

White Paper
25.02.2026

Identifizierungsmethoden gem. Art. 24 Abs. 1a eIDAS

1. Einleitung

Die eIDAS 2.0 – umgangssprachlich wird hiermit die aktuell gültige Fassung der eIDAS-Verordnung 910/2014 bezeichnet – sieht in Art. 24 Abs. 1a vier mögliche Arten von Identifizierungen vor:

- Wallet oder notifiziertes elektronisches Identifizierungsmittel („notified electronic identification means“)
- qualifiziertes Zertifikat
- andere Identifizierungsmethode
- persönlich durch physische Anwesenheit

„Persönlich durch physische Anwesenheit“ und durch „qualifiziertes Zertifikat“ ist selbsterklärend. Die „Wallet“ als spezielles elektronisches Identifizierungsmittel wird derzeit noch spezifiziert. Die aktuell „notifizierten elektronischen Identifizierungsmittel“ sind bei der [eID User Community](#) gelistet

Im vorliegenden Dokument soll es um die „**anderen Identifizierungsmethoden**“ gehen, die lt. Art. 24 Abs. 1a eIDAS „**die Identifizierung der Person mit einem hohen Maß an Vertrauen gewährleisten [soll] und deren Konformität von einer Konformitätsbewertungsstelle bestätigt wird.**“

Unter diese „anderen Identifizierungsmethoden“ fallen damit u.a. die beliebten **Video-Identifizierungen**,

- über ein **Call-Center mit Interaktion** durch sog. Video-Agenten,
- **moderne automatisierte Ident-Prozesse** oder
- als **Misch-/Hybridform** (zunächst automatisiert mit manueller Nachkontrolle).

Wie und wonach werden diese „anderen Identifizierungsmethoden“ geprüft, um „ein hohes Maß an Vertrauen zu gewährleisten“, so dass eine Konformitätsbewertungsstelle dies bestätigen kann? Wie spielt der **ETSI-Standard 119 461** und die **Implementing Acts** (Durchführungsrechtsakte) **2015/1502** und **2025/1566** hier hinein? Dies beleuchtet das vorliegende Dokument.

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: „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.

2.2. ETSI-Standards

Die deutschen eIDAS-Konformitätsbewertungsstellen nutzen für die Evaluierung und Zertifizierung von Vertrauensdiensten verschiedene ETSI-Standards, u.a.

- ETSI 319 401: Grundlegende Anforderungen an Vertrauensdiensteanbieter
- ETSI 319 411-1: Anforderungen an Vertrauensdiensteanbieter, die Zertifikate ausstellen
- ETSI 319 411-2: Anforderungen an Vertrauensdiensteanbieter, die qualifizierte Zertifikate ausstellen
- ETSI 319 421: Anforderungen an Zeitstempeldienste
- ETSI 119 511: Anforderungen an Langzeitarchivierung

2.3. ETSI 119 461

Die ETSI 119 461 enthält Anforderungen an Trust Service-Komponenten zur Identitätsprüfung.

Exakte Referenz: ETSI TS 119 461, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects, V2.1.1 (2025-02).

Die ETSI 119 461 besteht ganz zentral aus den folgenden Teilen:

- Konkretisierungen der ETSI 319 401:
 - Risikomanagement
 - Policies
 - technisch-organisatorische Maßnahmen (Identity proofing service management and operation): Internal organization, Human resources, Asset management, Access control, Cryptographic controls, Physical and environmental security, Operation security, Network security, Vulnerabilities and incident management, Collection of evidence, Business continuity management, Termination and termination plans, Compliance, Supply chain
- Anforderungen an den Identifizierungsprozess (Identity proofing service requirements)
- Use Cases: Use cases for identity proofing to Baseline and Extended LoIP
- Annex C:
 - Annex C.2 verweist auf die „alte“ eIDAS, die nicht mehr gültig ist; C.2 ist also nicht mehr anwendbar

- Annex C.3 verweist auf Use Cases zur aktuell gültigen eIDAS; C.3 ist damit relevant

