



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 7 June 2012

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

**10977/12
ADD 1**

**TELECOM 122
MI 411
DATAPROTECT 73
CODEC 1576**

COVER NOTE

from: Secretary-General of the European Commission,
signed by Mr Jordi AYET PUIGARNAU, Director

date of receipt: 5 June 2012

to: Mr Uwe CORSEPIUS, Secretary-General of the Council of the European
Union

No Cion doc.: SWD(2012) 136 final

Subject: COMMISSION STAFF WORKING DOCUMENT EXECUTIVE
SUMMARY OF THE IMPACT ASSESSMENT *Accompanying the document*
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

Delegations will find attached Commission document SWD(2012) 136 final.

Encl.: SWD(2012) 136 final



EUROPEAN COMMISSION

Brussels, 4.6.2012
SWD(2012) 136 final

COMMISSION STAFF WORKING DOCUMENT
EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

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

{COM(2012) 238 final}
{SWD(2012) 135 final}

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

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

1. POLICY CONTEXT, PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

Building trust in the online environment is key to economic development. Lack of trust makes consumers, businesses and administrations hesitate to carry out transactions electronically and to adopt new services. The proposed initiative for a regulatory framework aims at enabling secure and seamless electronic transactions between businesses, citizens and administrations, thereby increasing the effectiveness of public and private electronic services, e-business and e-commerce.

Barriers to cross-border e-services exist and need to be eliminated. In order to be productive enablers rather than obstacles, **electronic identification, authentication, signatures and related ancillary trust services (eIAS)** accordingly need to be mutually recognised and accepted throughout the EU.

There is no comprehensive EU cross-border and cross-sector framework for eIAS services. At EU level, a legal framework exists only for e-signatures but not for e-identification and authentication nor for related ancillary trust services. The Commission announced in the *Digital Agenda for Europe* that it would propose legal measures to further address e-signatures and to ensure mutual recognition of e-identification (eID) and e-authentication so as to eliminate fragmentation and lack of interoperability, enhance digital citizenship and prevent cybercrime.

To carry out the present impact assessment, the Commission collected feedback from Member States, the European Parliament and stakeholders during discussions, workshops and conferences. A number of studies related to eIAS were launched and literature was surveyed. A public consultation was launched in 2011 to collect input on how eID, authentication and signatures can contribute to the single market. The consultation was complemented by a targeted survey to record the specific views and needs of SMEs.

2. PROBLEM DEFINITION

Users may encounter difficulties when it comes to the cross-border use of eIAS services. The main obstacles to secure and seamless cross-border eIAS are:

1 — fragmentation of the market: different rules apply to service providers depending on which Member States they serve.

Regarding e-signatures, the harmonisation brought about by the e-signatures Directive 1999/93/EC is imperfect. Four problems have been identified: divergent implementation at national level due to differing interpretations of the Directive by Member States, *de facto* invoking of a derogation for public-sector applications, outdated standards and unclear supervision obligations which lead to cross-border interoperability problems, a segmented EU landscape and distortions in the internal market.

Regarding eID, different technological solutions for personal identification in individual Member States, the lack of legal certainty on the cross-border use of eIDs and the lack of clear liability for the correctness of identity data all lead to interoperability problems.

Regarding ancillary trust services, the lack of an EU legal framework leads to the adoption of national laws for some of these services in some Member States and high costs for providers wanting to offer their services in several Member States. Both situations result in internal-market barriers and fragmentation.

2 — lack of trust and confidence: the lack of trust and confidence in electronic systems, the tools provided and the legal framework can create the impression that there are fewer legal safeguards than with physical interaction.

For e-signatures, national supervision requirements are qualitatively different from one Member State to another, making it complex for parties relying on an e-signature to assess how a service provider is supervised.

For eID and ancillary trust services, heterogeneous national legislations make it difficult for users to feel secure when interacting online in cross-border scenarios.

The four main drivers of these problems are:

A: Insufficient scope of the current legal framework

eIAS services are pre-requisites for a wide range of electronic interactions such as e-banking, e-government or e-health services. At EU level, there is a limited and imperfect regulatory framework that essentially focuses on e-signatures. There is no specific framework for mutual recognition and acceptance of eID or for ancillary trust services such as time-stamping or e-seals.

