



Study on Mutual Recognition of eSignatures:
update of Country Profiles
Analysis & assessment report

October 2009



This report / paper was prepared for the IDABC programme by:

Coordinated by: Hans Graux (time.lex), Guy Lambert (Siemens), Brigitte Jossin (Siemens), Eric Meyvis (Siemens)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°13

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

<http://ec.europa.eu/idabc/>
<http://ec.europa.eu/idabc/en/document/6485>

© European Communities, 2009

Reproduction is authorised, except for commercial purposes, provided the source is acknowledged.

Table of Contents

EXECUTIVE SUMMARY	5
1 DOCUMENTS	14
1.1 APPLICABLE DOCUMENTS	14
1.2 REFERENCE DOCUMENTS	14
2 GLOSSARY	16
2.1 DEFINITIONS	16
2.2 ACRONYMS	18
3 INTRODUCTION	19
4 ANALYSIS	23
4.1 MAIN E-SIGNATURE SOLUTIONS	23
4.1.1 GENERAL OVERVIEW TABLE	23
4.1.2 ESIGNATURES BASED ON NATIONAL EID CARDS	26
4.1.3 ESIGNATURES BASED ON SECTOR SPECIFIC SMART CARDS	30
4.1.4 ESIGNATURES BASED ON GENERIC CRYPTO TOKENS	34
4.1.5 ESIGNATURES BASED ON SOFT CERTIFICATES	35
4.1.6 ESIGNATURES BASED ON MOBILE E-SIGNATURES	35
4.1.7 ESIGNATURES BASED ON MULTI-FACTOR AUTHENTICATION	35
4.1.8 ESIGNATURES BASED ON SINGLE-FACTOR AUTHENTICATION	35
4.2 REGULATORY FRAMEWORK FOR ELECTRONIC SIGNATURES	35
4.2.1 TRANSPOSITION OVERVIEW	35
4.2.2 REGULATORY ESIGNATURE REQUIREMENTS	35
4.3 EGOVERNMENT APPLICATIONS AND THEIR USAGE	35
4.3.1 GENERAL OVERVIEW TABLE	35
4.3.2 SPECIFIC APPLICATIONS	35
4.3.3 MANDATES AND AUTHORISATIONS	35
4.3.4 APPLICATION APPROACH MODELS	35
4.3.5 CLASSIFICATION BY MODEL	35
4.3.6 CLASSIFICATION BY COUNTRY	35
4.3.7 CLASSIFICATION BY SECTOR	35

5	IMPACT ASSESSMENT	35
5.1	INTRODUCTION	35
5.2	CONCEPTUAL CHALLENGES IN THE eSIGNATURES DOMAIN	35
5.2.1	SUPERVISION VS. ACCREDITATION, AND THEIR ROLE IN DETERMINING THE ACCESSIBILITY OF eGOVERNMENT APPLICATIONS	35
5.2.2	INTEROPERABILITY, SPECIFICALLY AT THE CROSS BORDER LEVEL	35
5.2.3	ELECTRONIC SIGNATURES AND THE AUTHENTICATION OF DATA AND ENTITIES	35
5.3	IDENTIFIED INTEROPERABILITY ISSUES	35
5.3.1	NATIONAL PERSPECTIVE IN CHOOSING SIGNATURE SOLUTIONS	35
5.3.2	LEGAL FRAMEWORK IS BASED ON CONCEPTS THAT ARE UNIQUE TO A SPECIFIC COUNTRY	35
5.3.3	LEGAL FRAMEWORK CONTAINS REQUIREMENTS THAT CANNOT BE MET BY FOREIGN SOLUTIONS	35
5.3.4	INTERPRETATION OF THE EUROPEAN LEGAL FRAMEWORK	35
5.3.5	EUROPEAN FRAMEWORK IMPLICITLY FAVOURS CERTAIN TYPES OF SIGNATURES	35
5.3.6	INCOMPLETENESS OF THE EUROPEAN LEGAL FRAMEWORK	35
5.3.7	PREVALENCE OF AD-HOC SOLUTIONS WITH LIMITED INTEROPERABILITY PERSPECTIVES	35
5.3.8	INCOMPATIBLE USE OF CERTIFICATE ATTRIBUTES	35
5.3.9	SIGNATURE TYPE ENFORCEMENT	35
5.3.10	SIGNATURE FORMAT	35
5.3.11	SIGNATURE VALIDATION	35
5.3.12	VALIDATION PROTOCOL	35
5.3.13	SIGNATURE ALGORITHM	35

Executive summary

The European Commission - DG DIGIT (hereafter the Commission) has undertaken a number of initiatives in recent years to improve the interoperability between electronic signature solutions at the European level, building on the legal framework created by the eSignatures Directive. One of these was the 2007 Preliminary study on mutual recognition of eSignatures for eGovernment applications¹. This study aimed to collect information on eSignature approaches in eGovernment applications in 29 countries (27 Member States and 2 candidate countries, Turkey and Croatia), which were subsequently analysed to determine interoperability barriers and potential interoperability solutions.

However, the field of eSignatures has advanced to a certain extent in recent years, including under the influence of the approaching implementation of the Services Directive² and due to recent projects with an interoperability impact, like the PEPPOL cross border eProcurement pilot project³. For this reason, changes in the EU eSignatures domain need to be carefully monitored.

The present study therefore aims to update the available information, and to assess to which extent the use of eSignatures in the EU has evolved in the past two years. The scope of the Study has also been expanded somewhat, both with respect to geographical scope (now covering the 3 EEA countries Norway, Iceland and Liechtenstein as well) and with respect to subject matter (now examining inter alia also specific applications in the eProcurement, eHealth and eJustice sectors, along with newer signature technologies like mobile eSignatures and new interoperability initiatives.

Below, we will summarize some of the main findings of the study, which are commented more extensively below.

Available eSignature solutions

Examining the eSignature solutions which were presented in the country profiles as being of key importance for eGovernment strategies, the following observations can be made:

- eID cards are now available in 8 out of 32 countries (25% of surveyed countries). Two of these are new compared to the 2007 edition of the study: Liechtenstein and Lithuania. It is interesting to note that all of these allow the creation of qualified signatures, making them a suitable basis for interoperability initiatives. In addition to these 8 countries, 8 more countries (25%) are currently planning the introduction of eID cards: Croatia (planned in the course of 2010), the Czech Republic, France (2012), Germany (Q4 2010), Malta, Norway, Poland (2011) and Romania (2011).
- Sector specific smart cards (i.e. issued only to a specific user group or in relation to a specific application field) were found in 9 countries (28%), whereas generic crypto tokens and soft certificates were found in respectively 22 and 18 countries (69% and 56%). Given that the latter two groups are typically issued by private sector parties, this shows the strong role that the private sector can play in supporting eGovernment policies.
- Mobile signatures are only available in 5 countries at this point (16%). However, a larger number of countries have solutions planned for the near future, as will be seen below.

¹ See <http://ec.europa.eu/idabc/en/document/6485>

² Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market; see http://ec.europa.eu/internal_market/services/services-dir/index_en.htm

³ See <http://www.peppol.eu/>

- Authentication solutions were reported only to a limited extent, undoubtedly because they are not commonly seen as signature solutions. Multi-factor and single factor authentications solutions were reported in only 4 (13%) and 5 countries (16%) respectively.

Legal evolutions and trends

Looking at the changes in the legal frameworks, it is clear that the legal framework for electronic signatures has reached a stage of maturity. Out of 32 countries, 26 made no noteworthy changes to their applicable laws. Of the six countries that did report specific changes, three related to organisational matters (changes in supervision/accreditation schemes in Croatia, Cyprus and Romania), and one to the updating of technical requirements (Italy). More extensive updates were seen in Austria and in Slovakia.

It is interesting to note that there is still some divergence between the concepts used by these different regulatory frameworks, with the concept of 'secure electronic signature' being an interesting example. This term is not defined at the European level, and thus has no clear European standing. None the less, it used to be a part of Austrian law where it related to a qualified signature. It still exists in Poland, where it corresponds roughly to an advanced signature created using an SSCD, and in Lithuania, where it is synonymous with an advanced electronic signature. While a purely terminological issue, one might see how the introduction of new categories of signatures on a national basis holds a risk of creating market confusion.

With regard to the use of electronic signatures in public sector applications, twelve countries have established specific eGovernment acts (generally designated as eGovernment Acts, Electronic Administration Acts, Electronic Communication in the Public Sector Act, etc). The precise scope and impact of these laws varies quite strongly, but the several broad categories of goals supported by the regulations can be identified. The most obvious and largest group consists of regulations that grant the citizens and/or businesses the right to communicate electronically with public administrations, and which clarify the modalities of doing so. A second group has implemented regulations addressing the reverse possibility: the right of public administrations to use electronic signatures in their communications with businesses and citizens (A2B and A2C). Finally, a third group has integrated specific incentives for the use of electronic signatures in communication with the public sector, i.e. they have implemented rules that not only *permit* the use of electronic signatures in eGovernment services but that *encourage* such use, including by introducing a right of acknowledgement (France), a right to a response (Bulgaria), a right to choose the desired communications channel (Spain and the Netherlands), and a right to access electronic documents (Spain), or simply by facilitating the validation of the official status of a public sector communication (the Austrian official signature).

None the less, some examples could also be noted in which provisions were introduced with a clear view of facilitating national interoperability (i.e. information exchange between services within a country and/or improving the quality of service, which may none the less result in interoperability barriers at the European level. Examples of this include requirements to use signature concepts which only exist at the national level, only granting certain rights when a signature from a nationally accredited CSP is used, or requiring the presence of a national identified in the certificate.

These restrictions appear to be applications of Article 3.7 of the eSignatures Directive (the so-called public sector clause), which allows Member States to "make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens." Given the considerations above, it seems that some countries have not respected the last restriction in the eGovernment/eSignature regulations.

Technical evolutions and trends

The changes on the technical level are not obvious to assess especially because the assessment was not made on the same applications. This is mainly due to the change of focus at sectoral level. In 2007, the focus was made on eProcurement only while in 2009, the focus was made on eProcurement, eHealth and eJustice. Following this focus change, only 28 eGovernment applications are common to both studies.

Nevertheless, technical evolutions and trends were detected. The main one is related to the signature validation interoperability issue. This issue was seen as the most important one in 2007. The ‘Preliminary Study on Mutual Recognition of eSignatures’ recommended to set-up a Federation of Validation Authorities to answer one of the major issues that eGovernment applications were facing, i.e. signature validation.

At the light of 2009 country profiles, it is clear that the signature validation landscape has changed in Europe since 2007. Indeed, in the previous study, Spain was the only country to mention the existence of a validation service, called @firma. In 2009, 5 validation services were reported: @firma in Spain, e-Notarius in Poland, MOA-SP in Austria, VPS/Governikus in Germany and BBS in Norway.

Another evolution has been detected at the level of the use of specific certificate attributes. In 2007, it was clearly shown that the use of incompatible identifier (such as National Registry Number ...) as part of the signature was creating an interoperability barrier. In 2009, the situation is has not improved. Not only applications making use of incompatible identifiers were detected but also applications making use of specific certificate fields to determine the signatory role (such as doctor, lawyer ...).

Applications

General

In total, 91 eGovernment applications were reported with full details covering sectors such as eProcurement, eHealth, eJustice but also Taxation, Social Security, Foreign Trade ...

Among those 91 applications, 69 ones were assessed to make effective use of electronic signatures, being Qualified signatures, Advanced signatures based on Qualified certificates or Advanced signatures.

The applications belonging to the 3 main sectors studied are further detailed below.

- **eProcurement**

In total, 19 eProcurement applications were reported, 15 of which were presently operational, three were in pilot stage, and one in the planning stages. With regard to signature solutions, and looking exclusively at the 15 operational applications, there is some diversity to be found:

- Six solutions presently rely on qualified signatures
- Two require advanced signatures based on qualified certificates
- Six require advanced signatures
- One requires a simple signature only

More interesting than the reported signature type of the supported signatures is the accessibility of the application to tenderers in other countries. In the previous study, the response to this question was universally negative: eTendering applications were only accessible provided that the tenderer obtained

local credentials. This situation has changed to a small extent in the past two years: while a majority of applications (10 out of 15) is still only accessible when using local credentials, two countries have a small list of foreign solutions which are also supported. This was the case in Austria, where the use of a signature validation component allowed the eTendering application to also accept signatures created using an eID card from Belgium, Italy, and Slovenia; and in Norway, where the eTendering platform could be extended to support electronic signatures supported by the private BBS Validation Authority. Finally, three countries have no restriction in place: Ireland, Denmark and Slovakia. In the Irish case, the application uses a simple online registration system that does not use any PKI components and therefore has no interoperability issues to be dealt with. In the Danish and Slovakian case, registration results in the recipient receiving an advanced signature certificate via e-mail that complies with national requirements, which he can use to sign the offer. These are all examples of a case where local credentials are still needed, and where there is thus strictly no interoperability, but where the need for interoperability has been avoided by introducing a sufficiently flexible user registration system.

Thus, it is clear that interoperability is still very limited, but none the less clear progress has been made in comparison to the previous edition of the study.

- **eHealth**

In total, 10 countries reported eHealth applications, 8 of which related to applications which were presently operational, and two were in pilot/design stage. eHealth applications using eSignature solutions are thus significantly fewer in number than eProcurement applications. Seven of the ten descriptions relate to general eHealth platforms that could be used to securely exchange information in the eHealth sector. The three other applications related to cancer research (Belgium), blood transfusions (Italy), and changing GP (Norway).

With regard to the type of signature required:

- Five solutions presently rely on qualified signatures;
- Two require advanced signatures;
- Three applications have components that can also operate on the basis of a simple signature.

Given the sensitive nature, the need to be able to verify the professional status of a health care professional, and the link to a specific sector, it could reasonably be anticipated that interoperability initiatives would be at a less advanced stage in eHealth applications than in the eProcurement applications described above. This is indeed confirmed by the overview above: all countries restrict accessibility of the solution to the holder of national credentials.

In a number of cases, this is due to the exclusive reliance on a sector specific national card, as is e.g. the case for Croatia (CIHI card), Germany (EGK and HBA card), Italy (EIC and NSC card), and the Netherlands (UZI-card). These cards serve to determine the capacity of the signatory (e.g. the UZI-card is only available to health care professionals registered in the Dutch UZI-Register), meaning that interoperability is much harder to achieve in this field.

It should be also noted however that for a number of applications the actual need for interoperability is also much smaller than for applications with a potentially unlimited user group. In these cases, the application's scope is delineated at the national level, which means that all users should have access to appropriate national credentials, and the need for interoperability is thus much smaller.

- **eJustice**

In total, 9 eJustice applications were reported, 7 of which were presently operational, and 2 of which were in pilot stage. Again, the number of applications is substantially smaller than for eProcurement applications, which may be linked due to the difficulty of establishing appropriate models for verifying

the legal capacity of the actors (notaries, judges, lawyers, etc.). This same problem is also present for eHealth applications, which may explain why the number of applications reported is similar.

Looking at the scope of the applications, four of the eight descriptions relate to court proceedings and court administration, three relate to the establishment and management of companies, and two related to notarial archiving services.

With regard to signature solutions, and looking exclusively at the 7 operational applications, the same diversity found in the eProcurement and eHealth applications is found again:

- Four solutions presently rely on qualified signatures;
- One required advanced signatures based on qualified certificates;
- One required advanced signatures;
- One used simple signatures.

As with the eHealth applications, given the sensitive nature, the need to be able to verify the professional status the service providers, and the link to a specific sector, it could reasonably be anticipated that interoperability initiatives would again be limited. In fact, all but one country (Estonia) restrict accessibility of the application to the holder of national credentials.

In the Estonian example, companies can be established not only by the holders of an Estonian signature solution (Estonian eID or Mobile-ID), but also by using a Portuguese, Belgian or Finnish ID-card or a Lithuanian Mobile-ID.

As with eHealth applications, here too the actual need for interoperability is again much smaller than for applications with a potentially unlimited user group. E.g. the Austrian application is aimed towards any notaries in Austria (who are required to use the archive), meaning that it is not problematic that the Austrian Chamber of Notaries attests to the professional qualification. Signature solutions are in this respect commonly linked to a specific capacity, not to nationality, In cases where this means that all users have access to appropriate national credentials, the need for interoperability is again much smaller.

Interoperability impact assessment

Based on the overview and analysis above, a list of interoperability issues has been drafted, which may provide a basis for a discussion in the perspective of future European strategies in this area. These issues will be briefly commented below, and a full assessment of the impact and possible solution strategies can be found in Section 5 of this report.

- **National perspective in choosing signature solutions**

It was already noted in the previous edition of the study that most of the surveyed countries, as far as they have adopted electronic signatures in their e-government applications, have organised this feature without taking into account electronic signatures solutions issued by CSPs in other countries. The regulatory, technical and organisational framework is always organised from a strictly national perspective. In most of the cases this national perspective is implicit. The application presumes that the user is a national living on the country's territory. In addition to all other kinds of practical obstacles that prevent other users to access and actually use the application, electronic signatures can in this way become an additional barrier.

- **Legal framework is based on concepts that are unique to a specific country**

As noted above, there are some cases where national laws have introduced terminological or real differences between the countries, where national laws established concepts which have no clear meaning at the European level. As long as these are purely terminological issues, this situation may prove to be slightly confusing but ultimately harmless. However, if these categories take up such a fundamental role in eGovernment processes that it becomes impossible or unreasonably complex to determine whether a foreign signature meets the applicable requirements, there is a real risk of these diverging concepts becoming a barrier to cross border interoperability. This can in particular be the case when national laws require the use of a signature type which is unknown at the European level. This issue will be examined further below.

- **Legal framework contains requirements that cannot be met by foreign solutions**

Some examples have been identified of national eSignature/eGovernment regulations aimed towards facilitating national interoperability (i.e. information exchange between services within a country) and/or improving the quality of service, but which may none the less result in interoperability barriers at the European level, due to the reliance on requirements which can only reasonably be met at the national level. In these cases, regulations may result in an impossibility of using foreign signature solutions. It should be stressed however that this is only the case if the regulations explicitly contain a requirement to use a specific solution as a precondition for specific service, and not if they merely support the use of a national solution. The distinction is important: there is no objection to establishing an approach to eSignature (including the use of specific identifiers or a voluntary accreditation scheme) with a view of ensuring that these solutions are easily identifiable to end users as a good option or with a view of ensuring a higher quality of service. However, when the approach results in the strict or de facto exclusion of foreign signature solutions, this can present a real problem.

- **Interpretation of the European legal framework**

The eSignatures Directive can be credited with the creation of the basic regulatory framework for the use of electronic signatures at the European level. It has established many of the main building blocks, but it can also be noted that some concepts leave a margin of interpretation that results in cross border interoperability barriers. The primary example identified in this study is the conceptual confusion behind qualified certificates, and specifically whether a qualified certificate can be issued to legal persons. This is an issue that would need to be clarified at the European level.

Other examples of differing interpretations exist as well. To some extent these are simply due to the margin of appreciation left by the Directive, and therefore do not (or rather should not) create specific interoperability concerns. The question of supervision of CSPs issuing qualified certificates to the public is one example in this respect: while a supervision regime has been established in each country, the exact modalities (and the resulting real reliability) of these regimes vary substantially. In principle this is not a problem: the Directive merely requires that supervision regimes must be 'appropriate' (article 3.3 of the Directive), without specifying the criteria to determine when a regime should be considered as such. While it is clear that the cross border validity of qualified signatures can a priori not be challenged on the basis that a foreign supervisory regime has not been found 'appropriate', it goes without saying that the cross border trustworthiness of supervision regimes could benefit from an improved exchange of best practices or more tangible guidelines.

A third and more significant example of differing interpretations can be found in the concept of secure signature creation devices (SSCDs), defined in the Directive as a signature-creation device which meets the requirements laid down in Annex III to the Directive. The different interpretations in this case relate to the provision of Article 3.4, stating that "*the conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States.*" Some Member States (e.g. Germany) have interpreted this provision to mean that a formal assessment process is always necessary to determine whether the requirements of

Annex III have been met (e.g. because the requirements of Commission Decision 2003/511/EC⁴ have been met), whereas other countries (e.g. Belgium) consider that such an assessment could serve to remove any doubt but is not strictly required. This is likely to surface as a future point of discussion, specifically because market distortions can occur if these differences in interpretation remain

- **European framework implicitly favours certain types of signatures**

Most of the comments above pertain specifically to signatures based on qualified certificates (i.e. advanced signatures based on qualified certificates and qualified signatures). The reason for this is that the current trust model of the Directive is substantially linked to this concept: trust in the signatures can be determined due to the fact that qualified certificates share common requirements (Annex I of the Directive), as do the CSPs issuing such certificates to the public (Annex II of the Directive), and compliance is supervised by specific supervisory bodies with a national mandate under Article 3.3. This mechanism is not as meaningful for other electronic signatures, specifically advanced signatures which are not based on qualified signatures or basic ('simple') signatures. In this case, the building blocks are fundamentally different: there are no common criteria to determine their reliability, no requirements in relation to CSPs (insofar as CSPs are involved, which is not necessarily the case for simple signatures), and no supervision model to ascertain whether such requirements are followed. While accreditation schemes fill this trust void to a certain extent, such schemes are currently established at the national level and offer little opportunity for cross border interoperability. Realistically, it is clear that little progress has been made in relation to the interoperability of signatures which are not based on qualified signatures, and that no short term progress can be foreseen, due to the fact that the aforementioned basic building blocks to establish trust are missing. Barring further initiatives at the European or otherwise cross border level, it seems doubtful that any large scale interoperability is possible for these signature types in the short term.

- **Incompleteness of the European legal framework**

This study focuses on one specific type of trusted third party (TTP) service, namely that of electronic signatures, and other TTP services are out of scope of this study. None the less, some countries have opted not to address the issue of electronic signatures in isolation, but have instead considered that it would be advisable to place this in a broader framework of certification services regulations. In these countries, electronic signatures were seen as implicitly linked to other TTP services which would be necessary to unlock the full potential of electronic signatures. These national regulations in relation to time stamping, long term archiving, electronic registered mail, identity management and authorisations seem to indicate that there is a certain normative gap to be filled, in the sense that each of these services would require a legal framework to ensure their trustworthiness to end users. On the other hand, the fact that these initiatives are taken at a strictly national level means that there is a risk of disparities emerging in the European market.

It should be stressed again that TTP services other than electronic signature are strictly speaking out of scope of this study. None the less, all of these examples of TTP services are also linked to the use and value of electronic signatures. The lack of a European framework thus creates a risk of interoperability gaps when national regulations begin to diverge.

- **Prevalence of ad-hoc solutions with limited interoperability perspectives**

⁴ Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council

Not all Member States have adopted a general all-encompassing central strategy with regard to electronic signatures in e-government applications. There are many ad-hoc solutions and regulations in this domain, especially in countries which do not favour strong PKI based approaches. This fragmentation can possibly hinder future interoperability initiatives. However, as was noted above, it's also clear that for some applications the importance of eSignature interoperability is not absolute. In those cases, it should be stressed that the lack of interoperability with other solutions is meaningless if the envisaged user group can easily gain access to the appropriate signature solutions. Cross border interoperability is an important factor in applications which are (or rather should be) open to end users from any country, such as e.g. eProcurement. Applications which are inherently only useful to end users in a specific country benefit relatively little from such interoperability.

- **Incompatible use of certificate attributes**

This issue concerns signatures based on certificates where the application requires the certificate to contain a specific attribute. In the previous study, the problem was already identified as "Incompatible use of identifiers" which could be National/Sectoral/Regional unique number. The issue can be considered as more important today. Indeed, the new sectoral applications considered above, especially in the eHealth and eJustice sectors, often require the signature certificate to contain a specific attribute allowing the identification of the role of the signatory (e.g. nurse, doctor, judge, lawyer, notary ...).

This new application requirement imposes, by essence, new barriers to the interoperability of eSignatures. Mainly for two reasons: first because there is no standardisation on the attribute which might be used by application to identify the role of the signer, and secondly because there is no standardisation on the values that such attributes may contain. Regarding the values of these attributes, the language is again another barrier. Indeed, is "lawyer" equivalent to "advocaat" or "Rechtsanwalt"?

- **Signature Type enforcement**

Technically, there are two ways for the applications to verify that a Qualified Signature received is actually a Qualified Signature as such, i.e. based on a qualified certificate and created using a Secure Signature Creation Device (SSCD): either because the application "knows" that the CSP provides only Qualified Signatures, or because the certificate makes use of the "qCStatements extension" as defined in the RFC 3739. Among the surveyed applications which are requiring a Qualified Signature, half of them are enforcing this need by limiting the list of CSPs they are trusting as provider of Qualified Signature. This way of working constitutes however a barrier to full European interoperability.

- **Signature format**

As in the previous study, it appears that among the surveyed applications, many different types of signature formats have been found (PKCS#7, XMLDSig, XAdES, CAdES ...). To avoid issues linked to signature format recognition, we still recommend promoting the use of international standards. Moreover, this recommendation fits in the strategy of other important initiatives such as ETSI PLUGTEST™ which is focusing on XAdES Interoperability, the STORK large scale pilot, the PEPPOL project or the Cross Border Interoperability of eSignatures [CROBIES] study.

- **Signature validation**

Most of the surveyed applications rely on the validation mechanisms provided by the CSP they trust or on the validation mechanisms provided by their national framework. In any case, they all usually only able to validate signature that have been generated by CSPs from their own country. In general, eGovernment applications have been developed in that way because no trust relationships exist with other CSPs but also because they want to limit the number of CSPs that they have to interact with.

The signature validation landscape has changed in Europe since 2007. Indeed, in the previous study, Spain was the only country to mention the existence of a validation service, called @firma.

But, among the surveyed applications of this study, 5 validation services were reported: @firma in Spain (currently being extended to cover certain Portuguese qualified signature solutions), e-Notarius in Poland, MOA-SP in Austria, VPS/Governikus in Germany and BBS in Norway. This trend proves that the signature validation issue has been deemed as sufficiently important to be quickly tackled also for the eGovernment applications.

The usage of validation services in the Member States will partially solve the interoperability issue of signature validation, but still a mean to federate (i.e. interconnect) those services at the European level will be missing. The preliminary conclusions of the EFVS feasibility study [RD9], whose goal is to address this signature validation interoperability issue, show that it will likely not be feasible for the European Union to set-up a Federation of Validation Services, and that alternative governance models will need to be explored.

- **Signature algorithm**

Not all surveyed countries have the same security requirements in terms of signature algorithm. E.g. as of 1/1/2010, SHA-1 will no longer be allowed for hash functions in use with Qualified Certificates in Germany. The decision was made following the discovery of a security issue within SHA-1. This type of problem will not be seen at signature creation time. But if the signed document needs to be sent out to another country, then the latter might reject the signature because it was created in year X using a signature algorithm which was already no longer allowed in the country where the signature is now being validated. To address this issue, harmonisation work is needed at European level. At any rate, decisions to no longer allow one signature/digest algorithm due to security issues should be made collegially by all Member States.

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:175:0045:0046:EN:PDF
[RD5]	IDABC Preliminary study on mutual recognition of eSignatures for eGovernment applications (2007) http://ec.europa.eu/idabc/en/document/6485
[RD6]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0018:EN:NOT
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0017:EN:NOT
[RD8]	IDABC Work programme 2005-2009 (sixth revision) http://ec.europa.eu/idabc/servlets/Doc?id=32115
[RD9]	Feasibility study European Federated Validation Service

	http://ec.europa.eu/idabc/en/document/7764
[RD10]	CROBIES study http://ec.europa.eu/information_society/policy/esignature (expected to be published by 1 November 2009)
[RD11]	e-Signature website http://ec.europa.eu/information_society/policy/esignature

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

It should be noted that for the purposes of this questionnaire, only services which rely on eSignatures are relevant, and that the focus is on eGovernment applications offered to citizens and businesses (A2C and A2B, rather than A2A).

- *eSignature or electronic signature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions. However, PKI solutions are the principal focus of this questionnaire, and non-PKI solutions should only be included if no PKI solutions are in common use. It should also be noted that the questionnaire only examines eGovernment applications in which the eSignature is used to sign a specific transaction, and not where the signature is merely used as a method of authentication of the eSignature holder as defined below.
- *Advanced electronic signature*: an electronic signature which meets the following requirements:
 - (a) it is uniquely linked to the signatory;
 - (b) it is capable of identifying the signatory;
 - (c) it is created using means that the signatory can maintain under his sole control; and
 - (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;Again, this definition may cover non-PKI solutions.
- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive⁵.

⁵ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML>

- *Simple electronic signature*: an electronic signature which does not meet the requirements of an advanced electronic signature as defined above (and thus also not of a qualified electronic signature).
- *Authentication*: the corroboration of the claimed identity of an entity and a set of its observed attributes (i.e. the notion is used as a synonym of “entity authentication”). It should be noted that the questionnaire is focused on the use of eSignatures as a method of signing a transaction, and not on their use as a method for authenticating the eSignature holder.
- *Relying party*: any individual or organisation that acts in reliance on a certificate (in a PKI solution) or an eSignature.
- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

2.2 Acronyms

A2A	Administration to Administration
A2B	Administration to Businesses
A2C	Administration to Citizens
CA	Certification Authority
CRL	Certificate Revocation Lists
CSP	Certificate Service Provider
eID	Electronic Identity
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
QES	Qualified Electronic Signature
SA	Supervision Authority
SOAP	Simple Object Access Protocol
SCVP	Server-based Certificate Validation Protocol
SSCD	Secure Signature Creation Device
USB	Universal Serial Bus
TTP	Trusted Third Party
TSA	Time Stamp Authority
TST	Time Stamp Token
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language
XML-DSIG	XML Digital Signature

3 Introduction

The European Commission - DG DIGIT (hereafter the Commission) has undertaken a number of initiatives in recent years to improve the interoperability between electronic signature solutions at the European level, building on the legal framework created by the eSignatures Directive. Specifically, the European Community Programme for the interoperable delivery of pan-European e-government services to public administrations, businesses and citizens (hereinafter **IDABC**) has been working on identifying, supporting and promoting the development and establishment of pan-European e-government services and the underlying interoperable communications networks.

One of these IDABC initiatives was the 2007 Preliminary study on mutual recognition of eSignatures for eGovernment applications. This study aimed to collect information on eSignature approaches in eGovernment applications in 29 countries (27 Member States and 2 candidate countries, Turkey and Croatia), which were subsequently analysed to determine interoperability barriers and potential interoperability solutions.

However, the field of eSignatures has advanced to a certain extent in recent years, including under the influence of the approaching implementation of the Services Directive and due to recent projects with an interoperability impact, like the PEPPOL cross border eProcurement pilot project. For this reason, changes in the EU eSignatures domain need to be carefully monitored.

The present study therefore aims to update the available information, and to assess to which extent the use of eSignatures in the EU has evolved in the past two years. The scope of the Study has also been expanded somewhat, both with respect to geographical scope (now covering the 3 EEA countries Norway, Iceland and Liechtenstein as well) and with respect to subject matter (now examining inter alia also specific applications in the eProcurement, eHealth and eJustice sectors, along with newer signature technologies like mobile eSignatures and new interoperability initiatives).

The first phase of this study provided an extensive overview of currently existing or envisaged relevant e-government applications in all Member States, which make use of electronic signatures. While eProcurement, eHealth and eJustice were particular areas of focus for this Study, other application domains were covered as well.

Per covered country, relevant information has been collected and a profile has been drafted by a local correspondent describing for each application the type of electronic signature legally required, the technical implementation of the interface between the application and the electronic signature, the applicable technical restrictions notably regarding interoperability with non-national electronic signatures and the authorities or institutions that have been contacted to obtain information. The collected information was validated by the IDABC eSignatures expert group, consisting of national experts on eSignatures in public administration, designated by the competent administration of the country itself, to ensure the reliability and completeness of the profiles.

The aim of this study is to analyse the national country profiles, to detect similarities and differences and, on the basis of this comparative study, to provide an assessment from the perspective of interoperability for cross-border e-government services in Europe.

The study focuses on signature applications with regard to the interaction between governmental authorities and the public (A2B and A2C services, i.e. services to citizens, professionals, companies). Purely internal interactions (A2A services, i.e. the e-government back-office) as such are not within the scope of the study. Applications merely serving entity authentication purposes (i.e. not involving electronic signatures) are not the aim of this study. They are the object of a further study in the framework of IDABC, focusing on electronic identity management schemes for e-government purposes.

The present report aims at:

- comparing existing solutions and requirements from the countries and identifying similarities and differences on the legal as well as on the technical levels. A topology of eGovernment applications/services will be built based on their legal and technical requirements.
- detecting potential interoperability issues, i.e. legal and technical obstacles for using electronic signatures in cross-border e-government transactions.

The report examines both legal and technical aspects of electronic signatures in e-government applications.

The legal framework pertaining to the use of e-signatures in e-government applications can be a deciding factor in its uptake. Particularly, the framework needs to meet the requirements of all involved parties:

- it needs to offer legal certainty with regard to the requirements to be met by the used e-signature technique;
- it needs to offer legal certainty with regard to the result of using the application (i.e. the legal effect of the signature and the signed document);
- it needs to offer sufficient guidelines to service providers in all stages of the process (application owners and designers, CSPs, token manufacturers, etc);
- it needs to ensure the long term validity of the signature and the signed document for any application to which this factor is relevant;
- a variety of additional legal requirements need to be met, including with regard to privacy protection, liability, and security.

In this report, we will describe what legal standards have been presented to the surveyed countries, and how they have taken these to heart in creating their own legal framework with regard to e-signatures in eGovernment applications. Specific attention will be devoted to the requirements for the most dominant signature techniques for the surveyed countries, and the impact that this may have on cross-border interoperability.

The main purpose is to provide a short descriptive overview of European regulatory initiatives and the issues they present, and a more thorough examination of national approaches, specifically with regard to their e-government regulations. To the extent possible, categories of approaches will be proposed for each examined legal aspect. An evaluation of this information will be included in the chapter on the impact of e-signature interoperability.

