BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Zertifizierungskonzept der Zertifizierungsstelle der Bundesnotarkammer für qualifizierte Zertifikate

Version: **2.4**

Datum: **15. Juni 2020**

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 (***eIDAS-Verordnung***) durch eine akkreditierte Konformitätsbewertungsstelle	20.06.2017
2.0	Aktualisierung aufgrund der Umstellung der PKI-Infrastruktur der Zertifizierungsstelle der Bundesnotarkammer auf eine native eIDAS-PKI sowie redaktionelle Änderungen in Folge des Inkrafttretens des Vertrauensdienstegesetzes	18.10. 2017
2.1	Aktualisierung aufgrund neuer Zertifikatshierarchie	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 der CA-Hierarchie	15.06.2020

Inhalt

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) und qualifizierte elektronische Zeitstempel. Die Nutzung der qualifizierten Zertifikate erfordert den Einsatz einer qualifizierten elektronischen Signaturerstellungseinheit (***QSCD***).

Dieses ist das Zertifizierungskonzept der Zertifizierungsstelle der Bundesnotarkammer (***VDA BNotK***) für qualifizierte Zertifikate für elektronische Signaturen (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 1.3.6.1.4.1.41460.5.1.1.1.2.1.3 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 Vertrauensdienstanbieter 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

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

PKI für qualifizierte Vertrauensdienste

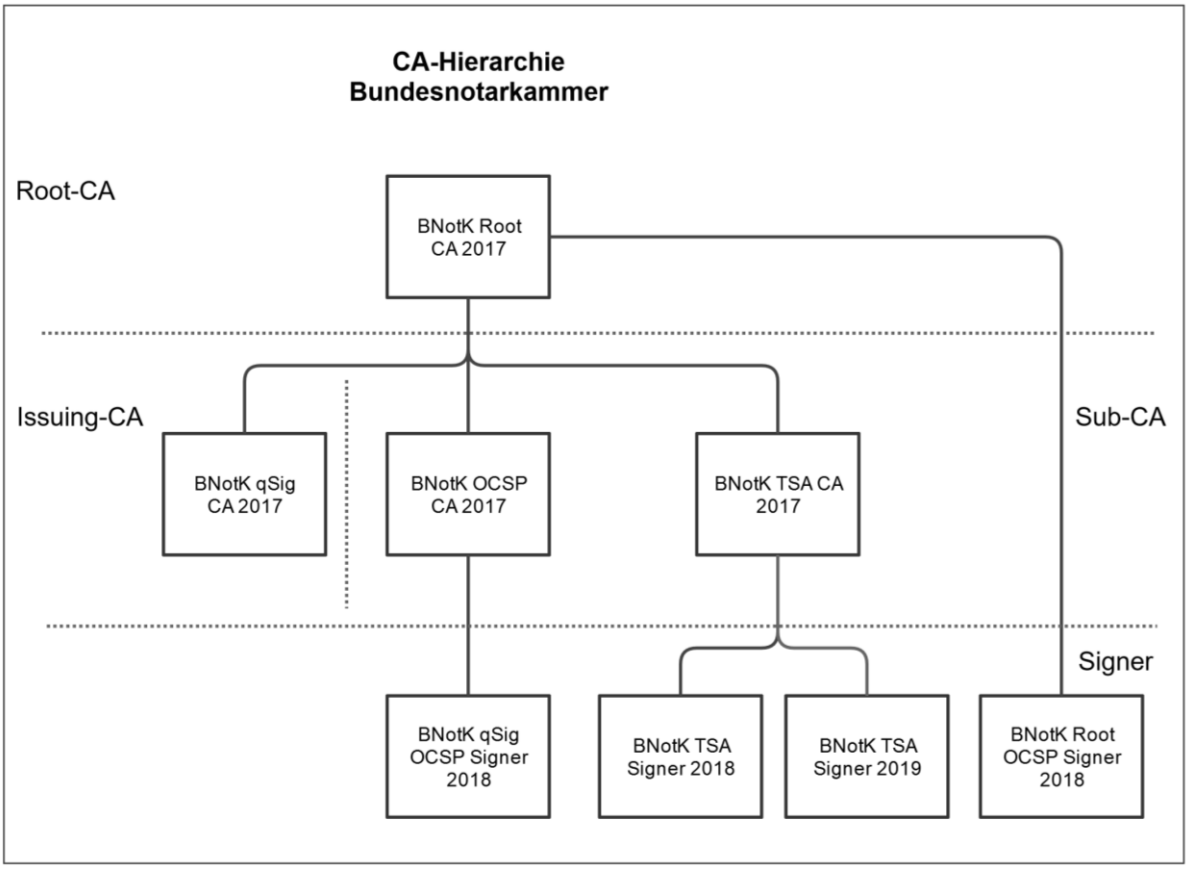

Abbildung 1: PKI Hierarchie für qualifizierte Zertifikate

Qualifizierte Zertifikate

Die ausgegebenen Endanwenderzertifikate entsprechen den Anforderungen der eIDAS-Verordnung sowie des folgenden Zertifizierungslevel nach ETSI EN 319 411-2:

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

1.2 Name und Kennzeichnung des Dokuments

Dokumentenname: Zertifizierungskonzept der Zertifizierungsstelle der Bundesnotarkammer

Kennzeichnung (OID): 1.3.6.1.4.1.41460.5.2.1.1.2.2.4

Version: 2.4

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 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 eine QSCD erforderlich.

