RIPE NCC Analysis of a European Commission Proposal for Regulation on Electronic Identification and Trust Services for Electronic Transaction in the Internal Market

17 June 2013

This paper examines:

- Whether Resource Public Key Infrastructure (RPKI, also known as Internet Resource Certification) or DNSSEC (Domain Name System Security Extensions) fall within the scope of the proposed Regulation
- Possible implications if RPKI or DNSSEC fall within the scope of the proposed regulation

1. RPKI or DNSSEC use covered by the Regulation

Whether RPKI or DNSSEC (the systems and their use) would fall under the proposed Regulation is not clearly indicated in the document. There are elements in the proposal that suggest that RPKI and DNSSEC could fall within its scope. These elements are the following:

1.1. Scope of the Regulation - Definition of "trust service"

The proposal provides that the Regulation should establish a general legal framework for the use of electronic trust services. [1]

Article 3 (12) of the Regulation defines:
'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;

RPKI or DNSSEC could be seen as an electronic service for the creation, verification, validation, handling and preservation of

- Website authentication, or
- Electronic certificates.

The proposal elaborates on these terms:

[1] Rationale 17. It is worth mentioning that Article 2 provides that the Regulation does not apply to the provision of electronic trust services based on voluntary agreements under private law. While this could be an argument that RPKI and DNSSEC are excluded as they are voluntary and under private law agreement, the Commission has indicated that this is not the intention of that article. As explained here [EURIM position paper on the proposal, ANNEX I, section 2, page 8 (http://dpalliance.org.uk/wp-content/uploads/2013/03/1303_Stakeholder-concerns-around-eID-Paper.pdf)] the EC exempts only services that do not potentially or actually implicate any third parties (i.e. which third parties cannot rely on).

- **Website authentication**

The Regulation intends to make *it possible to authenticate websites and the person owning them would make it harder to falsify websites and thus reduce fraud.* [2]

The EC explains this a bit further in the introductory document of the Regulation:[3]

Website authentication - This section is intended to ensure that the authenticity of a website with respect to the owner of the site will be guaranteed. Article 37 sets out the requirements for qualified certificates for website authentication, which can be used to guarantee the authenticity of a website. A qualified certificate for website authentication will provide a minimal set of trustworthy information on the website and on the legal existence of its owner.

The Commission, in its presentation of the proposal used the example of the SSL but given the "technical neutrality" spirit of the Regulation, both RPKI and DNSSEC can be seen as ways to guarantee the authenticity of a website with respect to its owner.

- **Certificate and electronic seal**

Art 3 (10) defines the term certificates:
'certificate' means an electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person;

If "certificate" refers only to validation data of e-signatures and e-seals, the question is whether RPKI and DNSSEC fall within this definition.[4] The definition of e-seals is the following:

'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 [5]

The Regulation in its Rationale explains that e-seals *should serve as evidence that an electronic document was issued by a legal person.*[6] However:

- This is only mentioned in a Rationale and not in the Regulation itself and
- The Rationale uses the modal "should", which is not as strict as the modals "shall" or "must".

Accordingly a broader interpretation of the e-seal, which may also include RPKI and DNSSEC, is possible.

---

[2] Rationale 48
[3] 3.3.3.8 Section 8
[4] E-signatures are related to natural persons only
[5] Art 3 (20)
[6] Rationale 43

Even if the references to e-seals do not cover RPKI or DNSSEC, the definition of "trust service" talks about certificates *including* the ones related to e-signatures and e-seals, as if this list is not exhaustive. It is thus not clear whether "certificate" is meant only in relation to e-signature and e-seals (as in the definition of certificates) or whether it can include more than that (as in the definition of trust services).

1.2. Additional types of trust services

Even if RPKI or DNSSEC are not meant to be included in any of the above definitions, the Rationale of the Regulation provides that *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.* [7]

Thus any Member State can decide that RPKI or DNSSEC are covered by this Regulation.

2. Implications if RPKI or DNSSEC within the scope

If RPKI or DNSSEC systems and their use are covered by the Regulation, the implications may include the following:

2.1. Eligibility

The Regulation is meant to ensure that *trust services and products which comply with this Regulation are permitted to circulate freely in the internal market.*[8]
This leaves some doubts about services and products not complying with the Regulation. Aren't these services and products permitted to circulate freely in the internal market?[9]

In particular relation to website authentication the Regulation governs only qualified website authentication, which provides some very strict requirements. Would that mean that any authentication not following these requirements is not allowed to circulate?

There is also a question about trust services providers that are not established within the Internal market? Are these services not permitted or eligible for public procurement?

2.2. List scheme

Trust service providers providing services that fulfill certain requirements can apply for their services to become "qualified".

Such applications are submitted to national supervisory bodies, which verify the compliance of the requirements. The verifications must be concluded no later

---

[7] Rationale 19
[8] Art 1 –Subject matter
[9] See also EURIM position paper on the proposal, ANNEX I, section 3, page 9 (http://dpalliance.org.uk/wp-content/uploads/2013/03/1303_Stakeholder-concerns-around-eID-Paper.pdf)

than one month after the submission but the supervisory body can delay the verification by informing the provider and specifying the reasons for the delay. All submissions are listed in “trusted lists” maintained by Member States.[10]

Qualified trust service providers must be audited by an independent body once a year to confirm that their requirements are still fulfilled and they must submit the audit report to the supervisory authority. Additionally, the supervisory authority can audit the provider at any time, either at their own initiative or at the Commission’s request. Supervisory authorities can issue binding instructions to remedy any failure to fulfill their requirements and the Commission can adopt specifications and procedures about the audits. Providers that are found to be no longer fulfilling their requirements are removed from the trust lists.

Such list schemes do not take into account the logic of "trust anchors", which is substantial for RPKI and DNSSEC. This could result in a provider serving the role of a "trust anchor" while not "qualified" as a trust service provider; meanwhile, a trust service provider serving as certificate authority for certificates based on this anchor may be "qualified". This may lead to a conflict of trust and will create uncertainty among network operators and users.

2.3. Security requirements

Trust service providers will be obliged to submit a report of a security audit carried out by a recognised independent body to a national supervisory authority. This report will confirm that the provider takes appropriate technical and organizational measures to manage risks to prevent and minimize the impact of security incidents and inform of adverse effect of any incidents.

Trust service providers are also obliged to notify the national supervisory authority for any breach of security within 24 hours after having become aware of the incident.

The Commission will be able to impose further specifications of the security measure the provider must take as well as procedures for the notification of security breaches. [11]

This is a big change. Currently security requirements and specifications are adopted through bottom up development processes and are codified in policies such as the ones created by IETF, IEEE, ETSI or ISO.

If this proposal is adopted, providers will be subject to national authorities and obliged to comply with their requests, which may contradict the requirements laid out in existing standards and restrict their ability to provide their services.

2.4. Liability

[10] Art 16,17,18
[11] Art 13 and Art 15

The Regulation provides that trust service providers are liable for any direct damage caused to any person due to a failure to comply with the obligations and requirements as set in the Regulation. [12]

This is a big change to the liability schemes according to which certificates are provided. Today, unless otherwise agreed by the parties, the affected person must prove that their damage is a result of a non-negligent misconduct of the service. This Regulation sweeps this liability so that the provider is liable by default, unless they can prove otherwise.

[12] Article 9