We will first take a brief look at the national legal framework with regard to e-signatures, first at a general level and then more specifically as it applies to e-government applications, since this is essentially the baseline that has been provided to the surveyed countries as a general target.

The second part of the analysis will indicate what e-signature solutions are endorsed/recommended/required in the surveyed countries, and which requirements have been imposed (including qualification according to the tiers of the e-signature directive, and accessibility of the application to non-nationals).

From a technical perspective we will look at the reported e-government applications to find if their approach is in some way illustrative of a given trend. The main purpose is to describe the technical and organisational solution models, which need to be taken into account for further analysis and recommendations. The applications will be classified in a limited number of models, in order to obtain some degree of transparency and to enable an assessment with regard to interoperability for cross-border e-government transactions. eProcurement, eHealth and eJustice applications will be examined in greater detail, specifically to determine what approaches the surveyed countries have taken to determine the legal mandates / authorisations of signatories.

The legal and technical analysis of the e-signature applications in the surveyed countries will lead us to a list of interoperability issues. The issues will be presented and can be used as a basis for the ongoing discussions on possible European strategies in this area.

Of course, reports such as these are only possible through the assistance of local experts who are capable and willing of providing information with regard to their legal frameworks and administrative

practices. The Study team especially wants to acknowledge the contributions of the following authors for each of the country profiles:

E.U. Member States		Report draft date (date of receipt or last update)
Country	Author(s)	
Austria	Herbert Leitold (A-SIT)	14/05/2009
Belgium	Prof. Jos Dumortier and Hans Graux (time.lex Law Offices)	31/08/2009
Bulgaria	George Dimitrov (Dimitrov, Petrov & Co Law Offices)	16/05/2009
Cyprus	Olga Georgiades (Lexact Business & Legal Solutions)	12/05/2009
Czech Republic	Lucie Urbanova (Ministry of Interior, Czech Republic)	15/05/2009
Denmark	Dr. Henrik Udsen (University of Copenhagen)	27/08/2009
Estonia	Tarvi Martens (AS Sertifitseerimiskeskus)	19/08/2009
Finland	Teemu Rissanen (Conseils Oy)	14/05/2009
France	Fanny Coudert (time.lex Law Offices)	01/09/2009
Germany	Hajo Bickenbach (2B Advice GmbH) and Jörg Apitzsch (bremen online services GmbH & Co. KG)	10/06/2009
Greece	Eleni Kosta (time.lex Law Offices)	26/05/2009
Hungary	Dr. András Gerencser	22/06/2009
Ireland	Prof. Maeve McDonagh and Fidelma White (University College Cork)	19/05/2009
Italy	Davide M. Parrilli (time.lex Law Offices)	31/08/2009
Latvia	Agris Repss and Inese Rendeniece (Sorainen Law Offices)	22/05/2009
Lithuania	Sergejs Trofimovs and Renata Beržanskienė (Sorainen Law Offices)	01/09/2009
Luxemburg	Claire Léonelli (Molitor, Fisch & Associés Law Offices)	15/05/2009
Malta	Paul Gonzi and Antonio Ghio (Fenech and Fenech Law Offices)	27/05/2009
The Netherlands	Dr. Nathan Ducastel (HEC – Het Expertise Centrum)	20/05/2009
Poland	Marcin Kalinowski (Unizeto)	25/08/2009
Portugal	Pedro Simões Dias	14/05/2009
Romania	Peter Buzescu (Buzescu Ca. Law Offices)	18/05/2009
Slovakia	Zuzana Halasova	31/08/2009
Slovenia	Alenka Zuzek (Dr. Alenka Zuzek Nemeč, Dept. of International Relations, Ministry of Public Administration)	16/09/2009
Spain	Cristina De Lorenzo (Sánchez Pintado & Núñez)	31/07/2009
Sweden	Prof. Christine Kirchberger (Swedish Law and Informatics Research Institute, University of Stockholm)	19/05/2009
United Kingdom	Richard Trevorah (xidm Limited)	15/05/2009
EEA		
Country	Author(s)	
Iceland	Haraldur A Bjarnason (Ministry of Finance)	19/05/2009
Liechtenstein	Norbert Ospelt ("IT-Technology, IT-Security, EU/EEA" Unit, Information Technology Service, Office of Human and Administration Resources) and Hans Graux (time.lex Law Offices)	24/08/2009
Norway	Thomas Myhr (Norwegian Broadcasting Corporation (NRK))	02/09/2009
Candidate countries		
Country	Author(s)	

Croatia	Dr. Leda Lepri (Central State Office for Administration)	13/05/2009
Turkey	Prof. Leyla Keser (Istanbul Bilgi University)	26/05/2009

4 Analysis

4.1 Main e-signature solutions

As a first and most basic step in assessing the current landscape of electronic signatures in e-government applications in the Member States, EEA countries and certain candidate countries, we will identify the main e-signature solutions currently in use. The sections below will first provide a general high-level overview table, and will then examine each type of electronic signature solution in more detail.

4.1.1 General overview table

As a first quick overview, the table below provides a mapping for each surveyed country against the possible electronic signature solutions which may be in use. A broad perspective was taken at this early stage, and the table below thus covers national eID cards, sector specific smart cards, generic smart cards, USB tokens, soft certificates, mobile e-signatures, and paper tokens. The table only includes available solutions, and not solutions which are in the planning/design/pilot stage. Each of these solutions, including their use and reported signature type, will be examined in greater detail in the following sections.

Country	National eID cards	Sector specific SC	Generic crypto token	Soft certificate	Mobile e-signature	Multi-factor authentication	Single-factor authentication
Austria		X	X				
Belgium	X		X	X		X	
Bulgaria			X				
Croatia		X	X				
Cyprus							
Czech Republic			X	X			
Denmark				X			
Estonia	X		X				
Finland	X			X	X	X	
France		X	X	X			
Germany		X	X				
Greece		X		X			
Hungary			X	X			X
Iceland			X	X			
Ireland		X					X
Italy	X	X	X				
Latvia				X			
Liechtenstein	X			X			
Lithuania	X	X			X		
Luxembourg			X				
Malta				X			
The Netherlands		X	X			X	
Norway			X	X	X	X	X

Country	National eID cards	Sector specific SC	Generic crypto token	Soft certificate	Mobile e-signature	Multi-factor authentication	Single-factor authentication
Poland			X	X	X		
Portugal	X		X				
Romania			X				
Slovakia			X	X			
Slovenia			X	X			
Spain	X		X	X			
Sweden			X	X			X
Turkey			X	X	X		
United Kingdom							X

Each of these specific categories will be examined separately in further detail below, specifically in order to assess to whom those solutions are available, and which types of signatures can be created using them. Provisionally, some notable comments can already be made:

- eID cards are available in 8 out of 32 countries (25% of surveyed countries). Two of these are new compared to the 2007 edition of the study: Liechtenstein and Lithuania.
- Sector specific smart cards (i.e. issued only to a specific user group or in relation to a specific application field) were found in 9 countries (28%), whereas generic crypto tokens and soft certificates were found in respectively 21 and 18 countries (66% and 56%). Given that the latter two groups are typically issued by private sector parties, this shows the strong role that the private sector can play in supporting eGovernment policies.
- Mobile signatures are only available in 5 countries at this point (16%). However, a larger number of countries has solutions planned for the near future, as will be seen below.
- Authentication solutions were reported only to a limited extent, undoubtedly because they are not commonly seen as signature solutions. Multi-factor and single factor authentication solutions were reported in only 4 (13%) and 5 countries (16%) respectively.

4.1.2 eSignatures based on national eID cards

4.1.2.1 Overview table

The table below will present a summary for each country that has a national eID card strategy in place, noting specifically the name, who can obtain an eID card (or is required to get it), and the legal classification of the signature that you can create with it (qualified signatures, advanced signatures based on qualified certificates, advanced electronic signatures, or simple signatures, as defined in the glossary above). The status of the eID card programme will be indicated as well by marking it as available, planned, or under consideration.

Country	Description	User group	Reported signature type ⁶	Status
Belgium	National eID card (BELPIC)	Belgian citizens over the age of 12 ⁷ Foreigners cards are also available.	Qualified signature	Available Roll-out is virtually complete (around 8.5 million cards issued)
Croatia	National eID card	Croatian citizens.	Not decided yet	Planned. Roll-out is anticipated in 2010.
Czech Republic	National eID card	Czech citizens	Not decided yet	New Act on ID cards is in the draft phase.
Estonia	National eID card	Estonian citizens over the age of 15 and foreigners with a residence permit of at least one year	Qualified signature	Available Roll-out is virtually complete (around 1 million cards issued)
Finland	National eID card (FINEID)	All Finnish citizens and foreigners with a residence permit above the age of 18	Qualified signature	Available
France	National eID card	French citizens	Qualified signature	Planned. Roll-out is

⁶ As indicated by the correspondent in the national reports.

⁷ The under-12 may voluntarily choose to request so-called Kids-IDs, but the signature certificate on these smart cards is revoked, so they are out of the scope of this study.

Country	Description	User group	Reported signature type ⁶	Status
	(CNIE)			anticipated in 2012.
Germany	National eID card (ePA -elektronischer Personalausweis)	German citizens	Qualified signature (if enabled; signature support is optional)	Planned. Limited pilots are running; deployment is expected in Q4 2010
Iceland	Citizen cards issued by the National Registry	Undecided (likely linked to natural persons in the National Registry)	Undecided	Under consideration
Italy	National eID card (EIC - Electronic Identity Card)	Italian citizens	Qualified signature (if enabled; signature support is optional)	Available (although some communes still issue paper ID cards)
Latvia	Personal identity cards	Latvian citizens	Undecided	Under consideration
Liechtenstein	lisign eID card	Liechtenstein citizens	Qualified signature	Available since 23 June 2009
Lithuania	National eID card	Lithuanian citizens	Qualified signature	Available since 1 January 2009
Malta	Personal identity cards	Maltese citizens	Qualified signature ⁸	Planned
The Netherlands	National eID card (eNIK)	Dutch citizens	Qualified signature	Under (re-) consideration ⁹
Norway	National eID card	Norwegian citizens (on a voluntary basis)	Qualified signature	Planned. Draft regulation and specifications are currently being finalised.

⁸ Information kindly provided by M. Adrian Camilleri of the Malta Information Technology Agency after the finalization of the Maltese country profile.

⁹ Plans for a Dutch eID card were set back when the procurement process for an eID solution was successfully challenged before a Dutch court, meaning that the procurement would need to be restarted. Since then, debates have reopened on the benefits of an eID card solution, and specifically whether an extended and more systematic use of the existing DigiD-scheme might not be a preferable option.

Country	Description	User group	Reported signature type ⁶	Status
Poland	National eID card (pl.ID)	Polish citizens	Qualified signature ¹⁰	Planned. Draft regulation has been introduced, and the project will begin in Q4 2009. The eID cards are scheduled to become available in 2011.
Portugal	National eID card Citizen's Card (Cartão de Cidadão)	Portuguese citizens	Qualified signature	Available
Romania	National eID card	Romanian citizens	Qualified signature	Planned. Regulation has been adopted, and issuance is expected in early 2011.
Slovenia	National eID card	Slovenian citizens	Not decided yet	Under consideration
Spain	National eID card (DNIe)	Spanish citizens	Qualified signature	Available

4.1.2.2 General conclusions

The table above shows a significant support for eID card related plans. Currently, 8 out of 32 countries (25%) have eID cards available (Belgium, Estonia, Finland, Italy (availability varies regionally), Liechtenstein, Lithuania, Portugal and Spain). Two of these are new in the list compared to the 2007 edition of the IDABC eSignatures study: Liechtenstein and Lithuania both began issuing eID cards in the first half of 2009. It is very interesting to note that all of these allow the creation of qualified signatures, making them a very suitable basis for interoperability initiatives.

¹⁰ More accurately, current draft regulations envisage that the Polish eID card will support so-called 'personal signatures', a new concept to be introduced. As personal signatures are currently planned to be considered legally equivalent to hand written signatures, the European equivalent term would appear to be a qualified signature.

Additionally, it should be noted that the table above includes only national eID cards which were identified as such in the country reports by the national correspondents. When a broad definition is used that includes any eID card issued by public administrations, but also cases where the eID card was issued by a private CSP with a specific government mandate¹¹ or where smart cards can be activated to be used in eGovernment applications though a decision from a governmental body¹², then the list of 'official eIDs' is much larger, and covers 13 countries, namely seven countries where an eID card is issued by public bodies (Belgium, Estonia, Finland, Italy, Lithuania, Portugal and Spain), and six countries relying on generic smart cards issued by private CSPs with a public sector mandate (Austria, Iceland, Liechtenstein, Luxembourg, the Netherlands and Sweden).

In addition to these, 8 more countries (25%) are currently planning the introduction of eID cards: Croatia (planned in the course of 2010), the Czech Republic, France (2012), Germany (Q4 2010), Malta, Norway, Poland (2011) and Romania (2011). Of these eight countries, five have decided that these should allow the creation of qualified signatures (France, Germany, Norway, Poland, Romania), whereas the other three (Croatia, Malta and the Czech Republic) have not yet decided on the issue.

Thus, 16 out of the 32 surveyed countries are currently issuing or are planning to issue eID cards in the next three years.

With respect to the other 16 countries, four report that they are considering eID cards, but no decision has been made yet (Iceland, Slovenia, the Netherlands, and Latvia). Provided that an eID card would be introduced, plans in the Netherlands point to a qualified signature enabled card, whereas the other four have not made any decisions in this respect yet.

Countries which are not in the list above rely on other signature solutions, including through collaboration with private sector partners as we will see in the sections below. In that respect, it is clear that the measure of uptake of eID cards should not be considered as not a proxy for eSignature sophistication, as e.g. the Austrian approach based on an open eSignature model clearly demonstrates.

Generally, eID card support seems to be increasing, but not universally so. The list of countries without eID card plans or ambitions contains 11 countries (34%), and it is also interesting to point out the example of the Netherlands, where existing eID card plans are currently under reconsideration, on the basis that private sector cooperation might prove to be a suitable and more cost effective approach. Thus, eID card support is not universal.

¹¹ As is e.g. the case in Luxembourg and Liechtenstein

¹² E.g. the Austrian Bürgerkarte can be issued by private sector parties, but it must be activated as a Bürgerkarte by a decision of the Austrian SourcePIN authority, which is part of the Austrian data protection authority.

4.1.3 eSignatures based on sector specific smart cards

4.1.3.1 Overview table

The table below will present a summary for each country that has a national sector specific smart card strategy in place (i.e. linked to a specific user group or a specific application domain), noting specifically the name, who can obtain the card (or is required to get it), and the legal classification of the signature that you can create with it (qualified signatures, advanced signatures based on qualified certificates, advanced electronic signatures, or simple signatures, as defined in the glossary above). The status of the card programme will be indicated as well by marking it as available, planned, or under consideration.

Country	Description	User group	Reported signature type	Status
Austria	Several varieties of the citizen card concept (including health card, civil servant card, student card, ...)	Depends on the variety of the citizen card	Qualified signature (provided that the citizen card is activated as such, i.e. that it includes a qualified certificate)	Available
Croatia	Croatian Institute for Health Insurance (CIHI) Card (aka isprava 2)	Croatian citizens	Advanced signatures	Available
Finland	Health Care Smart card	Users of the nationwide healthcare information systems	Qualified signature	Pilot
France	Healthcare Professionals card - CPS card	Healthcare providers and any professional led to deliver and to charge refundable services by the Health Insurance	Qualified signature	Available
Germany	HBA (health professional card) and the eGK (Patient health card), following the German Common PKI specifications	Health care professionals and patients	Qualified signature	Available
Greece	SYZEFXIS Smart	Civil servants that	Qualified signature	Available

Country	Description	User group	Reported signature type	Status
	Cards	have access to the SYZEFXIS network		
Ireland	Qualified signature solution issued by the Revenue Commissioners explicitly for the purpose of communicating with the Revenue Commissioners	Only for the communication with Revenue Commissioners; not in other applications	Qualified signature	Available
Italy	National Service Card ('Carta Nazionale dei Servizi', NSC)	Italian citizens who do not yet have an EIC; it is considered a solution to bridge the rollout period of the EIC	Qualified signature	Available
Lithuania	Civil servant eID cards	Civil servants of state institutions	Advanced signature	Available
The Netherlands	UZI-card (Unique Healthcare Provider Identification, Unieke Zorgverlener Identificatie)	Health care professionals	Qualified signature	Available

4.1.3.2 General conclusions

As was also noted in the previous edition of the study, sector specific smart cards remain a rather niche area, with only ten countries reporting a relevant solution. Realistically, two of these play only a limited role, with the Finnish example current still being in the planning stages, and the Irish example referring to niche situation where smart cards are issued directly by the Revenue Commissioners exclusively for the purposes of communicating securely with them.

Within the remaining 8 cards, the health care/health insurance sector represents the largest group, with specific cards being available in four countries: Croatia, France, Germany and the Netherlands. It is interesting to note that the latter three are aimed at health care professionals and support qualified signatures, whereas the Croatian card is a social insurance card and supports advanced signatures. In the section below on eHealth applications, we will examine whether this focus on qualified signature solutions for health care professionals is indeed a common trend.

It should be stressed that this low response rate is likely partially linked to the fact that other countries may have sector specific cards that are used for authentication purposes only (as is e.g. the case with the Belgian social security card), and which were therefore not covered by the present study. Thus, the actual number of health care/social insurance cards is likely to be greater.

In addition to the health care/social insurance cards, three countries also reported issuing specific civil servant cards, notably Greece, Italy and Lithuania, with the former two allowing the creation of qualified signatures.

The Austrian situation should be examined a bit further, as it is in fact a generic model (the citizen card¹³) that can be applied in any number of sectors, including (but not uniquely) as a sector specific solution. The card provides three major functions:

- Identification backed by principal eGovernment registers such as the Central Register of Residents (CRR), the Supplementary Registers, respectively. A so-called identity link is stored on the citizen card. The identity link holds the name and date of birth, and a sourcePIN which is a unique identifier that is cryptographically derived from the source registers' identifiers. A logical link to the qualified electronic signature is established to allow assigning a certain identity to an electronically signed statement. The identity link is signed by the sourcePIN Register Authority.
- Qualified electronic signature: The certification services may be provided either by the public sector or the private sector. Currently, the only certification service provider for qualified certificates is the private sector provider A-Trust¹⁴.
- Moreover, data on representation might be stored on the citizen card.

Various private sector and public sector projects issue tokens that can be activated as citizen cards. This inter alia includes each bank card, the health insurance card, or civil servant service cards. In quantitative figures this sums up to about 16 million smart-cards rolled out to a population of little less than 9 million. The major rollouts are:

- Each bank card issued since March 2004 is also a SSCD as per Annex III of the Signature Directive 1999/93/EC. About 7 million such cards are in circulation. The cards can be activated as citizen card by applying a qualified certificate using the private sector certification service provider A-Trust.
- The health insurance card has been rolled out to each citizen in 2005 (close to 9 million cards) by the Main Association of Social Insurance Organisations fulfilling the provisions in the General Social Insurance Act. The health insurance card "e-card" is also an SSCD as of Directive 1999/93/EC and can be activated as citizen card. Certification service provider used to be the Main Association of Social Insurance Organisations until end of 2007¹⁵. Since

¹³ www.buergerkarte.at/index_en.html

¹⁴ www.a-trust.at

¹⁵ So-called "administrative signatures" existed in a transition period until end of 2007. These have been advanced electronic signatures with defined technical criteria. The Main Association of Social Insurance Organisations and also by the mobile phone operator A1 for mobile phone signatures opted for this approach that used to have relaxed requirements compared to qualified signatures. As

beginning of 2008 the private sector certification service provider A-Trust has taken over this responsibility and issues qualified certificates.

- Federal ministries such as the Federal Chancellery and the Federal Ministry of Finance issued civil servant service cards as citizen cards. Qualified certificates are provided by the private sector certification service provider A-Trust. Further ministries, regional and local governments plan to issue such service cards for their staff.
- Several universities issue their student service cards as citizen cards. Qualified signatures are issued using the private sector certification service provider A-Trust.
- Several professions issue profession's ID cards as citizen cards, such as notaries public, lawyers, or pharmacists.

Thus, in the specific Austrian solution, the citizen card concept actually covers a multitude of potential application domains.

administrative signatures have been abandoned end of 2007, the solutions are not further discussed here.

4.1.4 eSignatures based on generic crypto tokens

4.1.4.1 Overview table

The table below will present a summary for each country that relies on generic smart cards other than eID cards described above. Typically these are issued by private sector parties. The table will describe who can obtain the card (or is required to get it), and the legal classification of the signature that you can create with it (qualified signatures, advanced signatures based on qualified certificates, advanced electronic signatures, or simple signatures, as defined in the glossary above). The status of the card programme will be indicated as well by marking it as available, planned, or under consideration.

Country	Description	User group	Reported signature type	Status
Austria	Several varieties of the citizen card concept	Depends on the variety of the citizen card	Qualified signature (provided that the citizen card is activated as such, i.e. that it includes a qualified certificate)	Available
Belgium	Smart cards/USB keys issued by three private CSPs (Certipost, GlobalSign and Isabel)	Enterprises and entrepreneurs	Qualified signatures	Available
Bulgaria	Universal Electronic signature, issued by private CSPs	Bulgarian	AdES based on QC	Available
Croatia	Smart cards issued by the CSP FINA, or the bank Zagrebačka banka	Citizens and businesses	FINA: Qualified signatures, AdES based on QC and AdES. Zagrebačka banka: Qualified signatures	Available
Czech Republic	Smart card, cryptographic token or validated HSM	Civil servant	AdES based on QC	Available
Estonia	Business-ID issued by a private CSP (AS Sertifitseerimiskeskus), resulting in a company stamp	Companies	AdES	Available
France	USB key, chipcard issued by private CSPs	Citizen	AdES based on QC	Available
	The REAL key	Any person using the services of clerks	AdES based on QC	Available

Country	Description	User group	Reported signature type	Status
Germany	Several private CSPs issuing cards implementing the Common PKI specifications	Citizens and businesses	Qualified signatures and AdES	Available
Hungary	Smart card, USB token	Citizens	Qualified signatures and AdES	Available
Iceland	Bank cards issued under a common root (currently only one issuer: Auðkenni hf)	Citizens and businesses who are customers with the bank	Qualified signatures	Available
Italy	Smart card and token usb issued by Italian accredited CSPs	Unrestricted	Qualified signatures	Available
Luxembourg	LuxTrust smartcard, LuxTrust signing stick, LuxTrust signing server certificate	Citizens	Qualified signatures	Available
The Netherlands	Smart cards/USB keys issued by private Dutch CSPs forming a part of the Dutch PKI-Overheid-hierarchy ¹⁶ , or outside of this hierarchy ¹⁷	Citizens and businesses	Qualified signature or AdES, depending on the customer's needs	Available
Norway	Smart cards issued by Buypass; BankID smart cards	Customers of these institutions	Advanced signature based on a qualified certificate	Available
Poland	Smart cards issued by private Polish CSPs	Unrestricted.	Qualified signature or AdES, depending on the customer's needs	Available

¹⁶ Beyond the four private CSPs, two public CSPs are also a part of this hierarchy. PKI-Overheid currently has two certificate hierarchies. The oldest is based on the SHA1-algorithm, the newest on the SHA-256 algorithm.

¹⁷ Qualified or advanced electronic signatures are also issued outside the PKI-overheid hierarchy; however, these are not a part of the same common trust infrastructure, and will therefore not necessarily be accepted in the same number of eGovernment applications. See also <http://www.pkioverheid.nl/over-pkioverheid/achtergrond-pkioverheid/> (Dutch only).

Country	Description	User group	Reported signature type	Status
Portugal	Smart cards issued by private CSPs	Unrestricted.	Qualified signature or AdES, depending on the customer's needs	Available
Romania	Smart cards or USB sticks issued by 3 private Romanian CSPs or by the AISS ¹⁸	Unrestricted.	Qualified signature	Available
Slovakia	Smart card, USB token	Citizens	AdES or qualified signature	Available
Slovenia	Smart card	Citizens	AdES based on QC	Available
Spain	Smart cards issued by private CSPs	Unrestricted.	Qualified signature or AdES, depending on the customer's needs	Available
Sweden	Smart cards issued by companies selected in a government frame agreement procurement	Swedish citizen and others that have been introduced in the population register can get cards. Most issuers today are banks.	AdES ¹⁹	Available
Turkey	Smart card, USB token	Citizens	AdES	Available

4.1.4.2 General conclusions

Given that private sector issued generic tokens were reported in 22 countries out of 32, it is clear that the private sector plays a significant role in supporting eGovernment eSignature policies. In 19 cases, these were issued by CSPs without links to the financial sector, and in 3 cases (Norway, Iceland and Croatia) they were issued by financial institutions. The aforementioned specific case of Austria should be mentioned again, as a generic model that can be issued by any party.

With regard to the legal classification of the signatures, all options are covered with no real dominant solution being apparent: 15 of the 22 countries referred to qualified signature solutions, 6 to advanced

¹⁸ Agency for Information Society Services (in Romanian Agentia pentru Serviciile Societatii Informationale)

¹⁹ eID issuers within the Swedish framework agreement do not claim (or feel the need to claim) that their certificates are "qualified" certificates or can be used to create "qualified" electronic signatures. They are considered sufficiently reliable without this label.

signatures based on qualified certificates, and 11 to advanced signatures (keeping into account of course that several CSPs issue multiple types of signature depending on user requirements and preferences, meaning that several CSPs are counted in multiple categories).

4.1.5 eSignatures based on soft certificates

4.1.5.1 Overview table

The table below will present a summary for each country that relies on soft certificates (usually issued by private sector parties), noting specifically the name and issuer, who can obtain the certificates (or is required to get it), and the legal classification of the signature that you can create with it (advanced signatures based on qualified certificates, advanced electronic signatures, or simple signatures, as defined in the glossary above). The status of the card programme will be indicated as well by marking it as available, planned, or under consideration.

Country	Description	User group	Reported signature type	Status
Belgium	Soft certificates issued by three private CSPs (Certipost, GlobalSign and Isabel)	Enterprises and entrepreneurs	AdES based on QC for Certipost; AdES for Globalsign and Isabel	Available.
Denmark	OCES (Offentlige certifikater til elektronisk service – public certificates for electronic services) signatures, based on certificates issued by DanID ²⁰	Natural persons and enterprises (4 different CPSs exist: for personal certificates, company certificates and employee certificates)	AdES	Available (and a mandatory standard for the implementation of electronic services)
Czech Republic	Soft certificates issued by one of three accredited CSPs	Citizen	AdES based on QC	Available
Finland	Soft certificates issued by SoneraCA or Elisa	natural and non-natural persons	AdES based on QC	Available
France	Soft certificates issued by PRISV1 qualified CSPs	Citizens, Businesses	AdES, Qualified Certificates	Available
Greece	Hermes	Citizens and enterprises	AdES	Planned
Hungary	Soft certificates	Private persons, enterprises, government	AdES, Qualified certificates	Available
Iceland	Soft certificates issued by private CSPs	Unrestricted (but limited in scope)	AdES	Available (but limited in scope; not

²⁰ In order to issue OCES certificates, a CA must enter into an agreement with the National IT and Telecom Agency

Country	Description	User group	Reported signature type	Status
				systematically promoted)
Latvia	Soft certificates issued by Latvijas Posts	Natural and legal persons	AdES	Available
Liechtenstein	Soft certificates issued by private CSP A-Trust	Unrestricted	AdES based on QC	Available.
Malta	Soft certificates issued by Malta Electronic Certification Services Ltd	Unrestricted	AdES	Available.
Norway	Soft certificates issued by a BankID member, stored securely on the bank server	Unrestricted	AdES based on QC	Available.
Poland	Soft certificates issued by private CSPs (mainly Unizeto Technologies S.A. (CSP: Certum), PWPW S.A. (CSP: Sigillum) and KIR S.A. (CSP: Szafir).	Unrestricted	AdES based on QC or AdES, depending on the customer's needs	Available.
Slovakia	Soft certificate	vendor/tenderer after approval by the contracting authority or utility	AdES	Available
Slovenia	Soft certificate	Natural person	AdES based on QC	Available
Spain	Soft certificate	Persons, companies, machine or automated processes	AdES, AdES based on QC	Available
Sweden	Soft certificate	Swedish citizen and others that have been introduced in the population register can get cards. Most issuers today are banks.	AdES ²¹	Available
Turkey	Soft certificate	Judges, prosecutors and staff, lawyers, citizens	AdES	Available

²¹ eID issuers within the Swedish framework agreement do not claim (or feel the need to claim) that their certificates are “qualified” certificates or can be used to create “qualified” electronic signatures. They are considered sufficiently reliable without this label.

4.1.5.2 General conclusions

In total, 18 out of 32 countries (56%) reported using soft certificates as part of their public sector eSignature strategy, showing again the strong role that the private sector can play in this respect. 13 out of these issued qualified soft certificates, whereas 12 relied on nonqualified solutions (with obviously some overlap for countries in which both possibilities are available).

For some countries, the use of soft certificates is not merely a supporting strategy, but the basis of the eGovernment eSignatures approach. This is most notably the case in Denmark the OCES signature is the primary solution:

“The Danish OCES standard is based on advanced electronic signatures. The legal framework of the OCES concept consists of an agreement between the CA and the National IT and Telecom Agency. Four OCES Certificate Policies (CPs) are part of this agreement. In order to issue OCES certificates, a CA must enter into an agreement with the National IT and Telecom Agency. In this agreement, the CA undertakes to comply with the terms of the certificate policies drawn up by the Agency. The report implies an external system audit of the CA. The terms governing the annual report have been drawn up on the same principles as those appearing from the Act on Electronic Signatures. At the moment an agreement exists with DanID (a company under PBS owned by the financial sector) as a CA issuing OCES signatures. DanID won the contract for the next generation digital signature and has also taken over the contract on the existing digital signature from TDC.

The requirements of the CP's are very similar to the requirements of the Danish Act on electronic signatures (which transposes the eSignature Directive into Danish law). An important difference concerning liability is that the CA within the OCES concept has the possibility to limit its liability in the relationship that exists between the CA and its contracting parties to the extent that such joint contracting parties are business operators or public authorities, but not at all in relation to private people as contracting parties.

A general assessment of the OCES standard being secure enough to logon, sign and send personal data with has been made by the National Data Protection agency, based on the security level described in the CPs.

Within the next couple of years a mobile solution for the next generation digital signature (OCES II) is planned. The solution will be based on wireless PKI (wPKI), where digital signatures are stored on the mobile phone's sim-card.

The OCES signature is available to both natural and legal persons.

In 2008 the OCES standard became a mandatory standard for the implementation of electronic services.”

Thus, to reach interoperability between all European Member States, an approach is needed that integrates nonqualified solutions issued by private sector parties at an appropriate level as well.

4.1.6 eSignatures based on mobile e-signatures

4.1.6.1 Overview table

The table below will present a summary for each country that relies on mobile phones as a part of its eSignature strategy, noting specifically the name and mobile phone operator, who can obtain the card (or is required to get it), and the legal classification of the signature that you can create with it (qualified signatures, advanced signatures based on qualified certificates, advanced electronic signatures, or simple signatures, as defined in the glossary above). The status of the card programme will be indicated as well by marking it as available, planned, or under consideration.

Country	Description	User group	Reported signature type	Status
Austria	Mobile signatures to be offered by any operator.	Any mobile phone subscriber	Qualified signature	Planned for Q4 2009
Croatia	Mobile signatures, to be managed by FINA	Croatian citizens	Not decided yet	Planned for 2010
Denmark	Mobile signatures based on wPKI (OCES II), with certificates stored on the SIM card	Not defined yet	Not decided yet	Planned, but no deadlines yet.
Estonia	Mobile signatures (MobileID) offered by operator operator EMT in co-operation with SK as the CA	Any mobile phone subscriber of EMT with an Estonian eID card (required for activation; see explanation below)	Qualified signature	Available; around 10.000 users
Finland	Soft certificates issued by SoneraCA or Elisa	natural and non-natural persons	AdES based on QC	Available
Italy ²²	Mobile signatures to be offered by any operator.	Unrestricted	Qualified signature	Not yet available; experimental –

²² Information kindly provided by M. Adriano Rossi of the CNIPA after the finalization of the Italian country profile.

Country	Description	User group	Reported signature type	Status
				HSM under SSCD verification process
Lithuania	Mobile signatures from certain CA's and operators UAB "Omnitel" ²³ and UAB "Bitè Lietuva"	Customers of these service providers	Qualified signature	Available
The Netherlands	Mobile signatures offered by qualified CSP Diginotar under the name EazyID	Not defined yet	Qualified signature	Planned for Q4 2009
Norway	Mobile authentication via SMS, including via Bypass	Users of the All-in or MyPage portal	Authentication ²⁴	Available
Poland	Mobile signatures offered by the Plus GSM operator, with Mobitrust as a CA	Plus customers, mostly in the business sector (used for public sector applications)	Qualified signature	Available since late 2008
Slovenia	Mobile signatures offered by MOBITEL operator	Natural and legal persons	Qualified signature	Pilot
Turkey	Crypto card embedded in SIM card ²⁵	Citizen	AdES based on QC	Available

4.1.6.2 General conclusions

Five countries out of 32 thus currently report using electronic signatures as a part of their eSignature strategy for eGovernment, which is a relatively modest 16%. However, 7 more countries have short term plans to begin using mobile phone based eSignatures, which would bring the total up to 37.5%. Thus, there seems to be a perception that there is a market based for this type of solution.

²³ In the case of Omnitel, the operator functions as a RA on behalf of the Estonian CA AS Sertifitseerimiskeskus.

²⁴ The mobile solution is considered a form of authentication; not as a form of signature.

²⁵ Only for the authentication of citizens

Looking at the types of signatures that can be created, of the five existing solutions three claim a qualified signature status (Estonia, Lithuania and Poland), one an advanced signature based on qualified certificates (Finland), and one only an authentication status (Norway, bringing it out of scope of this study). Of the six planned solutions, three more are expected to create qualified signatures (Austria, Slovenia and the Netherlands), one an advanced signature based on qualified certificates (Turkey), and the two remaining ones (Croatia and Denmark) have not yet been decided.

It is interesting to examine the different approaches to mobile electronic signatures, in which three large categories can be distinguished:

- In the first case, as e.g. seen in Norway, the mobile phone is used simply to support two-factor authentication, with an SMS providing a time restricted password to allow the end user to log on to a specific service. As was also noted in the Norwegian profile, it is debatable whether this can be considered a signature in the sense of the Directive, or more accurately whether it can be considered a signature that is attached to or logically associated with other electronic data (other than the username/static password of the end user).
- A second approach, which is e.g. seen in Estonia and Lithuania, requires a SIM-card which is PKI-enabled, thus allowing the SIM-card to act as a signature creation device. In these two examples, the certificate was labelled as qualified, and the SIM-card was considered to meet the requirements of an SSCD (although without having been formally assessed as such). These specific examples are also of interest because it is an example of cross border services, with the Estonian CA SK being one of the certificate issuers for both examples (other CAs are active in this domain in Lithuania as well). In addition, it is noteworthy that the mobile phone operator's registration process was not considered trustworthy enough by default, and that the user therefore needs to "activate" the signature solution using his/her eID-card in a web environment. In this manner, the service provider noted that the issuance of the Mobile-ID became implicitly bound to the security and quality of the ID-card.
- Finally, a third approach is currently being pioneered in Austria, which will use qualified certificates in which a hardware security module (HSM) managed by the operator will function as an SSCD storing the cryptographic keys, making the solution an application of the generic Austrian citizen card concept resulting in qualified signatures. Users can create signatures using their secret PIN codes, which are used to decrypt and trigger the private key for the electronic signature. Possession of the corresponding mobile phone is proven by a transaction number (TAN) sent via text message (SMS). This procedure ensures that the private key is under the sole control of its owner. The service provider will be A-Trust, and it will be possible to integrate the functionality into any existing mobile phone. This same possibility is currently also being examined by one of the main Italian accredited CSPs, who is experimenting the use of a HSM containing multiple keys owned by several users, where the signing functionality is initiated by means of a mobile authentication process. The status of this HSM as an SSCD is currently undergoing assessment.

Given the prevalence of mobile eSignature plans, it is clear that much is expected in this domain. However, to the extent that mobile eSignature solutions require the installation of specific software components with eGovernment service providers, interoperability between the aforementioned solutions may be hard to achieve.

4.1.7 eSignatures based on multi-factor authentication

4.1.7.1 Overview table

The table below will present a summary for each country that relies on multi-factor authentication for the creation of signatures (other than the mobile phone solutions described above), noting specifically the name and type of the scheme (paper token – PIN calculator), who can use the solution (or is required to use it), and the legal classification of the signature that you can create with it (advanced electronic signatures, or simple signatures, as defined in the glossary above). The status of the card programme will be indicated as well by marking it as available, planned, or under consideration.

Country	Description	User group	Reported signature type	Status
Belgium	Federal token, a paper token containing a password list	Natural persons	Simple signature	Available. Around 350.000 tokens have been issued.
Finland	The TUPAS token, paper based PIN-TAN lists containing a series of password strings	Natural persons and legal entities	Authentication ²⁶	Available
The Netherlands	The DigiD-scheme covers several options, including multi-factor authentication via mobile phone	Natural persons	Simple signature – advanced signature when using higher security levels of the scheme.	Available
Norway	Various multifactor authentication solutions are possible: one time passwords/PINs via mail or via mobile phone (MyID – controlled by the government)	Natural persons or businesses	Authentication ²⁷	Available

²⁶ TUPAS has become a prevalent solution for most of the online authentication uses and it can also be used to “sign” data within eGovernment and e-banking services. Signing with TUPAS has to be understood as electronically marking a contractually binding consent, or will, and not as electronically signing with a digital certificate in the framework of the EU Directive

²⁷ In Norway these solutions are emphatically considered to be a form of authentication; not as a form of signature.

4.1.7.2 General conclusions

Only four multifactor solutions were reported (13% of surveyed countries), including notably password lists (Belgium and Finland) and one-time password calculators (Netherlands and Norway, including via mobile phone). The main reason for this is undoubtedly the perception that these are entity authentication solutions, and not electronic signatures in the sense of the Directive. This was also explicitly noted in two of the aforementioned cases (Finland and Norway). Thus, these solutions are of lesser interest to this study.

4.1.8 eSignatures based on single-factor authentication

4.1.8.1 Overview table

The table below will present a summary for each country that relies on single-factor authentication (username-password) for the creation of signatures, noting specifically the name and type of the scheme and who can use the solution (or is required to use it). The status of the card programme will be indicated as well by marking it as available, planned, or under consideration.

Country	Description	User group	Reported signature type	Status
Hungary	ClientGate/CESPS username/password	natural persons	Authentication	Available
Ireland	Variety of PIN/password based schemes	Citizens and businesses	Simple signature	Available
Norway	Username / password scheme in the All-in or MyPage portal	Citizens and businesses	Authentication ²⁸	Available
Sweden	Personal security codes (login/password)	Tax payers	Authentication	Available
United Kingdom	User-ID/Password	Citizens/Organizations	Authentication	Available

4.1.8.2 General conclusions

While single-factor authentication solutions were thus clearly not commonly reported as signature solutions, this is of course not due to the fact that they are not commonly used, but due to the fact that they are usually considered to be entity authentication solutions, rather than electronic signatures. I was therefore to be expected that they would only rarely be reported, except in countries with flexible legal and technical traditions. As noted in the Norwegian report on the relationship between authentication and electronic signatures:

“Pursuant to Norwegian law there are very few legal regulations that require a signature in order to make the transaction legally binding. In addition the definitions in the Directive on Electronic Signatures, and subsequently of the Norwegian Act on Electronic Signature, are interpreted to also cover entity authentication. Thus, a qualified certificate under Norwegian law can be used for signature (non-repudiation) and/or entity authentication. This also applies to the national certificate classes

²⁸ In Norway these solutions are emphatically considered to be a form of authentication; not as a form of signature.

defined in the Requirement Specifications for PKI for the Public Sector; Person-High, Person-Standard and Enterprise. In the light of this a report on only eSignature related issues would be of limited value.”

As a result, single factor authentication solutions are of limited interest to the present study.

4.2 Regulatory framework for electronic signatures

4.2.1 Transposition overview

The table below will present a summary for each country of the main regulations transposing the e-Signatures Directive, including both principal laws and any bylaws (decrees etc.). Given the transposition deadline of this Directive (19 July 2001), all surveyed countries have implemented the required regulatory framework at this point. Therefore, the analysis to be added below will focus specifically on any known changes since the completion of the information collection phase in the previous edition of the study (i.e. since 1 January 2007), which will be added *in italics* and further commented, if necessary. In addition, any peculiarities in the interpretation of the Directive will also be commented below the table.

Country	Applicable regulations
Austria	<ul style="list-style-type: none"> • Signature Act which entered into force 1 January 2000 and has been amended in 2000, in 2001, and in 2008; • Signature Order of 2008. <p><i>Amendments in 2008 aimed to align Austrian law more closely with the Directive. Key changes have been:</i></p> <ul style="list-style-type: none"> • <i>Signatories can also be legal persons (qualified certificates can however just be issued to natural persons. Thus, qualified signatures are limited to natural persons)</i> • <i>Clarification that formal confirmation requirements of technical components by a designated body are limited to the SSCD</i> • <i>Introduction of advanced electronic signatures (the concept wasn't used in the Signature Act before)</i> • <i>Introduction of the commonly used term "qualified electronic signature" (previously the term "secure electronic signature" has been used)</i> • <i>Simplifications in the supervision system (e.g. limiting supervision to qualified certification service providers, whereas before all certification service providers fell under supervision)</i> • <i>Simplifications in the issuance process by not necessarily relying on ID cards, but allowing for methods that give equivalent levels of assurance</i>
Belgium	<ul style="list-style-type: none"> • Act of 9 July 2001 laying down a legal framework for electronic signatures and certification services • Royal Decree of 6 December 2002 organising the supervision and accreditation of certification service providers issuing qualified certificates • Act of 20 October 2000 introducing the use of telecommunications tools and

Country	Applicable regulations
Bulgaria	<p>electronic signatures in the judicial and extra-judicial procedure</p> <ul style="list-style-type: none"> • Electronic Document and Electronic Signature Act²⁹ (Закон за електронния документ и електронния подпис, EDESA) • Regulation for the Activity of the Certification Service Providers, the Procedure for its Termination and for the Requirements for Provision of Certification Services (Наредба за дейността на доставчиците на удостоверявателни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверявателни услуги); • Regulation for the Procedure for Registration of Certification Service Providers (Наредба за реда за регистрация на доставчиците на удостоверявателни услуги); • Regulation for the Requirements to the Algorithms for Advanced Electronic Signatures (Наредба за изискванията към алгоритмите за усъвършенстван електронен подпис); and <p>The main <i>differentia specifica</i> of the Bulgarian legislation in comparison to the eSignatures Directive is related to the definitions of different type of electronic signatures. According to Art. 13, Para. 1 of EDESA electronic signature is a data attached to the electronic statement (data message) in a way agreed between the author³⁰ (the signatory) and the addressee and enough secure for the needs of the turnover which:</p> <ul style="list-style-type: none"> ▪ reveals the identity of the author (the signatory); ▪ reveals the consent of the author (the signatory) with the signed electronic message; and ▪ protects the content of the electronic message against any further changes. <p>The meaning of electronic signature under EDESA is similar to the meaning of advanced electronic signature under the Directive.</p> <p>Electronic signatures under EDESA are also considered the advanced electronic signature and the universal electronic signature (UES). The meaning of the advanced electronic signature is different than the meaning of this term under the eSignatures Directive. The advanced electronic signature under EDESA could be equaled to the “qualified” electronic signature under the meaning of Art. 5, Para. 1 of the eSignatures Directive. UES is a type of advanced electronic signature which is supported by a qualified certificate issued by a <i>registered</i> Certification Service Provider.</p> <p>As mentioned above UES is the only type of electronic signature which has the effect of a handwritten signature in respect to everyone dislike the “basic” and the advanced electronic signature which have such an effect only between private persons. Thus, in practice UES is commonly used for the eGovernment needs.</p> <p>EDESA distinguishes two persons related to the electronic signature – the titular</p>

²⁹ Valid as of 6 October 2001, last amendment as of 11 May 2007, see http://www.crc.bg/files/en/ZED_ENG_15.01.2008.htm

³⁰ The author is the natural person who makes the electronic statement – on his own behalf or on behalf of a legal entity or another person as a proxy.

Country	Applicable regulations
	<p>and the author. The author signs with the electronic statement on behalf of the titular and could be only a natural person. In cases where the titular is a natural person who signs the statement by himself, he will be also seen as an author. If the titular is a legal entity or a natural person who will be represented by other person, then information about the grounds of the representative power must be entered in the certificate.</p>
Croatia	<ul style="list-style-type: none"> • Electronic Signature Act (Zakon o elektroničkom potpisu) (NN 10/2002) • <i>Amendments to the Electronic Signature Act (Zakon o izmjenama i dopunama Zakona o elektroničkom potpisu)³¹ (NN 80/08), aiming to bring the law in closer alignment with the Directive. In the context of Croatian law the advanced electronic signature is based on a qualified certificate. The major change in the Amendment on the eSignature Act was the definition of a voluntary accreditation and an accreditation body that still has to be defined by the Government.</i> • Ordinance on the register of qualified certification authorities for electronic signatures (Pravilnik o evidenciji davatelja usluga certificiranja elektroničkih potpisa)³² (NN 54/2002) • Amendments to the Ordinance on the register of qualified certification authorities for electronic signatures (Pravilnik o izmjenama i dopunama Pravilnika o evidenciji davatelja usluga certificiranja elektroničkih potpisa)³³ (NN 112/2007) • Ordinance on the records of certification authorities for electronic signatures (Pravilnik o registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certificate)³⁴ (NN 54/2002) • Ordinance on the measures and procedures for the use and protection of electronic signature and advanced electronic signature, electronic signature and advanced electronic signatures development tools and certification system and obligatory insurance for certification authorities issuing qualified certificates (Pravilnik o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja)³⁵ (NN 54/2002) • Ordinance on the technical rules and conditions for linking certifying systems for electronic signatures (Pravilnik o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa)³⁶ (NN 89/2002)

³¹ Zakon o izmjenama i dopunama Zakona o elektroničkom potpisu;

http://narodne-novine.nn.hr/clanci/sluzbeni/2008_07_80_2604.html

³² Pravilnik o evidenciji davatelja usluga certificiranja elektroničkih potpisa, in English

hrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/02/document/Ordinance_on_the_records_of_CA_OG5402.pdf

³³ Pravilnik o izmjenama i dopunama Pravilnika o evidenciji davatelja usluga certificiranja elektroničkih potpisa

³⁴ Pravilnik o registru davatelja usluga certificiranja elektroničkih potpisa koji izdaju kvalificirane certifikate, in English

http://www.e-hrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/01/document/Ordinance_on_register_of_QCA_OG542002.pdf

³⁵ Pravilnik o mjerama i postupcima uporabe i zaštite elektroničkog potpisa i naprednog elektroničkog potpisa, sredstava za izradu elektroničkog potpisa, naprednog elektroničkog potpisa i sustava certificiranja, in English

hrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/03/document/Ordinance_on_the_measuresOG542002.pdf

³⁶ Pravilnik o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa, in English

Country	Applicable regulations
	<ul style="list-style-type: none"> Regulation on the scope of operations, content and responsible authority for operations of electronic signature certification for state administration bodies (Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave)³⁷ (NN 146/2004)
Cyprus	<ul style="list-style-type: none"> Legal Framework for Electronic Signatures and Associated Matters Law of 2004, as amended by Law 34(I) of 2009 (hereinafter "the Law").³⁸ <i>The Law was amended on 10 April 2009 for the purpose of appointing the Ministry of Communications and Works, Department of Electronic Communications, as the competent authority (originally as task conferred to the Ministry of Commerce, Industry and Tourism).</i>
Czech Republic	<ul style="list-style-type: none"> Act on electronic signature 227/2000 Coll. (Zákon č. 227/2000 Sb., o elektronickém podpisu) Ordinance on electronic filing rooms 496/2004 Coll. (Vyhláška č. 496/2004 Sb. k elektronickým podatelnam) Ordinance on qualified certification service providers' procedures 378/2006 Coll. (Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb) Government decree 495/2004 Coll. implementing act on e-signature 227/2000 Coll. (Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů) Government Decree 140/2000 Coll. on the list of free trade licences (Nařízení vlády č. 140/2000 Sb., kterým se stanoví seznam oborů živností volných) Act on administrative fees 634/2004 Coll., as amended (Zákon č. 634/2004 Sb., o správních poplatcích) <p>The Act on electronic signature defines three instruments:</p> <ul style="list-style-type: none"> electronic signatures (transposition of the directive) electronic marks qualified time stamps
Denmark	<ul style="list-style-type: none"> Act no. 417 of 1 October 2000 on Electronic Signatures³⁹. It should be noted that the act covers <i>only</i> signatures based on qualified certificates. Since the OCES signature is an advanced signature, it is not covered by this or any other general eSignature legislation. Rather, its legal value is

http://www.e-hrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/04/document/Ordinance_on_tech_rulesOG892002.pdf

³⁷ Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave and an English version :

http://www.e-hrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/04/document/Ordinance_on_tech_rulesOG892002.pdf

³⁸ Law No. 188(I)/2004.

³⁹ See http://147.29.40.91/SHOWF_B762442665/1072&A20000041730REGL&0001&000001

Country	Applicable regulations
	<p>determined by general legal principles.</p> <ul style="list-style-type: none"> Executive Order no. 922 of 16 October 2000 on "Reporting of Information to the National Telecom Agency by CAs and system Auditors"⁴⁰; Executive Order no. 923 of 16 October 2000 on "Security Requirements etc. for Certification Authorities"⁴¹;
Estonia	<ul style="list-style-type: none"> Digital Signature Act (hereinafter DSA) of March 8, 2000, amended in January 2009. In the terms of the Directive, the DSA only regulates advanced electronic signatures. Other types of electronic signatures can of course be used, but DSA does not give them additional legal power.
Finland	<ul style="list-style-type: none"> The Act on Electronic Signatures (14/2003)⁴². The Act contains provisions on electronic signatures created by means of a qualified certificate. The Act came into force on 1 February 2003. The Regulation on the Requirements for Reliability and Information Security in the Operation of Certification Authorities Providing Qualified Certificates (8/2003M)⁴³. Regulation of FICORA (Communication Regulatory Authority) on CAs' notification obligations. <p><i>A new legislation is under preparation to replace the existing Act on Electronic Signatures by September 2009. The proposal adds the concept of electronic authentication to the proposed new law. As the eSignature Act did not make any reference to electronic authentication, the use of PKI certificates for authentication has remained in a legislative "no-man's-land". The proposal intends to clarify roles, requirements and obligations for all organisations that are and will offer services for strong electronic authentication, in the same model as has been already implemented for Qualified Certificate Service Providers. Also modifications to the role, mandate and operations of the current national CA (the PRC) is proposed.</i></p>
France	<ul style="list-style-type: none"> The Loi n° 2000-230 of 13 March 2000: this law has adapted the civil rules of evidence in order to make electronic documents and signatures legally acceptable. The Law changed the articles 1316, 1316-1, 1316-2, 1316-3, 1316-4 et 1326 of the Civil Code. The Loi n° 2004-575 of 21 June 2004, called "trust in the digital economy" of which article 33 has regulated the liability of certification service providers issuing qualified digital certificates. The Décret n° 2001-272 of 30 March 2001 implementing article 1316-4 of the Civil Code (requirements for electronic signatures equivalent to handwritten signatures). The Décret n° 2002-535 of 18 April 2002 with regard to the evaluation and

⁴⁰ See http://147.29.40.91/SHOWF_B762442665/1072&B20000092205REGL&0002&000001

⁴¹ See http://147.29.40.91/SHOWF_B762442665/1072&B20000092305REGL&0003&000001

⁴² Laki sähköisistä allekirjoituksista (14/2003):

<http://www.finlex.fi/en/laki/kaannokset/2003/en20030014.pdf>

⁴³ <http://www.ficora.fi/englanti/document/FICORA082003M.pdf>

Country	Applicable regulations
	<p>certification of the security level of IT products and systems.</p> <ul style="list-style-type: none"> • The Arrêté of 28 February 2003 which installs the <i>Comité directeur de la certification en sécurité des technologies de l'information</i> • The Arrêté of 26 July 2004 with regard to the qualification of certification service providers issuing digital certificates and to the accreditation of the bodies in charge of the evaluation of CSPs. This arrêté describes the national scheme for the qualification of CSPs issuing qualified certificates as defined in article 6 of the décret 2001-272. The scheme is completed by a "a posteriori " control by the DCSSI (Direction Centrale pour la Sécurité des Systèmes d'Information), as provided by article 9 of the décret 2001-272. <p>The <i>référentiel de qualification</i> used to evaluate the CSP is composed as follows :</p> <ul style="list-style-type: none"> • Document AFNOR Z74-400 entitled "Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés", which is a French translation of the ETSI TS 101 456 (Policy requirements for certification authorities issuing qualified certificates) ; • Additional technical specifications relating to e.g. the products and systems used by CSPs and the registration procedures as defined in the arrêté of the Ministry of Economy, Finance and Industry. <p>The «référentiel » is moreover completed by the EGAP audit guide developed by the DCSSI in collaboration with the stakeholders. The guide d'audit EGAP is the instrument used by the auditor to obtain a reasonable assurance that the CSP complies with the requirements of article 6 of the décret 2001-272</p>
Germany	<ul style="list-style-type: none"> • Law on the framework for electronic signatures and for amending other provisions, of 16.05.2001 , BGBl. (Official Gazette) 2001 I No. 22, p. 876 and following pages amended by Art. 1 law of. 04.01.2005 (BGB1. 2005 I No 1, p. 2 and following pages); • Electronic signature ordinance of 16.11.2001 , BGBl. 2001 I No. 59, p. 3074 and following pages amended by Art. 2 law of 04.01.2005 (BGB1. 2005 I No. 1, p. 2 and following pages); • These regulations are supported by the Common PKI specifications, a comprehensive profile for electronic signatures, encryption and PKI using recognised standards in international use⁴⁴. This ensures that product and services from the various CSPs and software manufacturers are mutually compatible.
Greece	<ul style="list-style-type: none"> • Presidential Decree 150/2001⁴⁵ of 25 June 2001

⁴⁴ <http://www.common-pki.org/>

⁴⁵ Presidential Decree 150/2001 Transposition of Directive 99/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, GG A' 125/25.06.2001 [Προεδρικό διάταγμα υπ' αριθ. 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές, ΦΕΚ Α' 125/25.06.2001].

Country	Applicable regulations
	<ul style="list-style-type: none"> Regulation on the Provision of Electronic Signature Certification Services⁴⁶. In 2004 EETT adopted a Decision for the selection of technological solution for the implementation of the Voluntary Accreditation scheme⁴⁷. EETT also adopted several Regulations on the designation of bodies for the conformity assessment of secure-signature-creation devices and secure cryptographic modules and on the designation of bodies for the conformity assessment of certification service providers using the voluntary accreditation criteria⁴⁸, on the conformity assessment of secure signature creation devices and secure cryptographic modules⁴⁹ and on the voluntary accreditation of certification service providers⁵⁰.
Hungary	<ul style="list-style-type: none"> Act XXXV of 29 May 2001 on electronic signature⁵¹ (hereafter: Eat, amended in 2004).

⁴⁶ Decision 248/71 of the Hellenic Telecommunications & Post Commission "Regulation on the Provision of Electronic Signature Certification Services" (G.G. B' 603/16.05.2002) [Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής (ΦΕΚ Β' 603/16.05.2002)], available online at http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/LawFramework.html.

⁴⁷ Decision of the Hellenic Telecommunications & Post Commission under the Protocol No. 308/37/2004 for the selection of technological solution for the implementation of the Voluntary Accreditation scheme (G.G. B' 601/23.04.2004) [Απόφαση EETT 308/37/2004 (ΦΕΚ Β' 601/23.04.2004) για την Επιλογή τεχνολογικής λύσης για την υλοποίηση του σχήματος Εθελοντικής Διαπίστευσης των Παρόχων Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής], available online at http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/LawFramework.html.

⁴⁸ Decision of the Hellenic Telecommunications & Post Commission under the Protocol No. 295/63, Regulation on the Designation of Bodies for the Conformity Assessment of Secure-Signature-Creation Devices and Secure Cryptographic Modules and on the Designation of Bodies for the Conformity Assessment of Certification Service Providers using the Voluntary Accreditation Criteria [Κανονισμός Ορισμού Φορέων για τη Διαπίστωση Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων και Φορέων για τη Διαπίστωση Συμμόρφωσης των Παρόχων Υπηρεσιών Πιστοποίησης προς τα Κριτήρια Εθελοντικής Διαπίστευσης(295/63)], available online at http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/LawFramework.html.

⁴⁹ Decision of the Hellenic Telecommunications & Post Commission under the Protocol No. 295/64, Regulation on the Conformity Assessment of Secure Signature Creation Devices and Secure Cryptographic Modules [Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων(295/64)], available online at http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/LawFramework.html.

⁵⁰ Decision of the Hellenic Telecommunications & Post Commission under the Protocol No. 295/65, Regulation on the Voluntary Accreditation of Certification Service Providers [Κανονισμός για την Εθελοντική Διαπίστευση των Παρόχων Υπηρεσιών Πιστοποίησης(295/65)], available online at http://www.eett.gr/opencms/opencms/EETT_EN/Electronic_Communications/DigitalSignatures/LawFramework.html.

⁵¹ http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0100035.TV

Country	Applicable regulations
Iceland	<ul style="list-style-type: none"> Act No 28/2001 on electronic signatures
Ireland	<ul style="list-style-type: none"> Electronic Commerce Act 2000. There is no separate overall legal framework for the use of eSignatures in government.
Italy	<ul style="list-style-type: none"> the Code of the Digital Administration (Legislative Decree 7 March 2005, n.82) the Decree 13 January 2004 concerning the “technical rules for the creation, transmission, conservation, copying, reproduction and validation (including time validation) of the electronic documents”. CNIPA ‘Circolare’ (regulation) 15 February 2007, no. 52 (CNIPA’s supervision rules); CNIPA Deliberation 18 May 2006, no. 34 (technical rules for the definition of the profile of encrypted envelope for digital signature in XML); CNIPA ‘Circolare’ 6 September 2005, no. 48 (CNIPA’s accreditation schema); CNIPA Deliberation 17 February 2005, no. 4 (rules for recognition and verification of the e-document); Decree of the Minister for Innovation and Technologies 2 July 2004 (the content of this Decree has been in practice transposed in the Code); <i>The government recently approved new technical rules regarding the electronic signature, which have been published as Prime Ministry Decree of 30 March 2009. These rules will enter into force in December 2009. Until this time, the Prime Ministry Decree of 13 Jan 2004 will remain applicable.</i>
Latvia	<ul style="list-style-type: none"> Electronic Documents Law effective as of 1 January 2003. Its latest amendments regarding qualified certificates and trusted certification service providers effective as of 7 July 2006 were adopted due to introduction of a qualified eSignature in September 2006. Regulations of the Cabinet of Ministers No. 473 on order of elaboration, formatting, storage and circulation of electronic documents in state and municipal institutions and order of circulation of electronic documents among state and municipal institutions and natural and legal persons of 28 June 2005. <p>Definitions of an electronic signature and a qualified electronic signature in the Latvian Electronic Documents Law correspond to their definitions in the Directive. The Latvian Electronic Documents Law does not provide for an advanced electronic signature, but regulates qualified electronic signature.</p>
Liechtenstein	<ul style="list-style-type: none"> Signaturgesetz⁵² (Act on e-Signatures) of 18 September 2003 Signaturverordnung⁵³ (Ordinance to the Act on e-Signatures),

⁵² See <http://www.gesetze.li/DisplayLGBI.jsp?Jahr=2003&Nr=215>

⁵³ See <http://www.gesetze.li/DisplayLGBI.jsp?Jahr=2004&Nr=130>

Country	Applicable regulations
Lithuania	<ul style="list-style-type: none"> • Law on Electronic Signature No VIII-1822 of 11 July 2000; • Decree No 2108 of the Government of the Republic of Lithuania on the Requirements for Certification Services Providers Issuing Qualified Certificates, Requirements for Electronic Signature Equipment, Procedure of Registration of Certification Services Providers Issuing Qualified Certificates and Regulation of electronic signature Supervision as of 31 December 2002; • Decree No T-7 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Establishment of Procedure of Registration of Individuals for Issuing of Certificates and Provision of Consultation Services as of 29 January 2003; • Decree No T-10 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Establishment of Procedure of the Provision of Time-Stamp Formation Services as of 29 January 2003; • Decree No T-9 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Requirements for Accreditation of Certification Services Providers and Accreditation Procedure as of 29 January 2003; • Decree No T-8 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Requirements for Electronic Signature Verification Procedure 29 January 2003; • Decree No T-31 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on the Minimum Requirements of Civil Liability Insurance of Certification Services Providers as of 31 March 2003; • Decree No T-153 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Recommendations on the Content of Electronic Document, on the Content of Signed Electronic Document, and the Use of Electronic Document's Formats in Change of Official Electronic Documents among State Institutions when Using Electronic Means as of 7 December 2007; • Decree No T-152 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Recommendations on Change of the Activities' Regulations and Internal Activities' Orders of the Institutions, and on Organization of the Institutions when Installing eSignature, moving to Usage of Electronic Documents as of 7 December 2007; • Decree No V-12 of the Director of Lithuanian Archives Department under the Government of the Republic of Lithuania on the Rules of Management of Electronic Documents as of 11 January 2006; • Decree No V-666 of the Director of State Social Insurance Fund Board of the Republic of Lithuania under the Ministry of Social Security and Labour on Rules of Qualified eSignature of the Information of Electronic Form as of 20 December 2007

Country	Applicable regulations
	Lithuanian law relies on the concept of “secure eSignature”, which is identical to the notion of “advanced eSignature” used by the eSignatures Directive.
Luxembourg	<ul style="list-style-type: none"> • Law of 14 August 2000 relating to the ecommerce, as amended (article 1322-1 §3 of the Luxembourg Civil Code⁵⁴). • Luxembourg Regulation of 1 June 2001 on electronic signatures⁵⁵
The Netherlands	<ul style="list-style-type: none"> • Act of 8 May 2003 on electronic signatures, entered into force on May 21, 2003. This act essentially sums up all the changes in the Civil Code and the Telecommunications Act • Royal decree of 8 May 2003 defining the requirements for Certification Service Providers, entered into force on May 21, 2003. • Ministerial regulation of 6 May 2003 on electronic signatures, entered into force on May 21, 2003. • Guidelines of the Ministry of Economic Affairs on Certification Service Providers, entered into force on May 21, 2003.
Norway	<ul style="list-style-type: none"> • The Act of 15 June 2001 no. 81 on electronic signatures (the eSignature Act)⁵⁶, which is more or less a transposition (in verbatim) of the Directive on Electronic Signatures. • The Regulations of 15 June 2001 no. 611 on requirements applicable to issuance of qualified certificates etc.⁵⁷ These regulations contain inter alia a requirement that issuance of qualified certificates shall be done by personal appearance, unless it already exist a relation between the certification service provider and the holder which is based on personal appearance. • The Regulations of 21 November 2005 no. 1296 on voluntary self-declaration scheme for certification service providers.⁵⁸ These regulations set up requirements for certification service providers that want to submit a declaration, that they fulfil the requirements in the "Requirement Specification for PKI for the public sector"; i.e. Person-High, Person-Standard and Enterprise. • The Regulations of 25 June 2004 no. 988 on Electronic Communication with and within the Public Sector⁵⁹

⁵⁴ see page 3:

http://www.legilux.public.lu/leg/textescoordonnes/recueils/COMMERCE_ELECTRONIQUE/SIGNATURE_ELECTRONIQUE.pdf

⁵⁵ Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du comité «commerce électronique – see page 22 to 25
http://www.legilux.public.lu/leg/textescoordonnes/recueils/COMMERCE_ELECTRONIQUE/CADRE.pdf

⁵⁶ No. Lov 15. juni 2001 nr. 81 om elektronisk signatur (esignaturloven).

⁵⁷ No. Forskrift 15. juni 2001 nr. 611 om krav til usteder av kvalifiserte sertifikater mv.

⁵⁸ No. Forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere, §11 første ledd.

⁵⁹ No. Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Country	Applicable regulations
Malta	<ul style="list-style-type: none"> Electronic Commerce Act⁶⁰ (Chapter 426 of the Laws of Malta) which also transposes European Directive 2000/31/EC on electronic commerce. (modelled predominantly on the UNICTRAL Model law for Electronic Transactions and the EU Directives for Electronic Commerce and Electronic Signatures).
Poland	<ul style="list-style-type: none"> Act on Electronic Signature from September, 18th, 2001 (Journal of Law - Dz.U. 2001 no 130, item 1450, with subsequent amendments) Act on changes of rules concerning publication of normative acts, some another legislative acts and the act on electronic signature from July, 21th, 2006 (Journal of Law - Dz.U. 2006 no 145, item 1050) The Regulation of Ministry Council from August, 7th, 2002 on technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Journal of Law – Dz.U. 2002 no 128, item 1094). The Regulation on a template and detailed scope of application form for register entry concerning qualified certification authorities providing electronic signature certification services (Journal of Law - Dz.U. 2002 no 128, item 1097). The Regulation on maintenance of register of qualified certification authorities providing electronic signature certification services, register entries specification and detailed procedures for an entry assignment (Journal of Law - Dz.U. 2002 no 128, item 1099). The Regulation on a detailed procedure for creation and issuance of public key certificates for qualified certification authorities providing electronic signature services (Journal of Law - Dz.U. 2002 no 128, item 1101). <p>Currently there are efforts ongoing for an updated Act on Electronic Signatures and the revision of the Act on Informatisation. Among other points, this will introduce the term of advanced electronic signature; current Polish laws rely instead on the term 'secure electronic signature', corresponding roughly to an advanced signature created using an SSCD.</p>
Portugal	<ul style="list-style-type: none"> Decree-Law no. 290-D/99, of August 2 (<i>Decreto-Lei n.º 290-D/99, de 2 de Agosto</i>) Decree-Law no. 62/2003, of April 3 (<i>Decreto-Lei n.º 62/2003, de 3 de Agosto</i>) Implementing Decree no. 25/2004, of 15 July, that regulates the referred Decree-Law no. 62/2003, comprising, namely, technical and security standards applicable to certifying entities established in Portugal as regards the issue of qualified certificates intended for the general public.
Romania	<ul style="list-style-type: none"> Law no. 455 of 2001 regarding the Electronic Signature ("Law no. 455"), which sets the legal status of the electronic signatures and electronic documents, as well as the conditions for certification service providers' activity in the electronic signature field;

⁶⁰ http://docs.justice.gov.mt/lom/legislation/english/leg/vol_13/chapt426.pdf

Country	Applicable regulations
	<ul style="list-style-type: none"> • Government Decision no. 1259 of 2001 on the Approval of the Technical and Methodological Norms for the Application of Law no. 455 of 2001 Regarding the Electronic Signature (“Application Norms of Law no. 455”); • <i>Decision no. 31 of 2008 issued by the ANCOM President regarding the Procedure of the Accreditation of the Certification Service Providers.</i>
Slovakia	<ul style="list-style-type: none"> • Act of 15 March 2002 on electronic signature and on amendment of some acts as amended⁶¹ • <i>Ordinance of the National Security Authority of 26 March 2009 No. 131/2009 Coll. on the format, content and administration of the certificates and qualified certificate and on the format, periodicity and manner of issuing the qualified certificate revocation list (on certificates and qualified certificates);</i> • <i>Ordinance of the National Security Authority of 26 March 2009 No. 132/2009 Coll. on the conditions for providing accredited certification services and on the requirements for audit, the scope of audit and qualification of auditors;</i> • <i>Ordinance of the National Security Authority of 26 March 2009 No. 133/2009 Coll. on the content and scope of operating documentation administered by a certification authority and on the security rules and rules for performing certification activities;</i> • <i>Ordinance of the National Security Authority of 26 March 2009 No. 134/2009 Coll. laying down details on the requirements for secure-time-stamping devices and the requirements for electronic signature products (on electronic signature products);</i> • <i>Ordinance of the National Security Authority of 26 March 2009 No. 135/2009 Coll. on the format and manner of creating a qualified electronic signature, the manner of issuing the Authority’s public key, the verification procedure and verification conditions of a qualified electronic signature, time stamp format and the manner of time stamping, requirements for the source of time data and requirements for holding documentation on time stamps (on the creation and verification of an electronic signature and time stamp);</i> • <i>Ordinance of the National Security Authority of 26 March 2009 No. 136/2009 Coll. on the manner and procedure of using an electronic signature in commercial and administrative intercourse.</i> <p>Slovak legislation defines only the electronic signature based on asymmetric cryptography (digital signature) and does not define the technologically neutral electronic signature according to Art. 2.1 of the Directive. The eSignature Act did not literally translate the definitions of advanced and “qualified” electronic signature of the European Directive: the advanced electronic signature according to the Directive was transposed into the Slovak legal system as an “electronic signature” (Art. 3 of eSignature Act) and the qualified electronic signature according to Art. 5.1 of Directive was transposed into the Slovak legal system as “guaranteed electronic signature (zaručený elektronický podpis - ZEP)” (Art. 4 eSignature Act).</p> <p><i>The amendment of eSignature Law that entered in force from 1st January 2009 introduced the so called mandate’s certificates (certificates for the people with special position, such as judges, notaries, advocats, solicitors etc.). The mandate’s certificate allows to determine the legal capacity in which a person is</i></p>

⁶¹ Zákon č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov), for an English translation of eSignature Law see http://www.nbusr.sk/NBU_SEP/leg_rozne/215_2002AJ.pdf.

