Axel Pawlik
Managing Director
RIPE Network Coordination Centre (RIPE NCC)
Singel 258
1016AB Amsterdam
The Netherlands

17 June 2013

Dear Sir/Madam

**Re. Amendments to Proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market [EUR-Lex Ref. 52012PC0238]**

The RIPE NCC is Regional Internet Registry for the Europe, the Middle East and parts of Central Asia, and facilitates the bottom-up policy development process of the RIPE community. This advice is offered on behalf of the RIPE NCC, and reflects concerns raised by members of the RIPE community.

At the recent RIPE Meeting in Dublin, Mr. Andrea Servida of the European Commission delivered a presentation that explained the proposed Regulation on electronic identification and trust services for electronic transactions in the internal market. Video and transcript of the session are available: https://ripe66.ripe.net/programme/meeting-plan/coop-wg/

Based on this presentation and the discussions that it provoked, the RIPE NCC has identified a number of serious concerns with the proposal, and we believe that the current proposal text may be interpreted in ways that conflict with the basic intent of the Regulation.

Specifically, we believe that the proposal could be interpreted as applying to technologies and services beyond electronic identification (eID) and eID-related trust services, perhaps extending to cover unrelated technologies to eID such as Domain Name Security Extensions (DNSSEC) and Resource Public Key Infrastructure (RPKI).

Such a broad scope would be contrary to what we understand is the intent of the Regulation, and in contradiction of other statements made by the European Commission regarding Internet regulation. More importantly, it could inhibit ongoing efforts by the Internet technical community in the EU (often in collaboration with colleagues and counterparts around the world) to secure the infrastructure of the Internet.

The RIPE NCC has identified three major areas of concern with the proposed Regulation:

1. Scope
The regulation should only cover eID and with eID-related trust services. We note that protocols and technical standards for securing communication, such as those used to secure computer and telecommunication networks, are managed very differently from security arrangements related to eID. Over-reach by the Regulation could have significant implications for global network security efforts.

2. Trust
All modern trust mechanisms rely on so-called "chains of trust", which are validated automatically. The proposed Regulation's requirement for lists of qualified trust providers would actually hinder the important, ongoing evolution of Internet security mechanisms. It may also result in conflicts arising between the "trusted list" and the digital chain of trust, which would have serious security implications.

3. Requirements
The proposed Regulation details explicit requirements for the provision of security trust services. Currently security requirements and specifications are adopted through bottom up procedures and are codified in standards created by bodies like the IETF, IEEE, ETSI or ISO.

Rather than creating such a rigid framework of requirements, the Regulation should refer to existing processes for establishing trust services, thereby accommodating the need for evolution of these processes and the technology over time.

We have attached a document that lays out some specific suggestions for changes to the wording of the Regulation.

The RIPE NCC would be happy to provide further information on any of these concerns if that would be helpful, and we would be happy to coordinate a face-to-face discussion with RIPE NCC staff or RIPE community members.

Best regards,

Axel Pawlik
Managing Director, RIPE NCC

Notes

**RIPE** (Réseaux IP Européens) is a collaborative forum open to all parties interested in wide area IP networks in Europe and beyond. The objective of RIPE is to ensure the administrative and technical coordination necessary to enable the operation of the Internet, including the bottom-up development of policy relating to the management and distribution of Internet number resources (IPv4, IPv6 and Autonomous System Numbers).

The **RIPE NCC** (RIPE Network Coordination Centre) was established in 1992 by the RIPE community to serve as an administrative body and as Regional Internet Registry (RIR) for Europe, the Middle East and parts of central Asia. It provides administrative support to RIPE and fulfills a number of technical roles, including operation of the RIPE Database and management of the k-root name server.

**APPENDIX: Proposed text amendments**

Recital 17

| Current text | Proposed text |
|---|---|
| (17) This Regulation should also establish a general legal framework for the use of electronic trust services. However, it should not create a general obligation to use them. In particular, it should not cover the provision of services based on voluntary agreements under private law. Neither should it cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Union law. | (17) This Regulation should also establish a general legal framework for the use of electronic trust services **that are related to electronic identification**. However, it should not create a general obligation to use them. In particular, it should not cover the provision of services based on voluntary agreements under private law. Neither should it cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Union law. |

Recital 19

| Current text | Proposed text |
|---|---|
| (19) Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services. | (19) Member States should remain free to define other types of **electronic identification related to** trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services. |

**Justification for amendments to Recitals 17 and 19**: It should be specified that the Regulation only covers services related to electronic identification.

Recital 35

| Current text | Proposed text |
|---|---|
| (35) It is the responsibility of trust service providers to meet the requirements set out in this Regulation for the provisioning of trust services, in particular for qualified trust services. Supervisory bodies have the responsibility to supervise how trust service providers meet these requirements. | (35) **Security requirements and specifications are adopted as technical standards in technical fora through bottom up procedures.** It is the responsibility of trust service providers to meet the requirements set out in **these technical standards** ~~this Regulation for the provisioning of trust services, in particular for qualified trust services~~. Supervisory bodies have |

| | |
|---|---|
| | the responsibility to supervise how trust service providers meet these requirements. |

**Justification for amendments to Recital 35**: Security requirements are being discussed and established in technical forums such as the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE). The Regulation should not establish specific requirements that providers are obliged to follow; rather it should refer to existing mechanisms for the development of security requirements, and could oblige providers to follow the requirements adopted through these processes.

Recital 36

| Current text | Proposed text |
|---|---|
| (36) In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with the view of facilitating the due diligence leading to the provisioning of qualified trust services. | (Delete) |

Recital 37

| Current text | Proposed text |
|---|---|
| (37) Trusted lists are essential elements to build trust among market operators as they indicate the qualified status of the service provider at the time of supervision, on the other hand they are not a prerequisite for achieving the qualified status and providing qualified trust services which results from respecting the requirements of this Regulation. | (Delete) |

Recital 38

| Current text | Proposed text |
|---|---|
| (38) Once it has been subject to a notification, a qualified trust service | (Delete) |

| | |
|---|---|
| cannot be refused for the fulfilment of an administrative procedure or formality by the concerned public sector body, for not being included in the trusted lists established by the Member States. For the present purpose a public sector body refers to any public authority or other entity entrusted with the provision of eGovernment services such as online tax declaration, request for birth certificates, participation to electronic public procurement procedures, etc. | |

**Justification for amendments in recitals 36, 37 and 38:** Today's security mechanisms rely on a system of digital chain of trust. Establishing trust lists may conflict with the current mechanism, hinter the security systems evolution and create confusion and mistrust to users.

Recital 48

| Current text | Proposed text |
|---|---|
| (48) Making it possible to authenticate websites and the person owning them would make it harder to falsify websites and thus reduce fraud | (Delete) |

**Justification for amendments to Recital 48**: The authentication of websites is a matter of global impact and should not be regulated at EU level.

Recital 51

| Current text | Proposed text |
|---|---|
| (51) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards which use would give a presumption of compliance with certain requirements laid down in this Regulation or defined in delegated acts. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 | (51) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards which use would give a presumption of compliance with **current technical standards, as developed through bottom up standards development procedures** ~~certain requirements laid down in this Regulation or defined in delegated acts~~. Those powers should be exercised in |

| | |
|---|---|
| laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[24]. | accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[24]. |

**Justification for amendments to Recital 51**: In line with the amendment in Recital 35.

Article 1, paragraph 1

| Current text | Proposed text |
|---|---|
| 1. This Regulation lays down rules for electronic identification and electronic trust services for electronic transactions with a view to ensuring the proper functioning of the internal market. | 1. This Regulation lays down rules for electronic identification and **associated** electronic trust services for electronic transactions with a view to ensuring the proper functioning of the internal market. |

**Justification for amendments to Article 1**: In line with the proposed amendments in Recitals 17 and 19.

Article 3, sections (12) and (20)
(Definitions)

| Current text | Proposed text |
|---|---|
| For the purposes of this Regulation, the following definitions shall apply:<br>(12) 'trust service' means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals; | For the purposes of this Regulation, the following definitions shall apply:<br>(12) 'trust service' means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic **identification as referred to in this Article, and in particular** signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, ~~website authentication,~~ and electronic certificates**, as defined in this Article** ~~including certificates for electronic signature and for electronic seals;~~ |

**Justification for amendments to Article 3, section 12**: The scope of trust services should be limited to eID related services only, as intended. Website authentication should be outside of the scope of the Regulation as explained in with our proposed amendments to Recital 48. The amendment proposed with regards to the electronic certificates is in line with the definition of the electronic certificate in Article 3, which refers exclusively to certificates for electronic signatures and electronic seals.

| Current text | Proposed text |
|---|---|
| (20) 'electronic seal' means data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data; | (20) 'electronic seal' means data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data **and serve as evidence that an electronic document is issued by a legal person**; |

**Justification for amendments to Article 3, section 20**: This amendment is in line with Recital 43, which clarifies that electronic seals should be used in relation to electronic documents.

