



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 4 April 2013**

**8083/13**

---

**Interinstitutional File:  
2012/0146 (COD)**

---

**TELECOM 63  
MI 253  
DATAPROTECT 37  
EJUSTICE 23  
CODEC 713**

**NOTE**

---

from: Presidency  
to: Delegations

---

No. Cion prop.: 10977/12 TELECOM 122 MI 411 DATAPROTECT 73 CODEC 1576

---

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  
- *Cluster 1 (Articles 5 to 8)*

---

1. In view of the objective of the IE Presidency to advance negotiations on the above proposal, delegations will find at Annex I a revised text on cluster 1 (Articles 5 to 8) on electronic identification. The proposed changes are based on discussions held at WP TELE meetings as well as on the many written comments provided by delegations in relation to cluster 1. The main changes of substance are outlined below.
2. As noted in the progress report (doc. 17269/12), many delegations had concerns with regard to the fact that all notified eID means had to be recognised, regardless of the security assurance levels applied. Several delegations suggested to address this issue by means of a reciprocity requirement. One of the main elements of the Presidency proposal is therefore the inclusion of the reciprocity principle in Article 5.

The Presidency is however aware that some delegations would prefer to define security levels in the Regulation. The Presidency therefore seeks the views of delegations also on possible alternatives to the reciprocity model.<sup>1</sup>

3. Another important element of the Presidency proposal is the introduction of a common interoperability model in Article 8 (including a corresponding reference in Article 7) which aims to address the concerns of many delegations with regard to possible interoperability problems. If the concept of the interoperability model is accepted, the criteria (Art. 8(1a)) defining this model should be further developed and discussed.
4. Further changes include new Article 7a (based on the previous Art. 6(1)(d)) specifying a procedure for revocation/suspension of eID schemes in the case of a security breach and new Article 7b on liability (largely based on the previous Art. 6(1)(e) and 6(2)), which makes a distinction between liability of the notifying Member State and that of the eID means issuer.

---

<sup>1</sup>

**Alternative 1 - Security levels defined in the Regulation**

- include a new eligibility condition for notification of eID schemes in Article 6, which could read:

'(ba) the electronic identification scheme meets the requirements of Annex I;' and

- include an Annex I that would lay down requirements for security assurance levels of eID schemes. Two levels of security assurance could be defined: a basic (minimum) level for all standard services and a high level for sensitive services (such as, for example, eHealth). These security assurance levels could be based on the two highest levels of the STORK classification (levels 3 and 4).

**Alternative 2 - Combination of approaches**

- reciprocity model for all standard services, combined with  
- a defined security assurance level for sensitive services

5. Moreover, the Presidency noted diverging views of delegations in relation to the scope of Article 5. While some delegations would like to limit the scope to public services online only, others have expressly asked to also include private services. The Presidency believes that, as suggested by several delegations, a gradual approach, starting with public services, could be the right solution and invites delegations to take positions in this regard.
  
6. The attached revised text of cluster 1 will be discussed in the WP TELE on 11 April 2013, where delegations will be invited to take position on the proposed changes and/or alternative solutions as outlined above. The Presidency would also welcome written comments.

---

## 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 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, 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.~~ Electronic identification schemes shall be eligible for notification pursuant to Article 7 if all the following conditions are met:

- (a) the electronic identification means are issued by, on behalf of, ~~or~~ under the responsibility of **or under the supervision of** the notifying Member State;
- (b) the electronic identification means can be used to access at least **one** public services requiring electronic identification in the notifying Member State;
- (c) the notifying Member State ensures that the person identification data are attributed unambiguously to the natural or ~~legal~~ **non-natural** person referred to in **point 1 of Article 3 point 1** ~~at the time of issuance of the electronic identification means;~~
- (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 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 public online services.** 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) **the notifying Member State provides to other Member States a description of the electronic 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).~~

~~2. Point (e) 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.~~

## *Article 7*

### **Notification**

1. ~~The notifying Member States 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 security assurance levels;**
  - (b) the **authorities entity** responsible for the notified electronic identification scheme;
  - (c) information on **the entity by whom which manages** the registration of the unambiguous person identifiers ~~scation data is managed;~~

- (ca) **a description of how the requirements of the interoperability model 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 amendments to the list referred to in paragraph 2** within ~~three~~ **one** months **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, the notifying Member State shall without delay suspend or revoke 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 has been remedied, the notifying Member State shall reestablish the authentication and shall inform other Member States and the Commission without undue delay.**

**3. If the notified electronic identification scheme or authentication is not remedied, the notifying Member State shall notify the withdrawal of the electronic identification scheme 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 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 person for failing to ensure:**
  - (i) the unambiguous attribution of the person identification data referred to in point (cb) of Article 6, and**
  - (ii) the correct operation of the authentication referred to in point (d) of Article 6.**
- 3. Paragraphs 1 and 2 are without prejudice to the liability under national legislation 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 interoperability model.**

**1a. The interoperability model shall meet the following criteria *[to be inserted]*<sup>2</sup>:**

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

---

<sup>2</sup> Such criteria could be:

- (a) the interoperability model and its security assurance framework shall aim to be technology neutral, and shall not discriminate between any specific national technical solutions for electronic identification within the Member State;**
- (b) the interoperability model and its security assurance framework shall follow European and international standards when possible;**
- (c) the interoperability model and its security assurance framework shall facilitate the principle of privacy by design.'**

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

2. The Commission shall, by means of implementing acts, establish the necessary modalities to facilitate the cooperation between the Member States referred to in paragraph 1c 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~~ 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.~~**

-----