Country	Applicable regulations
	<p><i>signing a document. The legal capacity (as a representative of a company, as a public official, judge, notary, lawyer, solicitor etc.) has to be verified during the registration process by certification services provider. The law introduced also the obligation of certification holder or the company or organisation that represents to notify to the CSP any change of his legal capacity and subsequently to apply for revocation of the mandate's certificate.</i></p> <p><i>An obligation was also introduced to state a birth number in qualified certificates that will be used in contact with public state administrative bodies, and an obligation of all public state administrative bodies to notify to the National Security Authority an address of e-registry, where they receive a electronic submission signed by e-signature.</i></p> <p><i>With regard to the long term validity of the signatures the eSignature Law regulates the so called archive electronic signature and the accredited certification service of the CSPs called long term storage of electronic documents signed by electronic signature (this additional service was introduced by amendment of eSignature Act being in force since 1st January 2009).</i></p>
Slovenia	<ul style="list-style-type: none"> • The Electronic Commerce and Electronic Signature Act (hereinafter ECESA) as a horizontal bill regulating e-commerce in a broad sense applies also to administrative, judicial and other similar procedures unless otherwise provided by another law. It provides the legal basis for using e-signatures, digital certificates and developing e-services in Slovenia (Official Gazette of the RS, No. 73/2004-ZN-C, 98/2004 - official consolidated text, 61/2006-ZEPT). • The Decree on Conditions for Electronic Commerce and Electronic Signing (Official Gazette of the Republic of Slovenia, No. 77/2000, 2/2001, 86/2006) defining in detail individual conditions from the act, prescribing special, rigorous conditions regarding Certification Authorities, who issue qualified certificates (compulsory liability insurance, special requirements regarding equipment and employees, exacting procedures, internal regulations, etc.). • Rules on official registration procedure for certification authorities register of the Republic of Slovenia (Official Gazette of the RS, No. 99/2001, 42/2007). • The General Administrative Procedure Act (Official Gazette of the Republic of Slovenia, No. /2006 - official consolidated text, 105/2006-ZUS-1, 126/2007, 65/2008), provides the general legal basis for all administrative proceedings; i.e. all Administration to Citizen (A2C) and Administration to Business (A2B) together with a major part of Administration to Administration (A2A) relations. Among the main provisions of the Act is one allowing for a two-way and full electronic communication between Public Administration and citizens. Prior to entering this text into force, citizens could post their eDocuments through the eServices of the eGovernment state portal by using the web application and digital signature; the answer from the administration could be expressed by regular mail only. In 2004 and in later amendments, this Act legalised what is qualified as "eDelivery". • The legal basis for the introduction of electronic signatures and authentication in eGovernment applications for administrative operations can be found in the Decree on administrative operations (Official Gazette of the Republic of Slovenia, No. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 122/2007, 31/2008, 35/2009) (available at http://zakonodaja.gov.si/rpsi/r02/predpis_URED3602.html, in Slovenian only). According to the decree the e-government application for citizens and private sector can be performed by any qualified certificates issued by

Country	Applicable regulations
Spain	<p>registered Certificate service providers, governmental CAs and other commercial certification authorities.</p> <ul style="list-style-type: none"> • eSignature Law⁶² of 2003 (<i>Ley 59/2003 de 19 de Diciembre, de firma electrónica</i>). • Royal Decree 1553/2005, of 23 December, ruling the expedition of the national identity document and its electronic signature certificate⁶³ (from now on, RD 1553/2005 on eID card) established, the framework of the electronic identity document, following the eSignature Law guidelines. • Law 11/2007 of electronic access promotes the use of ICTs in the relationships between Public Administrations and citizens, thus improving the services and reducing the digital breach, and establishes 31 December 2009 as limit term for all the State public administrations to render all their services electronically⁶⁴. <p>Among others, it guarantees the following rights to the citizens:</p> <ul style="list-style-type: none"> - Free choice of communication channel with the public administrations. - No need to provide data/information that the Administration already has, or if necessary, the possibility of presenting it in electronic format. - To follow up, by electronic means, the current situation of the procedures/files in which they are implied. - To get electronic copies of official documents.
Sweden	<ul style="list-style-type: none"> • the Act on Qualified Electronic Signatures (Sw: Lag (2000:832) om kvalificerade elektroniska signaturer)⁶⁵ applies to certificate providers established in Sweden and who issue qualified certificates to the public. • the Government Ordinance on Qualified Electronic Signatures (Sw: Förordning (2000:833) om kvalificerade elektroniska signaturer), in which the National Post and Telecom Agency is appointed supervisory authority. • the Government Ordinance on the financing of the National Post and Telecom's operations (Sw: Förordning (2003:398) om finansiering av Post- och telestyrelsens verksamhet), in which the fees for Certificate Providers issuing qualified certificates are regulated. • Post and Telecom Agency's regulations on fees (Sw: Post- och telestyrelsens föreskrifter om avgifter; PTSFS 2008:3), which stipulates fees

⁶² "Ley 59/2003 de 19 de Diciembre, de firma electrónica". Text of the Law, available at http://www.060.es/te_ayudamos_a/legislacion/disposiciones/28147-ides-idweb.html

⁶³ "Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica" available at http://www.060.es/te_ayudamos_a/legislacion/disposiciones/34023-ides-idweb.html

⁶⁴ List of transactions fully adapted to Law 11/2007 of electronic access (on-line transactions) at http://www.060.es/guia_del_estado/programas_de_la_administracion/administracion_electronica/LAECSP_11_2007/common/Anexo_I.pdf; and transactions only partially adapted (information, downloading and forms delivery) at http://www.060.es/guia_del_estado/programas_de_la_administracion/administracion_electronica/LAECSP_11_2007/common/Anexo_II.pdf

⁶⁵ Available in English at <http://www.pts.se/en-gb/Industry/Internet/Electronic-signatures/>

Country	Applicable regulations
	<p>for certificate providers falling under the Act on Qualified Electronic Signatures.⁶⁶</p> <ul style="list-style-type: none"> • The Technical Conformity Assessment Act (Sw: Lag (1992:1119) om teknisk kontroll), which provides a voluntary accreditation scheme for accreditation of certification bodies.
United Kingdom	<ul style="list-style-type: none"> • Electronic Communications Act 2000, which came into force on 25th May 2000, consisting of three parts: <ul style="list-style-type: none"> ○ part 1 concerns Certificate Service Providers and details the arrangements for registering providers of cryptography support services, such as electronic signature services and confidentiality services. However, the Government said that they would not commence this part of the act preferring to see the industry-led initiative, tScheme, carry out this function. On 25th May 2005, being the fifth anniversary of the day on which the Act was passed, having continued to be satisfied that tScheme meets the Government's objectives, part 1 effectively was repealed; ○ part 2 makes provision for the legal recognition of electronic signatures and the process under which they may be generated, communicated or verified. It will also facilitate the use of electronic communications or electronic storage of information, as an alternative to traditional means of communication or storage; ○ part 3 amends sections 12 and 46B of the Telecommunications Act 1984 and inserts a new section 12A into that Act. The new provisions are concerned with the modification of telecommunication licences otherwise than in pursuance of a reference to the Competition Commission. This Part also concerns matters such as general interpretation, the short title, commencement and territorial extent of this Act. ○ The Electronic Signatures Regulations 2002, which came into force on 8 March 2002, these include provisions relating to the supervision of certification service providers, their liability in certain circumstances and data protection requirements concerning them. They also transpose verbatim Annexes I and II of the Directive to enable the meaning of the term "qualified certificate" to be understood as it is used in these Regulations.
Turkey	<ul style="list-style-type: none"> • The Electronic Signature Act was published in the Official Gazette dated 15 January 2004 and entered into force in 23 July 2004. By virtue of this Act, Information and Communication Technologies Authority is given the duty of preparing and publishing secondary legislations and supervision of electronic certificate service providers. • Ordinance on Certificate Financial Liability Insurance" was published in Official Gazette No.25565 dated 26 August 2004, "Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law" and "Communiqué on Processes and Technical Criteria Regarding Electronic Signatures" were published in Official Gazette No.

⁶⁶ Available in Swedish at <http://www.pts.se/sv/Dokument/Foreskrifter/Avgifter/PTSFS-20083---PTS-foreskrifter-om-avgifter/>

Country	Applicable regulations
	<p>25692 dated 06.01.2005. Finally, "Schedule and Instructions on Certificate Financial Liability" was prepared by the Undersecretariat of Treasury in regard with the "Ordinance on Certificate Financial Liability Insurance" and published in Official Gazette No. 25709 dated 27 January 2005. All these regulations entered into force at the date of publications. Consequently, legal basis to electronic signatures has been established in Turkey.</p> <p>The Turkish Electronic Law does not make a distinction as qualified electronic signature and advanced electronic signature⁶⁷; but it merely puts legal emphasis on secure electronic signatures based on qualified electronic certificates.⁶⁸ As a consequence of this emphasis, it is merely the electronic documents signed by secure electronic signatures that will have the same legal effect as the written documents that are signed on paper; and it is clearly set forth as a legal interpretation that only the electronic documents signed by secure electronic signatures have the power of proof in terms of evidence law and will be deemed as conclusive proof until otherwise is proved.</p>

On the basis of the table above, some noteworthy trends can be identified.

Firstly, it is clear that the legal framework for electronic signatures has reached a stage of maturity. Out of 32 countries, 26 made no noteworthy changes to their applicable laws. Of the six countries that did report specific changes, three related to organisational matters (changes in supervision/accreditation schemes in Croatia, Cyprus and Romania), and one to the updating of technical requirements (Italy). More extensive updates were seen in Austria and in Slovakia:

- The 2008 regulatory reforms in Austria aimed to align Austrian law more closely with the Directive, including the introduction of the concept of advanced electronic signatures (which was not used in the prior version of the law), and the clarification that formal confirmation requirements of technical components by a designated body are limited to the SSCD (and not to the technical environment as a whole). The commonly used term "qualified electronic signature" was also taken up in the official act, whereas previously the term "secure electronic signature" had been used. In addition, the Austrian law now notes that legal persons can also be considered signatories, although this is not the case for qualified signatures, as qualified certificates can only be issued to natural persons. This particular issue will be examined further in the sections below.

⁶⁷ Keser Berber, Leyla/Beceni, Yasin/Sevim, Tuğrul ; The Improvement and Consequence Report of National Coordination Commission's Working Group on Electronic Signature Law, Istanbul 2005, http://bthukuku.bilgi.edu.tr/documents/e-imza_hukuk_calisma_grubu_raporu.pdf.

⁶⁸ The secure electronic signature is defined in Article 4 of Electronic Signature Law as follows:
"ARTICLE 4. — Secure Electronic Signature is an electronic signature, which;
a) exclusively belongs to the signatory,
b) is created only by means of secure electronic signature creation device that is under the exclusive disposal of the signatory,
c) enables the identification of the signatory based upon qualified electronic signature
d) enables the determination as to whether any subsequent alteration has been made in the electronic data that is signed". This definition is a mixed definition including the requirements attached to advanced electronic signature by virtue of Article 5/1 of EU 99/93/EC Directive. For detailed information please see Keser Berber/ Beceni/ Sevim, a.g.e.

- In Slovakia, a large number of Ordinances was passed in March 2009, aiming to update the legal framework and to ensure its comprehensiveness. These included ordinances on the format, content and administration of the certificates, qualified certificates, qualified certificate revocation lists, timestamps and qualified electronic signatures; on the conditions for providing accredited certification services and on the requirements for audit, the scope of audit and qualification of auditors; on the requirements for secure-time-stamping devices and the requirements for electronic signature products; on the verification procedure and verification conditions of a qualified electronic signature; and finally on the manner and procedure of using an electronic signature in commercial and administrative intercourse. Thus, the Slovakian framework now covers all relevant aspects of eSignature processes.

It is also interesting to note that there is still some divergence between the concepts used by these different regulatory frameworks. While Austria has replaced the concept of a secure electronic signature with the more universally understood concept of a qualified signature, some other examples of terminological or real differences remain:

- Bulgarian law (the Electronic Documents and Electronic Signatures Act, EDESA) uses a definition of electronic signatures that corresponds substantially to the meaning of 'advanced electronic signature' under the Directive. The EDESA provides an alternative definition of the 'advanced electronic signature', which is in fact similar to that of the so-called qualified electronic signature. Finally, the EDESA introduced the concept of a universal electronic signature (UES), a type of advanced electronic signature (in the sense of the Directive) which is supported by a qualified certificate issued by a CSP registered in Bulgaria. The UES is the only type of electronic signature which has the effect of a handwritten signature in respect to everyone under Bulgarian law, unlike the basic and the advanced electronic signature which have such an effect only between private persons. In practice the UES is commonly required for the eGovernment needs. The UES is thus a uniquely Bulgarian concept.
- In the context of Croatian law, the advanced electronic signature is defined as being based on a qualified certificate.
- French law relies on a specific and comprehensive reference framework, rather than on the concept of qualified certificates/signatures. French CSPs can choose to be evaluated against the requirements of the "Référentiel Intersectoriel de Sécurité" (RGS), part of which was previously called PRIS (Politique de Référencement InterSectorielle, version 2). The RGS aims to define requirements applying to a series of security functions in information systems. It is mandatory for public agencies and for their service providers. Three levels of security are defined for each service: middle (*), strong/standard (**) and strengthened (***). CSPs/CAs may make use of this qualification among public or private application promoters, thus ensuring that the reference framework acts as a voluntary accreditation scheme. To be referenced, the CSP must be first be qualified for a service and for a security level, and secondly the certificate profile must be compliant with the one defined to ensure the interoperability with all online services requiring such type of certificates. The certificates issued for signature purposes at high signature*** level allow a signature to be obtained that is presumed to be reliable, within the scope of the eSignatures Directive, corresponding to the European ETSI and CEN standards which technically reflect the requirements of the European Directive on electronic signatures.
- Lithuanian law relies on the concept of the 'secure eSignature', which is identical to the notion of "advanced eSignature" used by the eSignatures Directive.
- Polish law is currently under revision. Among other points, it is being considered to introduce the term of advanced electronic signature, in the same sense as defined in the Directive. Current Polish law instead relies on the term 'secure electronic signature', corresponding

roughly to an advanced signature created using an SSCD. Separate from this initiative, current draft regulations with regard to the planned Polish eID card envisage that the card will support so-called 'personal signatures', a new concept to be introduced. As personal signatures are currently planned to be considered legally equivalent to hand written signatures, the European equivalent term would appear to be a qualified signature.

- Finally, Slovak law defines only the electronic signature based on asymmetric cryptography (digital signature) and does not define the technologically neutral electronic signature as defined in Art. 2.1 of the Directive. The advanced electronic signature according to the Directive was transposed into the Slovak legal system as an "electronic signature" (much as in Bulgaria) and the qualified electronic signature according to Art. 5.1 of Directive was transposed into the Slovak legal system as "guaranteed electronic signature (zaručený elektronický podpis - ZEP)".

Thus, there are some substantial and interesting terminological disparities in national legislations, with the concept of 'secure electronic signature' being an interesting example. This term is not defined at the European level, and thus has no clear European standing. None the less, it used to be a part of Austrian law where it related to a qualified signature. It still exists in Poland, where it corresponds roughly to an advanced signature created using an SSCD, and in Lithuania, where it is synonymous with an advanced electronic signature. While a purely terminological issue, one might see how the introduction of new categories of signatures on a national basis holds a risk of creating market confusion.

A third point of interest is the diverging scope of existing electronic signature laws at the national level. While the majority of countries have adopted the most straightforward approach of creating an eSignatures Act that transposes the Directive and thus governs electronic signatures, some other noteworthy approaches can be identified.

- Firstly, some countries have opted not to address the issue of electronic signatures in isolation, but have instead considered that it would be advisable to place this in a broader framework of certification services regulations. The aforementioned example of the recently revised Slovakian regulatory framework is a case in point, with other examples including the German, Estonian and Czech legal framework (all of which include provisions in relation to e.g. timestamping, in the German and Czech case even defining qualified timestamping). The Slovak regulatory framework in addition contains provisions for an archive electronic signature and an accreditation for long term electronic document storage. Finally, the reforms also created so called mandate certificates (certificates for the people with special position, such as judges, notaries, advocats, solicitors etc.). The mandate certificate allows to determine the legal capacity in which a person is signing a document. The law introduced also the obligation of certification holder or the company or organisation that represents to notify to the CSP any change of his legal capacity and subsequently to apply for revocation of the mandate's certificate. An obligation was also introduced to state a birth number in qualified certificates that will be used in contact with public state administrative bodies. Thus, issues of identity management have also been addressed to some extent by these reforms. The same can be seen in Finland, where ongoing regulatory reforms envisage establishing a legal framework for electronic (entity) authentication, noting that the use of PKI certificates for authentication has remained in a legislative "no-man's-land". The proposal intends to clarify roles, requirements and obligations for all organisations that are and will offer services for strong electronic authentication, in the same model as has been already implemented for Qualified Certificate Service Providers. Other countries like Italy can similarly look back on a long tradition of regulation supported by clear technical standards, including in relation to e.g. electronic registered mail.

- Other countries have not considered electronic signatures in a strict PKI context, but rather as a part of a broader spectrum of issues such as electronic documents, eGovernment or e-commerce. Examples of this include the Irish and Maltese transpositions of the eSignatures Directive via their respective Electronic Commerce Acts, the Slovenian Electronic Commerce and Electronic Signature Act, and the UK Electronic Communications Act 2000. In the cases of Bulgaria, Croatia and Latvia, an Electronic Documents law was created containing the relevant provisions.
- Finally, a number of countries have considered it unnecessary to create a signatures act that explicitly addresses all types of electronic signatures defined in the Directive, based on the consideration that existing laws were already interpreted in a broad enough fashion to recognise the legal value of electronic signatures in their basic form. This is seen e.g. in Denmark, where the eSignatures Act covers only signatures based on qualified certificates (and thus not the OCES signature commonly used in Danish eGovernment applications), or the Estonian law which regulates advanced electronic signatures in general and establishes their equivalence to handwritten signatures without specific provisions in relation to qualified signatures. The aforementioned Latvian Electronic Documents law similarly defines an electronic signature and a qualified electronic signature, but not an advanced electronic signature. Slovak legislation defines only the electronic signature based on asymmetric cryptography (digital signature) and does not define the technologically neutral electronic signature.

The different approaches to transposing the Directive each have their own advantages, but also offer some drawbacks. The strategy chosen by the first group discussed above (which have introduced regulations also in relation to time stamping, long term archiving, electronic registered mail, identity management and authorisations) seems to indicate that there is a certain normative gap to be filled, in the sense that each of these services would require a legal framework to ensure their trustworthiness to end users. On the other hand, the fact that these initiatives are taken at a strictly national level means that there is a risk of disparities emerging in the European market. It may be worth examining whether further European guidance in these areas would be necessary to stop such disparities from disrupting the internal market.

4.2.2 Regulatory eSignature requirements

The sections above examined the general regulatory framework for electronic signatures. In this subsection, we will take a closer look at some specific legal questions in relation to eSignatures, most notably:

- Whether there is a specific framework for the use of electronic signatures in a public sector context;
- Whether there is a specific framework for the use of electronic signatures by public administrations;
- How the notion of qualified certificate is interpreted, and specifically whether qualified certificates can be issued to legal persons and whether they require personal appearance of the recipient;
- Which entity has been designated as the supervisory body and/or accreditation body in each country.

4.2.2.1 eSignatures in an eGovernment context

The table below will present a summary for each country of any main regulations in relation specifically to the use of eSignatures in an eGovernment context. The main scope of these regulations will be described, where known.

Country	Applicable regulations
Austria	<ul style="list-style-type: none"> • The E-Government Act defined so-called “administrative signatures” for a transition period until end of 2007. Administrative signatures had relaxed requirements compared to qualified signatures and were introduced to facilitate take-up.
Belgium	<ul style="list-style-type: none"> • No specific rules apply
Bulgaria	<ul style="list-style-type: none"> • The new eGovernance legal framework unifies the requirements concerning the provision of eGovernment services and the use of electronic signatures for the purposes of the eGovernment. It includes the Electronic Governance Act (<i>Закон за електронното управление, EGA</i>)⁶⁹, five secondary acts for its implementation and a tariff for the taxes for the accreditation of the information system certification organizations. This legislation is applicable both on central and regional level and respectively treat the central bodies and the bodies of the local self-governance equally. EGA provides the possibility for the addressees of eGovernment services to make electronic statements and to send them electronically. The submitted documents must be issued and signed in accordance with the requirements of the EDESA. The recipients of electronic administrative services and the authors of

⁶⁹ Valid as of 13 June 2008, see http://www.mdaar.government.bg/docs/ZEU_BG.pdf (available only in Bulgarian)

Country	Applicable regulations
	<p>electronic statements in accordance with EGA shall identify themselves by using their unique identifier, except in cases where a law allows the use of a specific administrative service without identification. The integrity and the authorship of electronically submitted statements relevant to electronic administrative services must be established with an electronic signature, created in accordance with EDESA and observing all other legislative requirements. The use of electronic signature is not required for services which are available without identification of their recipient.</p> <ul style="list-style-type: none"> Pursuant to EGA and EDESA the state and municipal authorities are not only obliged to accept electronic documents signed with UES and submitted electronically but also to issue official administrative documents in electronic form if such documents are requested by citizen or representative of a legal entity. These documents also must be signed with UES. In this respect and in accordance with the requirements of EGA the Council of Ministers adopted special ordinance which regulates the rules and the policies for the acquiring, the use, the renewal and the termination of the electronic signature certificates in the administrations (Ordinance for the Electronic Signature Certificates in the Administrations⁷⁰, <i>Наредба за удостоверенията за електронен подпис в администрациите</i>, OESCA).
Croatia	<ul style="list-style-type: none"> “General Administrative Procedures Act” of March 2009 (Zakon o općem upravnom postupku, NN 47/08)⁷¹. This Act enables a framework for official and legally valid communication of citizens and businesses with the administration by electronic means. The General Administrative Procedures Act gives all involved parties the possibility to communicate electronically with the public administration. All electronic documents have to be signed with an advanced electronic signature. This law will come into force on January 1, 2010. The Regulation on Office Transactions (Uredba o uredskom poslovanju⁷²). The Regulation stipulates the definition of a standardized project on electronic business transactions to be defined until end of January 2010. The Law on the Electronic Document (Zakon o elektroničkoj ispravi⁷³, NN 150/05). The Law defines the complete lifecycle of an electronic document. It defines that the electronic document consists of two parts that are inseparable. One part is the part with one or more electronic signatures. The concept electronic signature means the advanced electronic signature.
Cyprus	<ul style="list-style-type: none"> No specific rules apply
Czech Republic	<ul style="list-style-type: none"> eGovernment act (Act on electronic procedures and authorized conversion of the documents 300/2008 Coll. – <i>Zákon č. 300/2008 Sb., o elektronických</i>

⁷⁰ Valid as of 13 June 2008, see <http://www.mdaar.government.bg/docs/3A%20УДОСТОВЕРЕНИЯТА%20ЗА%20ЕЛЕКТРОНЕН%20ПОДПИС%20В%20АДМИНИСТРАЦИИТЕ.pdf> (available only in Bulgarian)

⁷¹ *Zakon o općem upravnom postupku*; http://narodne-novine.nn.hr/clanci/sluzbeni/2009_04_47_1065.html

⁷² *Uredba o uredskom poslovanju*; http://narodne-novine.nn.hr/clanci/sluzbeni/2009_01_7_171.html

⁷³ *Zakon o elektroničkom dokumentu*; in English <http://www.e-hrvatska.hr/sdu/en/Zakonodavstvo/RH.html>

Country	Applicable regulations
	<p><i>úkoněch a autorizované konverzi dokumentů</i>) was approved in August 2008 and will come into effect on 1st July 2009, Act on the Basic Registres 111/2009 Coll. (<i>Zákon č. 111/2009 Sb., o základních registrech</i>) was adopted on 26th March 2009 and will come into effect on 1st July 2010, the new Act on ID cards 328/1999 Coll. (<i>Zákon č. 328/1999 Sb., o občanských průkazech</i>) is in the draft phase.</p> <ul style="list-style-type: none"> • The act on e-signature states that in the public sector an advanced electronic signature based on a qualified certificate issued by an accredited CSP⁷⁴ must be used. • For the communication with the public administration the certificate has to contain a social security number. It is in the SubjectAlternativeName – Other Name and its OID is 1.3.6.1.4.1.11801.2.1. This identifier is stored in the information system of the state social assistance managed by the Ministry of Labour and Social Affairs (http://portal.mpsv.cz/soc/ssp).
Denmark	<ul style="list-style-type: none"> • The right to use electronic signatures follows from a general right to use electronic documents. In 2002-2005 a large “law modernising project”⁷⁵ was carried out by the government to ensure that formal requirements do not hinder the use of electronic documents except from the few situations where it has been considered necessary to require paper documents⁷⁶. In addition to these changes of more specific provisions a new provision, § 32a, was inserted in the Administrative Act (<i>forvaltningsloven</i>)⁷⁷. § 32a made it possible through administrative decrees to change rules on formal requirements if such rules were a barrier to the use of electronic communication. In this way it became possible to eliminate the legal barriers in a faster and more flexible way not having to go through the parliamentary process of adopting new legislation. In other words this provision allows easy adaptation of the existing legal framework.
Estonia	<ul style="list-style-type: none"> • The Digital Signature Act (DSA) states that the public sector must accept digitally signed documents.
Finland	<ul style="list-style-type: none"> • Act on Electronic Services and Communication in the Public Sector (13/2003)⁷⁸
France	<ul style="list-style-type: none"> • The Ordonnance n°2005-1516 of 8 December 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ». • Decree n° 2007-284 of 2 March 2007 defining the modalities of elaboration,

⁷⁴ A list of accredited CSPs can be found at <http://www.mvcr.cz/mvcren/article/scope-of-activities-egovernment-electronic-signature.aspx?q=Y2hudW09Mw%3d%3d>

⁷⁵ See http://www.e.gov.dk/offentlige_projekter/lovmodernisering/index.html (in Danish)

⁷⁶ The project was initiated base on recommendations given in report no. 1400, “e-signatur og formkrav i lovgivningen” drafted by a committee appointed by the Ministry of Justice.

⁷⁷ Act no. 571 of 19 December 1985. Available in Danish from <http://147.29.40.91/_SHOWF_A393870761/311&A20020105030REGL&0001&000001>

⁷⁸ Laki sähköisestä asiointista viranomaistoiminnassa (13/2003): <http://www.finlex.fi/en/laki/kaannokset/2003/en20030013.pdf>

Country	Applicable regulations
	<p>modification and publication of the Interoperability general frame of reference⁷⁹</p> <ul style="list-style-type: none"> • Circular of 12 September 2003 on the development of electronic administration www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=PRMX0306850C <p>The Ordonnance states inter alia:</p> <ul style="list-style-type: none"> • Article 2 : “An administrative authority may respond electronically to any request for information sent to it by that means by a user or by any other administrative authority.” • Article 3 : “When a user has forwarded a request or information electronically to an administrative authority and an acknowledgment of receipt has been given according to Article 5-I, that administrative authority is duly entered and deals with the request or information without asking the user for confirmation or to resend it in another format. A decree of the Council of State lays down cases in which an exception may be made to this rule, owing to special requirements of form or procedure.” • Article 4 : “The administrative authorities may set up teleservices, pursuant to the provisions of the aforesaid Law of 6 January 1978 and the rules on security and interoperability laid down in chapters IV and V of this Ordonnance. When they set up such a service, the administrative authorities make the decision on its creation and its procedures for use, particularly the possible means of communication, accessible from the latter. These procedures are compulsory for users.” • Article 5 : “Any request, declaration or production of documents sent by a user to an administrative authority electronically and any payment made within the scope of a teleservice shall be the object of an electronic acknowledgment of receipt and, when this is not immediate, an electronic acknowledgment of entry. This acknowledgment of receipt and this acknowledgment of entry are issued according to a process complying with the rules laid down by the general security reference system mentioned in Article 9 -I(...). • Article 8 : “The documents of administrative authorities may be the object of electronic signature, which may only be validly affixed by the use of a process complying with the rules of the general security reference system mentioned in Article 9-I, which allows the identification of the signatory, guarantees the link between the signature and the document to which it is affixed and ensures the integrity of that document.” • Article 9 : “I. A general security reference system lays down the rules that must be observed by the functions of the information systems contributing to the security of information exchanged electronically such as identification, electronic signature, confidentiality and time stamping functions. The conditions of preparation, approval, modification and publication of this reference system shall be laid down by decree.

⁷⁹ J.O. of 3 March 2007

Country	Applicable regulations
	<ul style="list-style-type: none"> Article 10 : “Electronic certificate issued to the administrative authorities and to their agents with a view to ensuring their identification within the scope of an information system shall be validated by the State under conditions laid down by decree.”
Germany	<p>Several sector specific regulations apply, including:</p> <ul style="list-style-type: none"> Act on the Amendment of Formal Regulations under Private Law and other Regulations governing modern Legal Transactions (FormAnpG) of 13.07.2001, BGBl 2001 I No. 35, p 1542 and following pages. FormAnpG introduces the electronic format as an optional written form. That means that according to section 126a of the German Civil Code the qualified electronic signature can be used instead of the handwritten signature in legal relations, with certain granted exceptions. Second Law amending the tax regulations (Tax Amendment Act 2003 – StÄndG 2003) Law on the use of electronic forms of communication in the judicial system (JKomG - Justice and Communication Act) of 22.03.2005, BGBl I No. 18, p. 837 and following pages. Third amendment of the Ordinance on the Award of Public Contracts (VgV) and Adjustment of Contract Terms for Freelance Services (VOF); in force since 1.11.2006 ID Card Act (Personalausweisgesetz, to be published soon) Draft citizens portal act (“Bürgerportalgesetz”), passed federal cabinet on 4 February 2009, service to start from 2010
Greece	<p>The Presidential Decree 342/2002⁸⁰ describes the use of electronic communication for administrative purposes. It provides that decisions and certificates can be communicated through e-mail from public services, legal persons of public law or organizations of local administration to private or legal persons, provided that they bear a digital signature.</p>
Hungary	<ul style="list-style-type: none"> Act CXL. of 2004 on the general rules of public administrative procedures and services (2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól hereafter: Ket) and its enacting Decrees⁸¹ regulate the use of e-Signature in the Hungarian public administration. It is a requirement of Ket for the electronic administration, that the electronic documents shall be signed at least with advanced electronic signature⁸²; however it is not necessary in the case of submission through the Client Gate. Ket gives the legal framework of electronic administration and public administrative services in Chapter X. Articles 160-169.

⁸⁰ Presidential Decree 342/2002 (GG A' 284/22.11.2002) [Προεδρικό Διάταγμα 342/2002 (ΦΕΚ Α' 284/22.11.2002)].

⁸¹ http://net.iogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400140.TV

⁸² The certification authority should use face to face registration, etc. See later and the Gov. Decree 193 of 2005.