Der Zertifikatsinhaber ist gemäß § 5 der Allgemeinen Geschäftsbedingungen des VDA BNotK insbesondere verpflichtet,

- die vereinbarten Entgelte entsprechend der zum Vertragsschluss gültigen Preisliste fristgerecht zu zahlen,
- die für die Leistungserbringung der Bundesnotarkammer notwendigen Mitwirkungsleistungen zu erbringen,
- sämtliche für den Antrag erforderliche Daten vollständig und wahrheitsgemäß anzugeben und die geforderten Nachweise zu erbringen; Änderungen der Daten sind dem VDA BNotK unverzüglich anzuzeigen,
- eine Bankverbindung eines im Inland zum Geschäftsbetrieb befugten Kreditinstituts für die Abwicklung der Bankgeschäfte im Zusammenhang mit der Einziehung der Entgelte zu benennen sowie diesbezüglich ein gültiges SEPA-Lastschriftmandat zu erteilen und für eine ausreichende Deckung des vereinbarten Abbuchungskontos zu sorgen,
- nach Erhalt der QSCD deren Empfang elektronisch zu bestätigen,
- die QSCD sicher im unmittelbaren Besitz zu halten und die PIN und die Antragsnummer weder Mitarbeitern noch Dritten zugänglich zu machen,
- dem VDA BNotK offenkundige Mängel oder Schäden am System oder Verfahren unverzüglich anzuzeigen (Störungsmeldung),
- den Verlust oder Missbrauch der QSCD bzw. des Zertifikats nach Kenntnis unverzüglich anzuzeigen und den Widerruf des betroffenen Zertifikats zu beantragen,

- Zertifikate dann unverzüglich widerrufen zu lassen, wenn die darin enthaltenen Angaben nicht mehr den Tatsachen entsprechen, insbesondere wenn in einer Weiterverwendung ein Verstoß gegen Berufs- und/oder Standesrecht oder andere Rechtsvorschriften läge,
- ein verwendetes Pseudonym auf seine Vereinbarkeit mit den Rechten Dritter, z.B. Namens-, Marken-, Urheber- oder sonstigen Schutzrechten, sowie mit den allgemeinen Gesetzen zu prüfen,
- für den Fall, dass vier Wochen nach Zustellung der QSCD der Kunde die Transport-PIN-Mitteilung noch nicht erhalten hat, das Zertifikat unverzüglich widerrufen zu lassen, die QSCD fachgerecht zu zerstören und eine neue QSCD beim VDA BNotK anzufordern,
- die ihm bekannten Einschränkungen (z.B. Einschränkungen der Vertretungsmacht) des Zertifikats zu beachten und die QSCD nicht zu nutzen, wenn ihm bekannt ist, dass das Zertifikat widerrufen oder das Wurzelzertifikat kompromittiert worden ist.

Nimmt der Zertifikatsinhaber nach seiner Identifizierung trotz Aufforderung durch den VDA BNotK notwendige Mitwirkungshandlungen nicht vor, hat er dem VDA BNotK die hierfür entstandenen Kosten zu erstatten, es sei denn, der Zertifikatsinhaber weist nach, dass die Kosten überhaupt nicht oder in wesentlich niedrigerer Höhe entstanden sind. Bei einer vom Zertifikatsinhaber zu vertretenden erfolglosen Zustellung der Signaturkarte fallen Kosten i. H. v. EUR 3,00 pro Zustellungsversuch und bei einer vom Kunden zu vertretenen Ausstellung einer unrichtigen Folgekarte und dem Austausch durch eine Ersatzkarte Kosten i. H. v. EUR 20,00 an.

Nach Vertragsbeendigung hat der Zertifikatsinhaber das qualifizierte Zertifikat widerrufen zu lassen und die QSCD fachgerecht zu zerstören.

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

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.

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

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.

Die qualifizierten Zertifikate werden unter den Adressen ldap://ldap.zs.bnotk.de und ldap://ldap.bnotk.de veröffentlicht.

2.2 Veröffentlichung von Informationen zu Zertifikaten

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

- die qualifizierten Zertifikate, sofern der Zertifikatsinhaber dem nicht widersprochen hat,
- die Informationsbroschüre für qualifizierte elektronische Signaturen,
- die Zertifikatsrichtlinie,

- dieses Zertifizierungskonzept,
- das PKI Disclosure Statement für qualifizierte Zertifikate.