B: Lack of coordination between e-signature and eID development

National eIAS infrastructures were developed in isolation without coordination at EU level. The resulting absence of cross-border interoperability of technical solutions creates barriers to e-transactions. The lack of mutual recognition and acceptance is one of the reasons why both users and providers of e-services are sceptical about the deployment of eIAS.

C: Lack of transparency in security guarantees

Strong and harmonised security is essential if trustworthy solutions are to be created. This is particularly relevant for access to services where sensitive personal data are involved, such as e-health. Directive 99/93/EC recognised that legal certainty can only be granted to e-signatures which guarantee security and which are thus sufficiently protected against forgery or fraud (advanced and qualified e-signatures).

The lack of secure eID systems is perceived by users as a major barrier. The lack of a harmonised legal framework for eID means that the security and reliability of official eIDs cannot be objectively determined across borders. This creates cross-border barriers, a consequent lack of trust and a fragmented market.

Another concern is ID theft. Secure eIDs can help reduce this risk. Conversely, badly-secured eIDs make it easier for criminals to obtain false or compromised eIDs

D: Lack of awareness/user adoption

The complexity of the technologies used for e-transactions, and the key role played by trusted third parties, create in an environment in which it is difficult to assess trust. In particular, end users, who generally do not have sufficient expertise, must be able to rely on rules which establish clear rights and responsibilities for all stakeholders (trust service providers, end users and governance bodies).

3. BASELINE SCENARIO

The baseline scenario of the initiative is the absence of any new regulatory intervention. It is anticipated that under this scenario, the current problems would evolve as follows:

Fragmentation and interoperability problems would not be solved: Member States would be likely to continue to implement and enforce Directive 99/93/EC.

Legal certainty would not be ensured: the problems generated by the lack of mutual recognition of e-signatures and by the absence of a legal framework regulating the mutual recognition and acceptance of eID and ancillary trust services would impede the legal recognition of a range of cross-border interactions.

User needs would not be fully satisfied: under the current framework, it is not possible to take full advantage of the opportunities offered by technological developments.

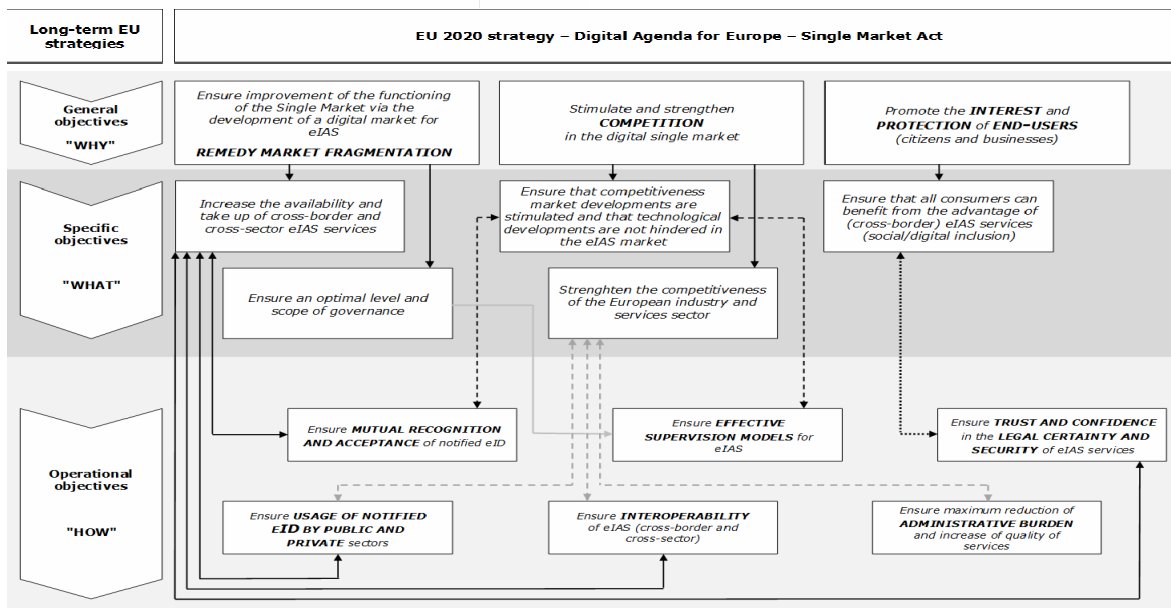
Leading European initiatives would not be fully leveraged: EU policies such as the Services, Public Procurement or VAT (e-invoices) Directives, or the ICT-PSP large-scale pilot projects¹ which endeavour to eliminate interoperability challenges and cross-border recognition problems related to certain types of e-interactions would be able to operate only at pilot level due to the lack of a cross-sector legislative framework.

