Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass die

Funktionsbibliothek
cv act *doc/verifier* V1R1M1

der

cv cryptovision GmbH

den nachstehend genannten Anforderungen des Signaturgesetzes bzw. der Signaturverordnung entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93164.TU.09.2008

registriert.

Essen, 26.09.2008

_____
Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007 (BGBl. I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 2 Abs. 18 des Gesetzes vom 23.11.2007 (BGBl. I S. 2631)

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek cv act *doc/verifier* V1R1M1[3]

Auslieferung:
Als Produkt an Anwendungsprogrammierer durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM mit den folgenden Bestandteilen:

Bezeichnung	**SHA-256 Hashwert**
doc_verifier.lib	`81657599b504d4867a9ede39d48cea09 6f1446cabe9b771ae27477b360aa9d49`
doc_verifier.dll	`966df09f2e232fe02e540ed7cba65310 a1ed4d7735deed13ded2b773ca29e743`
doc_verifier.h	`ea83262cb37875112912fe061d9ae7f6 144a9ff004cdeade8a006a8c5de4090a`
Handbuch_doc_verifier_ 1_1_1_DE.pdf	`6d62daf5032bc856588a0ea1412916de afeb4f6db0d9531dd111f75310d0c16f`
Integritaetsprueftool/ sha256sum.exe	`0906834a017935752eeabdb041238523 4501f0e53012b4c7a06ca30f6df55500`

Ferner enthält die CD noch 18 Zertifikate und die Dateien „hashwerte.txt“ mit den Hashwerten und „KL_V1.3_Auslieferung.doc“ mit der *Konfigurationsliste der Auslieferungsdateien* vom 08.09.2008.

Hersteller:
cv cryptovision GmbH
Munscheidstraße 14, 45886 Gelsenkirchen

[3] Im Folgenden kurz mit cv act *doc/verifier* bezeichnet.

2 Funktionsbeschreibung

cv act *doc/verifier* V1R1M1 ist eine Funktionsbibliothek zum Prüfen von qualifizierten elektronischen Signaturen und zugehörigen Zertifikatsketten gemäß Kettenmodell. Die Funktionsbibliothek ist alleine nicht lauffähig und muss daher vertrauenswürdig in eine Anwendung eingebunden werden. Die Anwendung selbst ist nicht Gegenstand dieser Bestätigung.

Der Umfang der Prüfung der Zertifikatskette ist durch den Parameter „Betriebsart" skalierbar und muss durch die Anwendung gewählt werden. Die folgenden 4 Betriebsarten (0-3) werden durch cv act *doc/verifier* unterstützt:

Betriebsart 0: Alle qualifizierten Zertifikate (d. h. das Benutzerzertifikat, dessen Ausstellerzertifikat des Zertifizierungsdiensteanbieters und das zugehörige Root-Zertifikat der Bundesnetzagentur[4]) werden inkl. aller notwendigen OCSP-Antworten (des Zertifizierungsdienste-anbieters und der Bundesnetzagentur) auf ihre mathematische Korrektheit und Gültigkeit (Zertifikat vorhanden und Zertifikat nicht gesperrt) hin überprüft. Die Prüfung erfolgt bis zum Root-Zertifikat der Bundesnetzagentur.

Betriebsart 1: Alle qualifizierten Zertifikate werden auf ihre mathematische Korrektheit hin überprüft. Lediglich das Benutzerzertifikat wird auf Gültigkeit geprüft. Dazu wird die OCSP-Antwort zum Benutzerzertifikat auf vorhanden und nicht gesperrt ausgewertet und die mathematische Korrektheit der OCSP-Antwort bis zum Root-Zertifikat der Bundesnetzagentur überprüft, d. h. Zertifikat der OCSP-Antwort und das zugehörige Root-Zertifikat der Bundesnetzagentur.

Betriebsart 2: Es wird ausschließlich die mathematische Korrektheit der Zertifikatskette vom Benutzerzertifikat bis zum Root-Zertifikat der Bundesnetzagentur geprüft.

Betriebsart 3: Es wird ausschließlich die mathematische Korrektheit des Benutzerzertifikats unter Verwendung des Ausstellerzertifikats des Zertifizierungsdiensteanbieters geprüft.

Es wird vorausgesetzt, dass die Signaturen im Format PKCS#1 v1.5 sind und auf qualifizierten Zertifikaten im Format X.509 v3 beruhen. Die unterstützten und unter diese Bestätigung fallenden RSA-Schlüssellängen betragen 1280, 1535, 1728, 2048 und 4096 Bit. Die unterstützten und unter diese Bestätigung fallenden Hashfunktionen sind SHA-256 bei der mathematischen Prüfung von Signaturen sowie RIPEMD-160, SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512 bei der Prüfung von Zertifizierungspfaden.

cv act *doc/verifier* ist somit geeignet als Modul eines zu bestätigenden Produktes für qualifizierte elektronische Signaturen gemäß § 2 Nr. 13 SigG, im Folgenden kurz Anwendung genannt, qualifizierte elektronische Signaturen und Zertifikate auf ihre mathematische Korrektheit (Betriebsarten 0, 1, 2 und 3) und Gültigkeit

[4] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (bis 12.07.2005: Regulierungsbehörde für Telekommunikation und Post – RegTP)

(Betriebsarten 0 und 1) zu überprüfen. Dabei ist zu beachten, dass eine vollständige Prüfung der Gültigkeit einer qualifizierten elektronischen Signatur nur in der Betriebsart 0 durchgeführt wird.

