



# Public consultation on electronic identification, authentication and signatures in the European digital single market

## Overview of responses

### INTRODUCTION

On 18 February 2011, the European Commission launched<sup>1</sup> in the context of the Digital Agenda for Europe<sup>2</sup> a public consultation regarding electronic identification, authentication and signatures, which closed on 15 April 2011. The purpose of the public consultation was to provide input for policymakers on how electronic identification, authentication and signatures can contribute to deliver the European digital single market.

The European Commission received more than 400 contributions from a wide range of actors, including Member States, EU and national organisations, regional and local authorities, business and professional federations, individual companies, NGOs, and many European citizens. Most contributions were made via the Commission's online consultation tool (IPM — Interactive Policy Making), and several others were sent in as separate submissions.<sup>3</sup>

This document provides an overview and a summary of the provided responses, and of the main trends emerging from the consultation. The report is mostly based on data and material received through the online tool used for the consultation, but also takes into account the submissions sent separately to the Commission.

This report consists of six primary sections: firstly a description of respondent profiles, followed by five sections that correspond to the five topics examined by the consultation, leading to the following report structure:

---

<sup>1</sup> See the press release at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/198&format=HTML&aged=0&language=EN&guiLanguage=en>

<sup>2</sup> See [http://ec.europa.eu/information\\_society/digital-agenda/index\\_en.htm](http://ec.europa.eu/information_society/digital-agenda/index_en.htm)

<sup>3</sup> Contributions can be accessed online at: [http://ec.europa.eu/information\\_society/policy/esignature/eu\\_legislation/revision/pub\\_cons/index\\_en.htm](http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/index_en.htm)

1. Respondent information
2. General expectations of respondents regarding EU legislation on e-signatures, e-identification and e-authentication
3. eSignatures tailored to face the challenges of the digital single market
4. Principles to guide e-identification and e-authentication in Europe
5. Legislative measures for the challenges ahead
6. Research and Innovation

## 1. RESPONDENT INFORMATION

A total of 434 contributions were received by the deadline of 15.4.2011. 417 respondents contributed via the online tool and 17 respondents contributed via email.

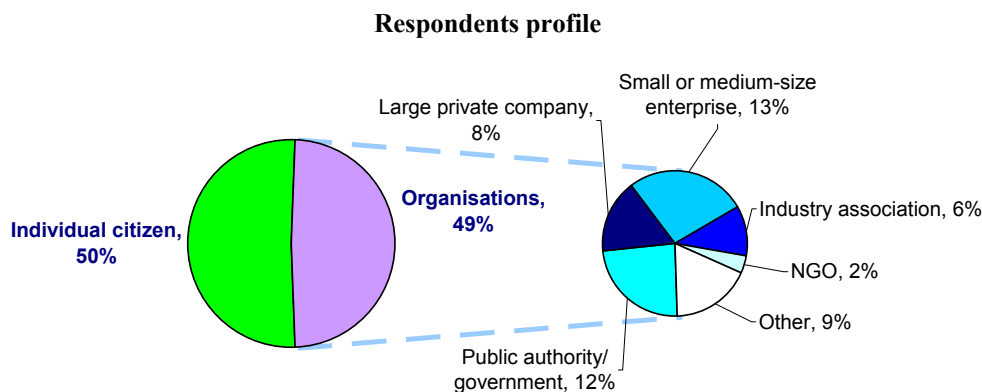
NB. The summary's statistics are based on the 417 online contributions<sup>4</sup>. Albeit not taken into account in the statistics, the additional contributions submitted by e-mail. are taken into account in the summary text. All contributions and raw statistics are posted on: [http://ec.europa.eu/information\\_society/policy/esignature/eu\\_legislation/revision/pub\\_cons/index\\_en.htm](http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/index_en.htm).

Online responses can be broken down as follows, according to the category respondents identified themselves with:

### **Respondents to the online public consultation on the SMA**

- Individual citizens — 214 responses (51.2%)
- Public authorities/governments — 49 responses (11.7%)
- Large private companies — 33 responses (7.9%)
- SMEs — 55 responses (13.2%)
- Industry associations — 23 responses (5.5%)
- Non-governmental organisations — 8 responses (1.9%)
- Others — 36 responses (8,6%)

Approximately half of the respondents answered as individual citizens, with the other half representing a specific organisation, company, association or public authority. The graphic below provides a visual representation of this breakdown:



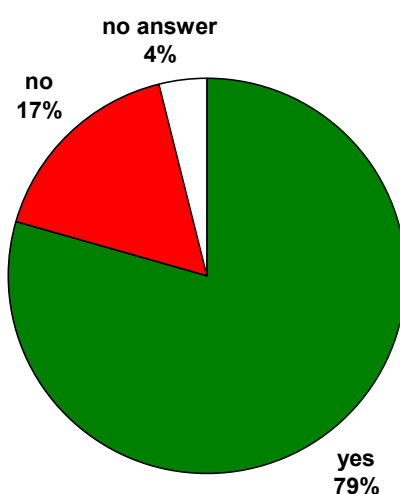
<sup>4</sup> The statistics are actually based on 418 online contributions. However, the 418<sup>th</sup> contributor used the survey tool to announce a contribution submitted by e-mail; the actual number of online contributions is thus 417.

Contributions were submitted from all over the EU, with the primary contributors being Germany, Spain, France, Belgium, Poland, the UK and the Netherlands, collectively totalling more than 50% of the contributions. 22 replies were received from non-EU respondents, including 9 responses from EEA and candidate countries:

## 2. GENERAL EXPECTATIONS OF RESPONDENTS REGARDING EU LEGISLATION ON E-SIGNATURES, E-IDENTIFICATION AND E-AUTHENTICATION

As a first material part of the consultation, respondents were presented with a series of questions to determine their use of e-signatures, e-identification and e-authentication, including specific application areas in which they currently used these, and the expected evolution of future use of e-signatures, e-identification and e-authentication.