In der ETSI 119 461 werden bzgl. der Identifizierung natürlicher Personen die folgenden Identifizierungsmittel genannt:

- **physical identity document**: ein physikalisches Dokument, für Menschen lesbar, bspw. Personalausweis oder Reisepass
- **digital identity document**: ein digitales Dokument, für Maschinen lesbar, bspw. aus einem Chip im Personalausweis (nPA) oder Reisepass (ICAO-kompatibel)
- **eID means** (electronic Identification means (eID means, eID): “material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service” (Übersetzung: “materielle und/oder immaterielle Einheit, die Identifizierungsdaten enthält und zur Authentifizierung für einen Online-Dienst oder gegebenenfalls für einen Offline-Dienst verwendet wird”)
- **digital signature means with certificate**

Weitere wichtige Definition aus eIDAS-VO:

- **‘electronic identification scheme’** means a system for electronic identification under which **electronic identification means** are issued to natural or legal persons or natural persons representing other natural persons or legal persons)

Es gibt **notifizierte eID means** (notifizierte elektronische Identifizierungsmittel). Bei der **eID User Community** sind notifizierte Identifizierungssysteme (Scheme) mit ihren Identifizierungsmitteln (means) angegeben. Hier ist etwa gelistet:

- **Finnland**:
 - Scheme: Citizen Certificate
 - LoA: high
 - eID means under the scheme: ID card, notified
 - Status: notified
- **Dänemark**:
 - Scheme: MitID eID
 - LoA: substantial, high
 - eID means under the scheme: MitID Mobile App MitID App enhanced security MitID chip, MitID code display MitID Audio code reader, MitID Password; notified
 - Status: notified
- **Deutschland**:
 - Scheme: German eID based on Extended Access Control
 - LoA: high
 - eID means under the scheme: National Identity Card (nPA), Electronic Residence Permit (Aufenthaltstitel), eID Card for Union Citizens and EEA Nationals; notified

- Status: notified

Ferner werden in der ETSI 119 461 die folgenden Use Cases aufgeführt:

- using an identity document with **physical presence** of the applicant
- using an identity document for **attended** and **unattended remote** identity proofing
- identity proofing by authentication using **eID means**
- identity proofing using **digital signature** with certificate

Bzgl. der aktuell gültigen eIDAS werden in Annex C.3 die folgenden Use Cases aufgeführt, die sich direkt auf Art. 24 Abs. 1a eIDAS beziehen:

- physical presence of the applicant
- authentication using eID means
- certificate of qualified electronic signature or qualified electronic seal
- other identification means

Bzgl. der “other identification means” werden in Annex C.3.4 ganz konkrete Anforderungen – z.T. als Referenzierung auf andere Teile der 119 461 – aufgeführt, die relevant sind, wenn als Identifizierungsmethode eine „andere Methode“ herangezogen werden soll.

Die Anforderungen der ETSI 119 461 unterscheiden z.T. zwischen den LoIP Baseline und Extended, d.h. für Extended werden höhere Anforderungen gestellt, um einem höheren Angriffspotential standhalten zu können.

Wichtig: ETSI 119 461 ist zunächst „nur“ ein Standard. Rechtskraft erlangt dieser Standard erst über den Implementing Act 2025/1566.

2.4. Implementing Act 2025/1566

Die eIDAS-VO bezieht hinsichtlich der Identifizierung in Art. 24 Abs. 1c Konkretisierungen über einen Implementing Act ein – hier: 2025/1566.

Exakte Referenz: 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.

Implementing Act 2025/1566 benennt im Annex die Anforderungen:

- ETSI 119 461, hierüber wird insb. erstmals EU-weit die ETSI 319 401 als Grundlage eingezogen
- mit Konkretisierungen

Es sind insb. folgende Konkretisierungen festgelegt:

Aus dem Annex sind für die Ausgabe der qualifizierten Zertifikate nur die Anwendungsfälle C3.1 bis C3.6 zulässig, d.h.

