

Zertifizierungskonzept des VDA BNotK für qualifizierte Zertifikate und den Server Signing Application Service (SSAS)



Version: 3.6
Datum: 09.04.2026

Dokumentenhistorie

Version	Anmerkung	Datum
1.0	Erstellung des Dokuments im Rahmen der Prüfung der Einhaltung der Vorgaben der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments 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	Aktualisierung aufgrund der Umstellung der PKI- Infrastruktur der Zertifizierungsstelle der Bundesnotarkammer auf eine native eIDAS-PKI sowie redaktionelle Änderungen in Folge des Inkrafttretens des Vertrauensdienstegesetzes	18.10.2017
2.1	Aktualisierung aufgrund neuer Zertifikathierarchie	28.02.2018
2.2	Redaktionelle Anpassungen und Aktualisierung aufgrund der Weiterentwicklung der Anwendungslandschaft (Antrags-, Prüf- und Produktionssystem) der Zertifizierungsstelle.	15.08.2018
2.3	Redaktionelle Änderungen sowie Anpassungen im Hinblick auf die Verfügung der BNetzA gemäß § 11 VDG zu anerkannten „sonstigen Identifizierungsmethoden“	07.06.2019
2.4	Aktualisierung CA-Hierarchie	15.06.2020
2.5	Redaktionelle Änderungen sowie Erweiterung um Inhalte zur Einführung der Fernsignatur gemäß EN 319 411-2.	09.12.2020
2.6	Review und Ergänzung Zertifikatsprofil um ECC.	31.05.2021
2.7	Aktualisierung Zertifikatsprofil Endanwenderzertifikate	07.12.2021
2.8	Aktualisierung CA-Hierarchie	31.03.2022
2.9	Aktualisierung eIDent um eIDAS-Token	30.05.2022
3.0	Detaillierung Attribut „countryName“ in Zertifikatsprofilen	07.07.2022

3.1	Einführung Dienstzertifikate und OCSP-Erweiterungen	28.03.2023
3.2	Aktualisierung Zertifikathierarchie aufgrund Erstellung von neuem TSA Signer	06.06.2023
3.3	Review, Anpassung OID-Kennzeichnung und Ergänzung Sperrung via qeS.	29.01.2024
3.4	Einführung des neuen qualifizierten Siegeldienstes (QCP-I-qscd)	25.07.2024
3.5	Aktualisierung PKI-Hierarchie (1.1.2), Computersicherheit (6.5), Sicherheitsmaßnahmen (6.6.2) und Netzwerksicherheit (6.7) sowie redaktionelle Überarbeitung	07.04.2025
3.6	Änderung des Dokumententitels, Adressaktualisierung VDA BNotK, Aktualisierung der PKI-Hierarchie, Anpassungen aufgrund neuer Anforderungen aus ETSI 319 401, ETSI 319 411-1/2 und ETSI TS 119 431, Aktualisierungen in den Kapiteln: 1.1, 1.5, 1.6, 2.1, 3.1.7,3.1.8, 3.2, 3.2.1, 3.2.1.1, 3.3, 4.2.1, 4.3.1, 4.5.1, 4.9.5, 4.9.9, 4.10, 5.8.2 Neues Kapitel 5.1 Risikomanagement, Behandlung von Verfügbarkeitsstörungen in 5.8.2, Einführung einer weiteren Authentifizierungsmethode für qeS in Kapitel 6.4, Erweiterung um den Vertrauensdienst „Server Signing Application Service (SSAS)“ in Kapitel 6.9, Erweiterung um Anhang A: Ergänzende Regelungen zur Identitätsprüfung gemäß ETSI TS 119 461, in 6.9.11 Referenz auf die Zertifizierung des eingesetzten QSCD & SAM gemäß Annex II ETSI TS 119 431.	09.04.2026

Inhaltsverzeichnis

1	Einleitung	10
1.1	Überblick	10
1.1.1	Über dieses Dokument	10
1.1.2	Eigenschaften der PKI des VDA BNotK	11
1.2	Name und Kennzeichnung des Dokuments	13
1.3	PKI-Teilnehmer	13
1.4	Verwendung von Zertifikaten	13
1.4.1	Verwendung von Dienstzertifikaten	13
1.5	Verwaltung des Zertifizierungskonzepts	14
1.6	Definitionen und Abkürzungen	15
2	Verantwortlichkeit für Verzeichnisse und Veröffentlichungen	16
2.1	Verzeichnisse	16
2.2	Veröffentlichung von Informationen zu Zertifikaten	16
2.3	Zeitpunkt und Häufigkeit von Veröffentlichungen	16
2.4	Zugang zu den Informationen	16
3	Identifizierung und Authentifizierung	17
3.1	Namensregeln	17
3.1.1	Arten von Namen	17
3.1.2	Aussagekraft von Namen	17
3.1.3	Pseudonyme	17
3.1.4	Regeln für die Interpretation verschiedener Namensformen	17
3.1.5	Eindeutigkeit von Namen	17
3.1.6	Anerkennung, Authentifizierung und die Rolle von Markennamen	18
3.1.7	Testzertifikate	19
3.2	Identifizierung der Zertifikatsinhaber	19
3.2.1	Identifizierungsverfahren der Antragsteller	21
3.2.1.1	Prüfung von Identitätsmerkmalen	23
3.2.1.2	Verfahren Notarident	24
3.2.1.3	Verfahren Gerichtident	25
3.2.1.4	Verfahren Rechtsanwaltskammerident	27
3.2.1.5	Verfahren eIDent	27
3.2.1.6	Verfahren RA-Ident	27
3.2.1.7	Nutzung vertrauenswürdiger Register	29

3.2.1.8	Umgang mit Abweichungen von Identitätsdaten.....	30
3.2.1.9	Archivierung von Nachweisen.....	30
3.2.2	Identifizierung bei Erweiterungen und Beschränkungen im Zertifikat	31
3.2.2.1	Aufnahme amts- und berufsbezogener oder sonstiger Angaben	31
3.2.2.2	Aufnahme und Prüfung einer Vertretungsmacht.....	31
3.2.2.3	Aufnahme eines Pseudonyms.....	32
3.2.2.4	Einschränkung der Nutzung	32
3.3	Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung (re-keying)	33
3.4	Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens.....	34
4	Betriebsanforderungen.....	34
4.1	Zertifikatsantrag	34
4.2	Verarbeitung des Zertifikatsantrags	35
4.2.1	Durchführung der Identifizierung und Authentifizierung	35
4.2.2	Annahme oder Ablehnung des Antrags.....	36
4.3	Ausstellung von Zertifikaten	36
4.3.1	Vorgehen der CA bei der Ausstellung des Zertifikats	36
4.3.2	Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats	37
4.4	Zertifikatsübergabe	37
4.4.1	Verhalten bei der Zertifikatsübergabe	37
4.4.2	Veröffentlichung des Zertifikats durch den VDA BNotK.....	38
4.4.3	Benachrichtigung Dritter über die Erstellung des Zertifikats	38
4.5	Verwendung des Schlüsselpaars und des Zertifikats	39
4.5.1	Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber oder Zeichnungsberechtigten	39
4.5.2	Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber.....	40
4.6	Zertifikatserneuerung (certificate renewal)	41
4.7	Zertifikatserneuerung mit Schlüsselerneuerung	41
4.8	Zertifikatsänderung	41
4.9	Widerruf und Suspendierung von Zertifikaten	41
4.9.1	Bedingungen für einen Widerruf	41
4.9.2	Widerrufsberechtigte	42
4.9.3	Verfahren zur Stellung eines Widerrufsverlangens	42
4.9.4	Fristen für ein Widerrufsverlangen	44
4.9.5	Zeitspanne für die Bearbeitung von Widerrufsverlangen	44
4.9.6	Methoden zum Prüfen von Widerrufsinformationen.....	45
4.9.7	Häufigkeit der Veröffentlichung von Widerrufslisten	45

4.9.8	Maximale Latenzzeit für Widerrufslisten	45
4.9.9	Online-Verfügbarkeit von Widerrufsinformationen	45
4.9.10	Notwendigkeit zur Online-Prüfung von Widerrufsinformationen	45
4.9.11	Andere Formen zur Anzeige von Widerrufsinformationen.....	45
4.9.12	Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels	46
4.9.13	Suspendierung des Zertifikats	46
4.10	Statusabfragedienst	46
4.11	Beendigung des Zertifizierungsdienstes.....	46
4.12	Schlüsselhinterlegung und –wiederherstellung	46
5	Nicht-technische Sicherheitsmaßnahmen.....	47
5.1	Risikomanagement.....	47
5.2	Bauliche Sicherheitsmaßnahmen Risikomanagement	47
5.3	Verfahrensvorschriften.....	48
5.3.1	Rollenkonzept.....	48
5.3.2	Vier-Augen-Prinzip	48
5.3.3	Sonstige Dienstanweisung	48
5.4	Personalkonzept.....	48
5.4.1	Qualifikation, Erfahrung und Zuverlässigkeit des Personals.....	48
5.4.2	Sicherheitsüberprüfung.....	49
5.4.3	Schulungen und Weiterbildungen.....	49
5.4.4	Rollenbesetzung, Rollenentzug und Rollenwechsel	49
5.4.5	Anforderungen an externes Personal.....	50
5.4.6	Sanktionen bei unerlaubten Handlungen.....	50
5.4.7	Dokumentation	50
5.5	Protokollierung von Überwachungsmaßnahmen.....	50
5.5.1	Überwachung des Zutritts.....	50
5.5.2	Überwachung von organisatorischen Maßnahmen	50
5.6	Archivierung von Unterlagen	51
5.6.1	Arten von Unterlagen	51
5.6.2	Aufbewahrungszeiten	51
5.6.3	Archivsicherheit.....	51
5.6.4	Datensicherung des Archivs	52
5.6.5	Anforderungen an die Zeitstempel der archivierten Protokolle	52
5.6.6	Ort der Archivierung	52
5.7	Umstellung des Schlüssels (key changeover).....	52
5.8	Notfallkonzept.....	52

5.8.1	Behandlung von Vorfällen.....	52
5.8.2	Behandlung von Verfügbarkeitsstörungen.....	52
5.8.3	Wiederherstellung von IT-Systemen	52
5.8.4	Wiederherstellung nach Kompromittierung von privaten CA-Schlüsseln	53
5.8.5	Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall	53
5.9	Beendigung des Zertifizierungsbetriebs.....	53
6	Technische Sicherheitsmaßnahmen.....	55
6.1	Erzeugung und Installation von Schlüsselpaaren.....	55
6.1.1	Erzeugung von Schlüsselpaaren	55
6.1.2	Auslieferung der privaten Schlüssel für Zertifikatsteilnehmer.....	55
6.1.3	Auslieferung der öffentlichen Schlüssel an die CA	55
6.1.4	Auslieferung der öffentlichen CA-Schlüssel.....	55
6.1.5	Schlüssellängen	56
6.1.6	Schlüsselparameter und Qualitätskontrolle der Parameter	56
6.1.7	Schlüsselverwendung	56
6.2	Sicherung des privaten Schlüssels und kryptographisches Modul.....	56
6.2.1	Standards und Sicherheitsmaßnahmen	56
6.2.2	Mehraugenprinzip bei der Schlüsselaktivierung.....	57
6.2.3	Schlüsselwiederherstellung	57
6.2.4	Schlüsselbackup	57
6.2.5	Schlüsselarchivierung	57
6.2.6	Schlüsseltransfer	57
6.2.7	Schlüsselspeicherung.....	57
6.2.8	Aktivierung privater Schlüssel.....	57
6.2.9	Deaktivierung privater Schlüssel	58
6.2.10	Zerstörung privater Schlüssel.....	58
6.2.11	Beschreibung der kryptografischen Module	58
6.3	Weitere Aspekte der Verwaltung des Schlüsselpaars.....	58
6.3.1	Archivierung der öffentlichen Schlüssel	58
6.3.2	Gültigkeitsdauer von Schlüssel und Zertifikaten.....	58
6.4	Signatur- und Siegelerstellungsdaten sowie Aktivierungsdaten	59
6.4.2	Schutz von Signatur- und Siegelerstellungsdaten	60
6.4.3	Weitere Aspekte der Aktivierungsdaten	60
6.5	Computersicherheit.....	60
6.6	Technische Kontrolle während des Lebenszyklus.....	61
6.6.1	Sicherheitsmaßnahmen beim Aufbau, der Entwicklung und Erweiterung der IT- Systeme und	

Softwarekomponenten.....	61
6.6.2 Sicherheitsmaßnahmen beim Betrieb	62
6.6.3 Lieferketten- und Assetmanagement	63
6.7 Netzwerksicherheit	63
6.8 Zeitstempel	64
6.9 Server Signing Application Service (SSAS) – Verwaltung von Fernsignatur- und Fernsiegelerstellungsgeräten –.....	65
6.9.1 Anwendungsbereich und Abgrenzung.....	65
6.9.2 Rollen und Verantwortlichkeiten.....	65
6.9.3 SSAS Policy – normative Festlegungen	66
6.9.4 SSAS Practice Statement – operative Umsetzung	66
6.9.5 Erzeugung und Verwaltung von Signaturschlüsseln.....	66
6.9.6 Identitätsbindung und Authentisierung	66
6.9.7 Auslösen eines Signatur- oder Siegelvorgangs	67
6.9.8 Löschung und Sperrung von Signaturschlüsseln	68
6.9.9 Protokollierung, Überwachung und Nachvollziehbarkeit.....	68
6.9.10 Audit, Konformität und Aufsicht.....	68
6.9.11 Qualifizierte Fernsignaturerstellungseinheit (Remote QSCD)	68
6.9.12 Verfügbarkeit des Server Signing Application Service (SSAS).....	69
7 Profile von Zertifikaten, Widerrufslisten und OCSP.....	70
7.1 Zertifikatsprofile	70
7.1.1 Root-CA	70
7.1.2 Sub-CA	73
7.1.3 Endanwenderzertifikatsprofil.....	77
7.2 Widerrufslistenprofile	85
7.3 Profile des Statusabfragedienstes	85
7.3.1 Versionsnummer.....	86
7.3.2 OCSP-Erweiterungen	86
8 Konformitätsprüfung	86
9 Sonstige geschäftliche und rechtliche Regelungen	86
Anhang I - Ergänzende Regelungen zur Identitätsprüfung gemäß ETSI TS 119 461-1	87
I. Identitätsprüfungsdienst (IPSP).....	87
a. Identitätsprüfungskontexte - Attribute und Mittel zur Erfassung und Prüfung.....	87
b. Zuordnung der Anwendungsfälle (Use Cases) entsprechend TS 119 641	87
c. Identitätsprüfungskontexte und Attribute	88

d.	Mittel, die zur Validierung von Identitätsattributen verwendet werden.....	91
e.	Validierung der Mittel und Attribute.....	92
II.	Geltungsbereich und Konformität.....	92
III.	Anwendungsfälle und Identifizierungsverfahren	93
a.	Identifizierung bei physischer Anwesenheit.....	93
b.	Identifizierung durch bestätigende Stellen	93
c.	Elektronische Identifizierung (eID)	93
IV.	Risikoanalyse und Bedrohungsmanagement	93
V.	Qualifikation und Schulung des Personals.....	94
VI.	Qualitäts- und Sicherheitsziele	94
VII.	Nachweise und Dokumentation der Identitätsprüfung	94
VIII.	Datenschutz und Vertraulichkeit	94
	Personenbezogene Daten aus der Identitätsprüfung werden ausschließlich zum Zweck der Zertifikatsbeantragung und -verwaltung verarbeitet. Der Zugriff auf diese Daten ist auf befugte Personen beschränkt. Es gelten die Datenschutzregelungen, dieses CPS sowie die einschlägigen gesetzlichen Vorschriften.	94
IX.	Überprüfung und Weiterentwicklung	95
	Die Regelungen dieses Anhangs werden regelmäßig überprüft und bei Bedarf aktualisiert, insbesondere bei Änderungen der ETSI-Normen, der eingesetzten Identifizierungsverfahren oder der rechtlichen Rahmenbedingungen.....	95
***	95	

1 Einleitung

1.1 Überblick

1.1.1 Über dieses Dokument

Dieses Dokument ist das Zertifizierungskonzept des Vertrauensdiensteanbieters Bundesnotarkammer (kurz VDA BNotK) für qualifizierte Zertifikate für elektronische Signaturen und elektronische Siegel in Form eines Certificate Practice Statement (**CPS**).

Darüber hinaus beschreibt dieses Zertifizierungskonzept die Anforderungen und Vorgaben für den qualifizierten Vertrauensdienst „Server Signing Application Service (SSAS) – Verwaltung von Fernsignatur- und Fernsiegelerstellungsgeräten“.

Die Ausstellung qualifizierter Zertifikate und der Betrieb des Server Signing Application Service (SSAS) erfolgen als getrennte qualifizierte Vertrauensdienste, die jeweils eigenen rechtlichen und normativen Anforderungen unterliegen.

Dieses Zertifizierungskonzept legt die Anforderungen und Vorgaben des VDA BNotK für die Ausgabe, Verwaltung, den Widerruf sowie die Erneuerung der ausgegebenen qualifizierten Zertifikate fest. Die Regelungen zum Server Signing Application Service (SSAS) sind in Kapitel 6.9 dieses Zertifizierungskonzepts enthalten und bilden vollständig die SSAS Policy sowie das SSAS Practice Statement gemäß ETSI TS 119 431-1 ab.

Nicht-qualifizierte Zertifikate sind nicht Gegenstand dieses Zertifizierungskonzepts.

Das Zertifizierungskonzept nimmt Bezug auf die Zertifikatsrichtlinie des VDA BNotK (**CP**) mit der OID 1.3.6.1.4.1.41460.5.1.1.1.2 sowie auf die ETSI Normen EN 319 401, EN 319 411-1, EN 319 411-2, ETSI TS 119 431-1 sowie auf die ETSI TS 119 461 und beschreibt die Umsetzung der daraus resultierenden Anforderungen.

Die Gliederung des Zertifizierungskonzepts basiert auf dem Standard RFC 3647, um einen Vergleich mit den Zertifizierungskonzepten anderer Vertrauensdiensteanbieter zu ermöglichen.

Maßgeblich ist allein die deutsche Fassung dieses Zertifizierungskonzepts.

Bei Abweichungen zwischen der deutschen und der englischen Fassung dieses Dokuments gilt daher ausschließlich die deutsche Fassung.

Das Zertifizierungskonzept ist nicht rechtsverbindlich. Für das Verhältnis zwischen VDA BNotK und dem Zertifikatsinhaber bzw. vertrauenden Dritten sind ausschließlich die vertraglichen oder, bei Fehlen eines Vertragsverhältnisses, die gesetzlichen Bestimmungen maßgeblich.

Soweit nicht ausdrücklich anders vermerkt, beinhaltet dieses Zertifizierungskonzept keine Zusicherungen, Garantien oder Gewährleistungen.

1.1.2 Eigenschaften der PKI des VDA BNotK

PKI für qualifizierte Vertrauensdienste

Die qualifizierte PKI besteht aus einer Root-CA und daraus abgeleiteten Sub-/Issuing-CAs. Endanwenderzertifikate werden jeweils von den Sub-/Issuing-CAs signiert.

Abbildung I

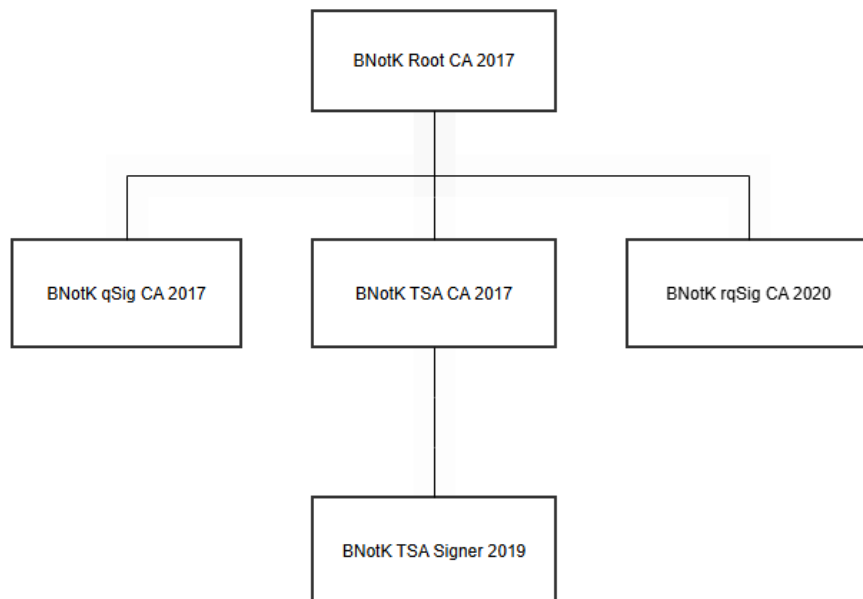
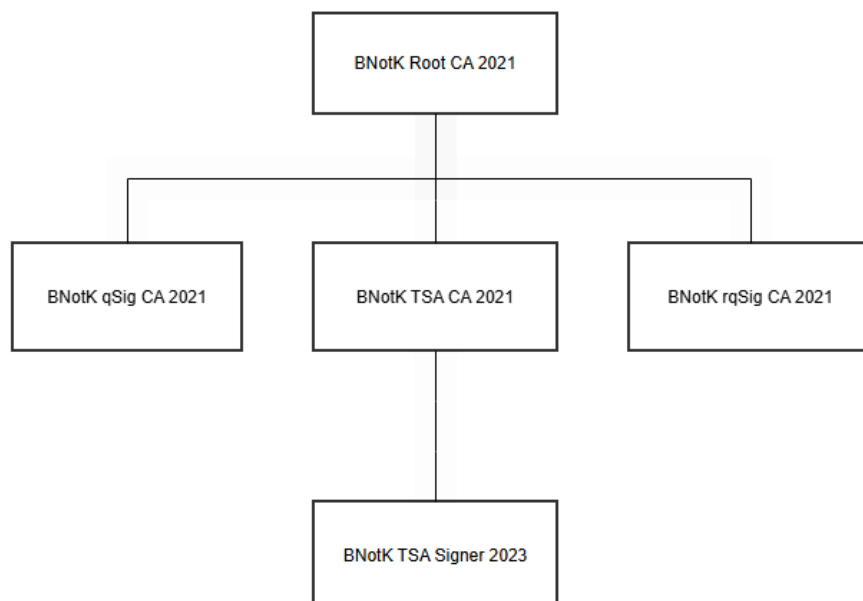


Abbildung II



Die Abbildungen I & II zeigen die aktive PKI Hierarchie des VDA BNotK mit RSA.

Abbildung III

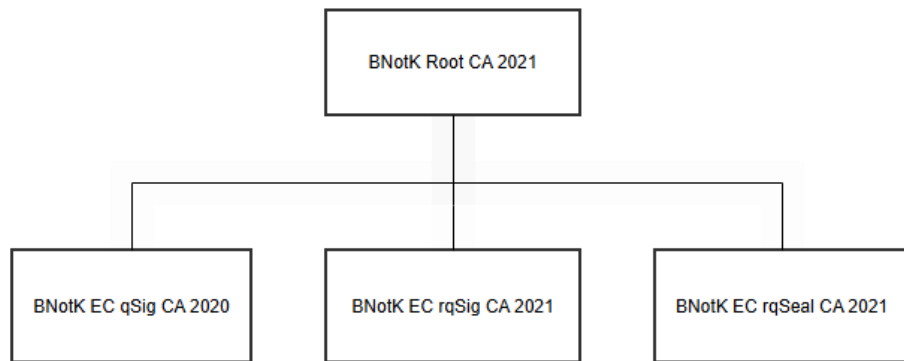
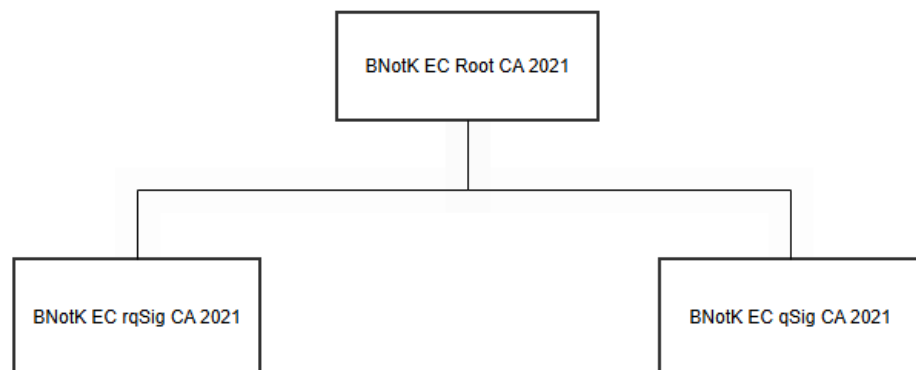


Abbildung IV



Die Abbildungen III & IV zeigen die aktive PKI Hierarchie des VDA BNotK mit Elliptic Curve (ECDSA).

