

White Paper
25.02.2026

Fernsignaturen gem. Art. 29a/39a eIDAS

1. Einleitung

Die eIDAS 2.0 – umgangssprachlich wird hiermit die aktuell gültige Fassung der eIDAS-Verordnung 910/2014 bezeichnet – sieht in Art. 29a „Anforderungen an einen qualifizierten Dienst zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten“ vor. Diese Remote-Signaturen erfreuen sich einer unveränderten Beliebtheit, weil das Handling mit einer sicheren Signaturerstellungseinheit – meist eine Signaturkarte – noch immer als umständlich gilt. Eventuell bessert sich die Situation mit der Wallet (Europäische Brieftasche für die Digitale Identität).

Beim Einsatz von Fernsignaturen werden die sicheren Signaturerstellungseinheit bei einem Vertrauensdiensteanbieter sicher verwahrt und betrieben. Und ein Anwender autorisiert von außen die Signierung.

In Art. 29a werden unter Abs. 2 nähere Details in einem Durchführungsrechtsakt versprochen, einem sogenannten Implementing Act. Dieser Implementing Act liegt jetzt vor: 2025/1567. Implementing Acts dienen der EU-weiten Harmonisierung. Sie greifen ganz zentral auf bestehende Standards zurück und konkretisieren einzelne Anforderungen.

Im Implementing Act 2025/1567 wird auf den ETSI-Standard ETSI TS 119 431-1 verwiesen. Titel: „TSP services operating a remote QSCD / SCDev“. Dieser Standard konkretisiert die grundlegenden Anforderungen an einen Trust Service Provider aus der ETSI 319 401 um spezifische Anforderungen. Ferner referenziert die ETSI TS 119 431-1 auf eine weitere Norm, die DIN EN 419 241-1.

Wichtig: Dieser Implementing Act 1567 adressiert lediglich den Dienst, nicht den Anbieter. Für den Vertrauensdiensteanbieter, der Fernsignaturen/-siegel anbietet, gilt der Implementing Act 2025/2530.

Wie diese Normen zusammenspielen, das beleuchtet das vorliegende Dokument

Übrigens gelten diese Aussagen auch für Fernsiegel gem. Art. 39a eIDAS.

2. Übersicht über rechtliche Grundlagen und Standards sowie Begriffe

Zunächst folgt eine Übersicht über die rechtlichen Grundlagen und Standards sowie einige Begriffe.

2.1. eIDAS 2.0

Die eIDAS-Verordnung 910/2014 ist gültig, nunmehr in der Fassung vom April 2025; exakte Referenz:

- [eIDAS] 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, geändert durch: Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, amended by: Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024

2.2. Implementing Act 2025/1567

Art. 29a Abs. 2 eIDAS referenziert auf einen Implementing Act, der nunmehr veröffentlicht ist; exakte Referenz:

- [ImplAct-1567] 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**
- Commission Implementing Regulation (EU) 2025/1567 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the management of **remote qualified electronic signature creation devices** and of **remote qualified electronic seal creation devices** as qualified trust services

Der Implementing Act 2025/1567 normiert im Annex die Anwendung der folgenden Standards: ETSI TS 119 431-1, V1.3.1 (2024-12)

2.3. ETSI TS 119 431-1

ETSI TS 119 431-1 definiert Anforderungen an einen Vertrauensdiensteanbieter, der Fernsignaturen anbietet; exakte Referenz:

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

Die 119 431-1 setzt auf der ETSI 319 401 auf, welche allgemeine Anforderungen an Vertrauensdiensteanbieter (Trust Service Provider) definiert.

Kapitel 4 beschreibt zunächst den grundsätzlichen Aufbau, wie Fernsignaturen erzeugt werden sollen. Wichtig in diesem Kontext sind auch die besonderen Begriffe:

- SAD: Signatur-Aktivierungsdaten

- SAM: Signatur-Aktivierungsmodul
- SAP: Signatur-Aktivierungsprotokoll
- SCA: Signaturerstellungsanwendung
- SCAL: Alleinige Kontrolle Sicherheitsniveau
- SCDev: Signaturerstellungseinheit
- SIC: Signer's Interaction Component, Interaktionskomponente des Unterzeichners

Kapitel 5 definiert Konkretisierungen in den Policies.

