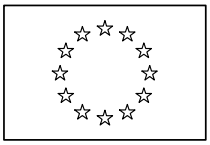

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 28.11.2008
COM(2008) 798 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market

(Text with EEA relevance)

1. INTRODUCTION

1.1. Issues addressed by the Action Plan

In the framework of the Lisbon Strategy, the EU has committed itself to improving the legal and administrative environment to unlock business potential. Bringing public administrations on line, and enabling enterprises and individuals to communicate electronically with public administrations across borders, contributes to creating an environment that favours entrepreneurship and facilitates citizen's contact with public authorities.

Electronic communications are becoming increasingly important in many aspects of economic and public life. Public authorities across Europe have started to offer electronic access to government services. In doing so they have been focusing mostly on national needs and means, which has led to a complex system with different solutions. This situation carries the risk of creating new barriers to cross-border markets and of hampering the functioning of the single market for enterprises and citizens.

Major barriers to cross-border access to electronic services of public administrations are linked to the use of electronic identification and of electronic signatures. Like in the non-digital environment, certain electronic procedures may require identification and signatures. Thus access to public administrations' electronic procedures often implies the need for the individuals involved to identify themselves (i.e. allowing the administration to make sure that the persons are who they claim to be by checking their personal credentials[1]) and the need to provide an electronic signature allowing the administration to identify the signatory as well as to make sure that the data submitted has not been altered during transmission). The main barrier is the lack of interoperability, be it legal, technical or organisational.

The current European Union framework offers horizontal and sectoral instruments to facilitate and enhance the use of e-signatures and e-identification. The e-Signatures Directive[2] establishes the legal recognition of electronic signatures and a legal framework to promote their interoperability. A number of practical, technical and organisational requirements need to be met to establish such interoperability.

Furthermore, effective interoperability is also required if Member States are to comply with their legal obligations under other EU legislation, in particular under specific internal market instruments. Several internal market initiatives foresee that businesses should be able to use electronic means to communicate with public bodies, exercise their rights and do business across borders.

The Services Directive obliges Member States to ensure by the end of 2009[3] that service providers are able to complete electronically and at a distance all procedures and formalities

---

1 Identification is the process of using claimed or observed attributes of an entity to deduce who the entity is. The term "identification" is also referred to as entity authentication. (ModinisIDM Terminology paper, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc.

2 Directive 1999/93/EC, OJ L 13, 19.01.00, p.12 and the Report on the operation of e-Signatures Directive COM(2006)120 final.

3 Article 8 of the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. The deadline for implementation of the Services Directive is the 28 December 2009.

necessary to provide a service activity. This implies, amongst other things, the possibility for cross-border identification of service providers and authentication of the data submitted.

The Directives on Public Procurement[4] aim to promote the development and use of electronic means in public purchasing procedures, with potentially substantial cost savings for business.[5] Member States may regulate the level of electronic signature required in line with the obligations of the e-Signatures Directive, and may restrict the choice of contracting authorities to qualified signatures[6].

Electronic invoicing — the electronic transfer of invoicing information (billing and payment) between business partners (supplier and buyer) — is an essential part of an efficient financial supply chain. To accompany the creation of Single Euro Payment Area, work is under way to prepare an e-invoicing initiative (the European Commission has set up an expert group tasked with establishing a European Electronic Invoicing Framework by 2009) with further savings for businesses. [7]

The objective of this Action Plan is therefore to offer a comprehensive and pragmatic framework to achieve interoperable e-signatures and e-identification, which will simplify access of enterprises and citizens to cross-border electronic public services. To achieve this objective, the Action Plan focuses on a number of practical, organisational and technical issues, complementing the existing legal framework.

