

**European Commission
Directorate-General Information Society and Media**

**PUBLIC CONSULTATION ON DIGITAL AGENDA FOR EUROPE:
ELECTRONIC IDENTIFICATION, AUTHENTICATION AND SIGNATURES IN
THE EUROPEAN DIGITAL SINGLE MARKET**

The European Commission has launched a public consultation on Digital Agenda for Europe: Electronic identification, authentication and signatures in the European digital single market. Finland Chamber of Commerce submits the following statement.

Question 1: Do you / Does your organization use e-signatures, e-identification and e-authentication

No

Question 2: For what online transactions do you consider electronic identification, authentication and signatures useful in coming years?

eGovernment services
eCommerce transactions
Online banking and financial transactions
Secure issuing and archiving of e-documents
Issuance of authentic electronic documents

Ageing of the population, long physical distances between customer and service providers, developed applications/devices and infra help the adaption of these e-services in the future.

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?

Processing costs in public/private sector decrease due to automated online processes which authentication of the customer/user is just one step in the whole chain. There is no need to build service branches to "meet" customers, online service will do the same in less cost. By providing e-services on a wide scale and automating processes workforce can be directed toward more productive work and better service providing. Drawback: individuals may not use service (especially elder people) if they don't rely on the service and their data integrity.

For electronic signatures, identification, and authentication to be useful on a wider scale, it is imperative to expand the concept from "digital IDs" to more granular authorizations. A "digital signature" without knowledge of the semantics is too inflexible, and provides no useful concept of transaction value. Digital authorizations need to be small, quick, and of limited risk when performing small digital transactions, and "full-blown" legacy digital signatures are only required on formal, high-value transactions.

All current solutions more or less ignore the critical "trusted terminal" problem, whereas current Web services are constantly attacked using trivial phishing and malware attacks.

To minimize the potential drawbacks proper testing with simple and widely accessible services where errors in the process of issuing of electronic documents / ID's would not risk significant benefits (ex fishing permit, bus ticket) and spending some time to collect experiences and learnings and spread the same widely before actually implementing this in an actual service where a falsely issued document has substantial significance (ex marriage certificate, certificates from school, criminal register extract).

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?

Banks in general are regarded as trustworthy partners. People rely their funds and investments in the hands of the bank therefore they may as well rely on e-services provided by banks. Financial institutions are early adaptors of such e-services at least in Europe so there's is a strong argument to involve them also in the future. Financial institutions play a key role in helping consumers' adaptation of e-signature and e-identification: financial institutions build the user behavior since financial services are the only area where there is a frequent usage of services requiring e-signature and e-identification. Same user behavior is automatically transferred to other sectors which lead to the economy of repetition.

However in addition to financial institutions relying parties may also carry or help carrying part of the burden of consumer protection.

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

Interoperability is a key requirement on mobile platform. Mobile operators have already built interoperability in the mobile network, which helps achieving economy or re-use. The network should be used both cost and implementation pace wisely. Utilizing the SIM provides a device free and (near) operating system free platform to build from. Key is to utilize standards to succeed in creating an interoperable environment. The requirement to succeed is to reach high coverage from day one. Focus should be put on the issuance process for the end-to-end process to be considered trusted. Governance/supervision is therefore needed. Operators would need to meet the same level of requirements on the issuance process and liability as governments and financial institutions are required. Technical protection e.g. against malware is a necessity. Only trusted mobile operators should be able to issue SIM based e-ids.

Standards should be adopted in as neutral way as possible in order not to distort competition, preferably through a public bid inviting proposals for alternative methods and identifying objective criteria for potential respondents. Interoperability would hopefully lead into better coverage for use of e-identification / e-authentication and thus ease of use of electronic services for consumers.

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?

Certified Electronic documents in general

The list includes technical solutions of trust building services. The revised legal framework should not regulate technical solutions in detail.

However if regulatory measures are to be considered, they need to define properly what is regarded a certified electronic document and subject to which conditions and ensure the term may only be used as reference to actual certified documents to avoid confusion of consumers.

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

The perception regarding take-up of electronic signatures varies according to the environment, e.g. in banking the take-up may be high compared to IT security providers that may consider the take-up only marginal.

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.

Cost of using e-signatures

Limited EU cross-border interoperability

Transactions can sufficiently be secured with other means

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?

Heterogeneous status and roles of the national security certification bodies

No common approach to the supervision of providers issuing qualified certificates to the public

Undefined legal status of signature validation and liabilities of validation service providers.

