

# Leitfaden Kriterien zur Übernahme in DA:VE

## 1. Das „Dauerhafte Verzeichnis“ (DA:VE)

### 1.1. DA:VE als Mittel zur Wahrung der Dienstekontinuität

Die Bundesnetzagentur hat mit dem Dauerhaften Verzeichnis (DA:VE)<sup>1</sup> eine Vertrauensinfrastruktur geschaffen, die in der Lage ist, sowohl qualifizierte elektronische Zertifikate als auch die dazugehörigen Statusauskünfte von qualifizierten Vertrauensdiensteanbietern, die beabsichtigen, ihren Betrieb einzustellen, zu übernehmen und deren dauerhafte Nachprüfbarkeit zu gewährleisten. Sie kommt damit ihrem gesetzlichen Auftrag gemäß § 16 Abs. 1 sowie 5 des Vertrauensdienstegesetzes (VDG) nach und ermöglicht die Dienstekontinuität i.S.d. Art. 24 Abs. 2 Buchstabe i der Verordnung (EU) Nr. 910/2014.

Bei der Erstellung der Vertrauensinfrastruktur wurde versucht, dem breiten Markt möglichst gerecht zu werden und eine breite Kompatibilität zu ermöglichen. Trotzdem kann es im Einzelfall zu Problemen kommen, für die im Abstimmungsprozess (Ziffer 1.3.1) bereits vor Übergabe eine Lösung herbeiführt werden muss. Aus diesem Grund sind die nachfolgenden technischen Anforderungen einzuhalten bzw. eine Kompatibilität herzustellen und Liste zur Überprüfung bereitzustellen.

Zu beachten ist hierbei, dass eine Übernahme nur für solche qualifizierten elektronischen Zertifikate erfolgen kann, die bereits gesperrt wurden oder deren Gültigkeitszeitraum abgelaufen ist. Das bedeutet, dass zuvor eine Sperrung der noch gültigen qualifizierten elektronischen Zertifikate gemäß § 14 Abs. 1 Nr. 3 VDG und § 16 Abs. 1 S. 2 VDG vom Vertrauensdiensteanbieter unter Angabe des entsprechenden Widerrufsgrundes (§ 4 Abs. 4 VDV) erfolgt sein muss. Das hat den Grund, dass der Status der übernommenen qualifizierten elektronischen Zertifikate und deren Statusauskünfte sich nach der Übernahme und der Einholung von Statusauskünften nicht mehr ändern dürfen, um dauerhaft eindeutige Prüfergebnisse gewährleisten zu können. Es kann und wird keine Änderung des Status eines übernommenen qualifizierten elektronischen Zertifikats durch die Bundesnetzagentur erfolgen.

DA:VE ist darüber hinaus in der Lage, für Zertifikate, für die der Bundesnetzagentur eindeutige Statusauskünfte vorliegen, aber keine OCSP-Auskünfte übergeben wurden, ausnahmsweise aus den vorhandenen Sperr-/Widerrufsinformationen „eigene“ OCSP-Statusauskünfte zu erstellen. Das soll aber eine Ausnahme zur Sicherung der Dienstkontinuität und des Verbraucherschutzes darstellen, die sich in der Regel auf Altbestände an Zertifikate bezieht, für die die Erstellung und Einholung von Auskünften technisch nicht mehr möglich ist.

Sind alle zu übernehmenden qualifizierten elektronischen Zertifikate in die Vertrauensinfrastruktur eingeflossen und ist die finale Betriebseinstellung vollzogen, kann durch eine Umstellung der bisherigen URL/IP-Adresse der Vertrauensinfrastruktur des Vertrauensdiensteanbieters auf die Bundesnetzagentur die Übernahme der Erteilung von Statusauskünften durch die Bundesnetzagentur abschließend erfolgen. Hierzu stellt der (ehemalige) Vertrauensdiensteanbieter frühzeitig die Übergabe und Kontinuität der Domain seines OCSP-Responders (bspw. [ocsp.des-vertrauensdiensteanbieters.de](https://ocsp.des-vertrauensdiensteanbieters.de)) der Bundesnetzagentur zur Verfügung (s. 1.3.4).

