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 und Teilsignaturanwendungskomponente für Zertifizierungsdienste BNotK TrustCenter, 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.93204.TE.12.2015

registriert.

Essen, 11.12.2015

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.93204.TE.12.2015 besteht aus 12 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

BNotK TrustCenter, Version 2.0[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.8 (File name: EJBCA-5.0.10_procilon.8.tar.gz) 4523FB18F6552F96382CD28D855EE6117DAF3BE927371AB24EC53E49952C1A289B4498E62760A8F80D61F1D0B7A15736BA519157907D83EFF1E12FE3B464670F	Sourcecode	V5.0.10_PROCILON.8
CertificateDataExtension 1.4.0 (File name: CertificateDataExtension-1.4.0.tar.gz) 5EFD079E2039A6C6B6074FFD6B1ECE990E6A5B8C8D408DA20D8ACC4DCD5DEB9106EB048612C6CA8C73BCFE3428A4B9A37AF078F0951EF32A80704FE076AAD65F	Java Archiv	1.4.0
manageCA 1.2.0 (File name: manageCA-1.2.0.tar.gz) 945B36495DBD4154645DB30AA080C8C91E8537F4336BF3CB195C9392EB99698E7339794DA61FCFFD7D8A53BDAA687527E27A6CE9BA0C9279D01139E30763D3E0	Shellscript	1.2.0
MessageTypeExtension 1.2.1 (File name: MessageTypeExtension-1.2.1.tar.gz) 7878C14C9C1E8B00F2ADAF78BE	Java Archiv	1.2.1

[3] Im Folgenden kurz mit BNotK TrustCenter bezeichnet.

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
7C3753DDE1FFBDA06A8C26C045 45AEB4E14BF65CD1260A26CA560 A30865EE3636BB9BE575A15E0A2 4D58C55AF272B8CC116147		
TimeStatusMonitor 1.2.0 (File name: TimeStatusMonitor.zip) ECDDD3089B9DDE877AFB671EA5 F75449D7AA930AC0EAF5E37B4D F5BE5BF6CDAB51398E6CD97880 8CC204C2731579B05EE0ADFBBF 477D26DB585B2F3682A27AEF	Shellscript	1.2.0
ActivationService v1.0.0 (File name: ActivationService-1.0.0.tar.gz) CD5398D51441AD478416C69AF10 E9CD19012CCF136173353AB03AB 448523E7C25EE32899EDC59F52D DE2BBCA4945DD49848C4E0F490 0552BD8049D2967DDF6E0	Web application archive	1.0.0
OCSP-Subsystem		
EJBCA v5.0.10_procilon.8 (File name: EJBCA-5.0.10_procilon.8.tar.gz) 4523FB18F6552F96382CD28D855 EE6117DAF3BE927371AB24EC53E 49952C1A289B4498E62760A8F80D 61F1D0B7A15736BA519157907D83 EFF1E12FE3B464670F	Sourcecode	V5.0.10_PROCILON.8
TimeStatusMonitor 1.2.0 (File name: TimeStatusMonitor.zip) ECDDD3089B9DDE877AFB671EA5 F75449D7AA930AC0EAF5E37B4D F5BE5BF6CDAB51398E6CD97880 8CC204C2731579B05EE0ADFBBF 477D26DB585B2F3682A27AEF	Shellscript	1.2.0
manageOCSP 1.2.0 (ManagementCLI OCSP) (File name: manageOCSP-1.2.0.tar.gz) 70C017A65542F1CF7A57F8776698	Shellscript	1.2.0

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
98DFC85EB6113CAB5C1CF322492FC9101C0C2FE39BE257708643B37930E955034326BF43D02C8ACCD5AC4B20600FFDF554C6		
ActivationService v1.0.0 (File name: ActivationService-1.0.0.tar.gz) CD5398D51441AD478416C69AF10E9CD19012CCF136173353AB03AB448523E7C25EE32899EDC59F52DDE2BBCA4945DD49848C4E0F4900552BD8049D2967DDF6E0	Web application archive	1.0.0
TSS-Subsystem		
manageTSS 1.2.0 (ManagementCLI TSS) (File name: manageTSS-1.2.0.tar.gz) 9914609CAC6D9C262DB233671A901AA0FD5BAE1FD86663016E58B89F640FB729F128B6807EFF5AE3E46699332629032F4EB1E3464C34E425A13D5A4BA4014BE0	Shellscript	1.2.0
SignServer 3.4.2_procilon.2 (File name: signserver-3.4.2_procilon.2.tar.gz) 885ABB9E50C0E0405F1CC58281A8DD1458A8CC952E5201F773F238BE32EF5FD5FDABC9803A67F39DB6F65424167CEFDC665F4933A32E3AFDC342776EE7796AE1	Sourcecode	V3.4.2_ PROCILON.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) 852CAC415938908B0A9DBF085DD	Shellscript	1.2.0

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
98782BD6279D6B435FEABFB1FEC448637974B9BC9B36BE238BF8BBA558D3611208C34BCCBC1184B9AC0BF6B63D3B35212C72B		
ActivationService v1.0.0 (File name: ActivationService-1.0.0.tar.gz) CD5398D51441AD478416C69AF10E9CD19012CCF136173353AB03AB448523E7C25EE32899EDC59F52DDE2BBCA4945DD49848C4E0F4900552BD8049D2967DDF6E0	Web application archive	1.0.0
CRL-Subsystem		
CRL v1.0.4 (File name: CRLService-1.0.4.tar.gz) 368290F5011B7C3F680BFA257F045B5CB6FAE1D793131881806576BA5814CAFE396E344D49AA1E25270663035BE4E75CA4F7478167463EC28AA03A67B1AC8539	Web application archive	1.0.4
StatusMonitor 1.2.0 (File name: StatusMonitor.zip) 852CAC415938908B0A9DBF085DD98782BD6279D6B435FEABFB1FEC448637974B9BC9B36BE238BF8BBA558D3611208C34BCCBC1184B9AC0BF6B63D3B35212C72B	Shellscript	1.2.0
manageCRL v1.0.0 (ManagementCLI CRL) (File name: manageCRL-1.0.0.tar.gz) F89A2648EB115ED9AA512AB31FF81E8AB61E60E623C86C84F1D77C7BE7A5711731287EE5A7C9C96126CE83144D230506FD8DB59ACF96EDAC4E6D49F9DC1DFD5F	Shellscript	1.0.0
ActivationService v1.0.0 (File name: ActivationService-1.0.0.tar.gz) CD5398D51441AD478416C69AF10	Web application archive	1.0.0

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
E9CD19012CCF136173353AB03AB448523E7C25EE32899EDC59F52DDE2BBCA4945DD49848C4E0F4900552BD8049D2967DDF6E0		
Benutzerdokumentation		
Preparative guidance documentation BNotK TrustCenter Installationshandbuch [AGD_PRE] (File name: Installationshandbuch_2.4.pdf) D9026C115AE76BA1B0F97B7125F7AB9FE5F75029FA45C1D32B1547833337376D233C726BFD50BEB1D3F7077E9F9BE549A25324888E060BAEBEF3D2A2CDE51CB7	Benutzerdokumentation	2.4
Preparative guidance documentation BNotK TrustCenter EJBCA Profile Content Overview (File name: EJBCA Profile Content Overview_1.3.pdf) 976FBE56DB5FEC43EB202E009A4EDFB066A4C0C6EFAA3ED558248E555661C8404988A28ED9EDC6AF0C2092D428BC04679518E9C2F5AEEBB49FA4737EA38D9685	Benutzerdokumentation	1.3
Preparative guidance documentation BNotK TrustCenter IndirectCrl Service (File name: TrustCenter IndirectCrl Service_1.3.pdf) 7E60982C1D311914D721D6666889260BD55EB59019A47778DEBE15DC84CE71618D1CC2BEC9D74C158C7EBDD2AAEC99E711F46E7E2876F78F8EDF265448F77030	Benutzerdokumentation	1.3
Preparative guidance documentation BNotK TrustCenter Worker LDAP Server	Benutzerdokumentation	1.0

Bezeichnung (File name) **SHA-512-Hashwert**	**Beschreibung**	**Version**
(File name: Worker LDAP Server_1.0.pdf) 2BF919BDC0FF4F53E7AE27F2CB3F37FFAB5190E386648E33928403E1074C61D4311F7028556800E18AA59D9C0FEBEB07CB17D97AF4BBAF4BCB1BE617C96A2B4D		
Preparative guidance documentation BNotK TrustCenter Activation Service (File name: Activation Service _1.3.pdf) 9C318C5D88F2C10426F5C520B0E2E5F1FFE27261AE1A1CBE90E548F807CA3BDB13459A6D5018ACF73BC3ADA3587F32D8BB3CE3A8A000BED3788846B7C69F75E6	Benutzerdokumentation	1.3
Operative guidance documentation BNotK TrustCenter Betriebshandbuch [AGD_OPE] (File name: Betriebshandbuch_2.6.pdf) FA356123E9E11DC303C336492E9A55818535C7D85259F3FC5EF62D1297AFE263E7315E506E427A4DB4560EF40C2D4D2E73EB574A52EFED25DA418BA214BFCA58	Benutzerdokumentation	2.6
BNotK TrustCenter TOE Specification [FSP] (File name: TOE_Specification_2.12.pdf) 8CD4E701E71FC178DB600EECC16126D1B96A69BD4A505A8E00817ACC12A137BADB95CF4B067D7B51857420C8B8FD35A01F9177270723EE455DB8802F6F0273E7	Benutzerdokumentation	2.12

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, CRL und TSS ist eine technische Komponente und Teilsignaturanwendungskomponente 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- (OCSP und CRL) und Zeitstempeldienst-Auskünften sowie zu den qualifizierten Zertifikaten erfolgt mittels der in Abschnitt 3.2 aufgeführten sicheren Signaturerstellungseinheiten (SSEE) mit den Hashfunktionen SHA-256 oder SHA-512 und den Signaturverfahren RSA-2048 sowie ECDSA-256 Bit basierend auf der Kurve brainpoolP256r1.

Eingehende Zeitstempelanfragen müssen die Hashfunktionen 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 SigV.

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-, CRL-, TSS-Subsystem Host-Rechner mit
  - Ubuntu 14.04 LTS Betriebssystem mit NTP Client, der für die Synchronisation genutzt wird,
  - WildFly 8.2.0 Anwendungsserver mit OpenJDK 1.8.0 (Linux x64),
  - Mozilla Firefox Browser V 25.0 oder nachfolgende kompatible Versionen,
  - Postfix 2.9 Mail Transfer Agent oder nachfolgende kompatible Versionen zum Senden von Meldungen.
- CA-, OCSP-, TSS-Datenbank Rechner mit
  - Oracle 11g Enterprise Edition oder Oracle 12c Standard Edition oder Oracle 12c 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), oder
  - STARCOS 3.5 ID ECC C1R (Bestätigung SRC.00021.TE.05.2013 vom 13.05.2013, 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), oder
  - cyberJack® RFID standard, Version 1.2 (Bestätigung TUVIT.93188.TU.07.2011 vom 19.07.2011, kein Ablaufdatum gemäß Bestätigung), oder
  - cyberJack® RFID komfort, Version 2.0 (Bestätigung TUVIT.93180.TU.12.2011 vom 16.12.2011, kein Ablaufdatum gemäß Bestätigung).
- Hardware Security Module (HSM)
  - NXP J3A080 and J2A080 Secure Smart Card Controller Revision 3, kurz JCOP v2.4.1 R3 (Zertifizierung BSI-DSZ-CC-0674-2011).

Die Komponente BNotK TrustCenter besteht aus vier Subsystemen. Das CA-Subsystem wird genutzt, um Zertifikate auszustellen und zu veröffentlichen, das OCSP-Subsystem stellt Informationen über den Status der Zertifikate zur Verfügung, das CRL-Subsystem erstellt Sperrlisten und das TSS- Subsystem stellt qualifizierte Zeitstempel aus. Die vier BNotK TrustCenter-Subsysteme (CA, OCSP, CRL, Zeitstempel) müssen auf vier verschiedenen Anwendungsservern installiert werden. Alle Zugriffe auf den Datenbankserver, die Hardware Security Module und die LDAP-Datenbank erfolgen über verschlüsselte Kanäle. 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 Zertifizierungs-diensteanbieter 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.
- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE als Dienstekarten) weitergereicht werden.
- Vertraulicher Umgang mit Identifikationsmerkmalen (Dienstekarten), die an die Hardware Security Module weitergereicht werden. Insbesondere dürfen diese während des Betriebs nur verschlüsselt auf den Hardware Security Modulen gespeichert werden. und für die Entschlüsselung müssen sich mindestens zwei Administratoren erfolgreich am Hardware Security Module authentifiziert haben.
- Vertraulicher Umgang mit Identifikationsmerkmale, die an die Chipkarten (Authentifizierungs-Hardware Security Module) weitergereicht werden.
- 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 die Hashfunktionen SHA-256 und SHA 512 sowie die Algorithmen RSA-2048 und ECDSA-256 basierend auf der Kurve brainpoolP256r1 (STARCOS 3.5 ID ECC C1 und STARCOS 3.5 ID ECC C1R) verwendet. Die durch die SSEE unterstützten Formatierungsverfahren (Padding) sind RSASSA-PKCS1-V1_5 und RSASSA-PSS aus PKCS#1 v2.2: RSA Cryptographic Standard, 27.10.2012.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht derzeit für die Hashalgorithmen SHA-256 und SHA-512 bis Ende des Jahres 2021 (siehe BAnz. AT 30.01.2015 B3).

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 2021 (siehe BAnz. AT 30.01.2015 B3). 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 / Signaturverfahren	SHA-256	SHA-512
2048 Bit RSASSA-PKCS1-V1_5 RSASSA-PSS	2016 (2017*) 2021	2016 (2017*) 2021
ECDSA 256 mit brainpoolP256r1	2021	-

*) 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 bei Verwendung von RSASSA-PKCS1-V1_5,
- 31.12.2021 bei Verwendung von RSASSA-PSS oder ECDSA 256 mit brainpoolP256r1.

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 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 Angriffs-potential) wird damit erreicht.

Ende der Bestätigung