Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Kommunikation BAKOM

Biel, 20. August 2025

Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate

(Ausgabe 3)

Erläuternder Bericht

1 Einleitung

Das vorliegende Dokument erläutert die Änderungen, die in der dritten Ausgabe (2025) der technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (TAV) vorgenommen worden sind.

2 Änderungen

Kapitel 1.2

Das Europäische Komitee für Normung (CEN) und das Europäische Institut für Telekommunikationsnormen (ETSI) haben neue Fassungen von Normen, auf die in der vorherigen Ausgabe der TAV verwiesen wurde, veröffentlicht. Den folgenden Neuerungen wurde in der Ausgabe 3 der TAV Rechnung getragen.

ETSI EN 319 411-2 V2.6.1 (2025-06)
Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

ISO/IEC 15408-3:2022
Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components

ETSI TS 119 431-1 V1.3.1 (2024-12)
Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

ETSI TS 119 461 V2.1.1 (2025-02)
Policy and security requirements for trust service components providing identity proofing of trust service subjects

ETSI EN 319 412-1 V1.6.1 (2025-06)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 V2.4.1 (2025-06)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 V1.3.1 (2023-09)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 V1.4.1 (2025-06)
Electronic Signatures and Infrastructures (ESI);
Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 V2.5.1 (2025-06)
Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

CA/Browser-Forum Guidelines for the Issuance and Management of Extended Validation Certificates, Version 2.0.1 (2024-05)

ETSI EN 319 421 V1.3.1 (2025-07)
Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Die Änderungen werden grundsätzlich im Anhang der neuen Versionen der Normen beschrieben. Im Rahmen der Normierungsarbeiten wurden einige kleinere redaktionelle Anpassungen vorgenommen, wie zum Beispiel das Hinzufügen von Verweisen oder Präzisierungen der Anforderungen. Andere zentrale Punkte werden in den nachfolgenden Kapiteln erläutert.

Es wird indirekt auf die Norm ETSI EN 319 401 *Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers* verwiesen, die kürzlich überarbeitet wurde, um die Anforderungen der 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* (NIS2-Richtlinie) umzusetzen, wie in ihrer Einleitung erwähnt. Es ist richtig, dass die NIS2-Richtlinie in der Schweiz nicht direkt anwendbar ist. Die Änderungen der ETSI-Norm berücksichtigen jedoch die Entwicklungen im Sicherheitsmanagement, die für eine sichere und qualitativ hochwertige Dienstleistungserbringung wichtig sind. Ausserdem ermöglicht die Verwendung der ETSI EN 319 401, die Schweizer Vorschriften mit denen der europäischen Länder zu harmonisieren. Anbieterinnen von Zertifizierungsdiensten befürchten jedoch, dass der Verweis auf diese Norm in den technischen und administrativen Vorschriften implizieren könnte, dass die Anforderungen der europäischen Vorschriften, insbesondere der NIS2-Richtlinie, erfüllt werden müssen. Diese Befürchtung ist unbegründet, denn wie bei den meisten ETSI-Normen und -Spezifikationen sind die Anforderungen der ETSI EN 319 401 neutral formuliert, wenn es um die Einhaltung der geltenden Gesetzgebung geht, sodass die Norm auch in einem Drittland angewendet werden kann. Formulierungen wie „*in accordance with relevant laws and regulations*“, „*as mandated by relevant legislative frameworks*“ oder „*in line with the applicable regulatory rules*“ werden verwendet, und Verweise auf das europäische Recht erscheinen nur als Beispiele oder in Anmerkungen. Anerkannte Anbieterinnen von Zertifizierungsdiensten in der Schweiz müssen daher bei der Verwendung solcher Formulierungen die schweizerische Gesetzgebung einhalten. Soweit möglich, werden sie sich auf das Prinzip der Anforderung beschränken, wenn keine Bestimmung des Schweizer Rechts diesen Aspekt abdeckt.