Qualifizierte Zertifikate

Die ausgegebenen Endanwenderzertifikate entsprechen den Anforderungen der eIDAS-Verordnung (EU 910/2014) sowie des folgenden Zertifizierungslevel nach ETSI EN 319 411-2:

QCP-n-qscd – Qualifizierte Personenzertifikate auf qualifizierter Signaturerstellungseinheit.

QCP-l-qscd – Qualifizierte Siegelzertifikate auf qualifizierter Signaturerstellungseinheit.

1.2 Name und Kennzeichnung des Dokuments

Dokumentename: Zertifizierungskonzept des VDA BNotK

Kennzeichnung (OID): 1.3.6.1.4.1.41460.5.2.1.1.2

Version: 3.6

1.3 PKI-Teilnehmer

Siehe Abschnitt 1.3 der Zertifikatsrichtlinie (CP) des VDA BNotK.

1.4 Verwendung von Zertifikaten

Zertifikatsinhaber dürfen die vom VDA BNotK ausgegebenen qualifizierten Zertifikate ausschließlich für eigene berufliche Zwecke nutzen. Sie handeln insoweit auf eigene Verantwortung. Die Einschätzung, ob dieses Zertifizierungskonzept den Anforderungen einer Anwendung entspricht und ob die Benutzung des betreffenden qualifizierten Zertifikats zu einem bestimmten Zweck geeignet ist, obliegt dem Zertifikatsinhaber.

Der VDA BNotK übernimmt keine Haftung für den Fall, dass ein Zertifikatsinhaber ein qualifiziertes Zertifikat zu anderen als beruflichen Zwecken nutzt.

Für die Verwendung der qualifizierten Zertifikate zur Erzeugung qualifizierter elektronischer Signaturen oder Siegel ist ausschließlich eine (remote-)QSCD erforderlich.

Ferner unterliegt der Zertifikatsinhaber den gesetzlichen Pflichten sowie ggf. weitergehenden oder abweichenden Pflichten aufgrund einzelvertraglicher Regelungen.

1.4.1 Verwendung von Dienstzertifikaten

Zur Erbringung von Vertrauensdiensten gemäß eIDAS nutzt der VDA BNotK Dienstzertifikate für den internen Gebrauch. Die Ausstellung erfolgt durch den VDA BNotK.

Dienstzertifikate finden in den folgenden Fällen Anwendung:

- CA-Zertifikate zur CA- und Zertifikatserstellung,
- Signatur von Statusauskünften (OCSP),
- Signatur von Zeitstempeln.

1.5 Verwaltung des Zertifizierungskonzepts

Das Zertifizierungskonzept wird durch die Zertifizierungsstelle der Bundesnotarkammer verwaltet. Es wird regelmäßig, mindestens alle zwölf Monate, überprüft und falls erforderlich aktualisiert. Eine Überprüfung des Zertifizierungskonzepts erfolgt insbesondere bei einer Änderung der für den VDA BNotK wesentlichen Gesetze sowie bei der Änderung betrieblicher Abläufe.

Verantwortlich für die Verwaltung dieses Dokuments ist der Leiter der Zertifizierungsstelle der Bundesnotarkammer oder, wenn dieser verhindert ist, sein designierter Stellvertreter.

Im Falle einer Änderung wird die geänderte Fassung auf der Internetseite des VDA BNotK (unter: <https://zertifizierungsstelle.bnotk.de/veroeffentlichungen>) veröffentlicht und durch die Vergabe einer neuen Versionsnummer kenntlich gemacht. Vor einer Veröffentlichung ist zunächst die Freigabe durch die Geschäftsleitung des VDA BNotK erforderlich.

Den für die Verwaltung zuständigen Ansprechpartner können Sie unter folgender Adresse erreichen:

Zertifizierungsstelle der Bundesnotarkammer

z. Hd. des Leiters der Zertifizierungsstelle

Anton-Wilhelm-Amo-Straße 34

10117 Berlin

E-Mail: zs@bnotk.de

1.6 Definitionen und Abkürzungen

Begriff	Beschreibung
Zertifikatsinhaber (Subject)	<p>Natürliche oder juristische Person, der ein qualifiziertes Zertifikat ausgestellt und eindeutig zugeordnet ist.</p> <p>Der Zertifikatsinhaber ist Träger der sich aus diesem CPS sowie aus den gesetzlichen und vertraglichen Regelungen ergebenden Rechte und Pflichten in Bezug auf die Nutzung des qualifizierten Zertifikats.</p> <p>Siehe auch Abschnitt 1.4.3 der Zertifikatsrichtlinie (CP).</p>
Antragsteller (Subscriber)	<p>Natürliche Person, die die Ausstellung eines qualifizierten Zertifikats beantragt. Siehe auch Abschnitt 1.4.3 der Zertifikatsrichtlinie (CP)</p>
Unterzeichner / Siegelersteller	<p>Natürliche Person, die im Rahmen des Server Signing Application Service (SSAS) eine qualifizierte elektronische Signatur oder ein qualifiziertes elektronisches Siegel auslöst.</p> <p>Der Unterzeichner handelt unter Nutzung eines Fernsignatur- oder Fernsiegelerstellungsgeräts und gibt die zur Signatur- oder Siegelerstellung erforderliche aktive und explizite Willensbekundung ab.</p>

Für weitere Definitionen siehe Abschnitt 1.7 der Zertifikatsrichtlinie (CP) des VDA BNotK.

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der VDA BNotK betreibt ein öffentlich zugängliches Repository zur Veröffentlichung von Zertifikatsrichtlinien (CP), Zertifizierungspraktiken (CPS) sowie weiterer relevanter Informationen unter:

<https://zertifizierungsstelle.bnotk.de/veroeffentlichungen>

Das Repository ist grundsätzlich 24 Stunden täglich an sieben Tagen pro Woche erreichbar. Die veröffentlichten Informationen werden aktuell gehalten.

Die maximale zulässige Nichtverfügbarkeit des Repository beträgt insgesamt höchstens drei Werk-tage pro Kalenderjahr. Geplante Wartungsarbeiten werden – soweit möglich – vorab angekündigt.

Widerrufsinformationen werden über einen öffentlich zugänglichen OCSP-Responder bereitgestellt. Die OCSP-Responder-Adresse ist im jeweiligen Zertifikat im Authority Information Access (AIA)-Feld enthalten (siehe Kapitel 7.1.).

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der VDA BNotK veröffentlicht die folgenden Informationen zu den von ihm ausgegebenen qualifizierten Zertifikaten:

- Statusinformationen,
- CA-Zertifikate
- die Unterrichtsbroschüre für qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel,
- die Zertifikatsrichtlinie,
- dieses Zertifizierungskonzept,
- das PKI Disclosure Statement für qualifizierte Zertifikate.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht. Der Status der von dem VDA BNotK erstellten CA-Zertifikate kann in einen Zeitraum von mindestens 10 Jahren nach Ende der Gültigkeit des jeweiligen Zertifikates abgerufen werden.

Weitere Regelungen sind in der Zertifikatsrichtlinie (CP) in Abschnitt 2.3 beschrieben.

2.4 Zugang zu den Informationen

Siehe Abschnitt 2.4 der Zertifikatsrichtlinie (CP) des VDA BNotK.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Qualifizierte Zertifikate müssen den Namen des Zertifikatsinhabers enthalten. Die qualifizierten Zertifikate entsprechen dem Profil des Standards ITU-T Recommendation X 509. V3 und enthalten einen aus mehreren Informationen zusammengesetzten Namen.

3.1.2 Aussagekraft von Namen

Die verwendeten Namen sind eindeutig (vgl. dazu Abschnitt 3.1.5).

3.1.3 Pseudonyme

Auf Verlangen eines Antragstellers führt der VDA BNotK in einem qualifizierten Zertifikat an Stelle eines Namens ein Pseudonym auf. Das Pseudonym muss dem Zertifikatsinhaber unverwechselbar zugeordnet sein und als solches kenntlich gemacht werden.

Qualifizierte Zertifikate, die ein Pseudonym enthalten, entsprechen dem Profil des Standards ITU-T Recommendation X 509. V3 und enthalten einen aus mehreren Informationen zusammengesetzten Namen. Es handelt sich hier um mindestens die folgenden Informationen:

- CN (common name) = Gebräuchlicher Name
- serialNumber = Seriennummer

Hinweis: Pseudonyme sind für qualifizierte Zertifikate für juristische Personen (Siegelzertifikate) ausgeschlossen.

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Siehe Abschnitt 7.1 dieses Dokuments.

3.1.5 Eindeutigkeit von Namen

- Bei natürlichen Personen (QCP-n-qscd)

Der Name muss eindeutig sein, um die Feststellung des Zertifikatsinhabers ohne Verwechslungsgefahr zu ermöglichen.

Die Namen setzen sich mindestens aus den folgenden Bestandteilen zusammen:

- Vorname (G)
- Nachname (SN)
- Common Name (CN)
- Seriennummer (= Zertifikatsnummer)
- countryName (C)

Die Seriennummer wird für jedes Zertifikat eindeutig vergeben. Eine Verwechslungsmöglichkeit von mehreren Zertifikaten für eine Person oder von mehreren Zertifikaten für verschiedene Personen mit gleichem Vor- und Nachnamen ist ausgeschlossen, da die Eindeutigkeit durch den Zusatz „Seriennummer“ gegeben ist.

- Bei juristischen Personen (QCP-I-qscd)

Der Name einer juristischen Person muss eindeutig sein, um die Feststellung des Zertifikatsinhabers ohne Verwechslungsgefahr zu ermöglichen.

Die Namen setzen sich mindestens aus den folgenden Bestandteilen zusammen:

- countryName (C)
- Common Name (CN)
- organizationName (O)
- organizationIdentifier Organisationssitz Deutschland
- Seriennummer (= Zertifikatsnummer)

Die Seriennummer wird für jedes Zertifikat eindeutig vergeben.

Anträge für qualifizierte Zertifikate für qualifizierte Siegel sind stets durch einen rechtlich vertretungsberechtigten Repräsentanten der juristischen Person zu stellen.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Der Antragsteller trägt die Verantwortung für die Vereinbarkeit des gewählten Pseudonyms bzw. Common-Name mit den Rechten Dritter, z.B. Namens-, Marken-, Urheber- oder sonstigen Schutzrechten, sowie mit den allgemeinen Gesetzen.

3.1.7 Testzertifikate

Der VDA BNotK kann qualifizierte Zertifikate aus der produktiven CA-Hierarchie ausstellen, die im Zertifikat als ‚Test‘ gekennzeichnet sind.

Die Kennzeichnung dient ausschließlich der transparenten Erkennbarkeit einer durch den Antragsteller beabsichtigten Nutzung zu Testzwecken und berührt nicht die rechtliche Einordnung als qualifiziertes Zertifikat.

Die Testzertifikate für natürliche Personen müssen eindeutig als Solche gekennzeichnet und erkennbar sein, z.B. durch den eindeutigen Ausdruck „TEST“ bei einer evtl. vorhandenen Organisationsbezeichnung. Für die Aufnahme von Pseudonymen ist die Angabe des Ausdrucks „Testkarte“ gefolgt von einer beliebigen Zeichenfolge erforderlich, welche den Zertifikatsinhaber im Kontext der PKI eindeutig identifiziert.

Testzertifikate werden unter Anwendung des vollständigen und unveränderten Antrags- und Identifizierungsprozesses ausgestellt und entsprechen in vollem Umfang den Anforderungen der jeweils gültigen Zertifikatsrichtlinie (CP) sowie den einschlägigen Anforderungen der ETSI EN 319 411-1 und EN 319 411-2.

Der VDA BNotK dokumentiert keinen konkreten Testzweck und überwacht keine Testzeiträume. Die Verantwortung für Nutzung und Widerruf liegt beim Zertifikatsinhaber bzw. dem vertretungsberechtigten Antragsteller.

Testzertifikate unterliegen keiner automatischen Sperrung oder vorzeitigen Widerrufsregelung.

Die maximale Gültigkeitsdauer beträgt fünf Jahre.

Ein Re-Key-Prozess ist nicht vorgesehen.

Für juristische Personen werden im Repository des VDA BNotK Testzertifikate zur Verfügung gestellt.

3.2 Identifizierung der Zertifikatsinhaber

Der VDA BNotK hat Personen, die ein qualifiziertes Zertifikat beantragen, eindeutig zu identifizieren. Dabei werden nur die Informationen erfasst, die zur Bereitstellung der vom VDA BNotK angebotenen Vertrauensdienste erforderlich sind.

Die Identifizierung ist notwendig, wenn der Zertifikatsinhaber bisher noch nicht identifiziert wurde oder sich identitätsrelevante Daten geändert haben, z.B. bei einer Namensänderung des Zertifikatsinhabers.

- Qualifizierte Zertifikate für natürliche Personen (für qualifizierte Signaturen)

Für die Identifizierung werden mindestens der vollständige Name, das Geburtsdatum, der Geburtsort sowie die Ausweisdaten des Antragstellers erhoben. Zudem muss der Antragsteller seine Anschrift und eine E-Mail-Adresse im Rahmen des Registrierungsprozesses angeben.

Die Identifizierung erfolgt grundsätzlich anhand der folgenden Lichtbilddokumente:

- Personalausweis der Bundesrepublik Deutschland,
- Personalausweis oder elektronischer Aufenthaltstitel der Bundesrepublik Deutschland mit elektronischer Ausweiskfunktion,
- Reisepass, der auf eine Person mit Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes ausgestellt worden ist,
- Dokumente oder geeignete technische Verfahren mit gleichwertiger Sicherheit zu einer Identifizierung wie die in den vorstehenden Absätzen genannten Dokumente.
- eID-Identifizierungsmittel mit dem Vertrauensniveau „hoch“.

- [Qualifizierte Zertifikate für juristische Personen \(für qualifizierte Siegel\)](#)

Bei qualifizierten Siegelzertifikaten werden sowohl die Organisation als Zertifikatsinhaber sowie der vertretungsberechtigte Antragsteller identifiziert.

Die Identifizierung des vertretungsberechtigten Antragstellers erfolgt gemäß den Anforderungen an die Identifizierung von natürlichen Personen.

Für die Identifizierung der Organisation sind insbesondere folgende Angaben und Nachweise erforderlich:

- Der amtliche Organisationsname,
- der Organisationssitz in Deutschland,
- eine Bescheinigung über den Organisationsnachweis (abhängig von der Organisationsform),
- der Nachweis der Vertretungsberechtigung des Antragstellers.

Die Identifizierung der Organisation erfolgt abhängig von der Organisationsform grundsätzlich anhand der folgenden Dokumente:

- Amtlicher Handelsregisterauszug (nicht älter als 4 Wochen),
- Beglaubigter Satzungsbeschluss;
- Notarielle Bescheinigung gem. § 21 i.V.m. § 24 BNotO (sog. Vertretungs- und Registerbescheinigung);
- Amtliche Bescheinigung der übergeordneten Behörde (Fach- oder Rechtsaufsichtsbehörde)

3.2.1 Identifizierungsverfahren der Antragsteller

- Zuordnung der Anwendungsfälle (Use Cases) entsprechend TS 119 641

Die Identitätsprüfung ist der Prozess, mit dem mit der erforderlichen Zuverlässigkeit nachgewiesen wird, dass die angegebene Identität eines Antragstellers korrekt ist.

Neben den beschriebenen Identifizierungsverfahren und Nachweisen können bei Bedarf weitere geeignete Nachweise, Bescheinigungen oder vertrauenswürdige Register als ergänzende Quellen herangezogen werden, sofern sie zur zuverlässigen Feststellung der Identität geeignet sind.

Die eingesetzten Identifizierungsverfahren entsprechen dem erweiterten Sicherheitsniveau (Extended LoIP) gemäß TS 119 461 und werden folgendermaßen den Uses Cases der Norm zugeordnet:

Natürliche Personen

Anwesenheit des Antragstellers	Vorgang	Umgesetzte TS 119 461 Referenz	Ausweis-dokument	Überprüfung der Nachweise	Binding an den Antragsteller
Notarident,	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell
Gerichtident	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell
Rechtsanwalts-kammerident	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell
RA-Ident	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell
eIDent	Automated	9.2.3.3 Annex C.3.2	Digital	Automated	Auto-mated

Juristische Personen

Anwesenheit des Antragstellers	Vorgang	Umgesetzte TS 119 461 Referenzen	Ausweis-dokument	Überprüfung der Nachweise	Binding an den Antragsteller
Notarident Gerichtident RA-Ident	Manuell	9.3+ 9.4 Annex C.3.6	Physisch	Manuell	Manuell

- [Qualifizierte Zertifikate für natürliche Personen \(für qualifizierte Signaturen\)](#)

Die Identifizierung des Antragstellers für ein qualifiziertes Signaturzertifikat kann grundsätzlich unter Nutzung folgender Verfahren erfolgen:

- Notarident – Identifizierung durch Notare,
- Gerichtident – Identifizierung durch deutsche Gerichte,
- Rechtsanwaltskammerident – Identifizierung durch Mitarbeiter von Rechtsanwaltskammern,
- eIDent – Identifizierung durch elektronischen Identitätsnachweis,
- RA-Ident – Identifizierung durch Mitarbeiter der RA des VDA BNotK.

Die Entscheidung über die Wahl der konkret angebotenen Identifizierungsverfahren obliegt dem jeweiligen Antragsteller. Allerdings werden nicht sämtliche Identifizierungsverfahren bei allen Produkten des VDA BNotK angeboten. Eine Identifizierung mit dem Verfahren Rechtsanwaltskammerident ist z.B. nur bei der Bestellung eines beA-Produkts möglich und nur dann, wenn die zuständige Rechtsanwaltskammer dieses Verfahren anbietet. Das Identifizierungsverfahren Gerichtident wird lediglich für Angehörige der Justiz angeboten. Eine Identifizierung mittels des RA-Identverfahrens ist nur bei der Identifizierung von Mitarbeitern der Bundesnotarkammer K.d.ö.R möglich.

Der Antragsteller hat im Zuge der Antragseingabe eines der ihm angebotenen Identifizierungsverfahren auszuwählen. Abhängig von der getroffenen Auswahl wird der Antragsteller im Anschluss an die Online-Eingabe der Antragsdaten darüber informiert, wie er das ausgewählte Verfahren zu nutzen hat. Zugleich werden ihm in Abhängigkeit vom gewählten Identifizierungsverfahren die passenden Identifizierungsunterlagen zum Ausdruck bereitgestellt.

- [Qualifizierte Zertifikate für juristische Personen \(für qualifizierte Siegel\)](#)

Die Identifizierung des vertretungsberechtigten Antragstellers für ein qualifiziertes Siegelzertifikat kann grundsätzlich unter Nutzung folgender Verfahren erfolgen:

- Notarident – Identifizierung durch Notare,
- Gerichtident – Identifizierung durch deutsche Gerichte,
- RA-Ident – Identifizierung durch Mitarbeiter der RA des VDA BNotK.

Die Entscheidung über die Wahl der konkret angebotenen Identifizierungsverfahren obliegt dem jeweiligen Antragsteller. Allerdings werden nicht sämtliche Identifizierungsverfahren bei allen Produkten des VDA BNotK angeboten. Eine Identifizierung mit dem Verfahren RA-Ident ist nur bei der Identifizierung von Tochtergesellschaften und Einrichtungen der Bundesnotarkammer K.d.ö.R möglich. Das Verfahren Gerichtident wird lediglich für Organisationen aus dem Bereich der Justiz angeboten.

Der Antragsteller hat im Zuge der Antragseingabe eines der ihm angebotenen Identifizierungsverfahren auszuwählen. Abhängig von der getroffenen Auswahl wird der Antragsteller im Anschluss an die Online-Eingabe der Antragsdaten darüber informiert, wie er das ausgewählte Verfahren zu nutzen hat. Zugleich werden ihm in Abhängigkeit vom gewählten Identifizierungsverfahren die passenden Identifizierungsunterlagen zum Ausdruck bereitgestellt.

Bei der Beantragung eines qualifizierten Siegelzertifikats ist zudem ein Nachweis über die Vertretungsberechtigung des Antragstellers zu erbringen. Dieser Nachweis erfolgt grundsätzlich anhand eines der folgenden Dokumente:

- Amtlicher Handelsregisterauszug (nicht älter als 4 Wochen),
- Beglaubigter Satzungsbeschluss;
- Notarielle Bescheinigung gem. § 21 i.V.m. § 24 BNotO (sog. Vertretungs- und Registerbescheinigung);
- Amtliche Bescheinigung der übergeordneten Behörde (Fachaufsichts- oder Rechtsaufsichtsbehörde).

3.2.1.1 Prüfung von Identitätsmerkmalen

Im Rahmen der physischen Identitätsprüfung erfolgt ein Abgleich zwischen dem Lichtbild im vorgelegten Identitätsdokument und dem Erscheinungsbild der vorstellenden Person.

Dabei werden insbesondere biometrische Merkmale (z. B. Gesichtsform, Augen, Nase und Mund) sowie Auffälligkeiten berücksichtigt. Die Bewertung erfolgt anhand der Übereinstimmung dieser Merkmale und dient der eindeutigen Zuordnung zur Person.

Die an der Identitätsprüfung beteiligten Mitarbeiter verfügen über ausreichend Zeit und geeignete Bedingungen, um eine sorgfältige und unbeeinträchtigte Prüfung durchzuführen. Zur Unterstützung stehen geeignete Hilfsmittel (z. B. Lichtquellen oder Anzeigenhilfen) zur Verfügung.

Die Mitarbeiter haben Zugriff auf aktuelle und verlässliche Informationsquellen zur Prüfung von Ausweisdokumenten, insbesondere auf öffentlich verfügbare Referenzdatenbanken wie das „Public Register of Authentic Travel and Identity Documents Online“ (PRADO). Diese werden zur Unterstützung der Prüfung der Echtheit und Gültigkeit vorgelegter Identitätsdokumente herangezogen.

Kann keine ausreichende Übereinstimmung festgestellt werden oder bestehen Zweifel an der Identität, ist der Identifizierungsprozess abubrechen.

Die Entscheidung über die Identitätsfeststellung erfolgt auf Basis der vorliegenden Nachweise und wird nachvollziehbar dokumentiert.

Die in diesem Abschnitt beschriebenen Prüfprozesse werden durch interne Handlungsanweisungen und Leitfäden weiter konkretisiert. Diese werden regelmäßig überprüft und dürfen den

Anforderungen dieses Zertifizierungskonzepts nicht widersprechen.

3.2.1.2 Verfahren Notarident

Beim Identifizierungsverfahren Notarident wird die Identifizierung durch einen Notar mit Amtssitz in Deutschland mittels Unterschriftsbeglaubigung des Antragstellers durchgeführt. Hierbei sind die Vorgaben des Beurkundungsgesetzes, insbesondere aus § 40 BeurkG, zu beachten.

- [Qualifizierte Zertifikate für natürliche Personen \(für qualifizierte Signaturen\)](#)

Das Verfahren Notarident umfasst bei qualifizierten Signaturzertifikaten:

- Die Entgegennahme der (unterschiedenen bzw. noch zu unterschreibenden) Antragsunterlagen und Beglaubigung der Unterschrift des Antragstellers auf dem Antragsformular i.S.d. § 40 BeurkG durch den Notar;
- Das Erstellen einer beglaubigten Abschrift des zur Identifizierung verwendeten Ausweisdokumentes sowie ggf. verwendeter Nachweise des Dr.-Titels durch den Notar;
- Der Versand der Urkunde bzw. einer elektronisch beglaubigten Abschrift der Urkunde durch den Notar an den VDA BNotK per Post oder auf elektronischen Weg.

Postalisch sind Unterlagen in einem Umschlag unmittelbar an den VDA BNotK zu versenden. Alternativ zum Postversand kann der Notar von sämtlichen Unterlagen elektronisch beglaubigte Abschriften i. S. d. § 39a BeurkG erstellen. Die mit einer qualifizierten elektronischen Signatur des Notars versehenen Dateien werden anschließend sicher elektronisch an das EGVP-Postfach der Zertifizierungsstelle der Bundesnotarkammer versandt. Die Übertragung erfolgt Ende-zu-Ende verschlüsselt.

Beim Verfahren Notarident erfolgt weder eine Prüfung der Antragsunterlagen noch eine Unterrichtung des Antragstellers durch den Notar.

- [Qualifizierte Zertifikate für juristische Personen \(für qualifizierte Siegel\)](#)

Bei der Identifizierung des Zertifikatsinhabers und des vertretungsberechtigten Antragstellers sind die Vorgaben des Beurkundungsgesetzes, insbesondere aus § 40 BeurkG, zu beachten.