**Q1: Do you / does your organisation use eSig, eID and eAuthentication?**



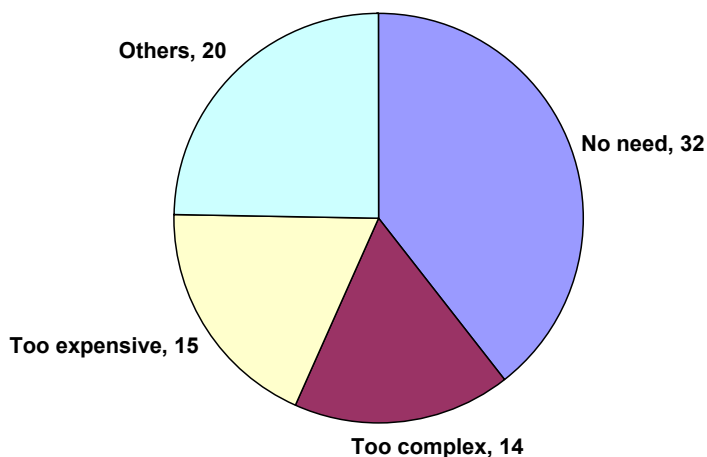
The overall usage of e-signatures, e-identification and e-authentication by the respondents is around 80 %, without responses showing no significant difference between organisations and individuals.

Respondents were also required to indicate their specific needs they considered to be the most important when using eSignatures, eID and eAuthentication. According to the overall online results, secure transactions and the integrity of electronic documents were the most indicated by far among the respondents to this question:

Q1. If you use eSignatures, eID or eAuthentication, what are your specific needs?			
	Number of replies	% of total number of replies to this question	% of total number of replies to this consultation
Secure transactions	253	76,2%	60,5%
Integrity of electronic documents	236	71,1%	56,5%
Legal effect	177	53,3%	42,3%
User convenience	152	45,8%	36,4%
Unambiguous identification of contract partners	144	43,4%	34,5%
Legal effect, contract signatures in particular	122	36,8%	29,2%
Others	58	17,5%	13,9%

Those respondents that do not use eID, eSignatures or eAuthentication indicated that the lack of a real need was a much more important reason than costs or complexity:

**Q1: I do not use eCredentials because**  
(multiple answers authorised):



A large number of respondents identified themselves to be frequent users, with the vast majority using eSignatures, eID or eAuthentication on a daily or weekly basis:

Q1. If yes, how frequently do you carry out secure transactions?			
	Number of replies	% of total number of replies to this question	% of total number of replies to this consultation
Daily	160	48,2%	38,3%
Weekly	81	24,4%	19,4%
Rarely	31	9,3%	7,4%
Monthly	23	6,9%	5,5%
The question is not relevant in my situation.	23	6,9%	5,5%
I do not know	4	1,2%	1,0%

The ranking of transactions considered to be the most useful in coming years by the respondents is the following (multiple answers were authorised):

<b>Q2. For what online transactions do you consider electronic identification, authentication and signatures useful in coming years?</b>			
	<b>Number of replies</b>	<b>% of total number of replies to this question</b>	<b>% of total number of replies to this consultation</b>
eGovernment services	355	84,9%	84,9%
Online banking and financial transactions	338	80,9%	80,9%
Issuance of authentic electronic documents	301	72,0%	72,0%
eCommerce transactions	279	66,8%	66,8%
eBusiness transactions	273	65,3%	65,3%
Secure archiving or storage of authentic electronic documents	270	64,6%	64,6%
Electronic Public Procurement	239	57,2%	57,2%
Others	65	15,6%	15,6%

eGovernment and eBanking are thus considered to be major application areas by over 80% of respondents, emphasizing the importance of authenticity and security in these domains.

Respondents were also asked to comment on the expected socio-economic benefits or drawbacks from the use of eSignatures, eID and eAuthentication in other sectors of activity than their own (question 3). Hard figures or statistics on this question are less obvious to determine since this was an open question, leading to significant differences in phrasing. Nonetheless, certain keywords together with trends and numbers can be provided on the basis of an analysis of the received replies. 269 respondents out of 417 (64,5%) provided a reply to this open question, with the following table providing an assessment of the main identified benefits and drawbacks:

<b>Expected benefit</b>			<b>Expected drawback</b>		
	<b>Number of replies</b>	<b>% of total number of replies to this question</b>		<b>Number of replies</b>	<b>% of total number of replies to this question</b>
Cost reduction or efficiency gains	116	43,1%	Inadequate user friendliness, transition / change management and training	35	13,1%
Security benefits and boosting confidence/trust	76	28,3%	Lack of e-Inclusion, accessibility, resulting in social isolation (including costs to users)	32	11,9%
Simplification, ease of use and transparency improvements	43	16,0%	Security risks and increased fraud opportunity	27	10,0%
Beneficial climate/environmental impact	38	14,1%	Fundamental rights concerns: privacy or free speech	19	7,1%
Driving innovation and boosting economic growth/competition	28	10,4%	None expected	5	1,9%
Improving inclusion and accessibility of services	21	7,8%			

Expected benefit			Expected drawback		
	Number of replies	% of total number of replies to this question		Number of replies	% of total number of replies to this question
Fraud prevention/crime reduction	22	8,2%			
Facilitating cross border activities (business, employment, study, mobility, entertainment)	19	7,1%			
None expected	5	1,9%			
Privacy / data control benefits	4	1,5%			

The primary expected benefits thus relate to reducing cost/improving efficiency (expected by 43,1% of respondents) and security/trust improvements (28,3%). The main challenges relate to a risk of user friendliness and difficulties of change management (13,1%) and the risk of exclusion and social isolation (11,9%). As shown by the table, respondents report significantly more benefits than drawbacks.

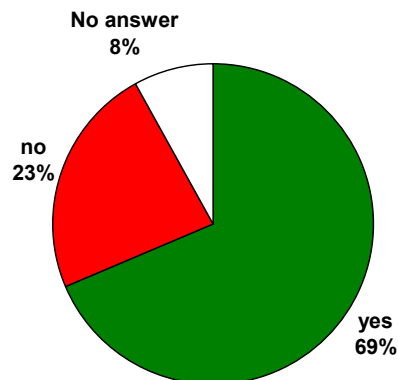
However, it is also interesting to note that several issues were both flagged as expected benefits and drawbacks by different correspondents:

- While security gains are an expected benefit with 28,3% of respondents, 10,0% also noted that more systematic use of eID/eSignatures/eAuthentication can also create new security risks, e.g. due to a lack of training or user awareness, or simply by creating more attractive targets to exploit.
- eID/eSignatures/eAuthentication are expected to result in simplification and greater ease of use by 16,0% of respondents, whereas 13,1% foresee insufficient user friendliness and complexity as a drawback.
- 7,1% of respondents saw privacy risks as a potential drawback (including the threat of reduced anonymity and freedom of speech on-line), whereas 1,5% felt that eIDs could provide privacy benefits if properly implemented.

Clearly, the list of benefits and drawbacks can also be read as a summary of risk factors, where the real life impact depends very much on correct implementation and use of eID/eSignature/eAuthentication tools.