Die Funktionsbibliothek cv act *doc/verifier* führt keine eigenständigen OCSP-Abfragen beim Verzeichnisdienst des Zertifizierungsdiensteanbieters und der Bundesnetzagentur durch. Daher müssen alle zur Überprüfung notwendigen Informationen (signiertes Dokument, Signatur, qualifizierte Zertifikate, OCSP-Auskünfte) von der Applikation vertrauenswürdig zur Verfügung gestellt werden.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek cv act *doc/verifier* erfüllt bei der Prüfung von qualifizierten elektronischen Signaturen und Zertifikatsketten gemäß Kettenmodell die folgenden Anforderungen:

- In der Betriebsart 0 werden die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 2 (Daten unverändert), Nr. 5 (Ergebnis der Nachprüfung von Zertifikaten) SigG und nach § 15 Abs. 2 Nr. 2a) (korrekte Prüfung der Signatur), Nr. 2b) (eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV für die gesamte Zertifikatskette erfüllt.

- In der Betriebsart 1 werden die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 2 (Daten unverändert) SigG und nach § 15 Abs. 2 Nr. 2a) (korrekte Prüfung der Signatur) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV erfüllt.

  Zusätzlich werden in der Betriebsart 1 die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 5 (Ergebnis der Nachprüfung von Zertifikaten) SigG und nach § 15 Abs. 2 Nr. 2b) (eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) SigV für das überprüfte Benutzerzertifikat erfüllt.

- In den Betriebsarten 2 und 3 werden die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 2 (Daten unverändert) SigG und nach § 15 Abs. 2 Nr. 2a) (korrekte Prüfung der Signatur) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV erfüllt.

  Die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 5 (Ergebnis der Nachprüfung von Zertifikaten) SigG und nach § 15 Abs. 2 Nr. 2b) (eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) SigV werden in den Betriebsarten 2 und 3 nicht erfüllt, da die Gültigkeit von Zertifikaten nicht überprüft wird.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Die Funktionsbibliothek cv act *doc/verifier* wurde auf Basis der folgenden Hard- und Softwarekonfiguration evaluiert:

- Betriebsysteme und Hardware-Plattformen:
  - Windows Vista Business mit mind. 1 GHz 32-bit Prozessor, mind. 1 GByte RAM, mind. 40 GByte Festplatte mit mind. 15 GByte freiem Speicher, DVD-ROM Laufwerk,
  - Windows XP mit mind. 233 MHz Pentium oder vergleichbarer CPU mit mind. 64 MByte RAM, Festplatte mit mind. 1,5 GByte freiem Speicher, CD-ROM- (oder DVD-) Laufwerk,
  - Windows 2003 Server Enterprise Edition mit mind. 133 MHz Pentium oder vergleichbarer CPU mit mind. 128 MByte RAM, mind. 1,2 GByte Festplatte zur Netzwerkinstallation und 2,9 GByte zur Installation von CD, CD-ROM-Laufwerk,
  - Windows 2003 R2 Server mit mind. 133 MHz Pentium oder vergleichbarer CPU mit mind. 128 MByte RAM, mind. 1,5 GByte Festplatte, CD-ROM-Laufwerk oder
  - Windows 2000 Server mit mind. 133 MHz Pentium oder vergleichbarer CPU mit mind. 64 MByte RAM , mind. 2 GByte Festplattenspeicher mit mind. 650 MByte freiem Speicherplatz, CD-ROM-Laufwerk).
- Compiler zur Einbindung von cv act *doc/verifier* in Anwendungen:
  - Microsoft 32-Bit C/C++ Compiler Version 12 für x86.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Funktionsbibliothek cv act *doc/verifier* darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Einbindung in die Softwareumgebung eines Anwenders

Die Funktionsbibliothek cv act *doc/verifier* V1R1M1 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek cv act *doc/verifier* ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer verwendet, um SigG-konforme Funktionen zur Prüfung von qualifizierten elektronischen Signaturen in Anwendungen zu integrieren. Dabei darf cv act *doc/verifier* nur in Verbindung mit vertrauenswürdigen, die Funktionsbibliothek nutzenden Anwendungen eingesetzt werden. Diese Anwendungen sind jedoch nicht Gegenstand dieser Bestätigung.