Kapitel 2.2.3, Bst. d)

In den Kapiteln 3.1 und 4.4 der neuen Ausgabe der Spezifikation ETSI TS 119 431-1, auf die in diesen TAV, Kapitel 2.2.3, Buchstabe d) verwiesen wird, wird der Begriff *One-time signing key* eingeführt. Dabei handelt es sich um einen kryptografischen Schlüssel, der nur für eine einmalige Signatursitzung verwendet werden kann. Die neue Ausgabe der Spezifikation sieht ausserdem die Möglichkeit vor, den Signaturschlüssel direkt mit der Identität des Dienstnutzers zu verknüpfen, anstatt auf eine eID zurückzugreifen. Eine solche Authentifizierung ist jedoch allerdings nur im Rahmen einer einmaligen Signatursitzung (*One-time signing key*) anwendbar.

Nach der Veröffentlichung der ersten Ausgabe der Spezifikation ETSI TS 119 461 haben die ETSI-Expertinnen und -Experten Anpassungsarbeiten unternommen, um die neuen Erkenntnisse über Bedrohungen und Risiken zu berücksichtigen. Die Anforderungen in der Spezifikation wurden aktualisiert, präzisiert oder ergänzt, um diesen Entwicklungen Rechnung zu tragen. Die Anpassungen wurden insbesondere bei der Validierung der Attribute der Zertifikatsinhaberin bzw. des Zertifikatsinhabers und der Nachweise für die Identifikation sowie bei der Erfassung und Bearbeitung biometrischer Informationen vorgenommen. Um besser auf die sich verändernden Bedrohungen reagieren zu können, wurden ausserdem neue Anforderungen an die Einschätzung der eigenen operativen Risiken sowie die Pflicht eingeführt, die Instrumente zur Erkennung von Angriffen durch biometrische Injektion

und von Präsentationsangriffen regelmässig von einer akkreditierten Bewertungsstelle beurteilen zu lassen.

Eine neue Ausgabe dieser Spezifikation ist seit Februar 2025 verfügbar. Um ein ausreichendes Mass an Sicherheit und Zuverlässigkeit in der schweizerischen Gesetzgebung aufrechtzuerhalten, ist es daher notwendig, diese Entwicklungen auch im Rahmen der TAV zu berücksichtigen. Die Anpassung der operativen Prozesse der anerkannten Anbieterinnen von Zertifizierungsdiensten an die geänderten Regeln ist jedoch mit einem nicht unerheblichen Aufwand verbunden. Daher ist in Kapitel 3 eine Frist für die Umsetzung vorgesehen.

Die Struktur und die Kapitelüberschriften der Spezifikation ETSI TS 119 461 wurden in der neuen Ausgabe kaum geändert, weshalb die Verweise auf die relevanten Kapitel in diesen TAV nicht angepasst werden müssen.

In der neuen Ausgabe der Spezifikation ETSI TS 119 461 wird zwischen den Anforderungsstufen *Baseline LoIP (Level of Identity Proofing)* und *Extended LoIP* unterschieden. Letztere ist für die Ausstellung qualifizierter Zertifikate im Sinne der Verordnung (EU) Nr. 910/2014 *des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS), geändert durch die Verordnung (EU) 2024/1183*, anwendbar. In Kapitel 2.3.1, Buchstabe a) muss daher präzisiert werden, welche Anforderungsstufe zu berücksichtigen ist.

Die Verweise auf die Kapitel 5 *Operational risk assessment*, 6 *Policies and practices* und 7 *Identity proofing service management and operation* der Spezifikation können gestrichen werden, da sie in Kapitel 9.1 *Introduction, compliance with the present document, general requirements for all use cases*, auf das in diesen TAV Bezug genommen wird, angegeben werden.