Country	Applicable regulations
	<ul style="list-style-type: none"> • Several government and ministerial decrees, government decisions insure the execution of Eat and Ket. <ul style="list-style-type: none"> – On the detailed rules of the scope of duties, competence and the rules of procedure of the National Communication Authority in connection with the electronic signature (Government decree 151 of 1. September 2001 amended by decree 45 of 11. March 2005.) – On the detailed rules of electronic administration. (Government decree 193 of 22 September 2005) – On the electronic signature used in public administration procedures and the certificates thereof, and the requirements for certification service providers issuing the certificates. (Government decree 194 of 22. September 2005.) – On the certificatory bodies for electronic signature products and the rules for the designation of these bodies (Decree of the Minister leading the Prime Minister`s Office, (hereafter MeHVM) No 15 of 27 August 2001 amended by the decree of the Minister of Informatics and Communications (IHM) No 9 of 21 July 2005) – On the detailed requirements for electronic signature services and service providers, (Decree of MeHVM No 16 of 1 September 2001 amended by the decree of the IHM No 3 of 18 March 2005) – On the registration of electronic signature service experts (decree of MeHVM No 7 of 26 April 2002) – On the security, interoperability and uniform use of IT systems in electronic administration (Government decree 195 of 22. September 2005.) – On the detailed technical rules for documents in electronic administration (Decree of IHM 12 of 27. October 2005.)
Iceland	<ul style="list-style-type: none"> • On 10 March 2003 an amendment (No. 51/2003)⁸³ was approved to the Public Administration Act, No. 37/1993⁸⁴, adding a special chapter on the electronic handling of matters by public administration. Through this modification, general obstacles to the development of electronic administration were removed. Article 38 in the act states: <i>“When established law, custom or general administrative provisions require material from a party or government authority to be signed, the authority may determine that electronic signatures can serve in place of handwritten signatures, insofar as electronic signatures assure, in a similar degree to handwritten signatures, the personal confirmation of the one from whom the material originates. A qualified electronic signature, according to the Act on electronic signatures, shall always be considered to fulfil the legal requirements on signatures.</i> <p><i>When established law, custom or general administrative provisions require material or certain aspects of it to be certified, this requirement shall be</i></p>

⁸³ <http://www.althingi.is/altext/128/s/1158.html>

⁸⁴ <http://eng.forsaetisraduneyti.is/acts-of-law/nr/17>

Country	Applicable regulations
	<p><i>considered to be fulfilled through certification by an electronic signature that conforms with the first paragraph above and confirms the aspects for which certification is demanded.</i></p> <p><i>When established law, custom or general administrative provisions do not require material from a party or government authority to be signed, the authority may determine that it is permissible to use means other than electronic signatures in order to confirm electronic material.”</i></p>
Ireland	<ul style="list-style-type: none"> No specific rules apply.
Italy	<ul style="list-style-type: none"> the Code of the digital administration plays a central role. The Code requires that the electronic document must be signed with a qualified electronic signature ('firma elettronica qualificata') or a digital signature ('firma digitale'). The 'digital signature' means a special type of qualified electronic signature based on a system of related cryptographic keys (one of them private and one public), ensuring its owner (through the private key) and the receiver (through the public key), to make the origin and the integrity of an electronic document clear and to verify such origin and integrity; it is therefore a type of qualified signature (with extra requirements). pursuant to Article 64(1) of the Code, the EIC and the national service card (see below) are the instruments to guarantee access to online services provided by public authorities when user authentication is required. The access to those services can happen in a transitory phase (actually until 31th December 2008, but this deadline was postponed) also through other ways of user identification and authentication on a local basis; but the access through EIC must always be guaranteed in the whole country by all public authorities that provide online services. Furthermore, pursuant to Article 65, all requests and declarations sent to public authorities are valid if: <ul style="list-style-type: none"> They are signed with a digital signature whose certificate has been issued by an accredited certification-service-provider; When the user is identified and authenticated through the use of the EIC or the national service card; In the transitory phase, when the user is identified and authenticated through other systems adopted at the local level; the Legislative Decree of 1 July 2009 n.78 - art. 17(28) – has amended the Code Art.65(1) adding a letter c-bis meaning to allow authentications based on the use of registered electronic email (the so called Citizen Certified Email, where the creation of the email account follows a de visu identification)⁸⁵.
Latvia	<ul style="list-style-type: none"> No specific rules apply
Liechtenstein	<ul style="list-style-type: none"> No specific rules apply

⁸⁵ Information kindly provided by M. Adriano Rossi of the CNIPA after the finalization of the Italian country profile.

Country	Applicable regulations
Lithuania	<ul style="list-style-type: none"> • Code of Administrative Law Violations No VIII-588 of 23 December 1997; • Decree No 2115 of the Government of the Republic of Lithuania on Position Paper on eGovernment as of 31 December 2002; • Decree No T-153 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Recommendations on the Content of Electronic Document, on the Content of Signed Electronic Document, and the Use of Electronic Document's Formats in Change of Official Electronic Documents among State Institutions when Using Electronic Means as of 7 December 2007; • Decree No T-152 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Recommendations on Change of the Activities' Regulations and Internal Activities' Orders of the Institutions, and on Organization of the Institutions when Installing eSignature, moving to Usage of Electronic Documents as of 7 December 2007; • Decree No V-12 of the Director of Lithuanian Archives Department under the Government of the Republic of Lithuania on the Rules of Management of Electronic Documents as of 11 January 2006; • Decree No V-666 of the Director of State Social Insurance Fund Board of the Republic of Lithuania under the Ministry of Social Security and Labour on Rules of Qualified eSignature of the Information of Electronic Form as of 20 December 2007 <p>The Law does not mention any specific requirements for the use of electronic signatures in the public sector. However, specific vertical (sector specific) regulations exist.</p>
Luxembourg	<ul style="list-style-type: none"> • Law of 20 April 2009 creating the "Information Technologies Center of the State" (ITCS)⁸⁶ (though not specifically focused on electronic signatures)
Malta	<ul style="list-style-type: none"> • No specific rules apply
The Netherlands	<p>The basic provisions for governmental use of electronic means of communication can be found in the 2004 Act on electronic governmental communication. The general principles of this Act are⁸⁷:</p> <ul style="list-style-type: none"> • Electronic messages qualify as 'written', thereby explicitly opening up the possibility of electronic service delivery between government, citizens and businesses. Only in cases where specific laws require a service to be delivered conventionally, electronic service delivery is forbidden. • Electronic communication is a full fledged additional alternative to conventional communication, but does not replace it. Governmental organisations must remain accessible by conventional means and cannot force citizens to use electronic means of communication. • Both citizen and governmental organisations must each determine their availability by electronic means of communication, and must make this

⁸⁶ See <http://www.legilux.public.lu/leg/a/archives/2009/0081/a081.pdf#page=2>

⁸⁷ <http://www.e-overheid.nl/thema/juridisch/webv/webv.xml>

Country	Applicable regulations
	<p>known.</p> <ul style="list-style-type: none"> The security norm is set at 'sufficiently reliable and confidential'. This sufficiency is determined by the nature and content of the electronic message, as well as by the purpose for which it is used.
Norway	<ul style="list-style-type: none"> The Regulations of 25 June 2004 no. 988 on Electronic Communication with and within the Public Sector⁸⁸
Poland	<ul style="list-style-type: none"> The Act on Electronic Signature contains the obligation for public authorities to enable the users of certification services to apply and communicate in an electronic form. The due date for this Regulation is stated as August, 16th, 2006, but was delayed to May, 1th, 2008 („Act on changes of rules concerning publication of normative acts, some other legislative acts and the act on electronic signature” from July, 21th, 2006). The fundamental condition enabling to submit applications and requests or to perform another activities via electronic means is a publication of relevant information by appropriate organs (e.g. the way electronic documents are received, form templates in XML format) and implementations of some necessary mechanisms (e.g. electronic delivery boxes, official confirmations of electronic documents' reception). Technical requirements for forms and templates accessibility are defined in the Regulation of the Minister of Interior and Administration from July, 24th, 2007, „on requirements concerning accessibility of forms and templates for electronic documents (Journal of Law - Dz. U. no 151, item 1078).
Portugal	<ul style="list-style-type: none"> Decree-Law no. 62/2003 contains one provision that is directly applicable to e-Government: Article 5 states as follows: <ul style="list-style-type: none"> Public bodies may issue electronic documents bearing a qualified electronic signature placed pursuant to the provisions of the Decree-Law no. 62/2003 (meaning advanced electronic signatures) and the Decree-Law no.116-A/2006, of June 16, Regarding operations that concern the creation, issue, storage, reproduction, copying and transfer of electronic documents, which formalize administrative acts through computer systems, including the transmission thereof by telecommunications means, the data relating to the interested body and the person who carried out each administrative act may indicate in readily identifiable language and in such a manner that it may confirm the functions or position of each document's signatory.
Romania	<ul style="list-style-type: none"> Law no. 161 of 2003 regarding Certain Measures for Ensuring the Transparency in the Exercising of Public Positions, Public Offices and the Business Environment, Prevention and Punishment of Corruption. The law notes that all the documents sent and received by using the electronic procedure must have an electronic form and must be signed electronically under the terms established by the operator of the eGovernment system, i.e. the Agency for Information Society Services (in Romanian Agentia pentru Serviciile Societatii Informatinale, “ASSI”).

⁸⁸ No. Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Country	Applicable regulations
Slovakia	<ul style="list-style-type: none"> No specific additional rules apply, due to the comprehensive nature of the general legal framework.
Slovenia	<ul style="list-style-type: none"> Decree on administrative operations (Official Gazette of the Republic of Slovenia, No. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 122/2007, 31/2008, 35/2009). According to the decree the e-government application for citizens and private sector can be performed by any qualified certificates issued by registered Certificate service providers, governmental CAs and other commercial certification authorities. The General Administrative Procedure Act (Official Gazette of the Republic of Slovenia, No. /2006 - official consolidated text, 105/2006-ZUS-1, 126/2007, 65/2008), provides the general legal basis for all administrative proceedings; i.e. all Administration to Citizen (A2C) and Administration to Business (A2B) together with a major part of Administration to Administration (A2A) relations. Among the main provisions of the Act is one allowing for a two-way and full electronic communication between Public Administration and citizens. Prior to entering this text into force, citizens could post their eDocuments through the eServices of the eGovernment state portal by using the web application and digital signature; the answer from the administration could be expressed by regular mail only. In 2004 and in later amendments, this Act legalised what is qualified as “eDelivery”.
Spain	<ul style="list-style-type: none"> Law 11/2007 of electronic access promotes the use of ICTs in the relationships between Public Administrations and citizens, thus improving the services and reducing the digital breach, and establishes 31 December 2009 as limit term for all the State public administrations to render all their services electronically⁸⁹. <p>Among others, it guarantees the following rights to the citizens:</p> <ul style="list-style-type: none"> Free choice of communication channel with the public administrations. No need to provide data/information that the Administration already has, or if necessary, the possibility of presenting it in electronic format. To follow up, by electronic means, the current situation of the procedures/files in which they are implied. To get electronic copies of official documents.
Sweden	<ul style="list-style-type: none"> No specific rules apply
United Kingdom	<ul style="list-style-type: none"> No specific rules apply
Turkey	<ul style="list-style-type: none"> No specific rules apply

Analysis of this overview will be included below the following section, dealing with eSignature use by public administrations.

⁸⁹ List of transactions fully adapted to Law 11/2007 of electronic access (on-line transactions) at http://www.060.es/guia_del_estado/programas_de_la_administracion/administracion_electronica/LAECSP_11_2007/common/Anexo_I.pdf; and transactions only partially adapted (information, downloading and forms delivery) at http://www.060.es/guia_del_estado/programas_de_la_administracion/administracion_electronica/LAECSP_11_2007/common/Anexo_II.pdf

4.2.2.2 eSignature use by public administrations

The table below will present a summary for each country of any main regulations in relation specifically to the use of eSignatures by public administrations. The main scope of these regulations will be described, where known.

Country	Applicable regulations
Austria	<ul style="list-style-type: none"> • So-called “official signatures” have been defined in the E-Government Act. Official signatures are indicated by an attribute in the certificate (an object identifier). They serve to facilitate recognition of the fact that a document originates from an authority. The official signature is represented in the electronic version of the document by an image which the authority has published on the Internet.
Belgium	<ul style="list-style-type: none"> • No specific rules apply
Bulgaria	<ul style="list-style-type: none"> • Pursuant to EGA and EDESA the state and municipal authorities are not only obliged to accept electronic documents signed with UES and submitted electronically but also to issue official administrative documents in electronic form if such documents are requested by citizen or representative of a legal entity. These documents also must be signed with UES. In this respect and in accordance with the requirements of EGA the Council of Ministers adopted special ordinance which regulates the rules and the policies for the acquiring, the use, the renewal and the termination of the electronic signature certificates in the administrations (Ordinance for the Electronic Signature Certificates in the Administrations⁹⁰, <i>Наредба за удостоверенията за електронен подпис в администрациите</i>, OESCA).
Croatia	<ul style="list-style-type: none"> • A new “Regulation on Office Transactions” (Uredba o uredskom poslovanju, NN 7/09)⁹¹ was adopted in early 2009. The Regulation regulates in art. 75 that a standardized project for electronic office transactions will be defined by the heads of the central state bodies responsible for general administration and the implementation of information technology.
Cyprus	<ul style="list-style-type: none"> • No specific rules apply
Czech Republic	<ul style="list-style-type: none"> • No specific rules apply (beyond those noted above)
Denmark	<ul style="list-style-type: none"> • No specific rules, given the already flexible general legal framework
Estonia	<ul style="list-style-type: none"> • No specific rules apply

⁹⁰ Valid as of 13 June 2008, see

<http://www.mdaar.government.bg/docs/3A%20УДОСТОВЕРЕНИЯТА%20ЗА%20ЕЛЕКТРОНЕН%20ПОДПИС%20В%20АДМИНИСТРАЦИИТЕ.pdf> (available only in Bulgarian)

⁹¹ *Uredba o uredskom poslovanju*; http://narodne-novine.nn.hr/clanci/sluzbeni/2009_01_7_171.html

Country	Applicable regulations
Finland	<ul style="list-style-type: none"> No specific rules apply
France	<ul style="list-style-type: none"> The Ordonnance n°2005-1516 of 8 December 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ». Decree n° 2007-284 of 2 March 2007 defining the modalities of elaboration, modification and publication of the Interoperability general frame of reference⁹² Circular of 12 September 2003 on the development of electronic administration www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=PRMX0306850C <p>The Ordonnance states inter alia:</p> <ul style="list-style-type: none"> Article 2 : “An administrative authority may respond electronically to any request for information sent to it by that means by a user or by any other administrative authority.” Article 5 : “Any request, declaration or production of documents sent by a user to an administrative authority electronically and any payment made within the scope of a teleservice shall be the object of an electronic acknowledgment of receipt and, when this is not immediate, an electronic acknowledgment of entry. This acknowledgment of receipt and this acknowledgment of entry are issued according to a process complying with the rules laid down by the general security reference system mentioned in Article 9 -I(...). Article 8 : “The documents of administrative authorities may be the object of electronic signature, which may only be validly affixed by the use of a process complying with the rules of the general security reference system mentioned in Article 9-I, which allows the identification of the signatory, guarantees the link between the signature and the document to which it is affixed and ensures the integrity of that document.” Article 9 : “I. A general security reference system lays down the rules that must be observed by the functions of the information systems contributing to the security of information exchanged electronically such as identification, electronic signature, confidentiality and time stamping functions. The conditions of preparation, approval, modification and publication of this reference system shall be laid down by decree. Article 10 : “Electronic certificate issued to the administrative authorities and to their agents with a view to ensuring their identification within the scope of an information system shall be validated by the State under conditions laid down by decree.”
Germany	<ul style="list-style-type: none"> No specific rules apply

⁹² J.O. of 3 March 2007

Country	Applicable regulations
Greece	<ul style="list-style-type: none"> No specific rules apply
Hungary	<ul style="list-style-type: none"> No specific rules apply
Iceland	<ul style="list-style-type: none"> On 10 March 2003 an amendment (No. 51/2003)⁹³ was approved to the Public Administration Act, No. 37/1993⁹⁴, adding a special chapter on the electronic handling of matters by public administration. Through this modification, general obstacles to the development of electronic administration were removed. Article 38 in the act states: <i>“When established law, custom or general administrative provisions require material from a party or government authority to be signed, the authority may determine that electronic signatures can serve in place of handwritten signatures, insofar as electronic signatures assure, in a similar degree to handwritten signatures, the personal confirmation of the one from whom the material originates. A qualified electronic signature, according to the Act on electronic signatures, shall always be considered to fulfil the legal requirements on signatures.</i> <p><i>When established law, custom or general administrative provisions require material or certain aspects of it to be certified, this requirement shall be considered to be fulfilled through certification by an electronic signature that conforms with the first paragraph above and confirms the aspects for which certification is demanded.</i></p> <p><i>When established law, custom or general administrative provisions do not require material from a party or government authority to be signed, the authority may determine that it is permissible to use means other than electronic signatures in order to confirm electronic material.”</i></p>
Ireland	<ul style="list-style-type: none"> No specific rules apply
Italy	<ul style="list-style-type: none"> The Digital Administration Code contains several articles that encourage the use of electronic documents and their electronic transmission e.g. Art. 40 (Production of Electronic Documents – i.e. document digitally signed), 45 (Legal Value of the Transmission), 47 (Transmission of Documents by E-Mail among Public Administrations) and 48 (Certified Electronic Mail i.e. electronic registered email).
Latvia	<ul style="list-style-type: none"> No specific rules apply
Liechtenstein	<ul style="list-style-type: none"> No specific rules apply
Lithuania	<ul style="list-style-type: none"> Code of Administrative Law Violations No VIII-588 of 23 December 1997;

⁹³ <http://www.althingi.is/altext/128/s/1158.html>

⁹⁴ <http://eng.forsaetisraduneyti.is/acts-of-law/nr/17>

Country	Applicable regulations
	<ul style="list-style-type: none"> • Decree No 2115 of the Government of the Republic of Lithuania on Position Paper on eGovernment as of 31 December 2002; • Decree No T-153 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Recommendations on the Content of Electronic Document, on the Content of Signed Electronic Document, and the Use of Electronic Document's Formats in Change of Official Electronic Documents among State Institutions when Using Electronic Means as of 7 December 2007; • Decree No T-152 of the Director of Information Society Development Committee under the Government of the Republic of Lithuania on Recommendations on Change of the Activities' Regulations and Internal Activities' Orders of the Institutions, and on Organization of the Institutions when Installing eSignature, moving to Usage of Electronic Documents as of 7 December 2007; • Decree No V-12 of the Director of Lithuanian Archives Department under the Government of the Republic of Lithuania on the Rules of Management of Electronic Documents as of 11 January 2006; • Decree No V-666 of the Director of State Social Insurance Fund Board of the Republic of Lithuania under the Ministry of Social Security and Labour on Rules of Qualified eSignature of the Information of Electronic Form as of 20 December 2007
Luxembourg	<ul style="list-style-type: none"> • No specific rules apply
Malta	<ul style="list-style-type: none"> • No specific rules apply
The Netherlands	<p>As noted above, the basic provisions for governmental use of electronic means of communication can be found in the 2004 Act on electronic governmental communication, and include notably the following key points:</p> <ul style="list-style-type: none"> • Electronic communication is a full fledged additional alternative to conventional communication, but does not replace it. Governmental organisations must remain accessible by conventional means and cannot force citizens to use electronic means of communication. • Both citizen and governmental organisations must each determine their availability by electronic means of communication, and must make this known.
Norway	<ul style="list-style-type: none"> • The Regulations of 25 June 2004 no. 988 on Electronic Communication with and within the Public Sector⁹⁵
Poland	<p>The Act on informatisation makes it legally allowable:</p> <ol style="list-style-type: none"> (a) to address petitions and applications to public authorities in the form of an electronic document, including documents supplied with qualified electronic signatures, (b) an electronic information exchange with public authorities confirmed by

⁹⁵ No. Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Country	Applicable regulations
	<p>both communication parties with electronic signatures,</p> <ul style="list-style-type: none"> (c) a storage of archive electronic materials in state archives, taking into account the provision of their integrity and longterm validity, (d) an electronic documents' transfer with data concerning ZUS (<i>Social Insurance Institution</i>) insurance contribution payers, supplied with a qualified electronic signature by persons responsible for this, (e) to publish normative acts and some other legislative acts in the form of electronic documents; the contents of an electronic document includes the confirmation of accordance with original and documents have to be supplied with secure electronic signature created by responsible signing entity.
Portugal	<ul style="list-style-type: none"> • Decree-Law no. 62/2003 contains one provision that is directly applicable to e-Governmen: Article 5 states as follows: <ul style="list-style-type: none"> ○ Public bodies may issue electronic documents bearing a qualified electronic signature placed pursuant to the provisions of the Decree-Law no. 62/2003 (meaning advanced electronic signatures) and the Decree-Law no.116-A/2006, of June 16, ○ Regarding operations that concern the creation, issue, storage, reproduction, copying and transfer of electronic documents, which formalize administrative acts through computer systems, including the transmission thereof by telecommunications means, the data relating to the interested body and the person who carried out each administrative act may indicate in readily identifiable language and in such a manner that it may confirm the functions or position of each document's signatory.
Romania	<ul style="list-style-type: none"> • No specific rules apply
Slovakia	<ul style="list-style-type: none"> • No specific additional rules apply, due to the comprehensive nature of the general legal framework.
Slovenia	<ul style="list-style-type: none"> • The General Administrative Procedure Act (Official Gazette of the Republic of Slovenia, No. /2006 - official consolidated text, 105/2006-ZUS-1, 126/2007, 65/2008), provides the general legal basis for all administrative proceedings; i.e. all Administration to Citizen (A2C) and Administration to Business (A2B) together with a major part of Administration to Administration (A2A) relations. Among the main provisions of the Act is one allowing for a two-way and full electronic communication between Public Administration and citizens. Prior to entering this text into force, citizens could post their eDocuments through the eServices of the eGovernment state portal by using the web application and digital signature; the answer from the administration could be expressed by regular mail only. In 2004 and in later amendments, this Act legalised what is qualified as "eDelivery". • The legal basis for the introduction of electronic signatures and authentication in eGovernment applications for administrative operations can be found in the Decree on administrative operations (Official Gazette of the Republic of Slovenia, No. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 122/2007, 31/2008, 35/2009) (available at http://zakonodaja.gov.si/rpsi/r02/predpis_URED3602.html, in Slovenian only). According to the decree the e-government application for citizens and private sector can be performed by any qualified certificates issued by

Country	Applicable regulations
	registered Certificate service providers, governmental CAs and other commercial certification authorities.
Spain	<ul style="list-style-type: none"> No specific rules apply.
Sweden	<ul style="list-style-type: none"> No specific rules apply
United Kingdom	<ul style="list-style-type: none"> No specific rules apply
Turkey	<ul style="list-style-type: none"> No specific rules apply

Examining the two sections above, it is clear that the different surveyed countries have taken different approaches to regulating the use of electronic signatures in their countries. It is interesting to examine these in a bit more detail, since they provide insights into potential interoperability barriers, but also into the drivers that are created to encourage the use of electronic signatures in public services.

A first group of countries has not defined general eGovernment eSignature rules (i.e. rules defining which signatures should be used in eGovernment applications, or which signatures should be used by public administrations. These countries include notably Belgium, Cyprus, Denmark, Ireland, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Slovakia, Sweden, the UK and Turkey (13/32 countries, 41%). Of course, this should not be taken to mean that eSignatures are not used in eGovernment applications, or that eSignature use is not encouraged. Rather, it can be indicative of many possible choices. In some countries, such as e.g. Denmark or Ireland, the general legal framework is considered to be flexible enough to enable electronic communication with the government without any additional rules (above and beyond the aforementioned general eSignatures framework) being required. In other countries such as Slovakia, the general legal framework is already so comprehensive that more specific rules are not generally needed. Finally, in some countries a strongly vertical approach is favoured, in which specific rules are created on a sector/application specific basis, without universal rules that apply to all eGovernment services.

Other countries have established specific eGovernment acts (generally designated as eGovernment Acts, Electronic Administration Acts, Electronic Communication in the Public Sector Act, etc). These countries include Austria, Bulgaria, Iceland, Finland, France, Hungary, Norway, Poland, Slovenia, and the Netherlands, with similar legislation about to enter into force in Croatia and the Czech Republic (12/32 countries, 37,5%). The precise scope and impact of these laws varies quite strongly, but the following broad categories of goals supported by the regulations can be identified:

- The most obvious and largest group consists of regulations that grant the citizens and/or businesses the right to communicate electronically with public administrations, and which clarify the modalities of doing so (i.e. a framework for C2A and/or B2A communication). Such rules exist in Bulgaria, Croatia, the Czech Republic, Estonia, France, Hungary, Italy, Poland, Romania, Slovenia, Spain and the Netherlands (12/32 countries, 37,5%). It should be noted that this list contains some countries which have not adopted an eGovernment Act, and this right is then enshrined in separate regulations. E.g. in Estonia and the Czech Republic, the right to use electronic signatures in communications with the government is directly integrated into the eSignatures Act.

- A second group has implemented regulations addressing the reverse possibility: the right of public administrations to use electronic signatures in their communications with businesses and citizens (A2B and A2C). This group is noticeably smaller, and includes Austria, Greece, France, Iceland, Portugal, Slovenia and Spain (7/32, 22%).
- A third group has integrated specific incentives for the use of electronic signatures in communication with the public sector, i.e. they have implemented rules that not only *permit* the use of electronic signatures in eGovernment services but that *encourage* such use. This includes countries which have included a right to reply to an electronically signed communication (Bulgaria), and the right to access electronic copies (Spain).

Some of the key examples and their relevant lessons will be examined in greater detail below.

- **Austria:** so-called “official signatures” have been defined in the E-Government Act. Official signatures are identified by an attribute in the certificate (an object identifier). They serve to facilitate recognition of the fact that a document originates from an authority. The official signature is represented in the electronic version of the document by an image which the authority has published on the Internet. Thus, the status of an official signature can be validated both automatically and manually based on the visual information on the graphical representation of the document.
- **Bulgaria:** under the eGovernment and eSignatures/eDocuments Acts, state and municipal authorities are not only obliged to accept electronic documents signed with UES and submitted electronically, but also to issue official administrative documents in electronic form if such documents are requested by citizen or representative of a legal entity. These documents also must be signed with UES. Thus, end users have the right to receive an electronic response, if they request one.
- **France:** an Ordinance (*Ordonnance n° 2005-1516 of 8 December 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives »*) governs the communication between end users and administrative authorities in detail, including :
 - The right of administrative authorities to respond electronically to any request for information sent to it by electronic means (A2A, A2B and A2C)
 - The obligation of an administrative authority to send an electronic acknowledgement of receipt in response to any request, declaration or production of documents sent by a user.
 - The right of administrative authorities to apply electronic signatures to electronic documents, in accordance with the rules of the general security reference system established in France.

Thus, the French legal framework provides a good set of encouragements to the use of electronic communications, including specifically an obligation to acknowledge electronic messages.

- **Hungary:** the Hungarian so-called Ket Act (Act CXL. of 2004 on the general rules of public administrative procedures and services (2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól) and its enacting Decrees are similarly comprehensive with respect to the use of e-Signatures in the Hungarian public administration.

The Ket requires that electronic documents should in principle⁹⁶ be signed at least with advanced electronic signature.

- **Iceland:** unlike the Hungarian and French approach, which are both supported by a comprehensive series of technical standards, the Icelandic Public Administration Act No. 37/1993 takes a generic and principles based approach. Article 38 in the act states: “When established law, custom or general administrative provisions require material from a party or government authority to be signed, the authority may determine that electronic signatures can serve in place of handwritten signatures, insofar as electronic signatures assure, in a similar degree to handwritten signatures, the personal confirmation of the one from whom the material originates. A qualified electronic signature, according to the Act on electronic signatures, shall always be considered to fulfil the legal requirements on signatures.” Thus, the Icelandic approach allows a greater deal of flexibility, but also more margin of appreciation since the acceptance of electronic signatures must be judged on a case by case basis.
- **Poland:** the Polish Act on informatisation contains similar broad communication rights, including the right:
 - to address petitions and applications to public authorities in the form of an electronic document, including documents supplied with qualified electronic signatures,
 - to engage an electronic information exchange with public authorities confirmed by both communication parties with electronic signatures,
 - to publish normative acts and some other legislative acts in the form of electronic documents; the contents of an electronic document includes the confirmation of accordance with original and documents have to be supplied with secure electronic signature created by responsible signing entity.
- **Spain:** the Spanish Law 11/2007 contains the ambitious objective of setting 31 December 2009 as limit term for all the State public administrations to render all their services electronically. Among others, it guarantees the following rights to the citizens:
 - Free choice of communication channel with the public administrations.
 - No need to provide data/information that the Administration already has, or if necessary, the possibility of presenting it in electronic format.
 - To follow up, by electronic means, the current situation of the procedures/files in which they are implied.
 - To get electronic copies of official documents.Thus, the Spanish law contains an obligation for systematic informatisation, along with free choice of communications channel and access rights.
- **The Netherlands:** the 2004 Act on electronic governmental communication contains a number of important principles, including:
 - Electronic messages qualify as ‘written’, thereby explicitly opening up the possibility of electronic service delivery between government, citizens and businesses. Only in cases where specific laws require a service to be delivered conventionally, electronic service delivery is forbidden.
 - Electronic communication is a full fledged additional alternative to conventional communication, but does not replace it. Governmental organisations must remain

⁹⁶ With the exception of electronic documents submitted through the Hungarian eGovernment portal, the Client Gate, where this requirement does not exist.

accessible by conventional means and cannot force citizens to use electronic means of communication.

- Both citizen and governmental organisations must each determine their availability by electronic means of communication, and must make this known.
- The security norm is set at 'sufficiently reliable and confidential'. This sufficiency is determined by the nature and content of the electronic message, as well as by the purpose for which it is used.

Thus, the Dutch law stresses the important of being able to choose an appropriate communications channel, and of transparently communicating the availability of such channels.

The list above shows that several good examples can be identified that either permit or encourage the use of electronic signatures, including by introducing a right of acknowledgement (France), a right to a response (Bulgaria), a right to choose the desired communications channel (Spain and the Netherlands), and a right to access electronic documents (Spain), or simply by facilitating the validation of the official status of a public sector communication (the Austrian official signature).

None the less, some examples could also be noted in which provisions were introduced with a clear view of facilitating national interoperability (i.e. information exchange between services within a country and/or improving the quality of service, which may none the less result in interoperability barriers at the European level. Examples of this include:

- **Bulgaria:** The Bulgarian eGovernment Act provides the possibility for the addressees of eGovernment services to make electronic statements and to send them electronically. Pursuant to Bulgaria law the state and municipal authorities are not only obliged to accept electronic documents signed with a universal electronic signature (UES) and submitted electronically but also to issue official administrative documents in electronic form if such documents are requested by citizen or representative of a legal entity. These documents also must be signed with UES. As was noted above however, the UES is a type of advanced electronic signature which is supported by a qualified certificate issued by a CSP registered in Bulgaria. Thus, non-Bulgarian signatures typically will not qualify for this status. Given that the UES is commonly required in eGovernment applications, this may be a legal interoperability barrier.
- **Czech Republic:** the eSignatures Act states that in the public sector an advanced electronic signature based on a qualified certificate issued by an accredited CSP must be used. For the communication with the public administration the certificate has to contain a social security number. This identifier is stored in the information system of the state social assistance managed by the Ministry of Labour and Social Affairs. Obviously, foreign certificates will not contain a social security number, meaning that foreign signature solutions will generally not be able to meet this requirement.

It should be stressed that the approaches above all serve the legitimate purpose of ensuring the reliability of electronic signatures being used (in all three countries), and of being able to easily identify the signatory in an automated fashion that allows the development of advanced eGovernment services (in the Czech Republic, where the social security number enables this).

In addition, it should be pointed out that these situations in which national solutions are strongly favoured or even supported exclusively are not at all exceptional. The reason that the examples above are mentioned is that their general eGovernment laws are more explicit in this respect. In many other countries (e.g. those using eID cards as listed above) the situation is highly similar: a national means of

identification is distributed that supports eSignature functionality, and future eGovernment applications are then developed with this specific solution in mind (or even explicitly limited to this solution, as we will see in the application analysis section below), thus excluding interoperability with other solutions.

These restrictions appear to be applications of Article 3.7 of the eSignatures Directive (the so-called public sector clause), which allows Member States to “make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.” Given the considerations above, it seems that some countries have not respected the last restriction in the eGovernment/eSignature regulations.

4.2.2.3 Qualified certificates

It is clear that qualified certificates were considered to be one of the key building blocks of trustworthiness under the eSignatures Directive. They are subject to national supervision regimes (see section 4.2.2.3.), which means that they enjoy a favoured position from an interoperability perspective: as a result of this supervision, the recipient of a signature based on a qualified certificate has at least some rudimentary guarantees with regard to the qualities of the certificate itself.

None the less, the notion of qualified certificates is interpreted in different ways. The Directive notes that a qualified certificate must meet the specific requirements indicated in Annex I, i.e. it must contain:

- (a) an indication that the certificate is issued as a qualified certificate;
- (b) the identification of the certification-service-provider and the State in which it is established;
- (c) the name of the signatory or a pseudonym, which shall be identified as such;
- (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
- (f) an indication of the beginning and end of the period of validity of the certificate;
- (g) the identity code of the certificate;
- (h) the advanced electronic signature of the certification-service-provider issuing it;
- (i) limitations on the scope of use of the certificate, if applicable; and
- (j) limits on the value of transactions for which the certificate can be used, if applicable.

In contrast, the notion of ‘certificate’ in general is simply defined as “an electronic attestation which links signature-verification data to a person and confirms the identity of that person”. A key difference between the notions is the fact that a certificate is linked to a *person*, whereas the qualified certificate refers to the *signatory*. The notion of a person is not defined in the Directive, but due to its frequent references in several provisions to ‘legal or natural persons’, it is generally accepted that this concept covers legal persons (most notably companies) as well. In contrast, the notion of signatory is defined in Article 2.3 as “a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents.” This has caused much debate as to

whether a qualified certificate can be issued to legal persons and whether they require personal appearance of the recipient.

The table below provides an overview of the interpretation of the Directive on both questions.

Country	For legal persons (without identifying the natural person who holds the certificate)?	Personal appearance required?
Austria	No	Yes ⁹⁷
Belgium	No	Yes
Bulgaria	No	Yes
Croatia	No	Yes
Cyprus	No	Yes
Czech Republic	No ⁹⁸	Yes
Denmark	No	Yes ⁹⁹

⁹⁷ As a general rule, the eSignature Law requires physical presence for issuing qualified certificates, although this is not required when the signature in the application form was drafted before a Public Notary; or the identity and other circumstances of the applicant are known by the certification service provider (CSP) due to a pre-existing relationship; or when a new certificate request is made presenting a valid prior one.

⁹⁸ While qualified certificate can only be issued to natural persons, the act on e-signatures also establishes a “qualified system certificate”, which can be issued to legal entities and can be used in automatically signing systems. The digital signature based on a qualified system certificate is called an “electronic mark”. A qualified certificate and qualified system certificate can be issued to any person (qualified system certificate also to a legal entity), including persons from another country.