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Die Teilnehmerzertifikate werden veröffentlicht, sobald ein Empfangsbekenntnis vorliegt und der Teilnehmer der Veröffentlichung zugestimmt hat. Widerrufslisten werden nicht veröffentlicht.

Weitere Regelungen sind in der Zertifikatsrichtlinie 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

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Siehe Abschnitt 7.1 dieses Dokuments.

3.1.5 Eindeutigkeit von Namen

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
- Nachname
- Common Name
- Seriennummer (= Zertifikatsnummer)

Die Seriennummer wird eindeutig vergeben. Eine Verwechslungsmöglichkeit von zwei Personen mit gleichem Vor- und Nachnamen ist ausgeschlossen, da die Eindeutigkeit durch den Zusatz „Seriennummer" gegeben ist.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

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

3.2 Identifizierung der Zertifikatsinhaber

Der VDA BNotK hat Personen, die ein qualifiziertes Zertifikat beantragen, eindeutig zu identifizieren. Dabei werden nur die Informationen erfasst, die zur Bereitstellung der vom VDA BNotK angebotenen Vertrauensdienste erforderlich sind. Erforderlich ist mindestens die Feststellung des vollständigen Namens sowie des Geburtsdatums und des Geburtsorts des Antragsstellers. Zudem muss der Antragsteller seine Anschrift und eine E-Mail-Adresse angeben.

Die Identifizierung erfolgt grundsätzlich anhand der folgenden Dokumente:

- Personalausweis der Bundesrepublik Deutschland,
- 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 Antragssteller bisher noch nicht identifiziert wurde oder die der Identifizierung zu Grunde liegenden Daten sich geändert haben (beispielsweise bei einer Änderung des Namens des Antragstellers).

3.2.1 Identifizierung des Antragstellers

Die Identifizierung des Antragstellers kann grundsätzlich unter Nutzung folgender Verfahren erfolgen:

- Notarident – Identifizierung durch Notare;
- Gerichtident – Identifizierung durch deutsche Gerichte;
- Rechtsanwaltskammerident – Identifizierung durch Mitarbeiter von Rechtsanwaltskammern;

- 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 angebotenen. Eine Identifizierung im Verfahren Rechtsanwaltskammerident ist z.B. nur bei der Bestellung eines beA-Produkts möglich und nur dann, wenn die zuständige Rechtsanwaltskammer dieses Verfahren anbietet. 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 die zum gewählten Identifizierungsverfahren passenden Identifizierungsunterlagen zum Ausdruck bereitgestellt.

3.2.1.1 Verfahren Notaridentt

Beim Identifizierungsverfahren Notaridentt wird die Identifizierung durch einen Notar mit Amtssitz in Deutschland durchgeführt.

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

Das Verfahren Notaridentt umfasst:

- Entgegennahme (i) der (unterschriebenen bzw. noch zu unterschreibenden) Antragsunterlagen und Beglaubigung der Unterschrift des Antragstellers oder (ii) des (unterschriebenen bzw. noch zu unterschreibenden) Datenblattes mit allen bei der Antragstellung angegebenen personenbezogenen Daten des Antragstellers und Beglaubigung der Unterschrift des Antragstellers durch den Notar;
- Erstellen einer beglaubigten Abschrift der zur Identifizierung verwendeten Ausweisdokumente durch den Notar;
- Versand der Urkunden durch den Notar an die RA auf dem Postweg oder Erstellung von einer elektronisch beglaubigten Abschrift und Versand an die RA auf elektronischem Weg. Postalisch sind Unterlagen in einem Umschlag unmittelbar an die RA zu übersenden, die diesen auf Unversehrtheit prüft. Die mit einer qualifizierten elektronischen Signatur des Notars versehenen elektronischen Dateien werden sicher elektronisch per EGVP an die RA übertragen werden. Die Übertragung erfolgt Ende-zu-Ende verschlüsselt.

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

3.2.1.2 Verfahren Gerichtident

Die Identifizierung des Antragstellers kann 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. Die entsprechenden Angaben werden durch Beifügung einer Kopie des zur Identifizierung verwendeten Ausweises zu dem Kartenantrag dokumentiert. Der Versand der Unterlagen erfolgt in einem Umschlag unmittelbar durch die beglaubigende Stelle an die RA des VDA BNotK, die diesen auf Unversehrtheit prüft. 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 Vereidigung eingesetzt wird, am Kammerident-Verfahren teilnimmt.

3.2.1.4 Verfahren RA-Ident

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:

- 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 Signaturkartenleser und ein Drucker/Scanner angeschlossen sind.