Weil es in der Schweiz derzeit keine gesetzlichen Regelungen für E-IDs gibt, soll das Kapitel 9.2.4 *Use case for identity proofing by authentication using eID means* weiterhin nicht integriert werden. Nach Inkrafttreten des Bundesgesetzes über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) müssen die TAV erneut angepasst werden, um die Identifikation einer Antragstellerin bzw. eines Antragstellers eines Zertifikats auf der Grundlage einer E-ID zu ermöglichen.

In Übereinstimmung mit der Änderung von Artikel 7 Absatz 3 VZertES reicht es aus, wenn die Antragstellerin oder der Antragsteller einen Antrag stellt, der mit einer geregelten elektronischen Signatur – die auf einem geregelten Zertifikat beruht – versehen ist, da die Regeln für die Identifikation und das Verfahren zur Ausstellung des Zertifikats für qualifizierte und geregelte Zertifikate gleich sind. Dadurch wird die Qualität und Zuverlässigkeit der in den geregelten Zertifikaten enthaltenen Identitätsinformationen sichergestellt.

Es ist nicht mehr gerechtfertigt, die in den Kapiteln 8.2.5 *Use of existing digital signature means as evidence* und 8.3.5 *Validation of digital signature with certificate* der Spezifikation ETSI TS 119 461 genannten Anforderungen nicht aufzunehmen, da sich herausgestellt hat, dass alle diese Anforderungen im von diesen TAV vorgesehenen Kontext umsetzbar sind.

In Bezug auf die Anforderungen an die Identifikation einer natürlichen Person, die eine UID-Einheit vertritt, muss die Bezugnahme auf Kapitel 8.4.5 *Binding to applicant for legal person and natural person representing legal person* der Spezifikation ETSI TS 119 461 hinzugefügt werden, weil eine solche in Kapitel 9.4, auf das in diesen TAV in diesem Fall verwiesen wird, nicht vorhanden ist.

Kapitel 2.3.1, Bst. c)

Kapitel 6.3.10 der neuen Ausgabe der Norm ETSI EN 319 411-2, auf das in diesen TAV unter Buchstabe g) verwiesen wird, schreibt künftig vor, dass der in Kapitel 5.2 der Norm EN 319 412-1 [5] definierte Erweiterung *validity assured short term certificate* im Zertifikat erwähnt wird, wenn es sich um ein Zertifikat handelt, das aufgrund seiner kurzen Gültigkeitsdauer nicht widerrufen werden kann (sog. *short term certificate*). Diese Information dient dem Signaturprüfer als Bestätigung für die Gültigkeit des Zertifikats.

Kapitel 2.3.1, Bst. g)

Die neu in Buchstabe g) eingeführten Anforderungen legen fest, wie die langfristige Online-Verfügbarkeit von Informationen über die Ungültigerklärung von geregelten Zertifikaten, die im geänderten Artikel 9 VZertES vorgesehen ist, konkretisiert wird. Sie richten sich nach den bewährten Verfahren der Norm ETSI EN 319 411-2, auf die sie verweisen.

Des Weiteren trägt die Formulierung der neuen Anforderungen auch der Tatsache Rechnung, dass Informationen zu widerrufenen Zertifikaten entweder über eine Sperrliste *(Certificate Revocation List, CRL*) oder über einen OCSP-Dienst (*Online Certificate Status Protocol*) abgefragt werden können. Gemäss den in Artikel 9 Absatz 2 vorgesehenen Ausnahmen sollen diese Anforderungen jedoch nicht für Zertifikate, deren Widerruf grundsätzlich nicht möglich ist (sog. *Short Term Certificates*), gelten. Sie sollen auch nicht für Zertifikate, auf denen Signaturen mit Langzeitvalidierungsinformationen (sog. *Long Term Validation Signatures, LTV*) beruhen, gelten.

Kapitel 2.3.2

Kapitel 4.2.3.1 der neuen Ausgabe der Norm ETSI EN 319 412-2, auf das in diesen TAV, Kapitel 2.3.2, Buchstabe b) verwiesen wird, schreibt künftig die Angabe einer Registrierungsnummer im Attribut *organizationIdentifier* des Felds Issuer vor, wenn eine solche Nummer vorhanden ist. Die anerkannte Anbieterin von Zertifizierungsdiensten gibt bei diesem Attribut ihre UID-Nummer an.

Kapitel 2.3.2, Bst. e) und f)

Die Angabe der Vor- und Nachnamen in Zertifikaten natürlicher Personen wurde in Kapitel 4.2.4 der Neuausgabe der Norm ETSI EN 319 412-2 präzisiert, auf die diese TAV verweisen. In der Norm wird klargestellt, dass der Inhalt der Felder *surname* und *givenName* identisch mit den Angaben im Ausweisdokument sein muss. Die Anforderungen unter den Buchstaben e) und f) sind daher redundant und können gestrichen werden.

Kapitel 2.3.2, Bst. g) (neu: Bst. e)

Der Verweis auf das Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG; SR 431.03) wird präzisiert.

Kapitel 2.3.3

Der Titel und der Einleitungssatz dieses Kapitels wurden angepasst, da es sich bei den genannten zusätzlichen Anforderungen im Grunde um Besonderheiten der qualifizierten Zertifikate handelt, die keine zusätzlichen Anforderungen beinhalten. Tatsächlich sind qualifizierte Zertifikate eine Sonderform der geregelten Zertifikate nach Artikel 2 Buchstabe h ZertES. Demnach gelten die Anforderungen der Kapitel 2.3.1 und 2.3.2 der TAV auch für qualifizierte Zertifikate, wobei die in Kapitel 2.3.3 aufgeführten Besonderheiten zu berücksichtigen sind.

Kapitel 2.3.4

Die Bundeskanzlei hat das *Konzept geregeltes Zertifikat ausgestellt für eine Behörde / Zusammenarbeit mit dem eGov Signaturvalidator* nach Konsultation der interessierten Kreise angepasst (die neue Version 1.5 vom 9.4.2024 ist auf der Webseite https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur.html abrufbar).

Kapitel 2.3.4, Buchstabe a) muss daher angepasst werden, um den vorgenommenen Änderungen Rechnung zu tragen.

Auf Antrag der anerkannten Anbieterinnen von Zertifizierungsdiensten wird Buchstabe b) gestrichen, da er sich auf eine Anforderung bezieht, die nur für TLS-Zertifikate (*Transport Layer Security*) gilt und nicht für geregelte Zertifikate, auf denen die von Behörden ausgestellten geregelten Siegel beruhen. Darüber hinaus sind die Informationen im Feld *businessCategory* redundant, da sie bereits im Feld *OrganizationalUnit* gemäss Buchstabe a) zwingend bereitgestellt werden müssen.

Kapitel 3 wird geändert, da die darin geregelten Umsetzungsfristen abgelaufen und damit obsolet geworden sind.

Für die Umsetzung der umfangreichen und anspruchsvollen Anforderungen, die sich aus der Anpassung der in Kapitel 2.3.1 Bst. a) referenzierten Spezifikation ETSI TS 119 461 ergeben, ist eine Frist zu setzen, damit die Anbieterinnen von Zertifizierungsdienste ihre betrieblichen Verfahren anpassen können. Die in Kapitel 2.3.1, Buchstabe g) vorgenommenen Anpassungen erfordern keine spezifische und sofortige Konformitätsbewertung. Die Anpassungen des Kapitels 2.3.1 sowie die mit der neuen Ausgabe der referenzierten ETSI TS 119 461 Spezifikation eingeführten Anforderungen haben spätestens bis zum 01. Juli 2027 zu erfolgen.

Für die Umsetzung der in Kapitel 2.3.4 vorgesehenen Anpassungen ist keine Frist geplant, da die meisten Anbieterinnen von Zertifizierungsdiensten diese seit der Aktualisierung des Konzepts geregeltes Zertifikat ausgestellt für eine Behörde / Zusammenarbeit mit dem eGov Signaturvalidator im Oktober 2024 anwenden können.