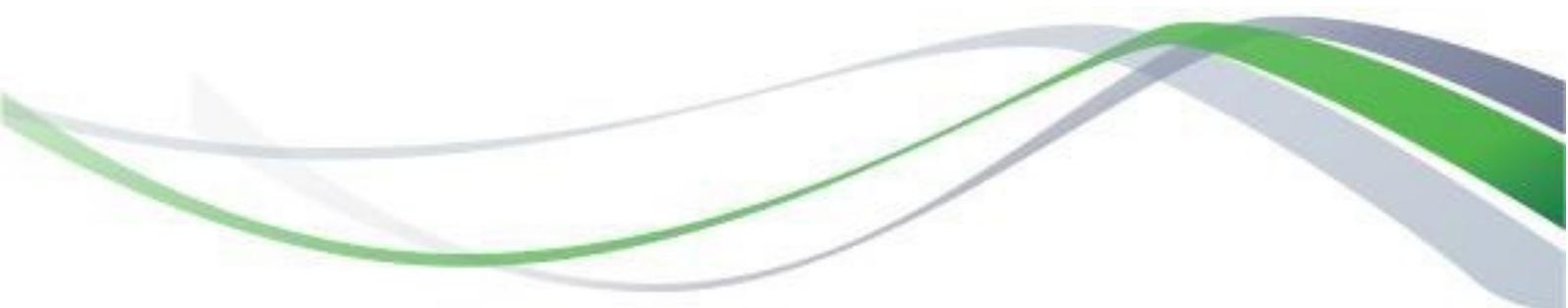


# Zertifizierungskonzept der Zertifizierungsstelle der Bundesnotarkammer für qualifizierte Zertifikate



**Version:** 3.4  
**Datum:** 25. Juli 2024

## 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 Parlamentes und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG ( <b>eIDAS-Verordnung</b> ) 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 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 nach Einführung 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

# Inhalt

1	Einleitung .....	8
1.1	Überblick .....	8
1.1.1	Über dieses Dokument .....	8
1.1.2	Eigenschaften der PKI der Zertifizierungsstelle der Bundesnotarkammer .....	9
1.2	Name und Kennzeichnung des Dokuments .....	11
1.3	PKI-Teilnehmer .....	11
1.4	Verwendung von Zertifikaten .....	11
1.4.1	Verwendung von Dienstzertifikaten .....	11
1.5	Verwaltung des Zertifizierungskonzepts .....	12
1.6	Definitionen und Abkürzungen .....	12
2	Verantwortlichkeit für Verzeichnisse und Veröffentlichungen .....	13
2.1	Verzeichnisse .....	13
2.2	Veröffentlichung von Informationen zu Zertifikaten .....	13
2.3	Zeitpunkt und Häufigkeit von Veröffentlichungen .....	13
2.4	Zugang zu den Informationen .....	13
3	Identifizierung und Authentifizierung .....	14
3.1	Namensregeln .....	14
3.1.1	Arten von Namen .....	14
3.1.2	Aussagekraft von Namen .....	14
3.1.3	Pseudonyme .....	14
3.1.4	Regeln für die Interpretation verschiedener Namensformen .....	14
3.1.5	Eindeutigkeit von Namen .....	14
3.1.6	Anerkennung, Authentifizierung und die Rolle von Markennamen .....	15
3.1.7	Test-Zertifikate .....	16
3.2	Identifizierung der Zertifikatsinhaber .....	16
3.2.1	Identifizierungsverfahren der Antragsteller .....	17
3.2.2	Identifizierung bei Erweiterungen und Beschränkungen im Zertifikat .....	25
3.3	Identifizierung und Authentifizierung bei Anträgen auf Schlüsselerneuerung (re-keying) .....	27
3.4	Identifizierung und Authentifizierung bei Stellung eines Widerrufsverlangens .....	27
4	Betriebsanforderungen .....	29
4.1	Zertifikatsantrag .....	29
4.2	Verarbeitung des Zertifikatsantrags .....	29
4.2.1	Durchführung der Identifizierung und Authentifizierung .....	29

4.2.2	Annahme oder Ablehnung des Antrags.....	30
4.3	Ausstellung von Zertifikaten .....	31
4.3.1	Vorgehen der CA bei der Ausstellung des Zertifikats .....	31
4.3.2	Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats .....	31
4.4	Zertifikatsübergabe .....	31
4.4.1	Verhalten bei der Zertifikatsübergabe .....	31
4.4.2	Veröffentlichung des Zertifikats durch den VDA BNotK.....	32
4.4.3	Benachrichtigung Dritter über die Erstellung des Zertifikats .....	32
4.5	Verwendung des Schlüsselpaars und des Zertifikats .....	34
4.5.1	Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber oder Zeichnungsberechtigten .....	34
4.5.2	Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsinhaber.....	36
4.6	Zertifikatserneuerung (certificate renewal) .....	36
4.7	Zertifikatserneuerung mit Schlüsselerneuerung .....	36
4.8	Zertifikatsänderung .....	36
4.9	Widerruf und Suspendierung von Zertifikaten .....	36
4.9.1	Bedingungen für einen Widerruf .....	36
4.9.2	Widerrufsberechtigte .....	38
4.9.3	Verfahren zur Stellung eines Widerrufsverlangens .....	38
4.9.4	Fristen für ein Widerrufsverlangen .....	40
4.9.5	Zeitspanne für die Bearbeitung des Widerrufsverlangens .....	40
4.9.6	Methoden zum Prüfen von Widerrufsinformationen.....	40
4.9.7	Häufigkeit der Veröffentlichung von Widerrufslisten .....	40
4.9.8	Maximale Latenzzeit für Widerrufslisten .....	40
4.9.9	Online-Verfügbarkeit von Widerrufsinformationen .....	40
4.9.10	Notwendigkeit zur Online-Prüfung von Widerrufsinformationen .....	41
4.9.11	Andere Formen zur Anzeige von Widerrufsinformationen.....	41
4.9.12	Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels .....	41
4.9.13	Suspendierung des Zertifikats .....	41
4.10	Statusabfragedienst .....	41
4.11	Beendigung des Zertifizierungsdienstes.....	41
4.12	Schlüsselhinterlegung und –wiederherstellung .....	41
5	Nicht-technische Sicherheitsmaßnahmen.....	42
5.1	Bauliche Sicherheitsmaßnahmen .....	42
5.2	Verfahrensvorschriften.....	43
5.2.1	Rollenkonzept.....	43