4. POLICY OBJECTIVES

Four **general objectives** have been identified: ensuring the development of a digital single market; promoting the development of key cross-border public services; stimulating and strengthening competition in the single market; enhancing user-friendliness (citizens and businesses). These objectives are in line with strategic EU policies such as the *EU 2020 Strategy*, the *Digital Agenda for Europe*, the *Single Market Act* and the *Roadmap for Stability and Growth*.

Specific objectives express the desired outcomes related to the eIAS market (*'what'*) of putting in place *operational objective ('how')*. For each specific objective, a number of **operational objectives** have been identified.

¹ http://ec.europa.eu/information_society/activities/ict_psp/about.



5. POLICY OPTIONS

To solve the problems and meet the above objectives, three sets of options were assessed: (1) scope of the envisaged framework, (2) legal instrument and (3) supervision level:

- Under the first set, ‘*scope of the framework*’, four options are examined:

Option 0: Repeal of Directive 99/93/EC and no regulatory activities concerning eID or ancillary trust services

This option consists in the cessation of all EU activities in the field of e-signatures. Directive 99/93/EC would be repealed and no legislative measures would be proposed for eID mutual recognition.

- Option 1: No policy changes (baseline scenario)

Directive 99/93/EC would be kept as it stands. No legislation on eID would be proposed.

- *Option 2: Enhancing legal certainty, boosting coordination of national supervision and ensuring mutual recognition and acceptance of eIDs*

The scope of Directive 99/93/EC would be expanded to add provisions covering the cross-border recognition and acceptance of ‘notified eID’ schemes². The provisions of the Directive related to e-signatures would be revised to remedy its current weaknesses and thus better harmonise national supervision models.

- *Option 3: Expansion to incorporate certain ancillary trust services*

²

‘Notified eID’: an eID scheme notified by a Member State to the Commission to be recognised and accepted across borders. The concept of notified eID is not limited to public-sector issued eIDs: Member States could also notify eIDs issued by the private sector that they recognise for use in their own public-sector services. This approach is necessary since not all Member States authorities issue eIDs. The cross-sector approach of the legislation would allow the private sector to integrate the use of notified eIDs in e-services when secure e-identification is needed.

This option expands Option 2 by including ancillary trust services and credentials in the scope of the proposal.

Essential ancillary features to be incorporated in the legislation would be: time-stamping, e-seals, long-term preservation of information, certified e-document delivery, admissibility of e-documents and website authentication.

- Under the second set, comprising a ‘legal instrument’, four options are considered:

Either one comprehensive legislative instrument (Option A) or two separate ones (Option B)

The legislation could consist of one single comprehensive measure covering e-identification, authentication and signature or two instruments, namely a Commission Decision on eID and a revision of the e-signatures Directive.

A Directive (Option C) or a Regulation (Option D):

The legislation could be a Directive or a Regulation.

- At the third, ‘supervision’ level, two options are considered:

Option i): Maintaining national supervision schemes

The current national-based supervision schemes would be maintained but with stronger harmonisation through essential common requirements.

Option ii): Establishing an EU-based supervision system

An EU-based supervision system would be established to reduce or eliminate differences between national supervision arrangements. This could take one of two forms:

Sub-option a: replacing the existing national supervision schemes by a single EU supervisory scheme and body.

Sub-option b: establishing an EU supervision scheme and body while maintaining in parallel national supervisory schemes (each Member States could choose its own or the European scheme).

6. COMPARISON OF POLICY OPTIONS AND IMPACTS

The policy options have been assessed and compared to the baseline scenario (Option 1) in terms of effectiveness, efficiency and coherence.