3.2.2 Identifizierung bei Erweiterungen und Beschränkungen im Zertifikat

Ein qualifiziertes Zertifikat 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 Kartenantrag 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 Kartenanträge mit Notarattribut zulässt, wenn die entsprechende Berechtigung zur Führung eines solchen Notarattributs sich bereits bei der Antragstellung aus dem Notarverzeichnis ergibt.

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.

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

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.

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

Eine Schlüsselerneuerung erfolgt durch die Produktion eines neuen qualifizierten Zertifikats auf einer QSCD. 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 wird vor Ablauf der Zertifikatsgültigkeit automatisiert über das Verfahren für die Ausstellung eines Folgezertifikates informiert. Hierbei wird die Identität über den Login mit der bestehenden und gültigen QSCD sichergestellt. Der Zertifikatsinhaber 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 der neuen QSCD 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 folgende Möglichkeiten des Widerrufs der von ihr ausgegebenen Zertifikate an:

- telefonisch sowie
- schriftlich mit eigenhändiger Unterschrift

Die Identifizierung und Authentifizierung erfolgt:

- bei einem telefonischen Widerrufsverlangen durch Angabe des Widerrufspassworts,
- bei einem schriftlichen Widerrufsverlangen durch Überprüfung der Unterschrift.

4 Betriebsanforderungen

4.1 Zertifikatsantrag

Der VDA BNotK gibt Zertifikate ausschließlich an Angehörige der in Abschnitt 1.3.3 der in der Zertifikatsrichtlinie (***CP***) der Zertifizierungsstelle der Bundesnotarkammer genannten Berufsgruppen aus.

Die Eingabe der Antragsdaten erfolgt stets über die Online-Antragsseite des VDA BNotK. Eine ausschließlich schriftliche Antragstellung ist nicht möglich. Die Eingabe erfolgt dabei stets durch den Antragsteller selbst. Im Zuge der Stellung des Antrags stimmt der Antragsteller der Einbeziehung der Allgemeinen Geschäftsbedingungen des VDA BNotK zu und bestätigt, dass er die Informationsbroschüre zu qualifizierten Zertifikaten zur Kenntnis genommen hat. Die Zustimmung zu den Allgemeinen Geschäftsbedingungen sowie die Bestätigung, von der Informationsbroschüre Kenntnis genommen zu haben, ist Voraussetzung für den Abschluss des Vertrages. Die Allgemeinen Geschäftsbedingungen sind in deutscher Sprache verfasst und werden den Antragstellern zusammen mit der Informationsbroschüre in elektronischer Form zum Download zur Verfügung gestellt.

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 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.

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 dann abgelehnt, wenn die Antragsdaten nicht mit Ausweisdokumenten bzw. Attributsbestätigungen übereinstimmen.

Anträge können zudem auch aus folgenden Gründen abgelehnt werden:

- keine Bezugsberechtigung des Antragsstellers, da dieser nicht Angehöriger einer der in Abschnitt 1.3.3. der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer aufgeführten Berufsgruppen ist,
- 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 QSCD 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 die Kartenpersonalisierung, d.h. das Speichern des Zertifikats auf der QSCD.

4.3.2 Benachrichtigung des Zertifikatsinhabers über die Erstellung des Zertifikats

Eine gesonderte Benachrichtigung des Zertifikatsinhabers erfolgt nicht.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Der VDA BNotK bietet zwei Varianten für die Übergabe eines Zertifikates an:

- postalischer Versand der QSCD oder
- Nachladen eines qualifizierten Zertifikates auf eine dem Antragsteller bereits übersandte QSCD.

Grundsätzlich erfolgt die Auslieferung des Zertifikats durch Übergabe der QSCD mittels postalischen Versands an die Meldeadresse des Antragstellers bzw. bei Notaren an deren Geschäftsadresse. Vor dem Versand wird die Funktionsfähigkeit der QSCD geprüft. Der Antragsteller muss den Empfang der QSCD online bestätigen. Nachdem der Antragsteller den Erhalt der QSCD bestätigt hat und der PIN-Brief erzeugt wurde, wird das Zertifikat freigeschaltet. Anschließend werden Transport-PIN und PUK an den Antragsteller versandt. Der Versand erfolgt postalisch oder elektronisch mittels EGVP. Mittels dieser PIN, die vor der ersten Nutzung geändert werden muss, kann der Antragsteller die QSCD in Betrieb nehmen. Die PIN kann nur erfolgreich geändert werden, wenn die QSCD nicht manipuliert wurde. Die einzelnen Schritte werden dokumentiert.

