BCS, The Chartered Institute for IT
Consultation Response to:

European Commission:
Digital Agenda for Europe – Electronic identification, authentication and signatures in the European digital single market

Dated: 15 April 2011
Submitted via EC’s online survey
This page is left deliberately blank.
BCS, The Chartered Institute for IT

The Institute promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. We deliver a range of professional development tools for practitioners and employees.

A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

www.bcs.org
Section 1: (Respondent Information for BCS to complete)

Section 2: General expectations regarding EU legislation on e-signatures, e-identification and e-authentication
Summary – to create a secure digital single market; removing barriers to enable seamless access to web-services and online interaction.

(Question 1: questions for organisations to answer)

Question 2:
For what online transactions do you consider electronic identification, authentication and signatures useful in coming years?
Select:
- eGovernment services
- electronic public procurement
- eCommerce transactions
- eBusiness transactions
- online banking and financial transactions
- Issuance of authentic electronic documents
- secure archiving or storage of authentic electronic documents or others.

Comments:
All of the above online transactions (and more) would benefit from eID, eAuthentication and eSignatures in coming years as Internet Protocol (IP) based communications over the Internet/WWW become the common and standard bearer service for online transactions. eGovernment services are an obvious starting point as implementation of IP based services will greatly reduce the costs of interaction by citizens, corporations and public servants. Tax collection and benefits payment will be substantially cheaper to process but these depend – as with all the other listed services above, and more – upon a reliable means of identification & authentication that can be delivered over fixed and wireless communications networks.

The US government proposal for a National Strategy for Trusted Identities in Cyberspace (NSTIC) is a model that should be closely monitored for international adoption. The reliable delivery of network enabled identification and authentication is a pre-requisite for trusted transactions to be carried out in an era of internet enabled communications.

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?

Comments:
The benefits hinge upon drastically reduced transaction costs coupled with improvements in trust levels for all parties involved in electronic transactions. The dramatic increase in trade over the Internet in the last two years – by individual consumers, corporations and government agencies - indicates the further potential demand for electronic transactions. The limitations, in terms of...
fraudulent and criminal use of internet based transactions, have only just started to be seen by law enforcement services.

The drawbacks that counterbalance the wide-spread introduction of standardised eID, eAuthentication and eSignatures stem from the perception that such mechanisms will be proposed by and used for government surveillance of the general population. If, however, the model of credit card transaction processing and settlement, as implemented by the financial services sector, is considered instead of the centralised government led approach, then multi-party, decentralised and federated services can be adopted without the need for the all-pervasive central database function.

Further drawbacks will become apparent as the use of electronic transactions continues to grow without an accompanying trusted identification/ authentication process. Crime and fraud will be a significant and ever present partner in this world. The Department for Work and Pensions, for example, is expecting to process all its benefits payments through electronic services within 12 months and this represents cash flows of over £3billion per week. This provides a clear target for criminal activity which is greatly aided by having no trusted means for electronic identification.

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

**Comments:**
Financial - and legal - institutions have a major part to play in the take-up of these trusted services for several reasons. They are not government agencies and are already operating in a market environment where federated (peer-to-peer) transactions are common and standardised. They have established means for developing and agreeing mutually beneficial new services and they also have mechanisms for keeping these services up to date as market forces change the environment e.g. the introduction of Chip and PIN as credit and debit card fraud increased with the increase in market size.

**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 through mobile devices (e.g. requirements on the SIM cards, on the handset, on the mobile operator)?

**Yes**

**Select:**
Legal aspects (including liability), business, operational, technical, standardisation, others.

**Comments:**
All of the above listed topics will be relevant but the wireless network operators already have mechanisms to address them. The GSM (and now 3GPP) market have an extremely well developed environment for discussing and agreeing common standards that will be adopted across their interconnected infrastructures. This applies to the network operators, their infrastructure providers and their handset suppliers as well as, increasingly, the applications developers who deliver software applications to the handsets across the infrastructure.

The EU and sovereign government roles are to ensure that the GSM/3GPP environment implements the necessary standards in an honest, balanced and transparent fashion so that neither incumbents...
nor new entrants are penalised. Above all, the government role is to ensure that the individual user is protected and, as far as possible, secure in their use of trusted services such as eID, eAuthentication and eSignatures. Law is set by government and the judicial system must be seen to be fair by the general population. Security and protection of the population is the first responsibility of government.

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

**Select:** Electronic seals, time stamping, long term archiving, authorisations/mandates, certified delivery of mail, official delivery address, electronic transferable records, pseudonyms, anonymous agents, certified electronic documents in general, others (please list).

**Comments:**

All of the items listed above should be considered at EU-level as a pan-European solution is required rather than separate country specific solutions. Indeed, global solutions are required rather than trading bloc specific solutions so even higher level legal and regulatory approaches should be considered at ISO and UN levels.

However, care should also be taken to avoid any EU-level regulatory body from delving into too much technical detail on some of these topics whilst the broad regulatory sweep and direction is overlooked.

**Section 3:** e-Signatures tailored to face the challenges of the digital single market

**Summary – Creating a wide electronic signature and identification infrastructure for all interested operators which could also stimulate innovative services.**

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

**Select:** Marginal, moderate, high, very high

**Comments:**
Marginal currently.

Only a few organisations make any use of electronic signatures and these are, by and large, portions of sizeable corporations or small government agencies that have in depth knowledge of the complexities inherent in eSignature infrastructure. Often they have significant security related interests which they use to justify the investments they make.

The whole topic needs to be dramatically simplified in a trusted fashion to be implemented by broad sections of the commercial and government domains.

**Question 8:**
*Which of the following issues have a negative impact on the uptake of e-signature? You may select up to three answers that have according to you the most important impact.*

**Select:**
Costs 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-signature, lack of ancillary services such as registered documents delivery, insufficient legal certainty of electronic signatures implementations, transactions can sufficiently be secured with other means, others.

**Comments:**
Lack of user-friendly signature solutions > leading to
Limited numbers of services relying on eSignature > leading to
Insufficient legal certainty of eSignature implementations
The current situation is similar to the chicken and egg scenario where the limited availability of usable eSignature solutions leads directly to the shortage of services making use of them and therefore an inadequate legal environment requiring and depending upon the services.

Whilst some individuals involved in email and file transfers do hold the requisite electronic certificates, the vast majority of individuals do not and it is quite straightforward to carry on communicating regardless in an untrusted fashion. Whilst this situation continues, there is little driving force for the widespread adoption of eSignature services.

**Question 9:**
*Which of the following specific issues have an impact on cross-border interoperability of e-signatures in Europe and should be addressed in a revised legal framework on e-signature (the references point to the articles and annexes of the eSignatures Directive)?*

**Select:**
- Unclear terminology in Directive 1999/93/EC and heterogeneous terminology in national legislations
- Divergent interpretations of what is meant by the "sole control" of the signatory (art. 2.2)
- No common approach to the supervision of providers issuing qualified certificates to the public (art. 3.2)
- Ambiguities between supervision and accreditation (art. 3.2 and 2.13)
- Heterogeneous usage by MS of the "public sector derogation" (art 3.7)
- Heterogeneous approach to security requirements (e.g. certification requirements on the signing software in some countries)
- Heterogeneous status and roles of the national security certification bodies (art. 3.4)
- No EU list of signature equipment formally recognised as "secure signature creation devices" (Directive 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.
- Undefined legal status of signature validation and liabilities of validation service providers
- Missing legal provisions on signature verification and validation (Directive Annex IV)
- Other

**Comments:**
All of the above issues contribute, to a greater or lesser extent, to the limited take-up and limited trust in a pan-European eSignature approach. This will not be fixed by identifying issues of detail for legislation at the EU level. The EU regulatory role should be to identify directions for the market that are to be encouraged and to define and apply legislation that moves the market towards adopting standards that support and encourage federated networks in adopting interoperable solutions with and between trading blocs.
Examples above including lack of ‘secure signature creation device’ lists and lack of common admissible cryptographic algorithms are simply detailed examples of market failures where the legislation is currently ahead of market implementation.

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

**Select:**
Governmental validation service per member State, Private validation services, European central validation service, other.

**Comments:**
The most successful market approach is always likely to be a federated solution where multiple free market operators offer competitive but interoperable options to the market. The EU and national regulators job is to create and encourage the market to develop and to encourage multiple providers to offer solutions into the market.

Government provided solutions on a national or supra-national (EU) basis are most likely to be viewed with suspicion by the general public and the commercial sector. Independent, private corporations – perhaps banks – are more likely to successfully offer trusted federated services into the market.

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

**Select:**
Mass signature (server signing), mobile signature creation devices, remote signature, others.

**Comments:** (note these comments are not included in the survey)
All of the above – and many more applications and components besides – should be covered by eSignature standards. Assuming a trusted common approach to eSignature can be identified (based upon international standards), then it should be possible to extend the process on a wider and wider basis to applications where an electronic signature is relevant. This is part of the basis for the Trusted Computing model which is starting to be supported by very widespread hardware support for the Trusted Processing Module (TPM).

**Question 12:** Do you use "qualified" e-signatures?

**Yes or No**
No – not currently. (Note: these comments not included in the survey)
However it should be considered a fundamental requirement that qualified eSignatures be supported where the full protection is not necessary and a lower level of protection is satisfactory. This is akin to the case where, at a bar, it is not necessary to prove who you are but it is sufficient simply to prove that you are over 18 in order to buy an alcoholic drink legally.

There are many situations where what is needed is an attribute of an individual (eg over-18) and "not* anything that could be used to identify them. "Identity" systems should definitely be constructed to support such disclosure of trustworthy attributes without accompanying identification information.

A concern is that the focus on eGovernment applications may cause this useful (both for commerce and privacy) function to be treated as a lower priority, resulting in exactly the sort of bad PR ("big brother systems") that the response correctly warns about.
Question 13:
What is your view on the need to revise the security provisions of "qualified" e-signatures?
Select:
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

Comments: (Note: these comments are not included in the survey)
The current provisions should stay as they are.

The market will need to be developed to handle both full and ‘qualified’ eSignatures and both should be capable of being accepted in current and future solutions. A number of ‘levels of qualification’ should be defined in order that interoperability be retained.

Question 14:
Would a classification of a range of e-signatures be desirable to match different levels of security?
Select:
No, a classification would bring no added value
No, because the negative impacts of a classification on complexity, implementation costs and ease of use would out weight its advantages.
Yes, a classification would be convenient but only as a technical standard without being defined by law.
Yes, a classification would be convenient and it should be defined by law.
Yes, a classification would be convenient, it should be defined by law and a legal effect should be associated to each or some classes.
I don’t know / no opinion

Comments:
Yes, a classification would be convenient but only as a technical standard without being defined by law.

There will be a variety of ways in which eSignatures are applied in the market and regulators should be concerned to ensure inter-operability rather than try to ‘pick winners’. As such, there will be a need to have an agreed classification structure but this should not be defined in law as legislation will, inevitably, fail to keep up with changes in technical implementation. Standards need to be set for guidance, compliance and interoperability purposes.

Question 15:
Should "electronic consent" be recognised formally by future European legislation?
Yes or No
Security of user interfaces (e.g. requirements on the display, notification or warning that consent is about to be given by the next click)
Reliability of the process (e.g. verifiable execution trails, guarantee by a trusted third party that the execution trails cannot be modified)
Liability
Archiving
Others
Comments:
Yes, electronic consent should be recognised formally by future European Legislation. Electronic consent will become an essential part of managing electronic transactions in the IP/internet enabled world but there will need to be supporting technical measures adopted for managing the ‘electronic consent’ so that non-repudiation, etc can be delivered.

Question 16:
Should “electronic consent” be considered as equivalent to electronic signatures?
Yes or No
Comments:
No – electronic consent is not directly comparable or equivalent to an eSignature.
For equivalence to apply, there needs to be some mechanism to effectively tie together consent with a trusted mechanism for assuring the identity of the person providing consent. Without this linkage, there can only be limited reliance upon the identity of the consenting party.

Question 17:
Are there specific aspects that should be taken into account to address electronic archiving?
Yes or No
Comments:
No, there are no specific aspects with respect to electronic archiving that should not already have been taken account of in storage, retrieval and confidentiality.

Section 4: Principles to guide e-identification and e-authentication in Europe
Summary – Using at least one electronic identity for each person which can be used across borders in Member States. It can be argued that such an identity could be beneficial for the trust and interoperability of e-services including eGovernment services.

Question 18:
Do you see a need for additional legal or regulatory measures on electronic identification at EU-level?
Yes or No
Select:
Non-discrimination, transparency, liability eID provider, affordability, accountability, federated approach, centralised approach, cross-sector permeability, personal data protection and privacy, others

Comments:
Yes – the EU legal and regulatory interest should be on encouraging the adoption of a private sector led, federated model for electronic identification.
Rather than the EU level trying to ‘pick winners’, EU regulatory involvement should be concentrating on striving to ‘level the playing field’ for private sector, federated solution providers in order to support transparency in the market and ensure non-discrimination and personal data protection and privacy whilst ensuring the lowest possible costs for electronic identification.
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?
Select:
Legal certainty, increase of economies of scales for eID solutions, reduction of administrative burden, increase of cross-border digital mobility, reduction of fraud, long-term sustainability of eID solutions, other.

Comments:
All of the above listed aspects will be boosted within the digital single market through EU-wide recognition and acceptance. If the EU can develop relations with other trading blocs and ensure mutual recognition and interoperability of eID approaches leading to global acceptance then this will be further significant advantage.

It must be clear that use of electronic signature must be decoupled from any ancillary surrender of privacy and it must not be tied in with agreement to processing that reduces an individual's rights under the Directive or obliges the individual to agree to other processing not essential to the use of the signature. This standard should be obligatory not merely 'good practice'.

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?
Select:
Increase of user convenience, simplification of access to online eservices, reduction of numerous UID/passwords, reduced exposure to ID theft, others.

Comments:
All of the benefits listed would apply but the primary benefit will be increased trust in electronic transactions by both consumers and traders/ corporations. Individual users will benefit through simplification of access, improved user convenience and reduction in the need for increasingly complex passwords whilst retailers and corporations will benefit from increased trading volumes without significant increases in fraud and crime.

In addition there will be significant benefits from common approaches, as implemented by systems integrators and service providers, in the reduction of variations of eGovernment services delivered within nation states. A key driver of eID is the resultant reduction in transaction costs and this is particularly relevant with respect to eGovernment services where cost reductions can lead to tax reduction with a benefit to all users.

Question 21:
What are the specific aspects that should be taken into account to achieve cross-sector interoperability of electronic identities?
Select:
Common legal basis, common specifications for electronic identities, identity portability, use of multiple identities issued by different providers, personal data protection, others.

Comments:
Cross-sector interoperability will be best delivered through the creation of an open market for private sector, federated solutions. As such all the topics listed are relevant.
Question 22:
Please indicate experiences and lessons learned in the private sector that could be transferred to the public sector.

Comments:
There is a significant reference programme that stretches across multiple government and contractors known as the Transglobal Secure Collaboration Program (TSCP – www.tscp.org) that can provide an operational model for federated eID/ eAuthentication and eSignatures. This program centred upon the development of the F-35 or Joint Strike Fighter where a number of governments and their contractors required trusted information sharing across national and corporate boundaries. Government members currently include the US, Dutch, French and UK Ministries of Defence whilst significant corporates included EADS, BAe, Rolls Royce, Finmeccanica, Northrop Grumman, Boeing and Lockheed Martin. A foundation for this approach was the US HSPD-12 (Homeland Security Presidential Directive) which mandated the adoption by US Government and contractors of PIV (Personal Identification Verification) and international PIV-I standards.

One of the most significant lessons learned was that the preparation of the information sharing agreements for acceptance by all the participants is the single largest task of such a mutual programme. The non-competitive legal basis for this approach and preparation of the agreements themselves is the most challenging step in developing such a joint service. This is a key task to be undertaken by or under the supervision of EU-level regulators. Once the legal and documentary base of the service is developed and agreed, the actual implementation of a federated eID/ eAuthentication and eSignature service is much more straightforward.

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 of the digital single market?
Select:
- Revise the existing legal framework embracing 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
- Don't know
- Other

Comments:
The Institute has no comments on this item.

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

Comments:
The Institute has no comments on this item.
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 deployment for service providers?

Comments:
The Institute has no comments on this item.

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

Comments:
The Institute has no comments on this item.

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?

Comments:
The Institute has no comments on this item.

Question 28:
Would you wish to share some best practices examples outside Europe?

Comments:
The Institute has no comments on this item.

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

Comments:
The Institute has no comments on this item.

End

A summary of the outcome will be published on the http://ec.europa.eu/egovernment
Our response has been successfully submitted on 15 April 2011. The IPM reference number is:
845086304321310511