011
		OpenLimit_3_2_0_Installationshandbuch_IT.pdf	1.6	04.01.2011
		README.TXT	-	-

Die optische Identifizierung des Produktes erfolgt über das Typschild auf der CD-ROM, auf dem der Produktname, die Produktversion und das Zielbetriebssystem angegeben sind.

b) Die Bestandteile der elektronischen Auslieferung sind die nachfolgend angegebenen Dateien:

Bestandteil	Dateiname	Software Version / Release Dokumentation	Datum
Installationsdatei der Haupt-Anwendung	OpenLimit_3_2_0_Client.msi	3.2.0	14.12.2011
Installationsdatei des Integrity Tool	OpenLimit_3_2_0_IT.msi	3.2.0	14.12.2011
Installationshandbuch der Haupt-Anwendung	OpenLimit_3_2_0_Installationshandbuch_Client.pdf	1.6	04.01.2011
Installationshandbuch des Integrity Tool	OpenLimit_3_2_0_Installationshandbuch_IT.pdf	1.6	04.01.2011

1.4 Antragsteller dieser Bestätigung und Hersteller des Produkts

Der Antragsteller für das aktuelle Bestätigungsverfahren ist

OpenLimit SignCubes AG
Zuger Str. 76 B
6411 Baar
Schweiz

Der Hersteller der SAK ist

OpenLimit SignCubes GmbH
Saarbrückerstr. 38A
10405 Berlin
Deutschland

2. Funktionsbeschreibung

Der EVG[3] stellt Funktionen zur Verfügung als Teil einer Signaturanwendungskomponente gemäß §2 SigG:

„Im Sinne dieses Gesetzes sind [...] 11. „Signaturanwendungskomponenten“ Software- und Hardwareprodukte, die dazu bestimmt sind, a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.“

2.1 Kurzbeschreibung

Der OpenLimit Signature Kernel V.3.0 ist eine Programmanwendung (Applikationssoftware), die für den Einsatz als Signaturanwendungskomponente vorgesehen ist. Auf einem Personal-Computer ermöglicht es die Nutzung eines Signaturerstellungssystems zur Erstellung elektronischer Signaturen.

Der OpenLimit Signature Kernel V.3.0 bietet dem Produkt-Benutzer hierbei die im Folgenden aufgeführten Funktionalitäten. Hierbei ist zu beachten, dass die vorliegende Bestätigung sich **ausschließlich auf qualifizierte** elektronische Signaturen bezieht; alle etwaigen Angaben zu anderen Arten von Signaturen als qualifizierte elektronische Signaturarten dienen ausschließlich der Information des Lesers.

- Der OpenLimit Signature Kernel V.3.0 ist in der Lage, von einem entsprechenden Signaturerstellungssystem - bestehend aus Kartenterminal und sicherer Signaturerstellungseinheit (SSEE) - erstellte elektronische Signaturen anzuwenden. Diese vom OpenLimit Signature Kernel V.3.0 angewendeten elektronischen Signaturen können *qualifizierte* oder fortgeschrittene elektronische Signaturen sein. Der OpenLimit Signature Kernel V.3.0 unterstützt die Erzeugung von Signaturen im Stapelmodus.
- Der OpenLimit Signature Kernel V.3.0 ist in der Lage, elektronische Signaturen zu prüfen. Diese geprüften elektronischen Signaturen können *qualifizierte* oder fortgeschrittene elektronische Signaturen sein.
- Der OpenLimit Signature Kernel V.3.0 ist in der Lage, von externen Einheiten empfangene Zeitstempel auf beliebige Daten oder Dateien anzuwenden.

Aus technischer Sicht ist der OpenLimit Signature Kernel V.3.0 ein Software-Produkt, das sowohl als eigenständige Anwendung betrieben als auch in Drittanwendungen zur Bereitstellung digitaler Signaturdienste integriert werden kann.

Der OpenLimit Signature Kernel V.3.0 bietet zwei externe Benutzerschnittstellen an – die grafische und die programmierbare Benutzerschnittstelle. Eine Anwendung, die eine dieser Benutzerschnittstellen nutzt, beeinflusst dabei keine der Sicherheitsfunktionen des Produkts, die von einer anderen Benutzerschnittstelle aus benutzt wird.

Das Produkt ist für den Einsatz im nichtöffentlichen Bereich mit geregelten Zugriffsmöglichkeiten vorgesehen (siehe auch Kapitel 3.2 weiter unten).

2.2 Beschreibung der evaluierten Sicherheitsfunktionalität

Der EVG bietet die folgenden Sicherheitsfunktionen, die nachfolgend erläutert werden. Hierbei ist zu beachten, dass die vorliegende Bestätigung sich **ausschließlich auf qualifizierte** elektronische Signaturen bezieht; alle etwaigen Angaben zu anderen Arten von Signaturen als qualifizierte elektronische Signaturarten dienen ausschließlich Information des Lesers.

SF.1 Anwendung elektronischer Signaturen und Einschränkung der zu signierenden Daten durch den Benutzer

Der OpenLimit Signature Kernel V.3.0 ist in der Lage, elektronische Signaturen, die von einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurden, die nicht Teil des Produktes ist, auf die zu signierenden Daten (DTBS[4]) anzuwenden, so wie sie vom Benutzer festgelegt wurden.

Die Auswahl der DTBS und die resultierende Berechnung des Hashwerts der DTBS[5] als eine Art ihrer Repräsentation können durch jeden Benutzer erfolgen, ohne dass hierfür eine Autorisierung notwendig ist, denn das Produkt setzt kein Rollenmodell für Benutzer um. Die Erzeugung dieser Repräsentation der DTBS garantiert die Gültigkeit der DTBS und bietet die Möglichkeit zur Prüfung der signierten Daten.

Der OpenLimit Signature Kernel V.3.0 ist im Stande, unter Benutzung eines entsprechenden Signaturerstellungssystems *qualifizierte* oder fortgeschrittene elektronische Signaturen gemäß SigG / SigV anzuwenden. Während des Vorgangs

---

3 Evaluierungsgegenstand (Engl.: TOE)

4 data to be signed

5 Die Berechnung des Hashwerts der DTSB kann durch das Produkt erfolgen, oder sie erfolgt teilweise oder vollständig durch die externe SSEE.

der Signaturanwendung bestimmt der OpenLimit Signature Kernel V.3.0 den Typ der unter Nutzung dieses Signaturerstellungssystems zu erstellenden elektronischen Signatur, und zwar entsprechend der verwendeten SSEE. Verwendet der Benutzer des Produkts hierbei ein qualifiziertes elektronisches Zertifikat gemäß SigG / SigV, wählt der OpenLimit Signature Kernel V.3.0 die Variante *SF.1a* dieser Sicherheitsfunktion, was zur Anwendung einer *qualifizierten* elektronischen Signatur führt. Andererseits wählt das Produkt Variante *SF.1b* dieser Sicherheitsfunktion, was zur Anwendung einer fortgeschrittenen elektronischen Signatur führt.