1.2. Current framework for e-signatures and e-identification at EU level

1.2.1. The e-Signatures Directive

The e-Signatures Directive was adopted in 1999 to promote the legal recognition of electronic signatures and to ensure the free circulation within the single market of e-signature products, equipment and services. However, a legal and technical analysis of the practical usage of e-signatures shows that there are interoperability problems that currently limit the cross-border use of e-signatures. The analysis highlights the need for a more effective mutual recognition approach. Fragmentation due to the lack of cross-border interoperability is likely to affect e-

---

4 Article 42(5)(b) and Annex X of Directive 2004/18/EC and Article 48(5)(b) and Annex XXIV of Directive 2004/17/EC on public procurement.

5 For further information, see the Action Plan for the implementation of the legal framework for electronic public procurement of 13 December 2004, COM(2004)841.

6 When conducting their procurement online, public purchasers must be able to receive and process electronic tenders across borders. Full electronic tenders are complex envelopes containing a variety of electronically signed documents and attestations from different sources, national origins and technical outlooks, including certified translations (e.g. to accept a service provider's proof of qualification). This means policy-makers must organise complex electronic communications in an open circuit, i.e. where the receiver of information (the public purchaser) does not previously know all the potential senders (the bidders).

7 In particular, the Expert Group on e-Invoicing has stated that electronic invoicing should not be hindered by disharmonious national electronic signature legislation. The scope of this horizontal action plan does not include assessing the implications of using electronic signatures for VAT compliance (electronic signatures for invoices are referred to in Council Directive on the Common System of VAT 2006/112 EC (Art. 233)) and electronic invoicing or the associated obstacles and actions needed to remedy these obstacles.

government services in particular, which today are the largest channel of transactions using e-signatures. [8]

1.2.2. The i2010 e-Government Action Plan

With regard to cross-border e-identification, there is still no Community instrument on which action at Community level could be based. Notwithstanding this, the Commission supports (both politically and financially) activities that aim at finding solutions to interoperable e-identification at EU level. In this regard, the i2010 e-Government Action Plan[9], adopted by the European Commission on 25 April 2006, considers interoperable electronic identity management (eIDM) as one of the critical key enablers for access to public services. The importance of interoperable eIDM has been recognised by the Member States who have made the clear commitment to ensure that *"by 2010 European citizens and businesses will be able to benefit from secure and convenient electronic means, issued at local, regional or national levels and complying with data protection regulations, to identify themselves to public services in their own or in any other Member State"*.

1.3. Enhancing the cross-border interoperability of e-signatures and e-identification

Despite the existing legal provisions and the political commitments taken by the Member States and the Commission, a more coordinated and comprehensive approach is needed to facilitate the cross-border use of e-identification and e-signatures in practice. This is essential to avoid fragmentation of the single market.

Therefore, the Commission proposed in its Communication "A single market for the 21st century Europe" of 20 November 2007 to adopt an **Action Plan on e-signatures and e-authentication[10]**.

This Action Plan aims to assist Member States in implementing mutually recognised and interoperable electronic signatures and e-identification solutions, in order to facilitate the provision of cross-border public services in an electronic environment. It sets out specific actions on e-signatures (part 1) and on e-identification (part 2). Although the Action Plan focuses mainly on e-government applications, the suggested actions will also benefit businesses' applications insofar as the means to be put in place can also be used in Business to Business (B2B) and Business to Consumers (B2C) transactions.

At the Spring European Council of March 2008, Heads of State or Government declared that it is crucial to put in place cross-border interoperable solutions for electronic signatures and e-authentication to improve the functioning of the 'e-Single Market'.

---

8 The European Commission is also working on a project to facilitate the introduction of electronic signatures in its internal and external exchanges. This project is called "*Electronic Signature Service Infrastructure" (ESSI).* This project constitutes a key requirement for dematerialisation of the European Commission processes, as foreseen in "Rules for the provisions on electronic and digitised documents" (SEC(2005)1578).

9 i2010 e-Government Action Plan: Accelerating e-Government in Europe for the Benefit of All [COM(2006) 173 final].

10 E-authentication is understood here as entity authentication, i.e. e-identification. The term e-identification is used in this document for the sake of clear separation between entity and data authentication.