6.1. Scope of the framework

Option 0 would not help attain the objectives identified in the Impact Assessment report. It would not increase the availability and take-up of cross-border and cross-sector eIAS services, ensure an optimal governance level, stimulate market developments, contribute to the strengthening of the competitiveness of the European industry and services sectors or ensure that all end-users can benefit from the advantage of eIAS services. It would on the contrary hinder technological developments in the eIAS market, disrupt the current process of working

towards the enabling of cross-border e-services and maintain a fragmented EU market and an uneven trust landscape.

Option 1 would not achieve the objectives. It would maintain the existing ambiguities and the trust landscape concerning supervision would remain uneven. Regulatory uncertainty would remain and a segmented EU landscape would continue to evolve, leading to distorted competition conditions in the internal market and increasing the likelihood of differing approaches at national level.

Option 2 would enhance legal certainty, boost supervision and ensure mutual recognition and acceptance of eIDs, and would significantly contribute to achieving each of the objectives identified in the IA report, yielding positive economic, social and environmental results.

eIAS services would have greater appeal, boosting the return on investments made in eIAS infrastructure and services. Also, eIAS would become available for all sectors and all types of companies while eliminating cross-border barriers. New markets and new investments would be opened up, thus stimulating innovation.

The current fragmentation of the market would be reduced, since cross-border interoperability would be improved by allowing references to technical standards.

Mutual recognition and acceptance of eID would further dismantle the current barrier to the single market. Finally, it is probable that the homogeneity of supervision that would result from common essential requirements would increase trust, facilitate fraud detection and contribute to preventing identity theft.

Option 3 would make eIAS services even more appealing and thus boost their positive impact by expanding the framework to incorporate certain essential ancillary trust services.

Option 3 is deemed more likely appropriate than Option 0, 1 or 2 to have a significant impact on secure and easy-to-use e-transactions.

6.2. Legal instrument

Providing a comprehensive framework within **one instrument** would ensure that the legislation regulating the various aspects of eIAS was consistent. **Two separate instruments** might introduce divergences in the legal provisions adopted for e-signatures and e-identification — and, more importantly, in the approach of the initiatives.

Adopting a **Directive** would not help solve the current e-signature interoperability issues stemming from diverging transpositions of Directive 99/93/EC. A **Regulation** provides immediate applicability without interpretation and thus greater harmonisation and is therefore more appropriate to achieve the objectives of the proposed legislation.

One single Regulation seems to be the most effective way of achieving the objectives..

6.3. Level of supervision

Under **Option ‘i’**, the new legislation would maintain the current national-based supervision schemes and impose common essential requirements on service providers. A harmonised approach at EU-level for both e-signature and ancillary trust services would improve effective supervision, enhance legal certainty and augment the trust and security of e-transactions.

Option ‘ii’ would provide homogenous, efficient and high-quality supervision throughout the EU. **Sub-option ‘b’** has the advantage of greater flexibility than with the single EU

supervisory body foreseen in **Sub-Option ‘a’**: it could be advantageous for Member States where no or few trust service providers are established to transfer supervision duties to an EU supervision body. Other Member States could if they wished maintain their supervision scheme. However, an centralised EU supervision model raises subsidiarity concerns.

*The respect of the principle of subsidiarity suggests that (**Option i**) is the most adequate.*

7. RATIONALE FOR EU ACTION, EU ADDED VALUE AND SUBSIDIARITY

As with Directive 99/93/EC, the legal basis for the legislative proposal is Article 114 TFEU on the internal market because it seeks to remove existing barriers to the functioning of the internal market by fostering the mutual recognition and acceptance of eID, authentication, signatures and ancillary trust services across borders when needed for e-transactions.

Due to the inherent non-territorial nature of eIAS services, action at EU level is adequate and proportionate to implement the digital Single Market. Regulatory measures taken at Member State level cannot be expected to achieve the same outcome. EU intervention is thus required, appropriate and justified.

8. MONITORING AND EVALUATION

The Commission would monitor the application of the legislation through continuous dialogue with stakeholders and the collection of statistics; and would report to the European Parliament and the Council on the impact of the new legislation four years after its entry into force.