

White Paper
25.02.2026

LoIP und LoA im eIDAS-Kontext

1. Einleitung

Im Kontext von eIDAS werden häufig die folgenden Begriffe genutzt:

- Baseline
- extended
- substantial
- high
- Level of Identity Proofing (LoIP)
- Level of assurance (LoA)/assurance level

Was ist denn das genau? Und warum ist das so wichtig?

Das vorliegende Dokument soll diese Begriffe erläutern, einordnen und abgrenzen.

2. Assurance Level (LoA)

Zunächst ist sicherlich ein Blick ins Gesetz sinnvoll. In der eIDAS

[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

werden die folgenden Begriffe definiert:

- assurance level high = Sicherheitsniveau hoch
- assurance level substantial = Sicherheitsniveau substanziell
- assurance level low = Sicherheitsniveau niedrig

Anmerkung: Leider ist Assurance Level – eigentlich Vertrauenswürdigkeitsniveau – mit Sicherheitsniveau übersetzt worden, was etwas unglücklich ist, weil ein Assurance Level eigentlich nur besagt, wie tief geprüft wurde, nicht welche Sicherheitsmechanismen etabliert sind. Überspitzt gesagt: Ein nur rudimentärer Sicherheitsmechanismus kann sehr tiefgehend – also mit einem hohen Assurance Level – untersucht werden, ein sehr guter Sicherheitsmechanismus hingegen auch nur sehr oberflächlich (mit einem niedrigen Assurance Level). Sicherheitsniveau hat eigentlich nichts mit Vertrauenswürdigkeitslevel zu tun. Aber: Das Gesetz setzt dies gleich. Und noch eine gesetzliche Unschärfe: In der eIDAS wird „Sicherheitsniveau“ auch synonym mit „Sicherheitsstufe“ bezeichnet.

Der exakte Wortlaut:

Artikel 8

Sicherheitsniveaus elektronischer Identifizierungssysteme

(1) Ein gemäß Artikel 9 Absatz 1 notifiziertes **elektronisches Identifizierungssystem** gibt die **Sicherheitsniveaus „niedrig“, „substanziell“** und/oder **„hoch“** an, die den nach diesem System ausgestellten **elektronischen Identifizierungsmitteln** zuerkannt wurden.

(2) Die Sicherheitsniveaus „niedrig“, „substanziell“ bzw. „hoch“ erfüllen folgende Kriterien:

a) Das **Sicherheitsniveau „niedrig“** bezieht sich auf ein **elektronisches Identifizierungsmittel** im Rahmen eines **elektronischen Identifizierungssystems**, das ein **begrenzttes Maß an Vertrauen** in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen — deren Zweck in der Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

b) Das **Sicherheitsniveau „substanziell“** bezieht sich auf ein **elektronisches Identifizierungsmittel** im Rahmen eines **elektronischen Identifizierungssystems**, das ein **substanzielles Maß an Vertrauen** in die beanspruchte oder behauptete Identität einer Person vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich entsprechender technischer Überprüfungen — deren Zweck in der substanziellen Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

c) Das **Sicherheitsniveau „hoch“** bezieht sich auf ein **elektronisches Identifizierungsmittel** im Rahmen eines **elektronischen Identifizierungssystems**, das ein **höheres Maß an Vertrauen** in die beanspruchte oder behauptete Identität einer Person als ein Identifizierungsmittel mit dem Sicherheitsniveau „substanziell“ vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Überprüfungen — deren Zweck in der Verhinderung des Identitätsmissbrauchs oder der Identitätsveränderung besteht — gekennzeichnet ist.

(3) Bis zum **18. September 2015** legt die Kommission unter Berücksichtigung der einschlägigen internationalen Normen vorbehaltlich des Absatzes 2 im Wege von **Durchführungsrechtsakten** technische Spezifikationen, Standards und Verfahren mit Mindestanforderungen fest, auf die sich die Festlegung der Sicherheitsniveaus niedrig, „substanziell“ und „hoch“ für **elektronische Identifizierungsmittel** bezieht.

Ganz wichtig: Wofür gelten denn nun diese Assurance Level (= Sicherheitsniveaus = Sicherheitsstufen)? Lt. eIDAS für **elektronische Identifizierungssysteme** und **elektronische Identifizierungsmittel**. Was ist das? Lt. Definition in Art. 3 eIDAS:

2. „**Elektronisches Identifizierungsmittel**“ ist eine materielle und/ oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten oder gegebenenfalls bei Offline-Diensten verwendet wird.

4. „**Elektronisches Identifizierungssystem**“ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die andere natürliche Personen oder juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden.

Im Original:

2. ‘**electronic identification means**’ means a 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;

4. ‘**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

Beispiele: Unter <https://ec.europa.eu/digital-building-blocks/sites/spaces/EIDCOMMUNITY/pages/48762251/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS> 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

Wichtig: Die Klassifizierung des Identifizierungsmittels (means) ist entscheidend für die Klassifizierung des ganzen Identifizierungssystems (Scheme). Zur Klassifizierung dieser Mittel macht Art. 8 (3) eIDAS nähere Vorgaben.

Der in Art. 8 (3) eIDAS versprochene Implementing Act (Durchführungsrechtsakt) liegt bereits vor:

[ImplAct_1502] 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

Dieser 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:

- 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 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:

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

Einschätzung: Hohes Angriffspotential ist eine sehr hohe Hürde.

Wichtig: Der Implementing Act 1502 greift die „Sicherheitsniveaus“ niedrig, substantiell 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 Angriffspotential (attack potential) gesprochen:

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

Frage: Wie ist ein Angreifer mit grundlegendem, mäßigem oder hohem Angriffspotential 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).

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

3. Level of Identity Proofing (LoIP)

Der Level of Identity Proofing (LoIP) ist nicht in der eIDAS definiert, aber in der ETSI-Norm 119 461:

[119 461] 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).

ETSI 119 461 definiert LoIP wie folgt:

- Level of Identity Proofing (LoIP): confidence achieved in the identity proofing

Es geht also um die Vertrauenswürdigkeit in den Prozess einer Identitätsüberprüfung.

ETSI 119 461 sieht zwei Arten:

- Baseline LoIP
- Extended LoIP

Baseline LoIP: Level of Identity Proofing (LoIP) reaching a **substantial level of confidence** based on the fulfilment of good practice minimum requirements for the identity proofing process

NOTE: This level is considered suitable for identity proofing for the NCP policy level defined in ETSI EN 319 411-1 [i.7] and for issuing qualified certificates according to the original eIDAS regulation [i.1].

Extended LoIP: Level of Identity Proofing (LoIP) reaching a **high level of confidence** based on the fulfilment of good practice minimum requirements for the identity proofing process

NOTE: This level is considered suitable for identity proofing for issuing of **qualified certificates** and qualified electronic attestations of attributes according to the **amended eIDAS regulation** [i.25].

Und hier sehen wir die Verschränkung – womöglich auch die Verwirrung:

- **Baseline** LoIP = **substantial** level of confidence
- **Extended** LoIP) = **high** level of confidence

Frage: Ist substantial/high level of confidence gleich zu assurance level substantial/high? Nein, ist eher “umgangssprachlich” gemeint. Außerdem gilt LoA nur für Identifizierungsmittel/-systeme, während hier ein Prozess zur Identitätsfeststellung (Identity Proofing) gemeint ist.

Ganz wichtig im Kontext qualifizierter Zertifikate: Baseline LoIP ist nicht für qualifizierte Zertifikat nach der aktuellen eIDAS geeignet, sondern nur für nicht-qualifizierte (oder die „alte“/originale eIDAS-VO). Das ist also ein neuer Sachverhalt.

4. Relevanz von LoA und LoIP

Die Assurance Level (LoA) und Level of Identity Proofing (LoIP) tauchen an verschiedenen Stellen im Kontext der eIDAS auf, beispielsweise:

- eIDAS: elektronische Identifizierungsmittel – auch im Rahmen eines elektronischen Identifizierungssystems; z.T. notifiziert
- Implementing Act 1502: definiert die LoA (Assurance Level = Sicherheitsniveau = Sicherheitsstufen) und grenzt sie voneinander ab
- Implementing Act 1566 definiert „Referenzstandards für die Überprüfung der Identität und der Attribute der Person“, hier wird insbesondere auf die ETSI 119 461 verwiesen und diese in Teilen konkretisiert.
 - So wird in Implementing Act 1566 beispielweise gefordert, dass ein identity verification process (Identitätsüberprüfungsprozess) unter gewissen Voraussetzungen als eine Alternative von einer Konformitätsbewertungsstelle gem. Sicherheitsstufe „hoch“ überprüft worden sein muss.
Das muss erläutert werden, denn – wie wir oben gelernt haben – sind Sicherheitsstufen (= Sicherheitsniveaus = Assurance Level) für elektronische Identifizierungsmittel und -systeme definiert. Wie ist ein Identitätsüberprüfungsprozess hier einzuordnen? Meinung dsc: Als Teil eines elektronischen Identifizierungssystems.
- ETSI 119 461
 - Die 119 461 definiert (nochmal) alle Begriffe:

- **Baseline LoIP:** Level of Identity Proofing (LoIP) reaching a **substantial** level of confidence based on the fulfilment of good practice minimum requirements for the identity proofing process
- **Extended LoIP:** Level of Identity Proofing (LoIP) reaching a **high** level of confidence based on the fulfilment of good practice minimum requirements for the identity proofing process
- **eIDAS LoA high = eIDAS high eID:** eID or eID scheme fulfilling the requirements for assurance level **high** in Article 8 of the amended eIDAS regulation and CIR (EU) 2015/1502
- **eIDAS LoA substantial = eIDAS substantial eID:** eID or eID scheme fulfilling the requirements for assurance level **substantial** in Article 8 of the amended eIDAS regulation and CIR (EU) 2015/1502
- Im Annex C.3 werden verschiedene Methoden der Identifizierung genannt; hier werden die o.g. Begriffe in den konkreten Anforderungen benannt – insbesondere zur Erstellung eines qualifizierten Zertifikates.
Dazu sollten die Trust Service Provider zunächst die für sie konkreten Anforderungsfälle (Use Cases) festlegen und die konkrete Umsetzung der Anforderungen darlegen.
- 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.

5. Fazit

Assurance Level (LoA):

- gilt für Identifizierungsmittel und -systeme
- gibt es in den Stufen normal, substanziell und hoch
- wird näher definiert im Implementing Act 1502

Level of Identity Proofing (LoIP):

- gilt für den Prozess der Identitätsüberprüfung
- gibt es in den Stufen baseline und extended
- qualifizierte Zertifikate erfordern ein extended LoIP