⁹⁹ No qualified electronic certificates are being offered by certification service providers in Denmark. One of the main obstacles has precisely been the requirement for signature holders to meet up and identify themselves in person. Realising that few people would do this the Government initiated the establishment of the above mentioned OCES standard. The OCES signature is a “light version” of the qualified electronic signature with the important difference that the holder of an OCES signature does not have to perform face to face identification.

Country	For legal persons (without identifying the natural person who holds the certificate)?	Personal appearance required?
Estonia	Yes (digital stamping; see below)	Yes ¹⁰⁰
Finland	No	Yes
France	No ¹⁰¹	Yes
Germany	No	Yes
Greece	No	Yes
Hungary	No	Yes
Iceland	No	Yes
Ireland	No	Yes
Italy	No	Yes
Latvia	No	Yes
Liechtenstein	No	Yes
Lithuania	No	Yes
Luxembourg	No	Yes
Malta	No	Yes

¹⁰⁰ More accurately, the Estonian Digital Signatures Act does not explicitly require personal appearance of the certificate applicant but puts the burden of accurate identification of a certificate holder to the issuer. However, in practice issuance of ID-card and Mobile-ID both require physical appearance

¹⁰¹ In France, in order to be qualified, the CSPs are evaluated against the requirements of the "Référentiel Intersectoriel de Sécurité" (RGS). The last version has been released in October 2008 after a series of public consultations. It should be approved by Decree by the end of 2009. The RGS aims at defining requirements applying to a series of security function in information systems. It is mandatory for public agencies and for their service providers. The RGS defines 3 services for certificates : authentication, signature and confidentiality. These certificates can be delivered to natural persons acting for themselves (individual) acting for their company (Enterprise) or their administration (administration). The RGS recommends one certificate for one usage. Three levels of security are defined for each service: middle (*), strong/standard (**) and strengthened (***). The RGS is available at: <http://www.references.modernisation.gouv.fr/rgs-securite>

Country	For legal persons (without identifying the natural person who holds the certificate)?	Personal appearance required?
The Netherlands	No	Yes
Norway	No	Yes
Poland	No	Yes
Portugal	No	Yes
Romania	Yes	Yes ¹⁰²
Slovakia	No	Yes
Slovenia	No	Yes ¹⁰³
Spain	No	Yes ¹⁰⁴
Sweden	No	Yes
United Kingdom	No	Yes
Turkey	No	Yes

For the interpretation of these figures, it should be pointed out that the overview above also indicates a 'No' for countries in which there are no CSPs issuing qualified certificates at all (such as e.g. Denmark and Ireland); however, it is possible that the situation will change in these countries if CSPs begin issuing qualified certificates there, meaning that the problem of the interpretation of the Directive would present itself in those countries as well.

When examining the 32 country reports, five appeared to be issuing qualified certificates directly to enterprises (Hungary, Latvia, Portugal, Romania and Spain). However, discussions with the national experts for each of these countries showed that the correct interpretation of the status of qualified signatures for legal persons in a given country can be quite complex, due to the fact that many commercial CSPs issue qualified certificates to natural persons who are entitled to represent a legal entity in some respect. When the qualified certificate itself identifies the legal entity (by name, company number or otherwise) and this certificate is thereafter used to create signatures on behalf of the

¹⁰² Physical presence of the users is needed, and their identification can only be performed based on official identification documents.

¹⁰³ Physical presence is only required for the first issuing of a qualified certificate; not for subsequent prolongations.

¹⁰⁴ As a general rule, the eSignature Law requires physical presence for issuing qualified certificates, although it is not required when: the signature in the application form was drafted before a Public Notary; or the identity and other circumstances of the applicant are known by the certification service provider (CSP) due to a pre-existing relationship (E.g. this could be presenting a DNle); or when a new certificate request is made presenting a valid prior one; in such a case, the CSP will check that the 4 years validity term has not expired yet.

company, the qualified certificate is easily and commonly misrepresented as being 'issued to a legal entity', when in fact it was issued to a natural person who is mandated to represent that legal entity.

During discussions with the national experts, the representatives of Spain, Hungary and Latvia noted that the aforementioned situation (qualified certificates being issued to a specific natural person authorised to act on behalf of a legal person) was in fact applicable in their respective countries:

- With respect to Spain, it was noted that the certificate is always issued to a physical person acting as the legal representative of the legal person, after due corroboration of the legal powers and mandates that enable that physical person to act on behalf of the company. Thereafter, the certificate can only be used to represent the legal person, which is the reason why it is labelled as a legal person certificate. Therefore, in addition to the identity data of the legal representative of the company, the certificate also includes the name and legal data of the company that the former is representing. Thus, while the certificate is labelled a legal person certificate in Spain, a natural person is still identified as the holder.
- A similar situation was noted to exist in Latvia: the holder of the certificate is not the legal person itself, but a natural person authorised to represent the legal person.
- In Hungary, this was confirmed to also be the case, noting however that the requirement to identify a natural person in the certificate was only known to exist in interactions with the public sector. In B2B or other private transactions on the other hand, it was not clear whether a natural person was always identified in the certificate itself. However, even if this would not be the case, the CSP should always be able to identify the natural person behind each certificate, so that a link between the certificate and the individual always existed.

No comments from the remaining two countries (Romania and Portugal) were received during or after the workshop; however, given the clarifications offered by the representatives from other Member States, it seems likely that the discussion is largely semantic, and that qualified certificates which are said to be issued to legal persons are in fact issued to natural persons authorised to act on behalf of legal persons.

In contrast, the Estonian expert noted that qualified certificates were issued directly to legal persons in Estonia, specifically in the form of so-called digital stamps. Estonian law and technical infrastructure allows companies to establish stamping policies, as a result of which their digital stamps can have a clear legal value. While they are not emphatically labelled as qualified certificates, they are considered as such. Similar situations exist in other Member States, although these were not identified as related to qualified certificates/signatures. For instance, the Czech Republic's act on e-signatures also establishes a so-called "qualified system certificate", which can be issued to legal entities and can be used in automatically signing systems. The resulting electronic signature is called an "electronic mark". Similarly, Slovakia knows the concept of mandate certificates allowing to determine the legal capacity in which a person is signing a document, in which the certificate itself clearly specifies the applicable rules. A legal framework for the latter was created in January 2009.

Given this ambiguity, there is conceptually a very real interoperability barrier, since it could result in a situation where a company uses a qualified certificate to create a qualified signature, which could then still be denied legal effectiveness in another Member State on the basis that it a legal entity cannot create a qualified signature under their laws. This issue would thus need to be clarified at the European level.

The Bulgarian eSignatures and eDocuments Act simplifies this question by distinguishing two roles related to the electronic signature – the titular and the author. The author signs with the electronic statement on behalf of the titular and could be only a natural person. In cases where the titular is a natural person who signs the statement by himself, he will be also seen as an author. If the titular is a legal entity or a natural person who will be represented by other person, then information about the grounds of the representative power must be entered in the certificate.

With regard to personal appearance, the result was uniform: in all countries, personal appearance is required in order to obtain a qualified certificate. It should be understood of course that in case of qualified certificates issued to legal persons, the personal appearance takes the form of appearance of the person who will be signing on behalf of the legal person. In addition, it should be noted that some countries accept a form of ‘indirect personal appearance’: the Estonian Digital Signatures Act does not explicitly require personal appearance of the certificate applicant but puts the burden of accurate identification of a certificate holder to the issuer. In practice, the eID card always requires personal appearance, and in case of mobile qualified signatures, it was already noted above that the mobile phone operator’s registration process was not considered trustworthy enough by default, and that the user therefore needs to “activate” the signature solution using his/her eID-card in a web environment. In this manner, the service provider noted that the issuance of the Mobile-ID became implicitly bound to the security and quality of the ID-card.

4.2.2.4 Supervisory bodies and accreditation

The table below will identify which entity has been designated as the supervisory body in each country and which accreditation schemes (if any) apply.

Country	Supervisory body and accreditation
Austria	<ul style="list-style-type: none"> Both supervision and accreditation are handled by Telekom-Control-Kommission which calls RTR-GmbH¹⁰⁵. Supervision is limited to certification services providers issuing qualified certificates.
Belgium	<ul style="list-style-type: none"> Supervision is handled by the Administration Quality and Safety, Accreditation Department, Service Electronic Signatures of the Ministry of the Economy. A voluntary accreditation scheme called BE.SIGN exists for CSPs issuing qualified certificates.
Bulgaria	<ul style="list-style-type: none"> Supervision is handled by the Bulgarian Communications Regulation Commission – UES, http://www.crc.bg
Croatia	<ul style="list-style-type: none"> The Financial Agency (FINA) – based on a contract with the Ministry of Economy, Labour and Entrepreneurship, acts as the supervisory body
Cyprus	<ul style="list-style-type: none"> the Ministry of Communications and Works, Department of Electronic Communications was designated in Q1 2009 as the competent authority (originally this task was conferred to the Ministry of Commerce, Industry and Tourism). The Authority may also create accreditation schemes (but doesn't presently).
Czech Republic	<ul style="list-style-type: none"> The competent authority for supervision and accreditation is the Ministry of Interior of the Czech Republic, www.mvcr.cz
Denmark	<ul style="list-style-type: none"> National IT and Telecom Agency acts as a supervisory authority (there are presently no qualified CSPs to supervise, but the supervision also extends to the OCES signatures, to a certain extent), www.itst.dk
Estonia	<ul style="list-style-type: none"> The State Register of Certification contains data about all Estonian CSPs and TSPs. It functions as a supervisory authority, confirming the results of service providers' annual audits. The Ministry of Economy and Transportation, in whose administration area the registry works, has the right to verify audit results and inspect the service providers' premises and relevant information.
Finland	<ul style="list-style-type: none"> In accordance with the Act on Electronic Signatures, qualified certification authorities are supervised by the Finnish Communications Regulatory Authority (FICORA), which is an agency under the administration of the MinTC, http://www.ficora.fi/en/index.html
France	<ul style="list-style-type: none"> The supervisory body is the DCSSI, www.ssi.gouv.fr; accreditation is delegated to auditors which are accredited by the Cofrac (the French accreditation body having sign the Multilateral agreements)

¹⁰⁵ www.signatur.rtr.at/en/

Country	Supervisory body and accreditation
Germany	<ul style="list-style-type: none"> Supervision and voluntary accreditation are handled by the Bundesnetzagentur (www.bundesnetzagentur.de)
Greece	<ul style="list-style-type: none"> The supervisory body is the Hellenic Telecommunication and Post Commission, which also manages a voluntary accreditation scheme; (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων – ΕΕΤΤ) www.eett.gr
Hungary	<ul style="list-style-type: none"> The National Communications Authority, Hungary (<i>Nemzeti Hírközlési Hatóság</i> hereafter: NHH) is an independent entity of public administration directed by the Government¹⁰⁶. NHH protects the interests of both service providers and users in the field of electronic communications, electronic commerce services and other on line services of the information society, e.g. electronic signature. The Authority performs the basic official tasks needed in the e-signature market according to the Act XXXV of 2001 on electronic signature.
Iceland	<ul style="list-style-type: none"> The Consumer Agency¹⁰⁷ (former name was State Accreditation Agency) is responsible for monitoring that the operation of certification-service-providers issuing qualified certificates conform to the provisions of the Act and regulations based on the Act.
Ireland	<ul style="list-style-type: none"> The supervisory body is Enterprise Ireland, www.enterprise-ireland.com
Italy	<ul style="list-style-type: none"> The supervisory and accreditation body is the CNIPA (<i>Centro Nazionale per l'Informatica nella Pubblica Amministrazione</i>, the National Centre for ICT in the Public Administration), http://www.cnipa.gov.it
Latvia	<ul style="list-style-type: none"> The supervisory body is the Data State Inspectorate, http://www.dvi.gov.lv/eng/
Liechtenstein	<ul style="list-style-type: none"> The supervisory body in Liechtenstein is the Communications Service (<i>Amt für Kommunikation</i>); see http://www.llv.li/amtstellen/llv-ak-home.htm
Lithuania	<ul style="list-style-type: none"> The Information Society development Committee under the Government of the of the Republic of Lithuania is the state institution responsible for the supervision and accreditation of electronic signatures¹⁰⁸.
Luxembourg	<ul style="list-style-type: none"> The Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS) via its in-house department : Office Luxembourgeois d'Accréditation et de Surveillance (OLAS), http://www.ilnas.lu; http://www.olas.public.lu/psc/index.html; ILNAS also provides a voluntary accreditation scheme
Malta	<ul style="list-style-type: none"> The supervisory body is the Malta Communications Authority, www.mca.org.mt
The Netherlands	<ul style="list-style-type: none"> Supervision is handled by the OPTA (<i>Onafhankelijke Post en Telecommunicatie Autoriteit</i>), the Independent Mail and

¹⁰⁶ <http://www.nhh.hu/index.php?id=hir&cid=891&mid=599&lang=en>

¹⁰⁷ <http://neytendastofa.is/Forsida/Oryggissvid/Rafraenar-undirskriftir>

¹⁰⁸ Appointed by the Decree No 568 of the Government of the Republic of Lithuania on eSignature Supervision Institution as of 23 April 2002.

Country	Supervisory body and accreditation
	Telecommunications Authority, www.opta.nl . Accreditation is provided via ECP.NL, http://www.ecp.nl/ . In addition, a supervision scheme for the PKI government model was created via PKIoverheid (http://www.pkioverheid.nl/), which acts as a unifying trust infrastructure for CSPs which meet certain quality requirements.
Norway	<ul style="list-style-type: none"> • Certification Service Providers issuing qualified certificates must register with the Norwegian Post and Telecommunication Authority (No. Post- og teletilsynet)¹⁰⁹
Poland	<ul style="list-style-type: none"> • Supervision is handled by the Ministry of Economy, http://www.mg.gov.pl
Portugal	<ul style="list-style-type: none"> • Decree-Law no. 234/2000, of 25 September, nominated the Accreditation Technical Committee as a consultative body aid the <i>Instituto das Tecnologias da Informação na Justiça</i> (ITIJ - Institute of Information Technologies in Justice) in its function of accreditation of digital signatures. The Decree-Law no.116-A/2006, of June 16, expressly revoked this power to public certification (SCEE) empowering <i>Antoridade Nacional de Segurança</i> as Accreditation Authority for public certification providers, and now by the Decree-Law no.88/2009 for other certification service providers.
Romania	<ul style="list-style-type: none"> • Both supervision and accreditation are handled by the National Regulatory Authority for Communications and Information Technology (ANRCTI); www.anrcti.ro
Slovakia	<ul style="list-style-type: none"> • National security authority, http://www.nbusr.sk/en/electronic-signature/index.html. It handles both supervision and accreditation.
Slovenia	<ul style="list-style-type: none"> • Supervision is handled by the Ministry of the Economy; Inspectorate for electronic communications, electronic signature and post, http://www.iekepp.gov.si/en/
Spain	<ul style="list-style-type: none"> • Supervision is handled by the Ministerio de Industria, Turismo y Comercio – Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, www.mityc.es; no accreditation scheme is in place.
Sweden	<ul style="list-style-type: none"> • Supervision is handled by the National Post and Telecom Agency (Post och Telestyrelsen), www.pts.se; whereas accreditation is provided by the SWEDAC, Swedish Board for Accreditation and Conformity Assessment; http://www.swedac.se/
Turkey	<ul style="list-style-type: none"> • Supervision is provided by the Turkish Telecommunications Authority (Telekomünikasyon Kurumu), http://www.tk.gov.tr/
United Kingdom	<ul style="list-style-type: none"> • Supervision is provided by the Department of Trade and Industry, and accreditation by tScheme Limited (http://www.tscheme.org/)

In summary, of the 32 countries surveyed, 15 (47%) have provided for accreditation schemes (Austria, Belgium, Czech Republic, France, Germany, Greece, Italy, Lithuania, Luxembourg, Portugal, Romania, Slovakia, Sweden, the Netherlands and the UK.

¹⁰⁹ Cf.

http://www.npt.no/portal/page/portal/PG_NPT_NO_EN/PAG_NPT_EN_HOME/PAG_SECURITY/PAG_EID?menuid=11787

Obviously, and as envisaged by the Directive, the accreditation schemes are a purely national matter, with specific requirements and goals of the accreditation schemes varying quite broadly, as examined in more detail via the CROBIES Study [RD10]. This is not problematic as such, since voluntary accreditation was always conceived in the Directive as tool to enhance the level of service-provision (enhanced levels of trust, security and quality, as noted in recital 11 to the Directive), and not as a tool to support interoperability. However, the voluntary nature of accreditation schemes has always been stressed as a vital characteristic distinguishing them from prior authorization schemes, and that same recital 11 also noted that CSPs “should be left free to adhere to and benefit from such accreditation schemes”. In cases where accreditation has become a de facto requirement for the use of eSignatures in a given country’s eGovernment applications, it is questionable whether this restriction has still been observed.

4.3 eGovernment applications and their usage

4.3.1 General overview table

The following table provides an overview of eGovernment applications presented in the Country Profiles, per country and per sector eProcurement, eHealth, eJustice, Taxation ...

Note that 'Other' represent all sectors at the exception of eProcurement, eHealth and eJustice.

Country	eProcurement	eHealth	eJustice	Other
Austria	X	X	X	X
Belgium	X	X		X
Bulgaria				X
Croatia		X	X	X
Cyprus	X	X		X
Czech	X	X	X	X
Denmark	X	X		
Estonia				X
Finland		X		
France	X	X	X	X
Germany	X	X	X	
Greece				X
Hungary		X	X	
Iceland				X
Ireland	X	X	X	X
Italy	X	X	X	
Latvia				X
Liechtenstein				
Lithuania	X			
Luxembourg				X
Malta				
The Netherlands	X	X		X
Norway	X	X		
Poland	X		X	X
Portugal	X			
Romania	X			X
Slovakia	X		X	
Slovenia	X	X	X	X
Spain	X	X	X	
Sweden	X			X
Turkey			X	X
United Kingdom				X

4.3.2 Specific applications

In this section, we will look at the three mandatory application sectors (eProcurement, eJustice and eHealth) in more detail, examining which applications have been reported, which types of signatures they use, and whether or not they are accessible across borders.

4.3.2.1 eProcurement

4.3.2.1.1 Overview

The table below will present a summary for each country of any reported eProcurement application, showing specifically the name of the application, an URL, a summary of its use/functionality, and its operational status (fully operational – pilot – implementation stage – design phase – planning stage). Specific eSignature aspects will be dealt with in the following section.

Country	Application name and URL	Use/functionality	Status
Austria	@-AVA-Online® eTendering Platform of the Austrian Federal Railways (ÖBB) https://www.ava-online.at	General platform for various procurement activities (construction work or supply contracts) for the Austrian Federal Railways	Operational
Belgium	eTendering - https://eten.publicprocurement.be/	Allows the submission of electronically signed tenders using the Belgian eID card	Pilot
Cyprus	e-PS https://www.eprocurement.gov.cy/ceproc/home.do	e-PS is a secure and interoperable web-based application of the Republic of Cyprus, which constitutes a total solution for the implementation of electronic procedures in conducting public procurement competitions. The system is compliant with the provisions of the European and Cypriot Law of public procurement. Amongst its provisions, it supports the procurement of contracts through one-off and repetitive procedures. The system is managed by the Public Procurement Directorate of the Treasury of the Republic of Cyprus.	Planned
Czech	The information system on public contracts – publication subsystem	"ISPC-PS" is the only one system that enables to publish the standard forms. The contracting authority/entity download the application for filling and sending the standard form intended for	Operational

Country	Application name and URL	Use/functionality	Status
		publishing and send completed standard form to the provider with advanced electronic eSignature based on qualified certificate.	
Denmark	ETHICS - http://www.innovasion.dk/1.html	Full eProcurement portal, including electronic submission and evaluation	Operational
France	Marches-public.gouv.fr	The application allows enterprises to access public procurements and submit their offer online.	Operational
Germany	eVergabe - http://www.evergabe-online.info	Allows the submission of electronically signed tenders using the signatures conforming to the Common PKI specifications	Operational
	AI Tendering platform (Governikus based) - www.ai-ag.de	Allows the submission of electronically signed tenders using the signatures conforming to the Common PKI specifications	Operational
Ireland	eTenders public procurement portal www.etenders.gov.ie	Allows the submission of electronically signed tenders, after simple on-line registration	Operational
Italy	Acquisti in Rete della Pubblica Amministrazione www.acquistinretepa.it	Allows the submission of electronically signed tenders using supported signatures	Operational
Lithuania	eCatalogue systems - https://www.cpo.lt/central-purchasing-body.html	eCatalogue based procurement system, with the Lithuanian Government acting as the Central purchasing body (www.cpo.lt). Service providers are able to prepare their price proposals using prefilled online forms. Proposals are signed using qualified e-signatures.	Operational
The Netherlands	TenderNed www.tenderned.nl	Allows the submission of electronically signed tenders using supported signatures	Implementation stage
Norway	eHandel www.ehandel.no	Allows the submission of electronically signed tenders using supported signatures	Operational
Poland	Five specific e-procurement applications were described	Each of the application platforms allows the submission of electronically signed tenders using supported Polish signatures	Operational
Portugal	e-Tendering – http://www.vortal-info.biz/vortalPT/Mercados/vortalGOV/tabid/57/default.aspx/	Allows the submission of electronically signed tenders using supported signatures	Operational
Romania	e-Procurement - http://www.e-licitatie.ro	Allows the submission of electronically signed tenders using supported signatures	Operational

Country	Application name and URL	Use/functionality	Status
Slovakia	Electronic Public Procurement System EVO, www.evo.gov.sk	Our system EVO is maintained centrally at the Office for Public Procurement. EVO supports all phases of the Tendering Process and e-Notification. When it comes to procedures we have implemented Open and Restricted procedures and e-auctions.	Operational
Slovenia	Electronic Procurement System (http://www.enarocanje.si/?podrocje=portal)	Allows to view and search all public procurement opportunities free of charge and without having to register or authenticate its identification on the national portal for public procurement "Portal javnih naročil". Allows the submission of electronically signed tenders using supported signatures. Allows electronic process for paper and electronic award procedure tenderers.	Pilot
Spain	Plataforma de contratación del estado (State Contracting Platform) www.contrataciondelestado.es	Virtual space for the eProcurement (including information on the contracting process, search for public procurement opportunities, bid announces, submission of bids and contract's adjudication).	Operational
Sweden	ChamberSign	The application allows aspiring tenderers to register and submit a bid electronically if the public authority has chosen to use this solution. Subsequently the bid is opened and processed electronically by the contracting authority.	Operational

4.3.2.1.2 Signature type

For each of the applications identified in the section above, the table below will indicate the type of signature used, reported signature type, and cross border accessibility (if any).

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
Austria	@-AVA-Online® eTendering Platform	Austrian citizen card, and several foreign cards via assistant software (e.g.	Qualified signatures	Several foreign cards are supported via assistant software (e.g.

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
		Belgium, Italy, Slovenia, etc)		Belgium, Italy, Slovenia, etc). In addition, foreigners can obtain citizen cards.
Belgium	eTendering	Belgian eID card only	Qualified signatures	None (unless the foreign user has a Belgian eID card).
Czech	The information system on public contracts – publication subsystem	No requirements. Both smartcards and software based certificates are used.	Advanced electronic signature based on qualified certificate	Yes, advanced electronic signatures based on qualified certificate according to e-signature directive are accepted.
Cyprus	e-PS	Not decided yet	Not decided yet	Not decided yet
Denmark	ETHICS	ETHICS contains a CA (certification authority) that issues digital certificates for use by vendors when signing proposals; certificates are specific to the tenderer and tender, following the OCES standard	Advanced signatures	Freely accessible via the internet.
France	Marches-public.gouv.fr	Certificates on a material carrier, depending on the specific solution acquired by the users with the certified certification authorities.	The system currently relies on an advanced electronic signature supported by a qualified certificate (RGS, security level **).	The only requirement is that the CSP is accredited according to the procedure established by the French Government.
Germany	eVergabe	Common PKI compliant qualified and advanced signatures	Advanced signatures[1]	User must have a German advanced signature.
	AI Tendering	Common PKI compliant qualified signatures by default.	Qualified signatures by default	Uses the Governikus platform, which supports German supervised CSPs by default. The operator can add additional CSPs, including nonqualified ones, if desired.
Ireland	eTenders public procurement portal	Simple login process based on chosen credentials after on-line registration.	Simple signatures	Freely accessible after on-line registration
Italy	Acquisti in Rete della Pubblica Amministrazione	Italian accredited CSPs; also, the legal representative of the company must have a valid Italian Fiscal Code number	Qualified signatures	User must have a signature solution of an accredited CSP; otherwise, usage is handled on a case by case basis.

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
Lithuania	eCatalogue	Lithuanian qualified CSPs issuing qualified certificates on USB sticks	Qualified signatures	User must have a signature solution from a supported qualified CSP.
The Netherlands	TenderNed	Two-factor authentication based on SMS	Simple/advanced signatures[2]	Freely accessible after on-line registration (which is verified by the Ministry of Economic Affairs).
Norway	eHandel	All certificate levels defined in the Requirement Specifications for PKI for public sector are accepted	AdES, AdES based on QC, and qualified signatures	International extension to unknown qualified eIDs is possible through validation authorities, specifically through the BBS Global Validation Service.
Poland	Five specific applications were described in general terms	Polish qualified CSPs	Qualified signatures	User must have a signature solution from a Polish qualified CSP.
Portugal	e-Tendering	Qualified signature solutions, either the eID card or commercial solutions	Qualified signatures	User must have a signature solution from a Portuguese qualified CSP.
Romania	e-Procurement	Romanian qualified CSPs (three private; one public)	Qualified signatures	User must have a signature solution from a supported qualified CSP.
Slovakia	Electronic Public Procurement System EVO	Software certificate (included in pfx (PKCS#12) format file). The use of the certificate file is protected by the password. The user (vendor) sets the password to the certificate token during the registration in the EVO system (eTendering system). The password is known only to the vendor. The user makes electronic signature by Adobe Acrobat Application and the software certificate. The certificate is sent to the user by e-mail automatically from the eTendering system.	At the present Slovak legislation (Act No. 25/2006 Coll. On Public Procurement and on Modification and Amendment) doesn't require usage qualified e-signature. We use just advanced e-signature in the field of public procurement.	No. The certificate for signing is provided by the EVO system (the e-Tendering application) after a vendor/tenderer has been approved by the contracting authority or utility.
Slovenia	Electronic Procurement	The application does not define the type of certificates and tokens. Most people use the authentication and	The system relies on the advanced signature based on a qualified certificate issued by SIGOV-CA or SIGEN-CA in	The application currently does not support foreign signatures and digital certificates.

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
		signature features of their software certificates, but some also use smartcards e.g. all governmental employees as clerks at the OSS offices.	accordance with Slovene legislation.	
Spain	Plataforma de contratación del estado (State Contracting Platform)	Advanced eSignature; Spanish eID card and certificates issued by the Royal Mint (FNMT)	The system requires, at least, the use of an advanced signature, according the eSignature Law (see above), and also admits the Spanish eID which creates qualified signatures	The application supports all non-national signatures admitted by the @firma platform (which at present already admits the Portuguese eID card)
Sweden	ChamberSign	N/A	Advanced electronic signature	Yes, the acceptance of Norwegian and Finnish eIDs is planned for this year.

4.3.2.1.3 Conclusions

In total, 19 eProcurement applications were reported, 15 of which were presently operational, three were in pilot stage, and one in the planning stages. Obviously, there are many more eProcurement applications available in practice, but the present study focuses only on eProcurement applications with an eSignatures component. Thus, applications which merely allow prospective tenderers to register and search for procurement opportunities are not included in the table above.

It should be noted that Estonia did not provide a specific profile for eProcurement applications, noting that the same signature infrastructure is universally usable (irrespective of application field). In addition, Estonian law does not require the usage of signatures for public procurement purposes, making the issue somewhat moot.

For Malta, it was reported that the www.contracts.gov.mt web site uses eID as the primary source of authentication. The services currently being offered do not require an eSignature but other services such as setting of alerts and downloading of tender documents can only be executed once the user had authenticated via eID or the system managed access control. Non-Maltese Identity Card holders are offered the facility of registering for a system managed account by providing details (Name, Surname, Address and Identifications Details), once the details have been verified the account is activated and the user given the same level of services¹¹⁰. As the application does not rely on electronic signatures, it was not included in the table above.

¹¹⁰ Information kindly provided by M. Adrian Camilleri of the Malta Information Technology Agency after the finalization of the Maltese country profile.

Given our focus on eProcurement solutions with eSignature functionality, the scope of the applications above is unsurprisingly homogenic, comprising exclusively applications that allow tenderers to electronically sign and submit electronic offers.

With regard to signature solutions, and looking exclusively at the 15 operational applications, there is some diversity to be found:

- Six solutions presently rely on qualified signatures (Austria, Italy, Lithuania, Poland, Portugal and Romania)
- Two require advanced signatures based on qualified certificates (Czech Republic and France)
- Six require advanced signatures: Denmark, Germany, Norway, Slovakia, Spain and Sweden;
- One (Ireland) requires a simple signature only.

More interesting than the reported signature type of the supported signatures is the accessibility of the application to tenderers in other countries. In the previous study, the response to this question was universally negative: eTendering applications were only accessible provided that the tenderer obtained local credentials. This situation has changed to a small extent in the past two years:

- For a majority of the applications (10 out of 15), the application is only accessible when using local credentials. This is the case in the Czech Republic, France, Germany, Italy, Lithuania, Poland, Portugal, Romania, Spain and Sweden.
- Two countries have a small list of foreign solutions which are also supported. This was the case in Austria, where the use of a signature validation component allowed the eTendering application to also accept signatures created using an eID card from Belgium, Italy, and Slovenia; and in Norway, where the eTendering platform could be extended to support electronic signatures supported by the private BBS Validation Authority.
- Finally, three countries have no restriction in place: Ireland, Denmark and Slovakia. In the Irish case, the application uses a simple online registration system that does not use any PKI components and therefore has no interoperability issues to be dealt with. In the Danish and Slovakian case, registration results in the recipient receiving an advanced signature certificate via e-mail that complies with national requirements, which he can use to sign the offer. These are all examples of a case where local credentials are still needed, and where there is thus strictly no interoperability, but where the need for interoperability has been avoided by introducing a sufficiently flexible user registration system. The Netherlands is similarly experimenting with a system that has not become fully operational yet, in which service providers would be able to register via the website, and would then become capable of signing bids using two-factor authentication via SMS (after verification of the registration by the Ministry of Economic Affairs).

Thus, there is some improvement to be found with respect to interoperability, as validation systems have entered into usage in Austria and Norway. It should be duly acknowledged that Spain already used (and still uses) a validation platform two years ago and can thus be considered a pioneer of this

approach; however, the Spanish @firma solution incorporates only Spanish CSPs at this time¹¹¹, and therefore currently only serves a national interoperability function. On 22 September 2009, the Ministries of the Presidency of Portugal and Spain were reported to have signed a bilateral agreement to set-up cross-border validation services in relation to the national eID cards and other qualified certificates issued in both countries, under the legal umbrella of the eSignature Directive¹¹². This is of course a very positive development, given the theoretical possibility of extending this approach to other countries.

Finally, it should be noted that Sweden is currently also planning to integrate support for Norwegian and Finnish eIDs by the end of this year.

Thus, it is clear that interoperability is still very limited, but none the less clear progress has been made in comparison to the previous edition of the study.

¹¹¹ The Portuguese national eID card is already integrated in the @firma preproduction environment and ready to be transferred to the production environment.

¹¹² The agreement reportedly defines a collaborative framework that will allow for the establishment of cross-border validation services needed for the mutual incorporation of qualified certificates in eGovernment applications in both Member States. Both countries agree to provide a predefined Service Level Agreement on validation services and make the appropriate technical integration of the national validation services.

4.3.2.2 eHealth

4.3.2.2.1 Overview

The table below will present a summary for each country of any reported eHealth application, showing specifically the name of the application, an URL, a summary of its use/functionality, and its operational status (fully operational – pilot – implementation stage – design phase – planning stage). Specific eSignature aspects will be dealt with in the following section.

Country	Application name and URL	Use/functionality	Status
Austria	eHealth Directory Service http://www.ehvd.at	Directory of health care professionals (HCP) and their respective roles. HCPs can apply for being registered to the directory using their citizen card. The competent authority (e.g. Ministry for Health, Medical Association, Chamber of Pharmacists, ... as defined by the Health Telematics Order) will certify the role. In addition a HCP-token ("GDA-Token", a signed statement of the HCP's role) can be stored on the citizen card	Operational
Belgium	On-line Cancer Registry https://www.kankerregistratie.be/wbc/r/	On-line registration of cancer occurrences, thus facilitating epidemiological research	Operational
Croatia	Primary Health Care Information System – PZZ http://www.hzzo-net.hr/	General platform for eHealth communication, building on the CIHI card and local clients in the doctors' praxes	Operational
	e-zdravstveno (e-health)	Application that allows businesses that are registered in the register of the Croatian Institute for Health Insurance (CIHI) to register employees and their family members.	Operational
	On-line supplementary insurance (on-line dopunsko osiguranje)	Submission of proposals for supplementary health insurance	Operational
Denmark	Sundhed.dk www.sundhed.dk	General platform for eHealth support, including signature functionality through OCES	Operational
Germany	National Health Telematic Infrastructure www.gematik.de	General platform for eHealth support, including signature functionality through specific smart cards.	Pilot

Country	Application name and URL	Use/functionality	Status
Ireland	HealthLinkOnline	Secure transfer of patient information over the internet between GPs and acute hospitals	Operational
Italy	Sistema Informativo dei Servizi Transfusionali, SISTRA http://www.iss.it/site/attivita/ISSWEB_istituto/UO/index.asp?idUO=1208(=1	Platform to support blood transfusion needs	Operational
The Netherlands	UZI card applications (UZI-Register) http://www.uziregister.nl/	Generic trust infrastructure for health care professionals	Operational
Norway	MyGP/MyDoctor (<i>MinFastlege</i>), an application within the MyPage (<i>MinSide</i>) portal www.minside.no	Allows natural persons to change their official GP	Operational
Slovenia	e-Health Portal	General platform for eHealth communication (exchange of the e-documents,	Being designed; not operational yet
	On-line access to health and health insurance data	On-line access to health and health insurance data	Under deployment

4.3.2.2.2 Signature type

For each of the applications identified in the section above, the table below will indicate the type of signature used, reported signature type, and cross border accessibility (if any).