Das Verfahren Notarident umfasst bei qualifizierten Siegelzertifikaten:

- Entgegennahme der (unterschiedenen bzw. noch zu unterschreibenden) Antragsunterlagen und Beglaubigung der Unterschrift des Antragstellers auf dem Antragsformular i.S.d. § 40 BeurkG durch den Notar;
- Erstellen einer beglaubigten Abschrift des zur Identifizierung verwendeten Ausweisdokumentes sowie ggf. verwendeter Nachweise des Dr.-Titels durch den Notar;

- Bei Personengesellschaften: Das Anfertigen einer Vertretungs- und Registerbescheinigung nach § 21 BNotO durch den Notar.
Für die Bescheinigung genügt ein sog. einfaches Zeugnis in Vermerkform.
In der Bescheinigung ist die Registereintragung der juristischen Person sowie die Vertretungsberechtigung des Antragstellers festzustellen. Zusätzlich ist das Register sowie der Tag der Einsichtnahmen in das Register oder eines beglaubigten Registerauszugs anzugeben
- Bei Behörden und Organisationen des öffentlichen Rechts: Die Entgegennahme einer ausgefüllten amtlichen Bescheinigung der übergeordneten Behörde als Nachweis für das Bestehen der Organisation sowie der Vertretungsberechtigung des Antragstellers.
- Versand der Urkunde bzw. einer elektronisch beglaubigten Abschrift der Urkunde durch den Notar an den VDA BNotK per Post oder auf elektronischen Weg.

Postalisch sind Unterlagen in einem Umschlag unmittelbar an den VDA BNotK zu versenden. Alternativ zum Postversand kann der Notar von sämtlichen Unterlagen elektronisch beglaubigte Abschriften i. S. d. § 39a BeurkG erstellen. Die mit einer qualifizierten elektronischen Signatur des Notars versehenen Dateien werden anschließend sicher elektronisch an das EGVP-Postfach der Zertifizierungsstelle der Bundesnotarkammer versandt. Die Übertragung erfolgt Ende-zu-Ende verschlüsselt.

Beim Verfahren Notarident erfolgt weder eine Prüfung der Antragsunterlagen noch eine Unterrichtung des Antragstellers oder des Zertifikatsinhabers durch den Notar. Die Prüfung der Antragsunterlagen sowie die abschließende Bewertung der Identitätsnachweise erfolgt durch den VDA BNotK.

3.2.1.3 Verfahren Gerichtident

- **Qualifizierte Zertifikate für natürliche Personen (für qualifizierte Signaturen)**

Die Identifizierung des Antragstellers kann bei Justizangehörigen auch durch den Präsidenten oder Direktor eines deutschen Gerichts erfolgen. Hierbei sind die Anforderungen an die Beglaubigung von Unterschriften durch Behörden (§ 34 VwVfG bzw. entsprechende landesrechtliche Vorschriften) einzuhalten.

Bei der Identifizierung durch ein Gericht gelten für die Kontrollpflichten und die Fassung des Beglaubigungsvermerks die gleichen Maßstäbe wie für die Identifizierung durch den Notar im Rahmen des Verfahrens Notarident (vgl. Abschnitt 3.2.1.1). Der Antragsteller hat bei der Identifizierung eines der in Abschnitt 3.2. genannten Dokumente vorzulegen.

Das Verfahren Gerichtident umfasst bei qualifizierten Signaturzertifikaten:

- Entgegennahme der (unterschriebenen bzw. noch zu unterschreibenden) Antragsunterlagen und Beglaubigung der Unterschrift des Antragstellers auf dem Antragsformular i.S.d. §

34VwVfG.;

- Beifügung einer Kopie des zur Identifizierung verwendeten Ausweisdokumentes sowie ggf. verwendeter Nachweise des Dr.-Titels zu den Antragsunterlagen;
 - Postalischer Versand der Antragsunterlagen durch die beglaubigende Stelle in einem Umschlag unmittelbar an den VDA BNotK. Die vom Antragsteller ggf. eingeholte Bestätigung berufsbezogener Angaben wird – wenn erforderlich – beigelegt, sofern sie nicht unmittelbar von der bestätigenden Stelle übersandt wird.
- **Qualifizierte Zertifikate für juristische Personen (für qualifizierte Siegel)**

Die Identifizierung des Zertifikatsinhabers und des vertretungsberechtigten Antragstellers kann bei Justizangehörigen auch durch den Präsidenten oder Direktor eines deutschen Gerichts erfolgen. Hierbei sind die Anforderungen an die Beglaubigung von Unterschriften durch Behörden (§ 34 VwVfG bzw. entsprechende landesrechtliche Vorschriften) einzuhalten.

Bei der Identifizierung durch ein Gericht gelten für die Kontrollpflichten und die Fassung des Beglaubigungsvermerks die gleichen Maßstäbe wie für die Identifizierung durch den Notar im Rahmen des Verfahrens Notarident (vgl. Abschnitt 3.2.1.1).

Der vertretungsberechtigte Antragsteller hat bei der Identifizierung die in Abschnitt 3.2. genannten Dokumente zum Nachweis seiner persönlichen Identität, zum Nachweis der Identität der juristischen Person als Zertifikatsinhaber sowie zum Nachweis seiner Vertretungsberechtigung für den Zertifikatsinhaber vorzulegen.

Das Verfahren Gerichtident umfasst bei qualifizierten Siegelzertifikaten:

- Entgegennahme der (unterschriebenen bzw. noch zu unterschreibenden) Antragsunterlagen und Beglaubigung der Unterschrift des Antragstellers auf dem Antragsformular i.S.d. § 34VwVfG;
- Beifügung einer Kopie des zur Identifizierung verwendeten Ausweisdokumentes sowie ggf. verwendeter Nachweise des Dr.-Titels zu den Antragsunterlagen;
- Entgegennahme und Beifügung einer ausgefüllten amtlichen Bescheinigung der übergeordneten Behörde als Nachweis für das Bestehen der Organisation sowie der Vertretungsberechtigung des Antragstellers.
- Postalischer Versand der Antragsunterlagen durch die beglaubigende Stelle in einem Umschlag unmittelbar an den VDA BNotK. Die vom Antragsteller ggf. eingeholte Bestätigung berufsbezogener Angaben wird – wenn erforderlich – beigelegt, sofern sie nicht unmittelbar von der bestätigenden Stelle übersandt wird.

Beim Verfahren Gerichtident erfolgt weder eine Prüfung der Antragsunterlagen noch eine Unterrichtung durch den Präsidenten oder Direktor des Gerichts.

Die Prüfung der Antragsunterlagen sowie die abschließende Bewertung der Identitätsnachweise

erfolgt durch den VDA BNotK.

3.2.1.4 Verfahren Rechtsanwaltskammerident

Die Identifizierung des Antragstellers kann auch durch einen Mitarbeiter einer deutschen Rechtsanwaltskammer erfolgen, beispielsweise im Rahmen der Vereidigung nach § 12a BRAO.

Das Verfahren Kammerident umfasst:

- Entgegennahme der unterschriebenen Antragsunterlagen und Prüfung auf formale und inhaltliche Richtigkeit durch einen Mitarbeiter der Rechtsanwaltskammer;
- Ablichten von Ausweisdokumenten bzw. Vergleich vom Antragsteller übergebener Ablichtungen mit dem (Original)-Ausweisdokument;
- Identifizierung des Antragstellers und Prüfung der Identifikationsdaten anhand der Ausweisdokumente;
- Einscannen sämtlicher Unterlagen (Antragsunterlagen und Ausweisdokumente) durch einen Mitarbeiter der Rechtsanwaltskammer unter Aufbringung einer mindestens fortgeschrittenen elektronischen Signatur.

Der Mitarbeiter bestätigt mit der Signatur, dass die Scans bildlich und inhaltlich mit dem Papieroriginal übereinstimmen.

- Übertragung der mit der mindestens fortgeschrittenen elektronischen Signatur versehenen elektronischen Dateien über eine Webapplikation durch die Rechtsanwaltskammer an die RA. Die Übertragung erfolgt transportverschlüsselt.

Die Geschäftsführer der Rechtsanwaltskammern werden vom VDA BNotK geschult und tragen Sorge dafür, dass nur unbedenkliches Personal, welches auch zur Identifizierung im Rahmen der Vereidigung eingesetzt wird, am Kammerident-Verfahren teilnimmt.

3.2.1.5 Verfahren eIDent

Bei der Identifizierung mittels elektronischen Identitätsnachweises erfolgt die Identifizierung während der Online-Eingabe der Antragsdaten und Übermittlung in das RA-System.

Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des Ausweisdokumentes bzw. des eID-Token über die sichere eID- Infrastruktur. Der Nachweis des Identifizierungsvorgangs wird zusammen mit den Antragsdaten dokumentiert.

Der VDA BNotK akzeptiert sämtliche elektronischen Identitätsnachweise, die über das Sicherheitsniveau „hoch“ verfügen und von der europäischen Kommission anerkannt wurden.

3.2.1.6 Verfahren RA-Ident

Antragsteller, die Mitarbeiter der Bundesnotarkammer K. d. ö. R. sind, können durch einen

RA-Mitarbeiter identifiziert werden. Die Antragstellung sowie die Identifizierung finden dabei in den Räumlichkeiten des VDA BNotK statt.

- [Qualifizierte Zertifikate für natürliche Personen \(für qualifizierte Signaturen\)](#)

Das Verfahren RA-Ident umfasst bei qualifizierten Signaturzertifikaten:

- Entgegennahme der Antragsunterlagen durch den RA-Mitarbeiter und Prüfung auf formale und inhaltliche Richtigkeit;
- Ablichten von Ausweisdokumenten bzw. Vergleich vom Antragsteller übergebener Ablichtungen mit dem (Original)-Ausweisdokument durch den RA-Mitarbeiter;
- Identifizierung des Antragstellers und Prüfung der Identifikationsdaten anhand der Ausweisdokumente durch den RA-Mitarbeiter;
- Unterschrift des Antragstellers auf der letzten Seite des Antragsdokumentes
- Prüfung und Abgleich der im Beisein des RA-Mitarbeiters durchgeführten Unterschrift mit der im Ausweisdokument ersichtlichen Unterschrift;
- Unterschrift des RA-Mitarbeiters auf dem Identifizierungsformular;
- Erstellung und Signierung einer Zusammenfassung der Identifikationsdaten durch den RA-Mitarbeiter;
- Übertragen des Identifizierungsformulars nebst der Antragsdaten und des Identifikationsdokumentes durch den RA-Mitarbeiter in das RA-System unter Aufbringung einer mindestens fortgeschrittenen elektronischen Signatur.

Um zu verhindern, dass bei Durchführung des RA-Ident-Verfahrens außerhalb der sicheren RA-Umgebung gefälschte Anträge eingebracht werden, unterschreibt der RA-Mitarbeiter auf jeder Seite der Antragsunterlagen oder bringt sein Kürzel an. Danach werden die Antragsdaten und Identifizierungsdokumente sowie ein Identifizierungsformular vom RA-Mitarbeiter gescannt, mindestens fortgeschritten signiert und an das RA-System übertragen.

- [Qualifizierte Zertifikate für juristische Personen \(für qualifizierte Siegel\)](#)

Vertretungsberechtigte Antragsteller von Tochtergesellschaften und Einrichtungen der Bundesnotarkammer K.d.ö.R. können durch einen RA-Mitarbeiter identifiziert werden. Die Antragstellung sowie die Identifizierung finden dabei in den Räumlichkeiten des VDA BNotK statt.

Das Verfahren RA-Ident umfasst bei qualifizierten Siegelzertifikaten:

- Entgegennahme der Antragsunterlagen durch den RA-Mitarbeiter und Prüfung auf formale und inhaltliche Richtigkeit;
- Ablichten von Ausweisdokumenten bzw. Vergleich vom Antragsteller übergebener Ablichtungen mit dem (Original)-Ausweisdokument durch den RA-Mitarbeiter;
- Identifizierung des Antragstellers und Prüfung der Identifikationsdaten anhand

- der Ausweisdokumente durch den RA-Mitarbeiter;
- Unterschrift des Antragstellers auf der letzten Seite des Antragsdokumentes
- Prüfung und Abgleich der im Beisein des RA-Mitarbeiters durchgeführten Unterschrift mit der im Ausweisdokument ersichtlichen Unterschrift;
- Unterschrift des RA-Mitarbeiters auf dem Identifizierungsformular;
- Entgegennahme und Prüfung eines amtlichen Handelsregisterauszugs (nicht älter als 4 Wochen) oder eines beglaubigten Satzungsbeschlusses als Nachweis für das Bestehen der Organisation sowie der Vertretungsberechtigung des Antragstellers;
- Erstellung und Signierung einer Zusammenfassung der Identifikationsdaten durch den RA-Mitarbeiter;
- Übertragen des Identifizierungsformulars nebst der Antragsdaten und des Identifikationsdokumentes durch den RA-Mitarbeiter in das RA-System unter Aufbringung einer mindestens fortgeschrittenen elektronischen Signatur.

Um zu verhindern, dass bei Durchführung des Verfahren RA-Ident außerhalb der sicheren RA-Umgebung gefälschte Anträge eingebracht werden, unterschreibt der RA-Mitarbeiter auf jeder Seite der Antragsunterlagen oder bringt sein Kürzel an. Danach werden die Antragsdaten und Identifizierungsdokumente sowie ein Identifizierungsformular vom RA-Mitarbeiter gescannt, mindestens fortgeschritten signiert und an das RA-System übertragen.

3.2.1.7 Nutzung vertrauenswürdiger Register

Das vom VDA BNotK im Rahmen der Identitätsprüfung verwendete vertrauenswürdige Register ist das Notarverzeichnis (NVZ). Dieses wird zur Übermittlung und Bestätigung von Daten für Notarattribute genutzt.

Zur Vermeidung von Einzelbestätigungen greift der VDA BNotK auf Grundlage schriftlicher Vereinbarungen mit den regionalen Notarkammern auf das bei der Bundesnotarkammer geführte Notarverzeichnis als vertrauenswürdige Datenquelle zurück.

Die Kommunikation mit dem Register erfolgt online und wird durch Verwendung aktueller TLS-Versionen oder eines Protokolls mit vergleichbarem Sicherheitsniveau gesichert.

Das Notarverzeichnis ist nicht öffentlich. Der Zugriff erfolgt über einen NVZ-Client unter Verwendung von HTTPS sowie eines Authentisierungsverfahrens auf Basis von Benutzername und Passwort.

Eine nachrichtenbasierte Kommunikation (via AMQ) erfolgt ausschließlich im Rahmen von Sperrprozessen (z. B. bei vorzeitiger Verkürzung einer Vertretung im NVZ). Nachrichten werden ausschließlich nach Eintragungen durch autorisierte Personen im NVZ erzeugt und versandt.

Vor Ausstellung eines Notarattributs werden die Gültigkeit des jeweiligen Eintrags sowie dessen Signatur validiert. Maßgeblich sind die im Verzeichnis enthaltenen Informationen. Ist ein Attribut zum Zeitpunkt der Prüfung oder der Produktion nicht mehr gültig, wird dieses nicht ausgestellt.

3.2.1.8 Umgang mit Abweichungen von Identitätsdaten

Der VDA BNotK stellt sicher, dass Unterschiede in der Darstellung oder Kodierung von Identitätsdaten sowie Abweichungen in Namen zwischen verschiedenen Nachweisen oder Datenquellen bewertet und einheitlich behandelt werden.

Hierzu werden definierte Regeln angewendet, insbesondere im Hinblick auf unterschiedliche Zeichensätze, Schreibweisen, Transliterationen sowie fehlende oder abweichende Namensbestandteile.

Maßgeblich ist die im jeweiligen Identifizierungsverfahren festgelegte Quelle (z.B. Ausweisdokumente, vertrauenswürdige Register).

Abweichungen werden unter Berücksichtigung von Plausibilität und Kontext bewertet. Unkritische Abweichungen können akzeptiert werden, sofern die Identität eindeutig feststellbar bleibt.

Nicht plausibel erklärbare oder widersprüchliche Abweichungen führen zur Anforderung zusätzlicher Nachweise oder zum Abbruch des Identifizierungsprozesses.

Die detaillierten Verarbeitungs- und Bewertungsregeln sind in internen Verfahrensanweisungen des VDA BNotK festgelegt.

3.2.1.9 Archivierung von Nachweisen

Der VDA BNotK archiviert alle im Rahmen der Identitätsprüfung erhobenen Nachweise und stellt sicher, dass diese während der gesamten Aufbewahrungsdauer gegen unbefugten Zugriff geschützt sowie in ihrer Integrität, Vertraulichkeit und Verfügbarkeit gesichert sind.

Die archivierten Nachweise umfassen insbesondere Kopien der zur Identitätsprüfung vorgelegten Identitätsdokumente, Validierungsnachweise sowie Vermerke zu den durchgeführten Identifizierungsverfahren (z. B. Beglaubigungsvermerke im Rahmen einer Unterschriftsbeglaubigung).

Für sämtliche Nachweise werden Angaben zur Art der verwendeten Identitätsdokumente sowie zu deren Quelle bzw. Aussteller dokumentiert.

Die Erhebung, Speicherung und Sicherung der Nachweise zur Identitätsprüfung entsprechen den Anforderungen gemäß Abschnitt 8.5.2 der ETSI TS 119 461.

3.2.2 Identifizierung bei Erweiterungen und Beschränkungen im Zertifikat

Ein qualifiziertes Signaturzertifikat für eine natürliche oder juristische Person kann auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie amts- und berufsbezogene oder sonstige Angaben zu seiner Person (Attribute) enthalten.

Hinsichtlich der Angaben über die Vertretungsmacht ist die Einwilligung der dritten Person nachzuweisen; amts- und berufsbezogene oder sonstige Angaben zur Person sind durch die jeweils zuständige Stelle zu bestätigen. Die Ausstellung von qualifizierten Zertifikaten mit entsprechenden Attributen erfolgt nur, wenn die Bestätigung der zuständigen Stelle vorliegt. Zu diesem Zweck erhält der Antragsteller im Anschluss an seinen Zertifikatsantrag einen entsprechenden Vordruck, welchen er seiner zuständigen Stelle vorlegen muss.

3.2.2.1 Aufnahme amts- und berufsbezogener oder sonstiger Angaben

Sofern ein Antragsteller die Aufnahme einer amts- und berufsbezogenen oder einer sonstigen Angabe als Attribut beantragt, muss die zuständige Stelle die Berechtigung zur Führung dieses Attributs bestätigen. Diese sog. bestätigende Stelle weist ihre Berechtigung durch geeignete Nachweise (z. B. Handelsregisterauszug) nach.

Die Attributsbestätigung wird von der bestätigenden Stelle an die RA des VDA BNotK übermittelt. Das Bestätigungsformular wird anschließend zusammen mit den weiteren Antragsunterlagen durch die RA-Mitarbeiter im Rahmen der Antragsprüfung geprüft und dokumentiert.

Für die Aufnahme von Notarattributen gilt eine abweichende Regelung:

Zur Vermeidung von Einzelbestätigungen greift der VDA BNotK auf Grundlage schriftlicher Vereinbarungen mit den regionalen Notarkammern auf das bei der Bundesnotarkammer geführte Notarverzeichnis (NVZ) als vertrauenswürdige Datenquelle zurück.

Es werden vom Antragssystem nur Zertifikatsanträge mit Notarattribut zugelassen, wenn die entsprechende Berechtigung bereits zum Zeitpunkt der Antragstellung im Notarverzeichnis nachgewiesen ist.

Die Aufnahme von amts-, berufsbezogenen oder sonstige Angaben sind für qualifizierte Zertifikate für juristische Personen (Siegelzertifikate) ausgeschlossen.

3.2.2.2 Aufnahme und Prüfung einer Vertretungsmacht

Die Regelungen dieses Abschnitts gelten sowohl für die Vertretung einer natürlichen Person als auch für die Vertretung einer juristischen Person oder Organisation.

Beantragt ein Antragsteller die Aufnahme der Vertretungsmacht für eine dritte Person,

ist dem VDA BNotK die Einwilligung dieser Person durch geeignete Nachweise (z. B. schriftliche Erklärungen oder vergleichbare Dokumente) nachzuweisen.

Bei juristischen Personen hat der Antragsteller seine Vertretungsberechtigung durch geeignete Unterlagen (z. B. Handelsregisterauszug, amtliche Bescheinigung oder vergleichbare Dokumente) nachzuweisen.

Die Prüfung der Vertretungsberechtigung erfolgt auf Grundlage der im Rahmen der Identifizierungsverfahren gemäß Abschnitt 3.2.1 erhobenen und geprüften Nachweise.

Hierzu zählen insbesondere Registerauszüge, behördliche Bescheinigungen oder beglaubigte Dokumente unter Angabe des Registers sowie des Zeitpunkts der Einsichtnahme bzw. Ausstellung.

Der VDA BNotK prüft die Authentizität, Integrität und Aktualität der Nachweise sowie deren Übereinstimmung mit der Identität des Antragstellers.

Die Nachweisführung entspricht den Anforderungen gemäß Abschnitt 9.4 der ETSI TS 119 461.

Die Vertretungsmacht wird nur dann in das qualifizierte Zertifikat aufgenommen, wenn die entsprechende Berechtigung zweifelsfrei festgestellt wurde.

Die Beantragung einer Vertretungsmacht für eine dritte Person ist für qualifizierte Zertifikate für juristische Personen (Siegelzertifikate) ausgeschlossen.

3.2.2.3 Aufnahme eines Pseudonyms

Beantragt der Antragsteller ein Pseudonym und soll eine Vertretungsmacht in das qualifizierte Zertifikat aufgenommen werden, so muss die Bestätigung die Zustimmung zur Aufnahme des Vertretenen zur Aufnahme eines Pseudonyms umfassen. Der Vertretene wird über das Pseudonym benachrichtigt.

Beantragt der Antragsteller ein Pseudonym und die Aufnahme berufsbezogener oder sonstiger Angaben zu seiner Person in das qualifizierte Zertifikat, so muss auch die Zustimmung der für diese Angaben zuständigen Stellen zu dem Pseudonym eingeholt werden.

Die Aufnahme eines Pseudonyms ist für Zertifikate für juristische Personen nicht vorgesehen.

3.2.2.4 Einschränkung der Nutzung

Die Nutzung des qualifizierten Zertifikats kann allgemein oder finanziell eingeschränkt werden.

Die entsprechende Einschränkung wird der bestätigenden Stelle im Rahmen der Bestätigung eines Attributes ebenfalls bekanntgegeben.

Die Aufnahme allgemeiner oder finanzieller Beschränkungen ist für Zertifikate für juristische Personen nicht vorgesehen.

3.3 Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung (re-keying)

Eine Schlüsselerneuerung erfolgt durch die Produktion eines neuen qualifizierten Zertifikats vor Ablauf des bestehenden Zertifikats. Dabei kann auf die bei der erstmaligen Identifizierung bereits geprüften Daten und Nachweise zurückgegriffen werden.

Eine erneute Identitätsprüfung ist nicht erforderlich, sofern die nachfolgenden Voraussetzungen kumulativ erfüllt sind:

- die ursprüngliche Identitätsprüfung wurde gemäß den zum Zeitpunkt der Durchführung geltenden normativen Anforderungen ordnungsgemäß durchgeführt und dokumentiert,
- das ursprünglich eingesetzte Identifizierungsverfahren ist weiterhin normativ zulässig und sicherheitstechnisch freigegeben,
- die beim VDA BNotK gespeicherten Identitätsdaten sowie etwaige bestätigte Attribute sind vollständig, unverändert und zutreffend,
- es liegen keine sicherheitsrelevanten Erkenntnisse, Risikobewertungen oder regulatorischen Änderungen vor, die eine erneute Identitätsprüfung erforderlich machen,
- das zugrunde liegende Vertragsverhältnis besteht unverändert fort.

Der Zertifikatsinhaber (für Signaturzertifikate für natürliche Personen) oder Antragsteller (für Siegelzertifikate für juristische Personen) wird vor Ablauf der Zertifikatsgültigkeit automatisiert über das Verfahren für die Ausstellung eines Folgezertifikats informiert.

Hierbei wird die Identität über den Login mit einer Chipkarte mit Authentisierungszertifikat sowie einer PIN (2FA), sichergestellt.

Vor Ausstellung des neuen Zertifikats wird dem Zertifikatsinhaber bzw. Antragsteller eine Übersicht über seine beim VDA BNotK gespeicherten Identitätsdaten bereitgestellt.

Er wird aufgefordert, die Daten zu überprüfen und innerhalb eines genannten Zeitraums (mindestens vier Wochen) dem VDA BNotK ggf. notwendige Korrekturen mitzuteilen.

Sofern das der ursprünglichen Identitätsprüfung zugrunde liegende amtliche Ausweisdokument zum Zeitpunkt der beabsichtigten Ausstellung des neuen Zertifikats nicht mehr gültig ist, ist vor Ausstellung ein aktuelles gültiges amtliches Ausweisdokument oder ein elektronischer Identitätsnachweis (eID) vorzulegen.

Die Prüfung der Dokumentengültigkeit ist Bestandteil des Re-Keying-Prozesses und wird dokumentiert.

