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
- ein Unternehmen der TÜV NORD Gruppe -
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* V1R1

der

cv cryptovision GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93115.TE.08.2005

registriert.

Essen, 11.08.2005

gez. Dr. Gruschwitz
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) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch 1. SigÄndG

Die Bestätigung zur Registrierungsnummer TUVIT.93115.TE.08.2005 besteht aus 6 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek cv act *doc/verifier* V1R1[3]

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

Bezeichnung	Datum	SHA-1 Hashwert
doc_verifier.lib	29.06.2005	b9f8794f3b880149eb64 ce5d46aaff872fa7b127
doc_verifier.dll	29.06.2005	22fb153e441a21252467 157a1d6aa167dbc57b78
doc_verifier.h	28.07.2005	e481714562ec19bcdaf3 32b3adfd02ac408e8462
Handbuch_doc_verifier_ 1_1_DE.pdf	28.06.2005	860e4f786f64c1cbd265 107673004c6ee1ba782c
Integritaetsprueftool/Win 32OpenSSL-v0.9.7g.exe	08.06.2005	55d3dbdf2c9de00ac01c 912beafe62379f864f84

Ferner enthält die CD noch 8 Test-Zertifikate und die Dateien „hashwerte.txt“ mit den Hashwerten und „KL_V2_Auslieferung.doc“ mit der *Konfigurationsliste der Auslieferungsdateien* vom 28.07.2005.

Hersteller:
cv cryptovision GmbH
Munscheidstraße 14, 45886 Gelsenkirchen

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

2 Funktionsbeschreibung

cv act *doc/verifier* V1R1 ist eine Funktionsbibliothek zum Prüfen von qualifizierten elektronischen Signaturen und Zertifikatsketten gemäß Kettenmodell. Dazu muss die Funktionsbibliothek vertrauenswürdig in eine Anwendung eingebunden werden. Die Anwendung selbst ist nicht Gegenstand dieser Bestätigung.

Der Umfang der Prüfung 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 BNetzA[4]) werden inkl. aller notwendigen OCSP-Antworten (des Zertifizierungsdienste-anbieters und der BNetzA) auf ihre mathematische Korrektheit und Gültigkeit (Zertifikat vorhanden und Zertifikat nicht gesperrt) hin überprüft. Die Prüfung erfolgt bis zum Root-Zertifikat der BNetzA.

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 BNetzA überprüft, d. h. Zertifikat der OCSP-Antwort und das zugehörige Root-Zertifikat der BNetzA.

Betriebsart 2: Es wird ausschließlich die mathematische Korrektheit der Zertifikatskette vom Benutzerzertifikat bis zum Root-Zertifikat der BNetzA 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 1024 – 4096 Bit. Als Hash-Verfahren werden SHA-1 bei der mathematischen Prüfung von Signaturen sowie RIPEMD-160 und SHA-1 bei der Prüfung von Zertifizierungspfaden unterstützt.

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 (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.

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

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

Laut Sicherheitsvorgaben wurde die Funktionsbibliothek cv act *doc/verifier* von der cv cryptovision GmbH entwickelt, um in unterschiedlichen Einsatzumgebungen in eigenständige Anwendungen integriert zu werden. Als eine solche Einsatzumgebung wird in den Sicherheitsvorgaben das Produkt *MediaTrust* in der *Version 1.0* der Firma MediaSec Technologies GmbH für den elektronischen Rechnungsversand und die Prüfung der elektronischen Signatur über die Rechnungsdaten genannt.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek cv act *doc/verifier* erfüllt folgende 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:

- Rechner mit Intel Pentium III oder vergleichbarer CPU mit mind. 64 MByte RAM, mind. 10 MBbyte freiem Plattenspeicher, CD-ROM- (oder DVD-) Laufwerk,
- Betriebssysteme Windows NT4, 2000, XP oder 2003,
- 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* V1R1 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 (z. B. das in den Sicherheitsvorgaben genannte Produkt MediaTrust V1.0) 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.

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 Signaturschlüsselzertifikate 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 auf der von der Funktionsbibliothek cv act *doc/verifier* und der Anwendung

benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.

- 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

Zur Überprüfung der mathematischen Korrektheit und Gültigkeit von Signaturen und Zertifikaten werden die Algorithmen SHA-1, RIPEMD-160 und RSA mit 1024 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hashalgorithmen SHA-1 und RIPEMD-160 mindestens bis Ende des Jahres 2010 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus (RSA) reicht für Mindestschlüssellängen von 1728 Bit bis mindestens Ende des Jahres 2010, für Mindestschlüssellängen von 1536 Bit bis Ende des Jahres 2009, für Mindestschlüssellängen von 1280 Bit bis Ende des Jahres 2008 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. 59 vom 30.03.2005, Seite 4.695).

Die festgestellte Eignung der Algorithmen reicht somit mindestens bis Ende des Jahres 2007.

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek cv act *doc/verifier* V1R1 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung