COUNCIL OF THE EUROPEAN UNION

Brussels, 29 April 2013

8901/13

Interinstitutional File: 2012/0146 (COD)

TELECOM 88
MI 331
DATAPROTECT 54
EJUSTICE 36
CODEC 919

NOTE

from:	Presidency
to:	Delegations
No. Cion prop.:	10977/12 TELECOM 122 MI 411 DATAPROTECT 73 CODEC 1576
No prev. doc. :	8083/13 TELECOM 63 MI 253 DATAPROTECT 37 EJUSTICE 23 CODEC 713
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 3 May, delegations will find at Annex a revised text on cluster 1 (Articles 5 to 8) on electronic identification. The proposed changes are based on discussions held at the WP TELE meetings of 4 and 12 April as well as on the written comments provided by some delegations in relation to the latest version of cluster 1 (doc. 8083/13). The main changes of substance are outlined below.

2. 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. 8083/13) are **underlined**. The following paragraphs outline the key principles underlying the revised text and concerning the role of *security assurance level*, the introduction of *a standstill period for interoperability arrangements,* the articulation between *interoperability and cooperation* and a *gradual approach as concerns the scope.*

3. The Presidency noted that at the last meeting of WP TELE devoted to cluster 1, most Member States favoured the introduction of security assurance levels. Therefore a new Annex 0, specifying two security assurance levels, has been included. The two levels correspond to the STORK level 4 ('high' level – point 2 of Annex 0) and STORK level 3 ('substantial' level – point 3 of Annex 0). The basic level for all services would be the 'substantial' level (see new eligibility condition in Article 6(1)(ba)) and a list of services requiring the 'high' level would be established in an implementing act (see new paragraph 6(4)). If this approach is accepted, conditions for the establishment of the list of services requiring 'high' security assurance level will need to be developed. Delegations are invited to provide suggestions. Moreover, in order to keep the Annex future proof, it could be amended via delegated acts (new paragraph 6(3)).

4. A standstill period of 6 months has been introduced in Article 5, which should provide sufficient time for Member States to fully roll out the technical interoperability arrangements before the obligation of mutual recognition would apply.

   This new provision is linked to the already existing obligation under Article 6(1)(da) which requires the notifying Member State to provide a description of the eID scheme to be notified 6 months prior to the notification. Beyond informing other Member States of the intention to notify and of the description of the eID scheme, Member States will engage in cooperation with regard to interoperability and security. This cooperation will also continue after the notification, during the above mentioned standstill period.

5. The text of Article 6.1(a) has been amended to include the wording in footnote 1 of the Commission's non-paper COM (2012) 238 of 4.6.2012. This makes clear that eID means issued by private bodies are eligible for notification and are required to be recognised in the Member State concerned. The Presidency considers that this obviates the need for the establishment of a supervisory scheme as it requires the issuer to meet any requirements the Member State may set for such recognition and accordingly, paragraph (ca) has been deleted.

6. Article 8 on interoperability and cooperation between Member States has been further developed. The Presidency would welcome further suggestions on the criteria for the interoperability framework.

The cooperation between Member States is an important element of the Presidency's proposal. The results of the cooperation shall be taken into account for example when adopting implementing acts concerning the list of services requiring 'high' security assurance level (Article 6(4)) or delegated acts amending Annex 0 (Article 6(3)).

7. The Presidency acknowledges that most Member States expressed a preference for a gradual approach, i.e. to limit initially the application of Chapter II to services provided by public sector bodies only, while not excluding private services from the scope of Chapter II. Such an approach could be reflected in Article 42 by specifying that as from the date of application of the Regulation (that date is still to be determined in future discussions) Chapter II will apply for a period of X years only to services provided by public sector bodies[1]. It is the Presidency's understanding that during that period, eID means could also be accepted for private services on a voluntary basis. After that period, Chapter II will apply to all services.

