COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

of 8 September 2015

on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 ([1]), and in particular Article 8(3) thereof,

Whereas:

(1) Article 8 of Regulation (EU) No 910/2014 provides that an electronic identification scheme notified pursuant to Article 9(1) needs to specify assurance levels low, substantial and high for electronic identification means issued under that scheme.

(2) Determining the minimum technical specifications, standards and procedures is essential in order to ensure common understanding of the details of the assurance levels and to ensure interoperability when mapping the national assurance levels of notified electronic identification schemes against the assurance levels under Article 8 as provided by Article 12(4)(b) of Regulation (EU) No 910/2014.

(3) International standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in this implementing act as being the principle international standard available in the domain of assurance levels for electronic identification means. However, the content of Regulation (EU) No 910/2014 differs from that international standard, in particular in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account. Therefore the Annex, while building on this international standard should not make reference to any specific content of ISO/IEC 29115.

(4) This Regulation has been developed as an outcome based approach as being the most appropriate which is also reflected in the definitions used to specify the terms and concepts. They take into account the aim of Regulation (EU) No 910/2014 in relation to assurance levels of the electronic identification means. Therefore, the Large-Scale Pilot STORK, including specifications developed by it, and the definitions and concepts in ISO/IEC 29115 should be taken into the utmost account when establishing the specifications and procedures set out in this implementing act.

(5) Depending on the context in which an aspect of evidence of identity needs to be verified, authoritative sources can take many forms, such as registries, documents, bodies inter alia. Authoritative sources may be different in the various Member States even in a similar context.

(6) Requirements for identity proofing and verification should take into account different systems and practices, while ensuring sufficiently high assurance in order to establish the necessary trust. Therefore, acceptance of procedures used previously for a purpose other than the issuance of electronic identification means should be made conditional upon confirmation that those procedures fulfil the requirements foreseen for the corresponding assurance level.

([1]) OJ L 257, 28.8.2014, p. 73.

(7) Certain authentication factors such as shared secrets, physical devices and physical attributes are usually employed. However, the usage of a greater number of authentication factors, especially from different factor categories, should be encouraged to increase the security of the authentication process.

(8) This Regulation should not affect representation rights of legal persons. However, the Annex should provide for requirements for the binding between the electronic identification means of natural and legal persons.

(9) The importance of information security and service management systems should be recognised, as should be the importance of employing recognised methodologies and applying the principles embedded in standards such as the ISO/IEC 27000 and the ISO/IEC 20000 series.

(10) Good practices in relation to assurance levels in the Member States should also be taken into account.

(11) IT security certification based on international standards is an important tool for verifying the security compliance of products with the requirements of this implementing act.

(12) The Committee referred to in Article 48 of Regulation (EU) No 910/2014 has not delivered an opinion within the time limit laid down by its chair,

HAS ADOPTED THIS REGULATION:

Article 1

1. Assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme shall be determined with reference to the specifications and procedures set out in the Annex.

2. The specifications and procedures set out in the Annex shall be used to specify the assurance level of the electronic identification means issued under a notified electronic identification scheme by determining the reliability and quality of following elements:

(a) enrolment, as set out in section 2.1 of the Annex to this Regulation pursuant to Article 8(3)(a) of Regulation (EU) No 910/2014;

(b) electronic identification means management, as set out in section 2.2 of the Annex to this Regulation pursuant to Article 8(3)(b) and (f) of Regulation (EU) No 910/2014;

(c) authentication, as set out in section 2.3 of the Annex to this Regulation pursuant to Article 8(3)(c) of Regulation (EU) No 910/2014;

(d) management and organisation, as set out in section 2.4 of the Annex to this Regulation pursuant to Article 8(3)(d) and (e) of Regulation (EU) No 910/2014.

3. When the electronic identification means issued under a notified electronic identification scheme meets a requirement listed in a higher assurance level then it shall be presumed to fulfil the equivalent requirement of a lower assurance level.

4. Unless otherwise stated in the relevant part of the Annex, all elements listed in the Annex for a particular assurance level of the electronic identification means issued under a notified electronic identification scheme shall be met in order to match the claimed assurance level.

Article 2

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 8 September 2015.

For the Commission
The President
Jean-Claude JUNCKER

ANNEX

Technical specifications and procedures for assurance levels low, substantial and high for electronic identification means issued under a notified electronic identification scheme

1. Applicable definitions

For the purposes of this Annex, the following definitions shall apply:

(1) 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity;

(2) 'authentication factor' means a factor confirmed as being bound to a person, which falls into any of the following categories:

(a) 'possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it;

(b) 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it;

(c) 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute;

(3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity;

(4) 'information security management system' means a set of processes and procedures designed to manage to acceptable levels risks related to information security.

2. Technical specifications and procedures

The elements of technical specifications and procedures outlined in this Annex shall be used to determine how the requirements and criteria of Article 8 of Regulation (EU) No 910/2014 shall be applied for electronic identification means issued under an electronic identification scheme.

2.1. *Enrolment*

2.1.1. Application and registration

Assurance level	Elements needed
Low	1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. 2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means. 3. Collect the relevant identity data required for identity proofing and verification.
Substantial	Same as level low.
High	Same as level low.

2.1.2. Identity proofing and verification (natural person)

Assurance level	Elements needed
Low	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. 2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid. 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.
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 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 [1] or by an equivalent body; or 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.

Assurance level	Elements needed
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; 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 (c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level 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 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 and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. OR 2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.

([1]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

2.1.3. Identity proofing and verification (legal person)

Assurance level	Elements Needed
Low	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.

Assurance level	Elements Needed
	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. 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.
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 2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 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 or by an equivalent body; or 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, 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.
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

Assurance level	Elements Needed
	2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 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 this previous procedure remain valid; or 3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, 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 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 and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.

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.

(3) Binding shall be done in the following manner:

Assurance level	Elements Needed
Low	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. 2. The binding has been established on the basis of nationally recognised procedures. 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.
Substantial	Point 3 of level low, plus: 1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high.

Assurance level	Elements Needed
	2. The binding has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source. 3. The binding has been verified on the basis of information from an authoritative source.
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.

2.2. *Electronic identification means management*

2.2.1. Electronic identification means characteristics and design

Assurance level	Elements needed
Low	1. The electronic identification means utilises at least one authentication factor. 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.
Substantial	1. The electronic identification means utilises at least two authentication factors from different categories. 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.
High	Level substantial, plus: 1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential 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.

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.

2.2.3. Suspension, revocation and reactivation

Assurance level	Elements needed
Low	1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner. 2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation. 3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.
Substantial	Same as level low.
High	Same as level low.

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.

2.3. *Authentication*

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls shall be understood to be commensurate to the risks at the given level.

2.3.1. Authentication mechanism

The following table sets out the requirements per assurance level with respect to the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party.

Assurance level	Elements needed
Low	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 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. 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.

Assurance level	Elements needed
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.
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.

2.4. *Management and organisation*

All participants providing a service related to electronic identification in a cross-border context ('providers') shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.

2.4.1. General provisions

Assurance level	Elements needed
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.
Substantial	Same as level low.
High	Same as level low.

2.4.2. Published notices and user information

Assurance level	Elements needed
Low	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. 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. 3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.
Substantial	Same as level low.
High	Same as level low.

2.4.3. 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.

2.4.4. Record keeping

Assurance level	Elements needed
Low	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. 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.
Substantial	Same as level low.
High	Same as level low.

2.4.5. Facilities and staff

The following table represents the requirements with respect to facilities and staff and subcontractors, if applicable, who undertake duties covered by this Regulation. Compliance with each of the requirements shall be proportionate to the level of risk associated with the assurance level provided.

Assurance level	Elements needed
Low	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. 2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures. 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. 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.
Substantial	Same as level low.
High	Same as level low.

2.4.6. Technical controls

Assurance level	Elements needed
Low	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. 2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay. 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. 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. 5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.
Substantial	Same as level low, plus: Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering
High	Same as level substantial.

2.4.7. Compliance and audit

Assurance level	Elements needed
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.

Assurance level	Elements needed
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	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. 2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.