Beim sog. „Nachladeverfahren" wird das qualifizierte Zertifikat auf eine dem Antragsteller vorliegende QSCD aufgeladen. Das „Nachladeverfahren" wird nur bei ausgewählten Produkten des VDA BNotK angeboten. Voraussetzung ist, dass dem Antragsteller eine vollständig mit qeS-Schlüsseln produzierte QSCD vorliegt und die Registrierung abgeschlossen wurde. Das qualifizierte Zertifikat wird Ende-zu-Ende verschlüsselt über eine Webseite (Dashboard) an den Antragsteller übermittelt. Mit Hilfe einer als Webanwendung zur Verfügung gestellten Signaturanwendungskomponente und eines geeigneten Kartenlesegerätes wird das qualifizierte Zertifikat auf die bereits vorher übersandte Signaturkarte aufgeladen. Mit dem Aufladen des qualifizierten Zertifikates auf die QSCD wird das qualifizierte Zertifikat freigeschaltet. Die erforderliche Transport-PIN ist mit dem nicht-qualifizierten Zertifikat der bereits ausgelieferten Karte verschlüsselt und wird erst im Zuge des Nachladeprozesses entschlüsselt und dem Anwender bereitgestellt.

4.4.2 Veröffentlichung des Zertifikats durch den VDA BNotK

Der VDA BNotK veröffentlicht das Zertifikat, sofern der Zertifikatsinhaber dem zustimmt.

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

Zertifikatsinhaber dürfen die Zertifikate nur für berufliche Zwecke verwenden und den privaten Schlüssel nicht von der QSCD exportieren.

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,
- 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

Eine Zertifikatserneuerung mit Schlüsselerneuerung wird nicht angeboten. In diesem Fall ist eine Folgekarte zu beantragen oder ein Neuantrag zu stellen.

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

In folgenden Fällen erfolgt ein Widerruf des Zertifikats durch den VDA BNotK:

- 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 ausgestellt wurde,
- bei Ungültigkeit von Angaben im Zertifikat,
- bei Beendigung der Tätigkeit als Vertrauensdiensteanbieter, wenn diese nicht von einem anderen qualifizierten Vertrauensdiensteanbieter fortgeführt wird 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 Zertifikate insbesondere auch dann, wenn

- das Vertragsverhältnis gekündigt wurde,
- der Antrag des Zertifikatsinhabers 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 verwendeten qualifizierte elektronische Signaturerstellungseinheit 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.

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 sind verpflichtet, ausgestellte Zertifikate widerrufen zu lassen, wenn

- die QSCD bzw. das Zertifikat verloren, missbraucht wurde oder möglicherweise kompromittiert wurde,
- die in dem Zertifikat enthaltenen Angaben nicht mehr den Tatsachen entsprechen, insbesondere wenn in einer Weiterverwendung ein Verstoß gegen Berufs- und/oder Standesrecht oder andere Rechtsvorschriften läge.

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

Befinden sich auf Signaturkarte mehrere Zertifikate so werden bei Widerruf eines der Zertifikate stets automatisch auch alle weiteren Zertifikate (qualifizierte und sonstige Zertifikate) der jeweiligen Signaturkarte widerrufen

4.9.2 Widerrufsberechtigte

Zum Widerruf des Zertifikats sind die folgenden Personen berechtigt:

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

Personen, denen der Zertifikatsinhaber oder ein Widerrufsberechtigter Dritter das Widerrufspasswort mitgeteilt hat, gelten ebenfalls als zum Widerruf berechtigt, vorausgesetzt, dass sie dem VDA BNotK das Widerrufspasswort mitteilen.

4.9.3 Verfahren zur Stellung eines Widerrufsverlangens

Widerrufsverlangen können (1) telefonisch unter der Rufnummer: (0800) 3550 400, (2) schriftlich mit eigenhändiger Unterschrift an die folgende Anschrift: Zertifizierungsstelle der BNotK, Burgmauer 53, 50667 Köln übermittelt werden.

Widerrufsberechtigte, die ein Widerrufsverlangen telefonisch stellen wollen, müssen sich durch Nennung des vereinbarten Widerrufspassworts und weitere persönliche Angaben authentifizieren. Stellt ein Zertifikatsinhaber ein telefonisches Widerrufsverlangen ohne sein Widerrufspasswort zu kennen, muss er das Widerrufsverlangen über einen an die beim VDA BNotK hinterlegte E-Mail-Adresse versandten Einmallink bestätigen.

Ein schriftliches Widerrufsverlangen muss eigenhändig unterschrieben sein und das zu widerrufende Zertifikat durch Angaben zu Zertifikat und Zertifikatsinhaber eindeutig bestimmen.

Der Widerruf des Zertifikats wird mittels eines automatisch erzeugten Widerrufsprotokolls dokumentiert. Ferner wird der Zertifikatsinhaber über den Widerruf informiert.

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.

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.

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

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

4.9.6 Methoden zum Prüfen von Widerrufsinformationen

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

4.9.7 Häufigkeit der Veröffentlichung von Widerruflisten

Es werden keine Widerruflisten für Zertifikate zur Verfügung gestellt.