Vor dem Beginn der Berechnung des Hashwerts zeigt der OpenLimit Signature Kernel V.3.0 eine eindeutige Meldung an, dass eine elektronische Signatur erstellt werden soll. Dabei ist zweifelsfrei feststellbar, auf welche Daten sich jede solcher elektronischen Signaturen bezieht. Der OpenLimit Signature Kernel V.3.0 stellt sicher, dass, falls der Benutzer des Produkts die Anzeige des Inhalts eines Dokuments anfordert, ihm dieser Inhalt eindeutig angezeigt wird. Zudem wird der Benutzer darüber informiert, falls der anzuzeigende Inhalt des Dokuments versteckte oder aktive Inhalte enthält oder falls dieser Inhalt nicht angezeigt werden kann. Um durch die sichere Anzeigeeinheit des Produkts eindeutig angezeigt zu werden, müssen die zu signierenden Daten eine Text- (also „ASCII-formatiert“), XML-, TIFF- oder PDF/A-formatierte Datei sein. Ein entsprechender Parser ermittelt dabei den Dateityp. Falls der Parser den Dateityp nicht ermitteln kann, wird eine eindeutige Fehlermeldung angezeigt, die einen Hinweis enthält, dass die Daten nicht wie angefordert angezeigt werden konnten. Nachfolgend werden die Daten auf versteckte und aktive Inhalte geprüft. Falls eine Datei unbekannte Tags, Auszeichnungs- oder Kontrollelemente enthält, wird der Benutzer darüber informiert, dass die Datei unbeabsichtigten Inhalt enthalten könnte. Falls der Parser aktive oder versteckte Inhalte entdeckt, wird dem Benutzer hierüber eine entsprechende Meldung präsentiert. Falls der Benutzer die Anzeige einer Datei wünscht, die solche versteckten oder aktiven Inhalte enthält, die nicht darstellbar sind, wird eine Warnmeldung erstellt und dem Benutzer angezeigt.

Die SAK integriert stets und automatisch die aktuelle Systemzeit als den Signaturerstellungszeitpunkt in die Signaturdaten. Zusätzlich ermöglicht die SAK dem Benutzer, einen qualifizierten Zeitstempel auf das signierte Objekt anzuwenden.

Der Benutzer hat die Möglichkeit, eine aktuelle OCSP-Auskunft (RFC 2560) für das Zertifikat des Benutzers, das dem Signaturschlüssel entspricht, mit dem die elektronische Signatur erstellt wurde, in das signierte Objekt aufzunehmen.

Nach der Hashwert-Berechnung veranlasst der OpenLimit Signature Kernel V.3.0 die Erstellung der elektronischen Signatur unter Benutzung eines sicheren Signaturerstellungssystems, das aus dem Kartenterminal und den weiter unten aufgeführten SSEE besteht (s. Abschn. 3.2). Der Benutzer des Produkts, der die zu signierenden Daten oder ihre Repräsentation zur SSEE senden möchte, muss

hierzu durch sichere Eingabe der PIN am PIN-Pad des Kartenterminals der SSEE – also außerhalb des Produkts – autorisiert sein, wodurch er als Signaturschlüsselinhaber eingestuft wird. Der OpenLimit Signature Kernel V.3.0 erzwingt, dass der Benutzer sich als Signaturschlüsselinhaber erfolgreich autorisieren muss, bevor die ausgewählten zu signierenden Daten an die SSEE gesendet werden.

Die elektronische Signatur wird durch die SSEE erzeugt (außerhalb des Produkts). Der OpenLimit Signature Kernel V.3.0 fügt den resultierenden Objekten das Signaturzertifikat hinzu. Durch die elektronische Signatur wird die Authentizität der Daten sichergestellt. Durch das Hinzufügen des Signaturzertifikats ergibt sich die Möglichkeit zur Verifikation der Daten.

Nach dem Vorgang der elektronischen Signaturerstellung prüft der OpenLimit Signature Kernel V.3.0 die elektronische Signatur unter Benutzung des öffentlichen Schlüssels des gegebenen Signaturzertifikats. Für jede Erstellung einer elektronischen Signatur prüft der OpenLimit Signature Kernel V.3.0 die Korrektheit der empfangenen Signaturdaten und die Übereinstimmung mit der Repräsentation der gesendeten zu signierenden Daten. Falls der ursprüngliche Hashwert und der in die elektronische Signatur kodierte Hashwert nicht übereinstimmen, ist der Hashwert während der Übertragung zur SSEE verändert worden. Nach diesem Vorgang wird eine eindeutige Meldung angezeigt, ob die korrekten Daten signiert worden sind. Im Falle, dass nach dem Senden der Repräsentation der zu signierenden Daten keine Signaturdaten empfangen werden, entdeckt dies der OpenLimit Signature Kernel V.3.0.

Variante SF.1a: Anwendung *qualifizierter* elektronischer Signaturen und Einschränkung der zu signierenden Daten durch den Benutzer

Beim Vorgang der Anwendung einer qualifizierten elektronischen Signatur berechnet der OpenLimit Signature Kernel V.3.0 den Hashwert der zu signierenden Daten ausschließlich unter Benutzung eines Algorithmus der SHA-2-Algorithmenfamilie, wobei der benutzte Algorithmus einer der folgenden Hashalgorithmen sein muss: SHA-224, SHA-256, SHA-384 oder SHA-512, vgl. dazu auch Abschn. 3.3 weiter unten.

Variante SF.1b: Anwendung fortgeschrittener elektronischer Signaturen und Einschränkung der zu signierenden Daten durch den Benutzer

Beim Vorgang der Anwendung einer beliebigen anderen Signatur, außer einer qualifizierten elektronischen Signatur, berechnet der OpenLimit Signature Kernel V.3.0 den Hashwert der zu signierenden Daten unter Benutzung eines Algorithmus der SHA/SHA-2-Algorithmenfamilie, wobei der benutzte Algorithmus einer der folgenden Hashalgorithmen sein kann: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 oder RIPEMD-160.

