COUNCIL OF THE EUROPEAN UNION

Brussels, 17 June 2013

11032/13

Interinstitutional File: 2012/0146 (COD)

TELECOM 170
MI 551
DATAPROTECT 79
EJUSTICE 55
CODEC 1482

NOTE

from:	Presidency
to:	Delegations
No. Cion prop.:	10977/12 TELECOM 122 MI 411 DATAPROTECT 73 CODEC 1576
No prev. doc. :	8901/13 TELECOM 88 MI 331 DATAPROTECT 54 EJUSTICE 36 CODEC 919
Subject:	Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market *- Revised Cluster 1 (Articles 5 to 8)*

1. In view of the WP TELE meeting of 25 June, delegations will find at Annex a revised text on cluster 1 (Articles 5 to 8) on electronic identification. For easier reference, the changes as compared to the original Commission proposal (doc. (10977/12) are in **bold** (and deletions in ~~**strikethrough**~~). The changes as compared to the latest text on cluster 1 (doc. 8901/13) are **underlined**. The main changes of substance are outline below. Some additional changes have been introduced for consistency reasons.

2. Bearing in mind the discussions in the WP TELE and the progress report presented at the last TTE Council (doc. 10100/13), it is clear that the main outstanding issue in cluster 1 is the issue of identity assurance levels. At the informal attachés meeting of 22 May, which was devoted to the discussion on underlying principles for cluster 1, and, as noted in paragraph 9 of the progress report, delegations supported specifying, in one way or another, the identity assurance levels in the Regulation.

3. The suggested Presidency's approach as outlined below seeks to bring delegations' views closer with regard to the recognition of eID means and, by extension, of the eID schemes under which they are issued.

   – The revised text of Article 5(1) provides for the obligation to recognise eID means issued under notified schemes having an identity assurance level as set out in Annex 0 (i.e. currently levels 3 or 4 of STORK). It would apply regardless of the identity assurance level required for purposes of accessing the service in question at national level. This is reflected in Article 5(1) read in conjunction with Article 6(1)(ba) and Annex 0.

   – If the public interest justifies it, the Commission may adopt implementing acts to establish certain categories of services for which a specific identity assurance level may be required. This would mean that, in the case of a service falling under that category, Member States could (but would not be obliged to) require a higher level of identity assurance. This is reflected in Article 5(2) read in conjunction with Article 8(2b). However, if a Member State decides to require the higher level, it should require it for all eID means originating in other Member States without discrimination.

   – A new recital (footnote on p. 4) clarifies that a Member State may, on a voluntary basis, accept eID means having lower identity assurance level(s) than those defined in the Regulation.

   – In the current text, the Annex contains only the 'substantial' and 'high' identity assurance levels (levels 3 and 4 of STORK). In order to ensure that the Annex is future proofed, Article 6(3) provides for a delegated act to amend it, if need be. It is to be noted that an implementing act is not a legally acceptable solution in this case. The only other option would be to amend the Annex through the ordinary legislative procedure.

4. In addition, further changes have been introduced in Article 8 on interoperability, since interoperability is essential for recognition to work in practice. From an operational perspective, the time sequence should be as follows:
   - Member States cooperate in accordance with Article 8(1c) and (1d);
   - the Commission adopts implementing acts, in particular on the interoperability framework while taking into account the results of the above mentioned cooperation: Article 8(2a);
   - the requirements of the interoperability framework have to be complied with when Member States design and before they notify their schemes, under which eID means operate: Article 6(db).

5. It is recalled that, as noted in paragraph 10 of the progress report, the scope of the Chapter should be limited initially to services provided by public sector bodies. This will be reflected at a later stage in an appropriate article.

6. At the meeting of 25 June, the Presidency does not foresee an article by article examination of the text but will rather seek to approximate delegations' positions with regard to the identity assurance levels and to collect further suggestions on the provisions on interoperability.

CHAPTER II

ELECTRONIC IDENTIFICATION

Article 5[1]

Mutual recognition ~~and acceptance~~

1. When an electronic identification using an electronic identification means and authentication is required under national legislation or administrative practice to access a service online **in one Member State**, **~~any~~ the** electronic identification means issued in another Member State **~~falling under a scheme, which is included in the list published by the Commission pursuant to the procedure referred to in Article 7,~~** shall be recognised **~~and accepted~~ in the first Member State** for the purposes of accessing **~~this~~ that** service **online, ~~not later than six months after the list, including that scheme, is published.~~ provided that the following conditions are met:**

a. that electronic identification means is issued under the electronic identification scheme included in the list published by the Commission pursuant to Article 7;

b. the identity assurance level of that electronic identification means corresponds to one of the identity assurance levels set out in Annex 0.

