



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 3 December 2012

17126/12

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

**TELECOM 239
MI 800
DATAPROTECT 139
EJUSTICE 85
CODEC 2889**

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
- *Progress report and exchange of views*

1. *On 4 June 2012, 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.*
2. *The Working Party on Telecommunications and the Information Society is in the process of examining the proposal. In order to inform Ministers about the progress made to date and to identify issues requiring further discussion, the Presidency has put together the attached progress report (Annex I).*
3. *In order to structure the foreseen Ministerial exchange of views on the proposal at the TTE Council on 20 December 2012, the Presidency has drafted the attached questions (Annex II).*
4. *The Coreper/Council are invited to take note of the progress report set out in Annex I. The Council will be invited to address the questions set out in Annex II.*

Progress report on the proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market

1. 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 existing EU legislation, namely *Directive 1999/93/EC on a Community framework for electronic signatures*, essentially only covers electronic signatures and, currently, there is no comprehensive EU legal framework for electronic identification and authentication. The revision of the Directive and the establishment of a legal framework for mutual recognition of electronic identification and authentication across Europe are two of the key actions identified by the Digital Agenda for Europe. Moreover, these proposals are also flagged in the Single Market Act and the EU's Roadmap to Stability and Growth. The European Council has called, on several occasions, for a rapid progress on this proposal.

2. After first presentations of the proposal and of its impact assessment in June and July 2012, the Council Working Party on Telecommunications and the Information Society (hereinafter: WP TELE) carried out an in-depth examination of the proposal in several meetings under the Cyprus Presidency. Although delegations generally welcomed the proposal and acknowledged its importance for the Digital Single Market the discussions have identified many issues of both general and technical nature that must be thoroughly analysed further. Moreover, it has to be born in mind that the complexity of the proposal requires substantial coordination efforts at national level, which will, in most cases, involve several ministries and administrative departments.

3. On the basis of the discussions in the WP TELE and delegations' written comments, the Cyprus Presidency put together the present progress report in order to inform Ministers about the progress made to date and to summarise and draw attention to difficult issues in the proposal. The progress report should contribute to the development, under the Irish Presidency, of Council position on the text also in the light of the positioning of the European Parliament.
4. In the European Parliament, Ms Marita Ulvskog (ITRE committee) has been appointed as the rapporteur and IMCO, LIBE and JURI committees are expected to deliver opinions. The indicative timetable for the rapporteur's report is currently in preparation.

2. THE COMMISSIONS PROPOSAL

1. In its proposal, the Commission seeks to ensure mutual recognition and acceptance of electronic identification across EU and to give legal effect and mutual recognition to trust services. The proposal aims at enhancing current rules on electronic signatures and at providing a legal framework for other trust services, such as electronic seals, time stamping, electronic document acceptability, electronic delivery and website authentication.

2. Electronic identification (Chapter II of the proposal)

Electronic identification (eID) is the process of determining identity of a person or an entity via electronic means. Many Member States have introduced some sort of an eID system; however, these systems diverge to a high degree. The proposal does not aim at direct harmonisation of Member States' eID systems but requires mutual recognition of various national eID means.

Mutual recognition should apply to eID means issued under a scheme that has been notified by a Member State to the Commission and subsequently included in the list of notified schemes published in the *Official Journal*.. The decision whether to notify a system lies purely with the Member States in question. The proposal sets out eligibility requirements for notification and lays down rules for the notification procedure.

Moreover, the proposed Regulation requires Member States to cooperate in order to ensure interoperability and security of eID means.

3. Trust services (Chapter III of the proposal)

The proposed Regulation contains a number of general provisions applicable to all trust services. These provisions cover, among others, liability of trust service providers, recognition of qualified trust services provided by providers established in third countries, data protection issues and accessibility of trust services for disabled people.

4. With regard to supervision, the proposal obliges Member States to establish supervisory bodies, sets out their tasks and provides for a mechanism of mutual assistance between them. It obliges trust service providers to adopt measures to manage security risks and introduces notification requirements with regard to security breaches. Qualified trust service providers are subject to additional requirements and to the obligation of regular auditing. The proposal sets out the procedure for the initiation of the provision of qualified trust services and the respective role of the supervisory bodies therein. Furthermore, it lays down rules on management of trusted lists containing information on qualified trust service providers in each Member State.

