EU Regulation

ELECTRONIC IDENTIFICATION AND TRUST SERVICES

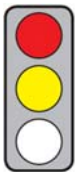
cep **Policy Brief** 2012-31 of 30 July 2012

Centrum für Europäische Politik

KEY ISSUES

Objectives of the Regulation: With its Proposal the Commission wishes to enhance trust in electronic transactions in the internal market.

Parties affected: Citizens, companies, authorities.



Pros: (1) The cross-border recognition and acceptance of electronic identification means can help reduce administrative and transaction costs.

(2) The provisions on the security of electronic signatures improve interoperability, which in turn facilitates cross-border activities.

Cons: (1) The waiver of a test to examine whether or not the identification schemes comply with the requirements facilitates misuse and thus jeopardises the security of personal data.

(2) The supervisory rules for providers of particularly sensitive "qualified trust services" are imprecise and inconsistent.

CONTENT

Title

Proposal COM(2012) 238 of 4 June 2012 for a **Regulation** of the European Parliament and of the Council **on electronic identification and trust services for electronic transactions in the internal market**

Brief Summary

- **Background and objectives**
  - The Regulation expands the existing provisions on the trust service e-signature (Directive 1999/93/EC) and complements them with new provisions on electronic identification and additional trust services.
  - The Commission's key objectives are (Recital p. 11) to
    - enhance trust in electronic transactions in the EU;
    - ensure the safety of electronic transactions;
    - improve the interoperability of electronic identification systems.
- **Definitions**
  - "Electronic identification" means the process of identifying a person through electronic data (Art. 3 (1)), for instance through electronic identity cards.
  - "Trust services" and "qualified trust services"
    - "Trust services" are electronic services for the "creation, verification, validation, handling and preservation" of electronic signatures, seals, time stamps, documents, delivery services and certificates as well as website authentication (Art. 3 (12)).
    - A "qualified trust services" is a trust service that satisfies the requirements provided for in the present Regulation (Art. 3 Abs. 13).
      This includes amongst other things "qualified certificates". These serve to link electronic signatures, seals or websites to a person (Art. 3 (10) in conjunction with (11), (24) and (30)).
  - Electronic signatures
    - "Simple electronic signatures" are electronic data used for signing purposes (Art. 3 (6)), e.g. scanned signatures.
    - "Advanced electronic signatures" are electronic signatures which, amongst other things, are (Art. 3 (7)):
      - uniquely linked to the signatory;
      - capable of identifying the signatory; and
      - designed using signature creation data that only the signatory can use.
    - "Qualified electronic signatures" are electronic signatures created by a "qualified electronic signature creation device" and based on a "qualified certificate for electronic signatures" (Art. 3 (8)).
      - "Qualified electronic creation devices" are configured "software or hardware" that comply with the requirements set forth under Annex II to the Regulation (Art. 3 (17) and (18)).
      - "Qualified certificate for electronic signature" must comply with the requirements of Annex I of the Regulation (Art. 3 (11)).
- **Scope**
  - The Regulation applies to (Art. 2 (1))
    - the electronic identification provided by, on behalf or under the responsibility of Member States, and
    - the activity of trust service providers established in the EU; exempted are trust services within closed groups based on "voluntary agreements under private law" (Art. 2 (2)); this includes e.g. special signature systems for the communication between lawyers and courts.

Authors: Anne-Kathrin Baran and Philipp Eckhardt | baran@cep.eu
CEP | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-105 | www.cep.eu