SF.2 Prüfung digital signierter Objekte

Der OpenLimit Signature Kernel V.3.0 ist in der Lage, elektronische Signaturen gemäß CMS[6] und Zeitstempel gemäß RFC 3161 zu prüfen. Diese elektronischen Signaturen können dabei *qualifizierte* oder fortgeschrittene elektronische Signaturen gemäß SigG / SigV sein. Der Typ der zu prüfenden Signaturen wird vom OpenLimit Signature Kernel V.3.0 gemäß dem Typ des Zertifikats des Signaturschlüsselinhabers ermittelt. Für die Prüfung *qualifizierter* elektronischer Signaturen, bei denen das Signaturzertifikat von einem Zertifizierungsdiensteanbieter gemäß SigG / SigV ausgegeben worden ist, wählt das Produkt die Variante SF.2a dieser Sicherheitsfunktion; für die Prüfung fortgeschrittener elektronischer Signaturen wählt der OpenLimit Signature Kernel V.3.0 die Variante SF.2b.

Das digital signierte Objekt kann hierbei auf einem SHA-1-, SHA-224-, SHA-256-, SHA-384-, SHA-512- oder RIPEMD-160-Hashwert beruhen. Während des Vorgangs der Prüfung digital signierter Objekte ist es eindeutig, auf welche Daten sich die elektronische Signatur bezieht. Zum Zwecke der elektronischen Signaturprüfung wird der Hashwert des digital signierten Objekts unter Benutzung des zugehörigen Algorithmus berechnet und der ursprüngliche Hashwert aus der Signatur unter Benutzung des RSA-, DSA- bzw. ECDSA-Algorithmus und des öffentlichen Schlüssels des gegebenen Signaturzertifikats extrahiert. Die Prüfung von DSA-Signaturen ist nur für die Prüfung von fortgeschrittenen Signaturen vorgesehen. Zusätzlich zu diesem Vorgang wird die Zertifikatskette unter Verwendung des Kettenmodells oder RFC 3280 geprüft.

Das Ergebnis der Prüfung des signierten Objekts wird dem Benutzer mittels eines vom OpenLimit Signature Kernel V.3.0 bereitgestellten Dialogfensters angezeigt. Dieser Dialog liefert die in dem signierten Objekt kodierten Informationen und bietet zudem die Möglichkeit zur Anzeige des für die Signatur benutzten Zertifikats. Der OpenLimit Signature Kernel V.3.0 zeigt eine eindeutige Meldung an, ob der in die Signatur kodierte Hashwert und der Hashwert der zu prüfenden Daten übereinstimmen oder nicht. Hierdurch ist es eindeutig, ob die Originaldaten verändert wurden oder nicht. Die Korrektheit der elektronischen Signatur wird zuverlässig festgestellt und angezeigt. Durch die Benutzung des OpenLimit Signature Kernel V.3.0 wird sichergestellt, dass der Inhalt des signierten Objekts eindeutig angezeigt wird.

Als Teil des Prüfvorgangs zeigt der OpenLimit Signature Kernel V.3.0 unter Benutzung der Sicherheitsfunktion SF.3 „Eindeutige Anzeige von Dokumenten“ die Ergebnisse des Vorgangs eindeutig an und identifiziert den Inhaber der für die Erstellung der Signatur benutzten Signaturerstellungsdaten. Der Benutzer, der die

---

6 RFC 5652

Prüfung der Gültigkeit der elektronischen Signatur unter Benutzung des OpenLimit Signature Kernel V.3.0 beabsichtigt, erhält die Möglichkeit, sich das bei der Erstellung der elektronischen Signatur verwendete Zertifikat eindeutig anzeigen zu lassen.

Während des Prüfvorgangs wird der Herausgeber des Signaturzertifikats ermittelt und eine OCSP-Anfrage gestellt, um die Gültigkeit des zu untersuchenden Zertifikats zu prüfen. Die zugehörige OCSP-Auskunft kann hierbei in die zu untersuchenden Signaturdaten kodiert sein. Falls eine existierende, gültige OCSP-Auskunft verfügbar ist (deren Erstellungszeit nach der Signaturerstellungszeit liegt), kann diese für die Signaturprüfung verwendet werden.

Falls eine gültige OCSP-Auskunft nicht verfügbar ist, kann eine Zertifikatssperrliste für den Prüfvorgang verwendet werden. Diese Sperrliste wird auf das Vorhandensein eines Sperrvermerks für das Signaturzertifikat geprüft. Falls dies zutrifft, wird diese Information verwendet. Falls das Zertifikat schon während der Signaturerstellung gesperrt war, wird dem Benutzer diese Information angezeigt.

Zudem hat der Benutzer die Möglichkeit, einen in die Signaturdaten kodierten Zeitstempel als Zeitpunkt der Signaturerstellung zu verwenden. Dieser Zeitstempel kann hierbei Teil der zu untersuchenden PKCS#7 bzw.CMS-kodierten Daten sein oder dem Produkt als separate Datei vorliegen. Auf Anforderung des Benutzers wird dieser Zeitstempel vom OpenLimit Signature Kernel V.3.0 verwendet, um Gültigkeitsinformationen über die zu untersuchende Signatur bezüglich des Zeitpunkts zu liefern, der im Zeitstempel festgehalten wird.

Die wesentlichen Gültigkeitsprüfungen erfolgen stets unter Benutzung der Zeitangabe, die in den Signaturcontainer kodiert ist. Diese Zeit ist normalerweise die Systemzeit, zu der die Signatur erstellt worden ist. *Falls keine solche Zeitangabe verfügbar ist, wird die aktuelle Systemzeit als Zeitpunkt der Signaturerstellung angenommen,* wobei der Benutzer diesen Umstand an der beinahe Identität zwischen dem Prüfzeitpunkt und dem (angenommenen) Signaturerstellungszeitpunkt erkennen kann, s. auch Abschn. 3.2.2 dieser Bestätigung.

Variante SF.2a: Prüfung *qualifiziert* signierter Objekte

Falls die durch den OpenLimit Signature Kernel V.3.0 zu prüfende elektronische Signatur eine qualifizierte elektronische Signatur gemäß SigG / SigV ist, benutzt der OpenLimit Signature Kernel V.3.0 das *Kettenmodell* für die Signaturprüfung. Die Gültigkeit der in der zu prüfenden qualifizierten elektronischen Signatur verwendeten Algorithmen wird hierbei durch den OpenLimit Signature Kernel V.3.0 unter Benutzung des Algorithmenkatalogs[7] bestimmt.

---

[7] Für diese Funktionalität benutzt das Produkt die entsprechenden Angaben aus der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über

Variante SF.2b: Prüfung fortgeschritten signierter Objekte
Falls die durch den OpenLimit Signature Kernel V.3.0 zu prüfende elektronische Signatur eine fortgeschrittene elektronische Signatur gemäß X.509 ist, benutzt der OpenLimit Signature Kernel V.3.0 das *Schalenmodell* für die Signaturprüfung. Die Gültigkeit der in der zu prüfenden fortgeschrittenen elektronischen Signatur verwendeten Algorithmen wird hierbei durch den OpenLimit Signature Kernel V.3.0 unter Benutzung des Algorithmenkatalogs[7] bestimmt.

SF.3 Eindeutige Anzeige von Dokumenten

Der OpenLimit Signature Kernel V.3.0 bietet die Funktionalität einer sogenannten *Sicheren Anzeigeeinheit*. Diese Funktionalität kann von einem Benutzer des Produkts während der Signaturerstellung oder der Signaturprüfung benutzt werden.

Der OpenLimit Signature Kernel V.3.0 stellt sicher, dass der Inhalt von Daten der Formate ASCII, XML, PDF/A und TIFF eindeutig dargestellt wird. Hierdurch kann der Benutzer des OpenLimit Signature Kernel V.3.0 den Inhalt des Dokuments eindeutig analysieren und während der Signaturerstellung sicherstellen, dass die Daten, die der Benutzer beabsichtigt zu signieren, tatsächlich diejenigen Daten darstellen, deren Signatur intendiert ist.

Die Funktionalität der sogenannten *Sicheren Anzeigeeinheit* ist unter Durchsetzung der folgenden Vorgaben umgesetzt: Zuerst wird der Typ des Dokuments bestimmt; danach werden die zugehörigen Bedrohungen für den bestimmten Dateityp identifiziert und letztlich wird die eindeutige Anzeige des Dokuments durchgeführt.

Hierdurch stellt der OpenLimit Signature Kernel V.3.0 sicher, dass die angezeigten Ergebnisse der Signaturprüfung für qualifizierte elektronische Signaturen gemäß SigG, CMS-Signatur oder Zeitstempel eindeutig sind und der Benutzer über die notwendigen Informationen unterrichtet wird.

Im Falle, dass Daten gemäß dem XML-Datenformat durch den OpenLimit Signature Kernel V.3.0 eindeutig anzuzeigen sind, ist es notwendig, dass dem Produkt die zugehörigen Transformationsvorschriften der XML-Daten bekannt sind. Ist dies nicht der Fall, zeigt der OpenLimit Signature Kernel V.3.0 den Dateninhalt in einer nicht transformierten Art in Form des Quelltexts des XML-Dokuments an.

---

geeignete Algorithmen), 20.05.2011, veröffentlicht am 07. Juni 2011 im Bundesanzeiger Nr. 85, Seite 2034“.

SF.4 Anwendung von Zeitstempeln

Der OpenLimit Signature Kernel V.3.0 bietet die Möglichkeit, Zeitstempel auf beliebige vom Produkt verarbeitete Daten und Dateien anzuwenden. Hierbei wird ein externer Zeitstempel-Handler zum Empfang des Zeitstempels verwendet, während die Korrektheit des Zeitstempels selbst durch den OpenLimit Signature Kernel V.3.0 sichergestellt wird.

Während des Vorgangs des Imports und der Anwendung von Zeitstempeln prüft der OpenLimit Signature Kernel V.3.0 mathematisch die elektronische Signatur des Zeitstempels unter Benutzung des öffentlichen Schlüssels aus dem entsprechenden Zertifikat. Das Zertifikat muss dem OpenLimit Signature Kernel V.3.0 bekannt sein, um die Signatur zu prüfen, andernfalls importiert der OpenLimit Signature Kernel V.3.0 den Zeitstempel nicht.

Die Signatur kann hierbei – abhängig vom Typ des anzuwendenden Zeitstempels – auf Hashwerten gemäß den Varianten SF.4a und SF.4b dieser Sicherheitsfunktion beruhen.

Nach dem Import des Zeitstempels wird der Zeitstempel auf diejenigen Daten angewendet, die durch den Benutzer hierzu ausgewählt wurden. Anwendung bedeutet hierbei, dass der Zeitstempel in eine bestehende Signatur kodiert oder dass der Zeitstempel als selbstständige Datei gespeichert wird.

Variante SF.4a: Anwendung *qualifizierter* Zeitstempel
Für die Anwendung qualifizierter Zeitstempel muss die Signatur auf einem Hashwert der SHA-2-Algorithmen-Familie beruhen, was bedeutet, dass dieser SHA-224, SHA-256, SHA-384, SHA-512 sein muss. Zum Zwecke der mathematischen Prüfung wird der Hashwert der signierten Daten gemäß dem entsprechenden Algorithmus der SHA-2-Familie berechnet und mit dem ursprünglichen Hashwert verglichen, der aus der Signatur unter Benutzung des RSA-Algorithmus und des öffentlichen Schlüssels des Zeitstempel-Signaturzertifikats extrahiert wird.

Variante SF.4b: Anwendung fortgeschrittener Zeitstempel
Für die Anwendung fortgeschrittener Zeitstempel muss die Signatur auf einem SHA-1-, SHA-224-, SHA-256-, SHA-384-, SHA-512- oder RIPEMD-160-Hashwert beruhen. Zum Zwecke der mathematischen Prüfung wird der Hashwert der signierten Daten gemäß dem entsprechenden Algorithmus der SHA-Algorithmen-Familie bzw. dem RIPEMD-160-Algorithmus berechnet und mit dem ursprünglichen Hashwert verglichen, der aus der Signatur unter Benutzung des RSA-Algorithmus und des öffentlichen Schlüssels des Zeitstempel-Signaturzertifikats extrahiert wird.

SF.5 Produktschutz

Prüfung der Produkt-Integrität

Die Integrität des OpenLimit Signature Kernel V.3.0 kann von jedem Benutzer durch Benutzung des sogenannten *Integrity Tools* sichergestellt werden. Dieses *Integrity Tool* ist ein Betriebssystem-spezifisches ausführbares Programm, das online erhältlich ist (s. Abschn. 3.2.2 weiter unten). Dieses Programm stellt die Integrität der Anwendung sicher, indem es den SHA-256-Hashwert der Programmmodule, aus denen der OpenLimit Signature Kernel V.3.0 besteht, berechnet und mit dem entsprechenden Hashwert als Teil einer in das *Integrity Tool* kompilierten Liste vergleicht. Um die Integrität des *Integrity Tools* selbst sicherzustellen, werden die Hashwerte der ausführbaren Programme in signierten Installationshandbüchern aufgeführt, vgl. Abschn. 1.3.

Falls die berechneten Hashwerte und die erwarteten Hashwerte der Programmmodule nicht identisch sind, wird eine Fehlermeldung erstellt und dem Benutzer angezeigt. Falls keine Unterschiede in der Konfiguration festgestellt wurden, zeigt das *Integrity Tool* einen eindeutigen Dialog mit einer entsprechenden Zusammenfassung an.

Das *Integrity Tool* prüft immer eine vollständige Liste der Binärdateien des OpenLimit Signature Kernel V.3.0. Falls Dateien fehlen, wird der Benutzer darüber anhand einer entsprechenden Meldung informiert. Es ist auch nicht möglich, Module hinzuzufügen, die das *Integrity Tool* nicht kennt.