5.2.2	Vier-Augen-Prinzip .....	43
5.2.3	Sonstige Dienstanweisung .....	43
5.3	Personalkonzept.....	43
5.3.1	Qualifikation, Erfahrung und Zuverlässigkeit des Personals.....	43
5.3.2	Sicherheitsüberprüfung.....	44
5.3.3	Schulungen und Weiterbildungen.....	44
5.3.4	Rollenbesetzung, Rollenentzug und Rollenwechsel .....	44
5.3.5	Anforderungen an externes Personal.....	45
5.3.6	Sanktionen bei unerlaubten Handlungen.....	45
5.3.7	Dokumentation .....	45
5.4	Protokollierung von Überwachungsmaßnahmen.....	45
5.4.1	Überwachung des Zutritts.....	45
5.4.2	Überwachung von organisatorischen Maßnahmen .....	45
5.5	Archivierung von Unterlagen .....	46
5.5.1	Arten von Unterlagen .....	46
5.5.2	Aufbewahrungszeiten .....	46
5.5.3	Archivsicherheit.....	46
5.5.4	Datensicherung des Archivs .....	47
5.5.5	Anforderungen an die Zeitstempel der archivierten Protokolle .....	47
5.5.6	Ort der Archivierung .....	47
5.6	Umstellung des Schlüssels (key changeover).....	47
5.7	Notfallkonzept.....	47
5.7.1	Behandlung von Vorfällen.....	47
5.7.2	Wiederherstellung von IT-Systemen .....	47
5.7.3	Wiederherstellung nach Kompromittierung von privaten CA-Schlüsseln .....	47
5.7.4	Weiterführung des Betriebs nach Kompromittierung oder Katastrophenfall .....	48
5.8	Beendigung des Zertifizierungsbetriebs .....	48
6	Technische Sicherheitsmaßnahmen .....	50
6.1	Erzeugung und Installation von Schlüsselpaaren.....	50
6.1.1	Erzeugung von Schlüsselpaaren .....	50
6.1.2	Auslieferung der privaten Schlüssel für Zertifikatsteilnehmer .....	50
6.1.3	Auslieferung der öffentlichen Schlüssel an die CA .....	50
6.1.4	Auslieferung der öffentlichen CA-Schlüssel .....	50
6.1.5	Schlüssellängen .....	51
6.1.6	Schlüsselparameter und Qualitätskontrolle der Parameter .....	51
6.1.7	Schlüsselverwendung .....	51

6.2	Sicherung des privaten Schlüssels und kryptographisches Modul.....	51
6.2.1	Standards und Sicherheitsmaßnahmen .....	51
6.2.2	Mehraugenprinzip bei der Schlüsselaktivierung.....	52
6.2.3	Schlüsselwiederherstellung .....	52
6.2.4	Schlüsselbackup .....	52
6.2.5	Schlüsselarchivierung .....	52
6.2.6	Schlüsseltransfer .....	52
6.2.7	Schlüsselspeicherung.....	52
6.2.8	Aktivierung privater Schlüssel .....	52
6.2.9	Deaktivierung privater Schlüssel .....	52
6.2.10	Zerstörung privater Schlüssel.....	53
6.2.11	Beschreibung der kryptografischen Module .....	53
6.3	Weitere Aspekte der Verwaltung des Schlüsselpaars .....	53
6.3.1	Archivierung der öffentlichen Schlüssel .....	53
6.3.2	Gültigkeitsdauer von Schlüssel und Zertifikaten.....	53
6.4	Aktivierungsdaten .....	53
6.4.2	Schutz von Signatur- und Siegelerstellungsdaten .....	54
6.4.3	Weitere Aspekte der Aktivierungsdaten .....	54
6.5	Computersicherheit.....	54
6.6	Technische Kontrolle während des Lebenszyklus .....	55
6.6.1	Sicherheitsmaßnahmen beim Aufbau, der Entwicklung und Erweiterung der IT- Systeme und Softwarekomponenten.....	55
6.6.2	Sicherheitsmaßnahmen beim Betrieb .....	56
6.7	Netzwerksicherheit .....	57
6.8	Zeitstempel .....	58
7	Profile von Zertifikaten, Widerruflisten und OCSP.....	59
7.1	Zertifikatsprofile .....	59
7.1.1	Root-CA .....	59
7.1.2	Sub-CA .....	62
7.1.3	Endanwenderzertifikatsprofil.....	65
7.2	Widerruflistenprofile .....	74
7.3	Profile des Statusabfragedienstes .....	74
7.3.1	Versionsnummer .....	75
7.3.2	OCSP-Erweiterungen .....	75
8	Konformitätsprüfung .....	75
9	Sonstige geschäftliche und rechtliche Regelungen .....	75

# 1 Einleitung

## 1.1 Überblick

### 1.1.1 Über dieses Dokument

Die Bundesnotarkammer ist qualifizierter Vertrauensdiensteanbieter i. S. d. Art. 3 lit. 20 der eIDAS-Verordnung (EU) Nr. 910/2014. Angebotene Vertrauensdienste sind qualifizierte Zertifikate für elektronische Signaturen für natürliche Personen (QCP-n-qscd), qualifizierte Zertifikate für elektronische Siegel für juristische Personen (QCP-l-qscd) und qualifizierte elektronische Zeitstempel. Die Nutzung der qualifizierten Zertifikate erfordert den Einsatz einer qualifizierten elektronischen Signaturerstellungseinheit (**QSCD**) oder qualifizierten Siegelerstellungseinheit (QSCD).

Dieses ist das Zertifizierungskonzept der Zertifizierungsstelle der Bundesnotarkammer (**VDA BNotK**) für qualifizierte Zertifikate für elektronische Signaturen und elektronische Siegel (die **qualifizierten Zertifikate** bzw. das **qualifizierte Zertifikat**) in Form eines Certificate Practice Statement (**CPS**) und stellt die Anforderungen der Zertifizierungsstelle der Bundesnotarkammer an und das Verfahren bei der Ausgabe, Verwaltung, Widerruf sowie Erneuerung der von ihr ausgegebenen qualifizierten Zertifikate dar. Nicht-qualifizierte Zertifikate sind nicht erfasst.

Das Zertifizierungskonzept nimmt Bezug auf die Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer mit dem OID 1.3.6.1.4.1.41460.5.1.1.1.2 sowie die ETSI Normen EN 319 401, EN 319 411-1 und EN 319 411-2. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen.

Dieses Zertifizierungskonzept wird auf der Website des VDA BNotK unter folgendem Link veröffentlicht: <https://zertifizierungsstelle.bnotk.de/veroeffentlichungen>.

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

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.

