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

Signaturanwendungskomponente proNEXT secure framework, Version 2.0

der

procilon IT-Solutions GmbH

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93200.TE.07.2016

registriert.

Essen, 21.07.2016

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 Absatz 111 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

Die Bestätigung zur Registrierungsnummer TUVIT.93200.TE.07.2016 besteht aus 10 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Die proNEXT secure framework, Version 2.0[3] ist eine Signaturanwendungskomponente, die aus einer Clientkomponente (Operations Subsystem) und einer zentralen Serverkomponente (Management Subsystem) besteht.

Auslieferung:

Die Auslieferung des Produktes proNEXT an Betreiber erfolgt durch persönliche Übergabe einer DVD-ROM. Die Checksummen für die Produktbestandteile einschließlich der Dokumentation werden in einer signierten und verschlüsselten E-Mail an den Kunden versandt. Der Lieferumfang des Produktes setzt sich aus folgenden Bestandteilen zusammen:

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
Clientkomponente		
SecureFramework-Operations-1.2.0.tar.gz 70e28c10fd44171919f00270c1a5adfa62487e8559ae43d9bb1fff9cf49a11c178213272bea72b3f2d38292881d3b178260aabcb18aa830040b319e8a287280e	Enthält die ausführbaren Dateien und die signierten Konfigurationen der Clientkomponente	1.2.0
Serverkomponente		
SecureFramework-Management-1.2.0.tar.gz 3b3c8bb4a52efa395ddecc43314f8b862b5b869fbbbf792b1998d688849a713086ec2b075e8310424de71d51d1c3b3999ae3c1e33d8347d92a98ada744bb1b71	Enthält die ausführbaren Dateien und die signierten Konfigurationen der Serverkomponente außer der Komponente Management Security CLI	1.2.0
manageCLI-1.2.0.tar.gz 92df9dcb53a9d10d2f4283fb3b9f2eb2f3f31db2ce51f43d9bc620e04ba0cd4d5da78501ef2e30d1fe9f5d7dacd06ce40292f81fc47af9a61448a384d8a9698e	Enthält die Komponente Management Security CLI, die aus den Skript-Dateien manageMS.sh und checksumMS.sh besteht.	1.2.0

[3] Im Folgenden kurz: proNEXT

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
Benutzerdokumentation		
Dokumentation SecureFramework Client v1.2.0-41.pdf	Installationshandbuch für das Operations Subsystem [AGD_PRE_C]	1.2.0 - 41
Dokumentation SecureFramework Server v1.2.0- 41.pdf	Installationshandbuch für die Clientkomponente [AGD_PRE_S].	1.0
proNEXT_Hardening_Guide_27.1.pdf	Härtungsrichtlinie für die Serverkomponente [AGD_PRE].	vom 11.07.2016
Betriebshandbuch_AGD_ProNEXT_SF_0.9.pdf	Betriebshandbuch [AGD_OPE].	1.2.0 - 41
TOE_Specification_FSP_ProNEXT_SF_1.15.pdf	Functional Specification of the TOE [FSP]	1.15

Tabelle: Auslieferungsbestandteile

Hersteller:

procilon IT-Solutions GmbH
Leipziger Straße 110
04425 Taucha

2 Funktionsbeschreibung

Die Komponente proNEXT ist eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, zum Erstellen und Verifizieren von qualifizierten elektronischen Signaturen.

Die Komponente proNEXT besteht aus zwei Subkomponenten. Die Clientkomponente (Operations Subsystem) wird genutzt, um die Erzeugung und Überprüfung von qualifizierten elektronischen Signaturen anzustoßen. Die Serverkomponente (Management Subsystem) wird genutzt, um die SSEE über die Clientkomponente anzusprechen, um den Signaturprozess auszulösen. Des Weiteren führt die Serverkomponente die Überprüfung einer qualifizierten elektronischen Signatur durch. Dabei werden sowohl die mathematische Korrektheit als auch der Zertifikatsstatus und die Zertifikatskette verifiziert. Die Verbindung zwischen den beiden Subkomponenten erfolgt integritätsgesichert und vertraulich.

Die Serverkomponente von proNext wurde als ausführbare Datei für Linux-Systeme entwickelt. Das Produkt stellt folgende Funktionalitäten zur Verfügung:

- Erstellung und Prüfung von Signaturen nach PKCS#7 und pdf

- Hashen mittels SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und RIPEMD-160 (SHA-1 und RIPEMD-160 nur zur Signaturprüfung)
- Formatierungsverfahren (Padding) RSASSA-PKCS1-V1_5 und RSASSA PSS nach PKCS#1 v2.1: RSA Cryptographic Standard
- ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ und einer Schlüssellänge von 256 Bit zur Prüfung von qualifizierten elektronischen Signaturen mit den oben angegebenen Hashverfahren.
- Überprüfung der Gültigkeit von qualifizierten Zertifikaten beim Zertifizierungsdiensteanbieter unter Verwendung des Online Certificate Status Protocol (OCSP) während der Signaturprüfung
- Unterstützung bestätigter Chipkartenleser mit sicherer PIN-Eingabe
- Unterstützung von sicheren Signaturerstellungseinheiten (SSEE)
- Unterstützung von externen Viewern durch Export von signierten Daten oder Daten die signiert werden sollen in einer vom Benutzer kontrollierten Umgebung. Ferner zeigt das Produkt Informationen an, die Rückschlüsse auf die signierten Daten oder Daten, die signiert werden sollen, zulassen.

Mittels der Clientkomponente der proNEXT wird die Erzeugung bzw. die Überprüfung von qualifizierten elektronischen Signaturen initiiert. Sie baut eine abgesicherte Verbindung zur Serverkomponente auf. Die Clientkomponente muss vertrauenswürdig in eine Anwendung (bspw. proNEXT SecureFramework WebApp, die ausgeliefert wird, aber nicht Gegenstand der Bestätigung ist) eingebunden werden. Sie stellt der Anwendung, die oben genannten Server-Funktionen zur Erzeugung bzw. Prüfung von qualifizierten elektronischen Signaturen und Zertifikaten zur Verfügung, indem sie die Daten an die zentrale Serverkomponente gesichert übermittelt und die Antworten gesichert entgegennimmt.

proNEXT ist eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, die elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen durch eine sichere Signaturerstellungseinheit zuführen kann.

Zusätzlich können mit proNEXT erzeugte qualifizierte elektronische Signaturen und qualifizierte Zertifikate auf ihre Gültigkeit hin überprüft und die Ergebnisse der Überprüfung angezeigt werden. proNEXT bietet hierzu die Möglichkeit, den Zertifikatstatus online bei einem OCSP-Verzeichnisdienst während der Überprüfung der Signatur abzufragen.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Komponente proNEXT erfüllt die Anforderungen nach § 17 Abs. 2 Satz 1 (eindeutige Anzeige und Feststellbarkeit der Daten bei Signaturerzeugung) sowie 2 (Feststellbarkeit der Daten, des Unverändertseins der Daten, der Zuordnung zum Signaturschlüsselinhaber, des Inhalts des qualifizierten Zertifikats und des Ergebnisses der Nachprüfung von Zertifikaten bei Signaturprüfung) SigG und nach

§ 15 Abs. 2 Satz 1 (keine Preisgabe der Identifikationsdaten, Signatur nur durch berechtigt signierende Person, eindeutige Anzeige der Signatur vor Erzeugung) und 2 (korrekte Prüfung der Signatur und eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) sowie Abs. 4 (Erkennbarkeit von sicherheitstechnischen Veränderungen) SigV.

3.2 Einsatzbedingungen

Die Anforderungen aus SigG und SigV gemäß Abschnitt 3.1 werden erfüllt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

Grundlage dieser Bestätigung ist der Einsatz von proNEXT in einem ***geschützten Einsatzbereich***. Für den sicheren Einsatz von proNEXT und zur Verhinderung von erfolgreichen Angriffen mit den Zielen, dass:

- Daten signiert werden, die nicht signiert werden sollen,
- das Prüfergebnis der Signatur- bzw. Zertifikatprüfung falsch angezeigt wird,
- die Geheimhaltung des Identifikationsmerkmals (PIN) nicht gewährleistet ist,

sind die folgenden Auflagen zu beachten:

3.2.1 Auflagen zur Anbindung an das Internet

Eine Netzverbindung von der Serverkomponente zum Verzeichnisdienst des Zertifizierungsdienstes ist für die Prüfung der Gültigkeit von Zertifikaten notwendig. Die Netzverbindung muss so abgesichert sein, z. B. durch geeignet konfigurierte Firewalls und Virenscanner, dass Schadsoftware und Angriffe aus dem Internet erkannt bzw. unterbunden werden. Die Verbindung zwischen der Client- und der Serverkomponente ist innerhalb des internen Netzwerks.

3.2.2 Auflagen zur Anbindung an ein Intranet

Wenn die zentrale Serverkomponente oder die Clientkomponente in einem Intranet betrieben werden, so muss die jeweilige Netzverbindung geeignet abgesichert sein, z. B. durch geeignet konfigurierte Firewalls und Virenscanner, dass Schadsoftware und Angriffe aus dem Intranet erkannt bzw. unterbunden werden.

Das Betriebssystem des Servers, auf welchem die Serverkomponente installiert wird, muss so konfiguriert sein, dass ein Fernzugriff nur nach erfolgreicher 2-Faktor Authentisierung über eine SSL geschützte Verbindung aus dem internen Netzwerk möglich ist. Neben dieser Verbindung, soll lediglich die Verbindung zwischen der Server- und Clientkomponente möglich sein.

3.2.3 Auflagen zur Sicherheit der IT-Plattform und Applikationen

Der Benutzer von proNEXT muss sich davon überzeugen, dass keine Angriffe von den Rechner-Plattformen und den dort vorhandenen Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf den Rechner-Plattformen installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf den Rechner-Plattformen keine Viren oder Trojanischen Pferde eingespielt werden können,

3. die Rechner-Plattformen nicht unzulässig verändert werden können,
4. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. Dieses kann die in Abschnitt 3.2 angegeben Folgen haben.

Die Integrität der proNEXT Installation ist auf den IT-Plattformen regelmäßig zu überprüfen.

3.2.4 Auflagen zur Auslieferung und Installation des Produktes

Die Auslieferungsbestandteile der proNEXT umfassen die beiden Dateien „SecureFramework-Operations-1.2.0.tar.gz“ (ausführbaren Dateien für die Clientkomponente) und „SecureFramework-Management-1.2.0.tar.gz“ (ausführbaren Dateien für die Serverkomponente) sowie die Datei „manageCLI-1.2.0.tar.gz“ (Skript-Dateien für die Serverkomponente).

Die Auslieferung der Dateien erfolgt durch persönliche Übergabe einer DVD-ROM. Die Checksummen für die Produktbestandteile einschließlich der Dokumentation werden in einer signierten und verschlüsselten E-Mail an den Kunden versandt.

Die Clientkomponente von proNEXT ist für die folgende technische Einsatzumgebung vorgesehen:

- Betriebssystem:
  - Microsoft Windows 7 / 10,
  - Apple Mac OS X 10,
  - Ubuntu Desktop 14.04 LTS,
  - Oracle Java SE Runtime Environment (JRE) 8 with Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8.
- sichere Signaturerstellungseinheit:
  - G&D STARCOS 3.4 Health QES C1 mit Bestätigungs-ID BSI.02120.TE.05.2009 vom 19.05.2009, gültig bis 31.12.2021
  - G&D STARCOS 3.5 ID ECC C1 mit Bestätigungs-ID SRC.00013.TE.10.2012 vom 12.11.2012, gültig bis 31.12.2018,
  - G&D STARCOS 3.5 ID ECC C1R mit Bestätigungs-ID n SRC.00021.TE.05.2013 vom 13.05.2013, gültig bis 31.12.2019,
  - TCOS 3.0 Signature Card Version 2.0 Release 1 mit Bestätigungs-ID SRC.00016.TE.11.2012 vom 28.11.2012, gültig bis 31.12.2018.
- bestätigte Kartenleser:
  - ReinerSCT cyberJack e-com 3.0 (USB) mit Bestätigungs-ID TUVIT.93155.TE.09.2008 vom 16.09.2008, gültig bis 31.12.2017
  - ReinerSCT cyberJack RFID standard (USB), Version 1.2 mit Bestätigungs-ID TUVIT.93188.TU.07.2011 vom 19.07.2011, gültig bis 31.12.2017

- ReinerSCT cyberJack RFID komfort (USB), Version 2.0 mit Bestätigungs-ID TUVIT.93180.TU.12.2011 vom 16.12.2011, gültig bis 31.12.2017
- ReinerSCT cyberJack secoder smartcard reader, Version 3.0 mit Bestätigungs-ID TUVIT.93154.TE.09.2008 vom 16.09.2008, gültig bis 31.12.2017
- Cherry SmartTerminal ST-2xxx smartcard reader, Version 6.01 mit Bestätigungs-ID BSI.02124.TE.09.2010 vom 24.09.2010 und Nachtrag vom 02.11.2015, gültig bis 31.12.2021. (Nutzung nur mit Windows oder Linux Betriebssystem).

Die Serverkomponente von proNEXT ist für die folgende technische Einsatzumgebung vorgesehen:

- Serverhost:
  - WildFly 8.2.0 Final application server running on OpenJDK 1.8.0 (Linux x64)
- Betriebssystem:
  - Ubuntu Server 14.04 LTS operating system (64bit),
- Datenbank:
  - Oracle Database 11g, 12c oder IBM DB2 Database 10.5
- weitere:
  - proNEXT CertificateManagement v1.0.0 oder höher und kompatibel als Certificate Management Server
  - JCOP v2.4.1 Revision 3 Hardware Security Module (HSM), Common Criteria Certification ID: BSI-DSZ-CC-0674

Eine Übertragung der Evaluationsergebnisse auf andere Einsatzumgebungen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Signaturanwendungs-komponente proNEXT darf deshalb ausschließlich in der oben beschriebenen Einsatzumgebung eingesetzt werden. Vor der Installation muss die Integritätsprüfung der ausgelieferten Bestandsteile vorgenommen werden. Dabei sollen die SHA-512 Checksummen der Bestandteile mit den jeweiligen, die durch den Herstelle per E-Mail geliefert worden sind.

Ferner ist zu beachten: Eine Frontend-Anwendung (proNEXT SecureFramework WebApp) wird mit dem Produkt ausgeliefert, ist jedoch nicht Gegenstand der Bestätigung. Es dürfen andere vertrauenswürdige Anwendungen eingesetzt werden, welche die bereitgestellten Sicherheitsfunktionen sachgerecht nutzen und auf Fehlermeldungen korrekt reagieren. Ferner müssen sicherheitstechnische Veränderungen an der Anwendung für den Nutzer erkennbar werden.

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

3.2.5 Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Die zentrale Serverkomponente und die Clientkomponente, sowie der verwendete Chipkartenleser müssen gegen eine unberechtigte Benutzung gesichert sein, damit:

1. die auf den jeweiligen Rechner-Plattformen installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,
2. auf den jeweiligen Rechner-Plattformen keine Viren oder Trojanischen Pferde eingespielt werden können,
3. die jeweiligen Rechner-Plattformen nicht unzulässig verändert werden können,
4. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wird, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. (siehe auch Abschnitt 3.2.3).

Die Unterrichtung durch den Zertifizierungsdiensteanbieter zur Handhabung der SSEE ist zu beachten.

3.2.6 Auflagen zum Schutz vor Angriffen über Datenaustausch per Datenträger

Bei Einspielung von Daten über Datenträger muss gewährleistet werden, dass

1. die installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann und
2. keine Viren oder Trojanischen Pferde eingespielt werden können,

um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern (siehe auch Abschnitt 3.2.3).

3.2.7 Auflagen zur Sicherheitsadministration des Betriebes

Eine Sicherheitsadministration des Betriebes von proNEXT secure framework ist nicht vorgesehen. Eine vertrauenswürdige Administration der jeweiligen Rechner-Plattformen sowie der Internet- bzw. Intranetanbindung muss sichergestellt werden.

Der Client-Administrator muss jederzeit die volle Kontrollmöglichkeit über die Rechner-Plattform haben, auf denen die Clientkomponente installiert wurde.

Der Server-Administrator muss jederzeit die volle Kontrollmöglichkeit über die Rechner-Plattform haben, auf denen die Serverkomponente installiert wurde. Zusätzlich muss die Serverkomponente in der Art geschützt werden, dass keine externen Personen Zugriff zum Netzwerk erlangen können, in welchen sie installiert wurde.

Der Server-Administrator muss sich erfolgreich identifizieren und authentifizieren, um Zugang zur Serverkomponente zu erlangen.

Das Betriebssystem des Servers, auf welchem die Serverkomponente installiert wird, muss so konfiguriert sein, dass ein Fernzugriff nur nach erfolgreicher 2-Faktor Authentisierung über eine SSL geschützte Verbindung aus dem internen Netzwerk möglich ist. Neben dieser Verbindung, soll lediglich die Verbindung zwischen der Server- und Clientkomponente möglich sein.

3.2.8 Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz von proNEXT secure framework zu beachten:

- Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Benutzer hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet wird noch dass die PIN anderen Personen bekannt gemacht wird.
- Die Integritätsprüfung der Auslieferungsbestandteile ist, so wie in Abschnitt 3.3 des Betriebshandbuchs beschrieben.
- Der Administrator der Serverkomponente muss alle Anforderungen und Sicherheitshinweise bei dem Betrieb der Serverkomponente befolgen, so wie in Abschnitt 4 des Betriebshandbuchs beschrieben.
- Der Administrator der Clientkomponente muss alle Anforderungen und Sicherheitshinweise bei dem Betrieb der Clientkomponente befolgen, so wie in Abschnitt 5 des Betriebshandbuchs beschrieben.
- Die verwendete Anwendung stellt der Clientkomponente die zu signierenden Daten integer zur Verfügung.
- Die Authentifizierungsdaten für die Anmeldung an der zentralen Serverkomponente sind vertraulich zu behandeln.
- Der Anwendungsentwickler hat den Anwender darauf hinzuweisen, wie er die Integrität der Anwendung überprüfen kann.

3.2.9 Anforderungen an das Wartungs-/Reparaturpersonal

Eine Wartung bzw. Reparatur von proNEXT secure framework ist nicht vorgesehen. Eine Wartung bzw. Reparatur der jeweiligen Rechner-Plattformen ist nur von vertrauenswürdigen und fachkundigen Personen durchzuführen. Im Falle einer fehlerhaften Integritätsprüfung (Abweichung von den hinterlegten Checksummen) ist der Betreiber der proNEXT zu informieren.

3.2.10 Authentisierung des Wartungs-/Reparaturpersonals

Eine Wartung bzw. Reparatur von proNEXT ist nicht vorgesehen.

3.2.11 Aufbewahrung/Transport der Produkte

Es ist darauf zu achten, dass das Produkt geschützt aufbewahrt wird.

Mit Auslieferung von proNEXT ist der Betreiber auf die Einhaltung aller oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt die Hashfunktionen SHA-256, SHA-384, SHA-512 sowie durch die unterstützten SSEE der Algorithmus RSA mit 2048 und 4096 Bit oder ECDSA mit 256 Bit verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden vom Produkt die Hashfunktionen SHA-1, RIPEMD-160, SHA-224, SHA-256, SHA-384, SHA-512 und RSA mit RSASSA-PKCS1-V1_5 und RSASSA PSS Padding und den Schlüssellängen 2048 und 4096 Bit sowie das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ und der Schlüssellänge 256 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht Verwendung für die Hashfunktionen SHA-256, SHA-384 und SHA-512 bis Ende des Jahres 2022 (siehe BAnz. AT 14.04.2016 B11).

Zur Prüfung qualifizierter Zertifikate reicht die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen SHA-1 und RIPEMD-160 bis Ende des Jahres 2015 (siehe BAnz. AT 14.04.2016 B11).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA mit RSASSA-PKCS1-V1_5 Padding reicht für die Mindestschlüssellänge von 1976 Bit bis Ende des Jahres 2016 (siehe BAnz. AT 14.04.2016 B11).

Die Gültigkeit der Bestätigung des Produkts in Abhängigkeit von Hash-Algorithmus, RSA-Mindestschlüssellänge sowie Padding-Verfahren kann der folgenden Tabelle entnommen werden:

Hash-funktion / **Signaturverfahren**	**RIPEMD-160, SHA-1 und SHA-224 zur Prüfung von qualifizierten Signaturen**	**SHA-256, SHA-384, SHA-512**
RSA: 2048 und 4096, RSASSA-PKCS1-V1_5	**-**	**2016**
RSA: 2048 und 4096, RSASSA-PSS	**-**	**2022**
ECDSA 256	**-**	**2022**

Diese Bestätigung der Komponente proNEXT ist für die Erzeugung von elektronischen Signaturen maximal gültig:

- bis 31.12.2016 bei Verwendung von RSASSA-PKCS1-V1_5
- bis 31.12.2022 bei Verwendung von RSASSA-PSS oder ECDSA.

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 proNEXT wurde erfolgreich nach der Prüfstufe EAL4+ mit AVA_VAN.5 (vollständige Missbrauchsanalyse und hohes Angriffspotential) der Common Criteria (CC) V3.1 Revision 4 evaluiert.

Die für die Signaturanwendungskomponenten nach SigV maßgebende Prüfstufe EAL4+ mit AVA_VAN.5 (vollständige Missbrauchsanalyse und hohes Angriffspotential) wird damit erreicht.

Ende der Bestätigung

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

Nachtrag 1 zur Bestätigung TUVIT.93200.TE.07.2016 vom 21.07.2016

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 o. g. Bestätigung der

Signaturanwendungskomponente proNEXT secure framework, Version 2.1

der

procilon IT-Solutions GmbH

ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen der Abschnitte 1, 2 und 3.3 beibehält.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 30.09.2016 festgehalten.

Essen, 30.09.2016

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 Absatz 111 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Dieser Abschnitt „1 Handelsbezeichnung des Produktes und Lieferumfang“ ersetzt den Abschnitt 1 der Bestätigung TUVIT.93200.TE.07.2016 vom 21.07.2016 aufgrund der Ablösung der Version 2.0 durch die Version 2.1 der Signaturanwendungskomponente proNEXT secure framework und die damit einhergehenden Änderungen der Auslieferungsbestandteile*.*

Die proNEXT secure framework, Version 2.1[3] ist eine Signaturanwendungskomponente, die aus einer Clientkomponente (Operations Subsystem) und einer zentralen Serverkomponente (Management Subsystem) besteht. Die proNEXT secure framework, Version 2.1 löst die Version 2.0 ab, die nicht mehr unter die Bestätigung fällt.

Auslieferung:

Die Auslieferung des Produktes proNEXT an Betreiber erfolgt durch persönliche Übergabe einer DVD-ROM. Die Checksummen für die Produktbestandteile einschließlich der Dokumentation werden in einer signierten und verschlüsselten E-Mail an den Kunden versandt. Der Lieferumfang des Produktes setzt sich aus folgenden Bestandteilen zusammen:

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
Clientkomponente		
SecureFramework-Operations-1.2.1.tar.gz 8b5ff193dd0a6d170ce8ec6829bce54d45dea6b462fc6f21d4d01ee926df65df0a3becc52ed4d4afc459b36fd2e13c1a1d02441e330eb97e77144cd1d37c540f	Enthält die ausführbaren Dateien und die signierten Konfigurationen der Clientkomponente	1.2.1
Serverkomponente		
SecureFramework-Management-1.2.1.tar.gz 702e18b2f12a20df420e88399496ec96b571d5e7a612b0f3582204d17a51038b40f1f07610e7c30e212311ebb7765af3e90083ea39620b2c5a0b0ad44e6c6347	Enthält die ausführbaren Dateien und die signierten Konfigurationen der Serverkomponente außer der Komponente Management Security CLI	1.2.1
manageCLI-1.2.1.tar.gz 0f6eb7b46f67d39b29e21fef6d955c	Enthält die Komponente Management Security CLI, die aus den Skript-Dateien	1.2.1

[3] Im Folgenden kurz: proNEXT

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
f18031e4f57582410cd1555256ce5d313f8a8ceefdfcf1bd95b1fda4c320e1f469030723bd0c2d3fcb4b1d1c8d59888772	manageMS.sh und checksumMS.sh besteht.	
Benutzerdokumentation		
Dokumentation SecureFramework Client v1.2.0-41.pdf	Installationshandbuch für das Operations Subsystem [AGD_PRE_C]	1.2.0 - 41
Dokumentation SecureFramework Server v1.2.0-41.pdf	Installationshandbuch für die Clientkomponente [AGD_PRE_S].	1.0
proNEXT_Hardening_Guide_27.1.pdf	Härtungsrichtlinie für die Serverkomponente [AGD_PRE].	vom 11.07.2016
Betriebshandbuch_AGD_ProNEXT_SF_0.9.pdf	Betriebshandbuch [AGD_OPE].	1.2.0 - 41
TOE_Specification_FSP_ProNEXT_SF_1.15.pdf	Functional Specification of the TOE [FSP]	1.15

Tabelle: Auslieferungsbestandteile

Hersteller:

procilon IT-Solutions GmbH
Leipziger Straße 110
04425 Taucha

2 Funktionsbeschreibung

Dieser Abschnitt „2 Funktionsbeschreibung“ ersetzt den Abschnitt 2 der Bestätigung TUVIT.93200.TE.07.2016 vom 21.07.2016 aufgrund des Wegfalls des Paddingsverfahrens RSASSA-PKCS1-V1_5.

Die Komponente proNEXT ist eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, zum Erstellen und Verifizieren von qualifizierten elektronischen Signaturen.

Die Komponente proNEXT besteht aus zwei Subkomponenten. Die Clientkomponente (Operations Subsystem) wird genutzt, um die Erzeugung und Überprüfung von qualifizierten elektronischen Signaturen anzustoßen. Die Serverkomponente (Management Subsystem) wird genutzt, um die SSEE über die Clientkomponente anzusprechen, um den Signaturprozess auszulösen. Des Weiteren führt die Serverkomponente die Überprüfung einer qualifizierten elektronischen Signatur durch. Dabei werden sowohl die mathematische

Korrektheit als auch der Zertifikatsstatus und die Zertifikatskette verifiziert. Die Verbindung zwischen den beiden Subkomponenten erfolgt integritätsgesichert und vertraulich.

Die Serverkomponente von proNext wurde als ausführbare Datei für Linux-Systeme entwickelt. Das Produkt stellt folgende Funktionalitäten zur Verfügung:

- Erstellung und Prüfung von Signaturen nach PKCS#7 und pdf
- Hashen mittels SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und RIPEMD-160 (SHA-1 und RIPEMD-160 nur zur Signaturprüfung)
- Formatierungsverfahren (Padding) RSASSA PSS nach PKCS#1 v2.1: RSA Cryptographic Standard
- ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ und einer Schlüssellänge von 256 Bit zur Prüfung von qualifizierten elektronischen Signaturen mit den oben angegebenen Hashverfahren.
- Überprüfung der Gültigkeit von qualifizierten Zertifikaten beim Zertifizierungsdiensteanbieter unter Verwendung des Online Certificate Status Protocol (OCSP) während der Signaturprüfung
- Unterstützung bestätigter Chipkartenleser mit sicherer PIN-Eingabe
- Unterstützung von sicheren Signaturerstellungseinheiten (SSEE)
- Unterstützung von externen Viewern durch Export von signierten Daten oder Daten die signiert werden sollen in einer vom Benutzer kontrollierten Umgebung. Ferner zeigt das Produkt Informationen an, die Rückschlüsse auf die signierten Daten oder Daten, die signiert werden sollen, zulassen.

Mittels der Clientkomponente der proNEXT wird die Erzeugung bzw. die Überprüfung von qualifizierten elektronischen Signaturen initiiert. Sie baut eine abgesicherte Verbindung zur Serverkomponente auf. Die Clientkomponente muss vertrauenswürdig in eine Anwendung (bspw. proNEXT SecureFramework WebApp, die ausgeliefert wird, aber nicht Gegenstand der Bestätigung ist) eingebunden werden. Sie stellt der Anwendung, die oben genannten Server-Funktionen zur Erzeugung bzw. Prüfung von qualifizierten elektronischen Signaturen und Zertifikaten zur Verfügung, indem sie die Daten an die zentrale Serverkomponente gesichert übermittelt und die Antworten gesichert entgegennimmt.

proNEXT ist eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, die elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen durch eine sichere Signaturerstellungseinheit zuführen kann.

Zusätzlich können mit proNEXT erzeugte qualifizierte elektronische Signaturen und qualifizierte Zertifikate auf ihre Gültigkeit hin überprüft und die Ergebnisse der Überprüfung angezeigt werden. proNEXT bietet hierzu die Möglichkeit, den Zertifikatstatus online bei einem OCSP-Verzeichnisdienst während der Überprüfung der Signatur abzufragen.

3.3 Algorithmen und zugehörige Parameter

Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93200.TE.07.2016 vom 21.07.2016 aufgrund des Wegfalls des Paddingsverfahrens RSASSA-PKCS1-V1_5.

Bei der Erzeugung qualifizierter elektronischer Signaturen werden vom Produkt die Hashfunktionen SHA-256, SHA-384, SHA-512 sowie durch die unterstützten SSEE der Algorithmus RSA mit 2048 und 4096 Bit oder ECDSA mit 256 Bit verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden vom Produkt die Hashfunktionen SHA-1, RIPEMD-160, SHA-224, SHA-256, SHA-384, SHA-512 und RSA mit RSASSA PSS Padding und den Schlüssellängen 2048 und 4096 Bit sowie das ECDSA-Verfahren basierend auf Gruppen $E(F_p)$ und der Schlüssellänge 256 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht Verwendung für die Hashfunktionen SHA-256, SHA-384 und SHA-512 bis Ende des Jahres 2022 (siehe BAnz. AT 14.04.2016 B11).

Zur Prüfung qualifizierter Zertifikate reicht die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen SHA-1 und RIPEMD-160 bis Ende des Jahres 2015 (siehe BAnz. AT 14.04.2016 B11).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA mit RSASSA PSS Padding reicht für die Mindestschlüssellänge von 1976 Bit bis Ende des Jahres 2022 (siehe BAnz. AT 14.04.2016 B11).

Die Gültigkeit der Bestätigung des Produkts in Abhängigkeit von Hash-Algorithmus, RSA-Mindestschlüssellänge sowie Padding-Verfahren kann der folgenden Tabelle entnommen werden:

Hash-funktion / **Signaturverfahren**	**RIPEMD-160, SHA-1 und SHA-224 zur Prüfung von qualifizierten Signaturen**	**SHA-256, SHA-384, SHA-512**
RSA: 2048 und 4096, RSASSA-PSS	**-**	**2022**
ECDSA 256	**-**	**2022**

Diese Bestätigung der Komponente proNEXT ist für die Erzeugung von elektronischen Signaturen maximal gültig:

- bis 31.12.2022 bei Verwendung von RSASSA-PSS oder ECDSA.

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.

Ende der Bestätigung