- C.3.1 Use case for identity proofing by **physical presence** of the applicant
- C.3.2 Use case for identity proofing by authentication using **eID means**
- C.3.3 Use case for identity proofing by certificate of **qualified electronic signature** or qualified electronic seal
- C.3.4 Use case for identity proofing by **other identification means**
- C.3.5 Use case for identity proofing of **legal person**
- C.3.6 Use case for identity proofing of **natural person representing legal person**

Wenn eine Identitätsüberprüfung zur Ausstellung eines verbindlichen Nachweises („authoritative evidence“) erfolgen soll, gilt zusätzlich QTS-C3-01:

- QTS-C3-01: „Falls eine Identitätsüberprüfung für ein qualifiziertes Zertifikat oder eine qualifizierte elektronische Bescheinigung in Verbindung mit einer Identitätsüberprüfung zur Ausstellung eines verbindlichen Nachweises erfolgt, so muss dieser Identitätsüberprüfungsprozess
 - von einer akkreditierten Konformitätsbewertungsstelle einer gegenseitigen Begutachtung unterzogen oder zertifiziert worden sein, um die Anforderungen der Sicherheitsstufe „hoch“ gemäß der Verordnung (EU) Nr. 910/2014 zu erfüllen, oder
 - die Anforderungen der Abschnitte C3.1 bis C3.6 erfüllen.“
- „Ausstellung eines verbindlichen Nachweises“ ist im Englischen etwas besser formuliert: „to issue authoritative evidence“. Was ist ein „authoritative evidence“? Glücklicherweise wird „authoritative evidence“ in der ETSI 119 461 definiert und mit einer Note versehen, die hilfreich ist:
 - “authoritative evidence: evidence that is presented by the applicant, holds identifying attribute(s) of the identity, and is trusted for the binding of these attributes to the applicant
 - NOTE: In the present document, authoritative evidence for a natural person is a physical or digital identity document, an eID used for authentication, and a certificate of a digital signature. For a legal person, documents and attestations are typically used as authoritative evidence.”
- Bedeutet also: Wenn es um die Ausstellung eines verbindlichen Nachweises geht (authoritative evidence), muss dieser Identitätsüberprüfungsprozess hinreichend geprüft und zertifiziert worden sein, oder die Anforderungen aus C.3.1 bis C.3.6 müssen erfüllt worden sein.

Im Anwendungsfall „**Identitätsnachweis mit anderen Identifizierungsmitteln**“ aus C.3.4 gibt es zusätzliche Anforderungen, wenn ein Identifizierungsmittel mit eIDAS-Level **substantial durch weitere Prüfungen erweitert** werden soll.

Für alle “other ID means“-Varianten (attended remote, unattended remote, enhancing by other means) muss eine Konformitätsbewertungsstelle eingebunden sein:

QTS-C.3.4-08: The conformity of the identity proofing method with the requirements of this clause C.3.4 of the present document shall be confirmed by a conformity assessment body.

Der Implementing Act gibt ferner Vorgaben an die Tests (False Acceptance Rate und False Rejection Rate) bei autom. Systemen, vgl. 4.9.2.3.4 Anwendungsfall für den automatisierten Betrieb:

- USE-9.2.3.4-04: „Der Identitätsnachweisdiensteanbieter (IPSP) legt Zielwerte für die Falschakzeptanzrate (FAR) und die Falschrückweisungsrate (FRR) auf der Grundlage einer Risikoanalyse und seines Bedrohungsanalyseverfahrens fest und befolgt dabei in vollständig automatisierten Identitätsnachweisprozessen die im ENISA-Bericht „Methodology for sectoral cybersecurity assessments“ (Methodik für sektorale Cybersicherheitsbewertungen) [i.28] festgelegte Methodik oder eine gleichwertige Methodik. Diese Zielwerte dürfen die für Hybrid-Anwendungsfälle festgelegten Werte, sofern vorhanden, nicht übersteigen. Der IPSP hält diese Zielwerte für die FAR und die FRR konsequent aufrecht und stützt sich dabei auf eine Risikoanalyse und sein Bedrohungsanalyseverfahren.“

Ferner wird zur Validierung von physischen Identitätsdokumenten auf entsprechende Labore verwiesen, vgl. 5.8.3.3 Validierung eines physischen Identitätsdokuments:

- VAL-8.3.3-21: „Die Wirksamkeit der Maßnahmen zur Erfüllung der Anforderungen VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A und VAL-8.3.3-07X wird von einem akkreditierten Laboratorium oder einer zuständigen nationalen Behörde, sofern eine solche benannt worden ist, spätestens bis zum 19. August 2027 und danach alle zwei Jahre getestet.“
- Aktueller Stand: Es ist unklar, nach welcher Norm diese Labore akkreditiert oder zugelassen werden sollen.

Und zuletzt konkretisiert der Implementing Act das Thema Termination, vgl. 6.7.12 Beendigung und Beendigungspläne:

- OVR-7.12-02: „Der Beendigungsplan muss den Anforderungen entsprechen, die in den gemäß Artikel 24 Absatz 5 der Verordnung (EU) Nr. 910/2014 [i.1] erlassenen Durchführungsrechtsakten festgelegt sind.“

Es ist festgelegt: „Diese Verordnung gilt ab dem 19. August 2027.“

2.5. Implementing Act 2015/1502

In der eIDAS werden für elektronische Identifizierungsmittel die Vertrauenswürdigkeitsstufen (Assurance Level) Substantial und High definiert. Was genau die Unterscheidung angeht, dazu dient der Implementing Act 2015/1502.

Der Implementing Act 2015/1502 dient dazu, elektronische Identifizierungsmittel bzgl. der Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ zu klassifizieren.

Der Implementing Act 2015/1502 ist granular aufgebaut:

- Anmeldung
 - Beantragung und Eintragung
 - Identitätsnachweis und -überprüfung (natürliche Person)
 - Identitätsnachweis und -überprüfung (juristische Person)
 - Verknüpfung von elektronischen Identifizierungsmitteln natürlicher und juristischer Personen

- Verwaltung elektronischer Identifizierungsmittel
 - Merkmale und Gestaltung elektronischer Identifizierungsmittel
 - Ausstellung, Auslieferung und Aktivierung
 - Aussetzung, Widerruf und Reaktivierung
 - Verlängerung und Ersetzung
- Authentifizierung
 - Authentifizierungsmechanismus
- Management und Organisation
 - Allgemeine Bestimmungen
 - Veröffentlichte Bekanntmachungen und Benutzerinformationen
 - Informationssicherheitsmanagement
 - Aufbewahrungspflichten
 - Einrichtungen und Personal
 - Technische Kontrollen
 - Einhaltung und Prüfung

Wichtig:

- Der Schritt „Anmeldung“ ist die initiale Identifizierung mit einem „anderen“ – authoritative evidence, etwa nPA, Reisepass, der also bereits hinreichend zugelassen ist.
- Im Schritt „Verwaltung elektronischer Identifizierungsmittel“ wird dann das „neue“ Identifizierungsmittel „erschaffen“ und ausgegeben und über Life-Cycle verwaltet.
- Die Nutzung dieses „neu“ erschaffenen Identifizierungsmittel erfolgt dann im Schritt „Authentifizierung“.

Welches Niveau kann ein neu erschaffenes Identifizierungsmittel erreichen? Ganz entscheidend unter Abs 2.2.1. „Merkmale und Gestaltung elektronischer Identifizierungsmittel“:

- substantiell:
 - mindestens zwei Authentifizierungsfaktoren unterschiedlicher Kategorien
 - alleinige Kontrolle
- hoch:
 - Anforderungen an substantiell
 - Schutz vor Duplizierung
 - Schutz vor Fälschung
 - alleinige Kontrolle
 - Resistent gegen hohes Angriffspotential

Ferner entscheidend ist die Authentisierung, d.h. die Nutzung des neu erschaffenen Identifizierungsmittels. Abs. 2.3.1. Authentifizierungsmechanismus fordert:

- **substanziell:**
 - zuverlässige Überprüfung
 - Gültigkeitsprüfung
 - dynamische Authentisierung
 - resistent gegen mäßiges Angriffspotenzial „durch Handlungen wie Erraten, Abhören, Replay oder Manipulation“
- **hoch:**
 - Anforderungen an substanziell
 - resistent gegen hohes Angriffspotenzial „durch Handlungen wie Erraten, Abhören, Replay oder Manipulation“

Einschätzung: Hohes Angriffspotenzial ist eine sehr hohe Hürde.

Wichtig: Der Implementing Act 1502 greift die „Sicherheitsniveaus“ niedrig, substanziell und hoch tatsächlich im Sinne von „mehr“ Sicherheit auf. Wie tief diese „Sicherheit“ geprüft wird – also im Sinne von Assurance –, darauf geht 1502 nicht ein. Es wird zwar gesagt, dass akkreditierte Konformitätsbewertungsstellen für die Einordnung zuständig seien, es gibt aber keinen Hinweis auf die Prüftiefe.

Gleichwohl wird unter 2.3.1. Authentifizierungsmechanismus von einem Angriffspotenzial (attack potential) gesprochen:

- bei niedrig: „Angreifer mit erhöhtem grundlegenden Angriffspotenzial“
- bei substanziell: „Angreifer mit mäßigem Angriffspotenzial“
- bei hoch: „Angreifer mit hohem Angriffspotenzial“

Frage: Wie ist ein Angreifer mit grundlegendem, mäßigem oder hohem Angriffspotenzial aufzufassen? Gegen welche Angriffe muss ein Identifizierungsmittel und -system geschützt werden? Vor allem im Hinblick auf eine harmonisierte Anwendung?

Dazu bietet die ETSI 119 461 eine Definition in Abs. 3.1:

attack potential: measure of the effort needed to exploit a vulnerability in a Target Of Evaluation (TOE)

NOTE: Source ISO/IEC 15408-1 [i.24], which has the following note to the definition: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

Meinung der datenschutz cert GmbH: Die Common Evaluation Methodology (CEM) bietet einen guten Ansatz, um Angriffspotenzial qualifiziert unter verschiedenen Gesichtspunkten einheitlich und objektiv zu bewerten – und vergleichbar zu machen.

2.6. BNetzA-Verfügungen

Es gab früher zwei Verfügungen der BNetzA zum Thema Video-Identifizierung und autom. Identifizierung; beides zur Ausstellung eines ad-hoc-Zertifikates.

Im Zuge der europäischen Harmonisierung soll diese nationale Regelung durch den Implementing Act 2025/1566 ersetzt werden.

3. Einsatz im qualifizierten Kontext

Zur Ausstellung eines qualifizierten Zertifikates sind lt. Art. 24 (1a) eIDAS die folgenden Identifizierungsmöglichkeiten zulässig:

- a) Wallet oder notifiziertes elektronisches Identifizierungsmittel mit LoA „high“
- b) qualifiziertes Zertifikat
- c) andere Identifizierungsmethode
- d) persönlich durch physische Anwesenheit

Über den Implementing Act 2025/1566 wird die ETSI 119 461 herangezogen, insbesondere die Use Cases in C.3.

3.1. C.3-Use Cases

Für die Ausstellung eines qualifizierten Zertifikates sind nur die Use Cases aus C.3 zulässig: „C.3 Use cases for issuing of qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, and 24.1b of the amended eIDAS regulation“. Danach sind die folgenden sechs Möglichkeiten zulässig:

- C.3.1 Use case for identity proofing by **physical presence** of the applicant
- C.3.2 Use case for identity proofing by authentication using **eID means**
- C.3.3 Use case for identity proofing by certificate of **qualified electronic signature** or qualified electronic seal
- C.3.4 Use case for identity proofing by **other identification means**
- C.3.5 Use case for identity proofing of **legal person**
- C.3.6 Use case for identity proofing of **natural person representing legal person**

Von besonderer Bedeutung ist Use Case C.3.4:

C.3.4 Use case for identity proofing by other identification means

[CONDITIONAL] If identity proofing is done for the **purpose of issuing qualified certificate** or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.25], and identity proofing is done by other identification means according to letter c of Article 24.1a and/or letter d of Article 24.1b, the following requirements apply.