Such recognition shall take place no later than 6 months after the list published by the Commission pursuant to Article 7, including the scheme referred to in point (a) of the previous subparagraph, is published.

2. Notwithstanding point (b) of paragraph 1, a specific assurance level set out in Annex 0 may be required for the electronic identification means to access online services defined in accordance with Article 8(2b).

---

[1] Article 5 to be complemented by the following recital:
'The obligation to recognise electronic identification means relates only to those means the identity assurance level of which corresponds to the levels defined by this Regulation. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels'.

Article 6

Conditions ~~of~~for notification of electronic identification schemes

1. An ~~E~~electronic identification scheme**~~s~~** shall be eligible for notification pursuant to Article 7 if all the following conditions are met:

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

(i) by**~~, on behalf of, or under the responsibility of or under the supervision of~~** 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 that scheme** can be used to access at least **one service provided by a** public **~~services~~ sector body** requiring electronic identification in the notifying Member State;

(ba) that scheme and the electronic identification means issued thereunder meet the requirements of ~~point 3 or, where applicable, of point 2 of~~ one of the identity assurance levels set out in Annex 0;

(c) the notifying Member State ensures that the person identification data are attributed unambiguously to the natural or legal[2] person referred to in **point 1 of** Article 3 **~~point1~~ at the time of issuance of the electronic identification means under that scheme**;

(cb) the party issuing the electronic identification means under that scheme ensures that ~~the person identification data~~ electronic identification means is attributed to the person referred to in point (c) ~~are unambiguously attributed to the electronic identification means~~ in accordance with the requirements for the relevant identity assurance level set out in Annex 0;

[2] The notion of the legal person could be clarified in a recital similar to recital 38 of Directive on service in the internal market 2006/123/EC which reads:
'The concept of 'legal persons', according to the Treaty provisions on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, 'legal persons', within the meaning of the Treaty, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.'

(d) the notifying Member State ensures the availability of ~~an~~ authentication ~~possibility~~ online, ~~at any time and free of charge~~ so that any relying party **established outside of the territory of that Member State** can validate the person identification data received in electronic form. **Such cross border authentication shall be provided free of charge when accessing a service online provided by a public sector body.** Member States shall not **unduly** impose any specific technical requirements on relying parties ~~established outside of their territory~~ intending to carry out such authentication~~. When either the notified identification scheme or authentication possibility is breached or partly compromised, Member States shall suspend or revoke without delay the notified identification scheme or authentication possibility or the compromised parts concerned and inform the other Member States and the Commission pursuant to Article 7~~;

(da) at least six months prior to notification pursuant to Article 7(1), the notifying Member State provides to other Member States for the purposes of the obligation under Article 8(1c) a description of ~~electronic identification~~ that scheme in accordance with the procedural modalities referred to in Article 8(1d).

(db) that scheme meets the requirements of the implementing act referred to in Article 8(2a).

~~**(e) the notifying Member State takes liability for:**~~

~~**(i) the unambiguous attribution of the person identification data referred to in point (c), and**~~

~~**(ii) the authentication possibility specified in point (d).**~~

~~**2. Point (c) of paragraph 1 is without prejudice to the liability of parties to a transaction in which electronic identification means falling under the notified scheme are used.**~~

3. For the purposes of taking into account technological progress, subject to the criteria set out in point 1 of Annex 0 and taking into account the results of the cooperation between Member States, the Commission shall be empowered to adopt delegated acts in accordance with Article 38 to amend that Annex, with the exception of point 1.

~~**4. By *[insert the date]* and taking into account the results of the cooperation between Member States, the Commission shall adopt implementing acts to establish a list of services requiring the 'high' security assurance level as referred to in point 2 of Annex 0, provided that the following conditions are met *[to be inserted]*:**~~

~~**Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).**~~

Article 7

Notification

1. **The notifying** Member State**s ~~which notify an electronic identification scheme~~** shall forward to the Commission the following information and without undue delay, any subsequent changes thereof:

(a) a description of the notified electronic identification scheme**, including its ~~security~~ identity assurance level~~s~~**;

(b) the **authority or authorities ~~entity~~** responsible for the notified electronic identification scheme;

(c) information on **the entity or entities ~~by whom~~ which manage~~s~~** the registration of the unambiguous person identifi**~~ers~~cation data ~~is managed~~**;

(ca) a description of how the requirements of the ~~interoperability framework referred to in Article 8~~ implementing act referred to in Article 8(2a) are met;

(d) a description of the authentication **~~possibility~~ referred to in point (d) of Article 6**;

(e) arrangements for suspension or revocation of either the notified identification scheme or authentication **~~possibility~~** or the compromised parts concerned.