Produkt-Selbstschutz

Der OpenLimit Signature Kernel V.3.0 wird teils mit elektronisch signierten teils mit mittels Hashwerts geschützten Bibliotheken und Dateien ausgeliefert.

Während des Anlaufs des OpenLimit Signature Kernel V.3.0 wird die Signatur aller signierten Bibliotheken und Dateien durch das Produkt unter Benutzung eines in das Produkt eingebauten öffentlichen Schlüssels verifiziert. Der private Schlüssel, der zum Signieren der Bibliotheken und benutzt wurde, ist im Besitz des Herstellers des OpenLimit Signature Kernel V.3.0. Falls die Prüfung einer dieser Signaturen misslingt, stoppt der OpenLimit Signature Kernel V.3.0 den Anlauf unter Anzeige einer eindeutigen Meldung.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Produkt erfüllt die Anforderungen nach:

SigG

§ 17 Produkte für qualifizierte elektronische Signaturen

§17 (2), Satz 1

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.

Diese Anforderungen sind durch die Sicherheitsfunktion SF.1a umgesetzt (s. Abschn. 2.2 weiter oben)

§17 (2), Satz 2

Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,
1. auf welche Daten sich die Signatur bezieht,
2. ob die signierten Daten unverändert sind,
3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und
5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 3 geführt hat.

Diese Anforderungen sind insbesondere durch die Sicherheitsfunktionen SF.1a und SF.2a umgesetzt (s. Abschn. 2.2 weiter oben)

§17 (2), Satz 3

Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.

Diese Anforderung ist durch die Sicherheitsfunktion SF.3 umgesetzt (s. Abschn. 2.2 weiter oben).

SigV

§ 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen

§ 15 (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,

Identifikationsdaten für die Erzeugung einer qualifizierten elektronischen Signatur werden von der IT-Umgebung des EVG verarbeitet, daher **ist diese Anforderung für den EVG selbst nicht anwendbar.**

b) eine Signatur nur durch die berechtigt signierende Person erfolgt,

Die Berechtigungsprüfung für die Erzeugung einer qualifizierten elektronischen Signatur wird durch die IT-Umgebung des EVG durchgeführt (durch eine sichere Signaturerstellungseinheit, mit der der EVG kommuniziert, s. Abschn. 3.2 weiter unten), daher **ist diese Anforderung für den EVG selbst nicht anwendbar.**

c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird […]

Diese Anforderung ist durch die Sicherheitsfunktion SF.1a umgesetzt (s. Abschn. 2.2 weiter oben).

2. bei der Prüfung einer qualifizierten elektronischen Signatur

a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und

b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

Diese Anforderungen sind insbesondere durch die Sicherheitsfunktion SF.2a umgesetzt (s. Abschn. 2.2 weiter oben).

§ 15 (4)

Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

Diese Anforderung ist vor allem durch die Sicherheitsfunktion SF.5 umgesetzt (s. Abschn. 2.2 weiter oben) sowie durch die Einsatzumgebung des EVG (s. Abschn. 3.2 weiter unten).

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen durch den Produktbetreiber / Produktbenutzer gewährleistet sind:

3.2.1 Anforderungen an die technische Einsatzumgebung

a) Plattform

Der OpenLimit Signature Kernel V.3.0 ist für den Einsatz als Softwareanwendung auf den vom Produkt unterstützten Personal Computern konzipiert. Die IT-Umgebung des Produkts muss hierbei durch Viren- und Malware-Schutzkomponenten gegen Netzwerk-basierte Angriffe geschützt sein.

Das Produkt ist ausschließlich für die Nutzung im geschützten Einsatzbereich mit geregelten Zugriffsmöglichkeiten vorgesehen.

Als **Betriebssysteme** werden folgende Produkte vom OpenLimit Signature Kernel V.3.0 unterstützt, wobei eines dieser aufgeführten Betriebssysteme für die Benutzung des Produkts einzusetzen ist:

Betriebssystem	Variante
Windows XP Service Pack 3	32-Bit-Version
Windows XP Service Pack 2[8]	64-Bit-Version
Windows Vista Service Pack 2	32- und 64-Bit-Version
Windows 7 Service Pack 1	32- und 64-Bit-Version
Windows Server 2008 R2 Service Pack 1	Als normale Plattform und als Terminal-Server

[8] Für die 64-Bit-Version von Windows XP ist kein SP3 verfügbar. Wenn auf Ihrem PC die 64-Bit-Version von Windows XP mit SP2 ausgeführt wird, verfügen Sie über das neueste Service Pack, siehe http://windows.microsoft.com/de-DE/windows/help/learn-how-to-install-windows-xp-service-pack-3-sp3.

b) Konnektivität

Für die Anwendung von Zeitstempeln durch OpenLimit Signature Kernel V.3.0 (vgl. SF.4 in Abschn. 2.2) ist ein Zugang zu einem Zeitstempeldiensteanbieter erforderlich.

Falls der OpenLimit Signature Kernel V.3.0 OSCP-Anfragen oder aktuelle Zertifikatssperrlisten für die Prüfung digital signierter Objekte verwenden soll (vgl. SF.2 in Abschn. 2.2), ist ein Zugang zu den entsprechenden Diensteanbietern notwendig.

c) Unterstützte sichere Signaturerstellungseinheiten (SSEE)

Der Anwender benutzt zur Erstellung qualifizierter elektronischer Signaturen ausschließlich bestätigte sichere Signaturerstellungseinheiten nach § 2 Nr. 10 SigG.

Die folgenden sicheren Signaturerstellungseinheiten werden vom OpenLimit Signature Kernel V.3.0 unterstützt, wobei mindestens eine dieser aufgeführten SSEE für die Benutzung des Produkts für Anwendung elektronischer Signaturen (vgl. SF.1 in Abschn. 2.2) und für Anwendung von Zeitstempeln (vgl. SF.4 in Abschn. 2.2) einzusetzen ist:

SSEE	Bestätigung nach SigG
Chipkarte mit Prozessor SLE66CX322P oder SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature (Einzel- und Massensignaturkarte)	T-Systems.02182.TE.11.2006
STARCOS 3.2 QES Version 1.1 (Einzelsignaturkarte)	BSI.02102.TE.11.2008
STARCOS 3.2 QES Version 2.0 (Einzel-, M100- und Massensignaturkarte)	BSI.02114.TE.12.2008
TCOS Identity Card Version 1.0 Release 1/SLE78CLX1440P [neuer Personalausweis]	SRC.00006.TE.11.2010
TCOS 3.0 Signature Card, Version 1.1 (Einzel- und Massensignaturkarte)	TUVIT.93146.TE.12.2006
ZKA Banking Signature Card, Version 7.1.2 (Einzelsignaturkarte)	TUVIT.93166.TU.06.2008, Nachtrag 2
ZKA Banking Signature Card, Version 7.1.3 (Einzelsignaturkarte)	TUVIT.93171.TU.06.2010
ZKA Banking Signature Card, Version 7.1.4 (Einzelsignaturkarte)	TUVIT.93181.TU.09.2010
ZKA Banking Signature Card, Version 7.2.1 (Einzelsignaturkarte)	TUVIT.93157.TU.06.2008
ZKA Banking Signature Card, Version 7.2.2 (Einzelsignaturkarte)	TUVIT.93172.TU.06.2010
ZKA Banking Signature Card, Version 7.2.3 (Einzelsignaturkarte)	TUVIT.93182.TU.09.2010
ZKA-Signaturkarte, Version 5.11 (Einzelsignaturkarte)	TUVIT.93138.TU.11.2006

SSEE	Bestätigung nach SigG
ZKA-Signaturkarte, Version 5.11 M (Massensignaturkarte)	TUVIT.93148.TU.06.2007
ZKA-Signaturkarte, Version 6.01 (Einzelsignaturkarte)	TUVIT.93169.TU.09.2008
ZKA-Signaturkarte, Version 6.20 (Einzelsignaturkarte)	TUVIT.93169.TU.09.2008, Nachtrag 1
ZKA-Signaturkarte, Version 6.21 (Einzelsignaturkarte)	TUVIT.93174.TU.06.2010
ZKA-Signaturkarte, Version 6.22 (Einzelsignaturkarte)	TUVIT.93183.TU.11.2010
ZKA-Signaturkarte, Version 6.30 (Einzelsignaturkarte)	TUVIT.93170.TU.07.2010
ZKA-Signaturkarte, Version 6.31 (Einzelsignaturkarte)	TUVIT.93175.TU.08.2010
ZKA-Signaturkarte, Version 6.32 (Einzelsignaturkarte)	TUVIT.93184.TU.11.2010
ZKA SECCOS Sig v1.5.3 (Einzelsignaturkarte)	BSI.02076.TE.12.2006
ZKA SECCOS Sig v2.6.4 R1.1.2 (Einzelsignaturkarte)	SRC.00009.TE.09.2010

d) Unterstützte Kartenterminals

Es dürfen für die Eingabe der Signatur-PIN im Rahmen der Erstellung qualifizierter elektronischer Signaturen ausschließlich nach § 2 Nr. 13 SigG bestätigte bzw. herstellererklärte Signaturanwendungskomponenten verwendet werden, welche die Sicherheitsfunktion zur sicheren PIN-Eingabe korrekt stimulieren.

Der Betrieb des OpenLimit Signature Kernel V.3.0 benötigt die Verfügbarkeit eines Kartenterminals. Die folgenden Kartenterminals werden hierbei unterstützt, wobei mindestens eines dieser aufgeführten Terminals für die Benutzung des Produkts für Anwendung elektronischer Signaturen (vgl. SF.1 in Abschn. 2.2) und für Anwendung von Zeitstempeln (vgl. SF.4 in Abschn. 2.2) einzusetzen ist:

Kartenterminal	Bestätigung nach SigG
Cherry SmartBoard xx44, Firmware-Version 1.04	BSI.02048.TE.12.2004
Cherry SmartTerminal ST-2xxx, Firmware Version 5.11	BSI.02095.TE.10.2007
Cherry SmartTerminal ST-2xxx, Firmware Version 6.01 (ST-2000UCZ)	BSI.02124.TE.09.2010
Cherry SmartTerminal ST-2xxx, Firmware Version 6.01 (ST-2052UCZ)	BSI.02124.TE.09.2010
Fujitsu KB SCR Pro, S26381-K329-V2xx HOS:01, Firmware Version 1.06	BSI.02082.TE.2007
Fujitsu SmartCase KB SCR eSIG (S26381-K529-Vxxx), Hardware Version HOS:01, Firmware-Version 1.20	BSI.02107.TE.03.2010
Fujitsu SmartCase KB SCR eSIG (S26381-K529-Vxxx), Hardware Version HOS:01, Firmware-Version 1.21	BSI.02107.TE.03.2010, Nachtrag vom 4.02.2011
Kobil KAAN Advanced, Firmware Version	T-Systems.02207.TU.04.2008

Kartenterminal	Bestätigung nach SigG
1.19, Hardware Version K104R3	als Nachtrag zu BSI.02050.TE.12.2006 vom 20.12.2006
Kobil EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A04, Firmware-Version 82.23)	T-Systems.02246.TE.10.2010
Kobil SecOVID Reader III (Artikel-Nr. HCPNCKS/B07, Firmware-Version 82.23)	T-Systems.02246.TE.10.2010
Kobil KAAN TriB@nk (Artikel-Nr. HCPNCKS/C08, Firmware-Version 79.23)	T-Systems.02246.TE.10.2010
OMNIKEY CardMan Trust CM3621, Firmware Version 6.99	BSI.02057.TE.12.2005
OMNIKEY CardMan Trust CM3821, Firmware Version 6.99	BSI.02057.TE.12.2005
Reiner SCT cyberJack pinpad, Version 3.0	TUVIT.93107.TU.11.2004
Reiner SCT cyberJack e-com, Version 3.0	TUVIT.93155.TE.09.2008
Reiner SCT cyberJack e-com plus, Version 3.0	TUVIT.93156.TE.09.2008
Reiner SCT cyberJack secoder, Version 3.0	TUVIT.93154.TE.09.2008
Reiner SCT cyberJack RFID standard, Version 1.2	TUVIT.93188.TU.07.2011
Reiner SCT cyberJack RFID komfort, Version 1.0	TUVIT.93187.TU.02.2011
SCM SPR532, Firmware Version 5.10	BSI.02080.TE.10.2006
SCM SPR332, Firmware Version 6.01	BSI.02117.TE.02.2010

3.2.2 Anforderungen an die organisatorische und administrative Einsatzumgebung

Grundsätzlich müssen Benutzer und Administratoren/Betreiber des Produkts vertrauenswürdig und qualifiziert sein und den Anweisungen der mit dem Produkt ausgelieferten Benutzerdokumentation folgen.

Insbesondere sind die folgenden Anforderungen zu beachten:

- Nach Download der zugehörigen Installationsanleitungen hat der Benutzer die qualifizierte Signatur der PDF-Dateien zu verifizieren (mit einem geeigneten Produkt seiner Wahl). Hierzu sind Angaben zum Zertifikat von der Webseite des Herstellers (https://www.openlimit.com/olscv3/download.html) zu benutzen. Das gleiche gilt, wenn auch ein anderes Installationsspeichermedium (z.B. Installations-CD-ROM) verwendet wird.