---

<sup>1</sup> [https://www.elektronische-vertrauensdienste.de/cln\\_121/EVD/DE/Nutzer/AuskunftDAVE/start.html](https://www.elektronische-vertrauensdienste.de/cln_121/EVD/DE/Nutzer/AuskunftDAVE/start.html)

Die Vertrauensinfrastruktur der Bundesnetzagentur ist darüber hinaus in der Lage, die langfristige Prüfbarkeit der übernommenen qualifizierten elektronischen Zertifikate und der zugehörigen Statusauskünfte durch eine Beweiswerterhaltung (§ 15 VDG) zu sichern. Hierzu wird die Eignung der verwendeten Algorithmen laufend überwacht und rechtzeitig eine Beweiswerterhaltung angestoßen.

Die Aufrechterhaltung des Betriebs und die Anpassung der Vertrauensinfrastruktur an den jeweiligen Stand der Technik und die Marktbegebenheiten ist ein fortlaufender Prozess, für den die aktuellen Begebenheiten im Auge zu behalten sind und der die Mithilfe der Marktteilnehmer voraussetzt. Hierfür wurde das Funktionspostfach [dave@bnetza.de](mailto:dave@bnetza.de) eingerichtet.

## 1.2. Technische Schnittstellen zur Übernahme in DA:VE

DA:VE ist in der Lage, mit den nachfolgenden Dateiformaten umzugehen bzw. benötigt nachfolgende Syntax:

### a) Elektronische Zertifikate

- Elektronische Zertifikate gemäß X.509, RFC 5280, ETSI EN 319 411, ETSI EN 319 412, nach mindestens nachfolgenden Kodierungsverfahren:
  - DER (typische Dateiendungen: .der, .cer, .crt) und
  - Base64 (typische Dateiendungen: .pem, .cer, .crt)

### b) Status-/Widerrufsinformationen

- Sperrlisten (CRL) gemäß X.509 bzw. RFC 5280, ETSI EN 319 411, die im Falle des automatisierten Abrufs von HTTP- und LDAP-URLs geladen und eingelesen werden können
- Abruf/Import über das OCSP-Protokoll gemäß RFC 6960 von OCSP-Antworten, die konform zu RFC 6960 und ETSI EN 319 411 erstellt wurden.
- Die finalen OCSP-Antworten sollen im Next-Update-Feld den Wert „99991231235959Z“ (gemäß ETSI EN 319 411-1, CSS-6.3.10-11) enthalten. Abweichungen sind nur in begründeten Ausnahmefällen zulässig.

## 1.3. Prozess zur Übernahme in DA:VE

### 1.3.1. Abstimmungsprozess

Nach erfolgter Anzeige der Absicht, den Betrieb des Vertrauensdienstes einzustellen, beginnt unverzüglich der Abstimmungsprozess, in dem ein Zeitplan sowie die Umsetzung der weiteren Anforderungen dieses Dokuments bzw. des Beendigungsplans abzustimmen sind.

Für diesen Prozessschritt ist eine verschlüsselte Kommunikation möglich. Auf den [Internetseiten zu elektronischen Vertrauensdiensten](#) der Bundesnetzagentur wird hierfür ein entsprechendes Zertifikat zum Download angeboten (Kontaktfeld unten auf der Seite).

Aus technischer Sicht ist mindestens abzustimmen bzw. vom Anbieter frühzeitig zu kommunizieren:

- Der Umfang der zu übernehmenden Daten (1.3.2)
- Der Zeitpunkt und die Art der Übernahme/Umleitung der Verzeichnisdienst-URL (1.3.4)
- Übernahmeweg und Übernahmemedien (1.3.5)
- Geplanter Zeitrahmen

### **1.3.2. Umfang der zu übergebenden elektronischen Daten**

Zu übergeben sind gemäß § 16 Abs. 1 VDG folgende elektronische Daten:

- Alle vom Vertrauensdiensteanbieter ausgegebenen qualifizierten elektronischen Zertifikate zur Erzeugung qualifizierter elektronischer Signaturen und Siegel,
- Alle qualifizierten und nicht-qualifizierten Zertifikate, die zur Ausstellung qualifizierter elektronischer Zertifikate vom Vertrauensdiensteanbieter genutzt wurden,
- Alle Widerrufsinformationen zu den zu übergebenden qualifizierten elektronischen Zertifikaten in Form OCSP-Antworten. In begründeten Ausnahmefällen sind auch Sperrlisten möglich, jedoch ist grundsätzlich sicherzustellen, dass die Widerrufsinformationen vollständig sind und sämtliche übergebenen Zertifikate abdecken.

Zur Gewährleistung der Dienstkontinuität (dauerhafte Prüfbarkeit) muss zudem sichergestellt werden, dass die URLs, unter denen der Verzeichnisdienst des Vertrauensdiensteanbieters erreichbar war/ist, übergeben oder umgeleitet werden (s. 1.3.4).

### **1.3.3. Konsistenzcheck der zu übergebenden Daten**

Zu beachten ist, dass die Bundesnetzagentur nur für solche Zertifikate eine dauerhafte Prüfbarkeit gewährleisten kann, für die eindeutige Sperr-/Widerrufsinformationen vorliegen. Der in Betriebseinstellung befindliche Vertrauensdiensteanbieter muss daher vor seiner Betriebseinstellung und vor Übergabe der notwendigen Unterlagen an die Bundesnetzagentur einen Konsistenzcheck durchführen. Dabei ist zu prüfen, dass keine widersprüchlichen Informationen übermittelt werden.

Praktische Beispiele für widersprüchlichen Informationen:

- Zertifikats-Statusinformationen, die nicht final sind (Status „unbekannt“)
- Unterschiedliche Sperr-/Widerrufsinformationen in Sperrlisten und OCSP-Antworten
- Mehrere Sperrlisten mit unterschiedlichen Einträgen
- Widersprüche zwischen Betriebsdokumentation und Zertifikatsstatus
- Statistische Ungereimtheiten (abweichende Zertifikatszahlen, Dopplungen etc.)

Treten im Rahmen dieses Konsistenzchecks Auffälligkeiten/Widersprüche in den Daten auf oder bestehen Zweifel an der Korrektheit der elektronischen Daten oder innerhalb der zu übergebenden Dokumentation, ist dies bei der Bundesnetzagentur anzuzeigen und bei der Übergabe entsprechend zu dokumentieren.

Eine nachträgliche Änderung an den elektronischen Daten oder der zu führenden Dokumentation darf nicht vorgenommen werden.

Sind elektronische Daten, bspw. Zertifikate oder Sperr-/Widerrufsinformationen, nicht konsistent, so sind diese Daten gesondert gemäß Ziffer 1.3.5.1, Buchstabe b oder c zu

übergeben. Die Bundesnetzagentur wird für Datensätze, deren Korrektheit nicht sichergestellt werden kann, keine dauerhafte Überprüfbarkeit gewährleisten können. Auskünfte nach § 16 Abs. 3 VDG und weiteren einschlägigen Gesetzen bleiben hiervon unberührt.

Die Daten und Übersichten, die zum Konsistenzcheck erzeugt oder herangezogen wurden, sollen der Bundesnetzagentur als übernehmende Instanz im Rahmen der Betriebseinstellung übergeben werden.

#### **1.3.4. Übergabe/Umleitung der OCSP-Adresse**

Vor Betriebseinstellung sind sämtliche Adressen, unter denen der Verzeichnisdienst des in Einstellung befindlichen Vertrauensdiensteanbieters erreichbar war und die als OCSP-Pfad in den übergebenen Zertifikaten angegeben wurden, auf „ocsp.bundesnetzagentur.de“ umzuleiten, damit zukünftige Anfragen an DA:VE gestellt und dadurch weiterhin beantwortet werden können. Die Umleitung darf als Ziel ausschließlich den genannten Namen, nicht jedoch eine entsprechende IP-Adresse verwenden. Die verwendeten Ports sind näher mit der Bundesnetzagentur abzuklären.

#### **1.3.5. Qualifizierte elektronische Zertifikate und Statusauskünfte**

Es ist sicherzustellen, dass die zu übergebenden qualifizierten elektronischen Zertifikate sowie der Status zum Zeitpunkt der endgültigen Betriebseinstellung von der Bundesnetzagentur nahtlos in die jeweiligen Auskunftssysteme übernommen werden können. Hierzu sind die unter Ziffer 1.2 genannten Schnittstellen zu beachten.