Dieses Zertifizierungskonzept ist nicht rechtsverbindlich. Für das Verhältnis zwischen VDA BNotK und dem Zertifikatsinhaber bzw. dem Vertrauenden Dritten sind vielmehr 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 der Zertifizierungsstelle der Bundesnotarkammer

### PKI für qualifizierte Vertrauensdienste

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

### RSA-Algorithmus

Aktiv

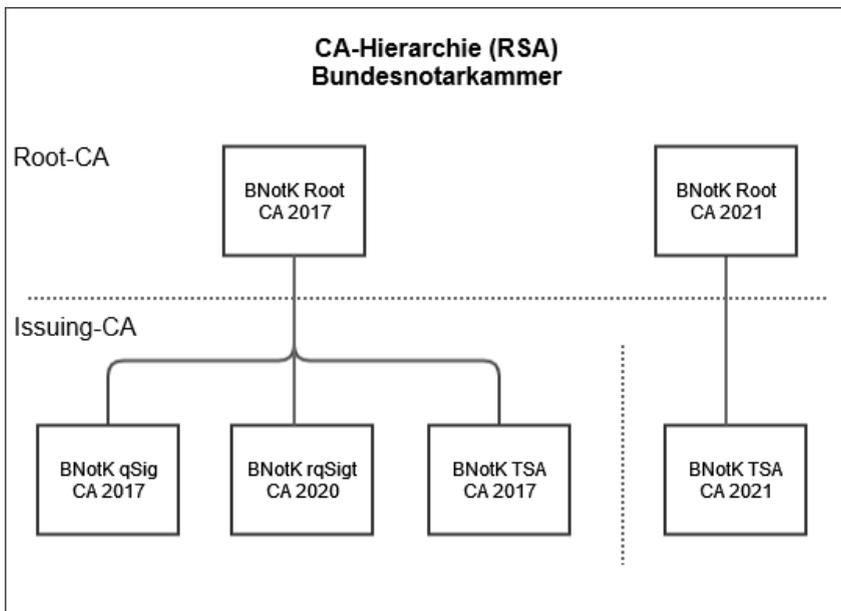


Abbildung 1: aktive PKI Hierarchie für qual. Signaturzertifikate für natürliche Personen und qual. Zeitstempel mit RSA

In Planung

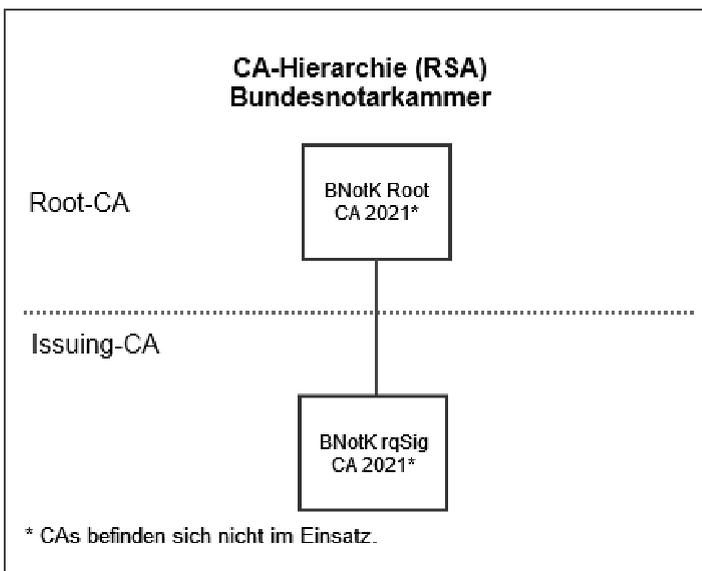


Abbildung 2: geplante PKI Hierarchie für qual. Signaturzertifikate für natürliche Personen mit RSA

## Elliptic Curve

Aktiv

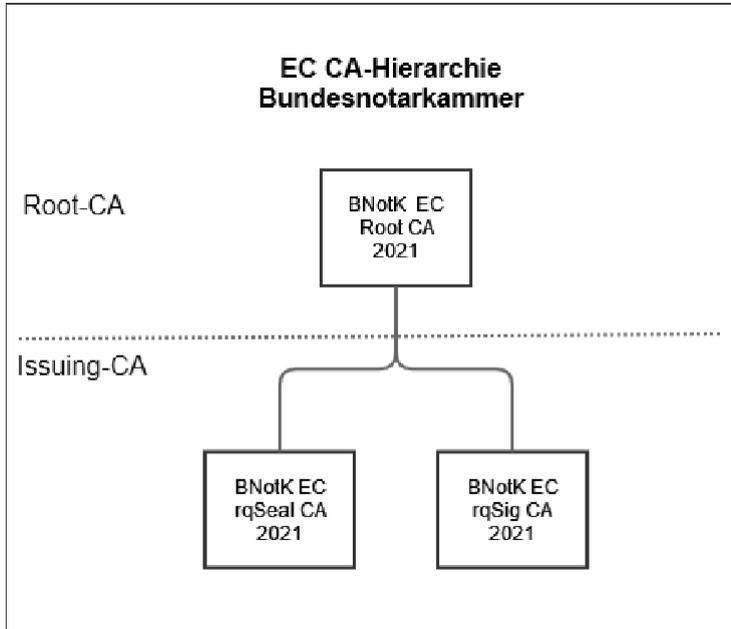


Abbildung 3: aktive PKI Hierarchie für qual. Signaturzertifikate für natürliche und juristische Personen mit Elliptic Curve

In Planung

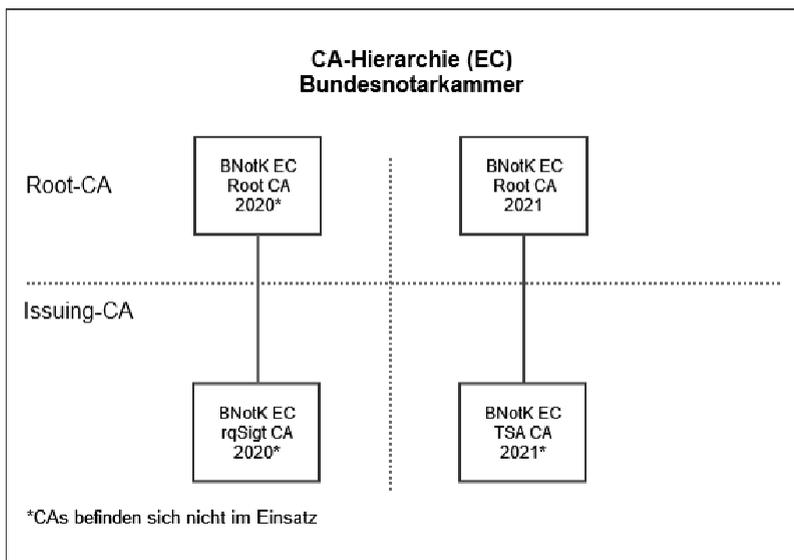


Abbildung 4: geplante PKI Hierarchie für qual. Zertifikate für natürliche Personen und qual. Zeitstempel mit Elliptic Curve

## 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

Dokumentenname: Zertifizierungskonzept der Zertifizierungsstelle der Bundesnotarkammer

Kennzeichnung (OID): 1.3.6.1.4.1.41460.5.2.1.1.2

Version: 3.4

### 1.3 PKI-Teilnehmer

Siehe Abschnitt 1.3 der Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bundesnotarkammer.