The Commission will contribute to developing a coordinated response to interoperability issues by monitoring progress and giving guidance to Member States and stakeholders on the implementation of the Action Plan.

2. PART 1: ACTIONS TO ENHANCE THE CROSS-BORDER INTEROPERABILITY OF E-SIGNATURES

The main objective of the e-Signatures Directive is to create a Community framework for the use of electronic signatures, allowing the free flow of electronic signature products and services cross-borders and ensuring a basic legal recognition of electronic signatures.

The Directive addresses three forms of electronic signatures. The first one is the "simple electronic signature". This one has a wide meaning. It serves to identify the signing person and to authenticate data. It can be as simple as signing an e-mail message with a person's name or using a PIN-code. The second form is the "advanced electronic signature" *(AES*). This form of signature needs first to be uniquely linked to the signatory, secondly it needs to be capable to identify the signatory, thirdly the means need to be such that they can be maintained under the whole control of the signatory and fourthly it needs to be linked to the data in such a way that any subsequent change in the data can be detected (see Article 2.2 of the Directive). The third form, a "qualified electronic signature" (*QES*) consists of an advanced electronic signature based on a qualified certificate (*QC*) and created by a secure-signature-creation device. It offers the highest level of security that the data comes from its purported sender and that the transmitted data have not been tampered with.

The general principle of legal recognition applies to all three kinds of electronic signatures established by the Directive. This means that none can be refused purely for the reason of being in an electronic form (see Article 5 of the e-Signatures Directive). In addition, Article 5.1 states a legal presumption of equivalence between a qualified e-signature and a handwritten signature. The cross-border acceptance of e-signatures applies however only to the qualified level, as Article 4.2 establishes the free circulation of e-signature products which comply with the Directive (meaning in practice complying with the requirements for qualified signatures as laid down in the annexes to the Directive).

Member States also have to ensure that when they apply additional requirements for e-signatures used in the public sector on the basis of Article 3.7 of the Directive, such requirements do not constitute obstacles for cross-border services, in line with the internal market basis of the Directive[11].

Alongside the need for correct implementation of these obligations of the e-Signatures Directive, a number of technical and organisational issues need to be addressed to improve the cross-border use of e-signatures in practice.

[11] Art. 3. 7 these additional requirements have to be objective, transparent, proportional and non-discriminatory and have to relate to the specific characteristics of the application concerned.

2.1. Qualified electronic signatures and advanced electronic signatures based on a qualified certificate

It is expected that the cross-border use of qualified e-signatures (*QES*) and advanced e-signatures based on qualified certificates (*AES* based on *QC*) can be improved relatively quickly[12]. Both types of signatures benefit from a clear legal status under the e-signatures Directive, namely the presumption of equivalence to a handwritten signature for the *QES* and the legal obligation of Member States to mutually recognise qualified certificates. In addition, substantial work already exists in the field of standardisation for both types of signature (*QES* and *AES based on QC*).

In practice, the main obstacle for the cross-border use of e-signatures lies in the lack of trust in e-signatures originating from other Member States, and difficulties linked to validating these signatures.

Firstly, in order to enhance trust in e-signatures from other Member States, the receiving party should be able to check the status of the Certification Service Providers (CSPs) issuing qualified certificates in other Member States. The e-Signatures Directive (Article 3.3) requires Member States to ensure that an appropriate system is set up to supervise the Certificate Service Providers established in their territory that issue qualified certificates.

Secondly, in order to validate a *QES* or an *AES based on a QC* originating from another Member State, a receiving party needs to check the "quality" of the signature. This means that the receiving party has to be able to verify whether the signature is an advanced electronic signature and whether it is supported by a qualified certificate issued by a supervised Certification Service Provider (see explanation on supervision (Article 3.3) above). In the case of a *QES*, it also has to be able to verify whether the signature is supported by a secure signature creation device.

All this information can in principle be retrieved from the signature itself and from the content of the qualified certificate. At present, however, it is difficult to obtain this information because of differences in the use of the existing standards and practices. These lead to a different scope and quality of the information that can effectively be read from the received signature and certificate. This in turn creates an additional burden for the receiving party, which may have to individually assess each signature originating from another Member State.

The validation process for e-signatures could therefore be facilitated by providing the receiving party with the necessary information on Certification Service Providers that are recognised and supervised at a national level and by providing guidance on the implementation of the existing standards and practices to allow interoperability.

In order to prepare the actions required to enhance trust and facilitate the cross-border validation of e-signatures, the Commission is carrying out a study to analyse the requirements for cross-border use of electronic signatures (*QES and AES based on QC*). The study concentrates in particular on the supervision model of the qualified certification services providers; the establishment of a "Trusted List of supervised qualified Certification Service Providers"; the profiles of qualified certificates issued by supervised CSPs in Member States; the profile of the secure signature creation devices and the format of qualified/advanced

[12] Indeed work in that respect is already being considered with Member States in the context of the implementation of the Service Directive.

signatures. The study is based on and takes account of the relevant provisions of the e-Signatures Directive, their national implementation and the existing standardisation work based on the Directive[13].

Actions:

- **By third quarter 2009**: the Commission will update Decision 2003/511/EC[14], establishing the list of generally recognised standards for e-signature products and will analyse the possible extension of the decision to other e-signature products than those covered by the present Commission Decision (e.g. profiles of the qualified certificates and of the secure signatures creation devices). This will help to reduce the current complex standardisation situation and help stakeholders to implement the standards in an interoperable way.
- **By second quarter 2009**: the Commission will compile a "Trusted List of Supervised Qualified Certification Service Providers" at European level. This list will centralise all the required information on existing and supervised qualified certification service providers in order to facilitate the validation process of e-signatures based on qualified certificates.
- **By third quarter 2009**: the Commission will establish guidelines and guidance on common requirements to help stakeholders implement QES or AES based on QC in an interoperable way.
- **Ongoing:** Member States are invited to provide the necessary information to the Commission on a regular basis, and where needed, complete the steps flowing from the actions on e-signatures as mentioned above.

2.2. Advanced electronic signatures

The cross-border use of advanced electronic signatures (*AES*) raises interoperability issues very similar to those discussed above for qualified electronic signatures and advanced signatures accompanied by a qualified certificate. However, in practice the situation with regard to *AES* is more complex, as there are currently more legal, technical and organisational constraints connected to *AES* than to *QES*.

Article 2.2 of the e-Signatures Directive defines the advanced electronic signature in a generic way. This has led Member States to use very diverse technical solutions with different security levels. Member States may also impose specific national solutions for specific applications, thus creating further obstacles for the cross-border use of advanced electronic signatures.

Under the e-Signatures Directive the *AES* do not have the same clear legal status of equivalence to handwritten signatures as the *QES*. Member States are only obliged not to deny

---

[13] In accordance with the e-Signatures Directive, standards have been developed by CEN (European Committee for Standardisation) and ETSI (European Telecommunications Standards Institute) within EESSI (European Electronic Signature Standardisation Initiative).

[14] OJ L 175, 15.07.2003, p. 45. The list contains generally recognised standards for electronic signature products that Member States shall presume are in compliance with the requirements laid down in the e-Signatures Directive.

AES legal effect purely because of their electronic form. This means that Member States have more discretion as to which advanced electronic signature solution to accept (or not), depending on the specific requirements of a given application. Moreover, although in principle an *AES* from another Member State could be accepted if it fulfils the requirements of that given application, the variety of available technical solutions may render the practical acceptance of an *AES* difficult.

In this context, both the validation of an *AES* by the receiving party and the assessment of its legal value or security level in a given application is a challenging task which at present often requires case-by-case assessment and treatment of the signature received. To facilitate the cross-border use of *AES*, the necessary conditions should be created that allow the receiving party to trust and validate the *AES* originating from any other Member State, similar to *QES* and *AES based on QC*.

