Informationen zur Aufsicht über Vertrauensdienste

Geschäftsstelle der Aufsichtsstelle für Vertrauensdienste

Stand: 17. August 2026

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)

Mariahilfer Straße 77–79
1060 Wien, Österreich
www.rtr.at

E: rtr@rtr.at
T: +43 1 58058 - 0

FN 208312t, HG Wien
UID-Nr.: ATU43773001

Inhaltsverzeichnis

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)

Mariahilfer Straße 77–79
1060 Wien, Österreich
www.rtr.at

E: rtr@rtr.at
T: +43 1 58058 - 0

FN 208312t, HG Wien
UID-Nr.: ATU43773001

RTR

Zweck dieses Dokuments

Dieses Dokument enthält Informationen für Vertrauensdiensteanbieter (VDA), die im österreichischen Hoheitsgebiet niedergelassen sind. Es enthält Vorgaben für Anzeigen, Anträge und andere Anbringen, beschreibt überdies Methoden der Aufsichtsstelle, insbesondere für den Beginn der Erbringung qualifizierter Vertrauensdienste, und umfasst eine Liste der maßgeblichen Rechtsvorschriften und Links zu einschlägigen technischen Normen. Das vorliegende Dokument enthält auch jene Angaben, die die Aufsichtsstelle für Vertrauensdienste gemäß Art. 2 Durchführungsverordnung (EU) 2025/1572 öffentlich zugänglich zu machen hat.

1 Kontaktangaben

1.1 Allgemeine Möglichkeiten der Kontaktaufnahme

Aufsichtsstelle für Vertrauensdienste ist die Telekom-Control-Kommission. Geschäftsstelle der Aufsichtsstelle ist die Rundfunk und Telekom Regulierungs-GmbH. Die Kontaktaufnahme mit der Aufsichtsstelle erfolgt über die Geschäftsstelle.

Schreiben sind an folgende Anschrift zu senden:

Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)
Elektronische Signaturen und Vertrauensdienste
Mariahilfer Straße 77-79
1060 Wien

Telefonisch ist die Geschäftsstelle montags bis donnerstags von 8 bis 16 Uhr und freitags von 8 bis 14 Uhr unter der Rufnummer +43 1 58058 0 erreichbar.

E-Mails können an die Adresse signatur@signatur.rtr.at gesendet werden.

1.2 Anzeigen, Anträge und andere Anbringen

Anzeigen, Anträge und andere Anbringen sind in deutscher Sprache[1] elektronisch über das Einbringungsportal einzubringen. Dabei ist keine themenspezifische Applikation zu verwenden. Um eine rasche Zuordnung zu ermöglichen, empfiehlt es sich, den Betreff mit dem Präfix *„Vertrauensdienste:“* zu beginnen und die Art des Anbringens anzugeben:

- *„Vorfall“* – Mitteilung einer Sicherheitsverletzung, eines Sicherheitsverstoßes oder einer Störung (Art. 19a Abs. 1 lit. b und Art. 24 Abs. 2 lit. fb eIDAS-VO);

[1] Anbringen sind jedenfalls in deutscher Sprache als Amtssprache gemäß Art. 8 Abs. 1 B-VG einzubringen. Beilagen, die nicht vom VDA stammen und nur in englischer Sprache existieren (z. B. Konformitätsbewertungsberichte) brauchen jedoch nicht übersetzt zu werden. Dokumente des Vertrauensdiensteanbieters (z. B. Trust Service Practice Statements, Trust Service Policies, Information Security Policy und allgemeine Geschäftsbedingungen) können nur dann in englischer statt in deutscher Sprache vorgelegt werden, wenn sich die betroffenen Vertrauensdienste nicht an österreichische Verbraucher richten. Sofern derartige Dokumente zwei- oder mehrsprachig herausgegeben werden, dürfen die anderen Sprachversionen von der deutschen inhaltlich nicht abweichen.

- *„Vertrauensliste“* – Antrag auf Aufnahme eines oder mehrerer nichtqualifizierter Vertrauensdienste in die Vertrauensliste (§ 14 Abs. 1 SVG in Verbindung mit Art. 22 eIDAS-VO);
- *„Neue Vertrauensdienste“* – Mitteilung der Absicht, mit der Erbringung eines oder mehrerer qualifizierter Vertrauensdienste zu beginnen (Art. 21 Abs. 1 eIDAS-VO);
- *„Konformitätsbewertungsbericht“* – Wiederkehrende Vorlage eines Konformitätsbewertungsberichts (Art. 20 Abs. 1 eIDAS-VO);
- *„Identifizierungsmethode“* – Vorlage der Bestätigung einer Konformitätsbewertungsstelle für die Konformität einer oder mehrerer Identifizierungsmethoden bzw. Methoden zur Überprüfung von Attributen (Art. 24 Abs. 1a lit. c und Art. 24 Abs. 1b lit. d eIDAS-VO);
- *„Änderung“* – Unterrichtung über bevorstehende Änderungen oder die Einstellung qualifizierter Vertrauensdienste (Art. 24 Abs. 2 lit. a eIDAS-VO);
- *„Vertrauenswürdige Systeme“* – Nachweis der Eignung vertrauenswürdiger Systeme, z. B. bei Anwendung von ETSI EN 319 411-1 anhand der in Anforderung OVR-6.5.2-01 vorgeschriebenen IT-Sicherheitszertifizierung (Art. 24 Abs. 2 lit. e eIDAS-VO);
- *„Qualifizierte Signatur- oder Siegelerstellungseinheiten“* – Nachweis der Zertifizierung qualifizierter elektronischer Signatur- bzw. Siegelerstellungseinheiten (Art. 30 Abs. 1 und Art. 39 Abs. 2 eIDAS-VO);
- *„Informationen“* – Übermittlung von Informationen oder Unterlagen aufgrund bescheidmäßig erteilter Auflagen;
- *„Sonstiges Anbringen“.*

Im Zuge der Einbringung können bis zu zwölf Beilagen in bestimmten Formaten (PDF, XML-basierte Office-Formate [.docx, .xlsx, .pptx], Rastergrafiken [JPEG, PNG, TIFF], CSV und ZIP) mit einer Gesamtgröße von bis zu 20 MB hochgeladen werden. Sind mehr als zwölf Dateien oder Dateien in anderen Formaten zu übermitteln, so können sie in eine ZIP-Datei gepackt und in dieser Form hochgeladen werden. Sollte die Gesamtgröße 20 MB überschreiten, so können die Dateien auf zwei oder mehrere Einbringungen verteilt werden, die jeweils mit einem Hinweis auf die Mehrteiligkeit des Anbringens versehen werden sollten. Am Ende jeder Einbringung kann man eine amtssignierte Bestätigung herunterladen, die den Zeitpunkt der Einbringung angibt und die hochgeladenen Beilagen in Form von PDF-Anhängen enthält.

2 Beginn der Erbringung eines qualifizierten Vertrauensdienstes

2.1 Mitteilung an die Aufsichtsstelle und vorzulegende Unterlagen

Wer als VDA beabsichtigt, die Erbringung qualifizierter Vertrauensdienste zu beginnen, hat dies der Aufsichtsstelle vorab mitzuteilen. Für die Mitteilung ist das Einbringungsportal (siehe Punkt 1.2) zu verwenden. Folgende Informationen müssen aus der Mitteilung hervorgehen:

- Name, Telefonnummer, E-Mail-Adresse, Postanschrift und, sofern vorhanden, weitere Geschäftsbezeichnungen des VDA;

- sofern der VDA eine juristische Person ist:
  - Firmenbuchnummer des VDA, sofern dieser ins Firmenbuch eingetragen ist;
  - Umsatzsteuer-Identifikationsnummer des VDA, sofern vorhanden;
  - *Legal Entity Identifier* gemäß ISO 17442, sofern vorhanden;
  - allenfalls weitere *Semantics Identifier* des VDA gemäß ETSI EN 319 412-1 V1.7.1 (2026-05), Abschnitt 5.1.4;
  - Name des Mitgliedstaats, in dem der VDA niedergelassen ist;
  - Namen der Personen, die die Mitteilung im Namen der juristischen Person unterzeichnen oder übermitteln;
  - Anzahl der Beschäftigten des VDA;
  - Jahresumsatz und Jahresbilanzsumme des VDA, sofern noch kein Jahresabschluss verfügbar ist (ggf. Schätzwerte für das laufende Geschäftsjahr);
- sofern der VDA eine natürliche Person ist:
  - Art und Nummer des amtlichen Lichtbildausweises des VDA (nach Möglichkeit Reisepass oder Personalausweis);
  - allenfalls weitere *Semantics Identifier* des VDA gemäß ETSI EN 319 412-1 V1.7.1 (2026-05), Abschnitt 5.1.3;
  - Geburtsdatum;
- Internetadressen (*Uniform Resource Identifiers*), unter denen Nutzer zusätzliche Informationen über den VDA erhalten können:
  - Webseite in deutscher Sprache mit Angaben zur Kontaktaufnahme mit einem Kundendienst oder einer Hotline;
  - Webseite in englischer Sprache mit Angaben zur Kontaktaufnahme mit einem Kundendienst oder einer Hotline;
  - Webseite in deutscher Sprache mit Beschreibungen der aktuellen und früheren Fassungen von Practice Statements, Policies, allgemeinen Geschäftsbedingungen und sonstigen generischen Informationen über die vom VDA erbrachten qualifizierten Vertrauensdienste;
  - Webseite in englischer Sprache mit Beschreibungen der aktuellen und früheren Fassungen von Practice Statements, Policies, allgemeinen Geschäftsbedingungen und sonstigen generischen Informationen über die vom VDA erbrachten qualifizierten Vertrauensdienste;[2]
- für jeden Vertrauensdienst, den der VDA als qualifizierten Vertrauensdienst zu erbringen beabsichtigt:
  - eine oder mehrere Kennungen und ggf. Zertifikate des Vertrauensdienstes zur Aufnahme in die Vertrauensliste im Einklang mit Durchführungsbeschluss (EU) 2015/1505 idgF;
  - *Service Type Identifier* gemäß ETSI TS 119 612 V2.4.1 (2025-08), Abschnitt 5.5.1;
  - Informationen, ob die im Rahmen des Vertrauensdienstes allenfalls ausgestellten Zertifikate für elektronische Signaturen, elektronische Siegel oder die Website-Authentifizierung verwendet werden;
  - bei Bedarf weitere *Service Information Extensions* gemäß ETSI TS 119 612 V2.4.1 (2025-08), Abschnitt 5.5.9;
  - beabsichtigtes Datum des Beginns der Erbringung des Vertrauensdienstes;

[2] Die genannten Webseiten sind gemäß ETSI TS 119 612 V2.4.1 (2025-08), Abschnitte 5.1.4, 5.3.5.2 und 5.3.7, jedenfalls in englischer Sprache bereitzustellen (dies bedeutet nicht, dass die dort verlinkten Dokumente in englischer Sprache vorliegen müssen). Auf entsprechende Webseiten in deutscher Sprache kann nur dann verzichtet werden, wenn sich die betroffenen Vertrauensdienste nicht an österreichische Verbraucher richten.

- Kontaktangaben der Konformitätsbewertungsstelle, die den Konformitäts-bewertungsbericht ausgestellt hat.

Als Teil der Mitteilung an die Aufsichtsstelle hat ein VDA folgende Unterlagen in elektronischer Form über das Einbringungsportal (siehe Punkt 1.2) vorzulegen:

- Risikoanalyse, die den in Art. 24 Abs. 2 lit. fa eIDAS-VO idgF genannten Maßnahmen zugrunde liegt;
- Risikoanalyse, die den in Art. 21 NIS-2-RL genannten Maßnahmen zugrunde liegt;
- Konformitätsbewertungsbericht einer akkreditierten Konformitätsbewertungs-stelle gemäß Art. 21 Abs. 1 eIDAS-VO idgF einschließlich der Dokumente, auf die im Konformitätsbewertungsbericht Bezug genommen wird;
- technische Berichte zur Untermauerung des Konformitätsbewertungsberichts, insbesondere:
  - Dokumentation der erfolgten Evaluierung im Zuge der Konformitätsbewertung (z. B. in Form eines Evaluation Report; vgl. auch ISO/IEC 17065:2012, Anforderung 7.4.9);
  - falls anwendbar, Bestätigungen einer Konformitätsbewertungsstelle gemäß Art. 24 Abs. 1a lit. c eIDAS-VO idgF und/oder Art. 24 Abs. 1b lit. d eIDAS-VO idgF einschließlich der zugehörigen Prüfberichte;
  - Zertifikate und zugrundeliegende Prüfberichte für kryptographische Module, die als vertrauenswürdige Systeme gemäß Art. 24 Abs. 2 lit. e und f eIDAS-VO idgF eingesetzt werden;
  - Zertifikate und zugrundeliegende Prüfberichte (Certification Reports einschließlich Security Targets nach Common Criteria oder dazu äquivalente Berichte einer gemäß Art. 30 Abs. 1 eIDAS-VO benannten Stelle) für die vom VDA eingesetzten oder unterstützten qualifizierten elektronischen Signatur- und/oder Siegelerstellungseinheiten gemäß Art. 30 eIDAS-VO idgF;
- Trust Service Practice Statements, Trust Service Policies, Information Security Policy und allgemeine Geschäftsbedingungen des VDA bzw. vergleichbare Dokumente, in denen detailliert beschrieben wird, in welcher Weise der VDA die Anforderungen für qualifizierte VDA erfüllt, einschließlich detaillierter Angaben zu den eingesetzten kryptographischen Algorithmen, Parametern und Protokollen, soweit sich dies nicht aus den zuvor genannten Berichten ergibt;
- Beendigungsplan gemäß Art. 24 Abs. 2 lit. i eIDAS-VO idgF;
- Firmenbuchauszug des VDA, sofern dieser ins Firmenbuch eingetragen ist;
- Nachweise in Bezug auf das Haftungsrisiko:
  - letzter verfügbarer Jahresabschluss des VDA oder sonstige Dokumente, die über die Eigenmittel, das eingezahlte Nennkapital, den Jahresumsatz und die Jahresbilanzsumme des VDA Aufschluss geben;
  - aktuelle Bestätigung über das Bestehen einer Haftpflichtversicherung, die Schäden im Sinne von Art. 13 eIDAS-VO idgF deckt, mit Angabe der Versicherungssumme und der Anzahl der gedeckten Versicherungsfälle pro Jahr.

2.2 Methode zur Überprüfung des VDA

Vertrauensdiensteanbietern, die die Erbringung qualifizierter Vertrauensdienste beabsichtigen, wird empfohlen, in einer möglichst frühen Phase dieses Vorhabens mit den zuständigen Experten der RTR-GmbH telefonisch oder per E-Mail (siehe Punkt 1.1) einen Termin zur informellen Besprechung der Rahmenbedingungen zu vereinbaren.

Die formelle Mitteilung an die Aufsichtsstelle gemäß Punkt 2.1 hat erst dann zu erfolgen, wenn eine hierfür akkreditierte Konformitätsbewertungsstelle die Erfüllung der in der eIDAS-VO idgF und Art. 21 NIS-2-RL festgelegten Anforderungen für den VDA und die beabsichtigten qualifizierten Vertrauensdienste bestätigt hat.[3] Der Mitteilung gemäß Punkt 2.1 ist zwingend der Konformitätsbewertungsbericht einer akkreditierten Konformitätsbewertungsstelle beizulegen.

Die Überprüfung durch die Aufsichtsstelle erfolgt in einem nach dem AVG geführten Verwaltungsverfahren. Nach Einlangen einer Mitteilung gemäß Punkt 2.1 wird diese in der Regel binnen drei Wochen von der Telekom-Control-Kommission behandelt. Die Telekom-Control-Kommission kann die RTR-GmbH als Geschäftsstelle beiziehen und diese mit einzelnen Tätigkeiten im Rahmen der Überprüfung des VDA beauftragen. Die Aufsichtsstelle überprüft, ob

- der VDA im Hoheitsgebiet der Republik Österreich niedergelassen ist,
- die angebotenen Dienste Vertrauensdienste im Sinne des Art. 3 Z 16 eIDAS-VO sind,
- alle Informationen und Unterlagen gemäß Punkt 2.1 vollständig vorliegen,
- die Konformitätsbewertungsstelle für die Durchführung von Konformitätsbewertungen gemäß eIDAS-VO akkreditiert ist (Liste der Europäischen Kommission) und der Akkreditierungsumfang die von der Konformitätsbewertungsstelle angewandten technischen Normen bzw. die geprüften Vertrauensdienste umfasst,
- der vorgelegte Konformitätsbewertungsbericht die Anforderungen erfüllt, die in den gemäß Art. 20 Abs. 4 eIDAS-VO erlassenen Durchführungsrechtsakten festgelegt sind,
- der Konformitätsbewertungsbericht alle für die Überprüfung durch die Aufsichtsstelle erforderlichen Informationen enthält (vgl. ETSI TS 119 403-3, Abschnitt 4.2),
- der Konformitätsbewertungsbericht und die technischen Berichte zur Untermauerung des Konformitätsbewertungsberichts hinreichend nachweisen, dass der VDA und die qualifizierten Vertrauensdienste, die er zu erbringen beabsichtigt, die in eIDAS-VO idgF (einschließlich der hierauf beruhenden Durchführungsrechtsakte, siehe Punkt 8.4), Art. 21 NIS-2-RL, DVO (EU) 2024/2690, SVG und SVV festgelegten Anforderungen erfüllt, und die genannten Berichte diesbezüglich vollständig, widerspruchsfrei und nachvollziehbar sind,
- der Konformitätsbewertungsbericht und die technischen Berichte zur Untermauerung des Konformitätsbewertungsberichts die Erfüllung der für

