BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Time-Stamp Policy und TSA Practice Statement der Zertifizierungsstelle der Bundesnotarkammer

Version: **2.8**

Datum: **29. Januar 2024**

Dokumenthistorie

Version	Anmerkung	Datum
1.0	Erstellung des Dokuments im Rahmen der Prüfung der Einhaltung der Vorgaben der Verordnung (EU) Nr. 910/2014 des europäischen Parlamentes und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (***eIDAS-Verordnung***) durch eine akkreditierte Konformitätsbewertungsstelle	20.06.2017
2.0	Anpassungen aufgrund des Aufbaus einer neuen CA-Hierarchie	28.02.2018
2.1	Redaktionelle Änderungen	31.05.2018
2.2	Redaktionelle Änderungen und Aktualisierung	07.06.2019
2.3	Erweiterung um Zertifikatsprofil für „BNotK TSA Signer 2019"	25.07.2019
2.4	Redaktionelle Änderungen und Aktualisierung	27.09.2019
2.5	Review und Aktualisierung	26.02.2021
2.6	Aktualisierung Zertifikatsprofile u.a. um ECC	12.01.2022
2.7	Jährliches Review	16.03.2023
2.8	Review und Anpassung OID-Kennzeichnung	29.01.2024

Inhalt

1 Einleitung

1.1 Über dieses Dokument

Die Bundesnotarkammer ist qualifizierter Vertrauensdiensteanbieter i. S. d. Art. 3 lit. 20 der eIDAS-Verordnung. Angebotene Dienste sind die Ausgabe von qualifizierten Zertifikaten und qualifizierten Zeitstempeln.

Dieses Dokument beschreibt die Vertrauensdiensterichtlinie der Zertifizierungsstelle der Bundesnotarkammer (auch Vertrauensdiensteanbieter Bundesnotarkammer – kurz ***VDA BNotK***) für qualifizierte elektronische Zeitstempel. Es stellt in Form einer Time-Stamp Policy sowie eines TSA Practice Statements dar, wie der VDA BNotK die Anforderungen und Vorgaben für die Erbringung der Zeitstempeldienste erfüllt.

Dieses Dokument nimmt Bezug auf die Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer mit der OID 1.3.6.1.4.1.41460.5.1.1.1.2 sowie die ETSI Normen EN 319 401, EN 319 411-2 und EN 319 421.

Die Gliederung des Dokuments basiert auf der Norm ETSI EN 319 421, um einen Vergleich mit entsprechenden Richtlinien anderer Vertrauensdiensteanbieter zu erleichtern.

Maßgeblich ist allein die deutsche Fassung dieser Richtlinie. Bei Abweichungen zwischen der deutschen und der englischen Fassung dieses Dokuments gilt daher ausschließlich die deutsche Fassung.

Diese Richtlinie ist nicht rechtsverbindlich. Für das Verhältnis zwischen VDA BNotK und dem Nutzer des Zeitstempeldienstes bzw. dem Vertrauenden Dritten sind vielmehr ausschließlich die vertraglichen oder, bei Fehlen eines Vertragsverhältnisses, die gesetzlichen Bestimmungen maßgeblich. Soweit nicht ausdrücklich anders vermerkt, beinhaltet diese Richtlinie keine Zusicherungen, Garantien oder Gewährleistungen.

1.2 Identifizierung

Dokumentenname: TSA Policy und Practice Statement der Zertifizierungsstelle der Bundesnotarkammer

Kennzeichnung (OID): 1.3.6.1.4.1.41460.5.4.1.1.2

Version: 2.8

Alle vom VDA BNotK ausgestellten Zeitstempel enthalten die OID dieser Richtlinie, welche durch Veröffentlichung auf der Website des VDA BNotK Zertifikatsinhaber und Vertrauenden Dritten zugänglich gemacht wird. Die Bereitstellung des Zeitstempeldienstes des VDA BNotK steht im Einklang mit der ETSI Best Practices-Zeitstempelrichtlinie (BTSP) gemäß ETSI EN 319 421.

2 Definitionen und Abkürzungen

Begriff	Beschreibung
TSA	Siehe Zeitstempelanbieter
Zeitstempelanbieter	Vertrauensdiensteanbieter, der (qualifizierte) elektronische Zeitstempel anbietet.

Siehe ferner Abschnitt 1.6 der Zertifikatsrichtlinie (*CP*) der Zertifizierungsstelle der Bundesnotarkammer.

3 Überblick

3.1 Zeitstempeldienste

Der VDA BNotK erstellt nur qualifizierte elektronische Zeitstempel.

Die angebotenen Zeitstempeldienste werden in dieser Richtlinie in zwei Bestandteile unterteilt:

- ***Bereitstellung von Zeitstempeln***

  Die Erstellung von Zeitstempeln.

- ***Verwaltung von Zeitstempeln***

  Die Überwachung und Kontrolle des Betriebs der Zeitstempeldienste, um sicherzustellen, dass die Dienste, wie in dieser Richtlinie vorgegeben, bereitgestellt werden. Dieser Dienst ist sowohl für die Implementierung als auch für Änderungen oder Einstellungen der Zeitstempeldienste zuständig.

Diese Unterteilung erfolgt nur für die Zwecke dieser Richtlinie und stellt keine Beschränkung der (internen) Organisation des Zeitstempeldienstes durch den VDA BNotK dar.

3.2 Zeitstempelanbieter (Time Stamping Authority – *TSA*)

Der VDA BNotK (nachfolgend auch als ***Zeitstempelanbieter*** bezeichnet) ist in seiner Eigenschaft als Zeitstempelanbieter für die Bereitstellung der in Abschnitt 3.1 genannten Dienste zuständig.

Der VDA BNotK kann Aufgaben auf Dritte übertragen. Auch bei der Übertragung von Aufgaben auf Dritte verbleibt die Gesamtverantwortung für den Betrieb des Vertrauensdienstes in der Hand des VDA BNotK. Vgl. zur Übertragung von Aufgaben auf Dritte Abschnitt 1.7 der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer.

3.3 Nutzer des Zeitstempeldienstes (Subscriber)

Der VDA BNotK stellt qualifizierte elektronische Zeitstempel nicht unmittelbar an Endnutzer zur Verfügung. In ausgewählten Einzelfällen werden qualifizierte elektronische Zeitstempel bzw. Zeitstempeldienste Dritten zur Verfügung gestellt, die diese ggf. Endnutzern zur Verfügung stellen. In diesem Fall ist der Dritte für die Information der Endnutzer verantwortlich sowie dafür, dass die Endnutzer ihren Pflichten nachkommen.

4 Richtlinien und Verfahren

4.1 Risikoanalyse

Der VDA BNotK führt eine regelmäßige Risikoanalyse durch, um die Risiken für die angebotenen Vertrauensdienste zu identifizieren, zu analysieren und zu bewerten. Einzelheiten sind im Sicherheitskonzept des VDA BNotK niedergelegt. Vgl. dazu Abschnitt 8 der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer.

4.2 Trust Service Practice Statement

4.2.1 Format des Zeitstempels

Der eingesetzte Zeitstempeldienst ist konform zu RFC 3161 unter Beachtung der ETSI EN 319 422 und unterstützt ausschließlich RSA Verschlüsselung mit 4096 bit und den SHA256, SHA384 & SHA512 Hash Algorithmen.

4.2.2 Genauigkeit der Zeit

Als verlässliche Zeitquelle werden Zeitserver mit einem DFC77-Epfänger genutzt, um die die gesetzlich gültige Zeit von der Physikalisch Technischen Bundesanstalt zu empfangen. Bei temporärem Signalverlust übernimmt ein hochgenauer Oszillator die Aufgabe des Zeitgebers für den NTP-Server. Als zusätzliche Referenzquelle sind weitere NTP-Server der Physikalisch Technischen Bundesanstalt eingebunden. Die durchschnittliche maximale Abweichung der Zeit liegt bei +/- 100 ms und ist in keinem Fall größer als eine Sekunde. Die Einhaltung der genauen Uhrzeit, sowie Änderungen und Manipulationsversuche an der Uhrzeit werden fortlaufend überwacht. Bei Überschreitung der maximal erlaubten Abweichung wird der Zeitstempeldienst automatisch deaktiviert. Schaltsekunden werden berücksichtigt, korrekt verarbeitet und protokolliert.

Vgl. Abschnitte 5.6 bis 5.7 zu den nicht-technischen und technischen Sicherheitsmaßnahmen gegen Angriffe und Manipulationsversuche der Uhrzeit.

4.2.3 Beschränkungen der Nutzung des Zeitstempeldienstes

Es gelten die gesetzlichen Bestimmungen, insbesondere etwaige Vorgaben der eIDAS-Verordnung und des Vertrauensdienstegesetzes.

4.2.4 Pflichten der Nutzer

Es gelten die gesetzlichen Bestimmungen, insbesondere etwaige Vorgaben der eIDAS-Verordnung und des Vertrauensdienstegesetzes.

Bitte beachten Sie, dass der VDA BNotK grundsätzlich keine Zeitstempeldienste unmittelbar an Endanwender zur Verfügung stellt.

4.2.5 Verifikation des Zeitstempels

Die Überprüfung des Zeitstempels erfordert die folgenden Schritte:

- ***1. Verifikation des Ausstellers des Zeitstempels***
  Zur Prüfung des Ausstellers wird der öffentliche Schlüssel der signierenden CA benötigt. Dieser kann auf der TSL und der Webseite heruntergeladen werden.

- ***2. Verifikation des Status des Zeitstempels***
  Die Prüfung des Zertifikatsstatus der signierenden CA erfolgt über einen OCSP-Responder. Die Adresse des OCSP-Responders ist Teil des Zertifikats.

- ***3. Verifikation der Integrität des Zeitstempels***
  Die Integrität des Zeitstempels lässt sich mit jeder RFC 3161 konformen Software prüfen.

4.2.6 Anwendbares Recht

Der VDA BNotK erfüllt die Voraussetzungen für die Erbringung eines Zeitstempeldienstes nach deutschem Recht.

4.2.7 Verfügbarkeit des Zeitstempeldienstes

Der Zeitstempeldienst wird auf hochverfügbaren IT-Systemen in einem hochverfügbaren Rechenzentrum betrieben, um eine jederzeitige Verfügbarkeit des Zeitstempeldiensts zu erreichen. Es gilt die mit dem VDA BNotK geschlossene einzelvertragliche Vereinbarung zur garantierten Verfügbarkeit.

4.3 Allgemeine Geschäftsbedingungen

Es gilt die mit dem VDA BNotK geschlossene einzelvertragliche Vereinbarung.

4.4 Informationssicherheitsrichtlinie

Siehe dazu Abschnitt 5.1 der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer.

4.5 Pflichten des Zeitstempelanbieters

Es gilt die mit dem VDA BNotK geschlossene einzelvertragliche Vereinbarung oder, bei Fehlen einer vertraglichen Vereinbarung, die gesetzlichen Bestimmungen.

Diese Richtlinie begründet keine zusätzlichen Pflichten des VDA BNotK, insbesondere enthält dieses Dokument keine Zusicherungen, Garantien oder Gewährleistungen.

4.6 Informationen für Vertrauende Dritte

Dieses Dokument sowie die Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer werden Dritten durch Veröffentlichung auf der Website des VDA BNotK zugänglich gemacht.

Vertrauende Dritte dürfen nur dann auf einen Zeitstempel des VDA BNotK vertrauen, wenn zumindest folgende Voraussetzungen vorliegen:

- der Zeitstempel wurde ordnungsgemäß signiert und der zur Signierung des Zeitstempels verwendete private Schlüssel wurde bis zum Zeitpunkt der Verifikation des Zeitstempels nicht kompromittiert,
- eventuelle Einschränkungen der Nutzung wurden beachtet,
- alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten,
- der Vertrauende Dritte hat die maßgebliche Vertrauensliste genutzt, um festzustellen, dass der Zeitstempel und die Zeitstempeleinheit (***TSU***) qualifiziert sind.

5 Verwaltung und Nutzung des Zeitstempeldienstes

5.1 Interne Organisation

Der VDA BNotK ist eine Körperschaft des öffentlichen Rechts nach deutschem Recht.

Der VDA BNotK verfügt über ein vertrauliches Sicherheitskonzept, in dem die betrieblichen Anforderungen unter anderem betreffend das Personal, die Zugriffskontrolle und die Risikobewertung niedergelegt sind.

Der VDA BNotK verfügt über zuverlässiges und qualifiziertes Personal in ausreichender Anzahl. Das eingesetzte Personal besitzt die für ihre Aufgaben notwendige Fachkunde, Erfahrungen und Qualifikationen und wird vor Übernahme einer Aufgabe und während der Tätigkeit geschult.

5.2 Personalkonzept

Im Personal- und Rollenkonzept des VDA BNotK sind zum einen die personellen Maßnahmen für den Betrieb von Zertifizierungsdiensten und zum anderen die Rollenverteilung innerhalb des VDA BNotK festgelegt. Es werden alle für den Zertifizierungsbetrieb erforderlichen Rollen identifiziert und festgelegt und ihre Aufgaben beschrieben.

Einzelheiten sind in Abschnitt 5.3 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.3 Asset Management

Der VDA BNotK hat ein den gesetzlichen Anforderungen entsprechendes Asset Management eingeführt.

Einzelheiten sind in Abschnitt 5.2 der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.4 Zugriffskontrolle

Siehe dazu Abschnitte 5.1, 5.4 und 6.5 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer.

5.5 Kryptographische Kontrolle

Alle für qualifizierten Zeitstempel genutzten Schlüssel und die darauf basierenden Zertifikate sind auf zertifizierten QSCDs gespeichert. Die QSCDs werden in einem sicheren Umfeld gemäß der Einsatzumgebung der Zertifizierung der QSCDs betrieben.

5.5.1 Schlüsselgenerierung

Schlüssel für Zeitstempel werden in einer sicheren Umgebung nach Vorgaben des Herstellers und unter Einhaltung der zertifizierten Bedingungen auf einem zugelassenen QSCD, welches gemäß den Common-Criteria-Vorgaben evaluiert wurde und auf der EU-Liste der vertrauenswürdigen zertifizierten Komponenten steht, generiert. Der Prozess und die Aktivierung des Schlüssels wird von Personen mit den entsprechenden Rollen laut Rollenkonzept (Vergleiche Abschnitt 5.2) im Vier-Augen-Prinzip in einer sicheren Umgebung durchgeführt. Die öffentlichen Zertifikate, die auf den Schlüsseln basieren, werden auf der Webseite des VDA BNotK unter der folgenden Adresse veröffentlicht: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen. Darüber hinaus sind sie auch auf den Seiten der Bundesnetzagentur und auf der deutschen Trusted List veröffentlicht. Der Prozess zur Schlüsselgenerierung wird rechtzeitig vor Ablauf der Gültigkeit der Schlüssel wiederholt, um einen reibungslosen Übergang zu gewährleisten. Um sicherzustellen, dass dies rechtzeitig erfolgt, wird die Gültigkeit der Schlüssel durch ein Monitoring-System überwacht.

Als Zeitstempeleinheit wird eine Gruppe von Hardware und Software bezeichnet, die als Einheit verwaltet wird und zu der jeweils ein einzelner privater Signaturschlüssel aktiv ist.

5.5.2 Schutz des privaten Schlüssels

Der private Schlüssel für Zeitstempel ist nur auf den installierten QSCDs nutzbar. Die QSCDs werden in einer sicheren, zutrittsgeschützten Umgebung betrieben. Nur berechtigte Personen laut Rollenkonzept haben Zugriff auf die QSCDs. Der Zugriff kann nur im Vier-Augen-Prinzip erfolgen.

5.5.3 Öffentlicher Schlüssel

Die öffentlichen Zertifikate, die auf den öffentlichen Schlüsseln basieren, werden auf der Webseite des VDA BNotK unter der folgenden Adresse veröffentlicht: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen. Zeitstempel werden erst dann ausgestellt, wenn das entsprechende öffentliche Zertifikat in die TSU oder deren kryptografisches Gerät geladen wurde.

5.5.4 Schlüssellängen

Für die Schlüssellänge gilt die Empfehlung der SOG-IS Crypto Working Group. Die momentan verwendeten Schlüssel haben eine Länge von 4096 Bit.

5.5.5 Schlüsselparameter und Qualitätskontrolle der Parameter

Die Schlüsselparameter richten sich nach den Empfehlungen der SOG-IS Crypto Working Group bzw. den Bestätigungsdokumenten der QSCD. Die Einhaltung der Vorgaben wird kontinuierlich von einer dafür verantwortlichen Person geprüft.

5.5.6 Schlüsselverwendung

Die Schlüssel werden ausschließlich zum Signieren von Zeitstempeln verwendet. Der Verwendungszweck ist im X.509 Zertifikat des Schlüssels hinterlegt.

5.5.7 Gültigkeitsdauer von Schlüssel und Zertifikaten

Die Gültigkeitsdauer der Schlüsselpaare und darauf basierenden Zertifikate beträgt maximal zehn Jahre. Beim Auslaufen der Eignung eines eingesetzten Algorithmus oder der eingesetzten QSCD werden die Schlüssel vor Ablauf der Zertifikatsgültigkeit gesperrt.

Nach Ablauf der Gültigkeit des privaten Schlüssels ist ein Ausstellen von Zeitstempeln nicht mehr möglich.

5.6 Nicht-technische Sicherheitsmaßnahmen

Der VDA BNotK hat den gesetzlichen Anforderungen entsprechende nicht-technische Sicherheitsmaßnahmen eingeführt.

Einzelheiten sind in Abschnitt 5 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.7 Technische Sicherheitsmaßnahmen

Der VDA BNotK hat den gesetzlichen Anforderungen entsprechende technische Sicherheitsmaßnahmen eingeführt.

Einzelheiten sind in Abschnitt 6 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.8 Netzwerksicherheit

Der VDA BNotK hat den gesetzlichen Anforderungen entsprechende Maßnahmen zur Netzwerksicherheit eingeführt.

Einzelheiten sind in Abschnitt 6.7 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.9 Notfallkonzept

Der VDA BNotK verfügt über ein Notfallkonzept.

Einzelheiten sind in Abschnitt 5.7 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.10 Archivierung von Unterlagen

Der VDA BNotK archiviert Unterlagen gemäß den gesetzlichen Anforderungen. Einzelheiten sind in Abschnitt 5.5 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben

Speziell für den Zeitstempeldienst gilt:

- TSU Schlüsselverwaltung

Alle Ereignisse betreffend (i) den Lebenszyklus (life-cycle) des TSU-Schlüssels sowie (ii) des TSU-Zertifikats (falls erforderlich) werden protokolliert.

- Synchronisation der Uhrzeit

Alle Ereignisse betreffend (i) die Synchronisation der Uhr des TSU und der UTC sowie (ii) die Erkennung von Synchronisierungsverlusten werden protokolliert.

5.11 Business Continuity Management

Der VDA BNotK verfügt über ein Notfallkonzept. Im Fall einer Kompromittierung des Zeitstempeldienstes oder bei ausgestellten Zeitstempeln mit falscher Uhrzeit werden die betroffenen Kunden informiert und der Zeitstempeldienst bis zur Behebung der Ursache deaktiviert. Darüber hinaus werden Informationen zur Identifizierung der falsch ausgestellten Zeitstempel auf der Webseite des VDA BNotK zur Verfügung gestellt.

Weitere Einzelheiten sind in Abschnitt 5.7 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.12 Beendigungsplan

Der VDA BNotK hat einen den gesetzlichen Anforderungen entsprechenden Beendigungsplan.

Einzelheiten sind in Abschnitt 5.8 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.13 Konformität

Der VDA BNotK betreibt den Zeitstempeldienst im Einklang mit dem geltenden Recht.

Eine akkreditierte Konformitätsbewertungsstelle überprüft in regelmäßigen Abständen, dass der VDA BNotK die gesetzlichen Anforderungen erfüllt.

Einzelheiten sind in der Zertifikatsrichtlinie beschrieben.

5.14 Zertifikatsprofil

5.14.1 Sub-CA

- Zertifikatsprofil RSA

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	z.B. [58 ac b6 41 e3 98 90 00]
Signaturalgorithmus	Kennzeichner (OID) Signaturalgorithmus	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signaturhashalgorithmus	Kennzeichner (OID) Signaturhashalgorithmus	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Kennzeichner (OID) Schlüsselalgorithmus	RSA (1.2.840.113549.1.1.1)
Schlüssellänge	Schlüssellänge	4096 Bits
Aussteller		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName (2.5.4.3)	Name Inhaber	z.B. CN = BNotK TSA CA 2017
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	z.B. 2019-06-27 12:20:24 UTC
	Ende	z.B. 2029-03-26 12:20:24 UTC
Inhaber		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238

organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName (2.5.4.3)	Name Inhaber	z.B. CN = BNotK TSA Signer 2019
Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	digitalSignature
extKeyUsage (2.5.29.37)	Erweiterter Verwendungszweck	timeStamping
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Nutzung des Zertifikats	Typ Antragsteller=End Entity Einschränkung Pfadlänge=None
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssel des Inhabers	[DB 5E EA 40 0B D2 8C F8 76 30 53 B6 52 0F 14 66 85 90 D3 6F]
ValidityModel (1.3.6.1.4.1.8301.3.5)	Zertifikatsextension für Gültigkeitsmodell bei der Zertifikatsprüfung	ValidityModelChain (1.3.6.1.4.1.8301.3.5.1)
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssel des Ausstellers	[C4 A0 FE 6F E8 D7 E0 84 80 E7 30 35 D7 A6 27 5E EC 5F 1A 02]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Verweis auf Aussteller und Dienst zur Statusabfrage	s. folgende Elemente
calssuers (1.3.6.1.5.5.7.48.2)	URL zur Aussteller-Info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	http://ocsp.zs.bnotk.de/eqsig
CertificatePolicies (2.5.29.32)	Zertifikatsrichtlinie TSA der ZS der BNotK	CPS: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)	Erklärung eIDAS-Konformität	s. folgende Elemente
QcCompliance (0.4.0.1862.1.1)	Qualifiziertes Zertifikat	0.4.0.1862.1.1
QcSSCD (0.4.0.1862.1.4)	Erzeugung auf SSCD	0.4.0.1862.1.4
QcType	Typ (Elektr. Siegel)	0.4.0.1862.1.6.2

(0.4.0.1862.1.6)		
QcPDS (0.4.0.1862.1.5)	URL-Verweis auf PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

- Zertifikatsprofil ECC

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	z.B. [58 ac b6 41 e3 98 90 00]
Signaturalgorithmus (1.2.840.10045.4.3.4)	Kennzeichner (OID) Signaturalgorithmus	SHA512WITHECDSA
Schlüssellänge	Schlüssellänge	521 Bits
Aussteller		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName (2.5.4.3)	Name Inhaber	z.B. CN = BNotK TSA CA 2017
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	z.B. 2019-06-27 12:20:24 UTC
	Ende	z.B. 2029-03-26 12:20:24 UTC
Inhaber		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName	Name Inhaber	z.B. CN = BNotK TSA Signer

(2.5.4.3)		2019
Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	digitalSignature
extKeyUsage (2.5.29.37)	Erweiterter Verwendungszweck	timeStamping
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Nutzung des Zertifikats	Typ Antragsteller=End Entity Einschränkung Pfadlänge=None
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssel des Inhabers	[DB 5E EA 40 0B D2 8C F8 76 30 53 B6 52 0F 14 66 85 90 D3 6F]
ValidityModel (1.3.6.1.4.1.8301.3.5)	Zertifikatsextension für Gültigkeitsmodell bei der Zertifikatsprüfung	ValidityModelChain (1.3.6.1.4.1.8301.3.5.1)
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssel des Ausstellers	[C4 A0 FE 6F E8 D7 E0 84 80 E7 30 35 D7 A6 27 5E EC 5F 1A 02]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Verweis auf Aussteller und Dienst zur Statusabfrage	s. folgende Elemente
calssuers (1.3.6.1.5.5.7.48.2)	URL zur Aussteller-Info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	http://ocsp.zs.bnotk.de/eqsig
CertificatePolicies (2.5.29.32)	Zertifikatsrichtlinie TSA der ZS der BNotK	CPS: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)	Erklärung eIDAS-Konformität	s. folgende Elemente
QcCompliance (0.4.0.1862.1.1)	Qualifiziertes Zertifikat	0.4.0.1862.1.1
QcSSCD (0.4.0.1862.1.4)	Erzeugung auf SSCD	0.4.0.1862.1.4
QcType (0.4.0.1862.1.6)	Typ (Elektr. Siegel)	0.4.0.1862.1.6.2
QcPDS (0.4.0.1862.1.5)	URL-Verweis auf PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen

Vom VDA BNotK ausgestellte Zeitstempel entsprechen RFC 3161

***

https://zertifizierungsstelle.bnotk.de/