According to the majority of respondents, a stronger involvement of financial institutions in the provision of trusted e-signature and e-identification services would impact the take-up of e-signature and e-identification (69%). This seems to be coherent in combination with the preceding question and the high relevance attributed to the eBanking sector. Several respondents commented that it was regretful that financial institutions still preferred to work with their own eID and eSignatures solutions (i.e. bank cards, one time pass-calculators, etc), rather than opening their applications to other credentials. Thus, there is a certain interest in bidirectional cooperation (using bank tools in non-banking applications, and vice versa).

**Q4: Would a stronger involvement of financial institutions in the provision of trusted e-signature and e-ID services have an impact on the take-up of e-signature and e-ID in other sectors?**



The vast majority (82%) of the respondents considers that there are specific interoperability or security aspects that should be taken into account to foster the usage of electronic signatures, identification and authentication through mobile devices (question 5). The five most important aspects selected by these respondents are (in descending order, multiple answers authorised):

- Standardisation (79%)
- Legal (77%)
- Technical (65%)
- Operational (53%)
- Business (36%)
- Others (17%)

The replies would suggest that standardisation problems and legal barriers (including liability rules) are currently seen as a larger interoperability challenge than operational or business issues.

Finally, respondents were asked to identify trust building services and credentials for which the need of future legislative measures should be explored. The following replies were provided:

<b>Q6 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?</b>			
	<b>Number of replies</b>	<b>% of total number of replies to this question</b>	<b>% of total number of replies to this consultation</b>
Certified electronic documents in general	270	64,6%	64,6%
Electronic seals	216	51,7%	51,7%
Time stamping	219	52,4%	52,4%
Certified delivery of mail	195	46,7%	46,7%
Authorisations / mandates	194	46,4%	46,4%
Long term archiving	191	45,7%	45,7%
Electronic transferable records	136	32,6%	32,6%
Official delivery address	119	28,5%	28,5%
Others (please list)	68	16,3%	16,3%
Pseudonyms	67	16,0%	16,0%
Anonymous agents	47	11,2%	11,2%
None	26	6,2%	6,2%

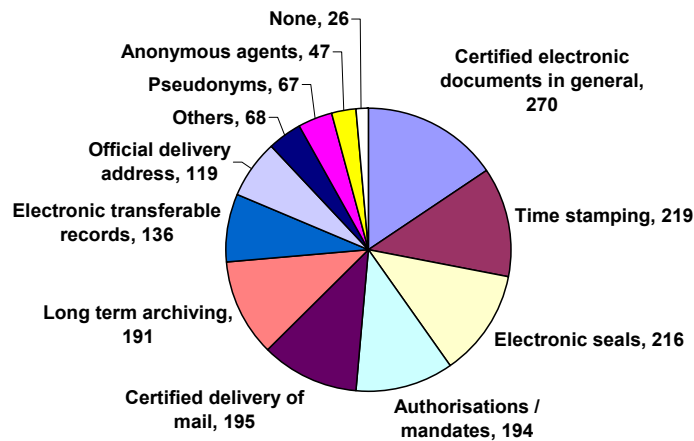
Among those respondents who felt that new legislation could be valuable, certified electronic documents in general were the main service type chosen for further regulation (64,6%), followed by electronic seals and time stamping (more than half of respondents). Privacy enhancing services (specifically pseudonyms (16,0%) and anonymous agents (11,2%) were least frequently indicated as suitable targets for regulation. Examining the comments provided, data protection was perceived as a horizontal concern which needs to be addressed by any type of service.

Around 6% felt that no further services required any regulation. Respondents who chose this answer and provided additional comments frequently stated that regulations were unnecessary or too rigid, and that standardisation, accreditation schemes and private sector initiative would be adequate to address cross border challenges.

Graphically, the replies can be presented as follows:

**Q6: 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?**

(multiple answers authorised)



The comments provided show the importance of basic principles which need to be taken into account by any new legislation, namely:

- Remain technologically neutral;
- Strive to avoid acting as a barrier or a slowing factor to developing or existing solutions, or to the development of new solutions;
- Focus on services that are susceptible to be used in cross-border scenarios, where mutual legal recognition and clear legal effect presents a certain added value.

Furthermore, respondents emphasized the importance of practical guidance based on good standards in addition to legislation, thus ensuring that the rules of the internal market can be correctly and homogeneously applied.

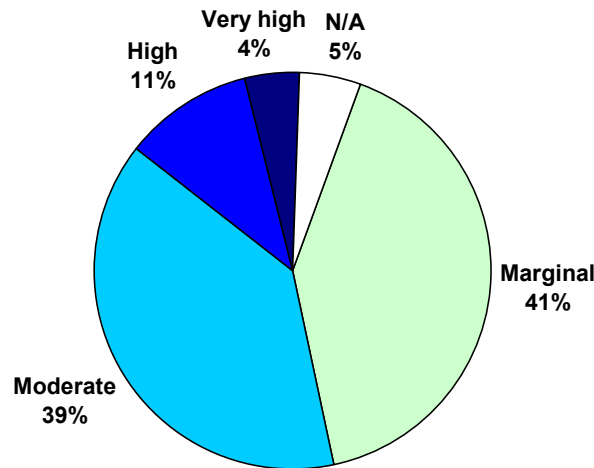


### 3. eSIGNATURES TAILORED TO FACE THE CHALLENGES OF THE DIGITAL SINGLE MARKET

The third section of the consultation examined how the respondents perceived the impact and role of eSignatures on the Digital Single Market, and the appropriateness of the existing eSignatures Directive to address the challenges related to eSignatures in this market.

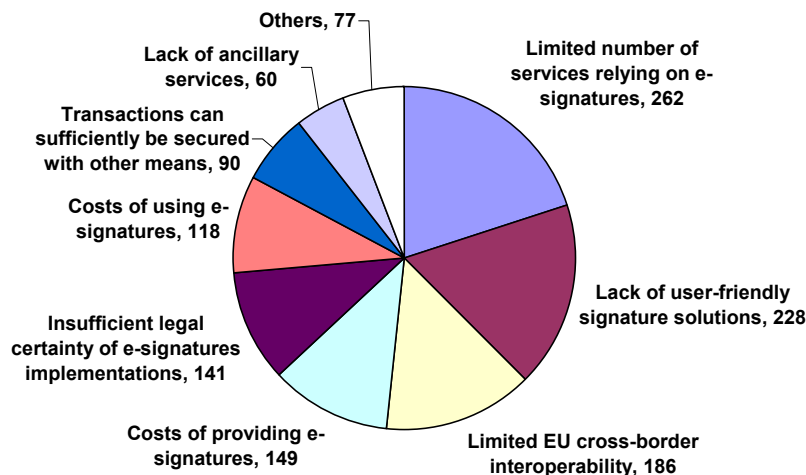
As a first point in this section, the consultation inquired how respondents judged the take-up of electronic signatures in Europe. Almost 80% of respondents in total estimated that take-up was marginal or moderate, whereas only 15% described it as high or very high:

**Q7: How do you judge the take-up of electronic signatures in Europe?**



Enquiring after the main reasons for this relatively modest take-up rate, respondents primarily noted the limited number of services requiring eSignatures, lack of user friendliness, and interoperability challenges. Costs and lack of legal certainty were smaller negative factors.

**Q8: Which of the following issues have a negative impact on the uptake of e-signature**  
(multiple answers authorised)



This would suggest that the lack of credible and viable use cases for eSignatures (i.e. applications where eSignatures are useful and sufficiently simple) remains the largest challenge to respondents.

With cross border interoperability in Europe being cited as the third largest barrier to uptake (by 44,5% of respondents), the consultation also asked respondents which issues have an impact on interoperability and should be addressed in a revised legal framework on eSignatures. This resulted in the following replies (sorted by frequency of the reply):

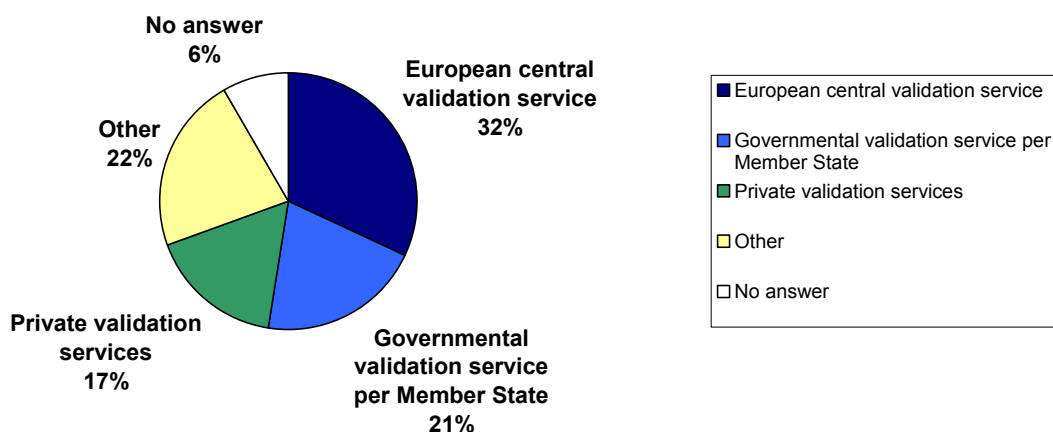
<b>Q9. Which of the following specific issues have an impact on cross-border interoperability of e-signatures in Europe and should be addressed in a revised legal framework on e-signature (the references point to the articles and annexes of the eSignatures Directive)?</b>			
	<b>Number of replies</b>	<b>% of total number of replies to this question</b>	<b>% of total number of replies to this consultation</b>
Heterogeneous approach to security requirements (e.g. certification requirements on the signing software in some countries)	144	34,5%	34,5%
Unclear terminology in Directive 1999/93/EC and heterogeneous terminology in national legislations	139	33,3%	33,3%
Insufficient harmonisation of profiles of qualified certificates	133	31,8%	31,8%
No EU list of signature equipment formally recognised as "secure signature creation devices" (Directive Annex III)	128	30,6%	30,6%
Undefined legal status of signature validation and liabilities of validation service providers	123	29,4%	29,4%
Divergent interpretations of what is meant by the "sole control" of the signatory (art. 2.2)	121	29,0%	29,0%
No common EU list of admissible e-signature cryptographic algorithms	112	26,8%	26,8%
No common approach to the supervision of providers issuing qualified certificates to the public(art. 3.2)	109	26,1%	26,1%

<b>Q9. 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)?</b>			
Missing legal provisions on signature verification and validation (Directive Annex IV)	88	21,1%	21,1%
Heterogeneous status and roles of the national security certification bodies (art. 3.4)	81	19,4%	19,4%
Ambiguities between supervision and accreditation (art. 3.2 and 2.13)	80	19,1%	19,1%
Heterogeneous usage by MS of the "public sector derogation" (art 3.7)	55	13,2%	13,2%
Heterogeneous financial liability for qualified certificate issuance.	47	11,2%	11,2%
Other	70	16,8%	16,8%
I don't know / no opinion	66	15,8%	15,8%

The three largest interoperability issues to be fixed by future regulation relate to the heterogeneous approach to security requirements in different Member States, unclear terminology in the eSignatures Directive and heterogeneous terminology in national legislations, and insufficient harmonisation of profiles of qualified certificates. These criticisms (and most others on the list) relate to areas in which the Directive has seemingly left a margin of appreciation or where its language is too ambiguous, resulting in diverging implementations that have caused market disruptions. Generally, the respondents appear to feel that future regulations could address interoperability challenges by clarifying these ambiguities and reducing national divergences.

Examining the possibilities to facilitate eSignature verification and validation at the European level, respondents did not express a clear preference for a given concept; there is a small preference for a European central validation service over national or private sector validation services:

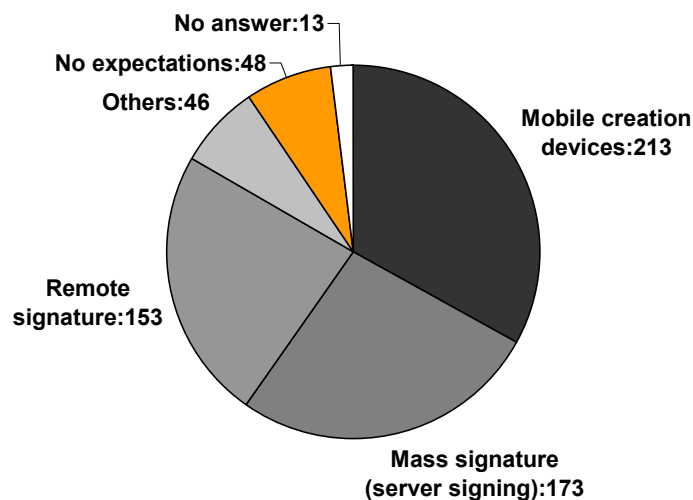
**Q10: Which among the following options could be solutions for signature verification and validation at EU level?**



Examining the comments made by respondents to clarify their choices, the main appeal of validation services (at the European or national level, or as a private service) is to remove the complexity and responsibility for verification/validation of eSignatures. However, respondents choosing the 'Other' reply generally felt that any of the three options could be viable depending on the use case; or inversely expressed doubt on the viability or necessity of any validation services. When questioning the viability or necessity, respondents mainly referenced the potential negative impact on existing service providers, the complexity (or even impossibility) of defining and applying common validation policies, and the difficulty of obtaining binding and reliable assurances of validity from validation service providers in light of different national laws and use cases. The reply thus does not show clear support for any single validation service model.

Given the large variety of existing eSignature technologies today, the consultation also asked what types of eSignatures the respondents expected European standardisation efforts to cover. The replies showed significant interest in more innovative eSignature solutions, including mobile creation devices (such as mobile phones) and mass signature devices (server signing). Mobile creation devices in particular were supported by more than half of the respondents (51%), with respondents frequently mentioning the ease of use and familiarity of European citizens with mobile phones as a potential breakthrough factor.

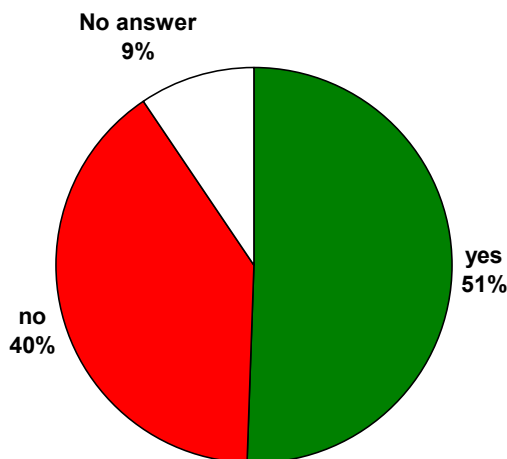
**Q11: Do you have expectations from eSig standardisation to cover?**  
(multiple answers authorised)



Inversely, only a relatively small group of 11,5% of respondents did not expect standardisation efforts to address any of these technologies. Clearly, there is an interest in expanding eSignature scenarios.

One of the pillars of the eSignatures Directive is the legal equivalence of so-called qualified signatures (i.e. eSignatures meeting the requirements of article 5.1 of the Directive) to hand written signatures. Enquiring after the impact of this provision, roughly half of the respondents indicate that they use such qualified signatures:

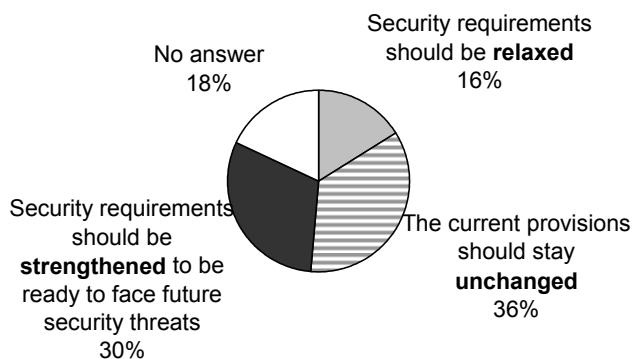
**Q12: Do you use "qualified" e-signatures?**



Comments from respondents showed that the areas where qualified eSignatures are mostly used seem the pharmaceutical sector, VAT, bank authorisation of payments, eInvoices, notaries transactions in a most of the countries with land or commercial registries, e-voting, certified delivery, enterprise annual reports, contract signatures and (public) procurement.

Given this relatively large reported usage rate, the consultation also asked whether respondents felt that the security provisions in relation to these qualified signatures should be altered, and in which sense. This question however yielded no unambiguous result: while the largest group of respondents (35,4%) felt that no change was required, a relatively sizable group of 30,6% felt that strengthening would be beneficial, and a smaller group of 16,0% felt that requirements should be relaxed:

**Q13: What is your view on the need to revise the security provisions of "qualified" e-signatures?**



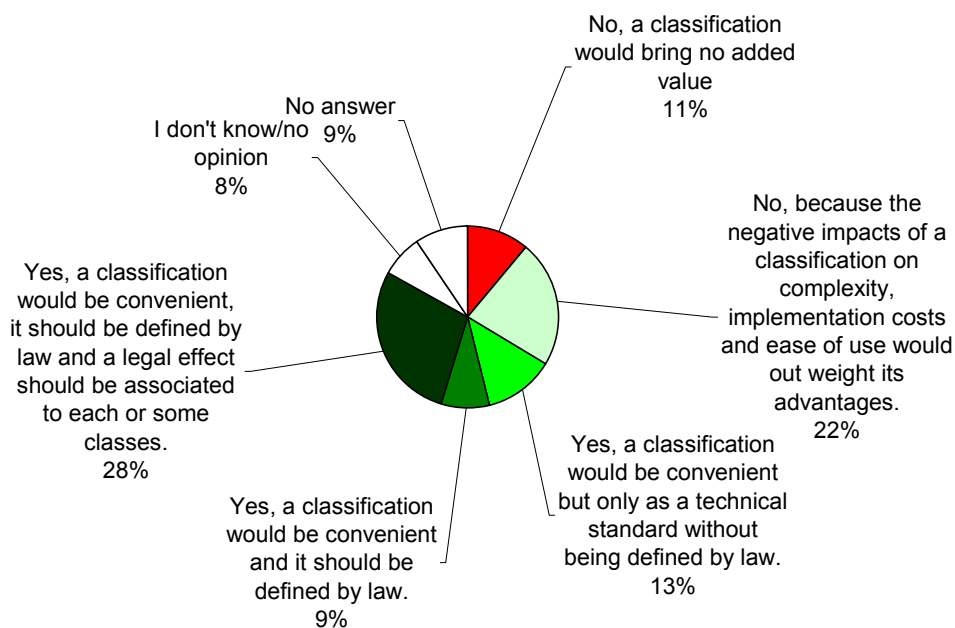
The consultation did not allow for further input on the motivation behind this position; however, it is clear that there is greater support among the respondents for tightening security requirements than for relaxing them, and that the largest group of respondents is satisfied with current security levels.

The eSignatures Directive refers to "electronic signatures", "advanced electronic signatures" and "advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device". This is not a classification of eSignatures; however it is sometimes perceived a kind of a classification. Furthermore, the legal effect of eSignatures has only two tiers:

- Non discrimination of all electronic signatures; and
- Legal equivalence of advanced electronic signatures based on qualified certificates and created by secure signature creation devices to handwritten signatures.