[3] Die Anforderungen gemäß Art. 21 NIS-2-RL müssen bei der Konformitätsbewertung gemäß Art. 21 Abs. 1 eIDAS-VO berücksichtigt werden – unabhängig von dem gemäß § 33 NISG 2026 gegenüber der Cybersicherheitsbehörde zu erbringenden Nachweis der Wirksamkeit von Risikomanagementmaßnahmen.

zertifizierte kryptographische Module sowie qualifizierte elektronische Signatur- und/oder Siegelerstellungseinheiten festgelegten Einsatzbedingungen ausweisen,
- der Konformitätsbewertungsbericht und die zugrundeliegende Dokumentation der Evaluierung leichte oder schwere Nichtkonformitäten ausweisen,
- die allenfalls ausgewiesenen Nichtkonformitäten behoben sind,
- die allenfalls noch bestehenden Nichtkonformitäten durch bescheidmäßige Auflagen behoben werden können,
- die finanziellen Ressourcen und die Haftpflichtversicherung des VDA für die Bewältigung von Haftungsrisiken ausreichen und
- der vorgelegte Beendigungsplan die Kontinuität der qualifizierten Vertrauensdienste, die der VDA zu erbringen beabsichtigt, nach den von der Aufsichtsstelle gemäß Art. 46b Abs. 4 lit. i eIDAS-VO und Art. 3 DVO (EU) 2025/2530 geprüften Vorgaben (unter Berücksichtigung der Fragen, wie die Informationen des VDA gemäß Art. 24 Abs. 2 lit. h eIDAS-VO idgF weiter zugänglich gehalten werden und wie ggf. die Zertifikatsdatenbank von einem anderen qualifizierten VDA oder der Aufsichtsstelle übernommen werden kann) sicherstellt.

Weist das Anbringen Mängel auf, so kann die Aufsichtsstelle dem VDA die Behebung des Mangels innerhalb einer angemessenen Frist mit der Wirkung auftragen, dass das Anbringen nach fruchtlosem Ablauf dieser Frist zurückgewiesen wird.

Bei der Überprüfung, ob der Vertrauensdiensteanbieter die Anforderungen gemäß Art. 21 NIS-2-RL erfüllt, arbeitet die Aufsichtsstelle gemäß Art. 21 Abs. 2 eIDAS-VO mit der Cybersicherheitsbehörde zusammen und tauscht Informationen mit dieser aus. Hierbei wird die Kommunikation jedenfalls durch Mechanismen geschützt, die der Sensibilität der übermittelten Informationen angemessen sind.

Im Zuge der Überprüfung kann die Aufsichtsstelle den VDA auffordern, weitere Informationen und/oder Unterlagen innerhalb einer angemessenen Frist vorzulegen. Die Aufsichtsstelle kann auch eine mündliche Verhandlung anberaumen und diese bei Bedarf mit einem Augenschein verbinden. Der VDA hat den im Auftrag der Aufsichtsstelle handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der Geschäftszeiten zu gestatten, die in Betracht kommenden Bücher und sonstigen Aufzeichnungen oder Unterlagen einschließlich der einschlägigen Informationen nach Art. 24 Abs. 2 lit. h eIDAS-VO idgF vorzulegen oder zur Einsicht bereitzuhalten, Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren.

Im Übrigen folgt das Ermittlungsverfahren den Bestimmungen des AVG. Bis zur Schließung des Ermittlungsverfahrens kann der verfahrenseinleitende Antrag (also die Mitteilung gemäß Punkt 2.1 einschließlich aller Beilagen) geändert werden. Somit können bei Bedarf Verbesserungen der vorgelegten Dokumente im laufenden Verfahren vorgenommen werden.

Dem VDA wird Gelegenheit gegeben, vom Ergebnis der Beweisaufnahme Kenntnis und dazu – in der Regel binnen einer Frist von zwei Wochen – Stellung zu nehmen (Parteiengehör).

Ergeben sich daraus keine neuen Tatsachen, so erlässt die Aufsichtsstelle nach Ablauf der Stellungnahmefrist einen Bescheid, mit dem entweder der Antrag des VDA abgewiesen oder der Qualifikationsstatus für den VDA und/oder die von ihm erbrachten Vertrauensdienste verliehen wird. In diesem Bescheid kann die Aufsichtsstelle auch Auflagen erteilen, um die Erfüllung der rechtlichen Anforderungen zu gewährleisten. Für die Überprüfung durch die Aufsichtsstelle schreibt diese dem VDA die in § 1 Abs. 1 Z 1, 3 und 4 SVV festgelegten Gebühren vor.

Faktisch können die meisten PKI-basierten qualifizierten Vertrauensdienste erst nach ihrer Eintragung in die nationale Vertrauensliste erbracht werden, weil dies für die Validierung technisch erforderlich ist. Die Eintragung des qualifizierten VDA und/oder der von ihm erbrachten qualifizierten Vertrauensdienste in die österreichischen Vertrauensliste erfolgt erst dann, wenn der Bescheid zur Verleihung des Qualifikationsstatus Rechtskraft erlangt, in der Regel nach Ablauf der Beschwerdefrist von vier Wochen ab Zustellung des Bescheides. Wenn der VDA nach Zustellung des Bescheides ausdrücklich auf Rechtsmittel verzichtet, kann die Eintragung in die Vertrauensliste unverzüglich erfolgen.

Die Aufsichtsstelle orientiert sich bei ihren Tätigkeiten generell an den von der Europäischen Kommission gemäß Art. 46b Abs. 7 eIDAS-VO angenommenen Leitlinien über die Wahrnehmung von Aufgaben der Aufsichtsstellen für Vertrauensdienste.

3 Änderungen qualifizierter Vertrauensdienste

3.1 Anzeige von Änderungen

Qualifizierte VDA haben Änderungen der von ihnen erbrachten qualifizierten Vertrauensdienste gemäß Art. 24 Abs. 2 lit. a eIDAS-VO idgF der Aufsichtsstelle im Voraus anzuzeigen. Für die Mitteilung ist das Einbringungsportal (siehe Punkt 1.2) zu verwenden.

Änderungen qualifizierter Vertrauensdienste sind gemäß Art. 1 DVO (EU) 2025/2530 zumindest dann anzuzeigen, wenn sich Modifikationen bei einem oder mehreren der folgenden Elemente ergeben:

- Dienstbeschreibungen, Regelungen, Praxiserklärungen oder damit verbundenen Nutzungsbedingungen (insbesondere Änderungen von Unterlagen, die gemäß Punkt 2.1 der Aufsichtsstelle vorzulegen sind)[4];
- technische Architektur der qualifizierten Vertrauensdienste oder vertrauenswürdige Systeme oder Produkte gemäß Art. 24 Abs. 2 lit. e und f eIDAS-VO idgF[5];

[4] Dokumente, die lediglich sprachlich berichtigt oder ohne inhaltliche Änderung mit einer neuen Versionsnummer versehen wurden, brauchen nicht als Änderung im Sinne von Art. 24 Abs. 2 lit. a eIDAS-VO angezeigt zu werden, sind aber dennoch der Aufsichtsstelle spätestens im Zeitpunkt ihres Wirksamwerdens zu übermitteln. Geänderte Risikoanalysen brauchen nur dann vorgelegt zu werden, wenn sich daraus Änderungen von Risikomanagementmaßnahmen ergeben.

[5] Die regelmäßige Wartung von Hardware und Software, insbesondere das Einspielen von Sicherheits-Updates, sind davon nicht umfasst, sofern dabei keine zertifizierungspflichtigen Komponenten geändert werden. Sollte

- Bereitstellung technischer Komponenten, die für die Erbringung der qualifizierten Vertrauensdienste erforderlich sind, oder die zu diesen technischen Komponenten gehörigen technischen Dienste;
- Verwendung kryptographischer Techniken oder kryptographischen Materials bei der Erbringung der qualifizierten Vertrauensdienste;
- Registrierungs- und Identifizierungsverfahren;
- Organisationsstruktur oder Leitung des Vertrauensdiensteanbieters;
- Beendigungsplan;
- in Art. 24 Abs. 2 lit. c eIDAS-VO idgF genannte Finanzmittel und Haftpflichtversicherungen;
- Elemente, die sich auf den Inhalt der betreffenden nationalen Vertrauensliste auswirken;
- an der Erbringung der qualifizierten Vertrauensdienste beteiligte Dritte, einschließlich Unterauftragnehmer oder Dienstleister, oder Änderungen an den Vertragsbedingungen mit diesen Dritten.