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
Austria	eHealth Directory Service	Austrian citizen card. Several foreign cards (e.g. Belgium, Italy) could be integrated easily via assistant software, but this is not operational yet.	Qualified signatures	Foreigners can obtain citizen cards. Several foreign cards can be supported via assistant software, but this is not operational yet.
Belgium	On-line Cancer Registry	Belgian eID card and federal token	Qualified signatures and simple signatures	None (unless the foreign user has a Belgian eID card or token).
Croatia	Primary Health Care	CIHI card	Advanced signatures	CIHI card holders

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
	Information System – PZZ			only (doctors and nurses registered in Croatia)
	e-zdravstveno (e-health)	FINA card, CIHI card, and Zagrebačka banka	Qualified signatures for FINA and Zagrebačka banka; advanced signatures for CIHI	Only available to businesses that are registered in the register of the Croatian Institute for Health Insurance (CIHI)
	On-line supplementary insurance (on-line dopunsko osiguranje)	FINA card	Qualified signatures	Persons holding a FINA card and registered for Croatian health insurance only.
Denmark	Sundhed.dk	OCES	AdES	OCES only; the certificate must contain the individual's social security-number
Germany	National Health Telematic Infrastructure	eGK (<i>elektronische Gesundheitskarte</i>) and the new HBA (<i>Heilberufsausweis, Health Professional Card</i>)	Qualified signatures for the HBA, Advanced and (optionally) qualified for the eGK	eGK and HBA only.
Ireland	HealthLinkOnline	Username, password and PIN	Simple signatures	Restricted to the health care practitioner user group.
Italy	Sistema Informativo dei Servizi Transfusionali, SISTRA	EIC, the NSC and, during the testing phase, authentication through credentials	Qualified signatures for the EIC and NSC	EIC and NSC only
The Netherlands	UZI-Register	UZI-card, a smart card issued to health care professionals ¹¹³	Qualified signatures	UZI-card holders only (i.e. health care professionals registered in the Dutch UZI-Register)
Norway	MinFastlege	MyID authentication solutions	Authentication based on PIN-codes	Only relevant to Norwegian residents to whom a GP has been assigned

¹¹³ Strictly speaking, there are four types of UZI-cards, two of which provide a clear answer to the question of whether the card holder is a healthcare practitioner and whether he or she is working on behalf of a healthcare institution. The *zorgverlenerpas* (Health care provider) and the *medewerker op naam* (*name-specific employee card*) allow for the user to place a qualified digital signature.

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
Slovenia	e-Health Portal	The professional health card will be supported	Qualified signature	Holders of the professional health card only
	On-line access to health and health insurance data	Health insurance card (HIC) for the insured persons and health professional card (HPC) for the professionals in health care and health insurance	Qualified signature for the HPC; advanced signature for the HIC	Holders of the supported card only

4.3.2.2.3 Conclusions

In total, 10 countries reported eHealth applications, 8 of which related to applications which were presently operational, and two where applications were in pilot/design stage. eHealth applications using eSignature solutions are thus significantly fewer in number than eProcurement applications.

It should be noted that again Estonia did not provide a specific profile for eHealth applications, noting that the same signature infrastructure is universally usable (irrespective of application field).

Looking at the scope of the applications, seven of the ten descriptions relate to general eHealth platforms that could be used to securely exchange information in the eHealth sector (Austria, Croatia, Denmark, Germany, Ireland, Slovenia and the Netherlands). The three other applications related to cancer research (Belgium), blood transfusions (Italy), and changing GP (Norway).

With regard to signature solutions, and looking exclusively at the 8 operational applications, there is some diversity to be found:

- Five solutions presently rely on qualified signatures (Austria, Belgium, Germany, Italy and the Netherlands)
- Two require advanced signatures: Croatia and Denmark;
- Three applications have components that can operate on the basis of a simple signature: the Irish example relies exclusively on a simple signature, whereas the Belgian and Norwegian application support it to some extent.

When breaking down the signature types per use case in the 8 operational applications:

- For the six operational general eHealth platforms (Austria, Croatia, Denmark, Germany, Ireland, and the Netherlands), three rely on qualified signatures, two on advanced signatures, and one on a simple signature.

- For the two operational specific applications (in Italy and Norway), one uses qualified signatures and the other a simple signature.

The sample size is too small to attach significant conclusions to this distribution.

Given the sensitive nature, the need to be able to verify the professional status of a health care professional, and the link to a specific sector, it could reasonably be anticipated that interoperability initiatives would be at a less advanced stage in eHealth applications than in the eProcurement applications described above. This is indeed confirmed by the overview above: all countries restrict accessibility of the solution to the holder of national credentials.

In a number of cases, this is due to the exclusive reliance on a sector specific national card, as is e.g. the case for Croatia (CIHI card), Germany (EGK and HBA card), Italy (EIC and NSC card), and the Netherlands (UZI-card). These cards serve to determine the capacity of the signatory (e.g. the UZI-card is only available to health care professionals registered in the Dutch UZI-Register), meaning that interoperability is much harder to achieve in this field.

It should be also noted however that for a number of applications the actual need for interoperability is also much smaller than for applications with a potentially unlimited user group. E.g. the Belgian application is targeted towards charting cancer occurrences in Belgium; the Norwegian application allows Norwegian residents to officially change their GPs; and the Italian one aims to facilitate the coordination of blood transfusions in Italy. In each of these examples, the application's scope is delineated at the national level, which means that all users should have access to appropriate national credentials. In those specific cases, the need for interoperability is thus much smaller.

4.3.2.3 eJustice

4.3.2.3.1 Overview

Finally, the table below will present a summary for each country of any reported eJustice application, showing specifically the name of the application, an URL, a summary of its use/functionality, and its operational status (fully operational – pilot – implementation stage – design phase – planning stage). Specific eSignature aspects will be dealt with in the following section.

Country	Application name and URL	Use/functionality	Status
Austria	Notarial document archive "CyberDoc » https://www.ava-online.at	Electronic archive used to register and store scanned paper documents or electronic documents, both converted to XML structures signed with the qualified signature of the notary. The document archive is used to transfer documents to courts, the Commercial Register or the Land Register	Operational
Croatia	e-Tvrtka (e-Company) www.pravosudje.hr	Site allowing notaries to create certain companies on-line	Pilot
Estonia	Company Registration Portal ¹¹⁴ https://ettevotjaportaal.rik.ee/?chlang=eng	Portal site allowing the creation of simple companies on-line	Operational
Germany	Federal company register platform (<i>Elektronische Handelsregisteranmeldung</i>) using the German EGVP system http://www.handelsregister.de www.eqvp.de	General portal for the submission of official documents to the company register.	Operational
Ireland	Small claims on-line www.smallclaims.ie	Consumer disputes before a small claims court	Operational
Italy	E-civil trial (' <i>processo civile telematico</i> ') http://www.processotelematico.giustizia.it/pdapublic/index.jsp	The application allows external users, mainly lawyers, to upload documents, signed with digital signature and encrypted, and to create an electronic file of the proceedings.	Implementation stage
Poland	e-KRS system (National Court Register (<i>Krajowy Rejestr Sądowy</i>))	The system supports the activity of National Court Register by enabling secure information	Operational

¹¹⁴ Described in the national report via a generic eSignature application description, noting that the same signature infrastructure is universally usable (irrespective of application field).

Country	Application name and URL	Use/functionality	Status
		exchange in relation to the legal status of any given legal entity.	
Portugal	Citius https://citius.tribunaisnet.mj.pt/habilus/CitiusRegisto.aspx	Platform for the communication of acts and other judicial proceedings by lawyers, judges and DAs (<i>procuradores do Ministério Público</i>)	Operational
Slovenia	Register of Wills http://www.notariz.si/register_oporok.php http://www.registeroporok.si/pomoc/ https://www.registeroporok.si/	The application provides an electronic Register of Wills, containing information about the wills that were prepared in the form of notarial protocol, that are deposited at notary, that were prepared by attorneys or are deposited at attorneys, judicial wills and wills deposited at courts.	Operational

With respect to Denmark, an electronic deed registration system became operational in September 2009¹¹⁵; however, no details were available yet at the time of analysis.

4.3.2.3.2 Signature type

For each of the applications identified in the section above, the table below will indicate the type of signature used, reported signature type, and cross border accessibility (if any).

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
Austria	Notarial document archive "CyberDoc »	Notary's profession cards are provided by the certification service provider A-Trust (i.e. a citizen card implementation).	Qualified signatures	Accessible to any notaries in Austria (who are required to use the archive). The Chamber of Notaries attests the professional qualification.
Croatia	e-Tvrta (e-Company)	FINA card	AdES based on QC	Accessible to holders of the solutions mentioned to the left. Support for other card holders is planned.
Estonia	Company Registration Portal	Estonian eID or Mobile-ID, Portuguese,	Qualified signatures	Accessible to holders of the solutions mentioned to the left.

¹¹⁵ Information kindly provided by Mrs. Charlotte Jacoby of the Danish Ministry of Science, Technology and Innovation after the finalization of the Danish country profile.

Country	Application name	Signatures used	Reported signature type	Cross border accessibility
		Belgian or Finnish ID-card or Lithuanian Mobile-ID		Support for other card holders is planned.
Germany	Federal company register platform	Common PKI compliant qualified signatures. QES must include an attribute certificate outlining the signature was applied by a notary.	Qualified signatures	Common PKI compliant QES only.
Ireland	Small claims online	Username/password, with the password being granted after payment of the 15 EUR fee	Simple signatures	Freely accessible.
Italy	E-civil trial (' <i>processo civile telematico</i> ')	Signatures issued by Postecom to the personnel of the Ministry. Lawyers and other categories use their particular systems of digital signature issued via the bar associations.	Qualified signatures	Only to holders of the appropriate signature solutions (linked to capacity, not to nationality)
Poland	e-KRS system	Signatures issued by one of the qualified CSPs in Poland: Certum, Sigillum and Szafir	Qualified signatures	Only to holders of the appropriate signature solutions
Portuguese	Citius	Signatures issued by the CA Multicert, with certificate confirming the professional capacity of the signatory, based on the Portuguese Bar Association as an RA	Advanced signatures	Only to holders of the appropriate signature solutions
Slovenia	Register of Wills	Signatures issued by Slovenian CSPs issuing qualified certificates	Advanced signatures based on qualified certificates	Only to holders of the appropriate signature solutions

4.3.2.3.3 Conclusions

In total, 9 eJustice applications were reported, 7 of which were presently operational, and 2 of which were in pilot stage. Again, the number of applications is substantially smaller than for eProcurement applications, which may be linked due to the difficulty of establishing appropriate models for verifying the legal capacity of the actors (notaries, judges, lawyers, etc.). This same problem is also present for eHealth applications, which may explain why the number of applications reported is similar.

Looking at the scope of the applications, four of the nine descriptions relate to court proceedings and court administration (Ireland, Italy, Poland and Portugal), three relate to the establishment and management of companies (Croatia, Estonia and Germany), and two related to notarial archiving services (Austria and Slovenia).

With regard to signature solutions, and looking exclusively at the 7 operational applications, the same diversity found in the eProcurement and eHealth applications is found again:

- Four solutions presently rely on qualified signatures (Austria, Estonia, Germany and Poland);
- One (Slovenia) required advanced signatures based on qualified certificates;
- One (Portugal) required advanced signatures;
- One (Ireland) used simple signatures.

When breaking down the signature types per use case in the 7 operational applications:

- For the three operational court proceedings/administration applications (Ireland, Poland and Portugal), one relies on qualified signatures, one on advanced signatures, and one on a simple signature.
- For the two operational company establishment/management applications (Estonia and Germany), both rely on qualified signatures.
- For the two operational archiving services (in Austria and Slovenia), one uses qualified signatures and the other an advanced signatures based on qualified certificates.

Again, the sample size is too small to attach significant conclusions to this distribution.

As with the eHealth applications, given the sensitive nature, the need to be able to verify the professional status the service providers, and the link to a specific sector, it could reasonably be anticipated that interoperability initiatives would again be limited. In fact, all but one country (Estonia) restrict accessibility of the application to the holder of national credentials.

In the Estonian example, companies can be established not only by the holders of an Estonian signature solution (Estonian eID or Mobile-ID), but also by using a Portuguese, Belgian or Finnish ID-card or a Lithuanian Mobile-ID. This is however an exceptional situation: all other countries limit usage of the application to holders of national credentials, thus excluding interoperability. The Irish example is however noteworthy in this respect, since its Small Claims application allows any end user to freely register on-line. Thus, while there is no interoperability with interoperability, there is more importantly

no barrier for usage across borders, insofar as this would be relevant for a small claims court application.

As with eHealth applications, here too the actual need for interoperability is again much smaller than for applications with a potentially unlimited user group. E.g. the Austrian application is aimed towards any notaries in Austria (who are required to use the archive), meaning that it is not problematic that the Austrian Chamber of Notaries attests to the professional qualification. Signature solutions are in this respect commonly linked to a specific capacity, not to nationality. In cases where this means that all users have access to appropriate national credentials, the need for interoperability is again much smaller.

4.3.3 Mandates and authorisations

4.3.3.1 Generic mandate and authorisation models

The application overview for the eHealth and eJustice sectors already noted the importance of being able to determine a specific person's authorisations or mandate, as this is crucial to determine (in these respective sectors) whether a person is entitled to provide health care or legal services. In this section, we will examine to what extent generic mandate and authorisation models have been developed, and in the following sections the specific approach in the eHealth and eJustice sectors will again be summarised.

The table below will identify per country whether there is a generic mandate/authorisation model using electronic signatures or integrated into the general e-signatures framework, and if so how it works.

Country	Generic mandate and authorisation models
Austria	<p>Several professions issue profession service cards, such civil law notaries, civil engineers, and lawyers. The main legal basis is given with the 2008 professional law amendment. It defines electronic signatures of professions that act in particular roles in legal or administrative proceedings, such as:</p> <ul style="list-style-type: none"> - Justice Signature: ("Signatur der Justiz"): An advanced electronic signature for court acts. - Notaries' Signature ("elektronische Notarsignatur"): A qualified electronic signature of the notary for the establishment of notarial deeds - Civil engineer signature ("elektronische Ziviltechnikersignatur"): A qualified signature of a civil engineer used in her/his professional duties - Notarisation Signature ("elektronische Beurkundungssignatur"); A qualified signature of a civil law notary or a civil engineer for the purpose of notarisation and establishment of public deeds. - Lawyer Signature ("elektronische Anwaltssignatur"): A qualified signature indicating a lawyer acting in her/his professional duties. <p>The certificates of these professional signatures include an object identifier indicating the particular role. The competent authorities (Chamber of Lawyers, Notarial Chambers, Chamber of Architects and Consultant Engineers) are in charge of attesting the profession or of revoking it in case of cessation. When using qualified certificates, these are citizen card implementations.</p>
Belgium	<p>For specific sectors (like eHealth; see below), Belgium uses a system of sector specific service integrators which link specific mandates/authorizations to generic identification/authentication systems like the eID card. This system is currently being generalized.</p>
Croatia	<p>No generic model; eHealth applications rely generally on the CIHI eHealth smart card; other sectors rely on ad hoc systems..</p>
Denmark	<p>Legal qualification/capacity is based either on each application's own</p>

Country	Generic mandate and authorisation models
	denomination (i.e. the Danish electronic deed registration) or on external registers (i.e. the Danish national health authorisation register) based on the Danish central personal registration number. The signature/certificate itself does not include such information.
Estonia	No generic model is in place yet. Authorisation details can be derived from specific registers, with support implemented on a case by case basis.
Germany	No generic model is in place yet. Specific sectors (including in eHealth and in eJustice) use certificates which are tailored to their needs.
Iceland	No generic model is in place yet.
Ireland	No generic model is in place yet; solutions are largely ad hoc.
Italy	No generic model is in place yet. Specific sectors (including in eJustice) use certificates which are tailored to their needs.
Liechtenstein	No generic model is in place yet.
Lithuania	No generic model is in place yet.
The Netherlands	<p>No generic model is in place yet. A relevant development is the programme eRecognition for companies and institutions. The programme aims to examine ID-mechanisms and realize a general infrastructure for eRecognition that can accommodate the need for different levels of authorization that may arise within companies and/or institutions while making use of market efforts in this area.¹¹⁶ eRecognition envisages an authentication “scheme” that will enable companies and institutions to use certain key services: Granting Access, Expression of Will and Authorisations to Represent. Core to the solution are private party suppliers. The first results of this programme are foreseen for 2009.</p> <p>In addition, the aforementioned UZI-card can be seen as a sector specific (eHealth) implementation allowing the verification of the capacity of health care professional.</p>
Norway	The current approach aims to leverage the general infrastructure created by the MinSide-portal, through collaboration with relevant service providers within the government. E.g. for the eHealth application described above, authorization is handled by the Norwegian Directorate of Health (<i>Helsedirektoratet</i>). The Directorate has in this case a register of parents and their children, that they may represent in the solution. This is based on the reference within the MyID entity authentication solution to the national identity number, which is used to identify the person.
Poland	No generic model is in place yet.
Portugal	No generic model is in place yet.
Romania	No generic model is in place yet.

¹¹⁶ http://www.ez.nl/Onderwerpen/Ruimte_voor_ondernemers/Elektronische_overheid/E_herkenning

4.3.3.2 Mandates and authorisations in eHealth

The table below will identify per country whether there is a mandate/authorisation model using electronic signatures or integrated into the e-signatures framework for eHealth applications, and if so how it works.

Country	Generic mandate and authorisation models
Austria	<p>The eHealth regulatory framework is established by;</p> <ul style="list-style-type: none"> - Health Telematics Act 2005 (“Gesundheitstelematikgesetz”) - Health Telematics Order 2008 (“Gesundheitstelematikverordnung”) <p>The regulation defines that the identity of a health care professional shall be established conformant with the eGovernment Act, i.e. using the eGovernment base registers (Central Resident Register, the Commercial Register, or the Supplementary Registers) and the citizen card function. The identification options are:</p> <ul style="list-style-type: none"> - Electronic signatures based on qualified certificates and accompanied by sector-specific identifiers - Lookup to an eHealth directory service (registration to this directory is voluntary) - Exemptions are cases where secure and dedicated network are used or where mistaken identities are impossible <p>The integrity and authenticity of health data needs to be ensured by</p> <ul style="list-style-type: none"> - Electronic signatures that are based on qualified certificates (i.e. also advanced electronic signatures and qualified certificate are possible) - Exemptions are where dedicated, secure networks ensure authenticity or in cases where modification is impossible <p>A directory of health care professionals (HCP) and their respective roles is maintained, and HCPs can apply for being registered to the directory using their citizen card. The competent authority (e.g. Ministry for Health, Medical Association, Chamber of Pharmacists, ... as defined by the Health Telematics Order) will certify the role. In addition a HCP-token (“GDA-Token”, a signed statement of the HCP’s role) can be stored on the citizen card.</p>
Belgium	<p>For specific sectors (like eHealth), Belgium uses a system of sector specific service integrators which link specific mandates/authorizations to generic identification/authentication systems like the eID card. In the eHealth sector, the service integrator is the recently established eHealth platform. Users can use their eID card or federal token to authenticate/sign, and the service integrator will determine their mandate/authorization on the basis of authentic databases that it manages through a network of intermediaries (like e.g. hospitals).</p>
Croatia	<p>Croatian eHealth applications generally build on a Central Health Database System located in the Croatian Institute for Health Insurance in Zagreb. All general practitioners have to have a connection to the central ICT system in CIHI. The data is collected in the local computer and then replicated into the CIHI system. All messages sent to CIHI are electronically signed. The doctors have to have a FINA or CIHI smart card to work with the system.</p>
Denmark	<p>Legal qualification/capacity in eHealth works by linking the personal registration number in the OCES certificate to the national health professional authorization</p>

Country	Generic mandate and authorisation models
	register. If a person is listed in this register the registers authorization-code states the type of health professional that he/she is. The signature/certificate itself does not include such information.
Estonia	No specific model has been implemented yet
Germany	Authorisations will be addressed via the new HBA (<i>Heilberufsausweis</i> , Health Professional Card), which will be QES-enabled.
Iceland	No specific model has been implemented yet
Ireland	No specific model has been implemented yet; existing solutions are ad hoc (username-password granted after registration).
Italy	No specific model has been implemented yet
Liechtenstein	No specific model has been implemented yet
Lithuania	At the moment the Ministry of Health of the Republic of Lithuania is implementing the project "eHealth services", which aims at creating the international standards based National electronic health and healthcare records system (EHR). Currently however, PKI certificates are not used for existing services. According to the eHealth strategy, eSignatures will be provided to all health care specialists, who will work with the eHealth system, to ensure sufficient protection for operation of the system. It is also anticipated that the eID card could be used in the future in eHealth applications (e.g. ePrescription, ePatient's card).
The Netherlands	Dutch healthcare providers are issued with an electronic identity, in the form of a UZI-card (UZI stands for Unique Healthcare Provider Identification, <i>Unieke Zorgverlener Identificatie</i>). This is done by the Dutch Unique Healthcare Provider Identification Register (UZI-register), an organisation under responsibility of the Health Secretary. The UZI-card has three main functionalities: it allows healthcare providers to identify and authenticate themselves, it guarantees the confidentiality of their communication and, most importantly in the current context, the UZI card enables healthcare providers to enter an electronic signature. The UZI-card and its services are based upon the so called 'trust model', a model based upon the hierarchy of PKI-Overheid, the national government PKI.
Norway	The current approach aims to leverage the general infrastructure created by the MinSide-portal, through collaboration with relevant service providers within the government. For the eHealth application described above, authorization is handled by the Norwegian Directorate of Health (<i>Helsedirektoratet</i>). The Directorate has in this case a register of parents and their children, that they may represent in the solution. This is based on the reference within the MyID entity authentication solution to the national identity number, which is used to identify the person.
Poland	No specific model has been implemented yet
Portugal	No specific model has been implemented yet
Romania	No specific model has been implemented yet. Legal provisions regarding the use

Country	Generic mandate and authorisation models
	of qualified digital certificates for electronic signature in hospitals were stipulated in Order no. 49/54 of 2004 of the Health Ministry and of National House of Health Insurances, and the first National Health Insurance Electronic Card ("NHI card") was supposed to be issued starting with the end of 2008. However, the projects have since been delayed, and a national health database is not operational yet.

4.3.3.3 Mandates and authorisations in eJustice

The table below will identify per country whether there is a mandate/authorisation model using electronic signatures or integrated into the e-signatures framework for eJustice applications, and if so how it works.

Country	Generic mandate and authorisation models
Austria	<p>Several professions issue profession service cards, including civil law notaries and lawyers. The main legal basis is given with the 2008 professional law amendment. It defines electronic signatures of professions that act in particular roles in legal or administrative proceedings, including:</p> <ul style="list-style-type: none"> - Justice Signature: (“Signatur der Justiz“): An advanced electronic signature for court acts. - Notaries’ Signature (“elektronische Notarsignatur“): A qualified electronic signature of the notary for the establishment of notarial deeds - Notarisation Signature (“elektronische Beurkundungssignatur“); A qualified signature of a civil law notary or a civil engineer for the purpose of notarisation and establishment of public deeds. - Lawyer Signature (“elektronische Anwaltssignatur“): A qualified signature indicating a lawyer acting in her/his professional duties. <p>The certificates of these professional signatures include an object identifier indicating the particular role. The competent authorities (Chamber of Lawyers, Notarial Chambers) are in charge of attesting the profession or of revoking it in case of cessation. When using qualified certificates, these are citizen card implementations.</p>
Belgium	<p>No infrastructure is available yet. It is envisaged to use the same generic mandate/authorization management model described above in the future: a sector specific service integrator would then be established for eJustice as well which would link specific mandates/authorizations to generic identification/authentication systems like the eID card. The service integrator would determine users’ mandate/authorization on the basis of authentic databases that it manages through a network of intermediaries (like e.g. local bars, courts etc.).</p>
Croatia	<p>No general infrastructure is available yet. For notaries public, one application relies on a database which allows certificate ID numbers to be linked to the quality of public notary after prior registration.</p>
Denmark	<p>Legal qualification/capacity is based either on each application’s own denomination (i.e. the Danish electronic deed registration) or on external registers (i.e. the Danish national health authorisation register) based on the Danish central personal registration number. The signature/certificate itself does not include such information.</p>
Estonia	<p>No specific model has been implemented yet</p>
Germany	<p>Common PKI compliant qualified signatures are used which include an attribute certificate outlining the signature was applied by a notary / lawyer / etc.</p>

Country	Generic mandate and authorisation models
Iceland	No specific model has been implemented yet
Ireland	No specific model has been implemented yet
Italy	<p>Article 66(8) of the Code of electronic administration states that cards used for identification purposes issued to employees of State authorities (public employees of central administrations) can be made in electronic form and they may allow holders to have access to e-government services. One example of the application of this principle regards the employees of the Ministry of Justice, namely: judges, prosecutors, managers, all personnel of the Ministry. Pursuant to the Decree of the Ministry of Justice 6 November 2007), these can be provided with a card that allows the online authentication for the access to ICT systems of the Ministry. The card is very similar to the EIC and has both a laser band and a microchip, which may contain a certificate of digital signature. In addition, lawyers use their particular systems of digital signature issued via the bar associations.</p>
Liechtenstein	No specific model has been implemented yet.
Lithuania	No specific model has been implemented yet.
The Netherlands	No specific model has been implemented yet
Norway	<p>No specific model has been implemented yet. The National Courts Administration has drafted a document on electronic communication with the courts in April 2009, indicating that a portal should be established, to cover the most basic needs, and making use of the national eID interoperability hub. It is deemed that the eID and PKI solutions that are and will be use in the hub will cover the needs also in this area.</p>
Poland	<p>No specific model has been implemented yet. Regulatory reform is currently underway to address this issue. Proposed changes concern:</p> <ul style="list-style-type: none"> • Operation of the National Court Register: it will be allowed to apply via electronic means; applications will have to be supplied with electronic signatures verified with the usage of valid qualified certificate, • Civil procedure reform: it will be possible to apply to register courts via electronic means, the same will be allowed for court statements and acts delivery; in all the cases a qualified electronic signature is the basis; Code revision assumes the possibility to create notarial certifications and their copies, and send them to the courts via electronic means if these electronic documents are supplied with electronic signatures verified with the usage of valid qualified certificate; • Reform of the Act on registered pledges and a pledge register: involved parties will be legally able to communicate electronically; that regulation will cover all type of information exchanged between entities and pledge register departments in regional courts and the central pledge register information office.
Portugal	<p>For the legal professions, signatures are issued by the CA Multicert, with certificate confirming the professional capacity of the signatory. In order to provide lawyers with an appropriate certificate, the Portuguese Bar Association entered into two Protocols in 2003 with Multicert - Serviços de Certificação Electrónica, S.A. : the first for the provision of digital signatures and the second for the provision of MDDE, a solution that combines the issuance of digital</p>

Country	Generic mandate and authorisation models
	signatures and time stamping. The Portuguese Bar Association is the Registration Authority (RA) for all the digital certificates that are issued to certify the professional quality of the signatory. Once identified by the RA, the lawyer generates the key pairs and the RA sends a Certificate Request message to the CA (Multicert).
Romania	No specific model has been implemented yet

4.3.4 Application approach models

In the previous study ([RD6]), eGovernment applications have been categorised into two groups of two technical models each.

At the light of the Country Profiles received in the frame of the current study, we think that these categories could be simplified. Therefore, eGovernment applications have been spread over two models:

- The shared service model regrouping applications which are making use of a common eSignature framework or of a common eSignature infrastructure;
- The ad-hoc model regrouping applications which are built up from scratch implementing e.g. their own signature functions or even their own certification authority.

Grouping applications by model will ease to find similarities between applications but also, and this is much more important, differences between applications and their related models, which differences might lead to interoperability issues.

The next sections will describe the models with full details.

4.3.4.1 Model 1: shared service model approach

The first model concerns countries that have set-up a shared approach in the design of their applications either by providing a one-stop shop infrastructure (government portal or sectoral portal) or by providing a common framework for the use of eSignatures.

There are several features that are specifically bound to this model. Among them:

Technical aspects:

eSignature type: The model do not impose a specific eSignature type, but none of the applications belonging to this model is supporting simple signatures.

Credential or token type: The majority of the applications are supporting either cryptographic tokens, being smartcards or USB tokens or software certificates. Some are supporting mobile eSignatures,

eSignature validation: one of the main advantages of this shared approach resides in the validation of eSignatures being realised either by a central service of the portal or external or by using common libraries provided by the framework. In both cases, the goal is to hide the validation complexity to the application. Applications do not need to know how much Certification Service Providers are involved, neither what type of validation protocols (CRLs, OCSP ...) is provided by the CSP.

Organisational aspects:

CSPs: as said previously, while choosing a shared approach, one of the implicit results is that many CSPs can be easily supported by/added to the applications.

Interoperability aspects

As far as interoperability is concerned, applications designed around this model are obviously more easily adaptable to provide true eSignature interoperability as this has only to be achieved in one central place (being the portal or within the framework).

4.3.4.2 Model 2: ad-hoc model approach

There are numerous applications described in the country profiles that do not make use of a central architecture nor of a common framework, mainly for historical reasons. They have been classified under this second 'ad-hoc' model. Within this model, stand-alone applications that can interact with various external CSPs or stand-alone applications that have set-up their own CSP inside the application are regrouped..

There are several features that are specifically bound to this model. Among them:

Technical aspects:

eSignature type: The eSignature type is imposed by the application: generally advanced eSignatures but sometimes also Qualified eSignatures are required .

eSignature validation: Every application validates eSignatures against CSPs they trust.

Credential or token type: The credential/token type can be smart-card (eID card ...) – USB Token or software certificates. No mobile eSignatures application belong to this model

Organisational aspects:

CSPs: Applications of this model may support one or several CSPs but addition of a new CSP requires a modification of the application.

Interoperability aspects

Applications of this model are not closed to interoperability. Achieving this interoperability would require sound modifications of every application.

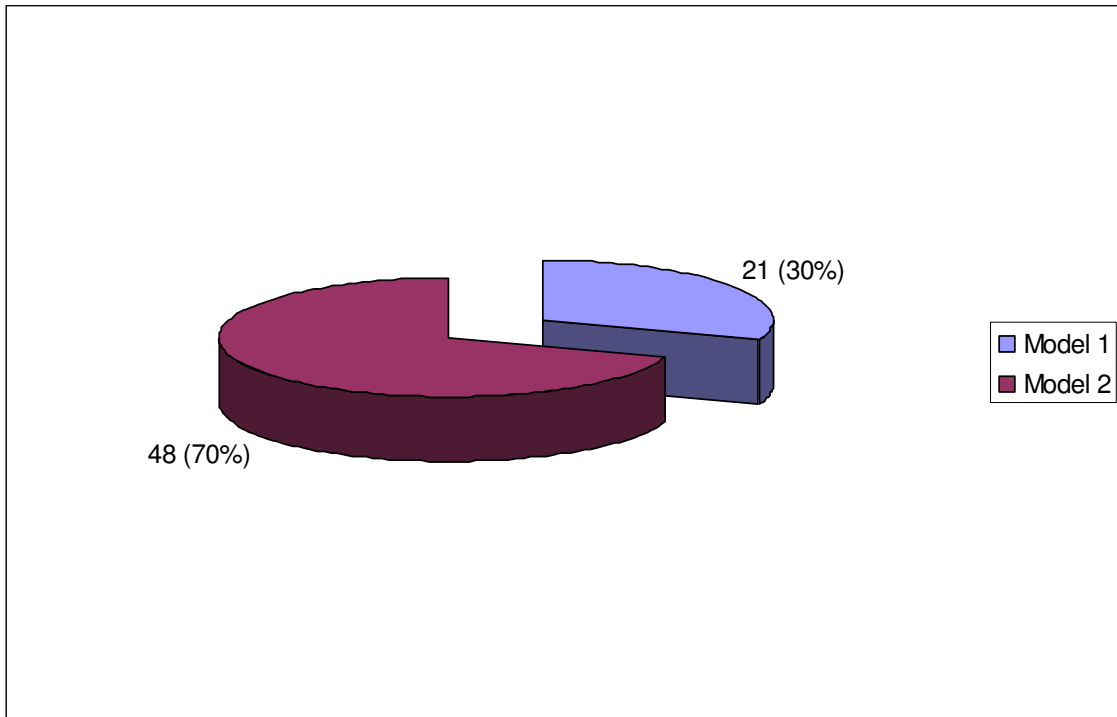
4.3.5 Classification by model

4.3.5.1 Introduction

Among the 91 eGovernment applications described in detail in the Country Profile collected for the 32 countries concerned by the study (27 Member States Countries + 2 Candidate Countries (Turkey and Croatia + 3 EEA countries (Norway, Liechtenstein, Iceland)), we have found 69 applications that make use of eSignatures.

The remaining 22 ones are mainly using electronic certificates for achieving strong authentication but not for signing any documents in the sense of Article 2.1 of the EC Directive on a Community framework for electronic signatures ([\[RD3\]](#)) that defines 'electronic signature' as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

The following figure illustrates how many applications, among the 69 concerned applications, are belonging to one of the two models presented in the previous section.



Without surprise, we noted that two thirds of these applications have followed an ad-hoc approach as defined above (see section [4.3.4.2](#)).

However, the trend is clearly to unify the way how applications are implementing electronic signatures in order to allow for better interoperability in the country itself, e.g. by setting-up a National Interoperability Framework.

These figures are quite similar to the ones observed in 2007 in the previous study (see [\[RD6\]](#)).