Article 13
(Supervisory body)

| Current text | Proposed text |
|---|---|
| 2. The supervisory body shall be responsible for the performance of the following tasks:<br>(a) monitoring trust service providers established in the territory of the designating Member State to ensure that they fulfil the requirements laid down in Article 15;<br>(b) undertaking supervision of qualified trust service providers established in the territory of the designating Member State and of the qualified trust services they provide in order to ensure that they and the qualified trust services provided by them meet the applicable requirements laid down in this Regulation;<br>(c) ensuring that relevant information and data referred to in point (g) of Article 19(2), and recorded by qualified trust service providers are preserved and kept accessible after the | 2. The supervisory body shall be responsible for the performance of the following tasks:<br>(a) monitoring trust service providers established in the territory of the designating Member State to ensure that they fulfil the requirements laid down in Article 15;<br>(b) undertaking supervision of qualified trust service providers established in the territory of the designating Member State and of the qualified trust services they provide in order to ensure that they and the qualified trust services provided by them meet the applicable **current technical standards as developed through bottom up procedures** ~~requirements laid down in this Regulation;~~<br>(c) ensuring that relevant information and data referred to in point (g) of |

| | |
|---|---|
| activities of a qualified trust service provider have ceased, for an appropriate time with a view to guaranteeing continuity of the service. | Article 19(2), and recorded by qualified trust service providers are preserved and kept accessible after the activities of a qualified trust service provider have ceased, for an appropriate time with a view to guaranteeing continuity of the service. |

Article 15
(Security requirements applicable to trust service providers)

| Current text | Proposed text |
|---|---|
| 1. Trust service providers who are established in the territory of the Union shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to state of the art, these measures shall ensure that the level of security is appropriate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents.<br>Without prejudice to Article 16(1), any trust service provider may submit the report of a security audit carried out by a recognised independent body to the supervisory body to confirm that appropriate security measures have been taken.<br>2. Trust service providers shall, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.<br>Where appropriate, in particular if a | 1. Trust service providers who are established in the territory of the Union shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. ~~Having regard to state of the art, these measures shall ensure that the level of security is appropriate to the degree of risk.~~ **In particular Trust service providers shall comply with current technical standards as developed through bottom up procedures** ~~measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents.~~<br>~~Without prejudice to Article 16(1), any t~~**T**rust service provider may submit the report of a security audit carried out by a recognised independent body to the supervisory body to confirm that appropriate security measures **in compliance with these technical standards** have been taken.<br>~~2. Trust service providers shall, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities of any breach of security or loss of integrity that has a~~ |

| | |
|---|---|
| breach of security or loss of integrity concerns two or more Member States, the supervisory body concerned shall inform supervisory bodies in other Member States and the European Network and Information Security Agency (ENISA).<br>The supervisory body concerned may also inform the public or require the trust service provider to do so, where it determines that disclosure of the breach is in the public interest.<br>3. The supervisory body shall provide to ENISA and to the Commission once a year with a summary of breach notifications received from trust service providers.<br>4. In order to implement paragraphs 1 and 2, the competent supervisory body shall have the power to issue binding instructions to trust service providers.<br>5. The Commission shall be empowered to adopt delegated acts, in accordance with Article 38, concerning the further specification of the measures referred to in paragraph 1.<br>6. The Commission may, by means of implementing acts, define the circumstances, formats and procedures, including deadlines, applicable for the purpose of paragraphs 1 to 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). | ~~significant impact on the trust service provided and on the personal data maintained therein.~~<br>~~Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the supervisory body concerned shall inform supervisory bodies in other Member States and the European Network and Information Security Agency (ENISA).~~<br>~~The supervisory body concerned may also inform the public or require the trust service provider to do so, where it determines that disclosure of the breach is in the public interest.~~<br>**2**~~3~~. The supervisory body shall provide to ENISA and to the Commission once a year with a summary of breach notifications received from trust service providers.<br>**3**~~4~~. In order to implement paragraph~~s~~ 1~~ and 2~~, the competent supervisory body shall have the power to issue binding instructions to trust service providers.<br>~~5. The Commission shall be empowered to adopt delegated acts, in accordance with Article 38, concerning the further specification of the measures referred to in paragraph 1.~~<br>**4**~~6~~. The Commission may, by means of implementing acts, define the circumstances, formats and procedures, including deadlines, applicable for the purpose of paragraphs 1 ~~to 3~~ **and 2**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). |

**Justification for amendments to Articles 13 and 15**: In line with the amendments in Recital 35, providers have to comply with requirements based on current technical standards with supervisory bodies acting to ensure this compliance. Also reporting incidents is a matter to be covered by another proposed legislation (i.e. Proposal for a Directive of the European Parliament and of the Council Concerning measures to

ensure a high level of network and information security across the Union [COM (2013) 48]).

Article 16 paragraph 4
(Supervision of qualified trust service providers)

| Current text | Proposed text |
|---|---|
| 4. With reference to paragraph 3, if the qualified trust service provider does not remedy any such failure within a time limit set by the supervisory body, it shall lose its qualified status and be informed by the supervisory body that its status will be changed accordingly in the trusted lists referred to in Article 18. | 4. With reference to paragraph 3, if the qualified trust service provider does not remedy any such failure within a time limit set by the supervisory body, it shall lose its qualified status and be informed by the supervisory body that its status will be changed ~~accordingly in the trusted lists referred to in Article 18~~. |

Article 17 Paragraphs 2-5
(Initiation of a qualified trust service)

| Current text | Proposed text |
|---|---|
| 2. Once the relevant documents are submitted to the supervisory body according to paragraph 1, the qualified service providers shall be included in the trusted lists referred to in Article 18 indicating that the notification has been submitted.<br>3. The supervisory body shall verify the compliance of the qualified trust service provider and of the qualified trust services provided by it with the requirements of the Regulation.<br>The supervisory body shall indicate the qualified status of the qualified service providers and the qualified trust services they provide in the trusted lists after the positive conclusion of the verification, not later than one month after the notification has been done in accordance with paragraph 1.<br>If the verification is not concluded within one month, the supervisory body shall inform the qualified trust service provider specifying the reasons of the delay and the period by which the verification shall be concluded.<br>4. A qualified trust service which has | (Delete) |

| | |
|---|---|
| been subject to the notification referred to in paragraph 1 cannot be refused for the fulfilment of an administrative procedure or formality by the concerned public sector body for not being included in the lists referred to in paragraph 3.<br>5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures for the purpose of paragraphs 1, 2 and.3 Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). | |

Article 18
(Trusted lists)

| Current text | Proposed text |
|---|---|
| 1. Each Member State shall establish, maintain and publish trusted lists with information related to the qualified trust service providers for which it is competent together with information related to the qualified trust services provided by them.<br>2. Member States shall establish, maintain and publish, in a secure manner, electronically signed or sealed trusted lists provided for in paragraph 1 in a form suitable for automated processing.<br>3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificate used to sign or seal the trusted lists and any changes thereto.<br>4. The Commission shall make available to the public, through a secure channel, the information, referred to in paragraph 3 in electronically signed or sealed form | (Delete) |

| | |
|---|---|
| suitable for automated processing.<br>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the definition of the information referred to in paragraph 1.<br>6. The Commission may, by means of implementing acts, define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). | |

**Justification for amendments in Articles 16, 17 and 18:** In line with amendments in Recitals 36, 37 and 38, technical validation of trust providers is not done through trust lists but electronically, via "chain of trust".

Article 37
(Requirements for qualified certificates for website authentication)

| Current text | Proposed text |
|---|---|
| 1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.<br>2. Qualified certificates for website authentication shall be recognised and accepted in all Member States.<br>3. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the further specification of the requirements laid down in Annex IV.<br>4. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall | (Delete) |

| | |
|---|---|
| publish those acts in the Official Journal of the European Union. | |

ANNEX IV
(Requirements for qualified certificates for website authentication)

| Current text | Proposed text |
|---|---|
| Qualified certificates for website authentication shall contain:<br>(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;<br>(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and<br>– for a legal person: the name and registration number as stated in the official records,<br>– for a natural person: person's name;<br>(c) a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name and registration number as stated in the official records;<br>(d) elements of the address, including at least city and Member State, of the legal person to whom the certificate is issued as stated in the official records;<br>(e) the domain name(s) operated by the legal person to whom the certificate is issued;<br>(f) details of the beginning and end of the certificate's period of validity;<br>(g) the certificate identity code which must be unique for the qualified trust service provider;<br>(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;<br>(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free | (Delete) |

| | |
|---|---|
| of charge;<br>(j) the location of the certificate validity status services that can be used to enquire the validity status of the qualified certificate. | |

**Justification for amendments in Article 37 and ANNEX IV**: In line with amendments in Recital 48 and Article 3.