### 1.4 Verwendung von Zertifikaten

Zertifikatsinhaber dürfen die vom VDA BNotK ausgegebenen qualifizierten Zertifikate nur für eigene berufliche Zwecke für qualifizierte elektronische Signaturen 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 ist ein (remote-)QSCD erforderlich. Ferner unterliegt der Zertifikatsinhaber den sich aus den gesetzlichen Regelungen ergebenden Pflichten sowie ggf. weitergehenden oder abweichenden Pflichten aufgrund einzelvertraglicher Regelung.

#### 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 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. Zuständig ist der Leiter der Zertifizierungsstelle der Bundesnotarkammer oder, wenn dieser verhindert ist, sein designierter Stellvertreter. Im Falle einer Änderung wird die geänderte Fassung unverzüglich auf der Internetseite des VDA BNotK veröffentlicht. Sind gravierende Änderungen an den Inhalten des Zertifizierungskonzeptes geplant, werden diese kenntlich gemacht und im Repository veröffentlicht.

Eine Änderung des Zertifizierungskonzepts kann ausschließlich der Leiter der Zertifizierungsstelle der Bundesnotarkammer oder, wenn dieser verhindert ist, sein designierter Stellvertreter vornehmen. Gemäß einer entsprechenden betrieblichen Anweisung werden Änderungen nur bei Freigabe des Leiters der Zertifizierungsstelle der Bundesnotarkammer oder, wenn dieser verhindert ist, seines designierten Stellvertreters veröffentlicht. Die Änderung wird durch die Vergabe einer neuen Versionsnummer kenntlich gemacht.

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

Zertifizierungsstelle der Bundesnotarkammer  
z.H. Leiter der Zertifizierungsstelle  
Burgmauer 53  
50667 Köln

Tel.: +49 (2 21) 27 79 35-0  
Fax: +49 (2 21) 27 79 35-20  
E-Mail: [zs@bnotk.de](mailto:zs@bnotk.de)

## 1.6 Definitionen und Abkürzungen

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

## 2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

### 2.1 Verzeichnisse

Siehe Abschnitt 2.1 der Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bundesnotarkammer.

### 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) der Zertifizierungsstelle der Bundesnotarkammer.

## 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. Pseudonyme werden innerhalb des Anwenderkreises des VDA BNotK nur einmal vergeben.

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-n-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 Test-Zertifikate

Der VDA BNotK behält sich das Recht vor, in Ausnahmefällen Testzertifikate auszustellen, deren Nutzung für Testzwecke (z.B. Integration, Schulung) notwendig ist. Die Anzahl ausgegebener Testzertifikate ist gering zu halten. Die Test-Zertifikate 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. Für Test-Zertifikate natürlicher Personen gilt ebenfalls, dass diese stets den vollständigen und korrekt durchgeführten Antragsprozess des VDA BNotK einschließlich aller Dokumentation durchlaufen.

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

## 3.2 Identifizierung der Zertifikatsinhaber

- Qualifizierte Zertifikate für natürliche Personen (für qualifizierte Signaturen)

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.

Erforderlich ist mindestens die Feststellung des vollständigen Namens, des Geburtsdatums und der Ausweisdaten des Antragstellers. Zudem muss der Antragsteller seine Anschrift und eine E-Mail-Adresse angeben.

Die Identifizierung erfolgt grundsätzlich anhand der folgenden Dokumente:

- ▶ Personalausweis der Bundesrepublik Deutschland,
- ▶ 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.

Eine Identifizierung ist notwendig, wenn der Zertifikatsinhaber bisher noch nicht identifiziert wurde oder die der Identifizierung zu Grunde liegenden Daten sich geändert haben (beispielsweise bei einer Änderung des Namens des Zertifikatsinhabers).

- Qualifizierte Zertifikate für juristische Personen (für qualifizierte Siegel)

Der VDA BNotK hat bei der Beantragung qualifizierter Siegelzertifikate sowohl die Organisation als Zertifikatsinhaber als auch die natürliche Person, die die Organisation vertritt und als Antragsteller fungiert, eindeutig zu identifizieren. Dabei werden nur die relevanten Informationen erfasst, die für die Bereitstellung der vom VDA BNotK angebotenen Vertrauensdienste erforderlich sind.

Die Identifizierung des vertretungsberechtigten Antragstellers erfolgt auf die gleiche Weise, wie bei der Identifizierung einer natürlichen Person für qualifizierte Signaturzertifikate.

Erforderlich für die Identifizierung der Organisation ist mindestens der amtliche Organisationsname, der Organisationssitz in Deutschland sowie die entsprechend der Gesellschaftsform zu erbringenden Bescheinigungen für den Organisationsnachweis und die 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 (Fachaufsichts- oder Rechtsaufsichtsbehörde)

Eine Identifizierung ist notwendig, wenn der Zertifikatsinhaber bisher noch nicht identifiziert wurde oder die der Identifizierung zu Grunde liegenden Daten sich geändert haben (beispielsweise bei einer Änderung des Namens des Zertifikatsinhabers)

### 3.2.1 Identifizierungsverfahren der Antragsteller

- 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 Verfahrens RA-Ident 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 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 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 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.

### 3.2.1.2 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 Gerichtes 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 (unterschiedenen bzw. noch zu unterschreibenden) Antragsunterlagen und Beglaubigung der Unterschrift des Antragstellers auf dem Antragsformular i.S.d. § 34VwVfG BeurkG.;
- ▶ 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 – beigefügt, 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 Gerichtes 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 (unterschiedenen bzw. noch zu unterschreibenden) Antragsunterlagen und Beglaubigung der Unterschrift des Antragstellers auf dem Antragsformular i.S.d. § 34VwVfG BeurkG.;
- ▶ 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 – beigefügt, sofern sie nicht unmittelbar von der bestätigenden Stelle übersandt wird.