5. The proposed Regulation builds upon and enhances the current legal framework for electronic signature (e-signature) and replaces the existing Directive 1999/93/EC. The proposal provides the rules related to the legal effect of natural person's e-signature and introduces an obligation to give to qualified e-signatures the same legal effect as to handwritten signatures. Member States must ensure the cross-border acceptance of qualified e-signatures in the context of the provision of public services, and they must not introduce any additional requirements. Furthermore, the proposal sets out requirements on qualified e-signatures certificates and provides rules on qualified e-signature creation devices, the corresponding certification procedure and lists. Finally, it lays down requirements and conditions for validation and for long term preservation of qualified e-signatures.

6. Next to the rules on electronic signature, the proposal provides a basic legal framework for other trust services. The proposal lays down rules on legal effects and admissibility in legal proceedings of electronic seals, electronic time stamping, electronic documents and electronic delivery and sets out a specific legal presumption and acceptance obligation of Member States for these services if they are qualified. Moreover, the proposed Regulation sets out requirements for qualified certificates for website authentication and stipulates that they should be recognised in all Member States.

3. MAIN GENERAL REACTIONS OF THE DELEGATIONS

1. It is the Presidency's understanding that the objectives of the Commission proposal are, in principle, welcome by delegations. However, a number of issues have emerged from the discussions at the WP TELE and will require further in-depth consideration. This report is without prejudice to particular points of interest and more detailed comments of individual delegations or provisions included in the proposal which have not yet been fully addressed in the WP TELE.
2. Delegations addressed a great number of questions, concerns and requests for clarification to the Commission. The Commission made an effort to address them at the WP TELE or via several non-papers. However, many issues remain unclear and will require further analysis and clarifications.
3. With regard to general issues, delegations had concerns about the complexity of the proposal and called for more legal certainty and clarity. Many delegations inquired about the impact of the proposal on existing national legislation and about the expected cost of putting the new system into place. Delegations sought clarifications on how to solve technical and organisational aspects of interoperability and how to achieve comparable security levels throughout the EU. Delegations pointed out the need to respect technological neutrality in the proposal and to ensure appropriate safeguards for personal data. Last but not least, most delegations had concerns about the abundant use of delegated and implementing acts throughout the proposal.

4. At the beginning of the examination of the proposal, many delegations expressed concerns about the choice of the legal instrument - Regulation as opposed to a Directive or a Decision. In addition, some delegations had doubts if electronic identification and electronic signature should be covered in a single piece of legislation. However, after the Commission addressed these issues in a non-paper, it seems that most delegations can support a single Regulation as an appropriate legal instrument, although some doubts still persist.
5. The WP TELE examined the concrete legislative provisions of the proposal on the basis of the following clusters, covering the main elements of the proposal:
- Cluster 1: General provisions (Chapter I)
 - Cluster 2: Trust services (Chapter III)
 1. General provisions (Section 1)
 2. Supervision (Section 2)
 3. Electronic signature (Section 3)
 4. Other trust services (Sections 4 to 8)
 - Cluster 3: Electronic identification (Chapter II)
 - Cluster 4: Delegated acts, implementing acts and final provisions (Chapters IV, V, VI) and preamble.

The principal reactions of delegations on these clusters are given below.

Cluster 1: General provisions (articles 1 - 4)

6. Delegations called for rephrasing of provisions on the subject matter and scope of the proposed Regulation in order to achieve more clarity and legal certainty. Some delegations suggested that more objectives related to the subject matter (such as building trust or proper functioning of e-government systems) be spelled out in Article 1. Delegations sought clarifications about the meaning of the phrases 'provided by, on behalf or under the responsibility of Member States' and 'based on voluntary agreements under private law' in Article 2 and questioned, in this respect, whether and how the proposed Regulation would apply to the private sector.

7. Delegations inquired why many definitions existing in the current legal framework have been changed. They asked for clarification or rephrasing of many of them and suggested that more definitions should be included. Some delegations pointed to the fact that many definitions refer to natural or legal persons, the notion of which might differ between Member States and could possibly be clarified in the proposal. The application of the proposal to entities without legal personality could also be considered.

Cluster 2: Trust services

8. With regard to all provisions concerning trust services, delegations insisted that the text should be made more precise and that ambiguous and unclear language should be avoided.

General provisions (articles 9 - 12)

9. Many delegations shared the view that the liability of trust service providers should be limited since unlimited liability might act as a disincentive to the development of the trust service industry. Some delegations sought clarity on how a determination will be made that trust service providers from third countries meet the requirements, which EU established trust service providers must meet. Some delegations had doubts how to find the right balance between the respect for privacy and the need for trust and confidence in cases when a pseudonym is used. With regard to access for persons with disabilities, some delegations inquired about the meaning of 'whenever possible' in Article 12.

Supervision (articles 13 - 19)

10. The majority of the delegations agreed that the proposal should be more precise regarding the tasks, powers, means and relevant procedures of the supervisory body and some feared of possible overlaps with other legislative proposals (such as those on data protection or cyber security). Some delegations sought explanations on how a designated supervisory body established in another Member State could act 'under the responsibility of the designating Member State'. Many delegations shared concerns with regard to the fact that non-qualified trust service providers would be subject to the monitoring activities of the supervisory body. Many delegations appeared to be sceptical regarding the extent of the reporting obligation.

11. Delegations asked for more information, and possibly a definition, of the ‘recognized independent body’ carrying out security audits of trust service providers. Delegations also discussed whether or not the audit obligation should apply to non-qualified providers. Some delegations considered the requirement of submitting a yearly security audit report for qualified trust service providers too burdensome and/or costly whereas others thought that the audit should not only focus on security requirements but should cover all the obligations. Many delegations questioned the principle that qualified trust service providers may start providing services once they have submitted their notification, meaning before the respective verification by the supervisory body has been concluded.
12. Some delegations mentioned that it is not entirely clear which body would be responsible for verifying the compliance of qualified trust service providers and qualified trust services provided by them with the requirements of the Regulation. With regard to requirements for qualified trust service providers, delegations sought clarifications on many issues, e.g. on verification of identity of the person to whom the certificate is issued and on the revocation policy. Some delegations were of the opinion that at least some of the provisions on requirements for (qualified) trust service providers should not be dealt with in the section concerning the supervision.

Electronic signature (articles 20 - 27)

13. Delegations sought clarifications on legal effects of e-signatures in legal proceedings and about the possible impact on national procedural law. Many delegations inquired about the practical implications of the phrase 'shall be recognised and accepted in all Member States' (Article 20(3)). Delegations also had concerns with regard to the acceptance of e-signatures of a lower security assurance level and were of the opinion that, as security levels constitute an essential element of the proposal, they should not be left to delegated acts. More clarity was sought with regard to validation and preservation of qualified e-signatures and the terminology and wording used in the respective provisions. A number of delegations would welcome definitions of validation and preservation to be included in the proposal.

Other trust services (articles 28 - 37)

14. On the issue of electronic seals, many delegations argued that the concept should be clarified and more details provided in the proposal. In particular, delegations felt that the scope of use, acceptance and effect of electronic seals on third parties should be stated more clearly. Some delegations questioned the added value of the provisions on electronic seals as such. There was an uncertainty if electronic seals should be understood as means to identify legal persons and some delegations raised the issue of extending the use of electronic seals to entities that do not have legal personality, e.g. political parties. Some delegations proposed that Annex II, which describes the requirements for qualified certificate of electronic seals, should include a unique identifier 'subject serial number' as a means to unambiguously identify the legal person. Many delegations' comments on e-signatures apply *mutatis mutandis* to electronic seals.
15. With regard to electronic documents some delegations questioned the added value of the relevant articles as they felt that certain rules on electronic documents might already follow from articles 20 and 28. Delegations were uncertain to what extent electronic documents would be admissible in legal proceedings and about the possible assessment by the court of integrity and authenticity of those documents.
16. In relation to website authentication, delegations also questioned the added value of such provisions. Some delegations sought clarification on how those provisions should be implemented in practice and why a certificate for website authentication may only be issued to legal persons.