4.9.8 Maximale Latenzzeit für Widerruflisten

Es werden keine Widerruflisten für Zertifikate zur Verfügung gestellt.

4.9.9 Online-Verfügbarkeit von Widerrufinformationen

Widerrufinformationen können über den OCSP-Responder abgefragt werden. Die Adresse des Dienstes ist Teil des Zertifikats. Widerrufinformationen sind unmittelbar, spätestens innerhalb von 60 Minuten, nach Widerruf eines Zertifikates verfügbar. Die Systemzeit aller am Widerruf beteiligten IT-System wird fortlaufend mit der gemäß des Einheiten- und Zeitgesetzes gesetzlich gültigen Zeit abgeglichen.

4.9.10 Notwendigkeit zur Online-Prüfung von Widerrufinformationen

Es gibt keine Pflicht zur Online-Prüfung von Widerrufinformationen.

4.9.11 Andere Formen zur Anzeige von Widerrufinformationen

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 wird geschützt.

4.11 Beendigung des Zertifizierungsdienstes

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

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 und Dritte, einschließlich Vertrauender Dritter und der zuständigen Aufsichtsbehörde, rechtzeitig, mindestens aber zwei Monate vorher, über die Einstellung des Zertifizierungsdienstes.

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. 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 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.

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
- Raumlufttechnische 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, 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. Personen, die in führende Rollen berufen werden, 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 kann 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.

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 Zertifikatslebenszyklus für qualifizierte Zertifikate. Das betrifft insbesondere die bei der Registrierung anfallenden Dokumente (vergleiche Abschnitt 3.2.), Dokumente zur Lieferung und Lagerung der Rohlinge sowie deren Entnahme zur Produktion, Dokumente für Folgekarten, Widerrufe und das Ausstellen von qualifizierten Zertifikaten. Zusätzlich werden Sicherheitskonzepte, Rollenbesetzungslisten, Schulungsunterlagen und Verfahrensanweisungen sowie sonstige für den Betrieb relevante Dokumente (z.B. die Zertifizierungen, Verträge mit Dienstleistern, 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. Nach Ablauf der Aufbewahrungszeit werden diese sicher gelöscht.

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 berechtigte 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 berechtigte 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-Zertifikate.

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 Zertifikate widerrufen und die Aufsichtsbehörde informiert. Je nach Art der Kompromittierung werden in Absprache mit der Aufsichtsbehörde ggf. auch die aus der CA generierten Teilnehmerzertifikate widerrufen. Betroffene Zertifikatsinhaber werden über den Vorfall und dessen Auswirkungen informiert. Die Widerrufinformationen können grundsätzlich über den OCSP-Responder abgefragt werden bzw. bei einer Kompromittierung des Zertifikats des OCSP-Responders über die von der BNetzA herausgegebene Trusted List.

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

6 Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Erzeugung von Schlüsselpaaren

CA-Schlüssel, OCSP-Schlüssel und Schlüssel für qualifizierte Teilnehmerzertifikate werden grundsätzlich in einer sicheren Umgebung auf einer zugelassenen QSCD, die gemäß den Common-Criteria-Vorgaben evaluiert wurde und auf der EU-Liste der vertrauenswürdigen zertifizierten Komponenten steht, generiert (siehe Abschnitt 5.1). Dabei wird technisch sichergestellt, dass das einem bestimmten Zertifikatsinhaber zugeordnete Schlüsselpaar mit der diesem Zertifikatsinhaber zugeordneten QSCD verknüpft wird. Im Rahmen der Kartenpersonalisierung in der RA wird automatisch geprüft, ob es sich um die für den Prozess vorgeschriebene QSCD mit den korrekten zertifizierten Parametern handelt.

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. 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 werden auf der QSCD an den Zertifikatsinhaber ausgeliefert (siehe Abschnitt 4.4.1). Die QSCD ist vom Zertifikatsinhaber diebstahlgesichert im unmittelbaren Besitz zu behalten und darf nicht an Mitarbeiter oder Dritte zur Verwendung übergeben werden.

6.1.3 Auslieferung der öffentlichen Schlüssel an die CA

Der öffentliche Schlüssel wir ihm Rahmen der Personalisierung der QSCD verschlüsselt an die CA übertragen und auf der Webseite veröffentlicht.

6.1.4 Auslieferung der öffentlichen CA-Schlüssel

Die öffentlichen Schlüssel der CA sind auf der QSCD aufgebracht.

6.1.5 Schlüssellängen

Für die Schlüssellänge gelten die Empfehlungen der SOG-IS Crypto Working Group. Zurzeit werden für die Teilnehmerzertifikate RSA-Schlüssel mit einer Länge von mindestens 2048 Bit verwendet. Die CA-Schlüssel haben eine Länge von 4096 bit für RSA.

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 Teilnehmerzertifikaten verwendet, die OCSP-Schlüssel zum Signieren der OCSP-Anfragen. Die CA- und OCSP-Schlüssel werden in einer sicheren Umgebung eingesetzt (vergleiche Abschnitt 5.1). Die Schlüsselverwendung für Teilnehmerzertifikate ist Teil des X.509 Zertifikats und darf ausschließlich für qualifizierte Signaturen verwendet werden.

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.

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 QSCDs gespeichert.

6.2.8 Aktivierung privater Schlüssel

Die CA-Schlüssel und OCSP-Schlüssel können nur in einem technisch erzwungenen Mehraugenprinzip unter Beteiligung mehrerer Rollen aktiviert werden. Schlüssel von Teilnehmerzertifikaten, CA- und OCSP-Schlüssel müssen durch die Eingabe der PIN aktiviert werden.

6.2.9 Deaktivierung privater Schlüssel

Die Deaktivierung der Schlüssel 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 dem Löschen der durch das HSM gesicherten Schlüssel CA- und OCSP-Schlüssel werden nach Ende der Gültigkeit zerstört.

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 Teilnehmerzertifikate 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 Aktivierungsdaten

Die PINs werden in der sicheren Umgebung der RA des VDA BNotK generiert. Der Teilnehmer erhält seine PIN je nach Produkt über einen gedruckten PIN-Brief oder elektronisch für den Teilnehmer verschlüsselt. Der Versand erfolgt stets getrennt von der Lieferung der QSCD. Der Teilnehmer kann sich von der Unversehrtheit der QSCD überzeugen, indem er prüft, ob die fünfstellige Transport-PIN funktioniert. Mit Hilfe der Transport-PIN kann die um mindestens eine Stelle längere Wirk-PIN gesetzt werden.

6.4.2 Schutz von Aktivierungsdaten

Die Aktivierungsdaten für Teilnehmer werden verschlüsselt in einem gesicherten Rechenzentrum des VDA BNotK gespeichert. 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. Die PUK dient zum Zurücksetzen des Fehlbedienungszählers 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 mit bereits in der Konzeptionsphase berücksichtigen 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 beispielswiese die Root CA, befinden sich in der Zone mit dem höchsten Schutzbedarf. Für die Administration der IT-Systeme wird ein separates Netz verwendet, welches ausschließlich dafür verwendet wird. 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 die die beiden Endpunkte gegeneinander 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

7.1.1 Root-CA-Zertifikatsprofil

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	[6f b8 e3 d6 dc a1 f6 bb]
Signaturalgorithmus	Kennzeichner (OID) Signaturalgorithmus	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signaturhashalgorithmus	Kennzeichner (OID) Signaturhashalgorithmus	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Kennzeichner (OID) Schlüsselalgorithmus	RSA (1.2.840.113549.1.1.1)
Schlüssellänge	Schlüssellänge	4096 Bits
Aussteller		
countryName (2.5.4.6)	Name Land	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
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	2017-10-09 08:57:57 UTC

	Ende	2037-10-09 08:57:56 UTC
Inhaber		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName (2.5.4.3)	Name Inhaber	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 Schlüssels des Inhabers	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssels des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Verweis auf Aussteller und Dienst zur Statusabfrage	s. folgende Elemente
calssuers (1.3.6.1.5.5.7.48.2)	URL zur Aussteller-Info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	http://ocsp.zs.bnotk.de/eqsig

7.1.2 Sub-CA Zertifikatsprofil

Feld (OID)	Beschreibung	Wert
Version	x.509-Versionsnummer	V3 (2)
serialNumber (2.5.4.5)	Seriennummer des Zertifikats	[6f b8 e3 d6 dc a1 f6 bb]
Signaturalgorithmus	Kennzeichner (OID) Signaturalgorithmus	SHA512withRSAandMGF1 (1.2.840.113549.1.1.10)
Signaturhashalgorithmus	Kennzeichner (OID) Signaturhashalgorithmus	SHA-512 (2.16.840.1.101.3.4.2.3)
algorithmIdentifier	Kennzeichner (OID) Schlüsselalgorithmus	RSA (1.2.840.113549.1.1.1)
Schlüssellänge	Schlüssellänge	4096 Bits
Aussteller		
countryName (2.5.4.6)	Name Land	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
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	2017-10-09 08:57:57 UTC
	Ende	2037-10-09 08:57:56 UTC
Inhaber		
countryName	Name Land	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 qSig CA 2017
Erweiterungen		
keyUsage (2.5.29.15)	Verwendungszweck	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=Zertifizierungsstelle Einschränkung Pfadlänge=0
subjectKeyIdentifier (2.5.29.14)	Identifizierung öffentlicher Schlüssel des Inhabers	[CC53A403E638247DD255 DA0567EE7D78B940B3BA]
authorityKeyIdentifier (2.5.29.35)	Identifizierung öffentlicher Schlüssel des Ausstellers	[FDF35084308EEC239AF5 33B2E38107DDE4EF80AE]
authorityInfoAccess (1.3.6.1.5.5.7.1.1)	Verweis auf Aussteller und Dienst zur Statusabfrage	s. folgende Elemente
calssuers (1.3.6.1.5.5.7.48.2)	URL zur Aussteller-Info	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)	URL zum OCSP-Dienst	http://ocsp.zs.bnotk.de/eqsig