### 3.2.1.3 Verfahren Rechtsanwaltskammerident

Die Identifizierung des Antragstellers kann ggf. auch anhand der Identifizierung durch einen Mitarbeiter der deutschen Rechtsanwaltskammer – z.B. bei der Vereidigung nach § 12a BRAO – erfolgen.

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 Verteidigung eingesetzt wird, am Kammerident-Verfahren teilnimmt.

#### 3.2.1.4 Verfahren eIDent

Bei der Identifizierung mittels elektronischen Identitätsnachweises erfolgt die Identifizierung während der Online-Eingabe der Antragsdaten und der Übermittlung dieser in das RA-System. Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des Ausweisdokumentes/eID-Token über die sichere eID-Infrastruktur. Der Nachweis des Identifizierungsvorgangs wird mit den Antragsdaten dokumentiert.

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

#### 3.2.1.5 Verfahren RA-Ident

- Qualifizierte Zertifikate für natürliche Personen (für qualifizierte Signaturen)

Antragsteller, die Mitarbeiter der Bundenotarkammer K. d. ö. R. sind, können durch einen RA-Mitarbeiter identifiziert werden. Die Online-Eingabe der Antragsdaten und/oder dessen Identifizierung werden in der Regel unmittelbar beim Antragsteller oder in den Räumlichkeiten des VDA BNotK vorgenommen.

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 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 übergeben. Es kann grundsätzlich von jedem beliebigen Computer-Arbeitsplatz mit Internetanschluss durchgeführt werden, an den ein Chipkartenleser und ein Drucker/Scanner angeschlossen sind.

- 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 Online-Eingabe der Antragsdaten und/oder dessen Identifizierung werden in der Regel unmittelbar beim Antragsteller oder in den Räumlichkeiten des VDA BNotK vorgenommen.

- ▶ 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 übergeben.

### 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 Ausgabe von qualifizierten Zertifikaten, die entsprechende Attribute enthalten, erfolgt nur, wenn die Bestätigung der zuständigen Stelle vorliegt. Zu diesem Zweck wird dem Antragsteller im Anschluss an seinen Zertifikatsantrag ein entsprechender Vordruck zum Ausdruck bereitgestellt, verbunden mit der Aufforderung, dies der zuständigen Stelle zuzuleiten.

#### 3.2.2.1 Aufführung amts- und berufsbezogener oder sonstiger Angaben

Sofern ein Antragsteller die Aufnahme einer amts- und berufsbezogenen oder einer sonstigen Angabe als Attribut beantragt hat, bestätigt die zuständige Stelle, dass der Antragsteller berechtigt ist, die amts- und berufsbezogene oder die sonstige Angabe zu verwenden und sendet die Bestätigung postalisch an die RA des VDA BNotK. Die bestätigende Stelle weist ihre Berechtigung durch entsprechende Unterlagen (z. B. Handelsregisterauszug) nach.

Die Bestätigungsformulare werden nebst den weiteren Antragsunterlagen vom RA-Mitarbeiter im Rahmen der Antragsprüfung geprüft. Darüber hinaus werden die Bestätigungen dokumentiert.

Eine Besonderheit gilt für die Einholung der Bestätigung bei der Aufnahme von Notarattributen. Um Einholung von Bestätigungen für beantragte Notarattribute in jedem Einzelfall zu vermeiden, greift VDA BNotK auf der Grundlage schriftlicher Vereinbarungen mit den regionalen Notarkammern bei der Prüfung von beantragten Notarattributen auf das bei der Bundesnotarkammer geführte Notarverzeichnis als vertrauenswürdige Notardatenbank zurück. Die Prüfung der Zulässigkeit eines beantragten Notarattributs erfolgt in diesem Fall in der Weise, dass das Antragssystem grundsätzlich nur Zertifikatsanträge mit Notarattribut zulässt, wenn die

entsprechende Berechtigung zur Führung eines solchen Notarattributs sich bereits bei der Antragstellung aus dem Notarverzeichnis ergibt.

Hinweis: Amts-, berufsbezogene oder sonstige Angaben sind für qualifizierte Zertifikate für juristische Personen (Siegelzertifikate) ausgeschlossen.

### 3.2.2.2 Aufführung einer Vertretungsmacht für eine dritte Person

Sofern ein Antragsteller die Aufnahme der Vertretungsmacht für eine dritte Person beantragt hat, muss dem VDA BNotK die Einwilligung der dritten Person nachgewiesen werden. Bei einer juristischen Person (des öffentlichen oder privaten Rechts) bestätigt der Vertreter der juristischen Person, dass der Antragsteller über die beantragte Vertretungsmacht verfügt, und sendet die Bestätigung postalisch an den VDA BNotK. Der Vertreter der juristischen Person weist seine Berechtigung durch entsprechende Unterlagen (z. B. einen Handelsregisterauszug) nach.

Bei Beantragung der Aufnahme der Vertretungsmacht für eine natürliche Person gilt dies entsprechend.

Hinweis: 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.

Hinweis: 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.

Hinweis: 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 alten Zertifikats. Dabei kann auf die bei der erstmaligen Identifizierung bereits geprüften Daten und Nachweise zurückgegriffen werden. Dies setzt voraus, dass die dem VDA BNotK vorliegenden Identifizierungsdaten und Bestätigungen zu Attributen vollständig und zutreffend sind. 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 Folgezertifikates informiert. Hierbei wird die Identität über den Login, z.B. mit einem Authentisierungszertifikat, sichergestellt. Der Zertifikatsinhaber oder Antragsteller erhält zugleich eine Übersicht über die beim VDA BNotK erfassten relevanten Daten und wird aufgefordert, die Daten zu überprüfen und innerhalb eines genannten Zeitraums (mindestens vier Wochen) dem VDA BNotK ggf. notwendige Korrekturen mitzuteilen. Sind die dem VDA BNotK vorliegenden Daten und Nachweise noch vollständig und zutreffend, wird ein neues qualifiziertes Zertifikat erstellt. Wenn sich die Identifizierungsdaten zwischenzeitlich geändert haben, ist ein erneuter Antrag und eine erneute Identifizierung erforderlich.

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 Widerrufspassworts und weitere persönliche Angaben,
- ▶ bei einem telefonischen Widerrufsverlangen für qualifizierte Siegelzertifikate durch Angabe des Widerrufspassworts, 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**) der Zertifizierungsstelle der Bundesnotarkammer 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) der Zertifizierungsstelle der Bundesnotarkammer genannten Gruppe.