Die Anzeige hat zumindest Folgendes zu enthalten:

- eine Beschreibung der Änderung,
- eine Angabe, in welchem Zeitpunkt die Änderung wirksam werden soll (Datum und Uhrzeit – frühestens einen Monat nach Einbringung der Anzeige; im Fall der beabsichtigten Einstellung der Tätigkeit des qualifizierten VDA frühestens drei Monate nach Einbringung der Anzeige),
- eine Begründung der Änderung und gegebenenfalls Nachweise für die Gründe,
- gegebenenfalls aktualisierte Dokumente (vorzulegende Unterlagen gemäß Punkt 2.1, soweit diese von der Änderung betroffen sind)[6];
- sofern anwendbar, die Bestätigung einer Konformitätsbewertungsstelle und technische Berichte zur Untermauerung der Bestätigung für eine Identifizierungsmethode oder eine Methode zur Überprüfung von Attributen.

Im Fall von Änderungen, die die bei der Ausstellung qualifizierter Zertifikate eingesetzten Identifizierungsmethoden oder die bei der Ausstellung qualifizierter elektronischer Attributsbescheinigungen eingesetzten Methoden zur Überprüfung von Attributen betreffen, sind besondere Nachweise erforderlich. Die Identifizierung von Personen und die Überprüfung von Attributen werden zwar oft ausgelagert, sind aber trotzdem Teil eines qualifizierten Vertrauensdienstes und unterliegen somit der Konformitätsbewertung und der Aufsicht. Wenn eine zusätzliche Identifizierungs- oder Überprüfungsmethode unterstützt oder geändert wird, hat der VDA der Aufsichtsstelle zumindest eine detaillierte Beschreibung dieser Methode sowie ihrer Einbindung in den qualifizierten Vertrauensdienst vorzulegen. Sofern Risiken im Zusammenhang mit der Identifizierung (z. B. in Bezug auf Identitätsdiebstahl) oder der Überprüfung von Attributen in der Risikoanalyse, die den in Art. 24 Abs. 2 lit. fa eIDAS-

eine kritische Schwachstelle in einer zertifizierungspflichtigen Komponente eintreten, so ist von der Möglichkeit auszugehen, dass diese Komponente den Anforderungen der eIDAS-VO, zumindest temporär, nicht mehr entspricht. In diesem Fall ist keine Änderungsanzeige, sondern eine Mitteilung gemäß Punkt 5.1 einzubringen.

[6] Ein aktualisierter Konformitätsbewertungsbericht ist nicht von vornherein erforderlich, kann aber im Zuge der Überprüfung gemäß Punkt 3.2 nach den dort festgelegten Grundsätzen von der Aufsichtsstelle angefordert werden.

VO idgF genannten Maßnahmen zugrunde liegt, nicht oder unzureichend berücksichtigt werden, kann die Vorlage einer gesonderten Risikoanalyse erforderlich sein.

Sofern es sich um eine Identifizierungsmethode gemäß Art. 24 Abs. 1a lit. c eIDAS-VO oder die eine Methode zur Überprüfung von Attributen gemäß Art. 24 Abs. 1b lit. d eIDAS-VO handelt, sind auch die entsprechende Bestätigung einer Konformitätsbewertungsstelle und technische Berichte zur Untermauerung der Bestätigung (z. B. Prüfberichte oder Evaluation Reports) vorzulegen. Aus der Bestätigung der Konformitätsbewertungsstelle muss hervorgehen, dass die Methode die Identifizierung oder die Überprüfung von Attributen mit einem hohen Vertrauensniveau gewährleitstet. Bei nachweislicher Erfüllung der Anforderungen für „extended LoIP“ gemäß ETSI TS 119 461 V2.1.1 (2025-02) kann davon ausgegangen werden, dass ein hohes Vertrauensniveau gewährleistet ist.

Weitere Pflichten zur Anzeige von Änderungen ergeben sich in der Regel aus bescheidmäßig erteilten Auflagen.

3.2 Methode zur Überprüfung des VDA

Die Überprüfung durch die Aufsichtsstelle erfolgt in einem nach dem AVG geführten Verwaltungsverfahren. Nach Einlangen einer Anzeige gemäß Punkt 3.1 wird diese in der Regel binnen drei Wochen von der Telekom-Control-Kommission behandelt. Die Telekom-Control-Kommission kann die RTR-GmbH als Geschäftsstelle beiziehen und diese mit einzelnen Tätigkeiten im Rahmen der Überprüfung des VDA beauftragen. Die Aufsichtsstelle überprüft, ob

- alle Informationen und Unterlagen gemäß Punkt 3.1 vollständig vorliegen,
- ob die vorgelegten Informationen und Unterlagen hinreichend nachweisen, dass die vom VDA angezeigten Änderungen den in eIDAS-VO idgF (einschließlich der hierauf beruhenden Durchführungsrechtsakte, siehe Abschnitt 8.4), Art. 21 NIS-2-RL, DVO (EU) 2024/2690, SVG und SVV festgelegten Erfordernissen entsprechen, und
- ob für einen hinreichenden Nachweis eine Konformitätsbewertung oder allenfalls weitere Unterlagen erforderlich sind.

Weist die Anzeige Mängel auf, so kann die Aufsichtsstelle dem VDA die Behebung des Mangels innerhalb einer angemessenen Frist mit der Wirkung auftragen, dass das Anbringen nach fruchtlosem Ablauf dieser Frist zurückgewiesen wird.

Von einer Konformitätsbewertung kann abgesehen werden, wenn die Aufsichtsstelle den Sachverhalt ohne Mitwirkung einer Konformitätsbewertungsstelle feststellen und beurteilen kann.

Vor der direkten Beauftragung einer Konformitätsbewertungsstelle durch die Aufsichtsstelle kann dem qualifizierten VDA die Möglichkeit eingeräumt werden, sich von sich aus einer Konformitätsbewertung zu unterziehen und den Konformitätsbewertungsbericht innerhalb einer von der Aufsichtsstelle vorgegebenen angemessenen Frist der Aufsichtsstelle vorzulegen.

Kann die Aufsichtsstelle die Überprüfung der angezeigten Änderung nicht bis zu dem in der Anzeige genannten Wirksamkeitsdatum abschließen, so kann sie den VDA auffordern, die Änderung bis zur Entscheidung der Aufsichtsstelle auszusetzen. In diesem Fall wird über allfällige Aufsichtsmaßnahmen ohne unnötigen Aufschub, spätestens aber sechs Monate nach Einlangen der Anzeige entschieden.

Bei der Überprüfung, ob der Vertrauensdiensteanbieter die Anforderungen gemäß Art. 21 NIS-2-RL erfüllt, arbeitet die Aufsichtsstelle gemäß Art. 20 NISG 2026 mit der Cybersicherheitsbehörde zusammen und tauscht Informationen mit dieser aus. Hierbei wird die Kommunikation jedenfalls durch Mechanismen geschützt, die der Sensibilität der übermittelten Informationen angemessen sind.

Im Zuge der Überprüfung kann die Aufsichtsstelle den VDA auffordern, weitere Informationen und/oder Unterlagen innerhalb einer angemessenen Frist vorzulegen. Die Aufsichtsstelle kann auch eine mündliche Verhandlung anberaumen und diese bei Bedarf mit einem Augenschein verbinden. Der VDA hat den im Auftrag der Aufsichtsstelle handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der Geschäftszeiten zu gestatten, die in Betracht kommenden Bücher und sonstigen Aufzeichnungen oder Unterlagen einschließlich der einschlägigen Informationen nach Art. 24 Abs. 2 lit. h eIDAS-VO idgF vorzulegen oder zur Einsicht bereitzuhalten, Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren.

Im Übrigen folgt das Ermittlungsverfahren den Bestimmungen des AVG.

Falls keine Aufsichtsmaßnahmen ergriffen werden, schreibt die Aufsichtsstelle dem VDA die in § 1 Abs. 1 Z 2 SVV festgelegte Gebühr vor und stellt das Verfahren ein. Die Höhe der Gebühr hängt davon ab, ob der Überprüfung sicherheitsrelevante Anlässe zugrunde liegen. Sicherheitsrelevante Anlässe liegen jedenfalls vor, wenn sich die angezeigte Änderung auf qualifizierte elektronische Signaturerstellungseinheiten, qualifizierte elektronische Siegelerstellungseinheiten oder vertrauenswürdige Systeme im Sinne von Art. 24 Abs. 2 lit. e und f eIDAS-VO idgF bezieht. Sicherheitsrelevante Anlässe können auch in anderen Fällen vorliegen. Die Entscheidung, ob sicherheitsrelevante Anlässe vorliegen, ist fallbezogen und kann nicht im Voraus anhand eines Kriterienkatalogs getroffen werden.

Vor allfälligen Aufsichtsmaßnahmen wird dem VDA Gelegenheit gegeben, vom Ergebnis der Beweisaufnahme Kenntnis und dazu – in der Regel binnen einer Frist von zwei Wochen, bei Gefahr in Verzug auch kürzer – Stellung zu nehmen (Parteiengehör).

Ergeben sich daraus keine neuen Tatsachen, so erlässt die Aufsichtsstelle nach Ablauf der Stellungnahmefrist einen Bescheid, mit dem Aufsichtsmaßnahmen gemäß Art. 46b Abs. 4 lit. j eIDAS-VO ergriffen werden. Solche Maßnahmen können beispielsweise die Erteilung von Auflagen und/oder die Setzung einer Frist zur Behebung von Mängeln umfassen oder auch die Untersagung der angezeigten Änderung umfassen. Für die Überprüfung und die Erteilung von Auflagen durch die Aufsichtsstelle schreibt diese dem VDA die in § 1 Abs. 1 Z 2 und 4 SVV festgelegten Gebühren vor.

Die Eintragung des qualifizierten VDA und/oder der von ihm erbrachten qualifizierten Vertrauensdienste in die österreichischen Vertrauensliste erfolgt erst dann, wenn der Bescheid zur Verleihung des Qualifikationsstatus Rechtskraft erlangt, in der Regel nach Ablauf der Beschwerdefrist von vier Wochen ab Zustellung des Bescheides. Wenn der VDA nach Zustellung des Bescheides ausdrücklich auf Rechtsmittel verzichtet, kann die Eintragung in die Vertrauensliste unverzüglich erfolgen.

Die Aufsichtsstelle orientiert sich bei ihren Tätigkeiten generell an den von der Europäischen Kommission gemäß Art. 46b Abs. 7 eIDAS-VO angenommenen Leitlinien über die Wahrnehmung von Aufgaben der Aufsichtsstellen für Vertrauensdienste.

4 Regelmäßige Konformitätsbewertung

4.1 Vorlage von Konformitätsbewertungsberichten

Ein Vertrauensdienst, dem bereits der Qualifikationsstatus verliehen wurde, ist gemäß Art. 20 Abs. 1 eIDAS-VO idgF spätestens 24 Monate nach Ausstellung des letzten Konformitätsbewertungsberichts einer neuerlichen Konformitätsbewertung durch eine akkreditierte Konformitätsbewertungsstelle zu unterziehen. Für die Durchführung der Konformitätsbewertung hat der VDA selbst Sorge zu tragen. Der VDA hat der Aufsichtsstelle den Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach dessen Eingang, jedenfalls aber vor Ablauf des für die betroffenen qualifizierten Vertrauensdienste zuletzt ausgestellten Konformitätszertifikats im Sinne von Art. 1 Z 3 DVO (EU) 2025/2162 vorzulegen. Für die Mitteilung ist das Einbringungsportal (siehe Punkt 1.2) zu verwenden. Dem Konformitätsbewertungsbericht sind die zugehörigen technischen Berichte zur Untermauerung des Konformitätsbewertungsberichts beizulegen.

Änderungen, die an qualifizierten Vertrauensdiensten im Zuge einer Konformitätsbewertung vorgenommen werden, sind der Aufsichtsstelle gemäß Punkt 3.1 anzuzeigen.

Falls aufgrund bevorstehender Änderungen an bestehenden qualifizierten Vertrauensdiensten vorzeitig eine neuerliche Konformitätsbewertung durchgeführt wird, ist der Konformitätsbewertungsbericht innerhalb von drei Arbeitstagen nach dessen Eingang der Aufsichtsstelle vorzulegen.

Berichte über Überwachungsaudits gemäß Art. 6 Abs. 5 lit. d und Art. 6 Abs. 11 DVO (EU) 2025/2162 sind ebenfalls innerhalb von drei Arbeitstagen nach deren Eingang der Aufsichtsstelle vorzulegen.

4.2 Methode zur Überprüfung des VDA

Die Analyse von Konformitätsbewertungsberichten entspricht weitestgehend der Beschreibung unter Punkt 2.2. Auch in diesem Fall handelt es sich um ein nach dem AVG geführtes Verwaltungsverfahren. Unterschiede zu Punkt 2.2 bestehen insofern, als die Aufsichtsstelle

- das Verwaltungsverfahren zwar ebenfalls ohne unnötigen Aufschub zu Ende führt, dabei aber nicht an die für neue qualifizierte Vertrauensdienste gemäß Art. 21 Abs. 2 eIDAS-VO idgF maßgebliche Frist von drei Monaten gebunden ist und
- im Fall, dass keine Aufsichtsmaßnahmen ergriffen werden, lediglich die Gebühr gemäß § 1 Abs. 1 Z 1 SVV mit Bescheid vorschreibt und das Verfahren einstellt.

Vor allfälligen Aufsichtsmaßnahmen wird dem VDA Gelegenheit gegeben, vom Ergebnis der Beweisaufnahme Kenntnis und dazu – in der Regel binnen einer Frist von zwei Wochen, bei Gefahr in Verzug auch kürzer – Stellung zu nehmen (Parteiengehör).

Ergeben sich daraus keine neuen Tatsachen, so erlässt die Aufsichtsstelle nach Ablauf der Stellungnahmefrist einen Bescheid, mit dem Aufsichtsmaßnahmen gemäß Art. 46b Abs. 4 lit. j eIDAS-VO ergriffen werden. Solche Maßnahmen können beispielsweise die Erteilung von Auflagen und/oder die Setzung einer Frist zur Behebung von Mängeln umfassen. Für die Analyse des Konformitätsbewertungsberichts und die Erteilung von Auflagen durch die Aufsichtsstelle schreibt diese dem VDA die in § 1 Abs. 1 Z 1 und 4 SVV festgelegten Gebühren vor.

Falls der VDA die erteilten Auflagen nicht erfüllt, entzieht die Aufsichtsstelle, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst gemäß Art. 20 Abs. 3 eIDAS-VO idgF den Qualifikationsstatus mit Bescheid.

Mit der Entscheidung der Aufsichtsstelle zusammenhängende Änderungen der österreichischen Vertrauensliste werden in der Regel erst dann vorgenommen, wenn der Bescheid zur Verleihung oder zum Entzug des Qualifikationsstatus Rechtskraft erlangt, und zwar nach Ablauf der Beschwerdefrist von vier Wochen ab Zustellung des Bescheides oder nach ausdrücklichem Verzicht auf Rechtsmittel durch den VDA. Wenn die Aufsichtsstelle Gefahr in Verzug feststellt, können die Änderungen an der Vertrauensliste unverzüglich vorgenommen werden.

5 Sicherheitsverletzungen, Sicherheitsverstöße oder Störungen

5.1 Mitteilung eines Vorfalls

VDA haben Sicherheitsverletzungen, Sicherheitsverstöße oder Störungen bei der Erbringung eines Vertrauensdienstes oder bei der Durchführung von Maßnahmen in Bezug auf

- Registrierungs- und Einbindungsverfahren für einen Vertrauensdienst,
- Verfahrens- oder Verwaltungskontrollen, die für die Erbringung von Vertrauensdiensten erforderlich sind, oder
- die Verwaltung und Durchführung von Vertrauensdiensten

unverzüglich, spätestens jedoch 24 Stunden, nachdem sie davon Kenntnis erlangt haben, der Aufsichtsstelle (sowie den identifizierbaren betroffenen Personen, der Öffentlichkeit, wenn es von öffentlichem Interesse ist, und gegebenenfalls anderen einschlägigen zuständigen Stellen) mitzuteilen, sofern die Sicherheitsverletzungen, Sicherheitsverstöße oder Störungen erhebliche Auswirkungen auf den erbrachten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten haben. Diese Pflicht besteht gemäß Art. 19a Abs. 1 lit. b und Art. 24 Abs. 2 lit. fb eIDAS-VO, unabhängig von der in § 34 NISG 2026 normierten Pflicht zur Meldung erheblicher Cybersicherheitsvorfälle.

Von erheblichen Auswirkungen ist jedenfalls auszugehen, wenn der Vorfall bei sinngemäßer Anwendung der Kriterien für Cybersicherheitsvorfälle gemäß Art. 3, 4 und 14 DVO (EU) 2024/2690 als erheblich einzustufen ist (unabhängig davon, ob es sich bei dem Vorfall auch um einen Cybersicherheitsvorfall handelt).

Für die Mitteilung ist das Einbringungsportal (siehe Punkt 1.2) zu verwenden. Die Mitteilung hat folgende Informationen zu enthalten:

- Name des VDA,
- Kontaktdaten (zumindest vollständiger Name, E-Mail-Adresse und Rufnummer) zweier mit dem Vorfall befassten Personen, die der Aufsichtsstelle für Auskünfte im Zusammenhang mit dem Vorfall zur Verfügung stehen,
- Zeitpunkt, in dem der VDA von dem Vorfall Kenntnis erlangt hat,
- gegebenenfalls Zeitpunkt, in dem der Vorfall aufgetreten ist bzw. begonnen hat,
- gegebenenfalls Zeitpunkt der Behebung des Vorfalls,
- möglichst detaillierte Beschreibung des Vorfalls und seiner (vermuteten oder tatsächlichen) Ursachen
- gegebenenfalls Beschreibung der zur Behebung des Vorfalls ergriffenen Maßnahmen,
- gegebenenfalls Maßnahmen, um ähnliche Vorfälle künftig zu verhindern.

Bei derartigen Störungen kommt es vor allem darauf an, die Aufsichtsstelle möglichst rasch zu informieren, auch wenn im Zeitpunkt der Meldung noch nicht alle Informationen vorliegen. Die Mitteilung an die Aufsichtsstelle braucht daher die mit „gegebenenfalls“ markierten Informationen nur dann zu enthalten, wenn diese dem VDA im Zeitpunkt der Mitteilung bekannt sind. Fehlende Informationen sind jedoch im Zuge der Überprüfung durch die Aufsichtsstelle nachzureichen.

Die Mitteilung eines Vorfalls an die Aufsichtsstelle ersetzt keine anderen gesetzlich erforderlichen Meldungen, insbesondere nicht jene gemäß § 34 NISG 2026 oder Art. 33 DSGVO.

5.2 Methode zur Überprüfung des VDA

Die Aufsichtsstellen unterrichtet in Fällen, in denen von einer Sicherheitsverletzung oder einem Integritätsverlust weitere Mitgliedstaaten betroffen sind, deren einheitliche Anlaufstellen für Vertrauensdienste, europäische Brieftaschen für die

digitale Identität und notifizierte elektronische Identifizierungssysteme (Art. 46c eIDAS-VO).

Sofern es sich beim mitgeteilten Vorfall um einen erheblichen Cybersicherheitsvorfall handelt, unterrichtet die Aufsichtsstelle die Cybersicherheitsbehörde und in Fällen, in denen weitere Mitgliedstaaten betroffen sind, deren zentrale Anlaufstellen für Cybersicherheit (Art. 8 Abs. 3 NIS-2-RL).

Wenn die Aufsichtsstelle feststellt, dass die Offenlegung einer Sicherheitsverletzung oder eines Integritätsverlusts im öffentlichen Interesse ist, informiert sie entweder selbst die Öffentlichkeit oder trägt dem VDA auf, dies zu tun.

Im Übrigen entspricht die Überprüfung des VDA der unter Punkt 6 beschriebenen Methode.

6 Methode zur Überprüfung des VDA von Amts wegen

Die Aufsichtsstelle kann gemäß Art. 20 Abs. 2 eIDAS-VO idgF jederzeit eine Überprüfung vornehmen oder eine Konformitätsbewertungsstelle um eine Konformitätsbewertung des qualifizierten VDA – auf dessen Kosten – ersuchen, um nachzuweisen, dass dieser und die von ihm erbrachten qualifizierten Vertrauensdienste die in dieser Verordnung festgelegten Anforderungen erfüllen. Solche Überprüfungen werden jedenfalls dann durchgeführt, wenn

- die Cybersicherheitsbehörde die Aufsichtsstelle von Verstößen des qualifizierten VDA gegen Art. 21 NIS-2-RL in Kenntnis setzt,
- die Datenschutzbehörde die Aufsichtsstelle von Verstößen des qualifizierten VDA gegen die DSGVO in Kenntnis setzt oder
- die Aufsichtsstelle von möglichen Verstößen des qualifizierten VDA gegen die eIDAS-VO oder von einer Sicherheitsverletzung, einem Sicherheitsverstoß oder einer Störung (Art. 19a Abs. 1 lit. b und Art. 24 Abs. 2 lit. fb eIDAS-VO) Kenntnis erlangt.

Von einer Konformitätsbewertung kann abgesehen werden, wenn die Aufsichtsstelle den Sachverhalt ohne Mitwirkung einer Konformitätsbewertungsstelle feststellen und beurteilen kann.

Vor der direkten Beauftragung einer Konformitätsbewertungsstelle durch die Aufsichtsstelle kann dem qualifizierten VDA die Möglichkeit eingeräumt werden, sich von sich aus einer Konformitätsbewertung zu unterziehen und den Konformitätsbewertungsbericht innerhalb einer von der Aufsichtsstelle vorgegebenen angemessenen Frist der Aufsichtsstelle vorzulegen.

Die Aufsichtsstelle kann das Verwaltungsverfahren jederzeit einstellen, wenn die Gründe für die von Amts wegen durchgeführt Überprüfung wegfallen.

Um während des Verwaltungsverfahrens fortwährende Verstöße gegen die oben genannten Vorschriften hintanzuhalten, kann die Aufsichtsstelle ohne

vorangegangenes Ermittlungsverfahren vorläufige Maßnahmen mit Mandatsbescheid anordnen.

Vor allfälligen Aufsichtsmaßnahmen wird dem VDA Gelegenheit gegeben, vom Ergebnis der Beweisaufnahme Kenntnis und dazu – in der Regel binnen einer Frist von zwei Wochen, bei Gefahr in Verzug auch kürzer – Stellung zu nehmen (Parteiengehör).

Ergeben sich daraus keine neuen Tatsachen, so erlässt die Aufsichtsstelle nach Ablauf der Stellungnahmefrist einen Bescheid, mit dem Aufsichtsmaßnahmen gemäß Art. 46b Abs. 4 lit. j eIDAS-VO ergriffen werden oder dem betreffenden Anbieter oder dem von ihm erbrachten betroffenen Dienst, soweit dies insbesondere durch die Tragweite, die Dauer und die Auswirkungen dieses Verstoßes gerechtfertigt ist, gemäß Art. 20 Abs. 3, 3a oder 3b eIDAS-VO idgF der Qualifikationsstatus entzogen wird. Der Entzug des Qualifikationsstatus kann auch erfolgen, wenn der VDA zuvor angeordnete Aufsichtsmaßnahmen nicht befolgt, Auflagen ignoriert oder Fristen verstreichen lässt.

Mit der Entscheidung der Aufsichtsstelle zusammenhängende Änderungen der österreichischen Vertrauensliste werden in der Regel erst dann vorgenommen, wenn der Bescheid zum Entzug des Qualifikationsstatus Rechtskraft erlangt, und zwar nach Ablauf der Beschwerdefrist von vier Wochen ab Zustellung des Bescheides oder nach ausdrücklichem Verzicht auf Rechtsmittel durch den VDA. Wenn die Aufsichtsstelle Gefahr in Verzug feststellt, können die Änderungen an der Vertrauensliste unverzüglich vorgenommen werden.

7 Verfahren für die Bearbeitung von Beschwerden im Zusammenhang mit dem Prozess der Überprüfung des VDA

Ein VDA kann seine Anliegen grundsätzlich jederzeit gegenüber der RTR-GmbH vorbringen. Die RTR-GmbH wird sich mit derartigen Anliegen befassen, sofern dem keine rechtlichen oder sonstigen Hindernisse entgegenstehen.

Im Zusammenhang mit dem Prozess der Überprüfung eines VDA sind Beschwerden im Sinne von Rechtsmitteln an das Bundesverwaltungsgericht (BVwG) zu richten. Ausführliche Informationen über das Verfahren vor dem BVwG finden Sie auf dessen Website.

8 Rechtsvorschriften

8.1 Gesetzgeberische Rechtsakte der Europäischen Union

- Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG in der geltenden Fassung

- Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)
- Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates
- Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen

8.2 Durchführungsrechtsakte der Europäischen Union zur europäischen Brieftasche für die digitale Identität

- Durchführungsverordnung (EU) 2024/2977 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf an europäische Brieftaschen für die digitale Identität ausgestellte Personenidentifizierungsdaten und elektronische Attributsbescheinigungen
- Durchführungsverordnung (EU) 2024/2979 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Integrität und die Kernfunktionen europäischer Brieftaschen für die digitale Identität
- Durchführungsverordnung (EU) 2024/2980 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Notifizierungen an die Kommission bezüglich des Ökosystems europäischer Brieftaschen für die digitale Identität
- Durchführungsverordnung (EU) 2024/2981 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Zertifizierung der europäischen Brieftaschen für die digitale Identität
- Durchführungsverordnung (EU) 2024/2982 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf vom europäischen Rahmen für die digitale Identität zu unterstützende Protokolle und Schnittstellen
- Durchführungsverordnung (EU) 2025/846 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014

des Europäischen Parlaments und des Rates in Bezug auf den grenzüberschreitenden Identitätsabgleich natürlicher Personen