7.1.3 Teilnehmerzertifikatsprofil

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	2048 Bits
Aussteller		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = Bundesnotarkammer
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = DE122788238
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = Zertifizierungsstelle
commonName (2.5.4.3)	Name Inhaber	CN = BNotK qSig CA 2017
Gültigkeit		
UTCTime (1.3.6.1.4.1.1466.115.121.1.53)	Beginn	2017-10-09 08:57:57 UTC
	Ende	2024-10-09 08:57:56 UTC
Inhaber		
countryName (2.5.4.6)	Name Land	C = DE
organizationName (2.5.4.10)	Name Organisation	O = [Organisation]
organizationIdentifier (2.5.4.97)	Identifizierung Organisation	2.5.4.97 = [Kennzeichner Organisation]
organizationalUnitName (2.5.4.11)	Name Organisationseinheit	OU = [Abteilung]
commonName (2.5.4.3)	Name Inhaber	CN = Vorname(n) Nachname

serialNumber (2.5.4.5)		Kennzeichner Inhaber	2.5.4.5 = (ggf. lokal definierte) Identifikationsnummer
givenName (2.5.4.42)		Vorname Inhaber	2.5.4.42 = Vorname(n)
surname (2.5.4.4)		Nachname Inhaber	2.5.4.4 = Nachname
title (2.5.4.12)		Titel Inhaber	2.5.4.12 = Titel
emailAdress (1.2.840.113549.1.9.1)		E-Mail-Adresse Inhaber	emailAdress = [name@domain.tld]
Erweiterungen			
keyUsage (2.5.29.15)		Verwendungszweck	nonRepudiation
basicConstraints (2.5.29.19)		Beschränkungen bzgl. Verwendung des Zertifikats	Typ Antragsteller=End Entity Einschränkung Pfadlänge=None
subjectKeyIdentifier (2.5.29.14)		Identifizierung öffentlicher 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	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
ocsp (1.3.6.1.5.5.7.48.1)		URL zum OCSP-Dienst	http://ocsp.zs.bnotk.de/eqsig
CertificatePolicies (2.5.29.32)		Verweis auf geltende Zertifizierungsrichtlinie	s. folgende Elemente
Policy Information	policyIdentifier	Kennzeichner (OID) und URL-Verweis auf CP	1.3.6.1.4.1.41460.5.1.1.1.2.1.3
	policyQualifier		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
Policy Information	policyIdentifier	Kennzeichner (OID) und URL-Verweis auf CPS	1.3.6.1.4.1.41460.5.2.1.1.2.2.3
	policyQ		https://zertifizierungsstelle.bnotk.de/veroeffent

	ualifier		lichungen
Policy Information	policyIdentifier	Kennzeichner (OID) und URL-Verweis auf PDS	1.3.6.1.4.1.41460.5.3.1.1.2.2.2
	policyQualifier		https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
qcStatements (1.3.6.1.5.5.7.1.3)		Kennzeichner (OID) eIDAS-Konformität qSig	s. folgende Elemente
QcCompliance (0.4.0.1862.1.1)		Qualifiziertes Zertifikat	0.4.0.1862.1.1
QcSSCD (0.4.0.1862.1.4)		Erzeugung auf SSCD	0.4.0.1862.1.4
QcType (0.4.0.1862.1.6)		Typ (Elektr. Signatur)	0.4.0.1862.1.6.1
QcPDS (0.4.0.1862.1.5)		URL-Verweis auf PDS	https://zertifizierungsstelle.bnotk.de/veroeffentlichungen
subjectAltName (2.5.29.17)		E-Mail-Adresse Inhaber	[name@domain.tld]
Subject Directory Attributes (2.5.29.9)		Zusätzliche den Inhaber bzw. Das Zertifikat beschreibende Merkmale	s. folgende Elemente
dateOfCertGen (1.3.36.8.3.1)		Datum der Zertifikats-Erstellung	2017-10-09 08:57:57 UTC
integratedCircuitCardSerialNumber (1.3.36.8.3.6)		Eindeutige Identifizierung der SSCD	[VDA-spezifische ID]
admission (1.3.36.8.3.3)		Berufliche Attribute Inhaber	[admissionAuthorithy, namingAuthorithy, 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]

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 und unterstützt auch Positivauskünfte (certHash-Erweiterung). Die Antworten des OCSP-Responders sind qualifiziert signiert.

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

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

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/