Eine erneute Antragstellung und Identifizierung ist insbesondere erforderlich, wenn:

- sich zertifikatsrelevante Daten oder bestätigte Attribute geändert haben,
- Zweifel an der Richtigkeit, Aktualität oder Integrität der gespeicherten Daten bestehen,
- sich die regulatorischen oder sicherheitsrelevanten Rahmenbedingungen wesentlich geändert haben,
- oder das ursprünglich verwendete Identifizierungsverfahren nicht mehr den geltenden normativen Anforderungen entspricht.

Die Prüfung der Voraussetzungen erfolgt im Rahmen des bestehenden Re-Keying-Prozesses. Sind alle vorgenannten Voraussetzungen erfüllt, wird ein neues qualifiziertes Zertifikat erstellt. Die Ausgabe des neuen qualifizierten Zertifikates erfolgt auf Grundlage des bestehenden Vertragsverhältnisses mit dem Zertifikatsinhaber. Eine Änderung der Allgemeinen Geschäftsbedingungen setzt voraus, dass diese wirksam in den Vertrag einbezogen worden sind. Ein abweichendes Vorgehen kann im Einzelfall vereinbart werden, wenn dies mit den gesetzlichen und sonstigen Vorgaben im Einklang steht.

3.4 Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens

Der VDA BNotK bietet für Zertifikatsinhaber und ihre Vertretungsberechtigten folgende Möglichkeiten des Widerrufs der von ihr ausgegebenen Zertifikate an:

- telefonisch sowie
- schriftlich mit eigenhändiger Unterschrift oder qualifiziert elektronisch signiert

Die Identifizierung und Authentifizierung erfolgt:

- bei einem telefonischen Widerrufsverlangen für qualifizierte Signaturzertifikate durch Angabe des Widerrufskennworts und weitere persönliche Angaben,
- bei einem telefonischen Widerrufsverlangen für qualifizierte Siegelzertifikate durch Angabe des Widerrufskennworts, durch weitere persönliche Angaben sowie durch einen Autorisierungslink, der an die bekannte geschäftliche Kontaktadresse (E-Mail oder EGVP) geschickt wird,
- bei einem schriftlichen Widerrufsverlangen für qualifizierte Signaturzertifikate durch Überprüfung der Unterschrift.
- bei einem schriftlichen Widerrufsverlangen für qualifizierte Siegelzertifikate durch Überprüfung der Unterschrift sowie der rechtsgültigen Vertretungsmacht des Widerrufsberechtigten.

4 Betriebsanforderungen

4.1 Zertifikatsantrag

Der VDA BNotK gibt Signaturzertifikate ausschließlich an Angehörige der in Abschnitt 1.3.3 der in der Zertifikatsrichtlinie (**CP**) des VDA BNotK genannten Berufsgruppen und im Rahmen des

Betriebs des Videokommunikationssystems gemäß § 78p BNotO aus. Ebenfalls vergibt der VDA BNotK Siegelzertifikate ausschließlich an juristische Personen der in Abschnitt 1.3.3 der in der Zertifikatsrichtlinie (CP) des VDA BNotK genannten Gruppe.

Die Eingabe der Antragsdaten erfolgt stets über das Online-Antragssystem des VDA BNotK. Eine ausschließlich schriftliche Antragstellung ist nicht möglich. Die Eingabe erfolgt dabei stets durch den Antragsteller selbst. Die Antragsdaten werden entweder per Webformular oder über eine gesicherte API-Schnittstelle nach Aufruf durch ein autorisiertes Fachverfahren übertragen. Im Zuge der Stellung des Antrags stimmt der Antragsteller der Einbeziehung der Allgemeinen Geschäftsbedingungen des VDA BNotK zu und bestätigt, dass er die Unterrichtungsbrochüre zu qualifizierten Zertifikaten zur Kenntnis genommen hat. Die Zustimmung zu den Allgemeinen Geschäftsbedingungen sowie die Bestätigung, von der Unterrichtungsbrochüre Kenntnis genommen zu haben, ist Voraussetzung für die Antragstellung sowie den Abschluss des Vertrages. Die Allgemeinen Geschäftsbedingungen sind in deutscher Sprache verfasst und werden den Antragstellern zusammen mit der Unterrichtungsbrochüre in elektronischer Form zum Download zur Verfügung gestellt.

Sofern für qualifizierte Siegelzertifikate neben dem Antragsteller weitere zeichnungsberechtigte Personen gesetzt werden sollen, müssen diese vor der offiziellen Antragstellung in der Online-Antragsseite des VDA BNotK vermerkt werden. Vgl. Abschnitt 3.2 zur Übermittlung der zur Identifizierung genutzten Unterlagen an den VDA BNotK.

Der VDA BNotK behält es sich vor, Anträge auf Ausstellung eines Zertifikates abzulehnen.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Nach Stellung des Online-Antrags wird der Antragsteller (Subscriber) im RA-System des VDA BNotK registriert. Die Registrierung umfasst die Erfassung der Identitätsdaten, die eindeutige Zuordnung einer Antragsnummer sowie die revisionssichere Dokumentation der Identifizierungsunterlagen. Die Registrierung des Antragstellers (Subscriber) sowie – sofern abweichend – des Zertifikatsinhabers (Subject) und die Identitätsvalidierung erfolgen gemäß ETSI EN 319 411-1, Abschnitt. 6.2.2.

Die Prüfung der Identifizierungsunterlagen erfolgt – abhängig vom gewählten Identifizierungsverfahren – durch RA-Mitarbeiter im Vier-Augen-Prinzip, sobald sämtliche erforderlichen Identitäts- und gegebenenfalls Attributsnachweise vorliegen.

Der VDA BNotK setzt zur Identifizierung unterschiedliche Identifizierungsverfahren gemäß Abschnitt 3.2 ein. In bestimmten Verfahren (z. B. Notarident oder Gerichtident) erfolgt die Identifizierung durch zuverlässige und sachkundige Dritte im Auftrag des VDA BNotK. Sie unterliegen den Vorgaben des VDA BNotK und den einschlägigen normativen Anforderungen.

Unter bestimmten Voraussetzungen können Anträge vom RA-System automatisiert geprüft werden. Dies gilt u.a. für Zertifikatsanträge, die unter Nutzung des Identifizierungsverfahrens elektronisch gestellt wurden. In diesem Fall erfolgt eine automatische Systemprüfung der Antragsdaten und des elektronischen Identitätsnachweises.

Sofern Antragsteller (Subscriber) und Zertifikatsinhaber (Subject) nicht identisch sind, darf das Zertifikat nur ausgestellt werden, wenn der Antragsteller im Rahmen des Antragsverfahrens der Ausstellung für den Zertifikatsinhaber zugestimmt hat.

Bei qualifizierten Siegelzertifikaten erfolgt die Antragstellung durch eine vertretungsberechtigte natürliche Person, die im Rahmen der Antragstellung ihre Vertretungsberechtigung bestätigt. Die Vertretungsberechtigung des Antragstellers wird vom VDA BNotK im Zuge der Antragsprüfung überprüft.

Nach abgeschlossener Registrierung sowie der vollständigen Identifizierung des Antragstellers und Validierung sämtlicher Antragsdaten und Dokumente im 4-Augen-Prinzip ist der Antragsprüfprozess erfolgreich durchlaufen.

4.2.2 Annahme oder Ablehnung des Antrags

Der VDA BNotK lehnt einen Antrag auf Erstellung eines Zertifikats ab, wenn die Antragsunterlagen nicht oder nicht vollständig vorliegen oder inkorrekt sind oder wenn Identifikationsunterlagen unvollständig, beschädigt bzw. inkorrekt sind. Anträge werden zudem abgelehnt, wenn die Antragsdaten nicht mit Ausweisdokumenten, Attributsbestätigungen oder sonstigen notwendigen Nachweisen (z.B. Organisations- und Vertretungsnachweise) übereinstimmen.

Anträge können zudem aus folgenden Gründen abgelehnt werden:

- keine Bezugsberechtigung des Antragstellers, da dieser nicht Angehöriger einer der in Abschnitt 1.3.3. der Zertifikatsrichtlinie des VDA BNotK aufgeführten Berufsgruppen ist,
- fehlender Organisationsnachweis der juristischen Person,
- fehlende Vertretungsmacht des Antragstellers,
- Keine Autorisierung oder Berechtigung zur Übertragung von Antragsdaten per API,
- Verstreichen von Fristen (in der Regel drei Monate) für den Nachweis von Daten und/oder Unterlagen.

Der VDA BNotK behält sich das Recht vor, Anträge auch aus anderen Gründen abzulehnen.

4.3 Ausstellung von Zertifikaten

4.3.1 Vorgehen der CA bei der Ausstellung des Zertifikats

Die Erstellung des Zertifikats, die Generierung des Schlüssels sowie die Personalisierung der

Chipkarte erfolgt in den Liegenschaften bzw. Räumlichkeiten des VDA BNotK.

Die eigentliche Zertifikatserstellung erfolgt durch die im gesicherten Rechenzentrum des VDA BNotK befindliche BNotK-Signierkomponente.

Ein qualifiziertes Zertifikat wird ausschließlich nach abgeschlossener Registrierung sowie vollständiger Identifizierung und Authentifizierung des Antragstellers ausgestellt.

Nach der Identifizierung des Antragstellers und abschließender Prüfung sowie Bewertung der Richtigkeit und Aktualität sämtlicher Antragsdaten und Dokumente erteilt der zweitprüfende RA-Mitarbeiter die Produktionsfreigabe.

Die Produktion des qualifizierten Zertifikats erfolgt unmittelbar nach Freigabe.

Dies beinhaltet das Anstoßen der Schlüsselgenerierung, die Erzeugung des Zertifikats, sowie das Speichern des Zertifikats auf der remote-QSCD.

Die vollständige Dokumentation zu einem Antrag und dem darin enthaltenen Zertifikat wird gemäß Abschnitt 5.5 revisionssicher abgelegt. Die Antragsdokumente können über die eindeutige Antragsnummer jederzeit dem erstellten Zertifikat zugeordnet werden.

4.3.2 Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats

Der Zertifikatsinhaber wird über die Erstellung seines Zertifikates via E-Mail oder EGVP benachrichtigt.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Der Zertifikatsinhaber ist vor der Verwendung seines Zertifikats verpflichtet, die Zertifikatsinhalte auf Korrektheit zu überprüfen. Bei der Zertifikatsübergabe wird zwischen Authentisierungszertifikaten und qualifizierten Zertifikaten unterschieden.

- [Authentisierungszertifikate](#)

Chipkarten

Grundsätzlich erfolgt die Auslieferung mittels postalischen Versands an die Meldeadresse des Antragstellers bzw. an deren Geschäftsadresse. Vor dem Versand wird die Funktionsfähigkeit der Chipkarte geprüft. Der Antragsteller muss den Empfang der Chipkarte online bestätigen. Nachdem der Antragsteller den Erhalt der Chipkarte bestätigt hat und der PIN-Brief erzeugt wurde, wird die Karte freigeschaltet. Anschließend wird der PIN-Brief mit PIN und PUK an den Antragsteller versandt. Der Versand erfolgt postalisch oder elektronisch mittels EGVP.

Mittels dieser PIN, deren Änderung vor der ersten Nutzung empfohlen wird, kann der Antragsteller die Chipkarte in Betrieb nehmen. Die PIN kann nur erfolgreich geändert werden, wenn

die Chipkarte nicht manipuliert wurde. Die einzelnen Schritte werden dokumentiert.

Software-Authentisierungszertifikate

Die Erstellung der Authentisierungszertifikate erfolgt durch den Nutzer selbst nach vorheriger Anmeldung an einem gesicherten, passwortgeschützten Portal. Das dafür notwendige Passwort kennt nur der (vertretungsberechtigte) Antragsteller selbst. Nach Anmeldung am Portal wird das Softwarezertifikat durch den Nutzer lokal erstellt und mit einer eigens vergebenen PIN verschlüsselt heruntergeladen.

- [Qualifizierte Zertifikate für natürliche und juristische Personen](#)

Fernsignaturzertifikat (Qualifizierte Zertifikate für natürliche Personen)

Der private Schlüssel des Zertifikatsinhabers wird in der sicheren Rechenzentrums Umgebung des VDA BNotK erzeugt und dort zur Signaturerstellung vorgehalten. Die Nutzung des Zertifikats ist nur nach vorheriger Anmeldung mit eindeutig dem Zertifikatsinhaber zugeordneten Authentifizierungsdaten (2-Faktor-Authentifizierung) mittels Chipkarte und PIN möglich.

Fernsiegelzertifikat (Qualifizierte Zertifikate für juristische Personen)

Die Nutzung von Siegelzertifikaten für juristische Personen findet ausschließlich mittels eines Fernsiegel-Verfahrens statt.

Der private Schlüssel des Zertifikatsinhabers wird in der sicheren Rechenzentrums Umgebung des VDA BNotK erzeugt und dort zur Siegelerstellung vorgehalten. Die Nutzung des Schlüssels zur Siegelerstellung ist nur nach vorheriger Anmeldung mit den Authentifizierungsdaten des Siegelersellers (2-Faktor-Authentifizierung) mittels Softwarezertifikat und PIN möglich, die eindeutig dem vertretungsberechtigten Antragsteller oder zeichnungsberechtigten Endanwendern zugeordnet werden.

4.4.2 Veröffentlichung des Zertifikats durch den VDA BNotK

Der VDA BNotK veröffentlicht Zertifikate nicht im öffentlichen Verzeichnisdienst.

Der Abruf ist über die OSCP-Erweiterung `RetrievelfAllowed` jederzeit möglich.

Der Status eines Zertifikats ist nach Produktion über OSCP abrufbar.

4.4.3 Benachrichtigung Dritter über die Erstellung des Zertifikats

Dritte, die Angaben im qualifizierten Zertifikat zur Vertretungsmacht oder amts- und berufsbezogene oder sonstige Angaben bestätigt haben, werden schriftlich über den Inhalt des qualifizierten Zertifikates unterrichtet und auf die Möglichkeit des Widerrufs des qualifizierten Zertifikates hingewiesen (**Widerrufsberechtigte Dritte**). Zu diesem Zweck wird ein Widerrufskennwort festgelegt. Eine gesonderte Benachrichtigung über die Erstellung des qualifizierten

Zertifikats erfolgt nicht.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber oder Zeichnungsberechtigten

- [Qualifizierte Zertifikate für natürliche Personen \(für qualifizierte Signaturen\)](#)

Zertifikatsinhaber dürfen die Zertifikate ausschließlich für berufliche Zwecke verwenden. Es gelten die Bestimmungen aus Abschnitt 1.4.

Die Erzeugung qualifizierter elektronischer Signaturen erfolgt ausschließlich unter Verwendung einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD).

Im Rahmen des Fernsignaturverfahrens wird der private Signaturschlüssel in der gesicherten Rechenzentrumsumgebung des VDA BNotK innerhalb einer QSCD erzeugt und verwaltet. Der private Schlüssel verlässt zu keinem Zeitpunkt die QSCD.

Der VDA BNotK stellt dem Zertifikatsinhaber eine personalisierte Chipkarte mit einem Authentisierungszertifikat zur Verfügung.

Dieses Authentisierungszertifikat ist eindeutig dem jeweiligen Signaturzertifikat zugeordnet.

Die Auslösung einer Fernsignatur ist ausschließlich nach vorheriger erfolgreicher Authentisierung des Zertifikatsinhabers mittels seiner personalisierten Chipkarte und seiner PIN möglich. Eine Signaturerzeugung ohne vorherige Authentisierung und aktive Auslösung durch den Zertifikatsinhaber ist ausgeschlossen.

Die zur Authentisierung verwendeten Daten stellen Aktivierungsdaten im Sinne der eIDAS-Verordnung (EU) Nr. 910/2014 dar.

- [Qualifizierte Zertifikate für juristische Personen \(für qualifizierte Siegel\)](#)

Die Verwendung des Zertifikats ist dem vertretungsberechtigten Antragsteller sowie berechtigten Endanwendern ausschließlich für berufliche Zwecke gestattet.

Die Erzeugung qualifizierter elektronischer Siegel erfolgt ausschließlich unter Verwendung einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD).

Im Rahmen des Fernsiegelverfahrens wird der private Siegelerstellungsschlüssel in der sicheren Rechenzentrumsumgebung des VDA BNotK innerhalb einer QSCD erzeugt und verwaltet. Der private Schlüssel verlässt zu keinem Zeitpunkt die QSCD.

Der VDA BNotK stellt für das Fernsiegelvorgänge ein personalisiertes Software-Authentisierungszertifikat sowie eine dazugehörige PIN zur Verfügung mit denen der vertretungsberechtigte Antragsteller sowie berechtigte Endanwender Siegelvorgänge autorisieren können. Dieses Software-Authentisierungszertifikat ist eindeutig dem jeweiligen Siegelzertifikat zugeordnet.

Eine Automatisierung von Siegelvorgängen im Rechenzentrum ist nur zulässig, sofern diese auf einer zuvor eingerichteten, kontrollierten und dauerhaft wirksamen Authentisierung basiert und ausschließlich im Rahmen der dem Antragsteller zugeordneten Berechtigungen erfolgt.

Die zur Authentisierung verwendeten Daten stellen Aktivierungsdaten im Sinne der eIDAS-Verordnung (EU) Nr. 910/2014 dar.

Die Verantwortung für den Schutz der Software-Authentisierungszertifikate und der zugehörigen PIN obliegt dem vertretungsberechtigten Antragsteller.

Diese sind vor unbefugtem Zugriff zu schützen und ausschließlich zum Auslösen von Siegelvorgängen für berufliche Zwecke zu verwenden.

Sofern der private Signatur- oder Siegelerstellungsschlüssel im Rahmen eines Fernsignatur- oder Fernsiegelverfahrens durch den VDA BNotK im Auftrag des Zertifikatsinhabers bzw. der juristischen Person verwaltet wird, stellt der VDA BNotK durch geeignete technische und organisatorische Maßnahmen sicher, dass die Signatur- oder Siegelerstellung ausschließlich innerhalb einer qualifizierten elektronischen Signaturerstellungseinheit (QSCD) erfolgt.

Der private Schlüssel verbleibt zu jedem Zeitpunkt innerhalb der QSCD und kann ausschließlich nach ordnungsgemäßer Authentisierung und eindeutiger Auslösung durch eine berechtigte Person oder ein entsprechend autorisiertes System verwendet werden.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber

Die Zertifikate können von allen Zertifikatsinhabern verwendet werden. Die Zertifikatsinhaber und Vertrauende Dritte dürfen jedoch nur dann auf den öffentlichen Schlüssel und das Zertifikat vertrauen, wenn folgende Voraussetzungen vorliegen:

- das Zertifikat wird gemäß der zulässigen Nutzungsarten benutzt und eventuelle Einschränkungen im Zertifikat wurden beachtet,
- die Zertifikatskette kann erfolgreich bis zu einem vertrauenswürdigen Root-Zertifikat verifiziert werden, um den Vertrauensstatus zu überprüfen, kann z.B. die EU-Trusted List gemäß eIDAS-Verordnung (EU) Nr. 910/2014 genutzt werden.
- die Gültigkeit des Zertifikats wurde über den Statusabfragedienst (OCSP) bestätigt,
- alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten.

4.6 Zertifikatserneuerung (certificate renewal)

Eine Zertifikatserneuerung wird nicht angeboten.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Die erneute Ausstellung eines Zertifikats mit neuem Schlüsselpaar, basierend auf den Zertifikatsdaten des Ursprungszertifikats, ist nach vorheriger Authentifizierung des Zertifikatsinhabers oder des vertretungsberechtigten Antragstellers gem. Kapitel 3.3 3.3 möglich. Der Zertifikatsinhaber oder der vertretungsberechtigte Antragsteller hat zu bestätigen, dass die bei der Identifizierung (siehe Kapitel 3.23.2) angegebenen Daten weiterhin gültig sind. Für die neuen Zertifikate gelten die zum Zeitpunkt der Erneuerung aktuellen Fassungen von CP und CPS.

4.8 Zertifikatsänderung

Eine nachträgliche Änderung des Zertifikats durch den VDA BNotK ist nicht möglich.

4.9 Widerruf und Suspendierung von Zertifikaten

4.9.1 Bedingungen für einen Widerruf

Der VDA BNotK widerruft in folgenden Fällen qualifizierte Zertifikate für natürliche und juristische Personen:

- Auf Verlangen des Zertifikatsinhabers, eines widerrufsberechtigten Dritten oder der BNetzA,
- wenn das qualifizierte Zertifikat auf Grund falscher Angaben zu den Anhängen I, III und IV der eIDAS-Verordnung (EU 910/2014) ausgestellt wurde,
- bei Beendigung der Tätigkeit als Vertrauensdiensteanbieter und diese nicht von einem anderen qualifizierten Vertrauensdiensteanbieter fortgeführt wird,
- wenn der VDA BNotK darüber in Kenntnis gesetzt wird, dass der private Schlüssel einer nicht autorisierten Person oder Organisation kommuniziert wurde, die dem Zertifikatsnehmer nicht zugehörig ist oder
- wenn Tatsachen die Annahme rechtfertigen, dass (i) das Zertifikat gefälscht oder nicht hinreichend fälschungssicher ist oder (ii) die verwendeten qualifizierten elektronischen Signaturerstellungseinheiten Sicherheitsmängel aufweisen.

Der VDA BNotK widerruft das ausgestellte Zertifikat zudem in folgenden Fällen:

- wenn das Vertragsverhältnis gekündigt wurde,
- der Antrag des Zertifikatsinhabers bzw. des vertretungsberechtigten Antragstellers aufgrund eines Rahmenvertrages erfolgt ist und dieser Vertrag gekündigt oder aus anderen Gründen beendet worden ist,
- die den angewendeten Verfahren zugrunde liegenden Algorithmen gebrochen wurden oder wenn Gründe vorliegen, die annehmen lassen, dass die den angewendeten Verfahren zugrunde

liegenden Algorithmen gebrochen wurden,

- eine Bestätigung, dass die verwendete qualifizierte elektronische Signatur- oder Siegelerstellungseinheit nicht den gesetzlichen Anforderungen entspricht oder nicht mehr gültig ist,
- eine gesetzliche Pflicht zum Widerruf besteht,
- keine Bezugsberechtigung besteht oder später entfallen ist. Eine Pflicht zum Widerruf ist damit nicht verbunden.

Der VDA BNotK ist zudem berechtigt, ein Zertifikat zu widerrufen, wenn ihm bekannt ist, dass das zugrunde liegende Wurzelzertifikat oder das Zertifikat selbst kompromittiert ist oder von der zuständigen Behörde widerrufen wurde.

Zertifikatsinhaber und Vertretungsberechtigte Antragsteller sind zudem verpflichtet, ausgestellte Zertifikate widerrufen zu lassen, wenn

- die Chipkarte bzw. das Zertifikat verloren geht, missbraucht oder möglicherweise kompromittiert wurde,
- das vom VDA BNotK ausgegebenen Zertifikat, welches das Authentisieren gegenüber dem VDA BNotK ermöglicht, verloren, missbraucht oder möglicherweise kompromittiert wurde,
- sich Änderungen an den Zertifikatsdaten ergeben oder wenn in einer Weiterverwendung ein Verstoß gegen Berufs- und/oder Standesrecht oder andere Rechtsvorschriften läge,

Erfährt der VDA BNotK durch einen Dritten, dass die Chipkarte bzw. das Zertifikat eines Zertifikatsinhabers verloren, missbraucht oder möglicherweise kompromittiert wurde, kontaktiert er den Zertifikatsinhaber bzw. den vertretungsberechtigten Antragsteller. Ein automatischer Widerruf des Zertifikats erfolgt nicht.

4.9.2 Widerrufsberechtigte

Zum Widerruf des qualifizierten Zertifikats sind die folgenden Personen berechtigt:

- der VDA BNotK,
- der Zertifikatsinhaber,
- der vertretungsberechtigte Antragsteller
- Widerrufsberechtigte Dritte,
- die BNetzA.

4.9.3 Verfahren zur Stellung eines Widerrufsverlangens

- **Qualifizierte Zertifikate für natürliche Personen (elektronische Signatur)**

Widerrufsverlangen für qualifizierte Zertifikate für natürliche Personen können auf den folgenden Wegen übermittelt werden:

- telefonisch unter den Rufnummern: (0800) 3550 400 bzw. (0800) 3550 100;

Widerrufsberechtigte, die ein Widerrufsverlangen telefonisch stellen wollen, müssen sich durch Nennung des vereinbarten Widerrufskenworts und weitere persönliche Angaben authentifizieren. Stellt ein Zertifikatsinhaber ein telefonisches Widerrufsverlangen ohne sein Widerrufskenwort zu kennen, muss er das Widerrufsverlangen über einen elektronisch versandten Einmallink bestätigen.

