COUNCIL OF THE EUROPEAN UNION

Brussels, 28 May 2013

10100/13

Interinstitutional File: 2012/0146 (COD)

TELECOM 141
MI 452
DATAPROTECT 69
EJUSTICE 52
CODEC 1219

NOTE

from:	Presidency
To:	Delegations
No. Cion prop.:	10977/12 TELECOM 122 MI 411 DATAPROTECT 73 CODEC 1576
No. prev. doc. :	9772/13 TELECOM 128 MI 422 DATAPROTECT 66 EJUSTICE 47 CODEC 1135
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 - *Progress report*

The present report has been drawn up under the responsibility of the Irish Presidency and is without prejudice to particular points of interest and more detailed comments of individual delegations. It sets out the work done so far in the Council's preparatory bodies and gives an account on the state of play in the examination of the above mentioned proposal.

I. INTRODUCTION

1. The Commission adopted its 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* on 4 June 2012, on the basis of Article 114 TFUE. The proposal seeks to review the existing legislation for electronic signatures, to ensure mutual recognition of electronic identification and authentication across Europe and to establish a legal framework for trust services, such as electronic seals, time stamping, electronic document admissibility, electronic delivery and website authentication.

2. This proposal is a high priority dossier that has been identified in the Single Market Act I as one of the main levers to boost growth and employment. Moreover, the proposal is also flagged as one of the key actions in the Digital Agenda for Europe and the EU's Roadmap to Stability and Growth. The European Council called, on several occasions, for a swift adoption of the proposed Regulation.

3. The proposal and its impact assessment were presented in June and July 2012 at the Council Working Party on Telecommunications and the Information Society (hereinafter: WP TELE). After a thorough examination of the proposal in several meetings of the WP TELE, the Cyprus Presidency put together a progress report[1] for the TTE Council in December 2012. Telecom Ministers held an orientation debate at the TTE Council focusing mainly on how to ensure progress on this important dossier and how to address the crucial issue of assurance levels for electronic identification, which provided useful guidance for the future work under the IE Presidency.

[1] Document 17269/12.

4. The Irish Presidency put considerable efforts into advancing negotiations on the proposal. Twelve WP TELE meetings on the proposal have taken place. Moreover, the Presidency and the Commission co-organised two informal seminars addressed to telecom attachés, one devoted to electronic identification and eSignatures and the other to certain other trust services. On the basis of the discussions in the WP TELE and of the many written comments submitted by delegations, the Presidency put together the present progress report in order to inform Ministers about the state of play of the proposal and to draw attention to the issues that will necessitate further discussions.

5. In the EP, the ITRE (Ms Marita Ulvskog) and IMCO (Ms Marielle Gallo) committees have each exclusive competence for certain specified provisions of the proposal and the LIBE and JURI committees are expected to deliver opinions. The votes in the IMCO and ITRE committees are tentatively scheduled for July and September 2013 respectively.

II. STATE OF PLAY

6. Following the endorsement, in early January, by the WP TELE of the way forward suggested by the Irish Presidency, the work was scheduled to progress through the consideration of six clusters of provisions:
   - cluster 1: electronic identification (art. 5-8),
   - cluster 2: trust services - general provisions (art. 9-12) and supervision (art. 13-19),
   - cluster 3: electronic signature (art. 20-27, Annexes I and II),
   - cluster 4: other trust services (art. 28-37, Annexes III and IV),
   - cluster 5: general provisions (art. 1-4) and final provisions, including delegated and implementing acts (art. 38-42),
   - cluster 6: preamble.

After an in-depth examination of the entire operative part of the proposal (clusters 1 to 5), the Presidency decided, given the difficult and lengthy discussions in the WP TELE meetings, to focus the efforts on cluster 1 and to a lesser extent 2, while collecting delegations' views on the remaining provisions. The Presidency provided several revised texts on cluster 1[2] and 2[3]. The main conclusions of the discussions on clusters 1 and 2 as well as the principal views of delegations on the remaining clusters are presented below.

Cluster 1: Electronic identification (articles 5 - 8)

7. A fundamental question that needed to be tackled in regard of cluster 1 on electronic identification was the question of assurance levels for electronic identification means. Based on many discussions in the WP TELE, the Presidency put forward two basic options on how to address the issue of assurance levels:

- A first option based on the principle of reciprocity [4]. Under this option, a Member State would, for the purposes of accessing an on-line service requiring the use of an eID means under its national law or administrative practice, recognise an eID means issued in another Member State that corresponds to an assurance level equal to or higher than the assurance level required for accessing that on-line service. This option should probably be complemented by defining different assurance levels in the Annex, which would make it easier to assess the assurance level of a particular eID scheme. Member States and/or service providers would be free to choose the appropriate level of assurance.