- **Electronic identification (electronic identification, e-ID) and notification**
  - Member States must recognise and accept any electronic identification means, such as electronic IDs issued in another Member State. The precondition for this is that the Member State concerned has notified the Commission as to the identification system it uses for issuing means of identification (Art. 5).
  - The Member States can notify electronic systems if (Art. 6 (1)) they:
    - issue or let issue electronic identification means;
    - accept these electronic identification means themselves;
    - ensure that the data necessary for identification are "unambiguously" attributed to one person;
    - enable any third party to test online at any time and free of charge the validity of the electronic identification (authentication); and
    - are liable for compliance with the last two requirements.
  - The Commission will draw up and publish a list of all notified electronic identification schemes (Art. 7 (2)).
  - Member States will cooperate to ensure the interoperability of electronic identification means issued as part of a notified scheme (Art. 8 (1)).
  - The Commission can
    - by means of implementing acts define the "details, formats and procedures" of the notification (Art. 7 (4)),
    - by means of delegated legal acts define "technical minimum requirements" in order to ensure the cross-border interoperability (Art. 8 (3)).
- **Trust services: requirements for all trust services providers**
  - Member States are to designate a supervisory body for trust service providers (Art. 13 (1) and (2)).
  - Such providers must take "technical and organisational measures" to ensure that the "level of security is appropriate" (Art. 15 (1) sub-para. 1). The competent national supervisory body and "other relevant third parties such as data protection authorities" must be notified of any "significant" breach of security "without undue delay and where feasible" not later than 24 hours after having become aware of it (Art. 15 (2) sub-para. 1).
  - Where providers of trust services infringe the general security requirements, they are held liable for any "direct damage caused" (Art. 15). In this case, a shifted burden of proof is required: the providers concerned must prove that they did not act negligently. (Art. 9)
- **Trust services: requirements for qualified trust services providers**
  - For providers of qualified trust services the following additional security requirements apply (Art. 19).
  - In particular, they must verify the identity of a person for whom they issue a "qualified certificate" (see above) (Art. 19 (1) sub-para. 1, Art. 3 (10)). Such verification is to be carried out (Art. 19 (1) sub-para. (2) lit. a and b):
    - by physical appearance of the natural person or of an authorised representative of the legal person, or
    - remotely, using electronic identification under a notified scheme issued after having verified the identity of its holder.
  - Providers may render a qualified trust service once they have notified the competent supervisory body of their intention and submitted an audit report from a "recognised independent body" confirming that the provider complies with the requirements of the Regulation. This report must be updated each year. (Art. 16 (1) in conjunction with 17 (1))
  - Having verified compliance of the qualified trust service provider and of the qualified trust services provided with the requirements of the Regulation, the supervisory body indicates the qualified trust service provider in a "trusted list" (Art. 17 (3)). In the case of an infringement of the Regulation they can be deleted from the list. (Art. 16 (4)).
  - If qualified trust service providers do not comply with the general and additional requirements of the Regulation, they are held liable for all "direct damages". In this case, a shifted burden of proof is required: the provider concerned must prove that they did not act negligently. (Art. 9)
- **Electronic signatures (eSignatures)**
  - Qualified electronic signatures can substitute a handwritten signature (Art. 20 (2)). All Member States must recognise and accept them (Art. 20 (3)).
  - Electronic signatures must not be denied legal effect and admissibility in legal proceedings solely because it is in an electronic form. (Art. 20 (1)).
  - For cross-border access to the online services of public bodies Member States must not request a higher security assurance level than the qualified electronic signature (Art. 20 (5)).
  - If a Member State requests a lower security assurance level, it must recognise and accept all electronic signatures which comply with at least this standard. The Commission is empowered to adopt delegated acts defining which electronic signatures in case of technical differences comply with which security level – simple, advanced or qualified. (Art. 20 (4) and (6))

Changes to the Status quo

- Newly introduced are provisions on electronic identification and on the additional trust services.
- The already existing provisions on electronic signatures are to be expanded to include rules regarding the degree of security standards of electronic signatures.

Statement on Subsidiarity by the Commission

According to the Commission, the "transnational nature" of electronic identification and electronic trust services requires EU action.

Policy Context

In the Communication "A digital Agenda for Europe" [COM(2010) 245; s. CEP Policy Brief], the Commission announced the revision of the Electronic Signature Directive (1999/93/EC) and a Proposal on the mutual recognition of electronic identification and authentication. Under the framework of the EU STORK project, ten Member States are cooperating to allow for the interoperability of electronic identity cards.

Legislative Procedure

04 June 2012	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Leading Directorate General:	DG for Communications Networks, Content and Technology
Committees of the European Parliament:	Industry, Research and Energy (leading), Rapporteur: Marita Ulvskog (S&D Group, SE); Economic and Financial Affairs; Internal Market and Consumer Protection; Legal Affairs; Civil Liberties, Justice and Home Affairs
Committees of the German Bundestag:	Economics and Technology (leading); Affairs of the EU; Internal Affairs; Legal Affairs
Decision mode in the Council:	Qualified majority (approval by a majority of Member States and at least 255 out of 345 votes; Germany: 29 votes)

Formalities

Legal competence:	Art. 114 TFEU
Form of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Legislative procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

Electronic identification and trust services will only prevail if promising, profitable business models exist. However, this is seriously hampered by today's lack of application possibilities, together with high costs, security concerns and regulatory uncertainty. The Regulation helps to reduce regulatory uncertainty and thus strengthens the digital internal market.