- schriftlich; mit eigenhändiger Unterschrift an die folgende Anschrift:
Zertifizierungsstelle der BNotK
Anton-Wilhelm-Amo-Straße 34
10117 Berlin
- mit eigenhändiger Unterschrift oder qualifiziert signiert via E-Mail oder via Kontaktformular an den VDA BNotK.

Ein schriftliches Widerrufsverlangen muss von der widerrufsberechtigten Person eigenhändig unterschrieben oder qualifiziert elektronisch signiert sein. Das zu widerrufende qualifizierte Zertifikat muss anhand der Angaben zu Zertifikat und Zertifikatsinhaber eindeutig bestimmbar sein.

Der Widerruf des qualifizierten Zertifikats wird mittels eines automatisch erzeugten Widerrufsprotokolls dokumentiert.

Der Zertifikatsinhaber und gegebenenfalls der Antragsteller werden, soweit möglich, über den Widerruf des Zertifikats informiert.

Wurden zusätzlich beantragte Attribute durch eine bestätigende Stelle bestätigt, wird diese Stelle ebenfalls über den Widerruf informiert.

Die Benachrichtigung erfolgt über die im Rahmen der Antragstellung hinterlegten Kontaktdaten.

- **Qualifizierte Zertifikate für juristische Personen (für qualifizierte Siegel)**

Widerrufsverlangen für qualifizierte Zertifikate für juristische Personen können auf den folgenden Wegen übermittelt werden:

- telefonisch unter den Rufnummern: (0800) 3550 400 bzw. (0800) 3550 100;

Widerrufsberechtigte, die ein Widerrufsverlangen telefonisch stellen wollen, müssen sich durch Nennung des vereinbarten Widerrufskenworts sowie durch weitere persönliche Angaben authentifizieren.

Nach der korrekten Angabe von Widerrufskenwort und der persönlichen Daten wird zudem ein Einmallink zur Bestätigung des Widerrufsverlangens an die beim VDA BNotK hinterlegte geschäftliche Kontaktadresse (E-Mail oder EGVP-Postfach) geschickt.

- schriftlich; mit eigenhändiger Unterschrift an die folgende Anschrift:
Zertifizierungsstelle der BNotK, Anton-Wilhelm-Amo-Straße 34, 10117 Berlin,
- qualifiziert signiert via E-Mail oder via Kontaktformular an den VDA BNotK.

Ein schriftliches Widerrufsverlangen muss von der widerrufsberechtigten Person entweder eigenhändig unterschrieben oder qualifiziert elektronisch signiert sein. Das zu widerrufende qualifizierte Zertifikat muss anhand der Angaben zu Zertifikat und Zertifikatsinhaber eindeutig bestimmbar sein. Darüber hinaus muss die widerrufsberechtigte Person eine rechtsgültige Vertretungsmacht der juristischen Person nachweisen.

Dieser Nachweis kann in Form eines amtlichen Handelsregistrauszugs (nicht älter als 4 Wochen) oder einer gültigen Vertretungsvollmacht erbracht werden.

Der Widerruf eines Zertifikates kann nicht rückgängig gemacht werden.

4.9.4 Fristen für ein Widerrufsverlangen

Zertifikatsinhaber haben Zertifikate unverzüglich widerrufen zu lassen, wenn Gründe für einen Widerruf vorliegen. Sofern der Zertifikatsinhaber eine juristische Person ist (im Falle von qualifizierten Siegelzertifikaten) ist der Widerruf durch den vertretungsberechtigten Antragsteller durchzuführen.

4.9.5 Zeitspanne für die Bearbeitung von Widerrufsverlangen

Widerrufsverlangen können telefonisch über eine speziell für diesen Zweck eingerichtete Telefonnummer (Sperrhotline) gestellt werden.

Die Sperrhotline ist 24 Stunden täglich an sieben Tagen in der Woche erreichbar.

Schriftliche Widerrufsverlangen können jederzeit postalisch, per E-Mail oder über das Kontaktformular auf der Webseite der Zertifizierungsstelle eingereicht werden.

Der Widerruf des Zertifikats erfolgt unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Eingang eines wirksamen Widerrufsverlangens.

Ein Widerrufsverlangen gilt als wirksam, wenn es von einer widerrufsberechtigten Person gestellt und gemäß Abschnitt 4.9.3 authentifiziert bzw. formwirksam übermittelt wurde.

Für dringende Widerrufe steht die Sperrhotline jederzeit als erreichbarer Kommunikationskanal zur Verfügung.

Kann die Bearbeitung von Widerrufsverlangen ausnahmsweise nicht innerhalb von 24 Stunden umgesetzt werden, wird ein geregeltes Notfallverfahren angewendet. Dieses stellt sicher, dass Widerrufsverlangen priorisiert bearbeitet, die Ursache der Verzögerung unverzüglich analysiert

und geeignete Maßnahmen zur schnellstmöglichen Umsetzung des Widerrufsverlangens ergriffen werden. Entsprechende Vorfälle sowie die ergriffenen Maßnahmen werden dokumentiert.

Der Widerruf erfolgt unverzüglich nach Wiederherstellung der ordnungsgemäßen Betriebsfähigkeit oder im Rahmen des Notbetriebs.

Das Notfallverfahren ist Bestandteil des internen Sicherheits- und Notfallkonzepts.

4.9.6 Methoden zum Prüfen von Widerrufsinformationen

Widerrufsinformationen können über den OCSP-Responder abgefragt werden.

Die OCSP-Responder-Adresse ist im jeweiligen Zertifikat im Authority Information Access (AIA)-Feld enthalten (siehe Kapitel 7.1.).

4.9.7 Häufigkeit der Veröffentlichung von Widerrufslisten

Es werden keine Widerrufslisten für Zertifikate zur Verfügung gestellt.

4.9.8 Maximale Latenzzeit für Widerrufslisten

Es werden keine Widerrufslisten für Zertifikate zur Verfügung gestellt.

4.9.9 Online-Verfügbarkeit von Widerrufsinformationen

Widerrufsinformationen können über den OCSP-Responder abgefragt werden.

Der OCSP-Dienst ist öffentlich zugänglich und ohne vorherige Authentisierung nutzbar.

Die OCSP-Responder-Adresse ist im jeweiligen Zertifikat im Authority Information Access (AIA)-Feld enthalten (siehe Kapitel 7.1.).

Widerrufsinformationen werden unverzüglich nach Wirksamwerden eines Widerrufs spätestens jedoch innerhalb von 60 Minuten im OCSP-Dienst veröffentlicht.

Der VDA BNotK stellt sicher, dass die geänderte Zertifikatsstatusinformation innerhalb der genannten Frist über die vorgesehenen Statusdienste allen vertrauenden Dritten zur Verfügung steht.

4.9.10 Notwendigkeit zur Online-Prüfung von Widerrufsinformationen

Einzelheiten zur Verpflichtung vertrauender Dritter zur Prüfung von Widerrufsinformationen sind in der Zertifikatsrichtlinie (CP) geregelt.

4.9.11 Andere Formen zur Anzeige von Widerrufsinformationen

Keine.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Im Falle einer Kompromittierung des privaten Schlüssels ist das Zertifikat unverzüglich gemäß Abschnitt 4.9.1 zu widerrufen

4.9.13 Suspendierung des Zertifikats

Eine vorübergehende Aussetzung (Suspension) von Zertifikaten wird nicht angeboten. Ein einmal widerrufenes Zertifikat bleibt dauerhaft widerrufen und kann nicht reaktiviert werden.

4.10 Statusabfragedienst

Statusabfragen erfolgen über einen OCSP-Responder.

Der OCSP-Dienst ist öffentlich zugänglich und ohne vorherige Authentisierung nutzbar.

Die OCSP-Responder-Adresse ist im jeweiligen Zertifikat im Authority Information Access (AIA)-Feld enthalten (siehe Kapitel 7.1.).

Der Dienst ist grundsätzlich 24 Stunden an sieben Tagen die Woche verfügbar.

Der Status von Zertifikaten bleibt mindestens mit dem während der Gültigkeitsdauer angebotenen Verfahren (OCSP) auch über das Ende der Zertifikatsgültigkeit hinaus abrufbar.

Die Integrität und Authentizität der Statusinformationen werden geschützt.

4.11 Beendigung des Zertifizierungsdienstes

Die Verträge können vom VDA BNotK und dem Zertifikatsinhaber gemäß der zwischen Ihnen geschlossenen vertraglichen Vereinbarungen gekündigt werden.

4.12 Schlüsselhinterlegung und –wiederherstellung

Ein Hinterlegen von Schlüsseln ist nicht möglich.

5 Nicht-technische Sicherheitsmaßnahmen

5.1 Risikomanagement

Das Risikomanagement des VDA BNotK erfolgt gemäß der „Leitlinie Risikomanagement (RL 0103)“. Die dort beschriebenen Prozesse zur Risikoidentifikation, -analyse, -bewertung und -behandlung bilden die Grundlage für die in diesem CPS beschriebenen Sicherheitsanforderungen und operativen Maßnahmen.

Die Risikobewertung wird mindestens jährlich sowie anlassbezogen bei wesentlichen Änderungen, Sicherheitsvorfällen oder veränderten Bedrohungslagen überprüft und fortgeschrieben.

5.2 Bauliche Sicherheitsmaßnahmen Risikomanagement

Alle sensiblen Daten und die für den Betrieb des VDA BNotK relevanten Systeme sind in physikalisch geschützten Sicherheitsbereichen untergebracht. Die Schutzklasse entspricht den Anforderungen an den Betrieb zur Ausstellung qualifizierter Zertifikate. Durch Zutrittskontrollmechanismen wird sichergestellt, dass keine unberechtigten Personen Zugang zu den Sicherheitsbereichen haben. Alle Zutritte, auch unerlaubte Zutrittsversuche, werden protokolliert. Versuche zur Überwindung der Sicherheitsmechanismen wie Einbruch, Diebstahl und Vandalismus lösen einen Alarm aus. Innerhalb des Sicherheitsbereichs gibt es einen zusätzlichen physikalischen Schutz der IT-Systeme und Schlüssel des VDA-BNotK. Der Zugriff auf die Systeme ist nur im Vier-Augen-Prinzip möglich. Diese Maßnahme und die zusätzliche Videoüberwachung bieten einen zusätzlichen Schutz vor Manipulation und Diebstahl. Die Komponenten des VDA BNotK sind getrennt von sonstigen Diensten der BNotK. Die Sicherheitsmaßnahmen und das zugrundeliegende Sicherheitskonzept werden regelmäßig durch eine anerkannte Prüf- und Bestätigungsstelle überprüft.

Das Rechenzentrum ist zusätzlich nach „Trusted Site Infrastructure Level 3 Erweitert“ durch die TÜV Informationstechnik GmbH geprüft und zertifiziert worden.

Die Prüfung umfasst folgende Bewertungsaspekte:

- Umfeld
- Baukonstruktion
- Brandschutz, Melde- und Löschtechnik
- Energieversorgung
- Raumluftechnische Anlagen
- Organisation
- Dokumentation

Die Zertifizierung nach Level 3 „Erweitert“ entspricht einem hohen Schutzbedarf, d.h. alle kritischen Versorgungssysteme (insbesondere die externe Netzwerkanbindung) sind vollständig redundant ausgelegt. Die Prüfung wird in regelmäßigen Abständen wiederholt.

5.3 Verfahrensvorschriften

5.3.1 Rollenkonzept

Das implementierte und im Sicherheitskonzept dokumentierte Rollenkonzept sieht eine Aufteilung in operative, beratende, administrative und führende Rollen vor. Die definierten Rollen umfassen unter anderem die Rolle des IT-Sicherheitsbeauftragten, der auch für die interne Revision zuständig ist, die Rolle als Syslog-Operator, als DB-Administrator, als CA-Administrator und als Netzwerkadministrator sowie die Rolle des RA-Mitarbeiters und des Sperrdienstmitarbeiters. Für die entsprechenden Rollen bestehende Stellenbeschreibungen definieren die Aufgaben sowie notwendigen Qualifikationen und Erfahrungen. Personen, die in führende Rollen berufen werden sowie im Bereich der Zertifizierungs- und Sperrdienste tätig sind, müssen frei von kommerziellen, finanziellen oder anderen Einflüssen sein, die geeignet sind das Vertrauen in den VDA BNotK erheblich zu beeinträchtigen. Alle Mitarbeiter erhalten durch einen definierten Prozess die Rollen, die zum Ausüben der Tätigkeit notwendig sind. Ein Rollenausschlussprinzip garantiert, dass keine einzelne Person sicherheitsrelevante Änderungen vornehmen oder unberechtigt Zertifikate ausstellen, löschen oder widerrufen kann. Der Entzug einer Rolle folgt ebenfalls einem definierten Prozess und wird dokumentiert.

5.3.2 Vier-Augen-Prinzip

Sicherheitskritische Vorgänge müssen grundsätzlich im Vier-Augen-Prinzip erfolgen. Dies wird durch technische und organisatorische Maßnahmen umgesetzt. Neben der Prüfung der Zertifikatsanträge in der RA werden sämtliche Handlungen von der Schlüsselaktivierung bis zum -backup im Vier-Augen-Prinzip durchgeführt.

Änderungen an den Sicherheitsmechanismen und IT-Systemen erfolgen nach einem festgelegten Prozess, werden dokumentiert und können nur im Vier-Augen-Prinzip durchgeführt werden. Das Vier-Augen-Prinzip wird technisch erzwungen und kann nicht umgangen werden. Dies gilt auch für die Wiederherstellung von Daten.

5.3.3 Sonstige Dienstanweisung

Den Mitarbeitern des VDA BNotK ist es nicht erlaubt, Unterlagen, Medien (mit der Ausnahme von Laptops) und Software, die sensible Daten enthalten, aus dem Sicherheitsbereich des VDA BNotK zu entfernen.

5.4 Personalkonzept

5.4.1 Qualifikation, Erfahrung und Zuverlässigkeit des Personals

Der VDA BNotK stellt ausschließlich zuverlässiges, qualifiziertes Personal ein.

Vor Aufnahme der Tätigkeit im sicherheitskritischen Bereich des VDA BNotK wird die Fachkunde geprüft und eine Schulung durchgeführt. Dies gilt auch für alle leitenden Rollen des VDA BNotK. Schulungsmaßnahmen werden dokumentiert. Der VDA BNotK stellt sicher, dass keine Interessenkonflikte bestehen. Mitarbeiter des VDA BNotK haben bei Interessenkonflikten ein Tätigwerden abzulehnen. Ihnen drohen in diesem Fall keine arbeitsrechtlichen Konsequenzen.

5.4.2 Sicherheitsüberprüfung

Alle für Zertifizierungsdienste eingesetzten Mitarbeiter des VDA BNotK müssen in regelmäßigen Abständen, mindestens alle zwei Jahre, ein polizeiliches Führungszeugnis vorlegen. Für leitende Rollen ist zusätzlich ein Führungszeugnis bei der Aufsichtsbehörde hinterlegt.

5.4.3 Schulungen und Weiterbildungen

Alle Mitarbeiter werden vor der Aufnahme ihrer Tätigkeit und bei Bedarf geschult. Nachschulungen der Mitarbeiter finden im Regelfall jährlich statt. Nachschulungen werden zudem dann durchgeführt, wenn Änderungen an den Prozessen, der Technik sowie den Rahmenbedingungen für den Betrieb des Vertrauensdienstes erfolgen oder wenn diese zur Vermittlung oder Aufrechterhaltung der notwendigen Fachkunde eines Mitarbeiters erforderlich sind.

5.4.4 Rollenbesetzung, Rollenentzug und Rollenwechsel

Rollenbesetzungen, Rollenentzug und Rollenwechsel erfolgen nach festgelegten internen Verfahren und werden dokumentiert und die entsprechenden Protokolle von Berufendem und Berufenem unterzeichnet.

Der Leiter des VDA BNotK wird vom Präsidenten der Bundesnotarkammer berufen und abberufen. Sonstige Personen, die leitende oder kontrollierende Rollen beim VDA BNotK übernehmen, z.B. der stellvertretende Leiter des VDA BNotK sowie der Sicherheitsbeauftragte des VDA BNotK, werden vom Leiter des VDA BNotK berufen und abberufen. Eine Berufung erfolgt erst, wenn die erforderliche Sicherheitsüberprüfung und die erforderlichen Schulungen durchgeführt worden sind. Durch das implementierte Rollenkonzept und die Rollenausschlusskriterien wird gewährleistet, dass jede für den VDA BNotK tätige Person nur die Zugänge und Zugriffsrechte erhält, die zum Ausüben seiner Rolle notwendig sind. Die Berufung wird dokumentiert, der Berufene erklärt sein Einverständnis mit der Rolle durch Gegenzeichnen des entsprechenden Protokolls.

Teil der Berufung und des Abberufens ist auch das Anlegen bzw. Entziehen von Zugangs-, und Zutrittsberechtigungen zu technischen Systemen und geschützten Bereichen. Zugangs- und Zutrittsberechtigungen werden nur insoweit erteilt, als dies für die entsprechende Rolle erforderlich ist.

5.4.5 Anforderungen an externes Personal

Externes Personal, welches temporär im Sicherheitsbereich arbeitet, wird stets von berechtigten Mitarbeitern begleitet und beaufsichtigt. Für dauerhaft eingesetztes Personal von anderen Firmen gelten die gleichen Regelungen wie für internes Personal.

5.4.6 Sanktionen bei unerlaubten Handlungen

Der VDA BNotK hat Maßnahmen implementiert (z.B. die Durchführung eines internen Revisionsverfahrens), um die Einhaltung der aufgestellten Regeln und Verfahren zum ordnungsgemäßen und sicheren Betrieb des Zertifizierungsdienstes zu kontrollieren. Festgestellte Verstöße werden behoben. Unerlaubte Handlungen können zudem arbeitsrechtliche und strafrechtliche Konsequenzen haben.

5.4.7 Dokumentation

Folgende Dokumentation wird dem Personal zur Verfügung gestellt:

- das Sicherheitskonzept (die zur Ausübung der Rolle relevanten Teile),
- das Rollenkonzept,
- Zertifikatsrichtlinie und Zertifizierungskonzept,
- die Prozessdokumentationen für die Tätigkeit in der RA,
- die Sicherheitsleitlinie des Unternehmens.

5.5 Protokollierung von Überwachungsmaßnahmen

5.5.1 Überwachung des Zutritts

Alle Zutritte zu den Sicherheitsbereichen des VDA BNotK sowie das Verlassen werden protokolliert und eine angemessene Zeit lang gespeichert (vergleiche Abschnitt 5.1). Zutritte von Besuchern werden ebenfalls protokolliert und sind bei Besuchen des Rechenzentrums mindestens 24 Stunden vorher anzumelden. Besucher werden grundsätzlich von zutrittsberechtigten Mitarbeitern begleitet. Im Bereich des Rechenzentrums werden auch Videoaufzeichnungen gespeichert.

5.5.2 Überwachung von organisatorischen Maßnahmen

Die organisatorischen Maßnahmen werden regelmäßig durch die leitenden Rollen der Zertifizierungsstelle überprüft. Änderungen von organisatorischen Maßnahmen werden angemessen im Sicherheitskonzept dokumentiert.

5.6 Archivierung von Unterlagen

5.6.1 Arten von Unterlagen

Archiviert werden alle gesetzlich geforderten Unterlagen zur vollständigen Dokumentation des Lebenszyklus der CA und der ausgegebenen qualifizierten Zertifikate und Schlüssel in Form von elektronischen Protokolldaten oder papiergebunden. Das betrifft für den Lebenszyklus von qualifizierten Zertifikaten insbesondere die bei der Registrierung anfallenden Dokumente (vergleiche Abschnitt 3.2) sowie die Belege zu Ausstellung, Akzeptanz, Veröffentlichung und Widerruf.

Der Lebenszyklus der CA und deren Systeme und Schlüssel wird vollumfänglich dokumentiert. Das betrifft u.a. Arbeiten am remote-QSCD sowie die Ausstellung, Zerstörung und das Backup der Schlüssel.

Zusätzlich werden Sicherheitskonzepte, Rollenbesetzungslisten, Schulungsunterlagen und Verfahrensanweisungen sowie sonstige für den Betrieb relevante Dokumente (z.B. die Zertifizierungen, Verträge mit Dienstleistern, Dokumente zur Lieferung und Lagerung der Rohlinge sowie deren Entnahme zur Produktion, die Ergebnisse der internen Revision, die Ergebnisse der Schwachstellen- und der Penetrationstests) archiviert.

5.6.2 Aufbewahrungszeiten

Die Aufbewahrungszeit der Dokumentationen entspricht den gesetzlichen Anforderungen für qualifizierte Zertifikate. Die vom VDA BNotK ausgestellten qualifizierten Zertifikate werden auch über den Zeitraum ihrer Gültigkeit hinaus zusammen mit den dazugehörigen Aufzeichnungen sowie Widerrufsinformationen nach Artikel 24 Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 für die gesamte Zeit des Betriebs des VDA BNotK aufbewahrt.

5.6.3 Archivsicherheit

Das elektronische Archiv entspricht dem Stand der Technik und garantiert eine beweiswerterhaltende Langzeitarchivierung nach TR-ESOR. Die papiergebundene Dokumentation wird in einem speziell geschützten Bereich des VDA BNotK gelagert. Zugang zu den Dokumenten haben nur berechnete Mitarbeiter. Die Integrität des elektronischen Archivs wird durch das Anbringen von Signaturen gewährleistet. Zudem besteht ein Back-Up zur Vermeidung von Datenverlust. Zur Langzeitarchivierung wird darüber hinaus die Evidence Record Syntax implementiert. Zur Absicherung der gebildeten Hashbäume werden qualifizierte Zeitstempel verwendet. Zugriff auf die Daten haben ausschließlich berechnete Mitarbeiter des VDA BNotK. Anträge auf Einsicht in die Dokumentation werden von der RA bearbeitet.

Zu diesem Zweck muss der Zertifikatsinhaber den VDA BNotK kontaktieren. Vom RA-Mitarbeiter werden dem Zertifikatsinhaber Kopien seiner Unterlagen zur Einsicht vorgelegt.

5.6.4 Datensicherung des Archivs

Die Sicherung der Daten erfolgt nach dem Stand der Technik.

5.6.5 Anforderungen an die Zeitstempel der archivierten Protokolle

Die Systemzeit der für die Archivierung zuständigen Systeme wird fortlaufend mit der gemäß des Einheiten- und Zeitgesetzes gesetzlich gültigen Zeit abgeglichen.

5.6.6 Ort der Archivierung

Die Archivierung findet ausschließlich bei der Bundesnotarkammer statt.

5.7 Umstellung des Schlüssels (key changeover)

Bei Bedarf und in angemessener Zeit vor Ablauf der Gültigkeit der bestehenden Zertifikate werden neue Schlüssel generiert und die dazu passenden Zertifikate veröffentlicht. Dies gilt sowohl für Endanwender- als auch für CA- und Dienstzertifikate.

5.8 Notfallkonzept

5.8.1 Behandlung von Vorfällen

Die Behandlung von sicherheitsrelevanten Vorfällen und Kompromittierungen ist im Sicherheitskonzept dokumentiert. Verantwortlich für die Umsetzung sind die leitenden Rollen.

5.8.2 Behandlung von Verfügbarkeitsstörungen

Der VDA BNotK überwacht die Verfügbarkeit der vertrauensdienstrelevanten Systeme und Dienste. Festgestellte Störungen werden erfasst, dokumentiert sowie gemäß ihrer Geschäftsauswirkung mit einem Schweregrad gekennzeichnet und priorisiert.

Meldungen zu sicherheitsrelevanten Ereignissen werden an die zuständige Stelle (Cybersecurity) übermittelt und nach festgelegten Prozessen ausgewertet. Die Behandlung von Störungsmeldungen erfolgt im Rahmen des Prozesses Incident Management.

Im Falle von Ausfällen werden alle angemessenen technischen und organisatorischen Maßnahmen ergriffen, um den ordnungsgemäßen Betrieb schnellstmöglich wiederherzustellen.

5.8.3 Wiederherstellung von IT-Systemen

Die IT-Systeme des VDA BNotK werden täglich gesichert und remote, an einer externen Stelle gespeichert. Die Wiederherstellung der Systeme ist Bestandteil der geübten und dokumentierten IT-Prozesse und wird von den Personen mit den entsprechenden Rollen laut Rollenkonzept ausgeführt.

Der VDA BNotK testet in geplanten Intervallen die Wiederherstellung von Backup-Kopien sowie die Wirksamkeit redundanter Systeme. Die Tests erfolgen mindestens jährlich auf Grundlage des BCM-Testplans. Die Ergebnisse werden dokumentiert und etwaige Abweichungen oder Feststellungen führen zu definierten Korrekturmaßnahmen.