Other: lack of commonly agreed state provided unique person identifiers cross border (for example social security number) and divergent interpretations of concept of e-signature.

From technical angle the eSignature directive restricts the technical development and innovations by concentrating on the PKI technology.

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

European central validation service

European central validation service if standard is interoperable between all EU-countries. This would compete seriously with local solutions offered today. Any validation – private as well as European Central – service that the provider is governed/supervised that meets the commonly set requirements.

Question 12: Do you use “qualified” e-signatures?

No

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

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

Classification, and thereby authorization and limiting of the consumer liability through a signature is essential to the rapid uptake of limited-value services.

Classification defined by law with legal effect assigned to each or some classes should be the next step after there is more experience of classification as a technical standard.

Question 15: Should "electronic consent" be recognised formally by future European legislation?

Yes

Reliability of the process

Liability

Archiving

Yes if the liability of consumer with regard to the so called trusted terminal problem can be resolved. Consider electronic commerce applications, where a user – a sole human being – wishes to make business with a remote partner. If sensitive data travels through an insecure network, it should be protected e.g. by cryptographic algorithms. When a protocol participant is supposed to be a human, it is implicitly assumed that she uses a terminal (e.g., a PC), which stores cryptographic keys, performs cryptographic computations, and handles network connections on behalf of her. It is also implicitly assumed that the terminal is trusted by the user for behaving as expected, and in particular for not compromising the security of the user (e.g., by leaking her keys). Unfortunately, most terminals cannot be called 'trusted'. Either because the party operating the terminal is not trusted by the user, or the user cannot be convinced that the terminal does not have hidden features. Moreover, it is often very hard to check if the hardware or software of the machine has been tampered with. This clarification is quoted from <http://www.hit.bme.hu/~buttyan/publications/BertaBV04itcc.pdf>.

Due to widely adopted principle of freedom of form, the regulatory framework should include all kind of declaration of intent – not mere consent or corresponding detailed transactions.

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

Yes

Personal data protection and privacy, encryption of the data at the host side, liability questions, ensuring the constancy of the signed content, audit trails, control of people in charge of archiving (role of IT admin users) and administering such archives (backups, actual location, personal data protection).

Question 18: Do you see need for additional legal or regulatory measures on electronic identification at EU-level?

Yes

Liability of eID provider
Accountability
Personal data protection and privacy

Defining liability of the party requesting electronic identification and for what type of situations such identification may be required.

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?

Legal certainty
Long-term sustainability of eID solutions
Reduction of administrative burden
Increase of cross-border digital mobility.

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 access to online services
Reduction of numerous UID/passwords.

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
Others

Technology neutrality, device independence.

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

Finland Chamber of Commerce is aware of following experiences and lessons learned.

E-identification services should not be priced as a separate element towards end-users (e.g. HST-card in FI that failed). Promote 4-corner model to ensure effectiveness and competition in the market. Very low cost of usage - benefits come from cost savings on physical processes and freed labor for more productive work. Devices should support multichannel usage. There should be no technical installations on the end user environment.

The question of reliably and strongly identifying the customer is not nearly as important as the ability to ensure the validity of a commercial transaction and the capability to charge for services provided. As a matter of fact, due to the increase of identity theft, and strict regulations regarding privacy protection, there is clear incentive to limit the amount of personal information collected to a minimum. Thus services that provide only the bare minimum of identification, but strong authentication and proof of payment are probably to be preferred.

Specifications developed for e-signatures, e-authentication and e-identification should allow for different implementations and EU directives should not regulate a one specific type of solution as a fix for all e-signature/e-authentication/e-identification needs, rather the consumers should be allowed to decide which methods work for them from a set of alternatives, as long as the interoperability issues are sufficiently resolved through the specifications.

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?

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

The revised legal framework should be technology neutral and instead of only PKI technology allow also other technical solutions and especially technical development.

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)?

Reduce the focus on strong identity and signatures and work on providing efficient, interoperable, and cost effective measures for reliable authorization of online transactions and payments. Addressing the “what you see is what you sign” issue can only be tackled by reducing the authorization of signatures to the necessary minimum, because the rapid development in consumer terminals (PCs, handsets, tablets, etc.) makes a proper solution of the trusted terminal dilemma almost infeasible.

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?

Technical interoperability and standardization needs to be global, not EU-specific. To the extent feasible the legal framework should aim at finding a solution that not only works within EU but also outside EU.

FINLAND CHAMBER OF COMMERCE

Leena Linnainmaa
Deputy Director General