Die Eingabe der Antragsdaten erfolgt stets über das Online-Antragsystem 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 Unterrichtungsbrochure zu qualifizierten Zertifikaten zur Kenntnis genommen hat. Die Zustimmung zu den Allgemeinen Geschäftsbedingungen sowie die Bestätigung, von der Unterrichtungsbrochure 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 Unterrichtungsbrochure 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 dieser in Abhängigkeit vom gewählten Identifizierungsverfahren durch die RA-Mitarbeiter im Vier-Augen-Prinzip geprüft. Die Prüfung erfolgt erst, wenn die Identifikationsunterlagen und die ggf. erforderlichen Attributsbestätigungen vorliegen.

Der VDA BNotK bedient sich zur Identifizierung der Antragsteller verschiedener Verfahren. Teilweise (z.B. beim Verfahren Notarident oder Gerichtident) sind zuverlässige und sachkundige Dritte mit der Identifizierung betraut. Vgl. dazu die Ausführungen in Abschnitt 3.2.

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

Die Identifizierung und Authentifizierung der Antragsteller sowie die Prüfung weiterer zertifikatsrelevanter Daten (z.B. Angaben zu berufsbezogenen Attributen) muss vor der Ausstellung des qualifizierten Zertifikats abgeschlossen sein.

Nachdem alle Antragsdaten gegengeprüft und bestätigt wurden, erteilt der zweitprüfende RA-Mitarbeiter die Produktionsfreigabe.

#### 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 auch aus folgenden Gründen abgelehnt werden:

- ▶ keine Bezugsberechtigung des Antragstellers, da dieser nicht Angehöriger einer der in Abschnitt 1.3.3. der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer 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.

Nach der Identifizierung des Antragstellers und der Gegenkontrolle der Antragsdaten zu den in elektronischer Form vorliegenden Daten wird der Produktionsprozess angestoßen. 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 per E-Mail bzw. EGVP benachrichtigt.

## 4.4 Zertifikatsübergabe

### 4.4.1 Verhalten bei der Zertifikatsübergabe

Der Zertifikatsnehmer 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 Rechenzentrumsumgebung 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 Rechenzentrumsumgebung des VDA BNotK erzeugt und dort zur Siegelerstellung vorgehalten. Die Nutzung des Schlüssels zur Siegelerstellung ist nur nach vorheriger Anmeldung mit den Authentifizierungsdaten des Siegelerstellers (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 RetrievalAllowed jederzeit möglich.

Der Status eines Zertifikats ist nach Produktion über OCSP 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

Widerrufspasswort 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 nur für berufliche Zwecke verwenden. Es gelten die Bestimmungen aus Abschnitt 1.4.

Für qualifizierte elektronische Signaturen vergibt der VDA BNotK Chipkarten, mit denen sich der Zertifikatsinhaber gegenüber dem VDA BNotK authentisieren kann, um die Signaturanbringung per Fernsignatur auszulösen. Erst nach der Anmeldung via Chipkarte und PIN ist das Auslösen von Fernsignaturen möglich. Das Authentisierungszertifikat auf der Chipkarte ist eindeutig mit dem Schlüssel des Signaturzertifikats verknüpft. Der Authentisierungsmechanismus auf Basis des Authentisierungszertifikates kann als Signaturerstellungsdaten im Sinne der eIDAS-Verordnung (EU 910/2014) betrachtet werden.

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

Die Verwendung des Zertifikats ist dem vertretungsberechtigten Antragsteller und zeichnungsberechtigten Endanwendern für ausschließlich berufliche Zwecke gestattet.

Für Siegelvorgänge vergibt der VDA BNotK Software-Authentisierungszertifikate, mit denen der vertretungsberechtigte Antragsteller und weitere zeichnungsberechtigte Endanwender sich gegenüber dem VDA BNotK authentisieren, um die Siegelanbringung per Fernsiegelung auszulösen. Das Auslösen von Fernsiegelungen ist erst nach der initialen Anmeldung mittels eines Software-Authentisierungszertifikates möglich. Berechtigt eine Siegelung auszulösen sind somit der vertretungsberechtigte Antragsteller sowie alle weiteren Endanwender (wie z.B. Mitarbeiter), die durch den Besitz eines Software-Authentisierungszertifikates autorisiert sind sich gegenüber dem VDA BNotK zu authentisieren. Die Authentisierungszertifikate sind eindeutig mit dem Schlüssel des Siegelzertifikats verknüpft. Das Auslösen einer Siegelung findet statt, indem sich der Antragsteller oder ein autorisierter Endanwender mittels eines Authentisierungszertifikats gegenüber dem VDA BNotK authentisieren. Die Authentisierung erlaubt anschließend das Auslösen einer Fernsiegelung durch den Antragsteller oder Endanwender. Der Authentisierungsmechanismus auf Basis der Authentisierungszertifikate kann als Siegelerstellungsdaten im Sinne der eIDAS-Verordnung (EU 910/2014) betrachtet werden.

Darüber hinaus ermöglicht es der VDA BNotK dem vertretungsberechtigten Antragsteller,

Siegelvorgänge mithilfe des Software-Authentisierungszertifikates im Rechenzentrum zu automatisieren.

Die Verantwortung zum Schutz der Software-Authentisierungszertifikate, obliegt ausschließlich dem vertretungsberechtigten Antragsteller des Siegelzertifikats. Authentisierungszertifikate sind ausschließlich zum Auslösen von Siegeln für berufliche Zwecke einzusetzen und vor dem Zugriff durch unberechtigte Dritte zu schützen.

## 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 auch, wenn

- ▶ das Vertragsverhältnis gekündigt wurde,
- ▶ der Antrag des Zertifikatsinhabers bzw. des vertretungsberechtigten Antragstellers aufgrund eines Rahmenvertrages erfolgt ist und dieser Rahmenvertrag 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, nicht vorliegt oder nicht mehr gültig ist,
- ▶ eine gesetzliche Pflicht zum Widerruf besteht,
- ▶ die Bezugsberechtigung nicht 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:

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

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

(2) schriftlich;

- ▶ mit eigenhändiger Unterschrift an die folgende Anschrift:  
Zertifizierungsstelle der BNotK, Burgmauer 53, 50667 Köln,
- ▶ mit eigenhändiger Unterschrift oder qualifiziert signiert via E-Mail oder EGVP 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 durch Angaben zu Zertifikat und Zertifikatsinhaber eindeutig zu bestimmen sein.

Der Widerruf des qualifizierten Zertifikats wird mittels eines automatisch erzeugten Widerrufsprotokolls dokumentiert. Ferner werden der Zertifikatsinhaber\_sowie die bestätigende Stelle im Falle zusätzlich beantragter Attribute über den Widerruf informiert.