5.8.4 Wiederherstellung nach Kompromittierung von privaten CA-Schlüsseln

Bei einer Kompromittierung von privaten CA-Schlüsseln werden die betroffenen CA- und Dienstzertifikate widerrufen und die Aufsichtsbehörde informiert. Je nach Art der Kompromittierung werden auf Basis des Notfallplans des VDA BNotK in Absprache mit der Aufsichtsbehörde ggf. auch die aus der CA generierten Endanwenderzertifikate widerrufen. Betroffene Zertifikatsinhaber und vertretungsberechtigte Antragsteller werden über den Vorfall und dessen Auswirkungen informiert.

Die Widerrufinformationen können grundsätzlich über den OCSP-Responder abgefragt werden bzw. bei einer Kompromittierung des Zertifikats des OCSP-Responders über die von der BNetzA herausgegebene Trusted List.

Nach der Umsetzung von geeigneten Maßnahmen, um zukünftige Kompromittierungen zu verhindern, werden neue CA-Schlüssel nach den entsprechenden Vorgaben erstellt, veröffentlicht und dann nach einem dokumentierten Prozess mit dem Ausstellen von neuen Endanwenderzertifikaten begonnen. Gleiches gilt für Dienstzertifikate. Der gleiche Prozess erfolgt beim ungültig werden der verwendeten Algorithmen oder dem Auslaufen sowie dem Widerruf einer Bestätigung der QSCD und betrifft auch die Endanwenderzertifikaten bzw. deren Schlüssel.

5.8.5 Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall

Die verantwortlichen Personen laut Rollenkonzept entscheiden je nach Art der Katastrophe darüber wie der Betrieb wieder aufgenommen werden soll. Die Wiederaufnahme des Betriebs soll nach 10 Werktagen erfolgen, vorausgesetzt, dass die Ursache der Kompromittierung oder des Katastrophenfalls behoben worden sind. Die Betriebsaufnahme kann entweder durch Neuinstallation oder Wiederherstellung nach dokumentiertem Verfahren oder einer Kombination aus beiden Verfahren erreicht werden. Bei Bedarf auch an einem alternativen Standort. Zuvor wird jedoch sichergestellt, dass geeignete Maßnahmen ergriffen werden, um die Ursachen des Ausfalls oder der Kompromittierung zukünftig auszuschließen.

5.9 Beendigung des Zertifizierungsbetriebs

Der VDA BNotK verfügt über einen fortlaufend aktualisierten Beendigungsplan, in dem Einzelheiten für den Fall der Einstellung der Tätigkeit niedergelegt sind. Ziel ist es, die Dienstleistungskontinuität und eine geordnete Abwicklung sicherzustellen.

Der VDA BNotK benachrichtigt Zertifikatsinhaber, Antragsteller und Dritte, einschließlich Vertrauender Dritter und der zuständigen Aufsichtsbehörde, rechtzeitig, mindestens aber zwei Monate vorher, über die Einstellung des Zertifizierungsdienstes. Zudem werden bei Einstellung der Tätigkeit alle weiteren, die Erbringung von Vertrauensdiensten durch den VDA BNotK betreffenden Vertragsverhältnisse mit Dritten beendet.

Der VDA BNotK versucht eine Übernahme aller qualifizierten Zertifikate (einschließlich der öffentlichen Schlüssel) durch einen anderen qualifizierten Vertrauensdiensteanbieter zu erreichen, kann dies aber nicht gewährleisten. Der VDA übergibt ferner – soweit zulässig – seine vollständige Dokumentation an den übernehmenden Vertrauensdiensteanbieter. Übergeben werden zumindest sämtliche Aufzeichnungen nach Artikel 24 Absatz 2 lit. h) der eIDAS-Verordnung (EU 910/2014) sowie insbesondere sämtliche Angaben und Unterlagen über die einzelnen Zertifikatsinhaber zur Registrierung,

Protokollierung sämtlicher Events des Zertifikatslebenszyklus und die Quelldaten des OCSP-Responders als Datenbankauszug. Die Beauskunftung der qualifizierten Zertifikate erfolgt durch den übernehmenden Vertrauensdiensteanbieter oder durch die BNetzA auf Basis von Export und Überführung des Zertifikatsstatus aller Zertifikate unabhängig von deren Status.

Wenn eine Übernahme der qualifizierten Zertifikate durch einen anderen qualifizierten Vertrauensdiensteanbieter nicht möglich ist, widerruft der VDA BNotK alle noch gültigen qualifizierten Zertifikate. Die ausgegebenen qualifizierten Zertifikate werden in diesem Fall in die von der BNetzA geschaffene Vertrauensinfrastruktur überführt. Die öffentlichen Schlüssel von Wurzel- und CA-Zertifikat werden an den die Zertifikate übernehmenden qualifizierten VDA oder die BNetzA übergeben und durch den VDA oder die BNetzA für einen angemessenen Zeitraum weiter öffentlich verfügbar gehalten. Die privaten Schlüssel betroffener CAs sowie vorhandene Backups werden zerstört.

Die Bundesnotarkammer hat zugesagt, die Kosten für die Übernahme der vom VDA BNotK als qualifiziertem Vertrauensdiensteanbieter ausgestellten qualifizierten Zertifikate durch einen anderen qualifizierten Vertrauensdiensteanbieter oder deren Übertragung in die Vertrauensinfrastruktur der zuständigen Aufsichtsbehörde sowie die Kosten der Benachrichtigung der Zertifikatsinhaber, der Aufsichtsbehörde und weiterer Dritter zu tragen.

6 Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

CA-Schlüssel, OCSP-Schlüssel und Schlüssel für qualifizierte Endanwenderzertifikate werden grundsätzlich in einer sicheren Umgebung auf einer zugelassenen remote-QSCD, die gemäß den Common-Criteria-Vorgaben evaluiert wurde und auf der EU-Liste der vertrauenswürdigen zertifizierten Komponenten steht, generiert (siehe Abschnitt 5.1).

Die Schlüssel der Endanwenderzertifikate für Fernsignaturen werden auf einem zertifizierten remote- QSCD, dem HSM, erzeugt und gespeichert. Dies gilt sowohl für qualifizierte Signatur-zertifikate für natürliche Personen als auch für qualifizierte Siegelzertifikate für juristische Personen.

Rechtzeitig vor Ablauf der Zertifikatsgültigkeit werden neue Schlüsselpaare und Zertifikate generiert, um einen reibungslosen Übergang zu gewährleisten. Der Prozess zur Erstellung von CA-Schlüsseln, die Key Ceremony, erfolgt nach festgelegten Verfahren. In Abhängigkeit der CA erfolgt die Key-Ceremony durch dafür vorgesehene Trusted Roles im Beisein des Informations-sicherheitsbeauftragten und falls erforderlich unter Aufsicht eines unabhängigen Dritten.

Die Tätigkeiten während der Key Ceremony werden geprüft und protokolliert. Gleiches gilt für die Erstellung von Dienstzertifikaten. Das Rollenkonzept des VDA BNotK sowie das Vier-Augen-Prinzip finden auf die Schlüsselerzeugung Anwendung. Entsprechend der bisherigen Praxis des VDA BNotK wird die Anzahl der Mitarbeiter des VDA BNotK, die zur Schlüsselerzeugung berechtigt sind, so gering wie möglich gehalten. Ein unabhängiger Auditor begleitet die Schlüsselerzeugung.

6.1.2 Auslieferung der privaten Schlüssel für Zertifikatsteilnehmer

Die privaten Schlüssel qualifizierter Zertifikate für natürliche und juristische Personen werden ausschließlich in einem HSM (remote-QSCD) erzeugt und gespeichert und nicht an die Zertifikatsinhaber ausgeliefert.

6.1.3 Auslieferung der öffentlichen Schlüssel an die CA

Der öffentliche Schlüssel wird im Rahmen der Zertifikaterstellung verschlüsselt an die CA übertragen.

6.1.4 Auslieferung der öffentlichen CA-Schlüssel

Die öffentlichen Schlüssel der CA sind für PKI-Teilnehmer in den Veröffentlichungen des VDA BNotK abrufbar. Die CA- und Dienstzertifikate können aus dem öffentlichen Verzeichnis bezogen werden.

6.1.5 Schlüssellängen

Für die Schlüssellänge gelten die Empfehlungen der SOG-IS Crypto Working Group. Zurzeit werden für die Endanwenderzertifikate für natürliche Personen entweder RSA-Schlüssel mit einer Länge von mindestens 3072 Bit oder ECDSA-Schlüssel mit einer Länge von mindestens 384 Bit verwendet. Für juristische Personen werden für die Endanwenderzertifikate ECDSA-Schlüssel mit einer Länge von mindestens 384 Bit verwendet.

Die CA-Schlüssel- und Dienstzertifikate haben eine Länge von 4096 bit für RSA und 521 bit für ECDSA (secp521r1).

6.1.6 Schlüsselparameter und Qualitätskontrolle der Parameter

Die Schlüsselparameter und die eingesetzten QSCDs 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.

6.1.7 Schlüsselverwendung

Die CA-Schlüssel werden ausschließlich zum Signieren von Endanwenderzertifikaten verwendet, die OCSP-Schlüssel (Dienstzertifikate) zum Signieren der OCSP-Anfragen. Die CA- und OCSP-Schlüssel werden in einer sicheren Umgebung eingesetzt (vergleiche Abschnitt 5.1).

- Qualifizierte Zertifikate für natürliche Personen (für qualifizierte Signaturen)

Die Schlüsselverwendung für Endanwenderzertifikate ist Teil des X.509 Zertifikats und darf ausschließlich für qualifizierte Signaturen erfolgen.

- Qualifizierte Zertifikate für juristische Personen (für qualifizierte Siegel)

Die Schlüsselverwendung für Endanwenderzertifikate darf ausschließlich für qualifizierte Siegel erfolgen.

6.2 Sicherung des privaten Schlüssels und kryptographisches Modul

6.2.1 Standards und Sicherheitsmaßnahmen

Die eingesetzten kryptographischen Module entsprechen den gesetzlichen Anforderungen und Normen und werden in der gemäß der Zertifizierung der Komponenten notwendigen Umgebung betrieben (siehe Abschnitt 5.1). Der Zugriff auf die Komponenten ist durch technische und organisatorische Maßnahmen geschützt.

Die QSCD wird in einem gesicherten Bereich des VDA BNotK aufbewahrt und betrieben.

Dadurch wird sichergestellt, dass die QSCD nicht durch Dritte manipuliert werden kann.

Die Zertifizierung der im Einsatz befindlichen QSCDs wird während des gesamten Lebenszyklus auf Aktualität überprüft. Sollte sich eine Änderung am Status der Zertifizierung ergeben, werden die Auswirkungen analysiert und entsprechende Maßnahmen definiert.

6.2.2 Mehraugenprinzip bei der Schlüsselaktivierung

Die CA-Schlüssel können nur in einem technisch erzwungenen Mehraugenprinzip unter Beteiligung mehrerer Rollen aktiviert werden.

6.2.3 Schlüsselwiederherstellung

Schlüssel können nicht hinterlegt und damit auch nicht wiederhergestellt werden.

6.2.4 Schlüsselbackup

Es gibt Backups der privaten CA-Schlüssel. Das Backup, die Wiederherstellung und der Zugriff auf die privaten durch das HSM verschlüsselten CA-Schlüssel ist nur von autorisierten Personen im Vier-Augen-Prinzip möglich.

6.2.5 Schlüsselarchivierung

Schlüssel werden nicht archiviert.

6.2.6 Schlüsseltransfer

Die vom HSM gesicherten Schlüssel können im Vier-Augen-Prinzip zum Zwecke des Tauschs eines HSMs transferiert werden.

6.2.7 Schlüsselspeicherung

Die Schlüssel werden auf remote-QSCDs gespeichert und liegen mit Hilfe eines HSM gemäß ETSI TS 119 431-1 verschlüsselt in einer Datenbank des VDA BNotK vor.

6.2.8 Aktivierung privater Schlüssel

Die CA-Schlüssel und OCSP-Schlüssel (Dienstzertifikate) können nur in einem technisch erzwungenen Mehraugenprinzip unter Beteiligung mehrerer Rollen aktiviert werden.

Schlüssel von Endanwenderzertifikaten, CA- und OCSP-Schlüssel müssen durch die Eingabe der PIN aktiviert werden.

6.2.9 Deaktivierung privater Schlüssel

Die Deaktivierung der privaten Schlüssel für CA-, Dienste und Endanwenderzertifikate erfolgt beim Trennen der Verbindung zwischen Anwendung, Kartenleser und QSCD oder bei der Trennung der QSCD vom Kartenleser bzw. beim Trennen oder Deaktivieren des HSMs, sowie beim Stoppen des darauf zugreifenden Applikation. Eine dauerhafte Deaktivierung erfolgt nach mehrmaliger Falsch-eingabe der PIN. Eine limitierte Anzahl von Reaktivierungsversuchen über eine PUK ist möglich.

6.2.10 Zerstörung privater Schlüssel

Die Zerstörung von Schlüsseln erfolgt durch eine Zerstörung des Chips auf der QSCD oder durch Löschen der auf dem HSM gesicherten Schlüssel. EE-, CA- und OCSP-Schlüssel werden nach Ende der Gültigkeit zerstört.

Alle Kopien/Backups privater Schlüssel werden nach Ablauf oder Widerruf vernichtet, sodass eine weitere Verwendung oder Ableitung davon ausgeschlossen ist.

6.2.11 Beschreibung der kryptografischen Module

Es kommen ausschließlich Module zum Einsatz, die zum Aufbringen von qualifizierten Signaturen nach den geltenden Vorgaben zertifiziert wurden.

Die im Rahmen des SSAS eingesetzten qualifizierten Fernsignaturerstellungseinheiten sind in Abschnitt 6.9.11 beschrieben.

6.3 Weitere Aspekte der Verwaltung des Schlüsselpaars

6.3.1 Archivierung der öffentlichen Schlüssel

Die öffentlichen Schlüssel der Endanwenderzertifikate werden gemäß den gesetzlichen Bestimmungen archiviert (siehe Abschnitt 5.5).

6.3.2 Gültigkeitsdauer von Schlüssel und Zertifikaten

Die Gültigkeitsdauer der Schlüsselpaare und darauf basierenden Zertifikate entspricht maximal der erlaubten Gültigkeit für qualifizierte Zertifikate nach dem Algorithmenkatalog der BNetzA. Beim Auslaufen der Eignung eines eingesetzten Algorithmus oder der eingesetzten QSCD werden die Schlüssel vor Ablauf der Zertifikatsgültigkeit widerrufen (siehe Abschnitt 4.9).

6.4 Signatur- und Siegelerstellungsdaten sowie Aktivierungsdaten

6.4.1 Erzeugung und Installation

Signatur- und Siegelerstellungsdaten sind gemäß der eIDAS-Verordnung (EU 910/2014) eindeutige kryptographische Daten, die vom Unterzeichner bzw. Siegelinhaber zum Erstellen einer elektronischen Signatur oder eines elektronischen Siegels verwendet werden.

Dabei handelt es sich regelmäßig um den privaten kryptographischen Schlüssel.

Aktivierungsdaten sind Daten, die zur Nutzung der Signatur- oder Siegelerstellungsdaten erforderlich sind. Hierzu zählen insbesondere PINs, Passwörter, Einmalpasswörter (OTP) oder vergleichbare Authentisierungsfaktoren. Aktivierungsdaten ermöglichen nach erfolgreicher Authentisierung den Zugriff auf die Signatur- bzw. Siegelerstellungsdaten, sind jedoch nicht selbst Bestandteil dieser kryptographischen Schlüssel.

Die Signatur- bzw. Siegelerstellungsdaten werden in einer sicheren Umgebung erzeugt und dem Zertifikatsinhaber eindeutig zugeordnet. Die Nutzung dieser Daten ist ausschließlich nach erfolgreicher Authentisierung durch eine mit der Identität des Zertifikatsinhabers verknüpfte Authentisierungsmethode möglich.

Als Authentisierungsmethode können dabei je nach Anwendungsfall

- Chipkarten,
- ein privater kryptographischer Schlüssel (mit Authentisierungszertifikat) oder
- ein mobiles Endgerät samt 2FA-App zum Einsatz kommen.

Nur berechtigte Personen verfügen über die zur Nutzung erforderlichen Aktivierungsdaten, mit denen der private Schlüssel nach Authentisierung durch eine mit der Identität verbundene Authentisierungsmethode verwendet werden kann.

Die für die Aktivierung des privaten Schlüssels notwendigen Aktivierungsdaten (insbesondere das Authentisierungszertifikat) werden für den Zertifikatsinhaber im Rahmen der Zertifikatsbeantragung und Identifizierung erzeugt und durch den VDA BNotK fest mit dem Zertifikatsinhaber verknüpft.

Im Fall von Software-Authentisierungszertifikaten erfolgt die Erstellung und Bereitstellung über ein ausschließlich dem (vertretungsberechtigten) Antragsteller zugängliches und gesichertes Portal (Kundenportal). Die Erzeugung des Schlüsselpaares sowie die Vergabe der PIN erfolgen lokal auf dem Client des Antragstellers.

Für den Anwendungsfall der Autorisierung einer qualifizierten elektronischen Signatur via Smartphone ist zuvor die Registrierung eines mobilen Endgeräts im Kundenportal des Unterzeichners

notwendig. Für den Registrierungsprozess ist eine Anmeldung am Kundenportal mithilfe einer Chipkarte erforderlich. Erst nach erfolgreicher Registrierung kann das mobile Endgerät als zusätzlicher Authentisierungsfaktor verwendet werden.

6.4.2 Schutz von Signatur- und Siegelerstellungsdaten

Die Aktivierungsdaten für Teilnehmer werden bei Fernsignaturen verschlüsselt in einem gesicherten Rechenzentrum des VDA BNotK gespeichert. Bei Fernsignaturen ist der Zertifikatsinhaber selbst für den Schutz seiner Aktivierungsdaten zur Autorisierung des privaten Schlüssels verantwortlich. Bei Fernsiegelungen ist der vertretungsberechtigte Antragsteller für den Schutz der Aktivierungsdaten zur Autorisierung des privaten Schlüssels verantwortlich. Dies gilt sowohl für Authentisierungszertifikate als auch für Authentisierungskarten.

Die Aktivierungsdaten für CA-Schlüssel sind nur dem Besitzer des CA-Schlüssels bekannt.

6.4.3 Weitere Aspekte der Aktivierungsdaten

Neben der PIN gehört auch eine PUK zu den Aktivierungsdaten von Chipkarten. Die PUK dient zum Zurücksetzen des Fehlbedienungs Zählers bei falscher Eingabe der PIN. Sie kann aber nicht genutzt werden, um eine neue PIN zu setzen. Die PUK wird analog zur PIN erstellt, installiert und gesichert.

6.5 Computersicherheit

Der VDA BNotK stellt über verschiedene technische und organisatorische Maßnahmen sicher, dass die IT-Systeme ausschließlich für den designierten Zweck eingesetzt werden können und immer konform zum Sicherheitskonzept betrieben werden. Zu den Mechanismen gehören u.a. Überwachungssysteme, Protokollierungssysteme, mehrstufige Firewall- und Zugangssysteme, strikte Netzsegmentierung, strikte Rollentrennung und personalisierte Accounts, Integritätsschutz und Überwachung der eingesetzten kryptografischen Module, Virenschutz, regelmäßige Penetrationstests und Revisionen. Die IT-Systeme werden in einer sicheren Umgebung betrieben (siehe Abschnitt 5.1), um sie vor unberechtigten Zugriffen, Modifikation und Diebstahl zu schützen. Nicht benötigte Dienste, Programme und Accounts werden vor Inbetriebnahme der IT- Komponenten entfernt

Die Systemzeit aller IT-Systeme des VDA BNotK wird fortlaufend mit dem deutschen DCF77-Zeitsignal abgeglichen. Die hierzu verwendeten DCF77-Funkuhren werden täglich mit den Referenz-Zeitservern der Physikalisch-Technische Bundesanstalt (PTB) auf die koordinierte Weltzeit (UTC) synchronisiert.

Der Zugang zu den Systemen des VDA BNotK wird erst nach Berufung in die entsprechende Rolle gewährt und bei der Abberufung sofort entzogen (siehe auch Abschnitt 5.3.4). Die Zugriffe erfolgen stets über Multifaktor-Authentifizierung und werden protokolliert. Änderungen an den Sicherheitsmechanismen und IT-Systemen erfolgen nach einem festgelegten Prozess, werden dokumentiert

und können nur im Vier-Augen-Prinzip durchgeführt werden. Das Vier-Augen-Prinzip wird technisch erzwungen und kann nicht umgangen werden. Dies gilt auch für die Wiederherstellung von Daten.

Durch das implementierte Rollenkonzept und die Rollenausschlusskriterien wird gewährleistet, dass jede für den VDA BNotK tätige Person nur die Zugänge und Zugriffsrechte erhält, die für die Ausübung ihrer Rolle notwendig sind. Zu diesem Zweck wird bei den technischen Rollen zwischen verschiedenen administrativen, operativen und auditierenden Rollen unterschieden.

Der Zugang und Zugriff werden ausschließlich nach dem Prinzip „least privilege“ vergeben. Grundsätzlich setzt die Einrichtung von Zugängen und Zugriffen folgende Bedingungen voraus:

- Es besteht ein Vertragsverhältnis (Angestellt oder Beauftragung) zur Bundesnotarkammer.
- Bei externen Mitarbeitenden besteht eine Auftragsverarbeitungsvereinbarung ergänzend zum Auftrag.
- Die Aufgabe ist klar definiert und damit der notwendige Zugang und Zugriff auf die BNotK-Systeme.
- Es ist eine Person bei der BNotK bestimmt, die den Zugang und Zugriff der internen/externen Mitarbeitenden verantwortet.

Speichermedien mit sensiblen Daten werden nicht wiederverwendet. Um zu verhindern, dass unautorisierte Personen Zugriff auf sensible Daten bekommen, werden nicht mehr verwendete Datenträger von einem Dienstleister gemäß den Sicherheitsstufen der DIN 66399-2 durch Zerkleinern, Vermischen und Verpressen des Datenträgermaterials vernichtet.

Es bestehen Arbeitsanweisungen für die Mitarbeiter des VDA BNotK betreffend die Einhaltung der Vorgaben zur Computersicherheit. Mitarbeiter des VDA BNotK sind gemäß den geltenden gesetzlichen Bestimmungen für ihr Handeln verantwortlich.

6.6 Technische Kontrolle während des Lebenszyklus

6.6.1 Sicherheitsmaßnahmen beim Aufbau, der Entwicklung und Erweiterung der IT-Systeme und Softwarekomponenten

Der VDA BNotK folgt den Prinzipien von „Security by Design“. Vor Änderungen, Erweiterungen oder dem Aufbau von neuen Systemen, sowie bei Softwareentwicklungsprojekten werden die Anforderungen an die Sicherheit erhoben, um sie bereits in der Konzeptionsphase mit berücksichtigen zu können. Die Anforderungen an die Sicherheit ergeben sich u. a. aus dem Zertifizierungskonzept, der Zertifikatsrichtlinie, den zugrunde liegenden Sicherheitskonzepten und folgenden Quellen:

- Gesetzliche Vorgaben,
- Herstellerangaben,
- Best Practices,

- ggf. technische Richtlinien des BSI,
- ggf. anwendbare sonstige Normen.

Die Inbetriebnahme von neuen Komponenten, Änderungen an Systemen sowie das Einspielen von Fixes folgen definierten Prozessen. Alle Änderungen werden angemessen dokumentiert. Der Lebenszyklus endet mit der sicheren Entsorgung der Systeme.

6.6.2 Sicherheitsmaßnahmen beim Betrieb

Der Betrieb der Komponenten und die Einhaltung der vorgegebenen Betriebsparameter werden fortlaufend mit Hilfe eines Monitoringsystems überwacht. Bei Entdeckung sicherheitsrelevanter Ereignisse wird ein Alarm ausgelöst. Dabei wird sichergestellt, dass über diesen Weg keine sensiblen Daten ausgeleitet werden. Die Monitoringdaten dienen zusätzlich zur Kapazitätsplanung.

Des Weiteren werden alle sicherheitsrelevanten Prozesse und Störungen sowie Zugriffe der Mitarbeiter protokolliert. Protokolliert werden in diesem Zusammenhang - sofern sicherheitsrelevant - insbesondere Start und Beendigung der IT-Systeme, Start und Beendigung der Logging- Funktionalität der relevanten IT-Systeme (insbesondere Firewall, Datenbanksysteme, TOE, RA- System), Systemabstürze, Ausfälle der Hardware, Aktivitäten der Firewall und der Router sowie Zugriffsversuche auf das PKI-System sowie Anfragen zu nicht ausgestellten Zertifikaten beim Responder. Die entsprechenden Protokolle werden entsprechend den gesetzlichen Vorgaben aufbewahrt.