Es sind ausschließlich qualifizierte elektronische Zertifikate zu übergeben, deren Gültigkeitszeitraum entweder bereits abgelaufen ist oder die gemäß § 14 Abs. 1 Nr. 3 VDG und § 16 Abs. 1 S. 2 VDG vom Vertrauensdiensteanbieter unter Angabe des entsprechenden Widerrufsgrundes (§ 4 Abs. 4 VDV) gesperrt wurden.

Auch sind nur solche qualifizierten elektronischen Zertifikate zu übergeben, die vom Vertrauensdiensteanbieter nachprüfbar gehalten wurden.

Es ist zu beachten, dass nur für die Zertifikate separate Statusauskünfte an die Bundesnetzagentur übergeben werden dürfen, für die kein automatischer Abruf (1.3.5.1, Buchstabe a) möglich war. Das dient der Konsistenz und Vermeidung von Widersprüchen.

##### **1.3.5.1. Übernahmewege und Übernahmemedien**

Die Übernahme von qualifizierten elektronischen Zertifikaten kann entweder durch automatisierten Abruf durch die Bundesnetzagentur (a) oder durch sichere Übergabe an die Bundesnetzagentur durch den Vertrauensdiensteanbieter erfolgen (b, c):

- a) Die Bundesnetzagentur fragt nach vorheriger Absprache vor endgültiger Betriebseinstellung des Vertrauensdiensteanbieters sein Verzeichnis zur Erteilung von Statusauskünften an, holt die dort vorgehaltenen Zertifikate (über LDAP) und Statusauskünfte (über OCSP) ein und speichert die Daten zur Gewährleistung dauerhafter Prüfbarkeit (Art. 24 Abs. 2 Buchstabe i der Verordnung (EU) Nr. 910/2014 sowie § 16 Abs. 5 VDG; sog. Dienstekontinuität).

- b) Zertifikate und Statusauskünfte, die nicht gemäß Ziffer 1 eingeholt werden können, etwa weil der Zertifikatsinhaber dem Abrufbarhalten/Download seines Zertifikats nicht zugestimmt hat, sind der Bundesnetzagentur vom Vertrauensdiensteanbieter auf einem Datenträger sicher und integritätsgeschützt zu übergeben und werden dann manuell unter Abgleich mit den übermittelten Übersichtsdokumenten (1.3.6) in das Verzeichnis aufgenommen. Sofern eine Statusanfrage nach Buchstabe a) für diese Zertifikate nicht mehr erfolgen kann, sind vom Vertrauensdiensteanbieter finale OCSP-Antworten auf demselben Weg zu übergeben.
- c) Zertifikate und Statusauskünfte können nach vorheriger Absprache auch verschlüsselt und mit einer qualifizierten elektronischen Signatur versehen elektronisch übergeben werden. Die Anforderungen aus Buchstabe b) gelten entsprechend.

Sowohl ein Abruf (a) als auch das Zusammenstellen der Daten zur Übergabe (b) bzw. Übermittlung (c) kann erst erfolgen, nachdem alle Statusinformationen der zu übergebenden qualifizierten elektronischen Zertifikate endgültig sind, sich der Status einzelner Zertifikate also nicht mehr ändern kann. Der Verpflichtung zur Sperrung noch gültiger Zertifikate gemäß § 14 Abs. 1 Nr. 3 und § 16 Abs. 1 S. 2 VDG muss der Vertrauensdiensteanbieter zu diesem Zeitpunkt bereits nachgekommen sein.

Unabhängig davon, ob die Zertifikate durch die Bundesnetzagentur abgerufen oder vom Vertrauensdiensteanbieter übergeben werden, ist zu beachten:

- Qualifizierte elektronische Zertifikate können in ZIP-Containern übermittelt werden. Hierbei ist darauf zu achten, dass der Container nicht mehr als zwei Ebenen haben soll. Dabei sollen abrufbare und nicht-abrufbare Zertifikate sowie Dienstzertifikate voneinander getrennt geordnet werden.
- Die Zertifikatsnamen (Dateinamen) sollen möglichst kurz und ohne die Nennung personenbezogener Daten gesetzt werden. Soweit möglich, ist die Zertifikatsnummer als Dateiname zu setzen.
- Die finalen Widerrufsinformationen (OCSP-Antworten) müssen im Next-Update-Feld den Wert „99991231235959Z“ enthalten (siehe ETSI EN 319 411-2, Kap. 6.3.10).
- Werden Sperr-/Widerrufsinformationen nicht oder nicht nur in Form von OCSP-Antworten übergeben/abgerufen, ist nur eine finale Sperrliste zu übergeben, deren Inhalt ggf. ebenso übergebener Statusauskünfte nicht widersprechen darf.
- Als Übergabemedium zu Buchstabe b) sollen nur CDs, DVDs, Blu-Ray-Discs oder Millennial-Discs verwendet werden. Ausnahmen hiervon bedürfen vorheriger Absprache mit der Bundesnetzagentur.

#### **1.3.5.2. Elektronische Root- und CA-Zertifikate (Dienstzertifikate)**

Sämtliche vom in Betriebseinstellung befindlichen Vertrauensdiensteanbieter selbst ausgestellten und genutzten Root- und CA-Zertifikate sind der Bundesnetzagentur separat zu übergeben, auch wenn diese dem Grunde nach auch aus dem Verzeichnis abrufbar waren.

Dabei ist zudem vom Vertrauensdiensteanbieter eine Erklärung abzugeben, ob diese Zertifikate abrufbar bzw. zum Download bereitgehalten wurden.

Zur Gewährleistung der Dienstkontinuität wird die Bundesnetzagentur diese Zertifikate auf Ihrer Homepage zum Download vorhalten.

#### **1.3.5.3. Nicht abrufbare oder nicht zum Download vorgehaltene qualifizierte elektronische Zertifikate**

Qualifizierte Endnutzerzertifikate, die vom Vertrauensdiensteanbieter nicht zum Abruf oder Download bereitgestellt wurden, können von der Bundesnetzagentur nicht auf elektronischem Wege per LDAP in DA:VE übernommen werden und sind daher gemäß Ziffer 1.3.5.1, Buchstaben b und c mitsamt einer Erklärung und Bezifferung der Anzahl zu übergeben bzw. übermitteln.

#### **1.3.6. Erläuternde Übergabedokumente**

Als Übergabebeleg sowie zur Prüfung auf Vollständigkeit im Rahmen des Importprozesses, sind seitens des betriebseinstellenden Vertrauensdiensteanbieters Unterlagen bei der Bundesnetzagentur zu hinterlegen und eine Erklärung abzugeben, dass der übergebene Datenbestand dem in der Übersicht enthaltenen Datenbestand entspricht und vollständig ist.

Aus den übergebenen Unterlagen soll mindestens hervorgehen:

- Anzahl der übergebenen Zertifikate
- Wie viele und welche Zertifikate wegen Einstellung des Betriebs gemäß § 14 Abs. 1 Nr. 3 VDG und § 16 Abs. 1 S. 2 VDG gesperrt wurden
- Genutzte Dateiformate, die nicht Ziffer 3.2 entsprechen
- Das Ergebnis des internen Konsistenzchecks (s. 1.3.3)
- Wie viele und welche Root- und CA-Zertifikate übergeben wurden (s. 1.3.5.2)
- Wie viele und welche Zertifikate nicht zum Download vorgehalten und übergeben wurden (s. 1.3.5.3)
- Für wie viele der übergebenen Zertifikate keine Statusauskunft übergeben wurde
- Wie viele Statusauskünfte übergeben/übermittelt wurden
- Welche Sperrliste(n) übergeben wurden

Dies dient der Vermeidung von Fehlern, der Revisionssicherheit sowie dem Verbraucherschutz.

Die übergebenen Listen müssen in einem durchsuchbaren Standardformat (vorzugsweise als PDF-Dokument), möglichst versehen mit einem prüfbaren Integritätsschutz, übergeben werden. Zudem muss die Gesamtanzahl übergebener Zertifikate sowie die jeweilige Teilmenge (s.o.; bspw. übergebene nicht-abrufbare Zertifikate) von qualifizierten elektronischen Zertifikaten jeweils klar und eindeutig erkennbar sein.

Die übergebene Liste(n) ist vom Vertreter des Vertrauensdiensteanbieters zu unterzeichnen und die Vollständigkeit der übergebenen Unterlagen damit zu bestätigen. Dies soll in der Regel im Rahmen der persönlichen Übergabe erfolgen.