2. **Six ~~Twelve~~** months after the entry into force of the Regulation, the Commission shall publish in the *Official Journal of the European Union* the list of the electronic identification schemes which were notified pursuant to paragraph 1 and the basic information thereon.

3. If the Commission receives a notification after the period referred to in paragraph 2 **has** expired, it shall ***publish in the Official Journal of the European Union*** **the** amend**ments to** the list **referred to in paragraph 2** within **~~three~~ ~~one~~ two** month**s from the date of receipt of that notification**.

4. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of the notification referred to in paragraph**~~s~~** 1 **~~and 3~~**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 7a

Security breach

1. When either the electronic identification scheme notified pursuant to Article 7(1) or the authentication referred to in point (d) of Article 6 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 suspend or revoke without delay ~~that scheme or~~ that cross border authentication or the compromised parts concerned and inform other Member States and the Commission.

2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross border authentication and shall inform other Member States and the Commission without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within 3 months of the suspension or revocation, the notifying Member State shall notify the withdrawal of the electronic identification scheme to other Member States and to the Commission. The Commission shall publish without undue delay in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 7(2).

Article 7b

Liability

1. The notifying Member State shall be liable under national law for any damage caused to any natural or legal person ~~due to a failure~~ for failing to comply with its obligations under points (c) and (d) of Article 6.

2. The party issuing the electronic identification means shall be liable under national law for any damage caused to any natural or legal person for failing ~~to ensure~~ in a cross border transaction to comply with the obligation ~~the unambiguous attribution of the person identification data~~ referred to in point (cb) of Article 6(1).

2a. The party operating the authentication procedure shall be liable under national law for any damage caused to any natural or legal person for failing to ensure in a cross border transaction the correct operation of the authentication referred to in point (d) of Article 6(1).

3. Paragraphs 1, 2 and 2a are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the notified scheme are used.

Article 8

~~Coordination~~ Cooperation and interoperability

1. **~~Member States shall cooperate in order to ensure the interoperability of electronic identification means falling under a notified scheme and to enhance their security.~~**

The national electronic identification ~~infrastructures~~ schemes notified pursuant to Article 7 shall be interoperable. ~~The interoperability between the national electronic identification infrastructures shall be ensured an interoperability framework.~~

1aa. For the purposes of the requirement under paragraph 1, the interoperability framework shall be established.

1a. The interoperability framework shall meet the following criteria:

(a) it shall aim to be technology neutral and shall not discriminate between any specific national technical solutions for electronic identification within the Member State;

(b) it shall follow European and international standards, when possible;

(c) it shall facilitate the implementation of the principle of privacy by design;

(d) it shall ensure that personal data is processed in accordance with Directive 95/46/EC.

1b. The interoperability framework shall consist of:

(a) reference to minimum technical requirements related to the identity assurance levels defined in Annex 0;

(b) a mapping of national identity assurance levels of notified electronic identification schemes into the identity assurance levels defined in Annex 0;

(c) reference to minimum technical requirements for interoperability;

(d) rules of procedure.

~~1b. By *[insert the date]*, in order to establish technical modalities for implementing paragraphs 1 and 1a, the Commission shall adopt implementing acts on standards, protocols and technical specifications for the interoperability framework.~~

1c. Member States shall cooperate with regard to the following:

- the interoperability ~~and security~~ of ~~electronic identification means falling under notified~~ the electronic identification schemes notified pursuant to Article 7 and the electronic identification schemes which Member States intend to notify;

- the security of the electronic identification schemes.

1d. The cooperation between Member States shall consists of :

(a) exchange of information, experience and good practice on electronic identification schemes, in particular on technical requirements~~, specifications, protocols and standards~~ related to interoperability and ~~security~~ identity assurance levels;

(b) exchange of information, experience and good practice on working with ~~security~~ identity assurance levels of electronic identification schemes referred to in Annex 0 and on categories of services requiring ~~the 'high'~~ a specific ~~security~~ identity assurance level ~~as referred to in point 2 of that Annex~~;

(c) peer review of electronic identification schemes falling under this Regulation;

(d) examination of relevant developments in the electronic identification sector.