3.2. C.3.4-Use Cases

C.3.4 enthält acht Anforderungen, die verschiedene Szenarien abdecken; zentral finden sich zwei Varianten:

- begleitete Remote-Identifizierung (attended remote identity proofing)
- unbegleitete Remote-Identifizierung (unattended remote identity proofing)

3.2.1. Begleitete Remote-Identifizierung (attended remote identity proofing)

Bei attended remote identity proofing werden zwei Anforderungen gestellt, die im Wesentlichen auf Anforderungen für Extended LoIP aus 119 461 verweisen: 9.2.2.1 und 9.2.2.3.

[CONDITIONAL] QTS-C.3.4-01: If **attended remote identity proofing** using physical or digital identity document as authoritative evidence is used, the requirements for **Extended LoIP of clause 9.2.2.1** of the present document shall apply.

[CONDITIONAL] QTS-C.3.4-02: If **attended remote identity proofing** using physical or digital identity document as authoritative evidence is used, the requirements for **Extended LoIP of clause 9.2.2.3** of the present document shall apply.

NOTE 1: Manual operation as described in clause 9.2.2.2 is not considered to support Extended LoIP and hence not issuing of qualified certificates or qualified electronic attestations of attributes according to the amended eIDAS regulation [i.25].

Die Anforderungen der ETSI 119 461 unterscheiden z.T. zwischen den LoIP Baseline und Extended, für den Einsatz im qualifizierten Kontext greifen nur die Extended LoIP-Requirements, um einem höheren Angriffspotential standhalten zu können.

3.2.2. Unbegleitete Remote-Identifizierung (unattended remote identity proofing)

Bei unattended remote identity proofing werden zwei Anforderungen gestellt, die im Wesentlichen auf Anforderungen für Extended LoIP aus 119 461 verweisen: 9.2.3.1 und 9.2.3.3 bzw. 9.2.3.4.

[CONDITIONAL] QTS-C.3.4-03: If **unattended remote identity proofing** using physical or digital identity document as authoritative evidence is used, the requirements for **Extended LoIP of clause 9.2.3.1** of the present document shall apply.

[CONDITIONAL] QTS-C.3.4-04: If **unattended remote identity proofing** using physical or digital identity document as authoritative evidence is used, the requirements for **Extended LoIP of either clause 9.2.3.3 or clause 9.2.3.4** of the present document shall apply.

NOTE 2: Manual operation as described in clause 9.2.3.2 is not considered to support Extended LoIP and hence not issuing of qualified certificates or qualified electronic attestations of attributes according to the amended eIDAS regulation [i.25].

Die Anforderungen der ETSI 119 461 unterscheiden z.T. zwischen den LoIP Baseline und Extended, für den Einsatz im qualifizierten Kontext greifen nur die Extended LoIP-Requirements, um einem höheren Angriffspotential standhalten zu können.

4. Fazit

Wenn ein TSP zur Ausstellung eines qualifizierten Zertifikates eine Identifizierung vornehmen will, gelten die Identifizierungsmöglichkeiten aus Art. 24 Abs. 1a eIDAS:

- Wallet oder notifiziertes elektronisches Identifizierungsmittel mit LoA „high“
- qualifiziertes Zertifikat
- andere Identifizierungsmethode
- persönlich durch physische Anwesenheit

Über den Implementing Act 2025/1566 mit der ETSI 119 461 werden die eIDAS-Vorgaben konkretisiert.

Auch wenn die Regelungen formal erst „ab dem 19. August 2027“ gelten, ist doch damit zu rechnen, dass insbesondere ETSI 119 461 schon vorher zur Anwendung kommen wird.