- Nach Download der zugehörigen Installationsdateien hat der Benutzer ihren jeweiligen Hash-Wert zu berechnen (SHA-256) und den aktuell berechneten Hash-Wert mit dem Referenzwert in der bereits verifizierten Installationsanleitung zu vergleichen. Nur bei Übereinstimmung darf das Produkt verwendet (installiert) werden.
  Das gleiche gilt auch, wenn auch ein anderes

Installationsspeichermedium (z.B. Installations-CD-ROM) verwendet wird.

- Der Benutzer hat sich vor der ersten Benutzung und dann regelmäßig (am besten vor jeder Benutzung des Produkts) von unversehrter Integrität der ausführbaren Teile des Produkts zu überzeugen. Hierfür ist das mitgelieferte *Integrity Tool* zu benutzen.

- Die SAK bestimmt die Gültigkeit der in der zu prüfenden qualifizierten elektronischen Signatur verwendeten Algorithmen unter Benutzung des im Produkt fest kodierten Algorithmenkatalogs[9].
  Bei der Nutzung der SAK soll der Benutzer wissen, ob es einen aktuelleren offiziell veröffentlichen Algorithmenkatalog gibt.
  Die tatsächliche Gültigkeit der in der zu prüfenden qualifizierten elektronischen Signatur verwendeten Algorithmen ist stets und ausschließlich gemäß dem aktuellen, offiziell veröffentlichen Algorithmenkatalog zu bestimmen[10].

- Der Einsatz des Produkts ist **ausschließlich für nichtöffentliche oder private Umgebungen** vorgesehen. Das Produkt ist also so zu betreiben, dass nur autorisierte Personen Zugang haben und eine gegen Manipulationsversuche geschützte Arbeitsumgebung gewährleistet ist (geschützter Einsatzbereich).

- Dem Benutzer **wird empfohlen**, die Möglichkeit zu benutzen, eine aktuelle[11] OCSP-Auskunft (RFC 2560) für das Zertifikat des Benutzers, das dem Signaturschlüssel entspricht, mit dem die elektronische Signatur erstellt wurde, in das signierte Objekt aufzunehmen (vgl. SF.1 in Abschn. 2.2).

- Produktunabhängiger Hinweis:
  In seine Entscheidung bzgl. der Verwertbarkeit eines SAK-Prüfergebnisses bzgl. einer qualifizierten Signatur sollte der Benutzer u.a.[12] die folgenden Informationen einfließen lassen:
  (i) Den Zeitpunkt, für den die Prüfung des Zertifikatsstatus stattgefunden

---

9 Für diese Funktionalität benutzt das Produkt die entsprechenden Angaben aus der „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 20.05.2011, veröffentlicht am 07. Juni 2011 im Bundesanzeiger Nr. 85, Seite 2034“.

10 Der z.Zt. aktuelle Algorithmenkatalog ist der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, veröffentlicht am 30.12.2011 auf der Internetseite der Bundesnetzagentur http://www.bundesnetzagentur.de/cln_1931/DE/Sachgebiete/QES/Aktuelles/Aktuelles_node.html, wird in Kürze im Bundesanzeiger veröffentlicht zu entnehmen.

11 Zeitnahe dem Zeitpunkt der Signaturerstellung

12 Zusätzlich zu den Anforderungen aus SigV § 15 (2) und zur Liste in SigG §17 (2)

hat (der Zertifikatsstatus nachweislich vorliegt)[13], und
(ii) Den Zeitpunkt der Signaturerzeugung.

3.2.3 Nutzung und Abgrenzung des Produkts

- Der OpenLimit Signature Kernel V.3.0 bietet zwei externe Benutzerschnittstellen an – die grafische und die programmierbare Benutzerschnittstelle – sowie die Schnittstelle zum darunterliegenden Betriebssystem. Diese Schnittstellen stellen die logische Grenze des Produktes dar.
  Bestandteile außerhalb dieser Grenzen wie das Betriebssystem selbst, die Hardware, auf dem das Betriebssystem ausgeführt wird, Kartenterminals und SSEE, die mit dem Produkt kommunizieren, sowie jegliche weitere Applikationen sind **nicht** Gegenstand dieser Bestätigung.

- Die funktionale Abgrenzung ist durch die evaluierte Sicherheitsfunktionalität (vgl. Abschn. 2.2) eindeutig gegeben.
  Insbesondere die folgende Funktionalität war außerhalb der Betrachtung der Sicherheitsevaluierung:
  - Zertifikatsmanagement,
  - Plugin zur Signaturerzeugung und –verifikation in Adobe Acrobat und Reader,
  - Fortgeschrittene Signatur von E-Mails,
  - Konfigurieren der OpenLimit Middleware,
  - Proxy-Einstellungen,
  - Ver- und Entschlüsselung von Dateien,
  - Ver- und Entschlüsselung von E-Mails,
  - Kontextmenü zur direkten Interaktion mit Dateien.

- Die vorliegende Bestätigung bezieht sich **ausschließlich auf qualifizierte** elektronische Signaturen. Alle anderen Arten elektronischer Signaturen inkl. fortgeschrittener sind **nicht** Gegenstand dieser Bestätigung.

3.3 Algorithmen und zugehörige Parameter im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2

Die folgenden Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 werden vom Produkt „OpenLimit Signature Kernel V.3.0“ bereitgestellt:

---

[13] der angegebene Zeitpunkt nach SigV § 15 (2)

a) Zur Erzeugung qualifizierter elektronischer Signaturen:

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[14]	Gültigkeit gem. aktuellen Festlegungen[14]
SHA-1	n.a.	n.a.	nicht geeignet	-
SHA-224	n.a.	n.a.	geeignet	bis Ende 2015
SHA-256	n.a.	n.a.	geeignet	bis Ende 2018
SHA-384	n.a.	n.a.	geeignet	bis Ende 2018
SHA-512	n.a.	n.a.	geeignet	bis Ende 2018
RIPEMD-160	n.a.	n.a.	nicht geeignet	-

b) Zur Prüfung qualifizierter elektronischer Signaturen:

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[14]	Gültigkeit gem. aktuellen Festlegungen[14]
SHA-1	n.a.	n.a.	geeignet ausschließlich zur Prüfung qualifizierter Zertifikate	bis Ende 2015
SHA-224	n.a.	n.a.	geeignet	bis Ende 2015
SHA-256	n.a.	n.a.	geeignet	bis Ende 2018
SHA-384	n.a.	n.a.	geeignet	bis Ende 2018

[14] vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, veröffentlicht am 30.12.2011 auf der Internetseite der Bundesnetzagentur http://www.bundesnetzagentur.de/cln_1931/DE/Sachgebiete/QES/Aktuelles/Aktuelles_node.html, wird in Kürze im Bundesanzeiger veröffentlicht.

