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

technische Komponente für Zertifizierungsdienste Nexus TSP-Responder, Version 3.1

der

Nexus Technology GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93137.TU.02.2007

registriert.

Essen, 20.02.2007

gez. Dr. Sutter
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.93137.TU.02.2007 besteht aus 7 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Nexus TSP-Responder, Version 3.1[3]

Auslieferung:
Als Produkt auf einer einmal beschreibbaren CD-ROM durch persönliche Übergabe.

Hersteller:
Nexus Technology GmbH
Willhoop 1, 22453 Hamburg

2 Funktionsbeschreibung

Der Nexus TSP-Responder ist eine technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12c SigG, die innerhalb der gesicherten Umgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG zum Einsatz kommt und qualifizierte Zeitstempel erstellt. Zu diesem Zweck muss der Nexus TSP-Responder sicher in die Infrastruktur eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG eingebunden werden.

Das Erzeugen der qualifizierten elektronischen Signaturen zu den Zeitstempeldienst-Auskünften erfolgt mittels der in Abschnitt 3.2 aufgeführten sicheren Signaturerstellungseinheiten mit RSA-1024 Bit (PKS-Card, E4KeyCard und E4NetKeyCard) bzw. RSA-2048 Bit (CardOS). Als Hash-Verfahren verwendet der Nexus TSP-Responder dabei SHA-1 oder RIPEMD-160.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der Nexus TSP-Responder erfüllt die Anforderungen nach SigG § 17 Abs. 3 Nr. 3 (Ausschluss von Fälschungen und Verfälschungen bei Zeitstempelerzeugung) sowie SigV § 15 Abs. 3 Satz 4 (unverfälschte Aufnahme der gesetzlich gültigen Zeit bei Zeitstempelerzeugung) und Abs. 4 (sicherheitstechnische Veränderungen erkennbar).

[3] Im Folgenden kurz mit Nexus TSP-Responder bezeichnet.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Der Nexus TSP-Responder wurde für die gesicherte Einsatzumgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration des Host-Rechners

- Host-Rechner: Ultra Sparc 5 Server (oder vergleichbar) mit Solaris 8 oder 10 Betriebssystem, Ultra Sparc II (oder vergleichbarer) Prozessor, mind. 128 MB RAM, mind. 2 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk, mind. 2 serielle Schnittstellen und mind. eine Fast Ethernet 100Mbit Netzwerkkarte.

und der benötigten Komponenten der Einsatzumgebung:

- Protokollierungsrechner (sofern Protokollierung nicht auf dem Host-Rechner erfolgt) mit Solaris 8 oder 10 Betriebssystem, Ultra Sparc II (oder vergleichbarer) Prozessor, mind. 128 MB RAM, mind. 2 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk und mind. eine Fast Ethernet 100Mbit Netzwerkkarte,

- DCF77-C51 Funkuhrempfänger von Meinberg,

- mind. ein B1-Chipkartenleser der die CT-API-Schnittstelle unterstützt,

- mindestens eine personalisierte sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:

  - PKS-Card, E4KeyCard und E4NetKeyCard jeweils Versionen 3.0 und 3.01 (Bestätigung: TUVIT.09339.TE.12.2000 vom 15.12.2000 mit Nachträgen vom 22.02.2002 und 07.12.2004) und

  - Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur (Bestätigung: T-Systems.02122.TE.05.2005 vom 27.05.2005).

Der Host-Rechner muss in einem verschlossenen und versiegelten Elektroschrank untergebracht werden. Das Netzwerksegment, in dem der Nexus TSP-Responder betrieben wird, muss netzwerktechnisch derart abgesichert werden (z. B. durch eine Firewall), dass von Außen ausschließlich TSP-Anfragen an den Nexus TSP-Responder (Host-Rechner) möglich sind, so dass unbefugte Veränderungen innerhalb des Netzwerksegmentes, insbesondere des Host-Rechners einschließlich der zugehörigen Software, unterbunden werden.

Eine geeignete Umsetzung dieser Anforderung an das Netzwerk ist vor dem Betrieb beim Zertifizierungsdiensteanbieter zu überprüfen.

Der Nexus TSP-Responder darf ausschließlich in der gesicherten Umgebung eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG mit der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden. Jeder Austausch oder jede Veränderung der Hard- und Softwarekonfiguration ist der Bestätigungsstelle anzuzeigen und erfordert ggf. eine Reevaluation.

b) Auslieferung und Inbetriebnahme

Der Nexus TSP-Responder, die Betriebs- und Systemverwalterdokumentation, die Konfigurationsliste sowie zusätzlich benötigte Dateien werden auf zwei CD-ROMs persönlich übergeben:

Bezeichnung	Übergabeform
SN_TSP, Version 3.1, 10.11.2006	CD-ROM 1
ProtCompD, Version 3.0, 26.07.2005	CD-ROM 1
libSignierkomponente.so, Version 1.4, 20.10.2006	CD-ROM 1
libCTClientStub.so, Version 3.0, 26.07.2005	CD-ROM 1
ctserver, Version 3.0, 26.07.2005	CD-ROM 1
b1htsi.cfg, 26.07.2005	CD-ROM 1
libACE.so.5.4.0, Version 5.4.0, 26.07.2005	CD-ROM 1
libstdc++.so.5, Version 5.0, 26.07.2005	CD-ROM 1
libgcc_s.so.1, Version 3.2, 26.07.2005	CD-ROM 1
Betriebsdokumentation – Nexus TSP-Responder 3.1, Version 1.2, 24.01.2007	CD-ROM 2
Systemverwalter-Dokumentation – Nexus TSP-Responder 3.1, Version 1.2, 24.01.2007	CD-ROM 2
Konfigurationsliste – Nexus TSP-Responder 3.1, Version 1.2, 26.01.2007	CD-ROM 2

Die korrekte Einbindung des Nexus TSP-Responders in das Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG ist durch einen Prüfnachweis zu belegen.

c) Nutzung des Produktes

Zum Starten und zur Aufrechterhaltung des Betriebes sind die beiden administrativen Rollen SecAdmin und TechAdmin zu trennen. Jeder der beiden Administratoren ist im Besitz eines Geheimnisteils, welches zum Start und zum sicheren Betrieb des Nexus TSP-Responders notwendig ist:

	SecAdmin	**TechAdmin**
Siegel	X	
Schlüssel zum Elektroschrank		X
Administrationsrechte		X
sichere Signaturerstellungseinheiten (SSEE)		X
PINs der SSEE	X	

SecAdmin
Zu den Aufgaben des SecAdmin gehören die Pflege und Kontrolle der Versiegelungen des Elektroschrankes, des Host-Rechners sowie der sonstigen technischen Komponenten.

Der SecAdmin muss bei jedem manuellen Zugriff des TechAdmin auf den Host-Rechner anwesend sein. Dazu gehören insbesondere die Initialisierung des Nexus TSP-Responders, das Einbringen der SSEE, das Beheben von Fehlern sowie weitere administrative Aufgaben. Der SecAdmin ist für die Aktivierung der SSEE verantwortlich. Er allein kennt die PINs der SSEE und teilt diese den SSEE während des Starts des Nexus TSP-Responders mit. Die Eingabe der PINs muss derart erfolgen, dass keine weitere Person Kenntnis über diese erhält.

TechAdmin
Der TechAdmin ist für das Starten, Beenden und das Überwachen des Nexus TSP-Responders und der Hardware des Host-Rechners verantwortlich. Hierzu gehören auch die Netzwerk-Verbindungen des Host-Rechners und die Funkuhr-Komponente. Der TechAdmin wird während des laufenden Betriebes durch Nachrichten auf dem Protokollierungsrechner über auftretende Fehlersituationen informiert und ist für das Abstellen der Fehlerursachen verantwortlich.

Zugang zum Elektroschrank des Host-Rechners hat der TechAdmin nur zusammen mit dem SecAdmin. Ihm unterliegt die Kontrolle der SSEE. Er darf jedoch nicht in Kenntnis deren PINs sein. Er ist verantwortlich für die einwandfreie Funktion der Kartenterminals.

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

- Betrieb des Nexus TSP-Responders nur in einer vertrauenswürdigen und zutrittsbeschränkten Trust Center Umgebung, die in ein gemäß SigG und SigV bestätigtes Sicherheitskonzept für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 eingebettet ist.

- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.

- Es ist sicherzustellen, dass auf der vom Nexus TSP-Responder benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.

- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE) weitergereicht werden.

- Beim Einsatz von Chipkarten des Typs „CardOS V4.3B“ darf zum Hashen ausschließlich der Hash-Algorithmus SHA-1 eingesetzt werden.

- Beim Einsatz von Chipkarten des Typs „PKS-Card“ dürfen zum Hashen ausschließlich die Hash-Algorithmen SHA-1 und RIPEMD-160 eingesetzt werden.

- Der Einsatz der in der Systemverwalterdokumentation erwähnten sicheren Signaturerstellungseinheiten „G&D StarCOS 3.0“ sowie „Telesec TCOS 3.0“ fällt nicht unter diese Bestätigung.

- Regelmäßige Kontrolle der Meldungen, die auf dem Protokollierungsrechner gespeichert und angezeigt werden, durch den TechAdmin.

- Regelmäßige Kontrolle der Versiegelungen durch den SecAdmin.

- Regelmäßige Überprüfung der Systemzeit (Empfehlung: wöchentlich) gemäß Kapitel 2 der o. g. Dokumentation „Systemverwalter-Dokumentation – Nexus TSP-Responder 3.1“.

Mit Auslieferung des Nexus TSP-Responders ist der Betreiber auf die Einhaltung aller oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch den Nexus TSP-Responder die Algorithmen SHA-1 und RIPEMD-160 und durch die unterstützten SSEE die Algorithmen RSA mit 1024 Bit (PKS-Card, E4KeyCard, E4NetKeyCard) bzw. 2048 Bit (CardOS V4.3B) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende des Jahres 2009 und für den Hash-Algorithmus RIPEMD-160 bis Ende des Jahres 2010 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA (wird durch die SSEE bereitgestellt) reicht für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2011 und für die Schlüssellänge von 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Diese Bestätigung des Nexus TSP-Responders ist somit, abhängig vom Hash-Verfahren und der Mindestschlüssellänge, maximal gültig bis 31.12.2010; 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 technische Komponente für Zertifizierungsdienste *Nexus TSP-Responder Version 3.1* wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung