

Response to *Digital Agenda for Europe*: Electronic identification, authentication and signatures in the European digital single market

Public consultation

(See <http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=eid4&lang=en>)

Note: When people outside the UK in Europe refer to ‘electronic signatures’ they actually mean ‘digital signatures’ (confusingly called the advanced electronic signature in the Directive). Please do not be confused by this, because this form of signature is not used widely, unless people and legal entities are forced by legislation to use them (for articles on their low use until forced to use them, see various issues of the *Digital Evidence and Electronic Signature Law Review*.)

Background

This is a collaborative submission from a group of academics based in the UK with expertise in information technology law and related areas. The preparation of this response has been funded by the Information Technology Think Tank, which is supported by the Arts and Humanities Research Council and led by the SCRIPT/AHRC Centre for Research in Intellectual Property and Technology, University of Edinburgh.

1. Respondent information

This response has been prepared by Mr Stephen Mason with some involvement by Mr Michael Bromby.

Stephen Mason is a barrister (<http://www.stephenmason.eu>) and an accredited mediator, with an interest in electronic signatures, authentication, security, electronic evidence, e-mail and internet use, interception and monitoring of communications, data protection and privacy. He is an Associate Research Fellow at the Institute of Advanced Legal Studies in London, a member of the IT Panel of the General Council of the Bar of England and Wales and an independent Board Member of tScheme Limited (tScheme is the national body responsible for accreditation and supervision referred to in Article 3(4) of the EU electronic signature Directive).

He is the author of *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2011), and the general editor of *Electronic Evidence*, (2nd edn, LexisNexis Butterworths, 2010), and *International Electronic Evidence*, (British Institute of International and Comparative Law, 2008). He is the electronic and digital signatures editor and author of Chapter VI ‘Electronic and Digital Signatures’ for the practitioner loose-leaf textbook by M-T. Michèle Rennie *International Computer and Internet Contracts and Law* (Sweet & Maxwell), and the founder, general editor and publisher of the *Digital Evidence and*

Response to Digital Agenda for Europe: Electronic identification, authentication and signatures in the European digital single market Public consultation

Electronic Signature Law Review (<http://www.deaeslr.org/>), now in its eighth year, and which is an international focal point for researchers in the area.

Mr Michael Bromby is a reader in law at Glasgow Caledonia University.

This response has been approved by the Executive of BILETA (the British and Irish Law, Education and Technology Association, <http://www.bileta.ac.uk/default.aspx>) and is therefore submitted on behalf on BILETA.

In addition, this response is submitted by the following individuals:

Mr Stephen Mason

Dr Abbe Brown, SCRIPT, University of Edinburgh

Mr Michael Bromby, Glasgow Caledonian University

Professor Joseph Cannataci, University of Central Lancashire

Mr Abhilash Nair, Sheffield Hallam University

Comments

The consultation process organized by the EU has set out a number of questions which people are requested to respond to. Unfortunately, the questions do not accurately reflect the reality about the use of electronic signatures globally, and certainly not in the EU. For this reason, the questions are considered below in brief, and the answers are supplemented by this commentary.

Stephen Mason was invited to attend the initial debate (*Stakeholder Workshop on “Digital Agenda for Europe: Electronic identification, authentication and signatures in the digital single market”*) (Room BU25 0/S1, 25 Avenue de Beaulieu, B – 1160 Brussels, Thursday 10.03.2011 from 10.00 to 16.30) on what legislative measures are needed to address the challenges ahead. The EU sent out invitations to high profile people who have the right insight to build a vision on electronic identification, authentication and signatures for digital single market. The objective of the workshop was to offer a platform for an exchange of views on the questions raised in the public consultation. In this respect, the workshop was an exemplary success, for which those organizing it are to be congratulated.

The following issues are of direct relevance to the consultation initiated by the EU, and bear careful scrutiny.

(1) Electronic identification, authentication and signatures

It cannot be emphasised too much that identification, authentication and electronic signatures are three separate topics, each with their own legal and practical complexities. The general agreement of those attending the initial meeting in Brussels was that the EU should deal with each of these issues separately. It is highly recommended that the EU adopt the view of those attending the meeting in Brussels, and consider each item in isolation from the legal, regulatory and practical point of view. To include each in the same legislative approach will only lead to a complex law (if a law is considered to be necessary), and by treating all the topics simultaneously, it is inevitable that the EU will not achieve much progress.

Many of the questions presuppose that the EU do not want to see different designs for electronic identity, which infer that the EU wish Member States to put in place a national database of ‘identity’. It is suggested that this is not desirable, and it will not be acceptable amongst some Member States.

(2) Electronic signature

For a primer on electronic signatures, see: <http://www.stephenmason.eu/e-signatures/>

There is a significant difficulty about the topic of electronic signatures in the EU. This was illustrated when a technical person involved in X509 at the meeting in Brussels indicated that they had never found any discussion on electronic signatures or the classification of electronic signatures. This comment was dispiriting for those who write on such topics, especially when they write on electronic signatures on a global basis. Two lawyers in England have written books on the topic. Each is complementary to the other. Lorna Brazell deals with legislation across the globe and standards in detail, and Stephen Mason deals with legislation and case law in detail and across the globe:

Lorna Brazell, *Electronic Signatures and Identities Law and Regulation*, (Second edition, 2008, Sweet & Maxwell)

Stephen Mason, *Electronic Signatures in Law*, (Third edition, 2011, Cambridge University Press)

There is a significant misunderstanding in the use of the term ‘electronic signature’ in Europe. In most European Member States, ‘electronic signature’ is taken to mean a digital signature (or ‘advanced electronic signature’ or ‘qualified electronic signature’). The terms used in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12 are confusing to people outside the EU (and also to many lawyers in the EU) that do not understand the code words in discussing electronic signatures. The fact is, the term ‘electronic signature’ is a generative term that includes all forms of electronic signature.

The consultation only refers to digital signatures, yet the vast majority of on-line trading of goods and services uses other forms of electronic signature, such as the ‘I accept’ icon, the PIN and typing a name into an e-mail. Digital signatures tend to be only used when they are made mandatory by legislation (for which see Ugo Bechini, ‘Bread and Donkey for Breakfast how IT law false friends can confound lawmakers: an Italian tale about digital signatures’, (2009) 6 *Digital Evidence and Electronic Signature Law Review*, 79 – 82 and Pawel Krawczyk, ‘When the EU qualified electronic signature becomes an information services preventer’, (2010) 7 *Digital Evidence and Electronic Signature Law Review*, 7 – 18).

(3) Underlying assumptions

There are certain underlying assumptions that need to be addressed, based on the press release, ‘Digital Agenda: Commission launches public consultation on eSignatures and eIdentification’ (IP/11/198), Brussels, 18 February 2011. The main assumptions are:

- (a) There are ‘low levels of consumer and business confidence in online transactions’. No evidence has been submitted to demonstrate the veracity of this assertion. E-commerce is generally very effective across the globe. It seems to be somewhat unusual to initiate a discussion about an assertion that has no basis in fact.

(b) There are ‘difficulties in verifying people’s identities and signatures are a significant factor holding back the development of the EU's online economy’. No evidence has been submitted to demonstrate the veracity of this assertion.

(c) This statement muddles several concepts together: ‘Electronic signatures and electronic identification (eID) and authentication can be an important tool to enable both users and providers to rely on secure, trustworthy and easy-to-use online services but must work in all Member States to be effective’.

First, most form of electronic signature (clicking the ‘I accept’ icon, the PIN, typing a name into an e-mail) are easy and simple to use.

Second, there is no evidence put forward to suggest that there is a difficulty about using these forms of electronic signature across any jurisdictional boundary, never mind the EU.

Third, it is not necessary to prove your identity to buy a service or goods, with exceptions. The airline industry is required to obtain evidence of identity, and does so successfully without the use of digital signatures. If this assertion indicates an intention by the EU to mandate the use of digital signatures across all citizens of the EU, then e-commerce will cease.

(d) It also appears that there is also a determination to introduce ‘identity cards’ in the EU: ‘the development of new eIdentification and eSignatures authentication, such as alternatives to Public Key Infrastructure (PKI) currently in use for the easy management of electronic signatures, and eID-cards.’ This comment also appears to indicate that electronic signatures are, as far as the EU is concerned, another word for digital signature.

The most fundamental point to make about the particular technology of digital signatures is the assertion that digital signatures are, in effect, perfect. Digital signatures are marketed as a form of electronic signature that enables the recipient to prove a document or communication actually came from the person whose digital signature was used to ‘sign’ the data. This is not correct.

The private key of a digital signature is protected by a password. If you use a digital signature (or you are the recipient of a document or e-mail with a digital signature affixed) the most important point to be aware of is this: *the private key of a digital signature is only as good as the password that protects it.* This means that when the password is inserted into a computer to provide access to the private key of a digital signature (or PIN) it proves any of the following:

The person that keyed in the password (or username and password) knew the password (or username and password); or

The person with access to the computer (whether they were sitting in front of the computer or whether they obtained control of the computer remotely) did not need to know the password because the computer was instructed to remember the password.

Many people (including lawyers) actually believe that if the private key of a digital signature is affixed to a document or e-mail, it means that the digital signature was actually affixed by the person whose key it was. For evidence that this is not the case, see the case law relating to digital signatures in Olga I. Kudryavtseva, 'The use of electronic digital signatures in banking relationships in the Russian Federation', (2008) 5 *Digital Evidence and Electronic Signature Law Review*, 51 – 57 and Alex Dolzhich, 'Digital evidence and e-signature in the Russian Federation: A change in trend', (2009) 6 *Digital Evidence and Electronic Signature Law Review*, 181 – 183.

The comments noted below were previously set out in White Paper Number Seven, 'Electronic Signatures – Signing up to the Digital Economy' (InterForum, 1999) [this paper no longer seems to be available on the internet]. On page 3, the following comments were made:

'Just as possessing a credit card does not prove you are the rightful owner, electronic signatures do not categorically prove that a signed document came from the claimed sender. It only shows that someone had access to the token or PC on which the digital certificate and signing process was stored.'

If businesses thought that digital signatures (or 'advanced electronic signatures') were necessary to conduct business over the internet, the technology would be in wide use now. It is not.

Recommendations

(1) It is recommended that the EU consider each item (electronic identification, electronic authentication and electronic signatures) separately.

(2) Each Member State of the EU has implemented the Directive on electronic signatures in a different way, taking into account their legal and cultural norms. The way the Directive has been implemented has not caused e-commerce to fail. No evidence has been put forward to suggest that e-commerce between Member States is not effective because of the way electronic signatures are implemented in different Member States. It is recommended that in relation to Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12, the EU either:

- (i) repeal the Directive, or
- (ii) alter the Directive to be a Regulation, or
- (iii) repeal those parts of the Directive dealing with the technical details relating to advanced electronic signatures and qualified electronic signatures.

2. General expectations regarding EU legislation on e-signatures, e-identification and e-authentication

Question 1: Do you or does your organisation use e-signatures, e-identification and e-authentication? If the answer is 'yes' for what purpose?

Virtually every person and legal entity that corresponds using e-mail, text messages on mobile telephones and buys and sells goods and services on the internet, and uses debit and credit cards use one or more types of electronic signature.

Question 2: For what on-line transactions do you consider electronic identification, authentication and signature useful in the future?

Electronic signatures, particularly the 'I accept' icon, are already used for on-line transactions. Some commercial entities choose to make the buyer register to buy goods or services, others do not.

Question 3: What socio-economic benefits or drawbacks do you expect from the use of electronic signatures, identification, and authentication in other sectors of activity than yours?

It is not clear what this particular question means.

Question 4: Would a greater involvement by financial institutions in the provision of trusted e-signature and e-identification services have an effect on the take-up of e-signature and e-identification in other sectors?

Electronic signatures are widely used without 'trusted' intermediaries, so it is difficult to understand what this questions poses.

Question 5: Do you think that there are specific interoperability or security aspects that should be taken into account to foster the use of electronic signatures, identification, and authentication by way of mobile devices (for instance, requirements on the SIM card, on the handset, on the mobile telephone operator?)

Electronic signatures (unlike digital signatures) do not have any interoperability problems, so this question only appears to refer to digital signatures. Digital signatures (also called advanced electronic signatures amongst some EU Member States) are not used widely (unless a government requires the use of such forms of electronic signature).

Question 6: For which of the following trust services and credentials should legal or regulatory measures be considered at EU level in order to ensure their cross-border use and why?

Electronic seals; time stamping; long term archiving; authorisation/mandates; certified delivery of e-mail; official delivery address; electronic transferable records; pseudonyms; anonymous agents; certified electronic documents in general

The question to ask is why are governments interested in such topics, when governments did not regulate electronic signatures when they were introduced by the use of telegrams in the nineteenth century?

3. E-signature tailored to face the challenges of the digital single market

Question 7: How do you judge the take-up of electronic signatures in Europe?

Many forms of electronic signature are very widely used in Europe and across the world. The three most popular are: PIN, name typed in an e-mail, 'I accept' icon. The PIN was in use and accepted by judicial authorities before the introduction of any electronic signature laws.

Question 8: Which of the following issues have a negative effect on the up-take of e-signatures?

Cost of providing e-signatures; costs of using e-signatures; limited EU cross-border interoperability; lack of user-friendly signature solutions; limited number of services relying on e-signatures; lack of ancillary services such as registered documents delivery; insufficient legal certainty of electronic signatures implementations; transactions can sufficiently be secured by other means

This is a question about digital signatures. Digital signatures are not used by people because they are not necessary to buy and sell goods and services on-line.

Question 9: Which of the following specific issues have an effect on cross-border interoperability of e-signatures in Europe and should be addressed in a revised legal framework on e-signature (the references are to the articles and annexes of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures)

Unclear terminology in the Directive and heterogeneous terminology in national legislations; divergent interpretations of what is meant by the 'sole control' of the signatory (article 2.2); no common approach to the supervision of providers issuing qualified certificates to the public (article 3.2); ambiguities between supervision and accreditation (article 3.2 and 2.13); heterogeneous use by MS of the 'public sector derogation' (article 3.7); heterogeneous approach to security requirements (for instance, certification requirements on the signing software in some countries); heterogeneous status and roles of the national security certification bodies (article 3.4); no EU list of signature equipment formally recognised as 'secure signature creation devices' (Annex III); no common EU list of admissible e-signature cryptographic algorithms; insufficient harmonisation of profiles of qualified certificates; heterogeneous financial liability for qualified certificate issuance; unidentified legal status of signature validation and liabilities of validation service providers; missing legal provisions on signature verification and validation (Annex IV)

The EU Directive was not necessary to enable electronic signatures, because electronic signatures were already in use for over 10 years before the Directive

was implemented, especially electronic signatures in the form of a name typed in an e-mail and the PIN.

Question 10: Which, among the following options could be solutions for signature verification and validation at EU level?

Government validation service for each Member State; private validation services; European central validation service; other

This question refers to digital signatures, because other forms of electronic signature do not suffer from the same problems as digital signatures.

Question 11: Do you have specific expectations from e-signature standardisation to cover?

This question refers to digital signatures, because other forms of electronic signature do not suffer from the same problems as digital signatures.

Mass signature (server signing); mobile signature creation device; remote signature; others

This question refers to digital signatures, because other forms of electronic signature do not suffer from the same problems as digital signatures.

Question 12: Do you use ‘qualified’ e-signatures?

This question refers to digital signatures: they are only generally used if a government forces their use, for which see:

Ugo Bechini, ‘Bread and Donkey for Breakfast how IT law false friends can confound lawmakers: an Italian tale about digital signatures’ *Digital Evidence and Electronic Signature Law Review*, 6 (2009) 79 – 82

Pawel Krawczyk, ‘When the EU qualified electronic signature becomes an information services preventer’ *Digital Evidence and Electronic Signature Law Review*, 7 (2010) 7 – 18

Question 13: What is your view on the need to revise the security provisions of ‘qualified’ e-signatures?

Security requirements should be relaxed; the current provisions should stay as they are; security requirements should be strengthened to be ready to face future security threats

It is not necessary to use qualified signatures.

Question 14: Would a classification of a range of e-signatures be desirable to match different levels of security?

No.

Question 15: Should ‘electronic consent’ be recognised formally by future European legislation? If yes, should legislation (where necessary supported by

operational and technical standards) define specific requirements on security of interfaces, reliability of the process, liability, archiving.

No.

Question 16: Should ‘electronic consent’ be considered as equivalent to electronic signatures? If no, to what extent would an effective consent differ from a signed document?

What is the difference between ‘consent’ and a ‘signature’?

Question 17: Are there specific aspects that should be taken into account to address electronic archiving?

4. Principles to guide e-identification and e-authentication in Europe

Question 18: Do you see a need for additional legal or regulatory measures on electronic identification at EU level? If yes, in your opinion, what are the general principles that should underlie the legal provisions on the mutual recognition and acceptance of e-identification at EU level?

No.

Question 19: What effects for the digital single market do you expect from legal provisions on an EU wide mutual recognition and acceptance of eID issued in the Member States?

People will stop using the internet.

Question 20: How could users provided with electronic identification and authentication means benefit from their mutual recognition and acceptance across Europe and in which sectors?

Increase of user convenience; simplification of obtaining access to on-line services; reduction of numerous user identification and passwords; reduced exposure to misappropriation of identity

What problems are there in relation to this topic?

Question 21: What are the specific aspects that should be taken into account to achieve cross-sector interoperability of electronic identities?

Common legal basis; common specifications for electronic identities; identity portability; use of multiple identities issued by different providers; personal data protection

This is not necessary unless the question relates to digital signatures.

Question 22: Please indicate the experiences and lessons learnt in the private sector that could be transferred to the public sector.

Do not impose one form of electronic signature on people that they do not need.

5. Legislative measures for the challenges ahead

Question 23: What European Union legislative measures on e-signatures, e-authentication of natural and legal person claims as well as e-identification would be appropriate in your opinion to best meet the challenges in the digital single market?

Revise the existing legal framework to include all requirements relating to e-signatures, e-identification and e-authentication and related issues; opt for different measures to allow for distinct focus, progress, and speed of adoption; focus on light and limited measures to facilitate faster decision and implementation; no EU legislation is needed

None.

6. Research and innovation

Question 24: On what issues should EU R & D and standardisation focus to have all the necessary technology to improve eID management?

Question 25: On which technologies should Research & Development focus to improve the usability of e-signatures and electronic identification for end users and to facilitate the use for service providers?

Question 26: What technologies could contribute to overcoming the lack of trust in electronic identification, authentication and signatures in the European Single Market (for instance, addressing the ‘what you see is what you sign’ issue)?

For an article on this topic, see Nicholas Bohm, ‘Watch what you sign!’, (2006) 3 *Digital Evidence and Electronic Signature Law Review*, 45 – 49

7. Others

Question 27: Europe is fully part of the global economy. However, the forthcoming legal framework cannot cover non EU countries. Are there nevertheless international issues that should be taken into account?

Yes. If you want people from outside Europe to stop trading with European commercial entities, force all Europeans to have a digital signature.

Response to Digital Agenda for Europe: Electronic identification, authentication and signatures in the European digital single market Public consultation

Question 28: Would you like to share some best practice examples outside Europe?

Question 29: Are there any other issues which you think should be addressed by policy makers?

End of submission.