- Qualifizierte Zertifikate für juristische Personen (für qualifizierte Siegel)

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

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

Widerrufsberechtigte, die ein Widerrufsverlangen telefonisch stellen wollen, müssen sich

- ▶ durch Nennung des vereinbarten Widerrufskenneworts sowie weiterer persönliche Angaben authentifizieren.
- ▶ Nach der korrekten Angabe von Widerrufskennewort und persönlicher Daten wird zudem ein Einmallink zur Bestätigung des Widerrufsverlangens an die beim VDA BNotK hinterlegte geschäftliche Kontaktadresse (E-Mail oder EGVP-Postfach) geschickt.

2. schriftlich;

- ▶ mit eigenhändiger Unterschrift an die folgende Anschrift:  
Zertifizierungsstelle der BNotK, Burgmauer 53, 50667 Köln,
- ▶ mit eigenhändiger Unterschrift oder qualifiziert signiert via E-Mail oder EGVP an den VDA BNotK.

(1)

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

Dieser Nachweis kann in Form eines amtlichen Handelsregisterauszugs (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 des Widerrufsverlangen

Der telefonische Widerruf von Zertifikaten ist 24 Stunden an sieben Tagen die Woche über eine speziell für diesen Zweck eingerichtete Telefonnummer erreichbar. Der Widerruf des Zertifikats erfolgt unmittelbar, spätestens jedoch innerhalb von 24 Stunden.

Schriftliche Widerrufsverlangen werden in der RA zügig bearbeitet und die Zertifikate innerhalb von 24 Stunden widerrufen.

Wenn der Zertifikatsinhaber, der vertretungsberechtigte Antragsteller oder Widerrufsberechtigte Dritte dies verlangen, erfolgt der Widerruf zu einem bestimmten Stichtag. Rückwirkende Sperrungen sind nicht möglich.

#### 4.9.6 Methoden zum Prüfen von Widerrufsinformationen

Widerrufsinformationen können über den OCSP-Responder abgefragt werden. Die Adresse des Dienstes ist Teil des Zertifikats.

#### 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. Die Adresse des Dienstes ist Teil des Zertifikats. Widerrufsinformationen sind unmittelbar, spätestens innerhalb von 60 Minuten, nach Widerruf eines Zertifikates verfügbar. Die Systemzeit aller am Widerruf beteiligten IT-Systeme wird fortlaufend mit der gemäß des Einheiten- und Zeitgesetzes gesetzlich gültigen Zeit abgeglichen.

#### 4.9.10 Notwendigkeit zur Online-Prüfung von Widerrufsinformationen

Es gibt keine Pflicht zur Online-Prüfung von Widerrufsinformationen.

#### 4.9.11 Andere Formen zur Anzeige von Widerrufsinformationen

Keine.

#### 4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine.

#### 4.9.13 Suspendierung des Zertifikats

Die Suspendierung des Zertifikates ist nicht möglich.

### 4.10 Statusabfragedienst

Statusabfragen erfolgen über den OCSP-Responder. Die Adresse des Dienstes ist Teil des Zertifikats und 24 Stunden an sieben Tagen die Woche verfügbar. Der Statusabfragedienst ist hochverfügbar, um einen Ausfall zu verhindern. Der VDA BNotK wird Störungen des Statusabfragediensts im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten spätestens innerhalb von 12 Stunden beseitigen.

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 Bauliche Sicherheitsmaßnahmen

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. „Erweitert“ bedeutet, dass alle Anforderungen eines Bewertungsaspekts des nächsthöheren Levels erreicht wurden. Die Prüfung wird in regelmäßigen Abständen wiederholt.

## 5.2 Verfahrensvorschriften

### 5.2.1 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.

### 5.2.2 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.

### 5.2.3 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.

## 5.3 Personalkonzept

### 5.3.1 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.

### 5.3.2 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.

### 5.3.3 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.

### 5.3.4 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.

### 5.3.5 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.

### 5.3.6 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.

### 5.3.7 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.

## 5.4 Protokollierung von Überwachungsmaßnahmen

### 5.4.1 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.

### 5.4.2 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.

## 5.5 Archivierung von Unterlagen

### 5.5.1 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.

### 5.5.2 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 Widerrufsinformationen sowie den dazugehörigen Aufzeichnungen nach Artikel 24 Absatz 2 Buchstabe h der Verordnung (EU) Nr. 910/2014 für die gesamte Zeit des Betriebs des VDA BNotK aufbewahrt.

### 5.5.3 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 berechnigte 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 berechnigte 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.

## 5.5.4 Datensicherung des Archivs

Die Sicherung der Daten erfolgt nach dem Stand der Technik.

## 5.5.5 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.

## 5.5.6 Ort der Archivierung

Die Archivierung findet ausschließlich bei der Bundesnotarkammer statt.

## 5.6 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.

## 5.7 Notfallkonzept

### 5.7.1 Behandlung von Vorfällen

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

### 5.7.2 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.

### 5.7.3 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 Widerrufsinformationen 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.

#### 5.7.4 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.

### 5.8 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 von der Zertifizierungsstelle 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 Signaturzertifikate 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 den entsprechenden Vorgaben und wird dokumentiert. 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 Zertifikatserstellung 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 der Zertifizierungsstelle 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 der

darauf zugreifenden Applikation. Eine dauerhafte Deaktivierung erfolgt nach mehrmaliger Falscheingabe 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.

### 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 Aktivierungsdaten

#### 6.4.1 Erzeugung und Installation von Signatur- und Siegelerstellungsdaten Aktivierungsdaten

Signatur- und Siegelerstellungsdaten im Sinne der eIDAS-Verordnung (EU 910/2014) sind definiert als solche eindeutigen Daten, welche vom Unterzeichner zum Erstellen einer elektronischen Signatur oder eines elektronischen Siegels verwendet werden. Diese eindeutigen Daten können sowohl die Form einer PIN-Nummer als auch eines privaten kryptographischen Schlüssels (mit Authentisierungszertifikat) annehmen die sich unter der Kontrolle des Unterzeichners befinden.

Die für die Aktivierung des privaten Schlüssels notwendigen Signaturerstellungsdaten (das Authentisierungszertifikat) werden für den Zertifikatsinhaber im Fall von Authentisierungskarten vom Teilnehmer 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 nur dem (vertretungsberechtigten) Antragsteller zugängliches und geschütztes Portal. Die Zertifikatserstellung samt PIN-Vergabe erfolgt lokal auf dem Client des (vertretungsberechtigten) Antragstellers.