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[14]	Gültigkeit gem. aktuellen Festlegungen[14]
SHA-512	n.a.	n.a.	geeignet	bis Ende 2018
RIPEMD-160	n.a.	n.a.	geeignet ausschließlich zur Prüfung qualifizierter Zertifikate	bis Ende 2015
RSA	Parameter n: 1024 ≤ n < 1976 Bit	EMSA-PKCS#1-v1.5 EMSA-PSS DIN V66291 ISO/IEC 9796-2	nicht geeignet	-
RSA	Parameter n: n ≥ 1976 Bit	EMSA-PKCS#1-v1.5	geeignet	Für Zertifikatssignaturen: bis 2017 Für alle anderen Anwendungen: bis Ende 2015
		EMSA-PSS	geeignet	bis Ende 2018
		DIN V66291: „digital signature scheme 2“ und „digital signature scheme 3“[15]	geeignet	bis Ende 2018
		ISO/IEC	geeignet	bis Ende 2018

[15] bezeichnet als “signature format appendix A” im Security Target

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[14]	Gültigkeit gem. aktuellen Festlegungen[14]
		9796-2		
ECDSA basierend auf Gruppen $E(F_p)$	p > 0 Bit 224 ≤ q < 250 Bit	n.a.	geeignet	bis Ende 2015
ECDSA basierend auf Gruppen $E(F_p)$	p > 0 Bit q ≥ 250 Bit	n.a.	geeignet	bis Ende 2018
ECDSA basierend auf Gruppen $E(F_{2^m})$	m > 0 Bit 224 ≤ q < 250 Bit	n.a.	geeignet	bis Ende 2015
ECDSA basierend auf Gruppen $E(F_{2^m})$	m > 0 Bit q ≥ 250 Bit	n.a.	geeignet	bis Ende 2018

3.4 Prüfstufe und Mindeststärke der Sicherheitsfunktionen

Die Signaturanwendungskomponente „OpenLimit Signature Kernel V.3.0“ wurde nach der Prüfstufe EAL4 der Common Criteria v. 3.1 rev. 3 mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV erfolgreich evaluiert.

Die eingesetzten Sicherheitsfunktionen[16] erreichen die Stärke "hoch".

[16] In Common Criteria 3.1: Teil der Schwachstellenbewertung (AVA_VAN); in Common Criteria 2.3: Strength of Functions (AVA_SOF)

3.5 Gültigkeit der Bestätigung

Die Gültigkeitsdauer der vorliegenden Bestätigung insgesamt ist auf das nächstliegende Gültigkeitsdatum beschränkt, das sich aus der Gültigkeit der Produktbestätigung und der maximalen Dauer eines bestätigungskonformen Betriebs des Produkts ergibt. So ist **die Gültigkeit dieser Bestätigung zeitlich beschränkt, und zwar bis 31.12.2017**. Für weitere Einzelheiten s. Abschn. 3.5.1 und 3.5.2 weiter unten.

Die Gültigkeit der Bestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

3.5.1 Gültigkeit der Produktbestätigung

Diese Produktbestätigung ist u.a. auf Grundlage

(i) der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung (s. Abschn. 3.4) und

(ii) der Angaben der aktuell gültigen „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, veröffentlicht am 30.12.2011 auf der Internetseite der Bundesnetzagentur http://www.bundesnetzagentur.de/cln_1931/DE/Sachgebiete/QES/Aktuelles/Aktuelles_node.html, wird in Kürze im Bundesanzeiger veröffentlicht“

zustande gekommen, woraus sich die Bestimmung ihrer Gültigkeit ergibt.

In Bezug auf die Gültigkeitsdauer der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung – unter Berücksichtigung der bei der Implementierung des EVG verwendeten Technologie und der beabsichtigten Einsatzumgebung (Software, die im geschützten Einsatzbereich ausgeführt wird) – agiert die Bestätigungsstelle auf der **Annahme**, dass diese Ergebnisse **7 Jahre** ab dem Zeitpunkt des Evaluierungsabschlusses (20.01.2012) gültig bleiben.

In Bezug auf Verwendung der Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 ergibt sich ihre Gültigkeitsdauer aus dem Abschnitt 3.3, wobei stets zu berücksichtigen ist, ob ein Algorithmus im Betrieb tatsächlich verwendet wird, und wenn Ja, für welche Dienste/Funktionen er verwendet wird.

Die Gültigkeitsdauer der vorliegenden Produktbestätigung ist dann auf das nächstliegende Gültigkeitsdatum beschränkt. So ist die Gültigkeit dieser Produktbestätigung zeitlich beschränkt, und zwar bis 31.12.2018.

Die Gültigkeit der Produktbestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

3.5.2 Maximale Dauer eines bestätigungskonformen Betriebs des bestätigten Produkts

Ein bestätigungskonformer Betrieb der SAK ist an Erfüllung aller Bedingungen aus Abschn. 3.2 „Einsatzbedingungen“ gebunden. Da der Betrieb der SAK die Verfügbarkeit mindestens einer SSEE und eines Kartenterminals benötigt (vgl. Abschn. 3.2.1), ist ihr bestätigungskonformer Betrieb an die Gültigkeit der Produktbestätigungen (bzw. Herstellererklärungen, solange SigG-konform) der eingesetzten SSEEs und Kartenterminals gebunden.

Daraus ergibt sich die maximal mögliche Dauer **eines bestätigungskonformen Betriebs** der SAK, und zwar wie folgt:

a) Das weitestliegende Gültigkeitsdatum der Bestätigungen aller in Abschn. 3.2.1 aufgelisteten SSEEs ist 31.12.2017 (TUVIT.93184.TU.11.2010 N1);
b) Das weitestliegende Gültigkeitsdatum der Bestätigungen / Herstellererklärungen aller in Abschn. 3.2.1 aufgelisteten Kartenterminals ist nicht definiert: Es gibt einige Kartenterminals, derer Bestätigungen kein Gültigkeitsablaufdatum ausweisen.

Die **maximal** mögliche **Dauer eines bestätigungskonformen Betriebs der SAK** ist auf das nächstliegende Gültigkeitsdatum beschränkt, nämlich auf 31.12.2017.

Die maximal mögliche Dauer eines bestätigungskonformen Betriebs der SAK kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

Ende der Bestätigung.

Bestätigung
T-Systems.02249.TE.01.2012

Hrsg.:	T-Systems GEI GmbH
Adresse:	Vorgebirgsstr. 49, 53119 Bonn
Telefon:	+49-(0)228-9841-00
Fax:	+49-(0)228-9841-6000
Web:	www.t-systems.de/ict-security
	www.t-systems-zert.com