Neben den in Kapitel 2 angegebenen und unter diese Bestätigung fallenden Hashfunktionen und RSA-Schlüssellängen unterstützt cv act *doc/verifier* weitere Algorithmen, z. B. SHA-1 für die Signaturprüfung und RSA-1024 Bit. Eine Überprüfung der Eignung der Algorithmen ist nicht implementiert. Diese muss durch die Anwendung erfolgen. Hierbei ist die aktuelle Veröffentlichung über die Eignung der Algorithmen im Bundesanzeiger zu berücksichtigen. Eine Übersicht über die Eignung der Algorithmen gemäß der aktuellen Veröffentlichung im Bundesanzeiger wird in Abschnitt 3.3 gegeben.

Entwickler und Administratoren von Anwendungen müssen die oben genannten Bedingungen einhalten.

c) Nutzung der Funktionsbibliothek cv act *doc/verifier* beim Anwender

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

- Nur in der Betriebsart 0 wird eine vollständige Prüfung der Gültigkeit einer qualifizierten elektronischen Signatur durchgeführt.
- Die Anwendung stellt der Funktionsbibliothek cv act *doc/verifier* alle Signatur-schlüsselzertifikate und OCSP-Antwortdaten, die zu einer Signaturprüfung herangezogen werden müssen, integer zur Verfügung.
- Die Hardwareplattform und die Software (Betriebssystem, cv act *doc/verifier*, nutzende Anwendung) sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass die von der Funktionsbibliothek cv act *doc/verifier* und der Anwendung benutzte Hardwareplattform frei von Viren und Trojanischen Pferden ist sowie Schutz vor deren Einspielung bietet.
- Zum Erkennen von sicherheitstechnischen Veränderungen am EVG sind die Bestandteile der Funktionsbibliothek cv act *doc/verifier* durch Berechung des Hashwerts mit dem mitgelieferten Tool wie in Kapitel 3 des Handbuchs beschrieben zu prüfen.
- Durch Veränderung der Einsatzumgebung dürfen die bekannten Schwachstellen in der Konstruktion und bei der operationalen Nutzung nicht ausnutzbar werden bzw. dürfen keine neuen Schwachstellen entstehen.

Mit der Auslieferung der Funktionsbibliothek cv act *doc/verifier* ist der Anwender auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Überprüfung der mathematischen Korrektheit qualifizierter elektronischer Signaturen werden durch die Funktionsbibliothek cv act doc/verifier die Hashfunktion SHA-256 sowie das Signaturverfahren RSA (PKCS#1 v1.5) mit 1280, 1535, 1728, 2048 und 4096 Bit verwendet. Bei der Überprüfung der Gültigkeit von qualifizierten Zertifikaten werden zusätzlich die Hashfunktionen SHA-1, SHA-224, SHA-384, SHA-512 und RIPEMD-160 verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hashfunktionen reicht für SHA-1 ausschließlich bei Erzeugung/Prüfung qualifizierter Zertifikate bis Ende des Jahres 2009 bzw. 2010 bei mindestens 20 Bit Entropie der Zertifikatsseriennummer, für RIPEMD-160 bis Ende des Jahres 2010 und für SHA-256, SHA-384 sowie SHA-512 bis Ende des Jahres 2014 (siehe BAnz. Nr. 19 vom 05.02.2008, Seite 367).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA reicht für Mindestschlüssellängen von 1976 Bit bis Ende des Jahres 2014, für Mindestschlüssellängen von 1728 Bit bis Ende des Jahres 2010, für Mindestschlüssellängen von 1536 Bit bis Ende des Jahres 2009 und für Mindestschlüssellängen von 1280 Bit bis Ende des Jahres 2008 (siehe BAnz. Nr. 19 vom 05.02.2008, Seite 367).

Die Gültigkeit der Bestätigung der Funktionsbibliothek cv act doc/verifier in Abhängigkeit von Hashfunktion und RSA-Mindestschlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-funktion / Schlüssellänge	SHA-1 bei Erzeugung (Prüfung) qualifizierter Zertifikate	RIPEMD-160, SHA-1 bei Erzeugung (Prüfung) qualifizierter Zertifikate und mind. 20 Bit Entropie der Seriennummer	SHA-224, SHA-256, SHA-384, SHA-512
1280	2008	2008	2008
1536	2009	2009	2009
1728	2009	2010	2010
1976, 2048 & 4096	2009	2010	2014

Neben den in der Tabelle angegebenen Hashfunktionen und RSA-Schlüssellängen unterstützt die Funktionsbibliothek cv act doc/verifier noch die Hashfunktion SHA-1 zur Signaturprüfung und die RSA-Schlüssellänge 1024 Bit. Die Eignung von SHA-1 zur Signaturprüfung ist Ende 2007 mit einer Übergangsfrist bis Ende Juni 2008 abgelaufen. Die Eignung von RSA-1024 ist Ende 2007 abgelaufen. Für die Überprüfung der mathematischen Korrektheit älterer Signaturen können diese Algorithmen noch verwendet werden. Dabei muss durch die Anwendung ein geeigneter Hinweis zur Eignung der Algorithmen gegeben werden.

Diese Bestätigung der Funktionsbibliothek cv act doc/verifier ist somit, abhängig vom Hashfunktion und der Mindestschlüssellänge, maximal gültig bis 31.12.2014; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek cv act *doc/verifier* V1R1M1 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung