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 BNotK TrustCenter Version 1.0

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93194.TE.02.2014

registriert.

Essen, 27.02.2014

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.93194.TE.02.2014 besteht aus 9 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

BNotK TrustCenter, Version 1.0[3]

Auslieferung:

Die Auslieferung des Produktes BNotK TrustCenter an Zertifizierungsdiensteanbieter erfolgt durch persönliche Übergabe einer DVD-ROM. Der Lieferumfang des Produktes setzt sich aus folgenden Bestandteilen zusammen:

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
CA-Subsystem		
EJBCA v5.0.10_procilon.5 (File name: EJBCA-5.0.10_procilon.5.tar.gz) 200468b7cde8bf15084963f5f567112565e08e88bb8655fb510c2d57f25b096afaad388692a4c7d59efcd9383eb95ebfc92bd6e95ba28c1e44acac68a359ee00	Sourcecode	5.0.10_procilon.5
CertificateDataExtension 1.2.2 (File name: CertificateDataExtension-1.2.2-1.tar.gz) cbbc3e6c770619abd4d39b656612d96a7a7f5de3bade41c71d34706031a8b4a2c48ad17389ae5bd3b2547cb5eeb98882098aa80c7b1e19635345e9b5323880e2	Java Archiv	1.2.2
manageCA 1.1.0 (File name: manageCA.zip) 5146a04f164e25af893caccb86ee0d1c4f4aba2839f45ddd1a881501d7925e1eee673113857520fa51ec571a96440f27b5092a6f09515a441f90119066270c7b	Shellscript	1.1.0
MessageTypeExtension 1.1.3 (File name: : MessageTypeExtension-1.1.3-	Java Archiv	1.1.3

[3] Im Folgenden kurz mit BNotK TrustCenter bezeichnet.

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
1.tar.gz) d7aa184cf5f086ae96ff8a7ec8d0719ecbb0bd81b72a5741bdad1d813b1f5d67aaa48ed667739212632a2c2c70680e9d6d94431f40b10d2aeea477acdb95b69a		
OCSP-Subsystem		
EJBCA v5.0.10_procilon.5 (File name: EJBCA-5.0.10_procilon.5.tar.gz) 200468b7cde8bf15084963f5f567112565e08e88bb8655fb510c2d57f25b096afaad388692a4c7d59efcd9383eb95ebfc92bd6e95ba28c1e44acac68a359ee00	Sourcecode	5.0.10_procilon.5
TimeStatusMonitor 1.2.0 (File name: TimeStatusMonitor.zip) ecddd3089b9dde877afb671ea5f75449d7aa930ac0eaf5e37b4df5be5bf6cdab51398e6cd978808cc204c2731579b05ee0adfbbf477d26db585b2f3682a27aef	Shellscript	1.2.0
manageOCSP 1.1.3 (File name: manageOCSP-1.1.3.tar.gz) e84f2bb6e8301224b951171a39aac59cb895e6913c4a109bab592e6ddf66e6cff1e49a03081bde8edb8e310367ac8de1bf382e4d2209d3d9941710347f9b6cfa	Shellscript	1.1.3
TSS-Subsystem		
manageTSS 1.1.0 (File name: manageTSS.zip) 784de4fe959e6c9542a16e67e984fad191566e4dd598847a23ed74959043ea4606a721708205a16a5f68d206219ca5f66ce8c5659a253e939cb227ff1f2d6086	Shellscript	1.1.0

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
SignServer 3.4.2 (File name: signserver-3.4.2.zip) fff96919013b641af73371356ed0b2fce0e5b514f4e133f68811bf113ce57ca7c01dd167ae628597cd9bf119f296b596cfea808d5d0f7af23d21aeac4b3baf1c	Sourcecode	3.4.2
SignServer-TimeMonitor 1.1.5 (File name: signserver-timemonitor-1.1.5.zip) a3ef3c68f63ca26c2c83235ad89f4e1403bf1bd6556b2793a8311aa4c6ebd8a12ea1bf925ed9ecfa027cc60e2e50a6cd7808404f07eb269d0e59b302ef1fccc3	Sourcecode	1.1.5
StatusMonitor 1.2.0 (File name: StatusMonitor.zip) 852cac415938908b0a9dbf085dd98782bd6279d6b435feabfb1fec448637974b9bc9b36be238bf8bba558d3611208c34bccbc1184b9ac0bf6b63d3b35212c72b	Shellscript	1.2.0
Benutzerdokumentation		
Preparative guidance documentation BNotK TrustCenter Installationshandbuch [AGD_PRE] (File name: Installationshandbuch_1.0.pdf) 95bd725e1f675a84e997a1976ac7ce14eb7605d04e0e5e2f1c67ddaeb39ecda5ba81612a6d6295f4d651dbdbc653e99c1e81937bde52303eec7ceac15a8ad10	Benutzerdokumentation	1.0
Operative guidance documentation BNotK TrustCenter Betriebshandbuch [AGD_OPE] (File name: Betriebshandbuch_1.0.pdf) 4a654719a57f25d35d93a70a8c6b	Benutzerdokumentation	1.0

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
24c9b4ac4f4bd0b95f537c9bd7c2d b9ef53cff6920f70887a93cc2db191 0e8bcb5ce1052d24a41f185764e81 81f45df53357		
BNotK TrustCenter TOE Specification [FSP] (File name: TOE_Specification_1.0.pdf) 426c85180f85061613f1127427d80 9e49e7197ce9b237555e17b30874 a8f0eec9b41c252e6501d8e349829 293240e4dcd64438f039f120c95e3 705b86f338e5e	Benutzerdokumentation	1.0

Tabelle: Auslieferungsbestandteile

Die Checksummen für die Produktbestandteile einschließlich der Dokumentation werden in einer signierten und verschlüsselten E-Mail an den Kunden versandt.

Hersteller:

procilon IT-Solutions GmbH
Leipziger Straße 110
04425 Taucha

2 Funktionsbeschreibung

Die Komponente BNotK TrustCenter mit den Subsystemen CA, OCSP und TSS ist eine technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12 b), c) SigG, die innerhalb der gesicherten Umgebung des Trustcenters eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG zum Einsatz kommt und qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar hält sowie qualifizierte Zeitstempel erstellt. Die Komponente BNotK TrustCenter führt im Sinne von § 2 Nr. 11 a) SigG Zertifikate dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zu. Für diese Zwecke muss die Komponente BNotK TrustCenter sicher in die Infrastruktur eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG eingebunden werden.

Das Erzeugen der qualifizierten elektronischen Signaturen zu den Verzeichnisdienst- und Zeitstempeldienst-Auskünften sowie zu den qualifizierten Zertifikaten erfolgt mittels der in Abschnitt 3.2 aufgeführten sicheren Signaturerstellungseinheiten (SSEE) mit der Hashfunktion SHA-256 und dem Signaturverfahren RSA-2048.

Eingehende Zeitstempelanfragen müssen die Hashalgorithmen SHA-256, SHA-384 oder SHA-512 verwenden.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Komponente BNotK TrustCenter erfüllt die Anforderungen nach SigG § 17 Abs. 3 Nr. 2 (Schutz vor unbefugter Veränderung und unbefugtem Abruf von qualifizierten Zertifikaten) und Nr. 3 (Ausschluss von Fälschungen und Verfälschungen bei Zeitstempelerzeugung) sowie SigV § 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 (sicherheitstechnische Veränderungen erkennbar).

Für die Erzeugung qualifizierter elektronischer Signaturen für qualifizierte Zertifikate erfüllt die Komponente BNotK TrustCenter zusätzlich die Anforderungen von § 15 Abs. 2 Nr. 1 SigG.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Der BNotK TrustCenter wurde für die gesicherte Einsatzumgebung des Trustcenters eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration:

- CA-, OCSP-, TSS-Subsystem Host-Rechner mit
  - Ubuntu 12.04 LTS Betriebssystem mit NTP Client, der für die Synchronisation genutzt wird,
  - JBoss 5.1.0 Anwendungsserver mit OpenJDK 1.6.0 (Linux x64),
  - Mozilla Firefox Browser V 25.0 oder nachfolgende kompatible Versionen,
  - Postfix 2.9 Mail Transfer Agent zum Senden von Meldungen.
- CA, OCSP-, TSS-Datenbank Rechner mit
  - Oracle 11g Enterprise Edition Datenbank Managementsystem.
- LDAP-Datenbank zum Abrufbarhalten der Zertifikate
  - OpenLDAP 2.4.
- Meinberg Lantime M300/PZF-MQ/RPS NTP Server mit DCF77 Empfänger.
- sichere Signaturerstellungseinheit:
  - STARCOS 3.5 ID ECC C1 (Bestätigung SRC.00013.TE.10.2012 vom 12.11.2012, Ablaufdatum gemäß Bestätigung 31.12.2018).
- Chipkartenleser
  - cyberJack® e-com 3.0 (Bestätigung TUVIT.93155.TE.09.2008 vom 16.09.2008, kein Ablaufdatum gemäß Bestätigung).

Die Komponente BNotK TrustCenter besteht aus drei Subsystemen. Das CA-Subsystem wird genutzt, um Zertifikate auszustellen und zu veröffentlichen, das OCSP-Subsystem stellt Informationen über den Status der Zertifikate zur Verfügung und das TSS- Subsystem stellt qualifizierte Zeitstempel aus. Die drei BNotK TrustCenter-Subsysteme (CA, OCSP, Zeitstempel) müssen auf drei verschiedenen Servern installiert werden. Alle Zugriffe auf den Datenbankserver und die LDAP-Datenbank erfolgen über einen verschlüsselten Kanal. Die SSEE müssen in von den Servern physikalisch getrennten Kartenleserracks untergebracht sein, die jeweils an die Server via USB-Verbindungen angeschlossen sind.

Eine geeignete Umsetzung dieser Anforderungen ist vor dem Betrieb beim Zertifizierungsdiensteanbieter zu überprüfen.

Der BNotK TrustCenter 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) Einbindung in die Trustcenter-Umgebung

Die korrekte Einbindung von BNotK TrustCenter in das Trustcenter eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG ist durch einen Prüfnachweis zu belegen.

c) Nutzung des Produktes im Trustcenter

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

- Der Betrieb der Komponente BNotK TrustCenter erfolgt nur in einer vertrauenswürdigen und zugangsbeschränkten Trustcenter Umgebung, 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 BNotK TrustCenter benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Der Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE) weitergereicht werden, ist vertraulich geregelt.
- Remote-Verbindungen mit dem BNotK TrustCenter müssen im Sicherheitskonzept des Zertifizierungsdiensteanbieters betrachtet werden. Die Remote-Verbindungen müssen eine Zweifaktor-Authentifizierung umsetzen und einen sicheren Kanal aufbauen.
- Die eingesetzten SSEE müssen eine gültige Bestätigung nach SigG aufweisen.
- Es ist sicherzustellen, dass ausschließlich die zum jeweiligen Zeitpunkt gültigen Algorithmen (laut Veröffentlichung im Bundesanzeiger) eingesetzt werden.

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

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch die unterstützten SSEE der Algorithmus SHA-256 und der Algorithmus RSA-2048 (STARCOS 3.5 ID ECC C1) verwendet. Das durch die SSEE unterstützte Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS#1 v2.1: RSA Cryptographic Standard, 14.06.2002. Das durch die SSEE unterstützte Formatierungsverfahren RSASSA-PSS ist nicht Gegenstand der Bestätigung.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht derzeit für die Hashfunktion SHA-256 bis Ende des Jahres 2020 (siehe BAnz. AT 20.02.2014 B4).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus reicht für Schlüssellängen von 2048 Bit bis Ende des Jahres 2020 (siehe BAnz. AT 20.02.2014 B4). Dabei ist zu beachten, dass das Paddingverfahren RSASSA-PKCS1-V1_5 für das Signaturverfahren nur bis Ende 2016 bzw. für Zertifikatssignaturen und für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen bis Ende 2017 geeignet ist.

Die Gültigkeit der Bestätigung des BNotK TrustCenter in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-funktion / **Schlüssellänge**	**SHA-256**
2048 Bit RSASSA-PKCS1-V1_5	2016 (2017*)

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen und für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen

Diese Bestätigung der Komponente BNotK TrustCenter ist für die Erzeugung von elektronischen Signaturen maximal gültig bis 31.12.2017.

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 BNotK TrustCenter Version 1.0 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