Es wird lediglich Software aus vertrauenswürdigen Quellen in Betrieb genommen. Die Integrität der Software wird fortlaufend überwacht und Veränderungen am System gemeldet. Sicherheitskritische Fehler werden innerhalb einer angemessenen Zeit behoben und sicherheitsrelevante Patches zeitnah eingespielt. Patches werden nicht eingespielt, wenn sich daraus Nachteile und Instabilitäten ergeben, die schwerwiegender sind als die Vorteile des Patches. Das Nichteinspielen solcher Updates sowie der Grund dafür wird dokumentiert.

Zertifizierte Komponenten werden immer gemäß der geforderten Einsatzumgebung betrieben. Zusätzlich findet eine automatische Protokollanalyse statt, um Fehler und Angriffsversuche frühzeitig zu erkennen. Diese Maßnahme wird durch regelmäßige manuelle Kontrollen ergänzt. Neben den Protokollen werden insbesondere auch die Audit Logs geprüft. Angriffsversuche, Verstöße gegen die Sicherheitsregeln und Meldungen des Monitoringsystems werden an die Administratoren gemeldet, die sich unverzüglich um eine Behebung des Fehlers bzw. eine Eingrenzung möglicher sicherheitsrelevanter Ereignisse kümmern. Sicherheitsrelevante Vorfälle und offene Sicherheitslücken werden unverzüglich an den Sicherheitsbeauftragten des VDA BNotK gemeldet, der die Umsetzung aller zur Behebung des Sicherheitsvorfalls notwendigen Maßnahmen bewertet und dann ggf. umsetzen lässt und den Vorgang dokumentiert. Relevante Sicherheitsvorfälle werden innerhalb von 24 Stunden an die aufsichtführende Stelle gemeldet. Sofern zutreffend, werden auch von dem Sicherheitsvorfall betroffene Personen und Firmen unverzüglich informiert.

Kritische Schwachstellen, die nicht anderweitig adressiert worden sind, werden innerhalb von 48 Stunden nach deren Entdeckung adressiert. Auf Grundlage einer Bewertung des mit derartigen Schwachstellen verbundenen Risikos wird der VDA BNotK diese beheben oder – wenn dies im Verhältnis zu den Auswirkungen nicht mit wirtschaftlich vertretbarem Aufwand möglich ist – dokumentieren, warum diese nicht behoben werden.

Alle IT-Systeme und Softwarekomponenten werden immer gemäß den Herstellerangaben betrieben.

Die Daten werden auf Festplatten gesichert, die ausgetauscht werden, sobald sie funktionsunfähig sind oder gemäß den Herstellerangaben nicht mehr betrieben werden dürfen. Datenverluste wegen alternder Datenträger werden durch die redundante Speicherung der Daten vermieden.

Der VDA BNotK lässt regelmäßig, alle drei Monate, Schwachstellenscans (*vulnerability scans*) sowie alle 12 Monate Penetrationstests (*penetration tests*) durch einen unabhängigen und fachkundigen Dritten bzw. Mitarbeiter der entsprechenden Fachabteilung der Bundesnotarkammer durchführen. Die Ergebnisse werden dokumentiert, durch den VDA BNotK bewertet und festgestellte Mängel beseitigt, soweit dies erforderlich ist.

6.6.3 Lieferketten- und Assetmanagement

Die Steuerung von Lieferanten und der Schutz von über die Lieferkette bereitgestellten Assets erfolgt gemäß der Lieferantenmanagementrichtlinie der Bundesnotarkammer.

Diese legt risikobasierte Anforderungen für die Auswahl, Bewertung und Klassifizierung von Lieferanten fest und regelt die vertragliche Absicherung von Informationssicherheitsanforderungen. Hierzu zählen insbesondere Vorgaben zu Subunternehmern, Incident-Meldepflichten, Change-Management, sicheren Entwicklungspraktiken sowie Audit- und Kontrollrechten.

Darüber hinaus umfasst die Richtlinie Regelungen zur sicheren Integration, zum Betrieb sowie zur Rückgabe, Löschung oder Vernichtung von bereitgestellten Assets und Daten nach Vertragsende. Die Einhaltung der festgelegten Anforderungen wird dokumentiert und regelmäßig überprüft.

6.7 Netzwerksicherheit

Die IT-Systeme des VDA BNotK werden durch Firewalls geschützt. Die Netzwerke des Sicherheitsbereichs sind in verschiedene Netzwerkzonen segmentiert und physikalisch voneinander durch mehrstufige Firewallsysteme getrennt. Die IT-Systeme sind je nach Schutzbedarf und Funktion auf die verschiedenen Netzsegmente verteilt. Systeme des gleichen Schutzbedarfs und mit gleicher Funktionalität befinden sich in den gleichen Zonen. Die für den Betrieb des VDA BNotK wichtigsten Systeme, wie beispielsweise die Root CA, befinden sich in der Zone mit dem höchsten Schutzbedarf. Für die Administration der IT-Systeme wird ein separates Netz verwendet. Für Testumgebungen existieren ebenfalls separate Netze.

Die Verbindungen und Protokolle zwischen den Segmenten sind auf das für den Funktionsumfang notwendige Minimum beschränkt. Alle anderen Verbindungen werden blockiert und die unerlaubten Zugriffe protokolliert. Die Übertragung sensibler Daten erfolgt grundsätzlich verschlüsselt. Besonders schützenswerte Kommunikationskanäle können nur aufgebaut werden, wenn sich die beiden Endpunkte gegenseitig authentisieren. Die Netzwerkkumgebung und die Anbindung der Netzwerke sind hochverfügbar ausgelegt.

Zur Gewährleistung der Netzwerk- und Systemsicherheit wird ein kontinuierliches Monitoring durchgeführt, das in regelmäßigen Abständen die Verfügbarkeit der Gateways, den Clusterstatus (Partner-Status) sowie den Systemzustand überprüft. Zudem werden Penetrationstests auf die extern zugänglichen und internen IP-Adressen vorgenommen. Die Überprüfungen erfolgen durch qualifiziertes Fachpersonal und werden bei sicherheitserheblichen Veränderungen wiederholt.

Die Einhaltung der Regeln wird einer jährlichen Revision unterzogen und protokolliert.

6.8 Zeitstempel

Die Regelungen zum qualifizierten Zeitstempeldienst werden im Dokument Time Stamp Policy und TSA Practice Statement des VDA BNotK geregelt.

6.9 Server Signing Application Service (SSAS) – Verwaltung von Fernsignatur- und Fernsiegelerstellungsgeräten –

Der nachfolgend beschriebene Server Signing Application Service (SSAS) – Verwaltung von Fernsignatur- und Fernsiegelerstellungsgeräten – ist ein eigenständiger qualifizierter Vertrauensdienst im Sinne von Art. 3 der Verordnung (EU) 2024/1183 (eIDAS 2.0).

Die in diesem Kapitel enthaltenen Regelungen stellen vollständig die SSAS Policy sowie das SSAS Practice Statement gemäß ETSI TS 119 431-1.

Separate SSAS-Policy- oder SSAS-Practice-Statement-Dokumente werden nicht geführt.

6.9.1 Anwendungsbereich und Abgrenzung

Der SSAS umfasst die sichere Verwaltung, Nutzung und Löschung von Fernsignatur- und Fernsiegelerstellungsgeräten einschließlich der zugehörigen Signaturschlüssel für qualifizierte elektronische Signaturen und Siegel.

Der Dienst ist organisatorisch und funktional von den anderen Vertrauensdiensten abgegrenzt. Der SSAS umfasst keine Zertifizierungsleistungen im Sinne der Ausstellung oder Verwaltung von Zertifikaten.

6.9.2 Rollen und Verantwortlichkeiten

Der VDA BNotK handelt als Server Signing Application Service Provider (SSASP) und trägt die Gesamtverantwortung für Betrieb, Sicherheit und Konformität des SSAS.

Eine Beauftragung Dritter ist zulässig, entbindet den VDA BNotK jedoch nicht von seiner Verantwortung.

Einzelheiten zur Übertragung von Aufgaben auf Dritte sind in Abschnitt 1.8 der Zertifikatsrichtlinie (CP) des VDA BNotK geregelt.

Am Server Signing Application Service (SSAS) sind insbesondere beteiligt:

- der Unterzeichner (Signer), der zur Auslösung von Signaturvorgängen autorisiert ist,
- Anwendungen oder Systeme, die Signaturanfragen an den SSAS übermitteln (funktionale Rolle einer Signature Creation Application),
- der Vertrauensdiensteanbieter VDA BNotK sowie
- die im Sicherheitskonzept beschriebenen unterstützenden Systemkomponenten.

Die im Rahmen der Zertifikatsausstellung erforderlichen Identifizierungs- und Registrierungsprozesse werden durch die Registration Authority (RA) durchgeführt. Diese Prozesse sind Bestandteil der Zertifizierungsinfrastruktur und nicht Teil des operativen Signaturprozesses des SSAS.

Die Erstellung qualifizierter Zertifikate sowie die zugehörigen Prozesse der Schlüsselgenerierung und Personalisierung erfolgen innerhalb der Certification Authority (CA) gemäß den Vorgaben des Sicherheitskonzeptes.

Die funktionalen Rollen gemäß ETSI TS 119 431-1 sind im Gesamtsystem umgesetzt und funktional voneinander getrennt.

Es wird sichergestellt, dass keine einzelne Rolle den gesamten Prozess von Identifizierung, Autorisierung und Signaturlösung allein durchführen kann.

6.9.3 SSAS Policy – normative Festlegungen

Der VDA BNotK stellt sicher, dass Signaturschlüssel ausschließlich innerhalb zertifizierter Fernsignatur- und Fernsiegelerstellungsgeräte (Remote-QSCD/SCDev) erzeugt, gespeichert und verwendet werden.

Der Unterzeichner besitzt jederzeit die alleinige Kontrolle über die Auslösung einer Signatur oder eines Siegels.

Jeder Signatur- oder Siegelvorgang erfordert eine explizite Authentisierung des Unterzeichners. Einzelheiten zur Authentisierung und Signaturlösung sind in Abschnitt 4.5 beschrieben.

6.9.4 SSAS Practice Statement – operative Umsetzung

Der SSAS wird in einer technisch und organisatorisch gesicherten Umgebung betrieben.

Alle sicherheitsrelevanten Prozesse sind dokumentiert, überwacht und unterliegen regelmäßigen Kontrollen.

6.9.5 Erzeugung und Verwaltung von Signaturschlüsseln

Die für die Fernsignatur und Fernsiegelerstellung verwendeten Signaturschlüssel werden innerhalb qualifizierter elektronischer Signatur- bzw. Siegelerstellungseinheiten (QSCD) erzeugt und verwaltet. Die Verwaltung umfasst Aktivierung, Nutzung, Sperrung und irreversible Löschung. Ein Einsatz gesperrter oder abgelaufener Schlüssel ist technisch ausgeschlossen.

Die Signaturschlüssel verlassen zu keinem Zeitpunkt die gesicherte Umgebung der QSCD. Eine Exportierbarkeit der privaten Schlüssel ist ausgeschlossen.

Die Erzeugung der Signaturschlüssel erfolgt im Rahmen der Registrierung des Unterzeichners und ist eindeutig an dessen Identität und das zugehörige qualifizierte Zertifikat gebunden.

6.9.6 Identitätsbindung und Authentisierung

Vor der erstmaligen Nutzung des Server Signing Application Service (SSAS) wird die Identität des Unterzeichners vom VDA BNotK überprüft und eindeutig festgestellt.

Die Identitätsfeststellung erfolgt nach den hierfür geltenden Regelungen dieses Zertifizierungskonzepts (Siehe Abschnitt 3.2) sowie gemäß den ergänzenden Vorgaben zur Identitätsprüfung, insbesondere unter Berücksichtigung der ETSI TS 119 461-1.

Die Identitätsprüfung des Unterzeichners erfolgt mit einem Sicherheitsniveau, das den Anforderungen für qualifizierte elektronische Signaturen und Siegel entspricht.

Dabei wird mindestens ein substantielles Sicherheitsniveau gemäß den einschlägigen normativen Vorgaben eingehalten.

Der VDA BNotk stellt sicher, dass eine eindeutige, überprüfbare und dauerhafte Zuordnung zwischen:

- der geprüften Identität des Unterzeichners,
- dem zugeordneten qualifizierten Zertifikat und
- dem zugehörigen Signaturschlüssel besteht.

Der Zugriff auf den SSAS sowie die Freigabe zur Nutzung des Signaturschlüssels erfolgen ausschließlich nach erfolgreicher Authentisierung des Unterzeichners unter Einsatz starker Authentisierungsmechanismen.

Die Zuordnung wird technisch und organisatorisch so umgesetzt, dass der Signaturschlüssel ausschließlich in Verbindung mit der erfolgreich authentisierten Identität des zugeordneten Unterzeichners genutzt werden kann.

Die Zuordnung bleibt über den gesamten Lebenszyklus des Zertifikats und des Signaturschlüssels hinweg erhalten und wird nur bei Widerruf oder Ablauf des Zertifikats oder des Signaturschlüssels aufgehoben.

6.9.7 Auslösen eines Signatur- oder Siegelvorgangs

Jeder Signatur- oder Siegelvorgang erfordert eine aktive Willensbekundung bzw. Autorisierung des Unterzeichners.

Signatursitzungen sind zeitlich begrenzt. Der Signaturschlüssel wird ausschließlich für die Dauer des jeweiligen Signaturvorgangs aktiviert und anschließend unverzüglich wieder deaktiviert.

Vor der Signaturerstellung wählt der Unterzeichner die zu signierenden Daten sowie den zu verwendenden Signaturschlüssel aus und bestätigt den Signaturvorgang mittels eines geeigneten Authentisierungsmechanismus. Einzelheiten sind in Abschnitt 4.5 beschrieben.

Wird der private Signatur- oder Siegelerstellungsschlüssel durch den VDA BNotK im Rahmen des Server Signing Application Service (SSAS) verwaltet, gewährleistet der VDA BNotK durch geeignete technische und organisatorische Maßnahmen, dass der private Schlüssel unter der alleinigen Kontrolle des Unterzeichners bzw. Siegelerstellers verbleibt.

Die alleinige Kontrolle wird insbesondere durch eine starke Authentifizierung, die eindeutige Zuordnung der Aktivierungsdaten sowie durch die Nutzung einer qualifizierten Signaturerstellungseinheit (QSCD) sichergestellt.

6.9.8 Löschung und Sperrung von Signaturschlüsseln

Signaturschlüssel werden bei Widerruf und Ablauf des Zertifikats unverzüglich und technisch irreversibel innerhalb der QSCD gelöscht.

6.9.9 Protokollierung, Überwachung und Nachvollziehbarkeit

Sämtliche sicherheitsrelevanten Ereignisse im Zusammenhang mit dem Betrieb des SSAS, insbesondere Registrierungs-, Authentisierungs- und Signaturvorgänge, werden vollständig protokolliert (Audit-Logs) und ermöglichen eine nachvollziehbare Rekonstruktion der durchgeführten Vorgänge.

6.9.10 Audit, Konformität und Aufsicht

Der Betrieb des SSAS unterliegt regelmäßigen internen Kontrollen sowie externen Prüfungen durch eine akkreditierte Konformitätsbewertungsstelle (TÜV NORD CERT GmbH).

Zudem arbeitet der VDA BNotK eng mit der Bundesnetzagentur als Aufsichtsstelle für qualifizierte Vertrauensdiensteanbieter in Deutschland zusammen.

6.9.11 Qualifizierte Fernsignaturerstellungseinheit (Remote QSCD)

Für die Erbringung des Server Signing Application Service (SSAS) setzt der VDA BNotK qualifizierte Fernsignaturerstellungseinheiten (Remote QSCD) ein.

Die im Rahmen des Server Signing Application Service eingesetzte qualifizierte Signaturerstellungseinheit (QSCD) entspricht den Anforderungen des Anhangs II der Verordnung (EU) Nr. 910/2014 (eIDAS) in der jeweils geltenden Fassung, einschließlich der Änderungen durch Verordnung (EU) 2024/1183. Die Konformität wird durch entsprechende Zertifizierungen nachgewiesen.

Die eingesetzte **QSCD/SSCD** ist:

proNEXT SignatureActivationModule, Version 1.0.0 der procilon GmbH

zertifiziert vom TÜV Informationstechnik GmbH, mit der Zertifizierungsnummer:

TUVIT.9802.QSCD.10.2020; TUVIT.9804.QSCD.07.2024

Die Zertifizierung erfüllt die Anforderungen des Anhangs II der Verordnung (EU) Nr. 910/2014 in der jeweils geltenden Fassung, einschließlich der Änderungen durch Verordnung (EU) 2024/1183. Die Zertifizierung ist gültig bis 05.12.2028.

Die Erzeugung, Speicherung und Verarbeitung der privaten Signatur- und Siegelerstellungsschlüssel erfolgt ausschließlich innerhalb der zertifizierten QSCD.

Für die Signaturaktivierung werden folgende zertifizierte Signature Activation Module (SAM) eingesetzt:

- **CryptoServer CP5 Se12 Version 5.1.0.0**
- **CryptoServer CP5 Se52 Version 5.1.0.0**
- **CryptoServer CP5 Se500 Version 5.1.0.0**
- **CryptoServer CP5 Se1500 Version 5.1.0.0**

Diese erfüllen die Anforderungen an Signaturaktivierungsmechanismen gemäß Anhang II der Verordnung (EU) Nr. 910/2014 in der jeweils geltenden Fassung.

Die Remote-QSCD-Architektur gewährleistet die alleinige Kontrolle des Unterzeichners über die Signaturerstellungsdaten sowie die Auslösung eines Signaturvorgangs ausschließlich nach erfolgreicher Authentisierung und expliziter Willensbekundung.

6.9.12 Verfügbarkeit des Server Signing Application Service (SSAS)

Der VDA BNotK stellt sicher, dass der Server Signing Application Service grundsätzlich 24 Stunden täglich an sieben Tagen pro Woche verfügbar ist.

Im Falle von Systemausfällen oder Störungen wird angestrebt, die Nichtverfügbarkeit so kurz wie möglich zu halten.

Eine Nichtverfügbarkeit von mehr als einem Arbeitstag je Ereignis wird als schwerwiegender Vorfall betrachtet und gesondert analysiert.

Die Regelungen zur Behandlung von Verfügbarkeitsstörungen sind in Abschnitt 5.8 beschrieben.

7 Profile von Zertifikaten, Widerrufslisten und OCSP

7.1 Zertifikatsprofile

Die Seriennummern der vom VDA BNotK ausgestellten Zertifikate werden zufällig erzeugt.

Die vom VDA BNotK ausgestellten Zertifikate entsprechen den Anforderungen der ISO/IEC 9594-8 (ITU-T X.509) sowie des IETF RFC 5280 in der jeweils geltenden Fassung.

7.1.1 Root-CA

Zertifikatsprofil RSA

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	[6f b8 e3 d6 dc a1 f6 bb]
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 Aussteller	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	CN = BNotK Root CA 2017 CN = BNotK Root CA 2021
Gültigkeit		

UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Zertifikatsgültigkeit	30 Jahre
--	-----------------------	----------

Inhaber		
----------------	--	--

countryName (2.5.4.6)	Name Land Inhaber	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	CN = BNotK Root CA 2017 CN = BNotK Root CA 2021
-------------------------	--------------	--

Erweiterungen		
----------------------	--	--

keyUsage (2.5.29.15)	Verwendungszweck	keyCertSign, cRLSign
-------------------------	------------------	----------------------

basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=Zertifizierungsstelle Einschränkung Pfadlänge=0
---------------------------------	---	--

subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssels des Inhabers	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
-------------------------------------	--	--

authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssels des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
---------------------------------------	---	--

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
------------------------------	---------------------	---

Zertifikatsprofil ECC

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	[6f b8 e3 d6 dc a1 f6 bb]
Signaturalgorithmus (1.2.840.10045.4.3.4)	Kennzeichner (OID) Signaturalgorithmus	SHA512WITHECDSA
Schlüssellänge	Schlüssellänge	521 Bits
Aussteller		
countryName (2.5.4.6)	Name Land Aussteller	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	CN = BNotK EC Root CA 2021
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Zertifikatsgültigkeit	30 Jahre
Inhaber		
countryName (2.5.4.6)	Name Land Inhaber	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	CN = BNotK EC Root CA 2017 CN = BNotK EC Root CA 2020 CN = BNotK EC Root CA 2021

Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=Zertifizierungsstelle Einschränkung Pfadlänge=0
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssel des Inhabers	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssel des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Verweis auf Aussteller und Dienst zur Statusabfrage	s. folgende Elemente
caIssuers (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

7.1.2 Sub-CA

Zertifikatsprofil RSA

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	z.B. [6f b8 e3 d6 dc a1 f6 bb]
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	Name Land Aussteller	C = DE

(2.5.4.6)		
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	CN = BNotK Root CA 2017 CN = BNotK Root CA 2021
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Zertifikatsgültigkeit	20 Jahre
Inhaber		
countryName (2.5.4.6)	Name Land Inhaber	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	CN = BNotK qSig CA 2017 CN = BNotK rqSig CA 2020 CN = BNotK rqSig CA 2021 CN = BNotK qSig CA 2021
Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	keyCertSign, cRLSign

basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=Zertifizierungsstelle Einschränkung Pfadlänge=0
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssel des Inhabers	z.B. [CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier	Identifizierung öffentlicher	[FDF35084308EEC239AF5

(2.5.29.35)	Schlüssel des Ausstellers	33B2E38107DDE4EF80AE]
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

Zertifikatsprofil ECC

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	z.B. [6f b8 e3 d6 dc a1 f6 bb]
Signaturalgorithmus (1.2.840.10045.4.3.4)	Kennzeichner (OID) Signaturalgorithmus	SHA512WITHECDS
Schlüssellänge	Schlüssellänge	521 Bits
Aussteller		
countryName (2.5.4.6)	Name Land Aussteller	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	CN= BNotK EC rqSig CA 2020 CN = BNotK EC rqSig CA 2021 CN= BNotK EC qSig CA 2021

Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Zertifikatsgültigkeit	20 Jahre

Inhaber		
countryName (2.5.4.6)	Name Land Inhaber	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 qSig CA 2017

Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=Zertifizierungsstelle Einschränkung Pfadlänge=0
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssel des Inhabers	z.B. [CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssel des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
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

7.1.3 Endanwenderzertifikatsprofil

QCP-n-qscd RSA – qualifizierte Signaturzertifikate auf qualifizierten Signaturerstellungseinheiten auf Basis eines RSA-Kryptoalgorithmus.

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber	Seriennummer des Zertifikats	z.B. [6f b8 e3 d6 dc a1 f6 bb]

(2.5.4.5)		
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	3072 Bits
Aussteller		
countryName (2.5.4.6)	Name Land Aussteller	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	CN = BNotK rqSig CA 2021
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Zertifikatsgültigkeit	7 Jahre
Inhaber		

countryName (2.5.4.6)	Name Land Inhaber	z.B. C = DE Land, in dem der Zertifikatsinhaber seinen Wohnsitz hat oder das vorgelegte Identifikationsdokument ausgestellt wurde.
organizationName (2.5.4.10)	Name Organisation	O = [Organisation]
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = [Kennzeichner Organisation]
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = [Abteilung]
commonName (2.5.4.3)	Name Inhaber	CN = Vorname(n) Nachname
serialNumber (2.5.4.5)	Kennzeichner Inhaber	2.5.4.5 = (ggf. lokal definierte) Identifikationsnummer
givenName (2.5.4.42)	Vorname Inhaber	2.5.4.42 = Vorname(n)
surname (2.5.4.4)	Nachname Inhaber	2.5.4.4 = Nachname
title (2.5.4.12)	Titel Inhaber	2.5.4.12 = Titel
emailAdress (1.2.840.113549.1.9.1)	E-Mail-Adresse Inhaber	emailAdress = [name@domain.tld]
userID (0.9.2342.19200300.100.1.1)	Eindeutige user ID zur Verknüpfung von Authentisierungsmittel und Fernsignatur	restrictedID des eID, eineindeutige UUID des Zertifikatsinhabers
Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	nonRepudiation
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=End Entity Einschränkung Pfadlänge=None
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssels des Inhabers	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]

authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssels des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
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/ve-roeffentlichungen
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)	Verweis auf geltende Zertifizierungsrichtlinie	s. folgende Elemente
Policy Information	policyIdentifier	Kennzeichner (OID) und URL-Verweis auf CPS
	policyQualifier	https://zertifizierungsstelle.bnotk.de/ve-roeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)	Kennzeichner (OID) eIDAS-Konformität qSig	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. Signatur)	0.4.0.1862.1.6.1
QcPDS (0.4.0.1862.1.5)	URL-Verweis auf PDS	https://zertifizierungsstelle.bnotk.de/ve-roeffentlichungen
subjectAltName (2.5.29.17)	E-Mail-Adresse Inhaber	[name@domain.tld] gemäß IETF RFC 5280 [7]
Subject Directory Attributes (2.5.29.9)	Zusätzliche den Inhaber bzw. das Zertifikat beschreibende Merkmale	s. folgende Elemente
dateOfCertGen (1.3.36.8.3.1)	Datum der Zertifikats-Erstellung	z.B. 2017-10-09 08:57:57 UTC
admission (1.3.36.8.3.3)	Berufliche Attribute Inhaber	[admissionAuthority, namingAuthority, professionInfo]
procuration (1.3.36.8.3.2)	Informationen zu Vertretungsvollmacht	[StringType]

restriction (1.3.36.8.3.1)	Sonstige Einschränkungen in Verbindung mit der Nutzung des Zertifikats	[StringType]
-------------------------------	--	--------------

QCP-n-qscd (ECDSA) – qualifizierte Signaturzertifikate auf qualifizierten Signaturerstellungseinheiten auf Basis eines ECDSA-Kryptoalgorithmus.