- Durchführungsverordnung (EU) 2025/847 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Reaktion auf Sicherheitsverletzungen europäischer Brieftaschen für die digitale Identität
- Durchführungsverordnung (EU) 2025/848 der Kommission vom 6. Mai 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Registrierung von auf Brieftaschen vertrauenden Beteiligten
- Durchführungsverordnung (EU) 2025/849 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Übermittlung von Informationen an die Kommission und die Kooperationsgruppe für die Liste der zertifizierten europäischen Brieftaschen für die digitale Identität
- Durchführungsverordnung (EU) 2026/798 der Kommission vom 7. April 2026 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für die Ferneinbindung von Nutzern in die europäischen Brieftaschen für die digitale Identität mit elektronischen Identifizierungsmitteln des Sicherheitsniveaus substanziell in Verbindung mit zusätzlichen Ferneinbindungsverfahren, sofern sie zusammen den Anforderungen des Sicherheitsniveaus hoch entsprechen
- Durchführungsverordnung (EU) 2026/1730 der Kommission vom 15. Juli 2026 zur Änderung der Durchführungsverordnung (EU) 2025/848 in Bezug auf geltende Standards bzw. Normen und Spezifikationen
- Durchführungsverordnung (EU) 2026/1731 der Kommission vom 15. Juli 2026 zur Änderung der Durchführungsverordnungen (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 und (EU) 2024/2982 in Bezug auf geltende Standards bzw. Normen und Spezifikationen

8.3 Durchführungsrechtsakte der Europäischen Union zur elektronischen Identifizierung

- Durchführungsverordnung (EU) 2015/1501 der Kommission vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
- Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
- Durchführungsbeschluss (EU) 2015/1984 der Kommission vom 3. November 2015 zur Festlegung der Umstände, Formate und Verfahren der Notifizierung gemäß Artikel 9 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments

und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

- Durchführungsverordnung (EU) 2025/1568 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Verfahrensmodalitäten für gegenseitige Begutachtungen elektronischer Identifizierungssysteme und für die Zusammenarbeit bei der Organisation solcher Begutachtungen innerhalb der Kooperationsgruppe und zur Aufhebung des Durchführungsbeschlusses (EU) 2015/296 der Kommission

8.4 Durchführungsrechtsakte der Europäischen Union zu Vertrauensdiensten

- Durchführungsverordnung (EU) 2015/806 der Kommission vom 22. Mai 2015 zur Festlegung von Spezifikationen für die Form des EU-Vertrauenssiegels für qualifizierte Vertrauensdienste
- Durchführungsbeschluss (EU) 2015/1505 der Kommission vom 8. September 2015 über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
- Durchführungsbeschluss (EU) 2015/1506 der Kommission vom 8. September 2015 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt anerkannt werden
- Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
- Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC)
- Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter

von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt

- Durchführungsverordnung (EU) 2025/1566 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für die Überprüfung der Identität und der Attribute der Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt werden soll
- Durchführungsverordnung (EU) 2025/1567 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Verwaltung von qualifizierten elektronischen Fernsignaturerstellungseinheiten und qualifizierten elektronischen Fernsiegelerstellungseinheiten
- Durchführungsverordnung (EU) 2025/1569 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf qualifizierte elektronische Attributsbescheinigungen und von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen bereitgestellte elektronische Attributsbescheinigungen
- Durchführungsverordnung (EU) 2025/1570 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Notifizierung von Informationen über zertifizierte qualifizierte elektronische Signaturerstellungseinheiten und zertifizierte qualifizierte elektronische Siegelerstellungseinheiten
- Durchführungsverordnung (EU) 2025/1571 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Formate und Verfahren für die jährlichen Berichte der Aufsichtsstellen
- Durchführungsverordnung (EU) 2025/1572 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf das Format und die Verfahren für die Absichtsmitteilung und die Überprüfung im Hinblick auf den Beginn der Erbringung qualifizierter Vertrauensdienste
- Durchführungsverordnung (EU) 2025/1929 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Verknüpfung von Datums- und Zeitangaben mit Daten und zur Bestimmung der Richtigkeit der Zeitquellen für die Bereitstellung qualifizierter elektronischer Zeitstempel
- Durchführungsverordnung (EU) 2025/1942 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf qualifizierte Validierungsdienste für qualifizierte elektronische Signaturen und qualifizierte Validierungsdienste für qualifizierte elektronische Siegel
- Durchführungsverordnung (EU) 2025/1943 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf

Referenzstandards für qualifizierte Zertifikate für elektronische Signaturen und qualifizierte Zertifikate für elektronische Siegel

- Durchführungsverordnung (EU) 2025/1944 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards für Prozesse des Absendens und Empfangens von Daten in qualifizierten Diensten für die Zustellung elektronischer Einschreiben und in Bezug auf die Interoperabilität dieser Dienste
- Durchführungsverordnung (EU) 2025/1945 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Validierung qualifizierter elektronischer Signaturen und qualifizierter elektronischer Siegel sowie die Validierung fortgeschrittener elektronischer Signaturen, die auf qualifizierten Zertifikaten beruhen, und fortgeschrittener elektronischer Siegel, die auf qualifizierten Zertifikaten beruhen
- Durchführungsverordnung (EU) 2025/1946 der Kommission vom 29. September 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf qualifizierte Bewahrungsdienste für qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel
- Durchführungsverordnung (EU) 2025/2160 der Kommission vom 27. Oktober 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards, Spezifikationen und Verfahren für das Management der Risiken bei der Erbringung nichtqualifizierter Vertrauensdienste
- Durchführungsverordnung (EU) 2025/2162 der Kommission vom 27. Oktober 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Akkreditierung von Konformitätsbewertungsstellen, die qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste bewerten, den Konformitätsbewertungsbericht und das Konformitätsbewertungssystem
- Durchführungsbeschluss (EU) 2025/2164 der Kommission vom 27. Oktober 2025 zur Änderung des Durchführungsbeschlusses (EU) 2015/1505 in Bezug auf die Version der Norm, auf der die gemeinsame Vorlage für die Vertrauenslisten beruht
- Durchführungsverordnung (EU) 2025/2527 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für qualifizierte Zertifikate für die Website-Authentifizierung
- Durchführungsverordnung (EU) 2025/2530 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Anforderungen an qualifizierte Vertrauensdiensteanbieter, die qualifizierte Vertrauensdienste erbringen
- Durchführungsverordnung (EU) 2025/2531 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr.

910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für qualifizierte elektronische Journale

- Durchführungsverordnung (EU) 2025/2532 der Kommission vom 16. Dezember 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Referenzstandards und Spezifikationen für qualifizierte elektronische Archivierungsdienste
- Durchführungsverordnung (EU) 2026/248 der Kommission vom 2. Februar 2026 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die von öffentlichen Stellen anzuerkennenden Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener elektronischer Siegel und zur Aufhebung des Durchführungsbeschlusses (EU) 2015/1506 der Kommission
- Durchführungsverordnung (EU) 2026/1735 der Kommission vom 15. Juli 2026 zur Änderung der Durchführungsverordnung (EU) 2025/1569 in Bezug auf geltende Standards bzw. Normen und Spezifikationen

8.5 Nationale Durchführungsvorschriften

- Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG)
- Bundesgesetz, mit dem das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2026 – NISG 2026) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden
- Bundesgesetz zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz – RKEG)
- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)
- Bundesgesetz über Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (Barrierefreiheitsgesetz – BaFG)
- Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV)
- Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ als Bestätigungsstelle
- Verordnung des Bundesministers für Inneres zur Durchführung des Resilienz kritischer Einrichtungen-Gesetzes (Resilienz kritischer Einrichtungen-Verordnung – RKEV)

8.6 Verwaltungsrechtliche Vorschriften

- Allgemeines Verwaltungsverfahrensgesetz 1991 – AVG
- Verwaltungsstrafgesetz 1991 – VStG
- Bundesgesetz über das Verfahren der Verwaltungsgerichte (Verwaltungsgerichts-verfahrensgesetz – VwGVG)

- Verordnung des Bundesministers für Finanzen betreffend die Gebühr für Eingaben bei den Verwaltungsgerichten (VwG-Eingabengebührverordnung – VwG-EGebV)

9 Technische Standards und bewährte Verfahren

9.1 Referenzstandards und normative Referenzen

- ETSI EN 301 549 V3.2.1 (2021-03), Accessibility requirements suitable for public procurement of ICT products and services in Europe
- ETSI TS 119 101 V1.1.1 (2016-03), ESI; Policy and security requirements for applications for signature creation and signature validation
- ETSI EN 319 102-1 V1.4.1 (2024-06), ESI; Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI TS 119 102-2 V1.4.1 (2023-06), ESI; Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report
- ETSI EN 319 122-1 V1.3.1 (2023-06), ESI; CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures
- ETSI EN 319 132-1 V1.3.1 (2024-07), ESI; XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
- ETSI EN 319 142-1 V1.2.1 (2024-01), ESI; PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
- ETSI TS 119 172-4 V1.1.1 (2021-05), ESI; Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
- ETSI TS 119 182-1 V1.2.1 (2024-07), ESI; JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
- ETSI EN 319 401 V3.1.1 (2024-06), ESI; General Policy Requirements for Trust Service Providers
- ETSI EN 319 401 V3.2.1 (2026-01), ESI; General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.5.1 (2025-04), ESI; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.6.1 (2025-06), ESI; Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for TSP issuing EU qualified certificates
- ETSI TS 119 411-5 V2.1.1 (2025-02), ESI; Policy and security requirements for Trust Service Providers issuing certificates; Part 5: QCP-w
- ETSI TS 119 411-8 V1.1.1 (2025-10), ESI; Policy and security requirements for Trust Service Providers issuing certificates; Part 8: Access Certificate Policy for EUDI Wallet Relying Parties
- ETSI EN 319 412-1 V1.6.1 (2025-06), ESI; Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 V2.4.1 (2025-06), ESI; Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 V1.3.1 (2023-09), ESI; Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