[1] A definition clarifying the notion of 'public sector body' could be introduced in Article 3. Such definition could for example read:
1.'public sector body' means the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law;
2. 'body governed by public law' means any body:
(a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and
(b) having legal personality; and
(c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law.

8. While the Presidency acknowledges that a number of other important issues[2] still need to be addressed, the aim of this meeting of the WP TELE is to discuss and possibly agree on the main elements and principles outlined above. The Presidency requests Member States to indicate their acceptance or non-acceptance of the following principles:

- The introduction of a minimum security assurance level for electronic identification schemes, with a higher level for certain services, as outlined.
- The development of an interoperability framework according to specified criteria and of co-operation between Member States regarding the interoperability and security of electronic identifications means in advance of the mutual recognition of notified schemes.
- The limiting of the obligation of mutual recognition for an initial period to services provided by public sector bodies, while allowing electronic identification means to access private services on a voluntary basis.

_____

[2] Such as e.g.:
- various timelines (for the notification/publication of eID schemes or for the adoption of relevant implementing/delegated acts) ;
- references to 'national law' and 'direct damage' in Article 7b on liability;
- the issue of legal person vs. non-natural person.

CHAPTER II

ELECTRONIC IDENTIFICATION

Article 5

Mutual recognition ~~and acceptance~~

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) those electronic identification means are issued under the electronic identification scheme included in the list published by the Commission pursuant to Article 7;**~~

~~**(b) those electronic identification means correspond to a security assurance level equal to or higher than the security assurance level required for access to that service online in the first Member State.**~~

Article 6

Conditions of notification of electronic identification schemes

1. An ~~**E**~~**e**lectronic 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) the electronic identification scheme meets the requirements of point 3 or, where applicable, of point 2 of Annex 0;

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

~~(ca) where the electronic identification means are issued under the supervision of the notifying Member State, the notifying Member State ensures the establishment of a supervisory scheme for the party issuing the electronic identification means;~~

(cb) the party issuing the electronic identification means under that scheme ensures that the person identification data referred to in point (c) are unambiguously attributed to the electronic identification means;

(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 authentication shall be provided free of charge ~~for~~ when accessing a service online provided by a public ~~online services~~ 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 a description of the electronic identification scheme ~~to be notified at least six months prior to notification~~.

~~(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).~~

---

[3] 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.'

~~**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 assurance levels**;

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

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

(ca) a description of how the requirements of the interoperability ~~**model**~~ **framework referred to in Article 8 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** 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 paragraphs 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 that scheme, the notifying Member State shall ~~without delay~~ suspend or revoke without delay that ~~electronic identification~~ scheme or that 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 ~~has been~~ is remedied, the notifying Member State shall re-establish the authentication and shall inform other Member States and the Commission without undue delay.

3. If the ~~notified electronic identification scheme or authentication~~ 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 ~~non-natural~~ legal person due to a failure to comply with its obligations under points (c)~~, (ca)~~ 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 ~~non-natural~~ legal person for failing to ensure~~: (i)~~ the unambiguous attribution of the person identification data referred to in point (cb) of Article 6~~., and~~

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 ~~(ii)~~ the correct operation of the authentication referred to in point (d) of Article 6.

3. Paragraphs 1, 2 and 2a are without prejudice to the liability under national ~~legislation~~ 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 shall be interoperable. The interoperability between the national electronic identification infrastructures shall be ensured through ~~the~~ an interoperability ~~model~~ framework.

1a. The interoperability ~~model~~ 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 principle of privacy by design;

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

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

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

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 specifications, protocols and standards related to interoperability and security assurance levels;

(b) exchange of information, experience and good practice on working with security assurance levels of electronic identification schemes referred to in Annex 0 and on services requiring the 'high' security 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.~~**

3. ~~Those i~~Implementing acts **referred to in paragraphs 1b and 2 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 assurance levels of electronic identification schemes

1. The criteria to establish a security 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 having 'high'[4] security 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*;**

[4] 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 protection against attacks.

3. An electronic identification scheme having 'substantial'[5] security 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 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.

---

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