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 der

Verzeichnis- und Zeitstempeldienst TC-DIR, Version 2.0

der

TC TrustCenter AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93104.TU.04.2005

registriert.

Essen, 15.04.2005

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.93104.TU.04.2005 besteht aus 7 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Verzeichnis- und Zeitstempeldienst TC-DIR, Version 2.0[3]

Auslieferung:

Als Produkt mittels persönlicher Übergabe an Anwendungsprogrammierer auf einer CD-ROM. Die folgenden Dokumente:

- TC TrustCenter: Benutzerdokumentation für den Evaluationsgegenstand des Verzeichnisdienstes (EVGDIR), Version 2.1, 28.01.2005
- Systemverwalterdokumentation für den Evaluationsgegenstand des Verzeichnisdienstes (EVGDIR), Version 2.3, 01.02.2005
- TC TrustCenter: Betriebsumgebung des Evaluationsgegenstandes des Verzeichnisdienstes EVG_DIR, Version 2.1, 01.02.2005

werden in Papierform übergeben.

Hersteller:

TC TrustCenter AG
Sonninstraße 24-28
20097 Hamburg

2 Funktionsbeschreibung

TC-DIR ist ein Verzeichnis- und Zeitstempeldienst gemäß § 2 Nr. 12b,c SigG, der innerhalb der gesicherten Umgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG zum Einsatz kommt und qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar hält sowie qualifizierte Zeitstempel erzeugt. Zu diesem Zweck muss der TC-DIR sicher in die Infrastruktur des Trust Centers eingebunden werden.

Im Rahmen seiner Funktionalität als Verzeichnisdienst liefert der TC-DIR auf Anfragen, die im OCSP-Format gestellt werden können, folgende Informationen:

- ein Zertifikat oder eine Liste von Zertifikaten,
- Sperrlisten in fest vorgegebenen Zeitabständen.
- Statusinformationen zu dem bzw. den die Anfrage betreffenden Signaturschlüssel- oder Attribut-Zertifikat bzw. Zertifikaten:
  - das Zertifikat ist im Verzeichnisdienst vorhanden und nicht gesperrt,
  - das Zertifikat ist im Verzeichnisdienst vorhanden und gesperrt,
  - das Zertifikat ist nicht im Verzeichnisdienst vorhanden.

In die Antworten wird jeweils – außer beim Abruf von Zertifikaten bzw. bei Statusanfragen zu gesperrten Zertifikaten – die gesetzlich gültige Zeit eingebunden. Erfolgen Auskünfte zu Zertifikaten, so werden zusätzlich neben dem

[3] Im Folgenden kurz mit TC-DIR bezeichnet.

Antwortzeitpunkt der Zeitpunkt der Freischaltung des Zertifikats im Verzeichnisdienst und gegebenenfalls der Zeitpunkt der Sperrung des Zertifikates angegeben.

Zur Gewähr der Integrität der Antwort als auch zur Angabe der Identität wird die Antwort mit Hilfe einer sicheren Signaturerstellungseinheit (SSEE) unter Beachtung folgender Regeln elektronisch signiert:

Zertifikate sind bereits elektronisch signierte Objekte und werden daher beim Abruf nicht noch einmal elektronisch signiert. Sperrlisten und Statusinformationen zu vorhandenen Zertifikaten werden elektronisch signiert. Statusinformationen zu nicht vorhandenen Zertifikaten werden nicht signiert und nicht protokollgerechte Status- bzw. Zertifikatsabfragen werden ebenfalls unsigniert mit einer Fehlermeldung beantwortet.

Darüber hinaus stellt TC-DIR berechtigten Personen jederzeit folgende Dienste zur Verfügung:

- das Sperren eines qualifizierten Zertifikates aufgrund der Übertragung eines Sperrpasswortes,
- das Sperren eines Signaturschlüssel- oder Attribut-Zertifikates aufgrund eines elektronisch signierten Antrags auf Sperrung, dessen Signatur vom Zertifikatbesitzer selbst oder von einem dazu berechtigten Mitarbeiter des Zertifizierungsdienstes stammt.

Im Rahmen seiner Funktionalität als Zeitstempeldienst stellt der TC-DIR folgenden Dienst zur Verfügung:

- Das Anbinden der gesetzlich gültigen Zeit an eingesandte Daten und deren Rücksendung an den Kunden. Die Anbindung ist durch eine elektronische Signatur seitens des Zertifizierungsdiensteanbieters gesichert.

Als Basis der Uhrzeit für den Verzeichnis- und Zeitstempeldienst gilt die Uhrzeit der Physikalisch Technischen Bundesanstalt PTB in Braunschweig.

TC-DIR kann auf dem DIR-Rechner in mehreren Instanzen betrieben werden. Dabei wird sichergestellt, dass die Daten der Instanzen voneinander getrennt sind und eine Instanz keinerlei Zugriff auf qualifizierte Zertifikate einer anderen Instanz erhält.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der Verzeichnis- und Zeitstempeldienst TC-DIR erfüllt die Anforderungen nach § 17 Abs. 3 Nr. 2 (Schutz vor unbefugter Veränderung und unbefugtem Abruf von qualifizierten Zertifikaten) und Nr. 3 SigG (Ausschluss von Fälschungen und Verfälschungen bei Zeitstempelerzeugung) sowie § 15 Abs. 3 Satz 1 (Sperrungen nicht unbemerkt rückgängig machbar, Auskünfte auf Echtheit überprüfbar), Satz 2 (Auskünfte enthalten, ob nachgeprüfte qualifizierte Zertifikate im Verzeichnis vorhanden und nicht gesperrt sind), Satz 3 (nur nachprüfbar gehaltene Zertifikate

sind nicht abrufbar), Satz 4 (unverfälschte Aufnahme der gesetzlich gültigen Zeit bei Zeitstempelerzeugung) und Abs. 4 SigV (sicherheitstechnische Veränderungen erkennbar).

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

TC-DIR wurde für die gesicherte Einsatzumgebung des Trust Centers eines Zertifizierungsdiensteanbieters evaluiert auf der Basis einer definierten Hard- und Softwarekonfiguration des DIR-Rechners und der benötigten Komponenten der Einsatzumgebung:

- DIR-Rechner: Sun Enterprise Server mit Sun Solaris 8 Betriebssystem und Betriebssystemaufsatz ARGUS Pitbull, Version 4.0, Ultra Sparc-II-Prozessor, mind. 512 MB RAM, mind. 2*4.2 GByte Festplatten, CD-ROM-Laufwerk, CD-Writer-Laufwerk, Multi I/O-Karte und 2 Fast Ethernet 100Mbit Netzwerkkarten, Datenbank PostgreSQL 8.0, bestätigte Funktionsbibliothek „Signier- und Prüfkomponente TC-SigPK“, Version 1.1.
- DCF77 Funkuhrempfänger und GPS167 Präzisionsuhr der Firma Meinberg
- mind. 5 B1-Chipkartenleser, die die CT-API-Schnittstelle unterstützen und mind. 5 sichere Signaturerstellungseinheiten nach § 2 Nr. 10 SigG (Chipkarten) mit Schnittstelle nach ISO 7816. Unterstützt wird das Chipkartenprofil StarCert für das Chipkartenbetriebssystem STARCOS SPK2.3 von Giesecke und Devrient basierend auf dem E4-hoch evaluierten Philips Chip P8WE5032V0G.
- geeignete Netzwerkabsicherung durch eine Firewall, Webserver für den direkten Zugriff auf den TC-DIR, unterbrechungsfreie Stromversorgung (USV).

Der Rechner muss in einem verschlossenen und versiegelten Elektroschrank mit durchsichtiger Fronttür untergebracht werden und in einem abgeschlossenen Netzwerksegment innerhalb des Trust Centers des Zertifizierungsdiensteanbieters betrieben werden.

Der TC-DIR darf ausschließlich in der gesicherten Umgebung eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG mit der in der Evaluation zugrunde gelegten Hard- und Softwareausstattung eingesetzt werden.

Jeder Austausch oder jede Veränderung der Hard- und Softwarekonfiguration ist der Bestätigungsstelle anzuzeigen und erfordert ggf. eine Reevaluation.

b) Einbindung in die Softwareumgebung des Trust Centers

TC-DIR ist ein Softwarepaket und besteht aus einer Sammlung einzelner Software-Komponenten in Form lauffähiger Programme, die in ein Solaris-Pakage gepackt und auf einer einmal beschreibbaren CD-ROM ausgeliefert werden.

Folgende Komponenten werden auf CD-ROM ausgeliefert:

Bezeichnung	Beschreibung
tcdir.pkg	Solaris-Package mit dem TC-DIR
tcscard.pkg	Solaris-Package mit der Chipkartentreiberbibliothek
openssl	Prüfprogramm zur Integritätsprüfung
sql	SQL-Skripte zur Generierung der Datenbank
auslkonf-sigpk.doc	Dokumentation zur Auslieferung und Konfiguration von TC-SigPK V1.1
bd.signpk.doc	Betriebsdokumentation zu TC-SigPK V1.1
ReleaseListe	Konfigurationsliste des TC-DIR

Darüber hinaus werden die in Kapitel 1 angegebenen Papierdokumente ausgeliefert.

Die korrekte Einbindung des TC-DIR in das Trust Centers des Zertifizierungsdiensteanbieters ist durch einen Prüfnachweis zu belegen.

c) Nutzung des Verzeichnis- und Zeitstempeldienstes im Trust Center

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

Betrieb des TC-DIR nur in einer vertrauenswürdigen und zugangsbeschränkten Trust Center Umgebung eines Zertifizierungsdiensteanbieters, die in ein gemäß SigG und SigV bestätigtes Sicherheitskonzept für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 SigG eingebettet ist.

- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.
- Es ist sicherzustellen, dass auf der vom TC-DIR benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE) weitergereicht werden insbesondere seitens handelnder Personen.
- Alle angebrachten Versiegelungen der technischen Einsatzumgebung müssen regelmäßig mit der Angabe des Datums durch den IT-Sicherheitsbeauftragten visuell überprüft und deren Unversehrtheit bestätigt werden.
- Die Inhalte der beiden Konfigurationsdateien DIR.CFG und SIGPK.CFG müssen durch den Systemadministrator SysAd1 gewartet werden. Bei der Wartung der Daten muss der IT-Sicherheitsbeauftragte anwesend sein.

- Die DIR-/ TSS-Chipkarten (SSEE) müssen jeweils spätestens nach fünf Jahren im Vier-Augen-Prinzip gegen neue Karten ausgetauscht werden. Der Austausch der DIR-/ TSS-Chipkarten muss zeitlich so erfolgen, dass zu keinem Zeitpunkt elektronische Signaturen mit ungültigen Signaturschlüsseln durch den TC-DIR erstellt werden.
- In einjährigen Abständen müssen die Komponenten von TC-DIR, die im Betrieb auf die STARCOS-Chipkarten zugreifen, beendet und neu gestartet werden, um die PIN der Chipkarten erneut einzugeben.
- Für den Zeitstempeldienst muss die freilaufende Präzisionsuhr jährlich durch den Systemadministrator SysAd2 an die GPS-Zeit angepasst werden. Zwischenzeitlich darf sie keinen Antennenkontakt besitzen. Bei unregelmäßigen Zeitsprüngen (Schaltsekunden) muss die Präzisionsuhr neu synchronisiert werden.
- Für das Überwachen des TC-DIR und der Hardware des DIR-Rechners ist der Systemadministrator SysAd1 verantwortlich. Hierzu gehören auch die Netzwerk-Verbindungen des DIR-Rechners und die Funkuhrkomponente. Der Systemadministrator SysAd1 wird während des laufenden Betriebes durch Nachrichten des TC-DIR über auftretende Fehlersituationen informiert und ist für das Abstellen der Fehlerursachen verantwortlich. Die Fehler- und Status-Meldungen müssen regelmäßig kontrolliert werden.
- Die Audit-Daten müssen regelmäßig vom CA-Mitarbeiter CAM2 in Anwesenheit des IT-Sicherheitsbeauftragten auf eine einmal beschreibbare CD-ROM gesichert werden.
- Es ist zu beachten, dass die bekannten Schwachstellen in der Konstruktion und bei der operationellen Nutzung nicht durch die Veränderung der Einsatzumgebung ausnutzbar werden dürfen bzw. neue Schwachstellen entstehen.

Mit Auslieferung des TC-DIR ist der Betreiber auf die Einhaltung aller oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Zur Erzeugung elektronischer Signaturen werden die Algorithmen SHA-1 und RSA mit 1024 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für SHA-1 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 reicht für RSA mit 1024 Bit bis mindestens Ende des Jahres 2007 (siehe BAnz. Nr. 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 Verzeichnis- und Zeitstempeldienst TC-DIR, Version 2.0 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung