Sicherheitsbestätigung und Bericht

T-Systems. 02175.TE.12.2007

Nexus Certificate Manager 6.2.1

Technology Nexus AB

Bestätigung
von Produkten für qualifizierte elektronische Signaturen

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

T-Systems GEI GmbH
- Zertifizierungsstelle -

Rabinstr.8, 53111 Bonn

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

Trust Center Komponente
„Nexus Certificate Manager 6.2.1“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems. 02175.TE.12.2007

Bonn, den 21.12.2007

(Dr. Heinrich Kersten)

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 Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. Jahrgang 2007, Teil I S. 179)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Art. 2 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 04. Januar 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 1)

Die Bestätigung zur Registrierungsnummer T-Systems. 02175.TE.12.2007 besteht aus 8 Seiten.

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:

Trust Center Komponente „Nexus Certificate Manager 6.2.1“

Lieferumfang:

Nr.	Typ	Bezeichnung	Version	Datum	Auslieferung
1	Dokumentation	Nexus Certificate Manager, CA Administrator’s Guide	2.0	08.06.2006	CD-ROM (pdf)
2	Dokumentation	Nexus Certificate Manager, System Administrator’s Guide	2.0	13.06.2006	CD-ROM (pdf)
3	Dokumentation	Nexus Certificate Manager, Installation Guide	2.1	29.05.2007	CD-ROM (pdf)
4	Dokumentation	Nexus Certificate Manager, Registration Officer’s Guide	2.0	13.06.2006	CD-ROM (pdf)
5	Dokumentation	Nexus Certificate Manager, High Availability Solution	1.1	27.09.2006	CD-ROM (pdf)
6	Dokumentation	Nexus Certificate Manager, SigG Environment Installation Guide	1.1	10.04.2007	CD-ROM (pdf)
7	Dokumentation	Nexus Certificate Manager, CA Management Handbook	2.0	08.06.2006	CD-ROM (pdf)
8	Software	Nexus Certificate Manager 6.2.1	build 641	12.06.2007	CD-ROM

Tabelle 1: Lieferumfang

Auslieferung:

Die CD-ROM wird per Post, durch einen privaten Zustelldienst oder durch persönliche Übergabe von Mitarbeitern des Herstellers ausgeliefert.

Mit separater Zustellung (per FAX, per Post / Zustelldienst oder persönlicher Übergabe durch Nexus-Mitarbeiter) werden Hashwerte aller Dateien der CD-ROM ausgeliefert, mit deren Hilfe die Integrität dieser Dateien auf der CD-ROM durch den Empfänger verifiziert werden kann.

Hersteller:

Technology Nexus AB
Årstaängsvägen 21c
P.O. Box 47057
100 74 Stockholm
Schweden

2. Funktionsbeschreibung

Nexus Certificate Manager 6.2.1 ist eine Trust Center Komponente und besteht ausschließlich aus Software.

Nexus Certificate Manager 6.2.1 besteht aus Server- und Client-Komponenten, die es einem ZDA insbesondere erlauben, CA- und OCSP-Dienste aufzusetzen.

Unter Nutzung sicherheitsbestätigter Dienste-Karten und sicherheitsbestätigter Signaturanwendungskomponenten steuert Nexus Certificate Manager 6.2.1 den Workflow innerhalb eines Trust Centers. Im Einzelnen besitzt die Komponente folgenden Funktionsumfang:

- Logical Access Control and Authorisation
  (Authentisierung zwischen Server- und Client-Komponenten, Nutzern und Anwendungen)
- CA Policy Administration
  (Verwaltung von Autorisierungen, Administrationsarbeiten z. B. den Inhalt und den Aufbau von Zertifikaten betreffend)
- Certificate Registration
  (Bearbeiten und Speichern von Zertifikatsanträgen)
- Certificate Preparation
  (Erstellen von Zertifikaten, Vorbereitung für die Signatur)
- Certificate Signing
  (Signieren von Zertifikaten mit Hilfe der Dienste-SSEE)
- Certificate Activation
  (Freischalten von Zertifikaten)
- Certificate Status Information Provision
  (Statusauskünfte zu Zertifikaten über OCSP)

- Certificate Publication
  (Veröffentlichung von Zertifikaten im Verzeichnis)
- Certificate Revocation
  (Sperrung von Zertifikaten)
- Audit and CIS Log Review
  (Überprüfen und Auswerten von Log-Aufzeichnungen)
- High Availability Configuration
  (Ausfallsicherheit durch redundante Konfiguration)
- SigG compliant installations
  (Unterstützung für SigG-konforme Installation, s. [6] in Tabelle 1)
- Initial Boot Process
  (Anlaufverfahren zur Erreichung eines sicheren Zustands)

Die Kommunikation zwischen den Servern und Clients erfolgt SSL-basiert (Client- / Server-Authentisierung).

Nexus Certificate Manager 6.2.1 realisiert ein rollenbasiertes Zugriffsmodell mit den Rollen Security Officer und Registration Officer (und weiteren Unterrollen wie Audit Officer, Revocation Officer), die durch Mitarbeiter des ZDA zu besetzen sind. Diese Rolleninhaber sind mit Bediener-Chipkarten[3] auszustatten, die entsprechende Authentisierungs- und Signaturschlüssel beinhalten. Jede Anforderung eines Bedieners an eine Server-Komponente von Nexus Certificate Manager 6.2.1 wird mit der entsprechenden Bediener-Karten elektronisch signiert und in Log-Files aufgezeichnet.

Hinweis:

Weitere Details zu den Eigenschaften von Nexus Certificate Manager 6.2.1 finden sich in den Herstellerunterlagen (s. Tabelle 1) und in den Sicherheitsvorgaben[4] „CM 6.2.1 Security Target“ (Abschnitt 1.6), die der Evaluierung zugrunde lag.

Die SigG-spezifische Konfiguration von Nexus Certificate Manager 6.2.1 wird in Abschnitt 1.6.12 der Sicherheitsvorgaben skizziert, für Details wird auf das Dokument [6] (s. Abschnitt „Lieferumfang“ in dieser Sicherheitsbestätigung) verwiesen.

---

3 Nicht notwendigerweise SigG-konforme SSEEen.

4 Beim Hersteller oder bei der Prüf- und Bestätigungsstelle (unter www.t-systems-zert.com) erhältlich.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ erfüllt die folgenden Anforderungen:

- §17 Abs. 3 Nr. 2 SigG
- §15 Abs. 3 S. 1 SigV
- §15 Abs. 3 S. 2 SigV
- §15 Abs. 3 S. 3 SigV
- §15 Abs. 4 SigV

Da die Schlüsselgenerierung nur innerhalb bestätigter SSEEen abläuft, ist §17 Abs. 3 Nr. 1 SigG für die Komponente nicht relevant.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ wurde evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration:

- Server- und Client-Rechner mit Intel-Prozessor,
- Server-Betriebssystem Windows 2003,
- SQL Server 2005 SP1 (ohne Express und Mobile Editions),
- Client-Betriebssystem Windows XP SP2,
- Java Run Time Environment J2SE 5.0 (internal version 1.5.0),
- sicherheitsbestätigte Funktionsbibliothek „secunet Signierkomponente, Version 1.41ke“ (Sicherheitsbestätigung TUVIT. 93158.TU.11.2007 vom 13.11.2007) als Signaturanwendungskomponente,
- sicherheitsbestätigte SSEEen, die in der Sicherheitsbestätigung TUVIT.93158. TU.11.2007 vom 13.11.2007 in Abschnitt 3.2 a) aufgeführt sind.

Bei den Server-Systemen, auf denen die Komponente installiert ist, ist auf eine gehärtete Konfiguration zu achten: Zusätzliche Software ist auf das betrieblich absolut notwendige Maß zu beschränken, nicht benötigte Dienste und Software sind zu deinstallieren.

Diese Sicherheitsbestätigung für die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ gilt ausschließlich für den Einsatz zusammen mit der oben beschriebenen Hard- und Softwareausstattung. Soll ihr Einsatz zusammen mit einer geänderten Hard- oder Softwareausstattung erfolgen, so ist die Bestätigungsstelle vorab zu informieren und einzubeziehen. Eine Übertragung der Evaluationsergebnisse auf eine andere Einsatzumgebung kann ggf. eine Reevaluation erforderlich machen.

b) Einbindung in die Hard- und Softwareumgebung

Die korrekte Einbindung der Trust Center Komponente „Nexus Certificate Manager 6.2.1“ in das Sicherheitskonzept eines ZDA ist von einer Prüf- und Bestätigungsstelle zu prüfen.

Die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ wird vom Hersteller gemäß Abschnitt 1 ausgeliefert. Das spezifizierte Auslieferungsverfahren ist einzuhalten.

Vor Installation der Trust Center Komponente „Nexus Certificate Manager 6.2.1“ ist zu prüfen,

- ob das in Kapitel 1 dieser Bestätigung genannte Auslieferungsverfahren eingehalten wurde,
- die Originaldatenträger vorliegen und die Hashwerte der Dateien mit den separat ausgelieferten Referenzwerten übereinstimmen,
- ob die Einsatzumgebung den Vorgaben unter 3.2 a) entspricht,
- ob die Konfigurationsvorgaben aus den Herstellerunterlagen (s. Tabelle 1) für den SigG-konformen Betrieb eingehalten wurden, insbesondere folgende Bedingungen erfüllt sind:
  - Die Nutzerart "Virtual Registration Officer" darf keinem Mitarbeiter der Rolle Registration Officer zugeordnet werden.
  - Um SSL-Kommunikation und Client-Authentisierung zu gewährleisten, muss der OCSP-Server so konfiguriert werden, dass in der Datei server.xml (im Lieferumfang [8] enthalten) die folgenden Parameter gesetzt sind: 'scheme="https" secure="true" clientAuth="true"'.
  - In der Konfigurationsdatei cm.conf ist die Priorität der für SSL verwendeten “cipher suites“ wie folgt festzulegen:

    SSLCipher.Prio1=SSL_RSA_WITH_3DES_EDE_CBC_SHA

    SSLCipher.Prio2=SSL_RSA_WITH_RC4_128_SHA
  - Die Komponente ist so zu konfigurieren, dass für jede Verbindung zu einem OCSP Responder Proxy das SSL-Protokoll verwendet wird. Für jede Verbindung, die von einem OCSP Responder Proxy verlangt wird, muss das SSL-

Zertifikat dieses OCSP Responder Proxy dahingehend geprüft werden, ob es gültig und weder abgelaufen noch gesperrt ist.

- Für das Signieren von Zertifikaten muss die Komponente so konfiguriert werden, dass die Algorithmenkombinationen "SHA1 with DSA" oder "SHA1 with ECDSA" nicht verwendet werden.

Über diese Prüfungen ist ein Prüfnachweis zu erstellen.

Die Inbetriebnahme und jede Wiederinbetriebnahme, die eine Neuinstallation erfordert, müssen durch fachkundiges Personal erfolgen.

Die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ darf nur in Verbindung mit vertrauenswürdigen, diese nutzende Anwendungen eingesetzt werden. Dies beinhaltet obligatorische und umfassende Tests dieser Anwendungen und eine Spezifikation der Sicherheitsziele, die diese Anwendungen abdecken. Entwickler und Administratoren solcher Anwendungen müssen diese Bedingungen nachweislich einhalten.

Anwendungen, die die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ nutzen, sind **nicht** Gegenstand dieser Bestätigung.

c) Nutzung des Produktes

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

- Der Betrieb der technischen Komponente ist nur in einer vertrauenswürdigen Umgebung (z. B. einem SigG-konformen Trust Center) zulässig.
- Es ist vertrauenswürdiges Personal einzusetzen.
- Es ist sicherzustellen, dass auf der von der Trust Center Komponente „Nexus Certificate Manager 6.2.1“ genutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Mit Identifikationsmerkmalen, die an Signaturerstellungseinheiten weitergereicht oder die im Zusammenhang mit Sperranträgen benutzt werden, ist vertraulich umzugehen, insbesondere seitens handelnder Personen und beteiligter Anwendungen.
- Alle Mitarbeiter der Rollen Security Officer und Registration Officer müssen mit Bediener-Chipkarten ausgestattet werden, welche den Mitarbeitern zugeordnete private Schlüssel für Zwecke der Authentisierung und Signatur tragen.
- Für Zwecke der internen Kommunikation auf der Basis der Bediener-Karten (nicht aber im Zusammenhang mit SigG-Operationen) nutzt die Komponente RSA-Schlüssel mit einer Länge von 1024 Bit. Es ist regelmäßig zu prüfen, ob die hierdurch gegebene Sicherheit noch ausreichend ist.

- Beim Signieren von qualifizierten Zertifikaten, OCSP-Auskünften und CRLs darf nur die in Abschnitt 3.2 a) angegebene sicherheitsbestätigte Signaturanwendungskomponente eingesetzt werden (mit den dazu passenden Signaturkarten aus der Bestätigung TUVIT.93158.TU.11.2007).
- Von der Trust Center Komponente „Nexus Certificate Manager 6.2.1“ erzeugte Meldungen sind regelmäßig zu kontrollieren und auszuwerten.
- Durch Veränderungen der Einsatzumgebung dürfen die bekannten Schwachstellen in der Konstruktion und bei der operationalen Nutzung nicht ausnutzbar werden, und es dürfen keine neuen Schwachstellen entstehen. In Zweifelsfällen ist eine Prüf- und Bestätigungsstelle hinzuzuziehen.

Mit Auslieferung der Trust Center Komponente „Nexus Certificate Manager 6.2.1“ ist der Anwender auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ verwendet folgende Algorithmen:

- Bei der Erzeugung und Prüfung elektronischer Signaturen wird die Hashfunktion SHA-1 bereitgestellt. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung (s. Bekanntmachung der Bundesnetzagentur vom 17.12.2007) reicht
    - übergangsweise bis zum 30.06.2008,
    - für die Erzeugung qualifizierter Zertifikate bis Ende 2009 bzw. unter zusätzlichen Voraussetzungen (mindestens 20 Bit Entropie bei der Erzeugung von Zertifikats-Seriennummern) bis auf weiteres bis Ende 2010,
    - für die Prüfung qualifizierter Zertifikate bis Ende 2014.

Diese Sicherheitsbestätigung ist somit – abhängig von der Nutzungsart von SHA-1 – mindestens bis zu den angegeben Zeitpunkten gültig.

3.4 Prüfstufe und Mechanismenstärke

Die Trust Center Komponente „Nexus Certificate Manager 6.2.1“ wurde erfolgreich nach der Prüfstufe **EAL3+** der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert.

Die eingesetzten Sicherheitsmechanismen erreichen die Stärke "**hoch**".

Ende der Bestätigung

Sicherheitsbestätigung:
T-Systems. 02175.TE.12.2007

Hrsg.: T-Systems GEI GmbH
Adresse: Rabinstr.8, 53111 Bonn
Telefon: +49-(0)228-9841-0
Fax: +49-(0)228-9841-60
Web: www.t-systems.com/ict-security
www.t-systems-zert.com