Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) 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)

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501

of 8 September 2015

on the interoperability framework pursuant to Article 12(8) 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 12(8) thereof,

Whereas:

(1) Article 12(2) of Regulation (EU) No 910/2014 provides that an interoperability framework should be established for the purposes of interoperability of the national electronic identification schemes notified pursuant to Article 9(1) of that Regulation.

(2) Nodes play a central role in the interconnection of Member States' electronic identification schemes. Their contribution is explained in the documentation related to the Connecting Europe Facility established by Regulation (EU) No 1316/2013 of the European Parliament and of the Council[(2)], including the functions and components of the ‘eIDAS node’.

(3) Where a Member State or the Commission provides software to enable authentication to a node operated in another Member State, the party which supplies and updates the software used for the authentication mechanism may agree with the party which hosts the software how the operation for the authentication mechanism will be managed. Such an agreement should not impose disproportionate technical requirements or costs (including support, responsibilities, hosting and other costs) on the hosting party.

(4) To the extent that the implementation of the interoperability framework justifies, further technical specifications providing details on technical requirements as set out in this Regulation could be developed by the Commission, in cooperation with Member States, in particular having regard to opinions of the Cooperation Network referred to in Article 14(d) of Commission Implementing Decision (EU) 2015/296[(3)]. Such specifications should be developed as part of the digital service infrastructures of Regulation (EU) No

Changes to legislation: *There are outstanding changes not yet made to Commission Implementing Regulation (EU) 2015/1501. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

1316/2013 which provides the means for the practical implementation of an electronic identification building block.

(5) The technical requirements set out in this Regulation should be applicable despite any changes in the technical specifications that might be developed pursuant to Article 12 of this Regulation.

(6) Large-scale pilot STORK, including specifications developed by it, and the principles and concepts of the European Interoperability Framework for European Public Services have been taken into the utmost account when establishing the arrangements of the interoperability framework set out in this Regulation.

(7) The results of the cooperation between Member States have been taken into utmost account.

(8) The measures provided for in this Regulation are in accordance with the opinion of the Committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation lays down technical and operational requirements of the interoperability framework in order to ensure the interoperability of the electronic identification schemes which Member States notify to the Commission.

Those requirements include in particular:

(a) minimum technical requirements related to the assurance levels and the mapping of national assurance levels of notified electronic identification means issued under notified electronic identification schemes under Article 8 of Regulation (EU) No 910/2014 as set out in Articles 3 and 4;

(b) minimum technical requirements for interoperability, as set out in Articles 5 and 8;

(c) the minimum set of person identification data uniquely representing a natural or legal person as set out in Article 11 and in the Annex;

(d) common operational security standards as set out in Articles 6, 7, 9 and 10;

(e) arrangements for dispute resolution as set out in Article 13.

Article 2

Definitions

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

(1) ‘node’ means a connection point which is part of the electronic identification interoperability architecture and is involved in cross-border authentication of persons and which has the capability to recognise and process or forward transmissions to other nodes by enabling the national electronic identification infrastructure of one

***Changes to legislation:** There are outstanding changes not yet made to Commission Implementing Regulation (EU) 2015/1501. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

Member State to interface with national electronic identification infrastructures of other Member States;

(2) 'node operator' means the entity responsible for ensuring that the node performs correctly and reliably its functions as a connection point.

Article 3

Minimum technical requirements related to the assurance levels

Minimum technical requirements related to the assurance levels shall be as set out in Commission Implementing Regulation (EU) 2015/1502[(4)].

Article 4

Mapping of national assurance levels

The mapping of national assurance levels of the notified electronic identification schemes shall follow the requirements laid down in Implementing Regulation (EU) 2015/1502. **[**[X1]The results of the mapping shall be notified to the Commission using the notification template laid down in Commission Implementing Decision (EU) 2015/1984[(5)].**]**

Editorial Information

X1 Substituted by Corrigendum to Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) 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 (Official Journal of the European Union L 235 of 9 September 2015).

Article 5

Nodes

1 A node in one Member State shall be able to connect with nodes of other Member States.

2 The nodes shall be able to distinguish between public sector bodies and other relying parties through technical means.

3 A Member State implementation of the technical requirements set out in this Regulation shall not impose disproportionate technical requirements and costs on other Member States in order for them to interoperate with the implementation adopted by the first Member State.

Changes to legislation: There are outstanding changes not yet made to Commission Implementing Regulation (EU) 2015/1501. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes

Article 6

Data privacy and confidentiality

1 Protection of privacy and confidentiality of the data exchanged and the maintenance of data integrity between the nodes shall be ensured by using best available technical solutions and protection practices.

2 The nodes shall not store any personal data, except for the purpose set out in Article 9(3).

Article 7

Data integrity and authenticity for the communication

Communication between the nodes shall ensure data integrity and authenticity to make certain that all requests and responses are authentic and have not been tampered with. For this purpose, nodes shall use solutions which have been successfully employed in cross-border operational use.

Article 8

Message format for the communication

The nodes shall use for syntax common message formats based on standards that have already been deployed more than once between Member States and proven to work in an operational environment. The syntax shall allow:

(a) proper processing of the minimum set of person identification data uniquely representing a natural or legal person;

(b) proper processing of the assurance level of the electronic identification means;

(c) distinction between public sector bodies and other relying parties;

(d) flexibility to meet the needs of additional attributes relating to identification.

Article 9

Management of security information and metadata

1 The node operator shall communicate the metadata of the node management in a standardised machine processable manner and in a secure and trustworthy way.

2 At least the parameters relevant to security shall be retrieved automatically.

3 The node operator shall store data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be stored for a period of time in accordance with national requirements and, as a minimum, shall consist of the following elements:

a node's identification;

b message identification.

***Changes to legislation:** There are outstanding changes not yet made to Commission Implementing Regulation (EU) 2015/1501. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

c message date and time.

Article 10

Information assurance and security standards

1 Node operators of nodes providing authentication shall prove that, in respect of the nodes participating in the interoperability framework, the node fulfils the requirements of standard ISO/IEC 27001 by certification, or by equivalent methods of assessment, or by complying with national legislation.

2 Node operators shall deploy security critical updates without undue delay.

Article 11

Person identification data

1 A minimum set of person identification data uniquely representing a natural or a legal person shall meet the requirements set out in the Annex when used in a cross-border context.

2 A minimum data set for a natural person representing a legal person shall contain the combination of the attributes listed in the Annex for natural persons and legal persons when used in a cross-border context.

3 Data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters.

Article 12

Technical specifications

1 Where it is justified by the process of implementation of the interoperability framework, the Cooperation Network established by Implementing Decision (EU) 2015/296 may adopt opinions pursuant to Article 14(d) thereof on the need to develop technical specifications. Such technical specifications shall provide further details on technical requirements as set out in this Regulation.

2 Pursuant to the opinion referred to in paragraph 1 the Commission in cooperation with Member States shall develop the technical specifications as part of the digital service infrastructures of Regulation (EU) No 1316/2013.

3 The Cooperation Network shall adopt an opinion pursuant to Article 14(d) of Implementing Decision (EU) 2015/296 in which it evaluates whether and to what extent the technical specifications developed under paragraph 2 correspond to the need identified in the opinion referred to in paragraph 1 or the requirements set in this Regulation. It may recommend that Member States take the technical specifications into account when implementing the interoperability framework.

4 The Commission shall provide a reference implementation as an example interpretation of the technical specifications. Member States may apply this reference implementation or use it as a sample when testing other implementations of the technical specifications.