As a first step, information on the *AES* currently being used in e-government applications will be improved. To this end, the Commission will update the existing relevant country profiles issued in 2007 in the IDABC study on the mutual recognition of e-signatures for e-government applications, and make these accessible online.

However, the variety of *AES* solutions that currently exist and to which different requirements are applied in Member States (including the supervision criteria) makes it impracticable to work out within the framework of this Action Plan a common policy and common criteria for *AES*. At the same time, in order to avoid multiple validation efforts in all Member States — which are the main obstacle to cross-border interoperability — one option may be to delegate verification and validation tasks to a centralised or distributed validation service mechanism, in an effort to gradually remove the main obstacle for interoperability of *AES*.

The Commission will examine through a feasibility study the available options for establishing such a validation mechanism at EU level. In particular, the study will look into the legal, technical and operational requirements of such a service, including the possible need for commonly defined requirement levels for different types of *AES* with an initial focus on *AES* used in e-government applications. If possible, the results of the feasibility study should also feed into the large-scale cross-border e-procurement pilot project 'PEPPOL' ('Pan European Public Procurement Online') which was launched by the Commission and several Member States in May 2008 (as part of the Information Communication Technologies Policy Support Programme (ICT PSP)[15] .

In addition to the above study, the Commission will define more precisely the possible actions needed to promote the cross-border use of *AES* based on the results of ongoing work and the progress achieved in the deployment and cross-border recognition of *QES* and *AES based on QC*.

Actions:

- **By second quarter 2009**: the Commission will update the country profiles of the IDABC (Interoperable Delivery of European e-Government Services to public

[15] Part of the Competitiveness and Innovation Framework Programme: http://ec.europa.eu/cip

Administrations, Business and Citizens)[16] study[17] on mutual recognition of e-signatures for e-government applications.

- **By second quarter 2009**: the Commission will study the feasibility (in terms of legal, operational and technical requirements) of a European federated validation service. Based on the results of the feasibility study, the Commission will determine if and how to implement such a validation service.

- **By 2010**: the Commission will report on further actions needed to facilitate the cross-border use of *AES* based on the results of ongoing work and the progress achieved in the deployment and cross-border recognition of *QES* and *AES based on QC.*

- **After results of the feasibility study** of the European federated validation service, Member States are invited to provide the Commission with all relevant information and ensure the cooperation required for the implementation of the actions, in particular those necessary for the creation of the validation service, subject to the results of the feasibility study.

- Member States are invited to test, **subject to the outcome of the feasibility study** on a European federated validation service and to agreement with the project consortium, the validation service in the CIP[18] large scale cross-border e-procurement pilot project PEPPOL ("Pan European Public Procurement Online").

3. PART 2: ACTIONS TO ENHANCE THE CROSS-BORDER INTEROPERABILITY OF ELECTRONIC IDENTITY

Today, Member States deploy electronic identity management (e-IDM) systems as part of the modernisation of the delivery of services. Electronic Identity Management is a key element for the delivery of any e-services. On the one hand, e-identification gives individuals using electronic procedures the assurance that no unauthorised use is made of their identity and personal data. On the other hand, administrations are able to make sure that the individuals are the persons they claim to be and have the rights that they claim to have (e.g. to receive the requested service).

Some Member States already have in place e-identification systems for access to electronic procedures of those Member States' public administrations. However the technical means vary greatly, even if the trend today is towards the use of electronic ID cards.

The means of e-identification have been deployed without coordination between Member States. Yet the interoperability of e-identification solutions is a further pre-requisite for cross-

---

16 The IDABC programme will end in December 2009. The Commission has proposed a programme on Interoperability Solutions for public Administrations (ISA) as a successor to the IDABC programme.

17 The objective of the study (preliminary results are available, completion date of the study is 2009) is to analyse the requirements in terms of interoperability of electronic signatures for different e-Government applications and services taking into account the relevant provisions of the e-Signatures Directive and their national implementation. The study should provide per e-Government application, and per Member State, the type of electronic signature legally required, and the applicable technical restrictions.