The consultation therefore explored whether respondents felt that an explicit classification of eSignatures against security requirements would be desirable, and if yes, whether such a classification should have some legal effects:

**Q14: Would a classification of a range of e-signatures be desirable to match different levels of security?**



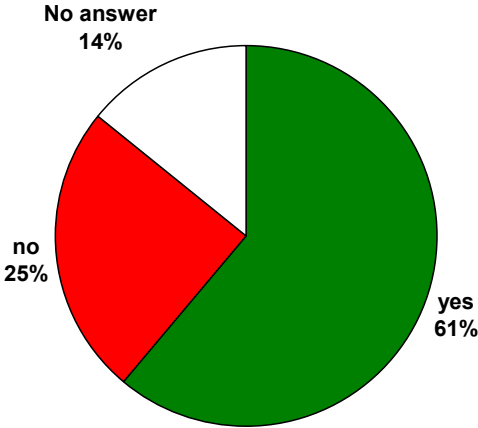
The replies to this question are somewhat polarized. The largest group of respondents (28%) feels that a classification defined by law and having legal effect for at least some classes of signatures would be convenient. However, the second largest group (22%) feels that a classification is not desirable because of its negative impacts on complexity, implementation, costs and ease of use. The third most popular reply (13%) favours classification as a purely technical approach without legal backing.

In total, the replies that argue against classification amount to 33% of respondents, whereas those in favour collectively represent half. Thus, while there are questions on what the legal value (if any) of a classification should be, the option of a common classification framework is supported by a majority of respondents when discounting the 'don't know / no opinion / no answer' groups.

The consultation also raised a few questions on how the eSignatures concept could be reoriented or broadened in new regulations. Two questions explored the concept of electronic consent as a possible addition to eSignatures. The eSignatures Directive currently does not examine the possible functionalities of an electronic signature, other than by establishing equivalence with handwritten signatures. The notion of expressing electronic consent by signing a document is not present in the current Directive.

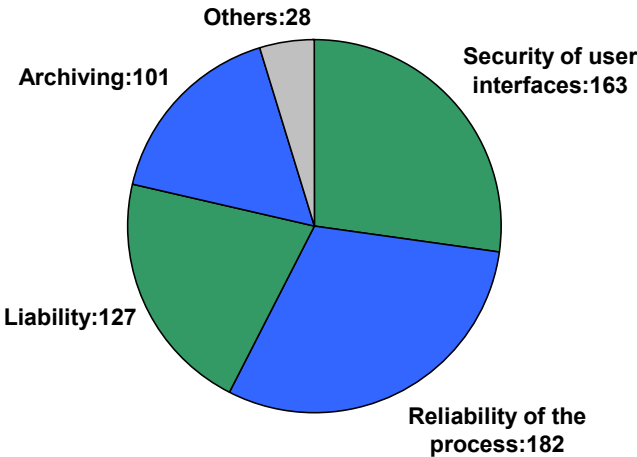
Firstly, examining whether the notion of 'electronic consent' should be formally recognized by future European legislation, a majority of 61% of respondents agree with this:

**Q15: Should "electronic consent" be recognised formally by EU legislation?**



Those who replied 'yes' were also asked to clarify which requirements new regulations should define in relation to electronic consent. Within this group, user interfaces (39%) and reliability requirements (more than 43%) scored particularly highly, followed by liability (around 30%):

**Q15, if yes, should legislation define specific requirements on:**  
(multiple answers authorised)



However, the largest group of respondents also feels that electronic consent and eSignatures are not equivalent notions (47%):

**Q16: Should "electronic consent" be considered as equivalent to e-signatures?**

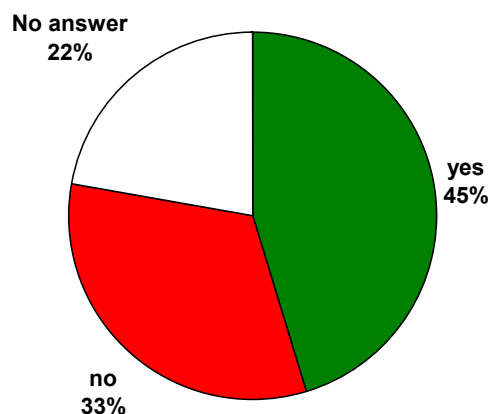


The main reasons mentioned by respondents against equivalence appear to be:

- the ambiguity of the notion of consent and its legal impact, which would create (even) more gray area than the more defined notion of an electronic signature.
- The perception of electronic consent as being too informal and free of clear commitment (with 'I agree' buttons to be clicked repeatedly given as an ambiguous example of consent)
- The opinion that signatures by definition require identification of the signatory, whereas consent does not.
- The differences between the ranges of the concepts, with consent being the will of the signatory as such, and the signature being a tool that can be used (among other purposes) as the formal expression of this will.

Finally, respondents were asked to indicate if they felt that there were specific issues concerning electronic archiving. The largest respondents group (45,2%) indeed replied that in the context of electronic archiving specific requirements should be taken into account:

**Q17: Are there specific aspects to be taken into account to address electronic archiving?**



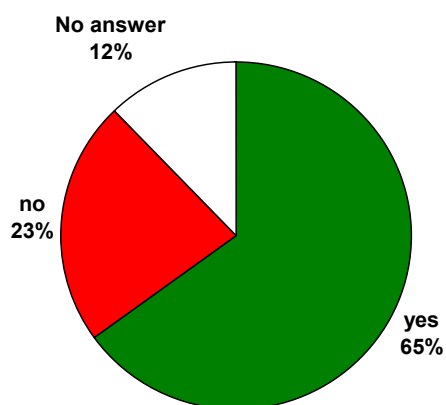
Among those who replied ‘yes’, such aspects to be considered included: the long term legal value of signed documents, personal data protection and privacy, algorithm validity periods, access control, encryption of the data at the host side, liability questions, ensuring the stability of the signed content, audit trails, control of people in charge of archiving (role of IT admin users) and requirements for administering such archives. The link to time stamping as a logical prerequisite for archiving was also mentioned by several respondents.

#### 4. PRINCIPLES TO GUIDE E-IDENTIFICATION AND AUTHENTICATION IN EUROPE

This fourth section of the consultation looked into the need for legislative measures addressing e-identification and e-authentication in particular, including the fundamental principles, expected effects on the digital single market, potential benefits for users, aspects of cross-sector interoperability and eventual lessons learned in the private sector that could be transferred to the public area.