Kapitel 6 beschreibt insbesondere den speziellen Prozess für Fernsignierung:

- Initialisierung (Signing key initialization) mit
 - der Erzeugung des Signaturschlüssels,
 - der Identitätsfeststellung sowie
 - der Zuordnung zum Zertifikat
- Betrieb (Signing key life-cycle operational requirements) mit
 - der Aktivierung,
 - der Löschung sowie
 - dem Backup.

Ferner konkretisiert Kap. 6.4ff Anforderungen aus der 319 401 an die Umgebung; hier ist insbesondere die Protokollierung zu beachten.

Wichtig ist noch Annex A, weil dessen Umsetzung für die aktuelle eIDAS zwingend erforderlich ist.

2.4. DIN EN 419 241-1

Die – kostenpflichtige Norm – DIN EN 419 241-1 enthält Anforderungen an Systeme, die Serversignaturen unterstützen; exakte Referenz:

[419 241-1] DIN EN 419241-1:2018, Vertrauenswürdige Systeme, die Serversignaturen unterstützen, Teil 1: Allgemeine Systemsicherheitsanforderungen; Deutsche Fassung EN 419241-1; September 2018

Aus der 119 431-1 heraus werden nur einzelne konkrete Anforderungen herangezogen, was über eindeutige Identifier gut funktioniert, beispielsweise SRG_KM.2.1.

2.5. Implementing Act 2025/2530

Art. 24 eIDAS enthält „Anforderungen an qualifizierte Vertrauensdiensteanbieter“, die über den Implementing Act 2025/2530 konkretisiert werden:

[ImplAct-2530] 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

Commission Implementing Regulation (EU) 2025/2530 of 16 December 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards requirements for **qualified trust service providers** providing qualified trust services

Im Implementing Act 2025/2530 ist ausgeführt, dass „diese Verordnung [...] ab dem 19. August 2027“ gilt.

3. Zentrale Anforderungen an den Dienst

Zentrale Anforderungen, die der Gesetzgeber über den Implementing Act und die einbezogenen Standards an Fernsignaturen stellt, sind insbesondere

- Signaturschlüssel-Erzeugung
- Identitätsfeststellung
- Auslösung einer Signatur
- Policy

3.1. Signaturschlüssel-Erzeugung

Für die Signaturschlüssel-Erzeugung ist eine sichere Signaturerstellungseinheit notwendig: Secure Signature Creation Device, SSCD; EAL4-zertifiziert. Im eIDAS-Kontext sogar noch schärfer – hier wird eine QSCD gefordert:

GEN-A.4-01 [EUSPv2]: Signer's signing key shall be generated in a **QSCD**.

Es sind hinreichend geeignete Algorithmen und Parameter notwendig. Die Initialisierung erfolgt im 4-Augen-Prinzip. Ferner gibt es Vorgaben für ein Backup. Schlüssel dürfen vorab erzeugt werden.

3.2. Identitätsfeststellung

Wie immer bei qualifizierten Zertifikaten ist die Identitätsfeststellung wichtig, also auf welcher Basis die Identität des Unterzeichners festgestellt wird. Und ob ein eID means (electronic Identification means) genutzt wird, welches dann auf die Identität verweist, oder ob direkt auf eine Identität verwiesen wird.

6.2.2 eID means or identity linking

NOTE 1: The signing key is either linked to an **eID means** which is linked to the identity or directly to the identity. The latter is only possible in a process using a **one-time** signing key.

LNK-6.2.2-00 [CONDITIONAL]: In case a **one-time signing key** is used, the key and the authentication may be linked directly to the identity instead of the linking to the eID means.

Auch kommen hier wieder die Level of Identity Proofing (LoIP) ins Spiel, für die über den Implementing Act 2025/1566 die ETSI-Norm 119 461 herangezogen wird:

- Baseline LoIP
- Extended LoIP

Wichtig: Im eIDAS-Kontext qualifizierter Zertifikate ist Extended LoIP erforderlich:

A.7 eID means linking

LNK-A.7-01 [EUSPv2]: The identity proofing of the signer shall fulfil the requirements of **extended Level of Identity Proofing (LoIP)** as defined in ETSI TS 119 461 [6].

3.3. Auslösung einer Signatur

Auch wenn der eigentliche Signaturschlüssel sicher beim Vertrauensdiensteanbieter verwahrt ist, ist für die Auslösung einer Signatur doch der Unterzeichner (Signer) verantwortlich; ihm wird auch die Signatur im Sinne einer Unterschrift zugeordnet.

Deshalb sind Maßnahmen zur alleinigen Kontrolle wichtig; dazu werden entsprechende Maßnahmen gefordert:

A.6 Signature activation data management

SIG-A.6-06A [EUSPv2]: Clause SRA_SAP.2.6 of EN 419241-1 [3], specifying signature activation data collection and protection, shall apply.

SRA_SAP.2.6: Die SAD MÜSSEN:

- unter der Kontrolle des Unterzeichners mit einer **hohen Vertrauensstufe** erfasst werden,
- so geschützt werden, dass **Schlüssel** in Einheiten **sicher** sind, und
- eventuell benutzte (einmalige oder langfristige) **Geheimnisse** nach SRA_SAP.1.4 schützen.

SRA_SAP.2.7: Das SAP MUSS so ausgelegt sein, dass beim Empfang von SAD im SAM angenommen werden kann, dass die SAD unter der **alleinigen Kontrolle** des Unterzeichners durch **Mittel in seinem Besitz** übermittelt worden sind.

Ferner sind sichere Protokolle erforderlich.

3.4. Policy

Im eIDAS-Kontext muss die Policy eine besondere OID aufweisen:

A.2 Policy name and identification

EUSPv2: EU SSAS Policy

itu-t(o) identified-organization(4) etsi(o) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)

4. Zentrale Anforderungen an den Anbieter

Der Implementing Act 2025/2530 normiert bzw. konkretisiert die folgenden Sachverhalte:

- Meldung bei der Aufsichtsstelle, vgl. Art. 1
 - Es wird spezifiziert, welche wesentlichen Änderungen der Aufsichtsstelle gemeldet werden müssen; die Auflistung ist umfangreich:
 - „a) **Dienstbeschreibungen, Regelungen, Praxiserklärungen** oder damit verbundenen **Nutzungsbedingungen**;
 - b) **technische Architektur** der qualifizierten Vertrauensdienste oder vertrauenswürdige Systeme oder Produkte gemäß Artikel 24 Absatz 2 Buchstaben e und f der Verordnung (EU) Nr. 910/2014;
 - c) Bereitstellung **technischer Komponenten**, die für die Erbringung der qualifizierten Vertrauensdienste erforderlich sind, oder die zu diesen technischen Komponenten gehörigen technischen Dienste;
 - d) Verwendung **kryptografischer Techniken** oder kryptografischen Materials bei der Erbringung der qualifizierten Vertrauensdienste;
 - e) **Registrierungs- und Identifizierungsverfahren**;
 - f) **Organisationsstruktur** oder **Leitung** des Vertrauensdiensteanbieters;
 - g) **Beendigungsplan**;
 - h) in Artikel 24 Absatz 2 Buchstabe c der Verordnung (EU) Nr. 910/2014 genannte **Finanzmittel** und **Haftpflichtversicherungen**;
 - i) Elemente, die sich auf den **Inhalt** der betreffenden nationalen **Vertrauensliste** auswirken;
 - j) an der Erbringung der qualifizierten Vertrauensdienste **beteiligte Dritte**, einschließlich **Unterauftragnehmer** oder **Dienstleister**, oder Änderungen an den Vertragsbedingungen mit diesen Dritten.“
 - Ferner wird der Inhalt der Meldungen spezifiziert:
 - a) **Beschreibung** der Änderung,
 - b) geplanter **Zeitpunkt** der Änderung (Datum und Uhrzeit),
 - c) **Gründe** der Änderung und gegebenenfalls Nachweise für die Gründe,
 - d) gegebenenfalls **aktualisierte Dokumente**.
 - Sicherlich ist es sinnvoll, sich über die Kategorisierung einer „wesentlichen“ Änderung mit der Aufsichtsstelle zu verständigen, um sicherzugehen, dass tatsächlich nur signifikante Änderungen mitgeteilt werden.
- Risikomanagement, vgl. Art. 2
 - Das Risikomanagement referenziert auf den Implementing Act 2025/2160, der eigentlich den nicht-qualifizierten Vertrauensdiensten zugedacht ist. Nichtsdestotrotz gelten Abs. 2, 3 und 4 von 2025/2160 auch für qualifizierte Vertrauensdienste aufgrund von Art. 24 Abs. 2 (fa) eIDAS:
 - „Unbeschadet des Artikels 21 der Richtlinie (EU) 2022/2555 haben sie angemessene Strategien und treffen entsprechende Maßnahmen zur Beherrschung