2. The Commission shall, by means of implementing acts, establish the necessary **procedural** modalities to facilitate the cooperation between the Member States referred to in paragraph**s** 1**c and 1d** with a view to fostering a high level of trust and security appropriate to the degree of risk. ~~**Those implementing acts shall concern, in particular, the exchange of information, experiences and good practice on electronic identification schemes, the peer review of notified electronic identification schemes and the examination of relevant developments arising in the electronic identification sector by the competent authorities of the Member States.**~~

2a. By [*insert the date*], for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission, subject to the criteria set out in paragraph 1a and taking into account the results of the cooperation between Member States, shall adopt implementing acts on the interoperability framework as defined in paragraph 1b.

2b. When public policy or public security or protection of personal data justifies it, the Commission, taking into account the results of the cooperation between Member States, may adopt implementing acts to establish categories of services for which a specific identity assurance level referred to in Annex 0 may be required, provided that the following conditions are met:

(a) analysis of the requirement for a specific identity assurance level has shown the appropriatness of such a requirement;

(b) the requirement for a specific identity assurance level shall be proportionate to the objective of public policy, public security or protection of sensitive personal data;

(c) there is a high risk that accepting a lower identity assurance level would expose a fundamental interest of society to threats.

3. ~~Those i~~Implementing acts **referred to in paragraphs ~~1b and~~ 2, 2a and 2b of this Article** shall be adopted in accordance with the examination procedure referred to in Article 39(2).

~~**3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the facilitation of cross border interoperability of electronic identification means by setting of minimum technical requirements.**~~

Annex 0.

~~Security~~ Identity assurance levels of electronic identification schemes and of electronic identification means issued thereunder

1. The criteria to establish a ~~security~~ identity assurance level of an electronic identification scheme and of the electronic identification means issued under that scheme shall be the following:

(a) reliability of the procedure to verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) reliability of the process to issue electronic identification means;

(c) quality of the entity issuing electronic identification means;

(d) types and robustness of the electronic identification means;

(e) security of the authentication mechanism.

2. An electronic identification scheme and the electronic identification means issued under that scheme ~~having~~ with 'high'[3] ~~security~~ identity assurance level shall fulfill all the following requirements:

(a) The identity of natural or legal persons applying for the issuance of electronic identification means is verified, in accordance with national law, by appropriate means similar to the verification performed for the issuance of official documents such as passports or identity cards, by the issuer of the electronic identification means or by an authorised third party.

The verification of the identity referred to in the previous subparagraph requires the physical appearance of the natural person or of an authorised representative of the legal person during the process of issuing the electronic identification means or on a prior occasion, if this prior verification is trusted by the issuer under national law.

(b) the electronic identification means is

- **directly given to the person after validation of his/her identity, or**
- **sent to the person and activated after validation of his/her identity.**

(c) the issuer of the electronic identification means

- **is a public body or**
- **meets the requirements in Article 19 (2) applied *mutatis mutandis*;**

[3] This level corresponds to level 4 of STORK.

(d) the electronic identification means is based on or logically linked to a qualified certificate or a qualified signature creation device;

(e) the authentication process offers ~~complete~~ state of art protection against attacks.

3. An electronic identification scheme and electronic identification means issued under that scheme ~~having~~ with 'substantial'[4] ~~security~~ identity assurance level shall fulfill all the following requirements:

(a) identification of natural or legal persons applying for the issuance of electronic identification means meets one of the following conditions:

- **it requires a physical presence, and the person identification data are validated against a public register, or**
- **it is remote, and the person identification data are validated by using trusted means under national law.**

(b) the electronic identification means is issued as follows:

- **it is directly given to the person after validation of his/her identity, or**
- **it is sent by registered mail after prior validation of the address against an official identity database, or**
- **it is downloaded on the Internet after the request is signed by the person with a qualified electronic signature, or**
- **it is downloaded directly by the person applying for the issuance of electronic identification means after entering a private password which was given physically to that person during the course of a registration fulfilling the requirements of point (a) of this paragraph.**

(c) the issuer of the electronic identification means meets the requirements in Article 19 (2) applied *mutatis mutandis*;

(d) the electronic identification means is based on a hard certificate or a soft certificate or one-time password device token or a qualified soft certificate;

(e) the authentication process offer protection against most type of attacks.

----

[4] This level corresponds to level 3 of STORK.