As a first issue, the consultation explored whether electronic identification needs to be regulated at the EU level, and if yes, which principles should be addressed. As to the first question, a large majority of 65% of respondents favours EU legislation for electronic identification:

**Q18: Do you see a need for additional legal or regulatory measures on eID at EU-level?**



Among those respondents who feel that electronic identification requires legislation, the main principles to be covered by legislation are notably data protection and privacy (78%), transparency (65%), and liability of the eID provider (59%). Affordability and cross-sector permeability were considered important by 39%. The option of a federated approach (44%) was preferred compared to the centralistic approach (23%):

Q18. 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?			
	Number of replies	% of total number of replies to this question	% of total number of replies to this consultation
Personal data protection and privacy	212	77,9%	50,7%
Transparency	177	65,1%	42,3%
Liability eID provider	161	59,2%	38,5%
Non-discrimination	130	47,8%	31,1%
Federated approach	121	44,5%	29,0%
Affordability	105	38,6%	25,1%
Cross-sector permeability	105	38,6%	25,1%
Accountability	97	35,7%	23,2%
Centralised approach	64	23,5%	15,3%
Others	37	13,6%	8,9%

Looking at the expected digital single market impact of legislative measures addressing mutual recognition and acceptance of eID across borders, the main expected effects (with positive reply rates of more than 50%) are higher legal certainty (62,2%), reduction of administrative burden (60,8%), and the increase of cross-border mobility (59,1%). Economically, an positive impact is expected through the increase of economies of scale (49%). However, no standard reply scored less than 45,0%, therefore, most of the effects are expected by the stakeholders to some extent:

<b>Q19. 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?</b>			
	<b>Number of replies</b>	<b>% of total number of replies to this question</b>	<b>% of total number of replies to this consultation</b>
Legal certainty	260	62,2%	62,2%
Reduction of administrative burden	254	60,8%	60,8%
Increase of cross-border digital mobility	247	59,1%	59,1%
Increase of economies of scales for eID solutions	205	49,0%	49,0%
Reduction of fraud	201	48,1%	48,1%
Long-term sustainability of eID solutions	188	45,0%	45,0%
Other	42	10,1%	10,1%

There are high expectations of users that mutual recognition and acceptance of eIDs throughout the EU would lead to a significant simplification. No reply scored less than around 45%, suggesting that most of the benefits are expected by the stakeholders to some extent.

Additional benefits were signalled in the respondents' comments to the question, mainly to stress that eID recognition would also be a significant trust enabler to end users. Finally, a small number of respondents also noted that it was conceivable that citizens in the future would have a selection of electronic personas to choose from, and that this might be beneficial too, including for privacy reasons.

This concern over user benefits was also reflected in the responses to the question of what the expected benefits for eID and eAuthentication users are (question 20).

<b>Q20 How could users provided with electronic identification and authentication means benefit from their mutual recognition and acceptance across Europe and in which sectors?</b>			
	<b>Number of replies</b>	<b>% of total number of replies to this question</b>	<b>% of total number of replies to this consultation</b>
Simplification of access to online services	305	73,0%	73,0%
Reduction of numerous UID/passwords	272	65,1%	65,1%
Increase of user convenience	263	62,9%	62,9%
Reduced exposure to ID theft	187	44,7%	44,7%
Others	40	9,6%	9,6%

73% of the respondents count on an easier access to online services and around 65% on getting rid of the numerous user IDs and passwords they need to manage today. Towards 63% expect more user convenience in general. Almost 45% of the respondents attend a positive effect of the cross-border use of eID by leading to the reduction of ID-theft.

In order to realise these expected benefits, the question was also raised on what aspects should be taken into account to achieve cross-sector interoperability of electronic identities:

<b>Q21. What are the specific aspects that should be taken into account to achieve cross-sector interoperability of electronic identities?</b>			
	<b>Number of replies</b>	<b>% of total number of replies to this question</b>	<b>% of total number of replies to this consultation</b>
Personal data protection	251	60,1%	60,05%
Common legal basis	249	59,6%	59,57%
Common specifications for electronic identities	245	58,6%	58,61%
Identity portability	176	42,1%	42,11%
Use of multiple identities issued by different providers	112	26,8%	26,79%
Others	47	11,2%	11,24%

The most dominant aspects chosen by respondents are personal data protection measures (60,1%), a common legislation (59,5%) and the existence of common specifications (58,6%). However, it is interesting to note the different perception of the importance of data protection by individuals and organisations. While individual respondents consider personal data protection as the most important aspect (65.4%) to be taken into account, organisations rank it on the third place (54.6%). Concerning multiple identities the relatively low score achieved (26,8%) seems not surprising, given that cross-sector interoperability would have the effect of reducing their need

Finally, there was also the possibility for respondents to share their knowledge on existing experiences and lessons learned in the private sector that could be transferred to the public sector (question 22). Replies to this question were in free form, and thus no statistics can be provided. The main trends can be summarized as follows:

- Use case analysis plays an important role, which has often been initially neglected, leading to delays in uptake and in incorrect expectations with respect to the market for electronic identification, authentication and signature services in certain areas. Risk assessment is important: requiring the highest security solution in all cases is not a good approach.
- Low cost and ease of use for end users is crucial since high security as such is not necessarily an added value that they are willing to pay a premium for. Simplicity can arise by hiding part of the technical and legal complexity; mobile authentication solutions are increasingly seen as an attractive prospect for this.
- Looking at success cases in the private sector, the financial sector (e-banking partnerships) seems to be a productive example for developing and introducing eID solutions that are used in practice and received positively.

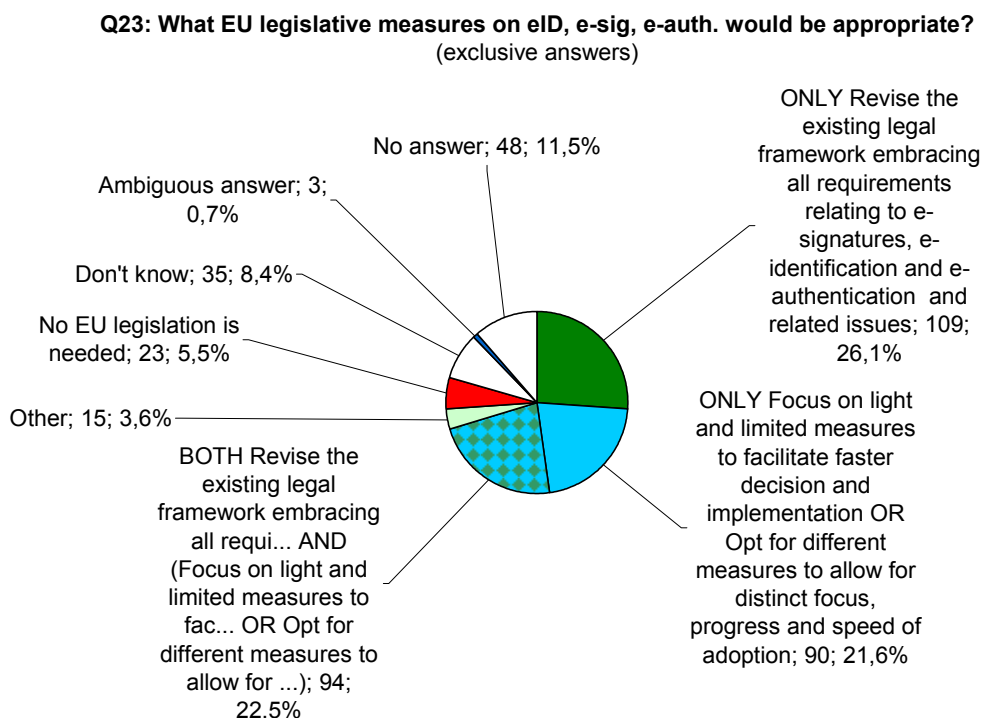
- Consolidation of solutions and interoperability has been slow to be achieved, mainly because of the multitude of ambiguous standards.
- Governance plays a crucial role: without a governance model that establishes a sufficient common ground, interoperability cannot be achieved.
- When looking at identification, reliability assurance needs to be determined by considering all relevant factors.

## 5. LEGISLATIVE MEASURES FOR THE CHALLENGES AHEAD

The fifth section of the consultation recalled the "Digital Agenda for Europe" communication in which the Commission has proposed two key actions directed at the creation of a well functioning digital single market with a view to eliminate the current barriers to the use of e-signatures, e-identification and e-authentication across Europe. Specifically, key action 3 of the Digital Agenda focuses on the revision of the eSignatures Directive, whereas key action 16 targets a Council and Parliament Decision to ensure the mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States.

In this context the respondents were asked what European Union legislative measures on e-signatures, e-authentication of natural and legal person claims as well as e-identification would be appropriate to best meet the challenges of the digital single market.

The responses received on the nature of necessary legal measures on e-signatures, e-identification and e-authentication show no clear indication<sup>5</sup>.



<sup>5</sup> The next pie chart shows the answers of the respondents in a re-processed manner. Respondents could provide multiple answers to the following six options: "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 / I don't know / Other".

The answers have been processed in the eight exclusive answers shown on the next pie chart because they are more meaningful for analysis.

The main observation is that only 5,5% of the respondents feel that no legislation is needed, whereas the largest group of 26,1% considers a comprehensive legal framework to be most appropriate. 21,6% are in favour of lighter and more limited measures to facilitate faster adoption and implementation or preferred more specific targeted measures. 22,5% prefer at the same time a comprehensive approach but achieved by light or different means. Although 48,6% of respondents prefer a revised legal framework embracing all requirements relating to e-signatures, e-identification and e-authentication and related issues, the answers do not allow however to find out if a majority prefers a set of measures or an all-encompassing measure.

## 6. RESEARCH AND INNOVATION

The consultation also sought to determine which standardization issues and technological research would still be required to support the use and usability of eSignatures and eID, and to strengthen trust in electronic identification, authentication and signatures in the European Single Market (questions 24, 25 and 26). Due to the use of open questions no statistics can be provided, but the main trends of the replies can none the less be highlighted.

Firstly, respondents were asked to indicate what issues European R&D and standardization efforts should focus on to have all the necessary technology to improve eID management. The responses varied quite widely, but frequently quoted topics included notably:

- Research into privacy and data protection requirements;
- The definition of basic requirements in term of security and reliability, including the use of cryptography;
- Innovative technologies, including notably mobile devices and their security requirements, and the use of biometrics;
- Policy standardization work, including notably the definition of standard assurance levels/trust levels (including identity proofing/verification), and common verification policies that could be used to establish Bridge Certification Authorities, cross certification networks, or identity federations;
- Hardware standardization (including smart cards and hardware security modules) and certificate profile standardization;
- Guidelines for ergonomics, usability and ease of use;
- Development and promotion of common APIs, interfaces and middleware.

As to the question on which technologies European R&D efforts should focus in order to improve the usability of e-signatures and electronic identification for end users and to facilitate the deployment for service providers, the use of mobile devices was the most frequently given response, with respondents indicating the user friendliness and familiarity of mobile devices to the general public as a key reason for this preference. User friendliness was a high priority in general, with the development of user friendly interfaces being frequently suggested as a promising area for further research. Other areas considered interesting by respondents included mainly biometrics, identity federation, and better harmonization of smart card technologies.

Finally, the consultation asked what technologies could contribute to overcoming the lack of trust in electronic identification, authentication and signatures in the European Single Market. The main suggestions made by the respondents referred to the development and use of secure and user friendly visualization interfaces (e.g. standardized secured viewers, or display/input facilities on smart cards). This proposal was occasionally mentioned in combination with the suggestion of increased use of mobile devices (including SMS/mail validation), due to the increased subjective trust that end users already have in their mobile devices.

## 7. OTHER ISSUES

The consultation concluded with three broader questions, in which respondents were allowed to communicate their opinion on:

- international issues that should be taken into account in EU policy (question 27),
- any best practices examples outside Europe that respondents might wish to share (question 28),
- any other issues which they thought should be addressed by policy makers (question 29).

The last of these questions does not lend itself well to summary, but responses to the first two shall be briefly examined here.

With respect to international issues, many responses made reference to the importance of international standardization, if possible supported through international agreements to use the same standards in international transactions. Respondents were of the opinion that European standards should be promoted at international level to support this process. The same observation was made related to information security and data protection aspects of eID, eSignatures and eAuthentication: while European collaboration and harmonization is beneficial and should be continued as a priority, a truly international framework would eventually need to emerge to address global challenges of the international economy. Several respondents however also warned against attempts to unilaterally impose European perceptions or solutions, as this could have an adverse impact on international trade.

Several respondents also suggested best practice examples from outside of Europe that could be beneficial. Leaving aside vendor specific examples, respondents notably referred to the USA (in particular, the US National Institute of Standards and Technology and the US National Strategy for Trusted Identities in Cyberspace) as well as industry driven eID-reuse solutions. For international success cases, the mobile telephony sector and the financial sector were referenced as two examples where international interoperability and monetization appears to have been achieved with fairly large rates of end user take-up.

- / -