rechtlicher, geschäftlicher, betrieblicher und sonstiger direkter oder indirekter Risiken bei der Erbringung des qualifizierten Vertrauensdienstes, einschließlich zumindest Maßnahmen in Bezug auf Folgendes:

- i) Registrierungs- und Einbindungsverfahren für einen Dienst;
- ii) Verfahrens- oder Verwaltungskontrollen;
- iii) die Verwaltung und Durchführung von Diensten.“
- Abs. 2, 3 und 4 des Implementing Acts 2025/2160 fordern ein klassisches Risikomanagement mit einem Konzept (**Framework**), der **Ermittlung, Dokumentation und Bewertung** von Risiken sowie **Risikobehandlungsmaßnahmen**.
- Beendigungsplan, vgl. Art. 3
 - Es werden konkrete Anforderungen an den Beendigungsplan spezifiziert, etwa zu **regelm. Kontrollen**, der Einbindung in das **Risikomanagement**, der hinreichenden **finanziellen** Absicherung, der **techn. und org. Beendigung** inkl. der **Benachrichtigung**.

- Referenzstandards und Spezifikationen im Annex, vgl. Art. 4

Im Annex werden hierzu die folgenden Dienste aufgeführt:

- Qualifizierte Dienste zur Verwaltung qualifizierter elektronischer Fernsignaturerstellungseinheiten
- Qualifizierte Dienste zur Verwaltung qualifizierter elektronischer Fernsiegelerstellungseinheiten

Diesen Diensten werden die folgenden Implementing Acts, ETSI-Standards und relevante Abschnitte zugeordnet:

- Implementing Act: 2025/1567
- Standard: ETSI TS 119 431-1
- Abschnitte: Abs. 5, 6.1, 6.4, 6.5, 6.7 und 6.8

Wichtig: Der Implementing Acts 2530 fordert also für den VDA nicht die gesamte Norm 119 431-1, sondern nur ausgewählte Aspekte.

Gleichwohl verfolgt die datenschutz cert GmbH im Rahmen ihrer Zertifizierungsprojekte einen anderen Ansatz, und nutzt den folgenden Anforderungsrahmen zur Zertifizierung des Vertrauensdienstes:

- eIDAS-Anforderungen an den Dienst und den Diensteanbieter
- Implementing Act 2530
- ETSI 319 401
- ETSI 119 431-1

5. Fazit

Qualifizierte Fernsignaturen werden über den Implementing Act 2025/1567 europaweit harmonisiert; hierüber wird insbesondere die ETSI-Norm 119 431-1 herangezogen,

die in zentralen Punkten auf die DIN 419 241-1 Bezug nimmt. Für qualifizierte Fernsignaturen bleibt als Identitätsfeststellung Extended LoIP verpflichtend.

Qualifizierte Vertrauensdiensteanbieter für die Nutzung von Fernsignaturen-/siegeln werden über den Implementing Act 2025/2530 europaweit harmonisiert; hierüber werden anerkannte ETSI-Standards eingezogen, hier: 391 401 und 119 431-1. Beide werden von der datenschutz cert GmbH im Rahmen der Zertifizierung genutzt.

Auch wenn der Implementing Act 2530 formal erst „ab dem 19. August 2027“ gilt, ist doch damit zu rechnen, dass er schon vorher zur Anwendung kommt.