

# Legal Issues in Computer Security 2023 eIDAS Regulation

Mirosław Kutylowski

**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**

- **electronic identification**
- **electronic signatures and seals**
- **webservices**
- **... and generally „trust services“ (as understood by eIDAS)**

# Scope

1. **electronic identification schemes notified** by a Member State,  
**trust service providers** that are **established in the Union**.
2. **does not apply to** ... trust services used exclusively within **closed systems** resulting from  
national law  
or from **agreements between a defined set of participants**.
3. **does not affect national or Union law** related to the conclusion and validity of contracts or other legal or procedural **obligations relating to form**.

# `electronic identification`

means the process of **using person identification data** in electronic form **uniquely representing** either a natural or legal person, or a natural person representing a legal person;

# **‘electronic identification means’**

means a **material and/or immaterial unit** containing person identification data and which is **used for authentication for an online service**;

# 'person identification data'

means a set of **data enabling the identity** of a natural or legal person,  
or a natural person representing a legal person **to be established**;

# `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 legal persons**;

# 'authentication'

means an electronic process that **enables the electronic identification** of a natural or legal person, **or the origin and integrity of data in electronic form to be confirmed;**



# **'electronic signature'**

**means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;**

# **advanced electronic signature'**

**means an electronic signature which meets the requirements set out in Article 26;**

# Art. 26

An advanced electronic signature shall meet the following requirements:

- (a) it is **uniquely linked to the signatory**;
- (b) it is **capable of identifying the signatory**;
- (c) it is created using electronic **signature creation data that the signatory can, with a high level of confidence, use under his sole control**; and
- (d) it is linked to the data signed therewith in such a way that any **subsequent change in the data is detectable**.

# **‘qualified electronic signature’**

means an advanced electronic signature that is **created by a qualified electronic signature creation device**, and which is **based on a qualified certificate** for electronic signatures;

## REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by **appropriate technical and procedural means**, that at least:
  - (a) the **confidentiality of the electronic signature creation data** used for electronic signature creation is **reasonably assured**;
  - (b) the electronic **signature creation data** used for electronic signature creation **can practically occur only once**;

(c) the electronic signature creation data used for electronic signature creation **cannot, with reasonable assurance, be derived** and the **electronic signature is reliably protected against forgery** using **currently available technology**;

(d) the **electronic signature creation data** used for electronic signature creation can be **reliably protected by the legitimate signatory against use by others.**

2. Qualified electronic signature creation devices **shall not alter the data to be signed** or **prevent such data from being presented** to the signatory prior to signing.

3. **Generating or managing** electronic signature creation data on behalf of the signatory **may only be done by a qualified trust service provider.**

Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory **may duplicate the electronic signature creation data only for back-up purposes** provided the following requirements are met:

- (a) the **security of the duplicated datasets** must be at the same level as for the original datasets;
- (b) the **number of duplicated datasets shall not exceed the minimum needed to ensure continuity** of the service.



## **‘certificate for electronic signature’**

means an electronic attestation which **links electronic signature validation data to a natural person** and **confirms** at least the **name** or **the pseudonym** of that person;

## **‘qualified certificate for electronic signature’**

means a certificate for electronic signatures, that is **issued by a qualified trust service provider** and meets the requirements laid down in Annex I;

## **‘electronic seal’**

means data in electronic form, which is attached to or logically associated with other data in electronic form **to ensure the latter’s origin and integrity;**

## **‘advanced electronic seal’**

means an electronic seal, which **meets the requirements set out in Article 36;**

**-- *mutatis mutandis as for advanced electronic signatures***

## **‘qualified electronic seal’**

means an advanced electronic seal, which is created by a **qualified electronic seal creation device**, and that is based on a **qualified certificate** for electronic seal;

## **‘electronic seal creation data’**

means unique data, which is used by the creator of the electronic seal to create an electronic seal;

## **‘electronic seal creation device’**

means configured software or hardware used to create an electronic seal;

## **‘qualified electronic seal creation device’**

means an electronic seal creation device that meets mutatis mutandis the requirements laid down in **Annex II**;

## **‘electronic time stamp’**

means data in electronic form which **binds other data in electronic form to a particular time** establishing **evidence that the latter data existed at that time;**

## **‘qualified electronic time stamp’**

means an electronic time stamp which meets the requirements laid down in Article 42;

# Art. 42

1. A **qualified electronic time stamp** shall meet the following requirements:

(a) it binds the date and time to data in such a manner as **to reasonably preclude the possibility of the data being changed undetectably**;

(b) it is **based on an accurate time source** linked to **Coordinated Universal Time**;  
and

(c) it is **signed** using an **advanced electronic signature** or **sealed** with an **advanced electronic seal** of the **qualified trust service provider**, or by some **equivalent method**.

## **‘validation data’**

**means data that is used to validate an electronic signature or an electronic seal;**

## **‘validation’**

**means the process of verifying and confirming that an electronic signature or a seal is valid.**

## **'electronic document'**

**means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;**



## **‘electronic registered delivery service’**

means a service that makes it possible to transmit data between third parties by electronic means and **provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data**, and that **protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;**

## **‘qualified electronic registered delivery service’**

means an electronic registered delivery service which meets the requirements laid down in Article 44;

**Art 44 1. Qualified electronic registered delivery services shall meet the following requirements:**

- (a) they are provided by one or more qualified trust service provider(s);**
- (b) they ensure with a high level of confidence the identification of the sender;**
- (c) they ensure the identification of the addressee before the delivery of the data;**

## **Art 44 1. Qualified electronic registered delivery services shall meet the following requirements:**

**(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;**

**(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;**

**(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.**

## **‘certificate for website authentication’**

means an attestation that **makes it possible to authenticate a website** and **links the website to the natural or legal person to whom the certificate is issued;**

## **‘qualified certificate for website authentication’**

means a certificate for website authentication, which is issued by a **qualified trust service provider** and meets the requirements laid down in **Annex IV;**

# Electronic identification ecosystem

**Goal:** enable citizens from country A to use electronic identification in country B

**Concept:** „roaming” like telecommunication services

## Mutual recognition

1. When an **electronic identification using an electronic identification means and authentication** is required under national law or by administrative practice to **access a service provided by a public sector body online** in one Member State,

**the electronic identification means issued in another Member State shall be recognised** in the first Member State for the purposes of cross-border authentication for that service online, **provided that the following conditions are met:**

a) the **electronic identification means** is issued under an electronic identification scheme that is **included in the list** published by the Commission pursuant to Article 9;

(b) the **assurance level** of the electronic identification means **corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State,** provided that the assurance level of that electronic identification means corresponds to the assurance level **substantial or high**;

Levels: low, substantial, high ... or no level can be assigned



2. An electronic identification means **which is issued under an electronic identification scheme included in the list** published by the Commission pursuant to Article 9 and **which corresponds to the assurance level low** **may be recognised** by public sector bodies for the purposes of cross-border authentication for the service provided online by those bodies.

## **Eligibility for notification of electronic identification schemes**

**An electronic identification scheme shall be eligible for notification ... provided that ...:**

**(a) the electronic identification means under the electronic identification scheme **are issued:****

**(i) **by the notifying Member State;****

**(ii) under a mandate from the notifying Member State; or**

**(iii) independently of the notifying Member State and are recognised by that Member State;**

b) the electronic identification means under the electronic identification scheme **can be used to access at least one service which is provided by a public sector body** and **which requires electronic identification in the notifying** Member State;

(c) the electronic identification scheme and the electronic identification means issued thereunder **meet the requirements of at least one of the assurance levels** set out in the implementing act referred to in Article 8(3);

(d) the notifying Member State ensures that the **person identification data uniquely representing the person in question is attributed**, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the **implementing act** referred to in Article 8(3), to the **natural or legal person** referred to in point 1 of Article 3 **at the time the electronic identification means under that scheme is issued**;

(e) the party issuing the electronic identification means under that scheme **ensures that the electronic identification means is attributed to the person** referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);

(f) the notifying Member State **ensures the availability of authentication online,** so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

**Member States shall not impose any specific disproportionate technical requirements**

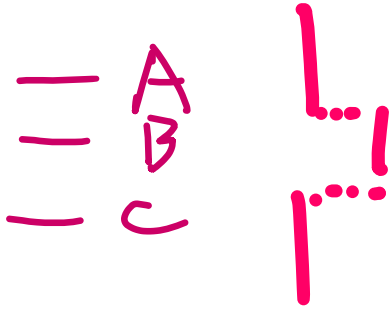
**on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability**

**of the notified electronic identification schemes;**

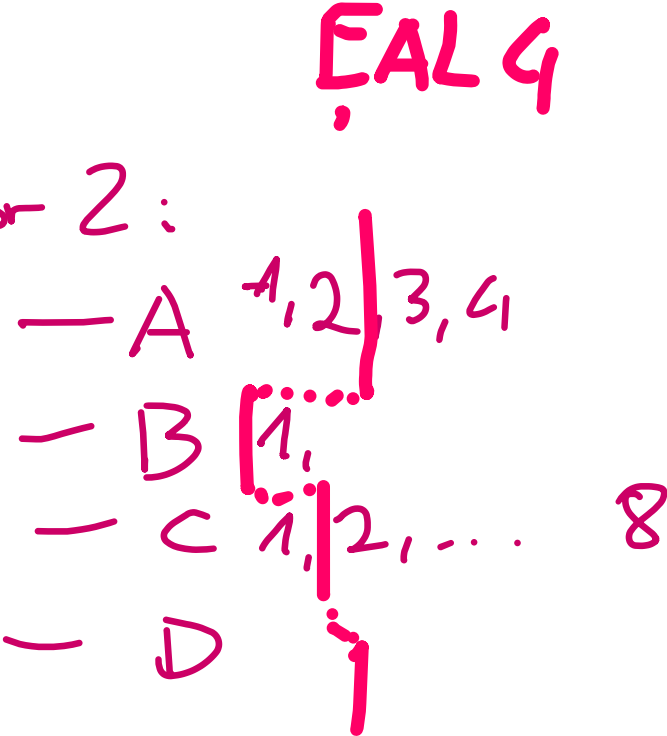
# Assurance levels

Idea: like EAL of Common Criteria

factor 1:



factor 2:



**(a) assurance level low**

shall refer to an electronic identification means in the context of an electronic identification scheme,

which provides a **limited degree of confidence** in the claimed or asserted identity of a person,

and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls,

the purpose of which is to **decrease** the risk of misuse or alteration of the identity;



**(b) assurance level substantial**

shall refer to an electronic identification means in the context of an electronic identification scheme,

which provides a **substantial degree of confidence** in the claimed or **asserted identity of a person**, and is

characterised with reference to technical specifications, standards and procedures related thereto, including technical controls,

the purpose of which is to **decrease substantially** the risk of misuse or **alteration of the identity**;

**(c) assurance level high**

shall refer to an electronic identification means in the context of an electronic identification scheme,

which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic

identification means with the assurance level substantial,

and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls,

the purpose of which is to prevent misuse or alteration of the identity.

# Notified schemes:

<https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS>

## Practice...

# Applying for notification

- (a) a **description** of the electronic identification scheme, including its **assurance levels** and the **issuer** or issuers of electronic identification means under the scheme;
  
- (b) the **applicable supervisory regime** and information on the **liability regime** with respect to the following:
  - (i) the party issuing the electronic identification means; and
  - (ii) the party operating the authentication procedure;
  
- (c) the authority or **authorities responsible** for the electronic identification scheme;

# Applying for notification

(d) information on the entity **or entities which manage the registration of the unique person identification data;**

(e) a **description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;**

(f) a description of the authentication referred to in point (f) of Article 7;

(g) **arrangements for suspension or revocation** of either the notified electronic identification scheme or authentication or **the compromised parts concerned.**

## **Implementing Act – example: 1502**

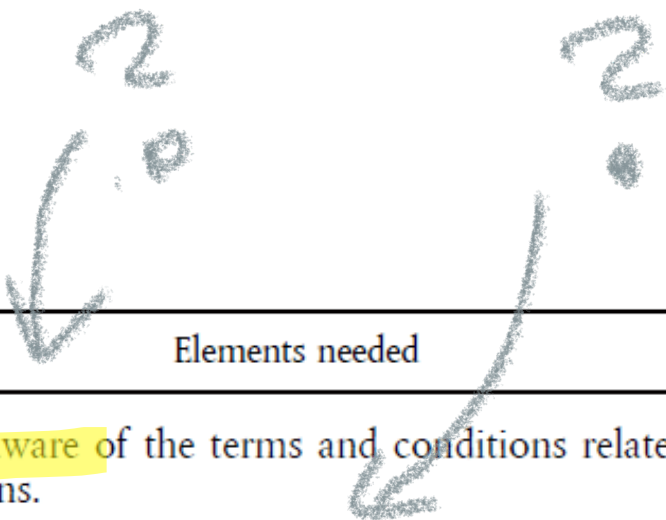
**minimum technical specifications and procedures for assurance levels for electronic identification**

### **List of requirements in different categories**

- **like Common Criteria EAL**
- **Verifiable?**

# Implementing Act – example: 1502

## 2.1.1. Application and registration

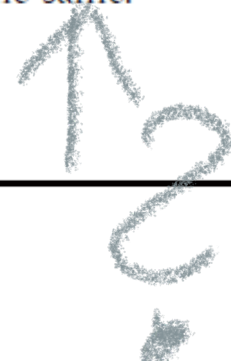


Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="805 532 2346 615">1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.</li><li data-bbox="805 651 2346 733">2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.</li><li data-bbox="805 769 2346 852">3. Collect the relevant identity data required for identity proofing and verification.</li></ol>
Substantial	Same as level low.
High	Same as level low.

# Implementing Act – example: 1502

## 2.1.2. Identity proofing and verification (natural person)

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="741 572 2262 704">1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.</li><li data-bbox="741 732 2262 825">2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.</li><li data-bbox="741 853 2262 939">3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.</li></ol>





## Implementing Act – example: 1502

Substantial

Level low, plus one of the alternatives listed in points 1 to 4 has to be met:

1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity

and

the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person

and

steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;

or

## Implementing Act – example: 1502

2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it

and

steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;

or

3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council <sup>(1)</sup> or by an equivalent body;

## Implementing Act – example: 1502

4. Where **electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high**, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.

# Implementing Act – example: 1502

High

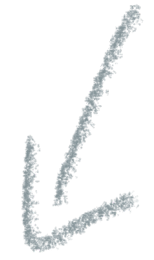
Requirements of either point 1 or 2 have to be met:

1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met:

(a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;

and

the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;



## Implementing Act – example: 1502

or

- (b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body

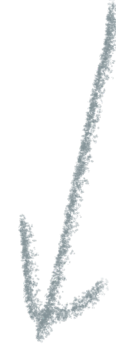
and

steps are taken to demonstrate that the results of the earlier procedures remain valid;

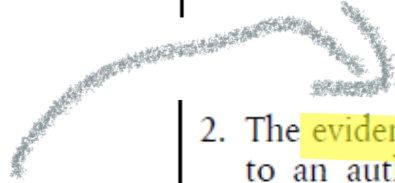
or

# Implementing Act – example: 1502

## 2.1.3. Identity proofing and verification (legal person)



Assurance level	Elements Needed
Low	<ol style="list-style-type: none"><li data-bbox="700 551 2005 665">1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made.</li><li data-bbox="700 836 2079 993">2. The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source, where the inclusion of a legal person in the authoritative source is voluntary and is regulated by an arrangement between the legal person and the authoritative source.</li><li data-bbox="700 1022 2079 1108">3. The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.</li></ol>



## Implementing Act – example: 1502

Substantial

Level low, plus one of the alternatives listed in points 1 to 3 has to be met:

1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable) its registration number

and

the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source, where the inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector

and

steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;

or



## Implementing Act – example: 1502

High

Level substantial, plus one of the alternatives listed in points 1 to 3 has to be met:

1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context

and

the evidence is checked to determine that it is valid according to an authoritative source;

or

**12.5.23**



## Implementing Act – example: 1502

### 2.1.4. Binding between the electronic identification means of natural and legal persons

Where applicable, for binding between the electronic identification means of a natural person and the electronic identification means of a legal person ('binding') the following conditions apply:

- (1) It shall be possible to suspend and/or revoke a binding. The life-cycle of a binding (e.g. activation, suspension, renewal, revocation) shall be administered according to nationally recognised procedures.
- (2) The natural person whose electronic identification means is bound to the electronic identification means of the legal person may delegate the exercise of the binding to another natural person on the basis of nationally recognised procedures. However, the delegating natural person shall remain accountable.

## Implementing Act – example: 1502

Assurance level	Elements Needed
Low	<ol style="list-style-type: none"><li data-bbox="644 454 2074 544">1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above.</li><li data-bbox="644 568 2074 615">2. The binding has been established on the basis of nationally recognised procedures.</li><li data-bbox="644 639 2074 729">3. The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.</li></ol>

## Implementing Act – example: 1502

High

Point 3 of level low and point 2 of level substantial, plus:

1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high.
2. The binding has been verified on the basis of a unique identifier representing the legal person used in the national context; and on the basis of information uniquely representing the natural person from an authoritative source.

## Implementing Act – example: 1502

Electronic identification means characteristics and design

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="772 425 2033 468">1. The electronic identification means utilises at least one authentication factor.</li><li data-bbox="772 496 2237 625">2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.</li></ol>
Substantial	<ol style="list-style-type: none"><li data-bbox="772 704 2237 796">1. The electronic identification means utilises at least two authentication factors from different categories.</li><li data-bbox="772 818 2237 911">2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.</li></ol>
High	<p data-bbox="772 989 1128 1032">Level substantial, plus:</p> <ol style="list-style-type: none"><li data-bbox="772 1061 2237 1153">1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential</li><li data-bbox="772 1175 2237 1268">2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.</li></ol>

# Implementing Act – example: 1502

## 2.2.2. Issuance, delivery and activation

Assurance level	Elements needed
Low	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.
Substantial	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.
High	The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

# Implementing Act – example: 1502

## 2.2.3. Suspension, revocation and reactivation

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="772 511 2211 596">1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.</li><li data-bbox="772 625 2211 711">2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.</li><li data-bbox="772 739 2211 825">3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.</li></ol>
Substantial	Same as level low.
High	Same as level low.

# Implementing Act – example: 1502

## 2.2.4. Renewal and replacement

Assurance level	Elements needed
Low	Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level.
Substantial	Same as level low.
High	Level low, plus: Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

# Implementing Act – example: 1502

## Authentication mechanism

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="708 491 2232 576">1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.</li><li data-bbox="708 605 2232 748">2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.</li><li data-bbox="708 776 2232 948">3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.</li></ol>



# Implementing Act – example: 1502

Substantial

Level low, plus:

1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.
2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.

## Implementing Act – example: 1502

High

Level substantial, plus:

The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

# Implementing Act – example: 1502

## Management

Low

1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services.
2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.
3. Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services.
4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.
5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.

## Implementing Act – example: 1502

Published notices and user information

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="652 454 2153 586">1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.</li><li data-bbox="652 611 2153 782">2. Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.</li><li data-bbox="652 815 2153 905">3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.</li></ol>
Substantial	Same as level low.
High	Same as level low.

## Implementing Act – example: 1502

### Information security management

Assurance level	Elements needed
Low	There is an effective information security management system for the management and control of information security risks.
Substantial	Level low, plus: The information security management system adheres to proven standards or principles for the management and control of information security risks.
High	Same as level substantial.

## Implementing Act – example: 1502

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="715 468 2254 611">1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.</li><li data-bbox="715 632 2254 811">2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.</li></ol>
Substantial	Same as level low.
High	Same as level low.

# Implementing Act – example: 1502

## Staff

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="848 425 2237 511">1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.</li><li data-bbox="848 532 2237 618">2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.</li><li data-bbox="848 639 2237 761">3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.</li><li data-bbox="848 782 2237 903">4. Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.</li></ol>
Substantial	Same as level low.
High	Same as level low.

# Implementing Act – example: 1502

## Technical controls

Assurance level	Elements needed
Low	<ol style="list-style-type: none"><li data-bbox="853 442 2081 549">1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.</li><li data-bbox="853 571 2081 649">2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.</li><li data-bbox="853 671 2081 778">3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.</li><li data-bbox="853 799 2081 878">4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.</li><li data-bbox="853 899 2081 978">5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.</li></ol>
Substantial	<p data-bbox="853 1049 1172 1085">Same as level low, plus:</p> <p data-bbox="853 1106 2081 1185">Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering</p>
High	<p data-bbox="853 1263 1184 1299">Same as level substantial.</p>



## Implementing Act – example: 1502 compliance and audit

Low	The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.
Substantial	The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.
High	<ol style="list-style-type: none"><li data-bbox="670 825 2305 925">1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.</li><li data-bbox="670 953 2305 1053">2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.</li></ol>

# Security breaches: obligations

is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme,

the notifying Member State shall, **without delay, suspend or revoke that cross-border** authentication or the compromised parts concerned,

**and shall inform** other Member States and the Commission.

# Breaches ...

3. If the breach or compromise referred to in paragraph 1 is **not remedied within three months** of the suspension or revocation,

the notifying Member State shall notify other Member States and the Commission of the **withdrawal** of the electronic identification scheme.

# Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.
2. The party issuing the electronic identification means shall be liable ...
3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.

# Interoperability

3. The interoperability framework shall meet the following criteria:

- (a) it aims to be **technology neutral and does not discriminate between any specific national technical solutions** for electronic identification within a Member State;
- (b) it follows European and international **standards, where possible**;
- (c) it **facilitates** the implementation of the **principle of privacy by design**; and
- (d) it ensures that personal data is processed in accordance with Directive 95/46/EC.

# Interoperability

4. The interoperability framework shall consist of:

(a) a **reference to minimum technical requirements** related to the assurance levels under Article 8;

(b) a **mapping** of national assurance levels of notified electronic identification schemes **to the assurance levels** under Article 8;

(c) a reference to minimum technical **requirements for interoperability**;

(d) a reference to a **minimum set of person identification data** uniquely representing a natural or legal person, which is available from electronic identification schemes;

(e) **rules of procedure**;

(f) arrangements for **dispute resolution**; and

(g) **common operational security standards**

## **‘trust service’**

means an electronic service normally provided for remuneration which consists of:

- (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or**
- (b) the creation, verification and validation of certificates for website authentication; or**
- (c) the preservation of electronic signatures, seals or certificates related to those services;**

# Trust services

...trust service providers shall be **liable for damage caused intentionally or negligently** to any natural or legal person due to a failure to comply with the obligations under this Regulation.

The burden of proving intention or negligence of **a non-qualified trust** service provider shall lie **with the natural or legal person claiming the damage** referred to in the first subparagraph.

The intention or negligence of a **qualified trust** service provider shall be **presumed** unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.



# Trust services

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

# Supervision over trust services in each country

(a) to **supervise qualified trust service providers** established in the territory of the designating Member State to ensure, through **ex ante and ex post** supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;

# Supervision over trust services in each country

(b) to **take action if necessary, in relation to non-qualified trust service** providers established in the territory of the designating Member State, through **ex post supervisory activities**, when **informed** that those non-qualified trust service providers or the trust services they provide **allegedly do not meet the requirements** laid down in this Regulation.

# Security requirements for trust services

1. **Qualified and non-qualified trust service** providers shall take **appropriate technical and organisational measures to manage the risks** posed to the security of the trust services they provide.

.

# Security requirements for trust services

**Having regard to the latest technological developments**, those measures shall ensure that the level of security is commensurate to the degree of risk.

In particular, measures shall be taken to **prevent and minimise the impact of security incidents** and **inform stakeholders** of the adverse effects of any such incidents.

# Security requirements for trust services

2. **Qualified and non-qualified trust service providers** shall, without undue delay but in any event within **24 hours** after having become aware of it, **notify the supervisory body and, where applicable, other relevant bodies**, such as the competent national body for information security or the data protection authority, **of any breach of security or loss of integrity that has a significant impact** on the trust service provided or on the personal data maintained therein.

## Security requirements for trust services

Where the breach of security or loss of integrity is **likely to adversely affect a natural or legal person** to whom the trusted service has been provided, the trust service provider shall **also notify the natural or legal person of the breach of security or loss of integrity without undue delay.**

**Where appropriate**, in particular if a breach of security or loss of integrity concerns **two or more Member States**, the notified supervisory body shall inform the supervisory bodies in other Member States concerned **and ENISA.**

# Supervision of qualified trust service providers

Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body.

The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation.

The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.



## Supervision of qualified trust service providers

... the supervisory body **may at any time** **audit or request a conformity assessment** body to perform a conformity assessment of the qualified trust service providers,

**at the expense of those trust service providers,**

to **confirm** that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation.

# Audit rules

The Commission **may**, by means of implementing acts, **establish reference number of the following standards:**

**(a) accreditation of the conformity assessment bodies and for the conformity assessment report...**

**(b) auditing rules** under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers ...

## Initiation of a qualified trust service

Where trust service providers, without qualified status, **intend to start providing qualified trust services**, they shall **submit to the supervisory body a notification of their intention together with a conformity assessment report** issued by a conformity assessment body.

## Initiation of a qualified trust service

2. The **supervisory body shall verify** whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, ...

## Initiation of a qualified trust service

**If the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements... , the supervisory body shall grant qualified status ... and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists... , not later than three months after notification...**

## Initiation of a qualified trust service

If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.

**Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists**

## eIDAS II

**‘electronic identification means’ means a material and/or immaterial unit, including **European Digital Identity Wallets or ID cards** following Regulation 2019/1157, containing person identification data and which is used for authentication for an online or **offline** service;’;**



## eIDAS II

**‘certificate for electronic signature’ means an electronic attestation or **set of attestations** which links electronic signature **validation data** to a natural person and confirms at least the name or the pseudonym of that person;’**

**‘trust service’ means an electronic service normally provided against payment which consists of:**

- (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, electronic attestation of attributes and certificates related to those services;**
- (d) the electronic archiving of electronic documents;**
- (e) the management of remote electronic signature and seal creation devices;**
- (f) the recording of electronic data into an electronic ledger.’;**

## eIDAS II

**‘product’ means hardware or software, or relevant components of hardware and / or software, which are intended to be used for the provision of electronic identification and trust services;’**

## eIDAS II

**‘remote qualified signature creation device’**

**means a qualified electronic signature creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a signatory;**

## eIDAS II

**‘remote qualified seal creation device’**

**means a qualified electronic seal creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a seal creator;**

**eIDAS II**

**‘validation’**

**means the process of verifying and confirming that an electronic signature or a seal**

**or person identification data or an electronic attestation of attributes is valid;’**

***Now: ‘validation’ means the process of verifying and confirming that an electronic signature or a seal is valid***

## eIDAS II

**'European Digital Identity Wallet'** is a product and service that allows the user **to store identity data, credentials and attributes linked to her/his identity,** **to provide them to relying parties on request and to use them for authentication, online and offline,** for a service in accordance with Article 6a; **and to create qualified electronic signatures and seals;**

## eIDAS II

**'attribute'** is a **feature, characteristic or quality** of a natural or legal person or of an entity, in electronic form;



## eIDAS II

**‘electronic attestation of attributes’** means an **attestation in electronic form** that **allows** the **authentication of attributes**;

**‘qualified electronic attestation of attributes’** means an electronic attestation of attributes, which is issued by a **qualified trust service** provider and meets ... in Annex V;

## eIDAS II

**'authentic source'** is a repository or system, held under the responsibility of a public sector body or private entity, that **contains attributes** about a natural or legal person and is **considered to be the primary source** of that information or **recognised as authentic in national law**;

## eIDAS II

**‘EU Digital Identity Wallet Trust Mark’** means an indication in a simple, recognisable and clear manner that a Digital Identity Wallet has been issued in accordance with this Regulation;

## eIDAS II

**'strong user authentication'** means an authentication based on the use of **two or more elements** categorised as user knowledge , possession and inherence that are **independent**, in such a way that the **breach of one does not compromise the reliability of the others**, and is designed in such a way to **protect the confidentiality of the authentication data**;

## eIDAS II

**'credential'** means a **proof** of a person's **abilities, experience, right or permission;**

## eIDAS II

**‘electronic ledger’** means

a **tamper proof electronic record** of data,  
providing **authenticity and integrity** of the  
data it contains,

**accuracy of their date and time,**

and of their **chronological ordering’**;

# eIDAS II

## Article 6 is deleted;

### Article 6

#### Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:

## **European Digital Identity Wallets**

**1. For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless access to cross-border public and private services, each Member State shall issue a European Digital Identity Wallet within 12 months after the entry into force of this Regulation.**

**2. European Digital Identity Wallets shall be issued:**

**(a) by a Member State;**

**(b) under a mandate from a Member State;**

**(c) independently but recognised by a Member State**



**eIDAS II**

**eIDAS II**

## eIDAS II

European Digital Identity Wallets shall enable the user to:

- (a) securely request and **obtain, store, select, combine and share**, in a manner that is **transparent to and traceable by the user**, the necessary legal person identification data and electronic attestation of attributes to **authenticate online and offline** in order to **use online public and private services**;
- (b) **sign** by means of **qualified electronic signatures**.

## eIDAS II

Digital Identity Wallets shall, in particular:

(a) provide a **common interface**:

(1) to **qualified and non-qualified trust service** providers issuing qualified and non-qualified electronic attestations of attributes or other qualified and non-qualified certificates **for the purpose of issuing such attestations and certificates** to the European Digital Identity Wallet;

## eIDAS II

(2) for **relying parties** to **request and validate** **person identification data and electronic attestations of attributes;**

(3) for the **presentation to relying parties** of person identification data, electronic attestation of attributes or other data such as credentials, **in local mode not requiring internet access for the wallet;**

## eIDAS II

(b) **ensure** that trust **service providers** of qualified attestations of attributes cannot receive any information about the use of these attributes;

## eIDAS II

meet the requirements set out in Article 8 with regards to **assurance level “high”**, in particular as applied to the requirements for **identity proofing and verification, and electronic identification means management and authentication;**

## eIDAS II

**Member States shall provide validation mechanisms for the European Digital Identity Wallets:**

**(a) to ensure that its authenticity and validity can be verified;**

**(b) to allow relying parties to verify that the attestations of attributes are valid;**

**(c) to allow relying parties and qualified trust service providers to verify the authenticity and validity of attributed person identification data.**



## eIDAS II

The European Digital Identity Wallets shall be issued under a **notified** electronic identification scheme of level of assurance 'high'.

The use of the European Digital Identity Wallets shall be **free of charge** to natural persons.

## eIDAS II

**The user shall be in full control** of the European Digital Identity Wallet.

**The issuer** of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services,

## eIDAS II

**nor shall it combine** person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet **with personal data from any other services** offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, **unless the user has expressly requested it.**

Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held.

## eIDAS II

The European Digital Identity Wallet shall be made **accessible for persons with disabilities** in accordance with the accessibility requirements of Annex I to Directive 2019/882.

## eIDAS II

**Within 6 months of the entering into force of this Regulation,**

**the Commission shall establish technical and operational specifications and reference standards**

**for the requirements referred to in paragraphs 3, 4 and 5 by means of an implementing act on the implementation of the European Digital Identity Wallet.**

**This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).**

**eIDAS II**

**...**