Electronic identification: the recognition and acceptance of the notified electronic identification means of other Member States **can help reduce administrative and transaction costs**. It enables quicker completion of any requests made to authorities and companies in other Member States that require electronic identification. Thus companies are given the incentive to act at cross-border level, for instance to apply for public tenders in other Member States.

However, it is problematic that no independent body controls whether or not the notified identification scheme actually complies with requirements stipulated by the Regulation and whether the schemes adhere to the minimum security standards and data protection requirements. Nevertheless, other Member States must recognise and accept the identification means of these schemes. **This makes misuse easier**, jeopardises the confidence of users in identification means **and challenges the security of sensitive personal data**. **The** proposed **Member State liability** mitigates this but **does not** really **suffice**. Notification should therefore only be carried out by an independent examination, or if necessary by the Commission itself.

The interoperability of the identification means is a basic precondition for mutual recognition and acceptance and consequently for the functionality of electronic identification. Where no interoperability is possible, Member States, who must recognise and accept a notified foreign identification means, would have to adjust their own identification systems technically. Hence, the interoperability issue should have been clarified before a mutual recognition and acceptance was laid down. Irrespective of this criticism, at the moment, it is questionable if the provisions on electronic identification can be fully effective in the near future at all. To start with, there are several Member States that do not have any electronic identification schemes; secondly the

notification of Member States is voluntary; and thirdly, there are hardly any applications available at present anyway.

Trust services: The fact that trust service providers (whether qualified or not) are held liable for direct damages in the case of security infringements increases the legal certainty for users and thus creates confidence in trust services, in particular in the cross-border service traffic.

The supervisory rules for providers of -.particularly sensitive - qualified trust services are imprecise and inconsistent. For instance, providers can be on the "trust list" even though they no longer comply with the requirements of the Regulation and thus have lost their status as qualified providers. Moreover, qualified providers may start providing qualified trust services without having been assessed by the supervisory body as to whether or not they comply with the requirements of the Regulation, as there is no admission. This issue needs urgent clarification in order to ensure security; the imprecise supervisory rules of the existing Signature Directive have already contributed to a loss in confidence.

The introduction of further trust services – seals, time stamps, documents, delivery services and certificates – into the Regulation is appropriate, for these trust services are currently only subject to national, often diverging legal and technical rules, which impedes the cross-border activities of providers. Moreover, there is uncertainty amongst users and providers as to the validity of the services in other Member States, which weakens the confidence in and attractiveness of the services.

Electronic Signature: The implementation of the Signature Directive into national law has led to different national quality and security levels for electronic signatures. This resulted in nationally characterised offers and a lack in cross-border interoperability. **The fact that cross-border access to public online services requires no higher security level than that of a qualified electronic signature, improves interoperability and facilitates cross-border activities**. Firstly, this ensures the quality and security of trust services; secondly, the user uncertainty regarding the validity of electronic signatures in non-EU countries is reduced; and thirdly, incentives are created for the providers to develop applicable signature procedures that can be used at cross-border level.

Legal Assessment

Competency

It is correct to base the Regulation on Art. 114 TFEU (approximation of laws in the internal market). This also applies to the provisions on electronic identification, which provide for mutual recognition, for this safeguards Member State autonomy to a larger degree than does a full or partial approximation.

Subsidiarity

Unproblematic.

Proportionality

It is appropriate to adopt a Regulation in order to ensure a consistent security level of trust services.

Compatibility with EU Law

Unproblematic.

Compatibility with German Law

It remains unclear as to how Member States can comply with the notification requirement, according to which the data required for identification must be attributed unambiguously to one person. The possibilities are attributing a personal identification number, the use of a serial number for the identification means or a combination of different features, such as name, birth name or address. However, the right to electronic self-determination (Art. 2 (1) in conjunction with Art. 1 (1) of the German Constitution) must be safeguarded. It may only be restricted on grounds of a "predominant general interest" [German Federal Constitutional Court: 1 BvR 209/83 amongst others (census)].

Conclusion

The cross-border recognition and acceptance of electronic identification means can help reduce administrative and transaction costs. The waiver of a test to establish whether or not the identification schemes comply with the requirements of the Regulation and minimum security standards facilitates misuse and jeopardises the security of personal data. The supervisory rules for providers of - particularly sensitive - qualified trust services are imprecise and inconsistent. The provisions on the security of electronic signatures improve interoperability which in turn facilitates cross-border activities.