18 Competitiveness and Innovation Framework Programme 2007-2013.

border access to public e-services. Without the deployment of an interoperable e-identification mechanism within the Union, new barriers will be raised in practice, thus at odds with internal market instruments which themselves have been trying to enhance the functioning of the internal market.

At a political level, Ministerial Declarations in 2005 and 2007[19] have called for the deployment of an interoperable identity management system in Europe to enable citizens and businesses to identify themselves when required to do so by public administrations.

Certain common actions are underway to find a solution for cross-border e-identification that would be able to rely on existing identification solutions. As in the case of e-signatures, a horizontal solution is sought on which sectoral applications can rely and which would be based on mutual acceptance of each other's e-identification mechanisms. However, a number of issues need to be resolved to enable the cross-border use and acceptance of e-identification in practice.

As a first step, under the already mentioned ICT PSP, a large-scale pilot project (called "STORK") addresses specifically the interoperability of e-identification in public services. The STORK pilot project considers a model of interoperable electronic identity mutually recognised in all Member States, but which allows Member States to keep their systems and practices in place.

The pilot project will be a first step toward interoperability. It is expected to demonstrate solutions in specific areas which could then be extended to other areas. Moreover, depending on the results of the pilot, the Commission will determine if and what additional actions are needed after the results have been delivered in 2012.[20]

Actions:

- **By end of 2009:** The Commission will update the country profiles of the IDABC study on "e-ID Interoperability for Pan European e-Government Services". This will allow Member States and the Commission to keep up with developments in the use of e-ID in the Member States.
- **By end of 2009:** The Commission will, in cooperation with Member States, launch specific surveys on the use of e-ID in Member States, complementary to and in support of the STORK project (e.g. in support of the further development of common specifications for e-identification interoperability).
- **After the delivery of results of the STORK project**: The Commission will determine if and what additional actions might be required to enable an effective EU wide usage of e-ID.

[19] http://ec.europa.eu/information_society/activities/egovernment/conferences/2005/index_en.htm
http://ec.europa.eu/information_society/activities/egovernment/docs/lisbon_2007/ministerial_declaration_180907.pdf

[20] The specific areas are: cross-border authentication platform for electronic services; student mobility; change of address; electronic delivery of documents; safe use of internet by children. Currently 13 Member States are involved plus Iceland, the project has 29 participants in total (private and public).

- **By 2012:** Member States are invited to demonstrate solutions for the cross-border use of e-ID in the STORK pilot project.

4. MONITORING AND IMPLEMENTATION

The implementation of the actions in this Action Plan will ensure a horizontal and coordinated approach to facilitate and enhance the cross-border use of e-government applications in all areas of the internal market. It will contribute to a better functioning of the internal market by offering a comprehensive approach to allow businesses and citizens easier access to cross border Government services. The means to be put in place will contribute to the improvement of the current framework and a further convergence of technical solutions. The added value for the private sector lies in the widespread use of tools enhancing secure electronic procedures which can also be deployed in Business to Business and Business to Consumers transactions.

The Commission will, in close cooperation with the Member States, monitor the implementation of the Action Plan; the aim being to ensure the coherence of the suggested measures, of the various legislative requirements at EU level and of relevant operational projects such as the CIP pilot projects. In particular, it will seek an ongoing dialogue with Member States to accompany this Action Plan, including the Member State authorities responsible for competitiveness and internal market policies.

Implementation by the Commission and Member States of this Action Plan and monitoring of progress are part of the follow up to the Single Market Review. A year after the adoption of this Action Plan the Commission, together with the Member States, will start reviewing the progress achieved, with a view to submitting a progress report to the Council in 2010. Member States are invited to provide the Commission with all the relevant information on the implementation and results of the actions proposed to ensure cross-border interoperability.

On the basis of the progress report and of a discussion with Member States in the relevant fora, the Commission will assess whether further horizontal and/or sectoral initiatives are needed.