[2] Documents 8083/13 and 8901/13.
[3] Document 8304/13.
[4] The Presidency notes that there appears to be some confusion about the meaning of the term 'reciprocity'. In future work it could be replaced by 'matching levels of assurance' or similar wording better capturing the idea behind the principle.

- As a second option, the recognition of e-Id means could be based on a required assurance level(s) in the Regulation, e.g. in an Annex,(for example STORK level 3 or STORK level 3 and 4). Under this option, services for which a higher assurance level could/would be required, would have to be determined.

8. With regard to the two basic options described in paragraph 7 above, while a significant number of delegations support the second option, subject to further fine-tuning, an important number of delegations favour the first option.

- Delegations supporting the second option mentioned one or the other following 'sub-options':
  - Some delegations would prefer to set only one required assurance level (e.g. STORK level 3). This would mean that eID means of this level (and higher) issued in one Member State would have to be recognised for the purposes of accessing a service online in another Member State.
  - Other delegations would agree with setting two assurance levels - a 'basic' one and a 'higher' one (e.g STORK level 3 and STORK level 4). This would mean that Member States would have to recognise eID means at the basic level for the purposes of accessing all services, with the exception of those, for which it would be allowed to require the higher level. The Presidency noted that most delegations were not in favour of linking types of services to specific assurance levels. In future discussions, it could be thus considered e.g. to set conditions/criteria under which the higher level could be required or provide for a reciprocity principle limited only to the 'basic' and 'higher' levels.

- Some delegations would also like to complement the second option with a possibility of a derogation, which would allow for lower assurance levels for certain other services, in which case the Annex could be expanded to include lower levels of assurance. Others would, however, not support this derogation possibility.

9. Moreover, the Presidency noted that, irrespective of their position on the two options above, most delegations could support the following, with regard to the issue of assurance levels:

- It could be helpful to specify assurance levels in the Annex. Some delegations suggested, as an alternative, that the assurance levels could be specified in the relevant implementing acts, as part of the interoperability framework.
- Services should however not be linked to specific assurance levels
- Service providers should be free to choose the appropriate assurance levels based on their risk assessment.

10. Without prejudice to further discussions on details and to further fine-tuning, there was broad support for the following general principles that might be retained as a basis for the further development of cluster 1:

a) The scope of the Chapter should be limited initially to services provided by public sector bodies, while allowing Member States to recognise the notified eID means for the purposes of accessing private sector services on a voluntary basis. Some delegations would like to go even further and begin only with certain types of services offered by public sector bodies, which could be listed in an annex.

b) The setting of an interoperability framework and cooperation in support of interoperability and trust between national identification infrastructures. Many delegations highlighted that the interoperability framework should be based on existing experience (e.g. the STORK project). It should also be known how interoperability would operate in practice.

c) Technological neutrality in respect of national solutions for electronic identification.

d) Adequate provisions to address security breach affecting the e-Id scheme or authentication.

11. Among other issues that still need to be further discussed are, in particular, the issue of liability of the notifying Member State and/or of the party issuing the electronic identification or operating the authentication possibility, and the issue of 'direct' damage in the newly introduced Art. 7b, the issue of 'unambiguous attribution' of person identification data, the issue of the authentication free of charge (both Art. 6) or the issue of terminology relating to security assurance levels.

Cluster 2: Trust services - general provisions (articles 9-12) and supervision (articles 13-19),

12. The Irish Presidency provided a revised text for cluster 2. While acknowledging that the meaning of some provisions of the original text was not always clear, the Presidency focused on substantive issues. The main changes proposed in the section on general provisions include;- simplifying Art. 9 on liability and providing for a possibility of a limitation on liability; simplifying Art. 10 on trust service providers from third countries and introducing a reciprocity obligation, and; simplifying Art. 11 on data processing and protection.

While a number of delegations could support the introduction of a limitation on liability, others expressed certain doubts in that regard. In any event the provision will need to be further improved. Some delegations would like to complement the liability provision with a reference to the liability of users and/or third parties. Regarding trust service providers from third countries, some delegations wondered how the verification that the necessary requirements are met could be carried out. Others would like to make sure that trust service providers from third countries are not treated any differently to those established in the Union as long as they comply with the Regulation. Moreover, with regard to the use of pseudonyms in Art. 11(4), views were expressed that the use of a pseudonym should not prevent the identity of the person behind the pseudonym being made known when legally required.

13. With regard to the main changes in the section on supervision, the Presidency made an effort to streamline and clarify the provisions concerning the supervision (Art. 13) and mutual assistance (Art. 14). The Presidency also aligned certain terminology used in Article 15 on security requirements for trust service providers with the Regulation 765/2008 on accreditation and market surveillance[5]. Furthermore, the Presidency suggested, at the request of many delegations, to reverse the order of events in relation to the initiation of qualified trust service providers in Art. 17. According to the revised text, qualified trust service providers may start providing qualified trust services only after the verification of compliance by the supervisory body.

While the above changes will need to be further discussed and/or developed, delegations expressed other concerns that will also need to be addressed. Most delegations suggested that the section on supervision should only apply to qualified trust service providers since it would be too burdensome and costly to keep track of all non-qualified trust service providers. There were also suggestions to restructure the section in order to separate clearly the requirements for trust service providers from the tasks of the supervisory body. Other questions include issues such as the appropriate time limit for the notification of security breaches (Art. 15(2)) or making sure that such notification obligation does not conflict with similar obligations imposed by other legislative acts.

[5] OJ L 218, 13.8.2008, p. 30

Cluster 3: Electronic Signature (articles 20-27, Annexes I and II)

14. Delegations provided a substantial number of comments on cluster 3. Some delegations would prefer to keep the relevant wording of the Directive 1999/93 on electronic signatures. Some delegations raised concerns with regard to the effects that some provisions (Art. 20, 28, 34) might have on national civil and procedural law. The views are split on whether the recognition of qualified electronic signatures should be recognised only by public or also by private entities. Some delegations believe that the wording of Art. 20(4) on the recognition of electronic signatures with a security assurance level below qualified electronic signature causes confusion between electronic signatures and electronic identification as it refers to 'accessing a service online'. Some delegations propose that qualified electronic signature creation devices have to be certified with regard to international security standards. Also, there is disagreement on whether Art. 20(4) should only apply to qualified electronic signatures. If this is not the case, then proper safeguards, such as specifying security assurance levels in the Regulation, might be necessary as suggested by few delegations. Some delegations asked for a provision on suspension of qualified certificates for electronic signatures since the proposal only deals with revocation at the moment. Among other matters, delegations also discussed e.g. whether the certification of qualified electronic signature devices should be mandatory or optional (Art. 23) or made various suggestions on how to improve requirements for qualified certificates for electronic signatures in Annex I.

Cluster 4: Other trust services (articles 28-37, Annexes III and IV)

15. Many delegations' comments made on the provisions regarding electronic signatures apply also to the provisions on electronic seals (Art. 28 and 29) (such as e.g. preference for some of the relevant wording of the Directive 1999/93 used mutatis mutandis, recognition of qualified electronic seals by public vs. private entities, recognition of electronic seals with security assurance level below qualified etc.). Many delegations have issues with the provisions on electronic documents (Art. 34). While some question the need to have such a provision in the Regulation at all, others point to the fact that an electronic document is not a trust service and therefore does not belong under this Chapter. Some delegations ask for the concept of electronic document and also electronic delivery (Art. 35 and 36) to be clarified and warn of possible interoperability problems. Several delegations questioned the added value of the provisions on website authentication (Art. 37).

Cluster 5: general provisions (art. 1-4) and final provisions, including delegated and implementing acts (art. 38-42)

16. Delegations would like to see improvements with regard to the subject matter (Art. 1) and scope (Art. 2), for which suggestions were made. With regard to the definitions (Art. 3), there is a consensus that they have to be clarified and improved. The most questioned definition is that of 'trust service', as it also has an impact on the scope of the proposal. Delegations also suggested adding other definitions, such as definition of 'online services', 'qualified validation services', 'preservation of qualified electronic signatures', and others. Most delegations were sceptical about the use of delegated acts throughout the proposal, especially taking into account the suggested legal form. Some indicated, however, that they were not opposed to delegated acts in principle. A number of delegations indicated that the content of those acts should be known before the entry into force of the Regulation. Regarding the legal form, it should be noted that one delegation is still not convinced that a Regulation is the appropriate legal instrument. Many delegations asked for a longer period of time before the entry into force of the proposed Regulation (Art. 42).

*

* *

Following its consideration by Coreper on 28 May, the Presidency presents this progress report to Council with the invitation to take note of it.