- ETSI EN 319 412-4 V1.4.1 (2025-06), ESI; Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations
- ETSI EN 319 412-5 V2.5.1 (2025-06), ESI; Certificate Profiles; Part 5: QCStatements
- ETSI TS 119 412-6 V1.1.1 (2025-09), ESI; Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers
- ETSI EN 319 421 V1.3.1 (2025-05), ESI; Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 V1.1.1 (2016-03), ESI; Time-stamping protocol and time-stamp token profiles
- ETSI TS 119 431-1 V1.3.1 (2024-12), ESI; Policy and security requirements for TSP; Part 1: TSP service components operating a remote QSCD/SCDev
- ETSI TS 119 432 V1.3.1 (2026-03), ESI; Protocols for remote digital signature creation
- ETSI TS 119 441 V1.2.1 (2023-10), ESI; Policy requirements for TSP providing signature validation services
- ETSI TS 119 442 V1.1.1 (2019-02), ESI; Protocol profiles for trust service providers providing AdES digital signature validation services
- ETSI TS 119 461 V2.1.1 (2025-02), ESI; Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI TS 119 471 V1.1.1 (2025-05), ESI; Policy and Security requirements for Providers of Electronic Attestation of Attributes Services
- ETSI TS 119 472-1 V1.2.1 (2026-02), ESI; Profiles for Electronic Attestation of Attributes; Part 1: General requirements
- ETSI TS 119 472-2 V1.2.1 (2026-03), ESI; Profiles for Electronic Attestation of Attributes; Part 2: Profiles for EAA/PID Presentations to Relying Party
- ETSI TS 119 472-3 V1.1.1 (2026-03), ESI; Profiles for Electronic Attestation of Attributes; Part 3: Profiles for issuance of EAA or PID
- ETSI TS 119 475 V1.2.1 (2026-03), ESI; Relying party attributes supporting EUDI Wallet user's authorization decisions
- ETSI TS 119 478 V1.1.1 (2026-01), Specification of interfaces related to Authentic Sources
- ETSI TS 119 511 V1.1.1 (2019-06), ESI; Policy and security requirements for TSP providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI TS 119 512 V1.2.1 (2023-05), ESI; Protocols for long-term preservation
- ETSI EN 319 521 V1.1.1 (2019-02), ESI; Policy requirements for registered electronic mail
- ETSI EN 319 522-1 V1.2.1 (2024-01), ESI; Electronic Registered Delivery Services; Part 1: Framework and Architecture
- ETSI EN 319 522-2 V1.2.1 (2024-01), ESI; Electronic Registered Delivery Services; Part 2: Semantic contents
- ETSI EN 319 522-3 V1.2.1 (2024-01), ESI; Electronic Registered Delivery Services; Part 3: Formats
- ETSI EN 319 522-4-1 V1.2.1 (2019-01), ESI; Electronic Registered Delivery Services; Part 4-1: Message delivery bindings
- ETSI EN 319 522-4-2 V1.1.1 (2018-09), ESI; Electronic Registered Delivery Services; Part 4-2: REM Capability/requirements

- ETSI EN 319 522-4-3 V1.1.1 (2018-09), ESI; Electronic Registered Delivery Services; Part 4-3: REM Message Disposition (MD)
- ETSI TS 119 602 V1.1.1 (2025-11), Lists of trusted entities; Data model
- ETSI TS 119 612 V2.4.1 (2025-08), ESI; Trusted Lists
- CEN/TS 18170:2025, Functional requirements for the electronic archiving services
- CEN/TS 419261:2015, Security requirements for trustworthy systems managing certificates and time-stamps
- EN 419241-1:2018, Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
- EN 419241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing
- ISO/IEC 15408-1:2022, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model
- ISO/IEC 15408-2:2022, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components
- ISO/IEC 15408-3:2022, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components
- ISO/IEC 15408-4:2022, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities
- ISO/IEC 15408-5:2022, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements
- ISO/IEC 18013-5:2021, Personal identification - ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application
- ISO/IEC TS 18013-7:2025, Personal identification - ISO-compliant driving licence - Part 7: Mobile driving licence (mDL) add-on functions
- ISO 14641:2018 (ersetzt ISO 14641-1:2012), Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications
- ISO 14721:2003, Space data and information transfer systems - Open archival information system (OAIS) - Reference model
- ISO 23257:2022, Blockchain and distributed ledger technologies - Reference architecture
- ISO/TS 23635:2022, Blockchain and distributed ledger technologies - Guidelines for governance
- RFC 3161 (2001), Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- RFC 3339 (2002), Date and Time on the Internet: Timestamps
- RFC 4998 (2007), Evidence Record Syntax (ERS)
- RFC 5280 (2008), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5322 (2008), Internet Message Format
- RFC 5816 (2010), ESSCertIDv2 Update for RFC 3161
- RFC 6283 (2011), Extensible Markup Language Evidence Record Syntax (XMLERS)
- RFC 6960 (2013), X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

- RFC 7515 (2015), JSON Web Signature (JWS)
- RFC 7519 (2015), JSON Web Token (JWT)
- RFC 7800 (2016), Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)
- RFC 8610 (2019), Concise Data Definition Language (CDDL): A Notational Convention to Express CBOR and JSON Data Structures
- RFC 8943 (2020), Concise Binary Object Representation (CBOR) Tags for Date
- RFC 8949 (2020), Concise Binary Object Representation (CBOR)
- RFC 9360 (2023), CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates
- RFC 9901 (2025), Selective Disclosure for JSON Web Tokens
- OAuth Status List Draft, Entwurf, Token Status List (TSL)
- OpenID4VCI 1.0, OpenID for Verifiable Credential Issuance
- OpenID4VP 1.0, OpenID for Verifiable Presentations
- OpenID4VC HAIP 1.0, OpenID4VC High Assurance Interoperability Profile
- WebAuthn Level 2, W3C Rec. (2021-04), Web Authentication: An API for accessing Public Key Credentials, Level 2
- VC Data Model v2.0, W3C Rec. (2025-05-15), Verifiable Credentials Data Model v2.0
- ECCG Agreed Cryptographic Mechanisms, Version 2.0 (April 2025), Agreed Cryptographic Mechanisms (European Cybersecurity Certification Group)
- EUCC Guidelines Cryptography, Version 2 (2025-05), EUCC Guidelines Cryptography
- FIPS 140-3 (2019), Security Requirements for Cryptographic Modules

9.2 Weitere Standards von Normungsorganisationen

- Europäisches Institut für Telekommunikationsnormen (ETSI), Technical Committee (TC) Electronic Signatures and Trust Infrastructures (ESI)
- Europäisches Komitee für Normung, CEN/TC 224 – Persönliche Identifikation und damit verbundene persönliche Geräte mit sicherem Element, Systeme, Verfahren und Privatsphäre in einem sektorübergreifenden Umfeld
- Internationale Organisation für Normung

9.3 Dokumente der Agentur der Europäischen Union für Cybersicherheit (ENISA)

- Digital Identity and Data Protection
- EUCC Certification Scheme
- EUCC Guidelines on Cryptography

9.4 Requests for Comments (RFCs) und Internet Drafts der Internet Engineering Task Force (IETF)

- PKIX Working Group (Public-Key Infrastructure [X.509])
- TSL Working Group (Transport Layer Security)
- SMIME Working Group (S/MIME Mail Security)
- LAMPS Working Group (Limited Additional Mechanisms for PKIX and SMIME)

9.5 Andere relevante Standards und bewährte Verfahren

- Internationale Fernmeldeunion, ITU-T Recommendations X series: Data networks, open system communications and security
- Common Criteria for Information Technology Security Evaluation
- National Institute of Standards and Technology, Federal Information Processing Standards (FIPS)
- CA/Browser Forum
- Cloud Signature Consortium

10 Listen der Europäischen Kommission

- Nach Artikel 9 Absatz 1 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt notifizierte elektronische Identifizierungssysteme
- Aufsichtsstellen für Vertrauensdienste
- Nationale Akkreditierungsstellen und Konformitätsbewertungsstellen für qualifizierte Vertrauensdienste
- Qualifizierte elektronische Signaturerstellungseinheiten, qualifizierte elektronische Siegelerstellungseinheiten und sichere elektronische Signaturerstellungseinheiten
- Benannte Stellen zur Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten, qualifizierter elektronischer Siegelerstellungseinheiten und sicherer elektronischer Signaturerstellungseinheiten
- Alternative Verfahren zur Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten und qualifizierter elektronischer Siegelerstellungseinheiten