Der Authentisierungsmechanismus auf Basis eines Authentisierungszertifikats, kann als Signaturerstellungsdatum im Sinne der eIDAS Verordnung (EU 910/2014) betrachtet 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 der gemäß des Einheiten- und Zeitgesetzes gesetzlich gültigen Zeit abgeglichen.

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 zum Ausüben seiner Rolle notwendig sind. Zu diesem Zweck wird bei den technischen Rollen zwischen verschiedenen administrativen, operativen und auditierenden Rollen unterschieden.

Es bestehen Arbeitsanweisungen für die Mitarbeiter des VDA BNotK betreffend die Einhaltung der Vorgaben zur Computersicherheit.

Um zu verhindern, dass unautorisierte Personen Zugriff auf sensible Daten bekommen, werden Datenträger vor der Wiederverwendung sicher gelöscht. Defekte Datenträger werden nach einem sicheren Verfahren zerstört.

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. 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, vierteljährlich bzw. jährlich, Schwachstellenscans (*vulnerability scans*) und 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.

## **6.7 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 Netzwerkumgebung und die Anbindung der Netzwerke sind hochverfügbar ausgelegt. Zur Sicherstellung der Einhaltung der Netzwerk- und Systemsicherheit werden regelmäßig Penetrationstests auf die extern zugänglichen und internen IP-Adressen durch qualifiziertes Personal durchgeführt. Die Penetrationstests werden bei sicherheitserheblichen Veränderungen wiederholt.

Die Einhaltung der Regeln wird regelmäßig überwacht.

## 6.8 Zeitstempel

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

## 7 Profile von Zertifikaten, Widerrufslisten und OCSP

### 7.1 Zertifikatsprofile

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

#### 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
<b>Aussteller</b>		
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
<b>Gültigkeit</b>		

UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	z.B. 2017-10-09 08:57:57 UTC
	Ende	z.B. 2037-10-09 08:57:56 UTC
<b>Inhaber</b>		
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
<b>Erweiterungen</b>		
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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	<a href="http://ocsp.zs.bnotk.de/eqsig">http://ocsp.zs.bnotk.de/eqsig</a>

#### 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
<b>Aussteller</b>		
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	z.B. CN = BNotK Root CA 2017
<b>Gültigkeit</b>		
UTCTime	Beginn	Zertifikat gültig ab
	Ende	Zertifikat gültig bis
<b>Inhaber</b>		
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 Root 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	[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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	<a href="http://ocsp.zs.bnotk.de/eqsig">http://ocsp.zs.bnotk.de/eqsig</a>

## 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
<b>Gültigkeit</b>		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	Beginn Zertifikatsgültigkeit
	Ende	Ende Zertifikatsgültigkeit
<b>Inhaber</b>		
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
<b>Erweiterungen</b>		
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
<b>Aussteller</b>		
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	z.B. CN = BNotK Root CA 2017
<b>Gültigkeit</b>		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	Beginn Zertifikatsgültigkeit
	Ende	Ende Zertifikatsgültigkeit

<b>Inhaber</b>		
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
<b>Erweiterungen</b>		
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
caIssuers (1.3.6.1.5.5.7.48.2)	URL zur Aussteller-Info	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	<a href="http://ocsp.zs.bnotk.de/eqsig">http://ocsp.zs.bnotk.de/eqsig</a>

### 7.1.3 Endanwenderzertifikatsprofil

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

<b>Feld (OID)</b>	<b>Beschreibung</b>	<b>Wert</b>
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	2048 Bits
<b>Aussteller</b>		
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	z.B. CN = BNotK qSig CA 2017
<b>Gültigkeit</b>		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	Beginn Zertifikatsgültigkeit
	Ende	Ende Zertifikatsgültigkeit
<b>Inhaber</b>		
countryName (2.5.4.6)	Name Land Inhaber	z.B. C = DE  Land, in dem der Zertifikatsinhaber seinen Wohnsitz hat oder das vorgelegte Identifikationsdokument des Zertifikatsinhabers 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, eindeutige UUID des Zertifikatsinhabers
<b>Erweiterungen</b>		
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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	<a href="http://ocsp.zs.bnotk.de/eqsig">http://ocsp.zs.bnotk.de/eqsig</a>

CertificatePolicies (2.5.29.32)		Verweis auf geltende Zertifizierungsrichtlinie	s. folgende Elemente
Policy Information	policyIdentifier	Kennzeichner (OID) und URL- Verweis auf CPS	1.3.6.1.4.1.41460.5.2.1.1.2
	policyQualifier		<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
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)
algorithmIdentifier	Kennzeichner (OID) Schlüsselalgorithmus	ECDSA (1.2.840.10045.4.3.4)
Schlüssellänge	Schlüssellänge	521 Bits
<b>Aussteller</b>		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName (2.5.4.3)	Name Inhaber	z.B. CN = BNotK qSig CA 2017

<b>Gültigkeit</b>		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	Beginn Zertifikatsgültigkeit
	Ende	Ende Zertifikatsgültigkeit
<b>Inhaber</b>		
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
emailAddress (1.2.840.113549.1.9.1)	E-Mail-Adresse Inhaber	emailAddress = [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
<b>Erweiterungen</b>		
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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	<a href="http://ocsp.zs.bnotk.de/eqsig">http://ocsp.zs.bnotk.de/eqsig</a>
CertificatePolicies (2.5.29.32)	Verweis auf geltende Zertifizierungsrichtlinie	s. folgende Elemente

Policy Information	policyIdentifier	Kennzeichner (OID) und URL-Verweis auf CPS	1.3.6.1.4.1.41460.5.2.1.1.2
	policyQualifier		<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
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

<b>Aussteller</b>		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName (2.5.4.3)	Name Inhaber	z.B. CN = BNotK EC rqSeal CA 2021
<b>Gültigkeit</b>		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	Beginn Zertifikatsgültigkeit
	Ende	Ende Zertifikatsgültigkeit
<b>Inhaber</b>		
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	eineindeutige UUID des Zertifikatsinhabers
<b>Erweiterungen</b>		

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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	<a href="http://ocsp.zs.bnotk.de/eqsig">http://ocsp.zs.bnotk.de/eqsig</a>
CertificatePolicies (2.5.29.32)	Verweis auf geltende Zertifizierungsrichtlinie	s. folgende Elemente
Policy Information	policyIdentifier	Kennzeichner (OID) und URL- Verweis auf CPS
	policyQualifier	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
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	<a href="https://zertifizierungsstelle.bnotk.de/veroeffentlichungen">https://zertifizierungsstelle.bnotk.de/veroeffentlichungen</a>
---------------------------	---------------------	---

## 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 beaufkundet 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.

\*\*\*

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