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	z.B. [6f b8 e3 d6 dc a1 f6 bb]
Signaturalgorithmus (1.2.840.10045.4.3.4)	Kennzeichner (OID) Signaturalgorithmus	SHA512WITHECDSA (1.2.840.10045.4.3.4)
Signaturhashalgorithmus	Kennzeichner (OID) Signaturhashalgorithmus	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifizier	Kennzeichner (OID) Schlüsselalgorithmus	ECDSA (1.2.840.10045.4.3.4)
Schlüssellänge	Schlüssellänge	521 Bits
Aussteller		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifizier (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	CN = BnotK EC rqSig CA 2021

Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Zertifikatsgültigkeit	7 Jahre
	Ende	Ende Zertifikatsgültigkeit
Inhaber		

countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = [Organisation]
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = [Kennzeichner Organisation]
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = [Abteilung]
commonName (2.5.4.3)	Name Inhaber	CN = Vorname(n) Nachname
serialNumber (2.5.4.5)	Kennzeichner Inhaber	2.5.4.5 = (ggf. lokal definierte) Identifikationsnummer
givenName (2.5.4.42)	Vorname Inhaber	2.5.4.42 = Vorname(n)
surname (2.5.4.4)	Nachname Inhaber	2.5.4.4 = Nachname
title (2.5.4.12)	Titel Inhaber	2.5.4.12 = Titel
emailAdress (1.2.840.113549.1.9.1)	E-Mail-Adresse Inhaber	emailAdress = [name@domain.tld]
userID (0.9.2342.19200300.100.1.1)	Eindeutige user ID zur Verknüpfung von Authentisierungsmittel und Fernsignatur	restrictedID des eID, eineindeutige UUID des Zertifikatsinhabers
Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	nonRepudiation
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=End Entity Einschränkung Pfadlänge=None
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssels des Inhabers	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssels des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]

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 http://qcsp.zs.bnotk.de/eqsig
CertificatePolicies (2.5.29.32)	Verweis auf geltende Zertifizierungsrichtlinie	s. folgende Elemente
Policy Information	policyIdentifier	Kennzeichner (OID) und URL-Verweis auf CPS
	policyQualifier	
		1.3.6.1.4.1.41460.5.2.1.1.2
		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)	Kennzeichner (OID) eIDAS-Konformität qSig	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. Signatur)	0.4.0.1862.1.6.1

QcPDS (0.4.0.1862.1.5)	URL-Verweis auf PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
subjectAltName (2.5.29.17)	E-Mail-Adresse Inhaber	[name@domain.tld]
Subject Directory Attributes (2.5.29.9)	Zusätzliche den Inhaber bzw. das Zertifikat beschreibende Merkmale	s. folgende Elemente
dateOfCertGen (1.3.36.8.3.1)	Datum der Zertifikats-Erstellung	z.B. 2017-10-09 08:57:57 UTC
admission (1.3.36.8.3.3)	Berufliche Attribute Inhaber	[admissionAuthority, namingAuthority, professionInfo]
procuration (1.3.36.8.3.2)	Informationen zu Vertretungsvollmacht	[StringType]

restriction (1.3.36.8.3.1)	Sonstige Einschränkungen in Verbindung mit der Nutzung des Zertifikats	[StringType]
-------------------------------	--	--------------

QCP-I-qscd (ECDSA) – qualifizierte Siegelzertifikate auf qualifizierten Siegelerstellungseinheiten auf Basis eines ECDSA-Kryptoalgorithmus.

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	z.B. [6f b8 e3 d6 dc a1 f6 bb]
Signaturalgorithmus	Kennzeichner (OID) Signaturalgorithmus	SHA512withECDSA (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	ECDSA_P384 (1.2.840.113549.1.1.1)
Schlüssellänge	Schlüssellänge	384 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	CN = BNotK EC rqSeal CA 2021
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Zertifikatsgültigkeit	7 Jahre
Inhaber		

countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = [Organisation]
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = [Abteilung]
commonName (2.5.4.3)	commonName	CN = Organisationsname oder abweichende, der Organisation zugehörige, Bezeichnung.
userID (0.9.2342.19200300.100.1.1)	Eindeutige user ID zur Verknüpfung von Authentisierungsmittel und Fernsignatur	eindeutige UUID des Zertifikatsinhabers
Erweiterungen		

keyUsage (2.5.29.15)	Verwendungszweck	nonRepudiation
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=End Entity Einschränkung Pfadlänge=None
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssels des Inhabers	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssels des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
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)	Verweis auf geltende Zertifizierungsrichtlinie	s. folgende Elemente
Policy Information	policyIdentifier	Kennzeichner (OID) und URL- Verweis auf CPS
	policyQualifier	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)	Kennzeichner (OID) eIDAS-Konformität qSig	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

7.2 Widerrufslistenprofile

Für qualifizierte Zertifikate werden keine Widerrufslisten angeboten.

7.3 Profile des Statusabfragedienstes

Zur Statusabfrage der Zertifikate wird ein OCSP-Responder nach RFC 6960 betrieben, welcher auch Positivauskünfte (certHash-Erweiterung) unterstützt. Die Antworten des OCSP-Responders sind qualifiziert signiert.

Der BNotK OCSP Responder beauskunftet die Gültigkeit eines Zertifikats zu einem bestimmten Zeitpunkt für einen anfragenden Dritten. Dabei werden folgende Status zurückgeliefert:

- good – Das Zertifikat ist im Verzeichnisdienst vorhanden und nicht widerrufen,
- unknown – Das Zertifikat ist nicht im Verzeichnisdienst vorhanden,
- revoked – Das Zertifikat wurde zu dem angegebenen Zeitpunkt widerrufen.

7.3.1 Versionsnummer

Es wird OCSP v1 gemäß RFC 6960 eingesetzt.

7.3.2 OCSP-Erweiterungen

Anfragen

Erweiterung	Wert
RetrievelfAllowed	Ein angefragtes Zertifikat wird in der Antwort mitgeliefert, wenn gesetzt (optional)

Antworten

Erweiterung	Wert
RequestedCertificate	Enthält das angefragte Zertifikat, wenn RetrievelfAllowed gesetzt ist.
archiveCutOff	Definiert den Zeitraum, in dem der OCSP- Responder ab Zertifikatserstellung die Statusinformationen bereitstellt.

8 Konformitätsprüfung

Siehe Abschnitt 8 der Zertifikatsrichtlinie (CP) des VDA BNotK.

9 Sonstige geschäftliche und rechtliche Regelungen

Siehe Abschnitt 9 der Zertifikatsrichtlinie (CP) des VDA BNotK.

Anhang I - Ergänzende Regelungen zur Identitätsprüfung gemäß ETSI TS 119 461-1

I. Identitätsprüfungsdienst (IPSP)

Diese Ergänzung zum Zertifizierungskonzept (CPS) des VDA BNotK, beschreibt die organisatorischen, technischen und prozessualen Regelungen zur Durchführung der Identitätsprüfung im Sinne eines Identitätsprüfungsdienstes (Identity Proofing Service Provider, IPSP). Sie dient der Abbildung der Anforderungen der ETSI TS 119 461 V2.1.1 und ist als integraler Bestandteil dieses CPS zu verstehen.

Die Regelungen dieses Anhangs gelten für alle Identifizierungsverfahren, die im Rahmen der Beantragung qualifizierter Zertifikate für natürliche Personen (Signaturzertifikate) und juristische Personen (Siegelzertifikate) eingesetzt werden, soweit diese Verfahren der Feststellung oder Bestätigung der Identität dienen.

a. Identitätsprüfungskontexte - Attribute und Mittel zur Erfassung und Prüfung

Der Antragsteller erhält in jedem Verfahren klare Anweisungen darüber, wie das Verfahren zur Identitätsprüfung durchgeführt wird, welche Identitätsdaten erfasst werden, welche Daten wie lange gespeichert werden, welche Nachweise der Antragsteller vorlegen muss und welche Hilfsmittel er verwenden muss. Nutzungsbedingungen und AGB stehen zur Verfügung.

b. Zuordnung der Anwendungsfälle (Use Cases) entsprechend TS 119 641

Die Identitätsprüfung ist der Prozess, mit dem mit der erforderlichen Zuverlässigkeit nachgewiesen wird, dass die angegebene Identität eines Antragstellers korrekt ist. Eingesetzte Identifizierungsverfahren entsprechen dem erweiterten Sicherheitsniveau (Extended LoIP) gemäß TS 119 641 und sind folgendermaßen den Use Cases der Norm eingestuft:

Natürliche Personen

Anwesenheit des Antragstellers	Vorgang	Umgesetzte TS 119 461 Referenz	Ausweisdokument	Überprüfung der Nachweise	Binding an den Antragsteller
Notarident	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell

Gerichtident	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell
Rechtsanwalts- kammerident	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell
RA-Ident	Manuell	9.2.1.2 Annex C.3.1	Physisch	Manuell	Manuell
eIDent	Automated	9.2.3.3 Annex C.3.2	Digital	Automated	Automated

Juristische Personen

Anwesenheit des Antragstellers	Vorgang	Umgesetzte TS 119 461 Referenzen	Ausweisdokument	Überprüfung der Nachweise	Binding an den Antragsteller
Notarident Gerichtident RA-Ident	Manuell	9.3+ 9.4 Annex C.3.6	Physisch	Manuell	Manuell

c. Identitätsprüfungskontexte und Attribute

Der Kontext der Identitätsprüfung umfasst alle externen Rahmenbedingungen, denen ein Identitätsprüfungsprozess unterliegt und die Anforderungen und Einschränkungen für die Identitätsprüfung mit sich bringen können. Ein Kernelement des Kontexts der Identitätsprüfung sind die regulatorischen Anforderungen, die durch die geltenden Rechtsvorschriften für den definierten Zweck an die Identitätsprüfung gestellt werden. Der Kontext der Identitätsprüfung variiert je nach Zweck der Identitätsprüfung.

Unterstützte Identitätsprüfungskontexte sind:

- Fernsignatur
- Fernsiegel
- notarielles Online-Verfahren.

Identitätsprüfungskontexte und Attribute für **natürliche Personen**:

Attribut	Fernsignatur	notarielles Online-Verfahren
	<ul style="list-style-type: none"> • Notarident • Gerichtident • Rechtsanwaltskammerident • RA-Ident 	<ul style="list-style-type: none"> • eIDent
Nachname	m	m (Minimumset)
Vornamen	m	m (Minimumset)
Geburtsname	o	o
Dr.-Titel	o	m (falls vorhanden)
Geburtsdatum	m	m (Minimumset)
Geburtsort	m	o
Meldeadresse (Straße, Hausnummer, PLZ, Ort)	-*	-/o (abhängig vom eID-Datensatz des ausstellenden Landes)
Staatsangehörigkeit	o	-
Ausweisart	m	- (impliziert)
Ausweisnummer	m	-
Ausstellungsdatum	m	-
Ablaufdatum	m	m
Unique Identifier (inkl. "Ausstellender Staat")	-	m (Minimumset)

Foto (nachgelagert im Rahmen des notariellen Online Verfahrens gemäß §16c BeurkG)	-	m (elektronisch aus dem Ausweis ausgelesen)
Zusätzliche Identitätsattribute (Prüfung durch bestätigende Stelle)		
berufsbezogenes Attribut (Notar, Notarvertreter, Justizangehöriger, ÖbVI etc.)	p	-

Die Auswahl der mandatorischen Attribute stellt sicher, dass die Personen eindeutig identifiziert wird. Im Rahmen der Verfahren Notarident, Gerichtident, Rechtsanwaltskammerident und RA-Ident können Pseudonyme für die Zertifikate für die Fernsignatur beantragt werden. Der Ablauf der Verfahren bleibt unberührt.

Legende

Erforderlichkeit		verwendetes Mittel/Validierung**	
m	<i>mandatorisch</i>		<i>Lichtbilddokument</i>
o	<i>optional</i>		<i>eID Verfahren</i>
-	<i>keine Aufnahme</i>		<i>ergänzende Dokumente</i>
p	<i>produktabhängig</i>		<i>Register</i>
			<i>sonstige Verfahren</i>

*Weitere erforderliche Daten, wie beispielsweise die Meldeadresse werden für die Auftragsabwicklung erhoben, sind aber nicht Bestandteil der Identifizierungs- und Validierungsprozesse.

**Ausführungen siehe Abschnitt "Mittel, die zur Validierung von Identitätsattributen verwendet werden"

Identitätsprüfungskontexte und Attribute für **juristische Personen**:

Attribute*	Fernsiegel
vollständiger Name der juristischen Person	m
Land der Registrierung der juristischen Person	m

Zusätzliche Identitätsattribute im Rahmen der Prüfung der vertretenden natürlichen Person	
	siehe Identifizierungsverfahren bei "Fernsignatur"

Die Auswahl der mandatorischen Attribute stellt sicher, dass die Personen eindeutig identifiziert wird.

Legende

Erforderlichkeit		verwendetes Mittel/Validierung**	
m	<i>mandatorisch</i>		<i>Lichtbilddokument</i>
o	<i>optional</i>		<i>eID Verfahren</i>
-	<i>keine Aufnahme</i>		<i>ergänzende Dokumente</i>
p	<i>produktabhängig</i>		<i>Register</i>
			<i>sonstige Verfahren</i>

*Weitere erforderliche Daten, wie beispielsweise die Adresse werden für die Auftragsabwicklung erholen sind aber nicht Bestandteil der Identifizierungs- und Validierungsprozesse.

** Ausführungen siehe Abschnitt "Mittel, die zur Validierung von Identitätsattributen verwendet werden"

d. Mittel, die zur Validierung von Identitätsattributen verwendet werden

Die in den Tabellen dieses Abschnitts dargestellten Farben veranschaulichen, welche Mittel, zur Validierung der Identitätsattribute verwendet werden. Im Folgenden werden die Mittel und Rahmenbedingungen ausführlich dargestellt.

	<p>Manueller Abgleich mit dem originalen, gültigen und zuverlässigen Lichtbilddokumenten. Zulässig sind:</p> <ul style="list-style-type: none"> • Personalausweis oder elektronischer Aufenthaltstitel der Bundesrepublik Deutschland mit elektronischer Ausweisfunktion, • Reisepass, der auf eine Person mit Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes ausgestellt worden ist, • Dokumente oder geeignete technische Verfahren mit gleichwertiger Sicherheit zu einer Identifizierung wie die in den vorstehenden Absätzen genannten Dokumente. Gesetzlich anwendbare Regelungen sind den Verfahrensbeschreibungen im Folgenden zu entnehmen bspw. § 40 BeurkG bei NotraIDENT oder § 34VwVfG für Gerichtident
--	---

	<p>Automatisiertes Erfassen über notifizierte eID Verfahren mit dem Sicherheitsniveau "hoch". Der genutzte Dienst ist BSI TR-03130 konform.</p> <p>Zulässige Dokumente sind:</p> <ul style="list-style-type: none"> • Personalausweise und elektronischen Aufenthaltstitel, die NACH dem 1.8.2021 ausgestellt wurden. • Gültige Reisepässe vieler Staaten, sofern technisch nach allen Anforderungen validiert werden können. <p>Es wird ein Authentifizierungsprotokoll ausgeführt, das bestätigt, dass der Inhaber der eID erfolgreich authentifiziert wurde und dass die verwendete eID gültig ist (nicht abgelaufen, gesperrt oder widerrufen).</p>
	<p>Abgleich mit gültigem, zulässigem, ergänzendem Dokument, das einschließlich des jeweiligen Ausstellers bzw. der Quelle dieser Nachweise dokumentiert wird:</p> <ul style="list-style-type: none"> • Amtlicher Handelsregisterauszug (nicht älter als 4 Wochen) • Beglaubigter Satzungsbeschluss • Notarielle Bescheinigung gem. § 21 i.V.m. § 24 BNotO (sog. Vertretungs- und Registerbescheinigung) • Amtliche Bescheinigung der übergeordneten Behörde (Fachaufsichts- oder Rechtsaufsichtsbehörde) • Beglaubigte Kopie der Promotionsurkunde, sofern Titel nicht im Ausweisdokument vorhanden
	<p>verpflichtender Abgleich mit Register: automatisierter Abruf aus dem Notarverzeichnis gemäß § 78I der Bundesnotarordnung (NVZ)</p>
	<p>sonstiges Verfahren</p>

e. Validierung der Mittel und Attribute

Je nach Identitätsprüfungsverfahren müssen mindestens alle mandatorischen Attribute erfasst sein. Alle Attribute müssen erfolgreich validiert sein, um den Prozess erfolgreich zu durchlaufen.

Im Rahmen des Identitätsprüfungsverfahrens wird die jeweilige Echtheit, Gültigkeit und Integrität aller Nachweise validiert, d. h. es wird sichergestellt, dass die Nachweise echt und gültig sind und in ihrer ursprünglichen Form vorgelegt werden. Dabei werden insbesondere Abbildungen von Musterdokumenten zum visuellen Abgleich genutzt und Sicherheitsmerkmale von Dokumenten überprüft. Die prüfenden Personen haben Zugriff auf entsprechende Referenzinformationen, z.B. auf das öffentliche Online-Register echter Identitäts- und Reisedokumente. Bei elektronischen Dokumenten werden außerdem vorhandene Signaturen oder Siegel überprüft. Verfahrensspezifische Prüfungen sind den Verfahrensbeschreibungen unter 3.2 zu entnehmen. Nur zweifelsfrei validierte Nachweise aus zuverlässigen Quellen werden akzeptiert und führen zur Fortsetzung des Prozesses. Nicht in diesem Sinne validierte Nachweise führen zu einem Abbruch des Prozesses. Der Prozess stellt sicher, dass die Aktualität der geprüften Nachweise zum Zeitpunkt der Ausstellung der Zertifikate und Siegel gewährleistet ist. Die Validierung wird dokumentiert.

II. Geltungsbereich und Konformität

Der Identitätsprüfungsdienst wird ausschließlich zur Unterstützung der Ausstellung qualifizierter Zertifikate gemäß eIDAS genutzt.

Die eingesetzten Identifizierungsverfahren für qualifizierte Zertifikate für natürliche Personen (Signaturzertifikate) sowie juristische Personen (Siegelzertifikate) erfüllen das Vertrauensniveau „Extended“ (LoIP Extended) gemäß ETSI TS 119 461 und ETSI TS 119 641.

Die Zuordnung der jeweiligen Verfahren zu LoIP Extended ergibt sich aus der Umsetzung der in Abschnitt I beschriebenen Identitätsprüfungskontexte, Validierungsmaßnahmen und Kontrollmechanismen.

Eine formale Konformitätserklärung nach ETSI TS 119 461-1 wird für die in Abschnitt A.3 beschriebenen Verfahren abgegeben, soweit diese im jeweiligen Anwendungsfall eingesetzt werden.

III. Anwendungsfälle und Identifizierungsverfahren

Die folgenden Identifizierungsverfahren werden als Identitätsprüfungs-Use-Cases im Sinne der ETSI TS 119 461-1 angewendet:

a. Identifizierung bei physischer Anwesenheit

Die Identifizierung erfolgt durch persönlich anwesende Antragsteller gegenüber einem autorisierten Mitarbeiter (z. B. RA-Mitarbeiter, Notar, Gericht, Kammer). Dabei werden gültige amtliche Ausweisdokumente geprüft, die Identität festgestellt und der Identifizierungsvorgang dokumentiert.

Dieses Verfahren entspricht einem Identitätsprüfungs-Use-Case mit physischer Präsenz und erfüllt das LoIP Extended.

b. Identifizierung durch bestätigende Stellen

Bei der Identifizierung durch Notare, Gerichte oder Kammern wird die Identität des Antragstellers durch eine hierfür gesetzlich oder organisatorisch befugte Stelle bestätigt. Die Bestätigung erfolgt schriftlich oder elektronisch und basiert auf einer zuvor durchgeführten Identitätsprüfung.

Dieses Verfahren erfüllt die Anforderungen an eine starke Identitätsprüfung und wird dem LoIP Extended zugeordnet.

c. Elektronische Identifizierung (eID)

Sofern eine Identifizierung mittels staatlich anerkannter elektronischer Identitätsmittel (z. B. Personalausweis mit eID-Funktion) mit dem Vertrauensniveau „hoch“ erfolgt, wird das Verfahren dem LoIP Extended gemäß ETSI TS 119 461 zugeordnet.

IV. Risikoanalyse und Bedrohungsmanagement

Der Identitätsprüfungsdienst verfügt über ein dokumentiertes und wirksames Verfahren für Bedrohungsinformationen, das sicherstellt, dass der Dienst an neue Bedrohungen angepasst wird und von qualifiziertem Personal durchgeführt wird. Für den Identitätsprüfungsdienst wird eine dokumentierte Risikoanalyse durchgeführt. Diese berücksichtigt insbesondere Risiken der Falschakzeptanz, Risiken der Falschrückweisung, Missbrauch von Ausweisdokumenten, Insider-Risiken sowie IT- und Informationssicherheitsrisiken.

Die Risikoanalyse wird mindestens jährlich sowie anlassbezogen bei wesentlichen Änderungen der Verfahren, der Bedrohungslage oder der eingesetzten Systeme aktualisiert.

Zur Erkennung neuer Bedrohungen werden Informationen aus geeigneten Quellen ausgewertet. Erkenntnisse aus diesen Quellen fließen in die Risikoanalyse und gegebenenfalls in Anpassungen der Prozesse ein.

V. Qualifikation und Schulung des Personals

Die an der Identitätsprüfung beteiligten RA-Mitarbeiter werden vor Aufnahme ihrer Tätigkeit sowie regelmäßig geschult. Die Schulungen umfassen insbesondere die Erkennung gültiger und ungültiger Ausweisdokumente, die Prüfung von Sicherheitsmerkmalen, das Erkennen von typischen Betrugsmustern, datenschutz- und sicherheitsrelevante Anforderungen sowie Dokumentations- und Nachweispflichten.

Der Schulungsbedarf wird im Rahmen der Risikoanalyse überprüft und bei Bedarf angepasst.

VI. Qualitäts- und Sicherheitsziele

Für den Identitätsprüfungsdienst werden qualitative Ziele festgelegt, insbesondere zur Minimierung von Falschakzeptanzen und Falschrückweisungen.

Die Einhaltung dieser Ziele wird regelmäßig überprüft, unter anderem durch Stichprobenkontrollen, Anwendung des Vier-Augen-Prinzips bei kritischen Prozessschritten sowie durch Auswertung von Fehler- und Korrekturstatistiken.

Erkannte Abweichungen führen zu Korrektur- und Verbesserungsmaßnahmen.

VII. Nachweise und Dokumentation der Identitätsprüfung

Für jeden Identifizierungsprozess werden geeignete Nachweise erhoben und gespeichert.

Diese umfassen je nach Verfahren insbesondere Kopien oder Scans der geprüften Identitätsdokumente, Angaben zur prüfenden Person und zur prüfenden Stelle, Datum und Abschlusszeitpunkt der Identitätsprüfung sowie das Ergebnis der Identitätsprüfung.

Die Nachweise werden gegen unbefugte Veränderung geschützt gespeichert.

Der Abschluss des Identifizierungsprozesses wird eindeutig dokumentiert, sodass eine nachträgliche Überprüfung möglich ist.

Die Aufbewahrung der Nachweise erfolgt entsprechend den gesetzlichen und regulatorischen Vorgaben, insbesondere § 16 Abs. 4 VDG i.V.m. Art. 24 Abs. 2h eIDAS-VO.

VIII. Datenschutz und Vertraulichkeit

Personenbezogene Daten aus der Identitätsprüfung werden ausschließlich zum Zweck der Zertifikatsbeantragung und -verwaltung verarbeitet.

Der Zugriff auf diese Daten ist auf befugte Personen beschränkt. Es gelten die Datenschutzregelungen, dieses CPS sowie die einschlägigen gesetzlichen Vorschriften.

IX. Überprüfung und Weiterentwicklung

Die Regelungen dieses Anhangs werden regelmäßig überprüft und bei Bedarf aktualisiert, insbesondere bei Änderungen der ETSI-Normen, der eingesetzten Identifizierungsverfahren oder der rechtlichen Rahmenbedingungen.

<https://zertifizierungsstelle.bnotk.de/>