Cluster 3: Electronic identification (articles 5 - 8)

17. The majority of delegations welcomed the initiative to provide a legal framework for mutual acceptance of eID means. The delegations emphasized, however that the text of the proposal is complex and calls for more legal certainty and clarity.

18. Many delegations expressed concerns in relation to the *rationale* of the proposal requiring all relying parties to accept all notified eIDs regardless the security levels applied. A number of delegations proposed that harmonized “minimum security levels” should be clearly stated in the proposal, the adherence to which would make eID schemes eligible to be notified by the respective Member State. Defining a minimum level of security would prevent the mutual recognition mechanism from compromising a high-security national system with a weaker system from another Member State.
19. Many delegations questioned whether or not the provision for mutual recognition and acceptance of eIDs applies not only to electronic identity of natural persons but also to electronic identity of legal persons or other entities. To this respect, delegations expressed the view that the scope of application should be explicitly stated in the proposal.
20. Delegations had concerns in relation to the technical implementation of the provisions on eID and its possible impact in terms of time required and costs for the all the players involved. A number of delegations could support a gradual approach to the implementation, and emphasized that the six months timeframe set out in article 7 is too short for eID suppliers to adapt. The issue of technical interoperability is of the utmost importance in this respect.
21. Many delegations inquired about the impact of the proposed Regulation on the existing national systems and business models and about the application to sectoral (e.g. eHealth) eID cards. Moreover, there is a need to make sure that systems already introduced in Member States could be notified.
22. With regard to the liability of Member States as set out in Article 6 (e), discussions focused on the extent, consequences and practical implementation of the liability. Many delegations were of the opinion that this provision goes too far and the liability should be limited. Many delegations asked for a clear definition of what “unambiguous attribution” encompasses. Some delegations were not convinced about providing authentication services for free.

23. Delegations appeared to be uncertain as to whether private providers can also be eligible to notification pursuant to Article 7. In this respect, some delegations asked for an explanation of what “on behalf of or under the responsibility of the notifying Member State” in article 6 (a) means. Delegations were also sceptical in relation to the possibility of States to assume liability for the negligent behaviour of private providers.

Cluster 4: Delegated acts, implementing acts and final provisions (articles 38 - 42)

24. Delegations were concerned about the extensive reference, throughout the Regulation, to delegated acts. They suggested that the use of delegated acts be limited to supplement or amend non-essential elements of a more technical character and were of the opinion that it was not, in fact, always the case in the proposal. Some delegations would prefer to use implementing acts instead. Moreover, many delegations pointed out that the implementation of the proposed Regulation would be complicated if the necessary delegated and implementing acts were not in place when the Regulation become applicable.
25. Delegations also expressed concerns with regard to the implementation time-frame and the transition between the repeal of the current Directive and the entry into force of the Regulation. The proposed Regulation is supposed to enter into force and become applicable 20 days after the publication in the Official Journal, which many delegations consider unrealistic. Delegations therefore suggested applying appropriate transition periods to allow the sector to adapt to the new legislation. A gradual approach could also be envisaged.

Questions for the exchange of views
at the TTE Council on 20 December 2012

The proposed legal framework seeks to enable secure and seamless electronic interactions between businesses, citizens and public authorities, thereby increasing the effectiveness of cross-border online services, e-business and electronic trade in the EU. It is expected to contribute substantially to the achievement of a fully integrated digital single market. The European Council has repeatedly called for a swift adoption of this proposal.

- **Bearing in mind the scope and complexity of the proposed Regulation that covers e-identification, e-signatures and other trust services, how do you assess the feasibility of a rapid progress on this piece of legislation and on which issues should efforts be focused in order to secure this progress?**

The system of mutual recognition as proposed by the Regulation is based on trust and cooperation between Member States and no minimum security requirements are laid down in the Regulation. However, as indicated in the progress report set out in Annex I, security levels differ greatly throughout Europe and many Member States, and in particular those having high-security national systems, are clearly concerned about the possible compromising effect that the mutual recognition mechanism could have.

- **In the light of the above, would you agree that setting the harmonised minimum security levels in the proposed Regulation would effectively address these concerns and would help to ensure adequate security of cross-border transactions throughout the EU?**