4.3.5.2 Model 1: shared service model approach

4.3.5.2.1 List of applications belonging to the model

Country	Application/Service Name
Austria	@-AVA-Online® eTendering Platform of the Austrian Federal Railways (ÖBB)
	eHealth Directory Service (eHealth Verzeichnisdienst eHVD)
	CyberDoc (Urkundenarchiv der Notare)
	Criminal Record Certificate (Elektronische Strafregisterbescheinigung)
Belgium	e-Tendering - https://eten.publicprocurement.be/
	Web Based Cancer Registry - https://www.kankerregistratie.be/wbcr/
Bulgaria	Company Registration – submission of an application for company registration https://public.brra.bg/Internal/Registration.ra?0
Estonia	Generic eGovernment application

Country	Application/Service Name
France	Marches-public.gouv.fr
Germany	eVergabe
Greece	SYZEFXIS - http://www.syzefxis.gov.gr
Norway	eProcurement portal (No. eHandel) www.ehandel.no
Slovakia	Electronic Services of Companies Register http://www.portal.gov.sk
	eLegal Actions - Electronic Submissions to Courts (ežaloby) - application is currently in preparation and development phase (pilot project)
Spain	Plataforma de contratación del estado (State Contracting Platform) www.contrataciondelestado.es
	Tarjeta Sanitaria (eHealth card) https://sns.msp.es
	Historia Clínica Digital en el SNS (HCDSNS) – Patient medical record in the National Health System https://sns.msp.es
	Ensayos Clínicos de Medicamentos https://sinaem4.agemed.es/ecm/paginaPresentacion.do
	LexNet
Sweden	eINK, Personal income taxes declarations (Sw: Inlämning av självdeklarationsuppgifter)

4.3.5.2.2 Major differences observed

4.3.5.2.2.1 Use of unique Identifier

Applications use information coming from the signature certificate to uniquely identify the user or its role. Most of the time this information is a national or sectoral unique number.

Spain - “Plataforma de contratación del estado (State Contracting Platform)”

Question: “Is there specific information in the certificate that plays a notable role in the functioning of the application?”

Answer: “The application reads the ID no, or fiscal no, and then connects with the ROLEC, to check that the representative is duly empowered to act on behalf of the company.”

Austria - “CyberDoc (Urkundenarchiv der Notare)”

Question: “Is there specific information in the certificate that plays a notable role in the functioning of the application?”

Answer: “Yes, the object identifier indication a Notarial Signature or an Official Certification Signature”

4.3.5.2.2 Signature format

Applications belonging to the model 1 are using XML-based signatures, at the exception of one.

Bulgaria - “Company Registration – submission of an application for company registration”

Question: “Which standards have been implemented in the eSignatures application?”

Answer: “The documents submitted to the Commercial Register could be signed separately and be enclosed and attached in file formats which include electronic signature (standardized format p7s - PKCS#7 standard)”

4.3.5.3 Model 2: ad-hoc model approach

4.3.5.3.1 List of applications belonging to the model

Country	Application/Service Name
Belgium	FINProf – declaration of income tax corporate prepayment - http://minfin.fgov.be/portail1/fr/finprof/welcomefinproffr.html
Croatia	PZZ - Primary Health Care Central System and application for general practitioners – G2
	e-zdravstveno
	On-line registration of supplementary insurance
	e-Tvrtka (e-Company)
	e-Porezna (translated e-TAX)
Czech	e-Pension (e-Mirovinsko)
	The information system on public contracts – publication subsystem
	Central repository for electronic drug prescriptions
	E-order for Payment Procedure

Country	Application/Service Name
	Tax portal (daňový portál)
	Government Gateway - DIS system
Denmark	ETHICS
Finland	eResepti (no web address available yet)
France	CPS card (Carte de professionnel de la santé)
	Real
	TéléTVA
	Télé-c@rte grise (http://impots.gouv.fr)
Germany	AI Tendering manager and AI Tending portal, AI Bidding Cockpit
	National Health Telematic Infrastructure
	Electronic input into the register of companies (administrated by courts in Germany) using the German EGVP system
Hungary	Online Web Auctioning (hereafter: OWL) Online Web Auctioning system, which applies electronic signature, authentic time-stamping and encrypted transactions over the Internet: https://owl.oep.hu
	Electronic Company Register www.ceginformacioszolgalat.irm.gov.hu
Iceland	Income Tax Declaration from accountants
Ireland	Revenue On-line Service (ROS). The system is accessible at www.ros.ie .
	Companies Office Registration Environment (CORE) e-filing available at www.cro.ie
Italy	'Acquisti in Rete della Pubblica Amministrazione' - www.acquistinretepa.it
	Processo Civile Telematico' - http://www.processotelematico.giustizia.it/pdapublic/index.jsp?sid=1&id=1&pid=1
Lithuania	Electronic Catalogue CPO.It™
Luxembourg	Declaration of personal income tax for 2008 http://www.impotsdirects.public.lu/formulaires/pers_physiques/2008/100F_2008_signature_electronique.pdf
Netherlands	TenderNed
	UZI card (UZI pas)
Poland	e-KRS
	EWD: Electronic exchange of data (social insurance documents).
	e-GIODO (http://www.giodo.gov.pl)
Portugal	e-Tendering – http://www.vortal-info.biz/vortalPT/Mercados/vortalGOV/tabid/57/default.aspx/
	CITIUS- https://citius.tribunaisnet.mj.pt/habilus/CitiusRegisto.aspx (project on civil procedures)
Romania	Tax Electronic Declarations (http://www.anaf.ro/public/wps/portal)
Slovakia	Electronic Public Procurement System EVO, www.evo.gov.sk
Slovenia	Electronic Procurement System (http://www.enarocanje.si/?podrocje=portal)
	Register of Wills http://www.notar-z.si/register_oporok.php
	http://www.registeroporok.si/pomoc/

Country	Application/Service Name
	https://www.registeroporok.si/
	One-Stop-Shop - State Portal for businesses (http://evem.gov.si)
	Intrastat (http://intrastat-surs.gov.si/)
	EPOS (e-business)
	Annual Reports
Sweden	ChamberSign
Turkey	National Judiciary Network Project - http://www.uyap.gov.tr/

4.3.5.3.2 Major differences observed

4.3.5.3.2.1 Use of specific application identifier in the certificate

Applications use information coming from the signature certificate to uniquely identify the user or its role.

Croatia - “e-zdravstveno”

Question: “Is there specific information in the certificate that plays a notable role in the functioning of the application?”

Answer: “Yes, the permanent unique identifier in the health insurance that is used as an identifier to grant access to the service.”

Italy - “Processo Civile Telematico”

Question: “Is there specific information in the certificate that plays a notable role in the functioning of the application?”

Answer: “The certificate includes: the name of the signer, the title of the signer (e.g. lawyer, judge) ...”

Turkey - “ National Judiciary Network Project”

Question: *“Is there specific information in the certificate that plays a notable role in the functioning of the application?”*

Answer: *“National register number in the signature certificate is used to determine the signatory's role.”*

4.3.6 Classification by country

This section provides a list of all the eGovernment applications grouped by country and then by model. It reflects that many countries are on the way of unifying their eGovernment approach from an ad-hoc model to an integrated model sharing the same infrastructure or the same framework.

Country	Model	Application/Service Name
Austria	1	@-AVA-Online® eTendering Platform of the Austrian Federal Railways (ÖBB)
		eHealth Directory Service (eHealth Verzeichnisdienst eHVD)
		CyberDoc (Urkundenarchiv der Notare)
		Criminal Record Certificate (Elektronische Strafregisterbescheinigung)
Belgium	1	e-Tendering - https://eten.publicprocurement.be/ Web Based Cancer Registry - https://www.kankerregistratie.be/wbcr/
	2	FINProf – declaration of income tax corporate prepayment - http://minfin.fgov.be/portail1/fr/finprof/welcomefinproffr.html
Bulgaria	1	Company Registration – submission of an application for company registration https://public.brra.bg/Internal/Registration.ra?0
Croatia	2	PZZ - Primary Health Care Central System and application for general practitioners – G2
		e-zdravstveno
		On-line registration of supplementary insurance
		e-Tvrtka (e-Company)
		e-Porezna (translated e-TAX)
Czech	2	The information system on public contracts – publication subsystem
		Central repository for electronic drug prescriptions
		E-order for Payment Procedure
		Tax portal (daňový portál)
		Government Gateway - DIS system
Denmark	2	ETHICS
Estonia	1	Generic eGovernment application
Finland	2	eResepti (no web address available yet)
France	1	Marches-public.gouv.fr
	2	CPS card (Carte de professionnel de la santé)
		Real
		TéléTVA
		Télé-c@rte grise (http://impots.gouv.fr)
Germany	1	eVergabe
	2	AI Tendering manager and AI Tending portal, AI Bidding Cockpit
		National Health Telematic Infrastructure
		Electronic input into the register of companies (administrated by courts in Germany) using the German EGVP system
Greece	1	SYZEFXIS - http://www.syzefxis.gov.gr

Country	Model	Application/Service Name
Hungary	2	Online Web Auctioning (hereafter: OWL) Online Web Auctioning system, which applies electronic signature, authentic time-stamping and encrypted transactions over the Internet: https://owl.oep.hu
		Electronic Company Register www.ceginformacioszolgalat.irm.gov.hu
Iceland	2	Income Tax Declaration from accountants
Ireland	2	Revenue On-line Service (ROS). The system is accessible at www.ros.ie .
		Companies Office Registration Environment (CORE) e-filing available at www.cro.ie
Italy	2	'Acquisti in Rete della Pubblica Amministrazione' - www.acquistinretepa.it
		Processo Civile Telematico' - http://www.processotelematico.giustizia.it/pdapublic/index.jsp?sid=1&id=1&pid=1
Lithuania	2	Electronic Catalogue CPO.lt™
Luxembourg	2	Declaration of personal income tax for 2008 http://www.impotsdirects.public.lu/formulaires/pers_physiques/2008/100_F_2008_signature_electronique.pdf
Netherlands	2	TenderNed
		UZI card (UZI pas)
Norway	1	eProcurement portal (No. eHandel) www.ehandel.no
Poland	2	e-KRS
		EWD: Electronic exchange of data (social insurance documents).
		e-GIODO (http://www.giodo.gov.pl)
Portugal	2	e-Tendering – http://www.vortal-info.biz/vortalPT/Mercados/vortalGOV/tabid/57/default.aspx/
		CITIUS- https://citius.tribunaisnet.mj.pt/habilus/CitiusRegisto.aspx (project on civil procedures)
Romania	2	Tax Electronic Declarations (http://www.anaf.ro/public/wps/portal)
Slovakia	1	eLegal Actions - Electronic Submissions to Courts (eŽaloby) - application is currently in preparation and development phase (pilot project)
		Electronic Services of Companies Register http://www.portal.gov.sk
	2	Electronic Public Procurement System EVO, www.evo.gov.sk
Slovenia	2	Electronic Procurement System (http://www.enarocanje.si/?podrocje=portal)
		Register of Wills http://www.notar-z.si/register_oporok.php http://www.registeroporok.si/pomoc/ https://www.registeroporok.si/
		One-Stop-Shop - State Portal for businesses (http://evem.gov.si)
		Intrastat (http://intrastat-surs.gov.si/)
		EPOS (e-business)

Country	Model	Application/Service Name
		Annual Reports
Spain	1	Plataforma de contratación del estado (State Contracting Platform) www.contrataciondelestado.es
		Tarjeta Sanitaria (eHealth card) https://sns.msps.es
		Historia Clínica Digital en el SNS (HCDSNS) – Patient medical record in the National Health System https://sns.msps.es
		Ensayos Clínicos de Medicamentos https://sinaem4.agemed.es/ecm/paginaPresentacion.do
		LexNet
Sweden	1	eINK, Personal income taxes declarations (Sw: Inlämning av självdeklarationsuppgifter)
	2	ChamberSign
Turkey	2	National Judiciary Network Project - http://www.uyap.gov.tr/

4.3.7 Classification by sector

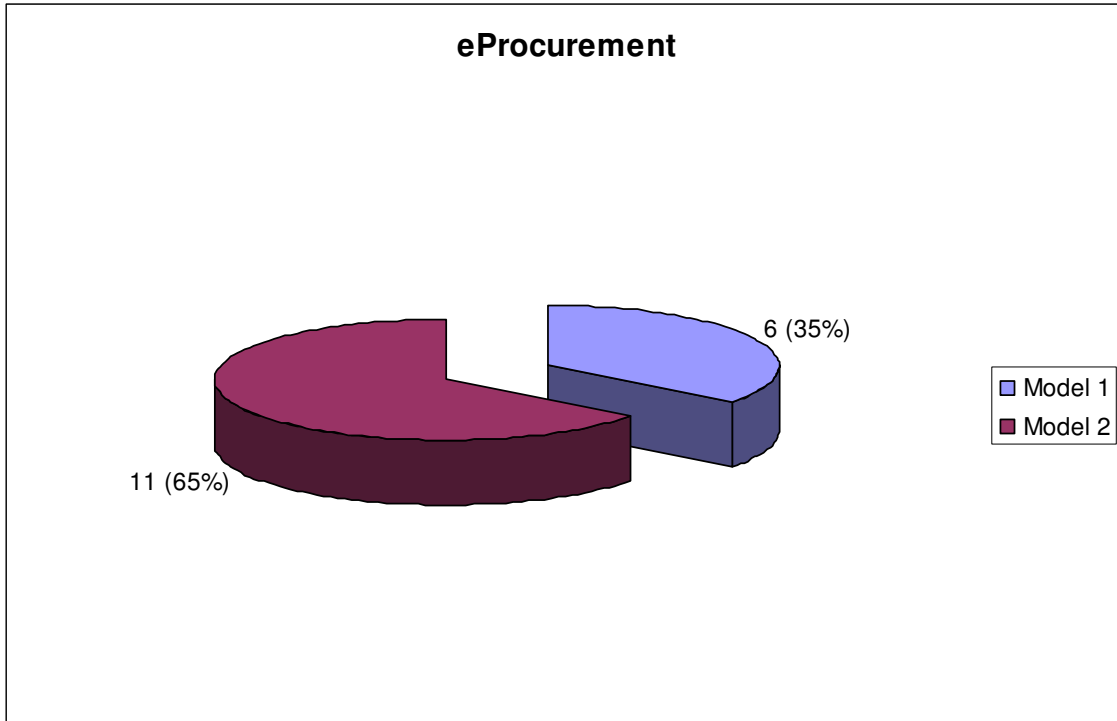
4.3.7.1 eProcurement applications

As reported by the national correspondents, the following signature types are required for existing eProcurement applications:

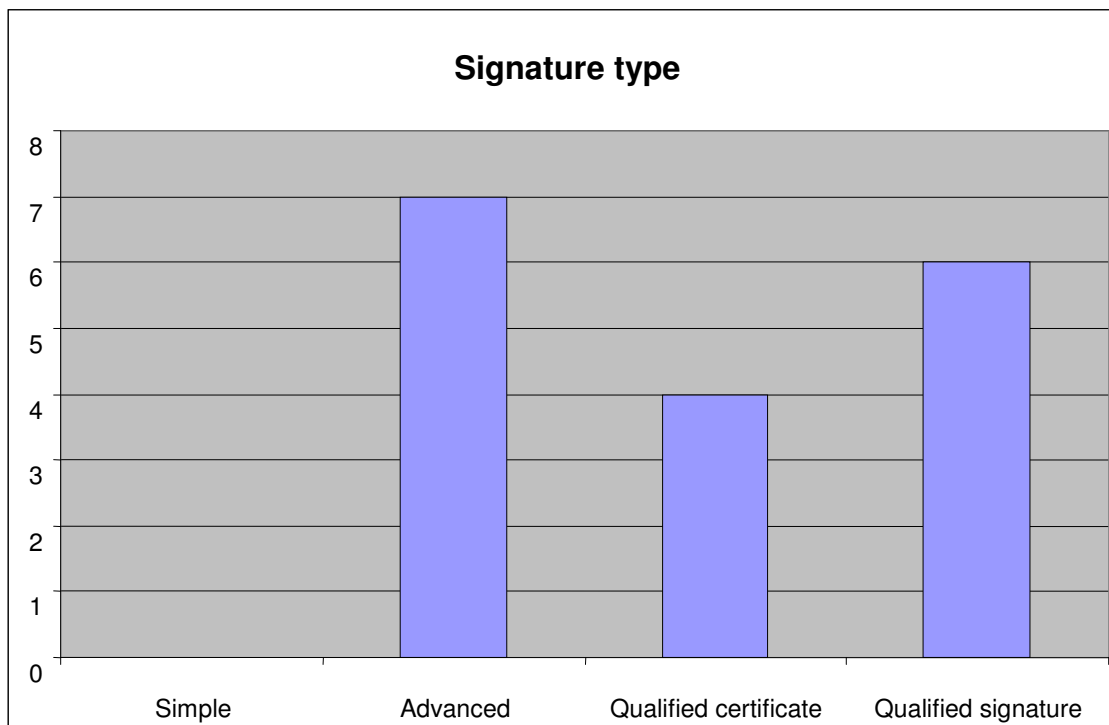
Country	Model	Signature requirements	Application/Service Name
Austria	1	Qualified signature	@-AVA-Online® eTendering Platform of the Austrian Federal Railways (ÖBB)
Belgium	1	Qualified signature	e-Tendering - https://eten.publicprocurement.be/
Czech	2	Advanced signature with qualified certificate	The information system on public contracts – publication subsystem
Denmark	2	Advanced signature	ETHICS
France	1	Advanced signature with qualified certificate	Marches-public.gouv.fr
Germany	1	Qualified signature	eVergabe
Germany	2	Advanced signature with qualified certificate	AI Tendering manager and AI Tending portal, AI Bidding Cockpit

Country	Model	Signature requirements	Application/Service Name
Italy	2	Qualified signature	'Acquisti in Rete della Pubblica Amministrazione' - www.acquistinretepa.it
Lithuania	2	Qualified signature	Electronic Catalogue CPO.lt™
Netherlands	2	Advanced signature	TenderNed
Norway	1	Advanced signature	eProcurement portal (No. eHandel) www.ehandel.no
Poland	2	Qualified signature	PPP, EPP, SAP, MP and PE
Portugal	2	Qualified signature	e-Tendering – http://www.vortal-info.biz/vortalPT/Mercados/vortalGOV/tabid/57/default.aspx/
Slovakia	2	Advanced signature	Electronic Public Procurement System EVO, www.evo.gov.sk
Slovenia	2	Advanced signature with qualified certificate	<u>Electronic Procurement System</u> (http://www.enarocanje.si/?podrocje=portal)
Spain	1	Advanced signature	Plataforma de contratación del estado (State Contracting Platform) www.contrataciondelestado.es
Sweden	2	Advanced signature	ChamberSign

The following figure depicts the classification by model of applications belonging to this sector.
The clear domination of model 2 follows the trend observed at the European level.



The figure below represents the signature type support by applications belonging to this sector.
0 applications support Simple signature type – 7 applications support advanced signature type – 4 applications support qualified certificate - 6 applications support "qualified" signature type.



Practically, the figures are the same as the ones observed in 2007.

4.3.7.2 eHealth applications

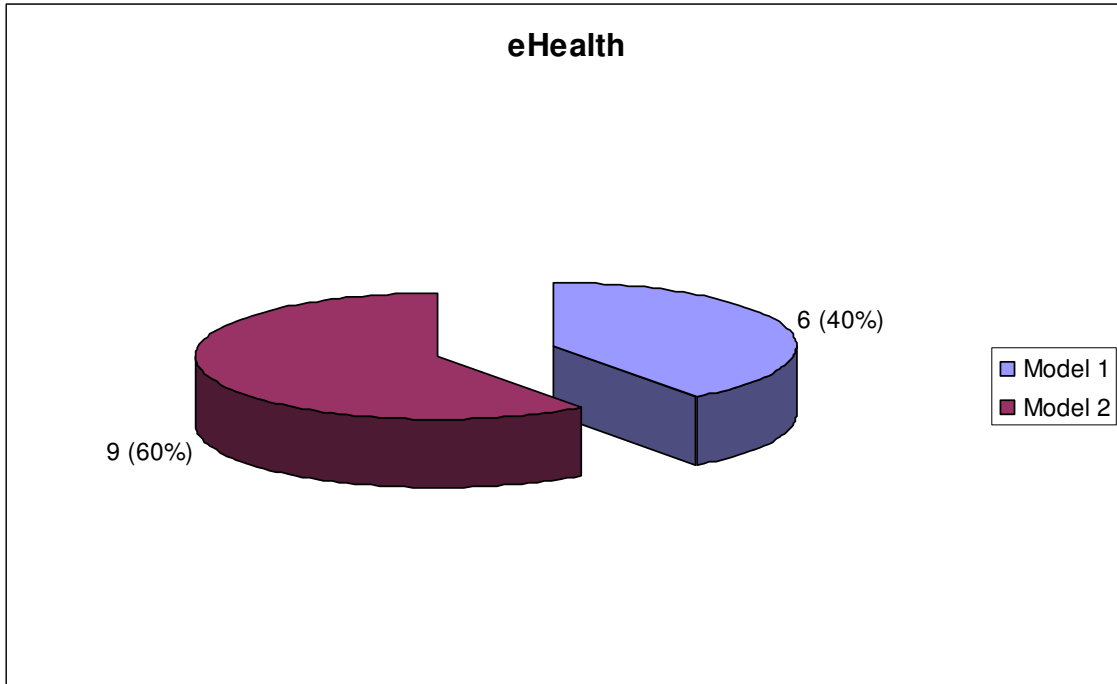
As reported by the national correspondents, the following signature types are required for existing eHealth applications:

Country	Model	Signature requirements	Application/Service Name
Austria	1	Qualified signature	eHealth Directory Service (eHealth Verzeichnisdienst eHVD)
Belgium	1	Advanced signature with qualified certificate	Web Based Cancer Registry - https://www.kankerregistratie.be/wbcr/
Croatia	2	Advanced signature	PZZ - Primary Health Care Central System and application for general practitioners – G2
Croatia	2	Advanced signature with qualified certificate	e-zdravstveno

Country	Model	Signature requirements	Application/Service Name
Croatia	2	Advanced signature with qualified certificate	On-line registration of supplementary insurance
Czech	2	Advanced signature with qualified certificate	Central repository for electronic drug prescriptions
Estonia	1	Advanced signature	Generic eGovernment application
Finland	2	Advanced signature with qualified certificate	eResepti (no web address available yet)
France	2	Qualified signature	CPS card (Carte de professionnel de la santé)
Germany	2	Qualified signature	National Health Telematic Infrastructure
Hungary	2	Advanced signature with qualified certificate	Online Web Auctioning (hereafter: OWL) Online Web Auctioning system, which applies electronic signature, authentic time-stamping and encrypted transactions over the Internet: https://owl.oep.hu
Netherlands	2	Qualified signature	UZI card (UZI pas)
Spain	1	Advanced signature with qualified certificate	Tarjeta Sanitaria (eHealth card) https://sns.msps.es
Spain	1	Advanced signature with qualified certificate	Historia Clinica Digital en el SNS (HCDSNS) – Patient medical record in the National Health System https://sns.msps.es
Spain	1	Advanced signature with qualified certificate	Ensayos Clínicos de Medicamentos https://sinaem4.agemed.es/ecm/paginaPresentacion.do

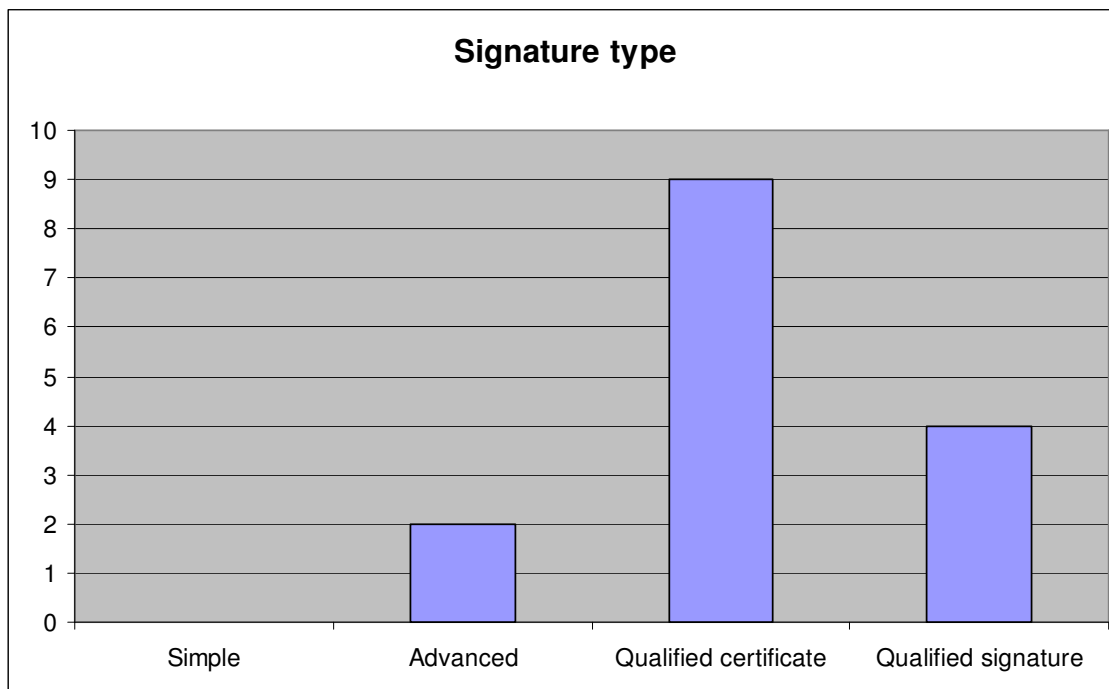
The following figure depicts the classification by model of applications belonging to this sector.

The general trend of European applications is also followed by applications belonging to this model.



The figure below represents the signature type support by applications belonging to this sector.

0 applications support Simple signature type – 2 applications support advanced signature type – 9 application supports qualified certificate - 4 applications support "qualified" signature type.



4.3.7.3 eJustice applications

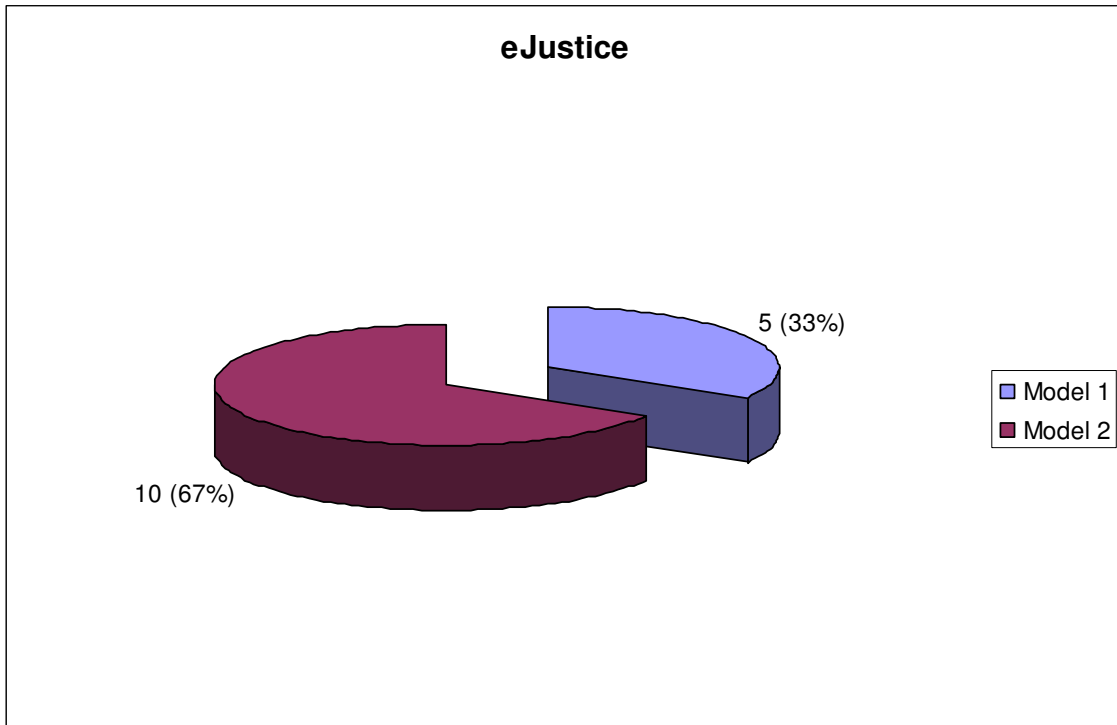
As reported by the national correspondents, the following signature types are required for existing eJustice applications:

Country	Model	Signature requirements	Application/Service Name
Austria	1	Qualified signature	CyberDoc (Urkundenarchiv der Notare)
Croatia	2	Advanced signature with qualified certificate	e-Tvrtka (e-Company)
Czech	2	Advanced signature with qualified certificate	E-order for Payment Procedure
Estonia	1	Advanced signature	Generic eGovernment application
France	2	Qualified signature	Real
Germany	2	Qualified signature	Electronic input into the register of companies (administrated by courts in Germany) using the German EGVP system
Hungary	2	Qualified signature; Advanced signature	Electronic Company Register www.ceginformacioszolgalat.irm.gov.hu
Italy	2	Qualified signature	Processo Civile Telematico' - http://www.processotelematico.giustizia.it/pdapublic/ind

Country	Model	Signature requirements	Application/Service Name
			ex.jsp?sid=1&id=1&pid=1
Poland	2	Qualified signature	e-KRS
Portugal	2	Advanced signature	CITIUS- https://citius.tribunaisnet.mj.pt/habilus/CitiusRegisto.aspx (project on civil procedures)
Slovakia	1	Qualified signature	Electronic Services of Companies Register http://www.portal.gov.sk
Slovakia	1	Qualified signature	eLegal Actions - Electronic Submissions to Courts (ežaloby) - application is currently in preparation and development phase (pilot project)
Slovenia	2	Advanced signature with qualified certificate	Register of Wills http://www.notar-z.si/register_oporok.php http://www.registeroporok.si/pomoc/ https://www.registeroporok.si/
Spain	1	Qualified signature	LexNet
Turkey	2	Advanced signature	National Judiciary Network Project - http://www.uyap.gov.tr/

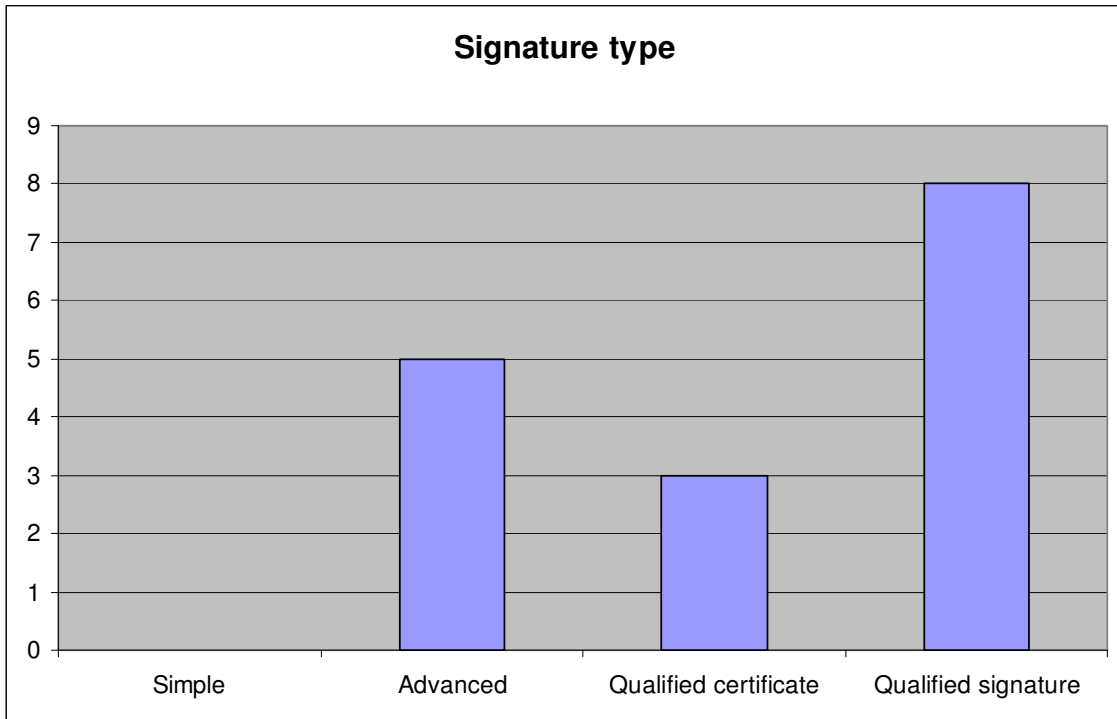
The following figure depicts the classification by model of applications belonging to this sector.

The clear domination of model 3 follows the trend observed at the European level.



The figure below represents the signature type support by applications belonging to this sector.

0 applications support Simple signature type – 5 applications support advanced signature type – 3 application supports qualified certificate - 8 applications support "qualified" signature type.



5 Impact Assessment

5.1 Introduction

The section above contained an in-depth examination of the available eSignature options in each of the 32 surveyed countries, the applicable legal framework (both in relation to eSignatures in general and more specifically in an eGovernment context), available applications, including supported signature types, mandates/authorisations and cross border accessibility (with a specific emphasis on eProcurement, eHealth and eJustice), and technical approach models. On the basis of this, an impact assessment of the similarities and differences for the eGovernment applications identified is provided below. The most important interoperability problems are listed.

5.2 Conceptual challenges in the eSignatures domain

As was already noted at several points above, there are several concepts which commonly lead to discussions at the national level. The next sections aims to clarify the definitions and the key understandings of some of these concepts.

5.2.1 Supervision vs. accreditation, and their role in determining the accessibility of eGovernment applications

As can be clearly seen in the applications descriptions above, application owners need to make certain choices when deciding which signature solutions they will support. Key considerations in this respect are whether they are technically capable of validating a signature, and whether they can determine its reliability¹¹⁷. In the current environment, it is not possible to open up most applications to any type of electronic signature, due to the complexity of addressing both of these questions, and the high costs and efforts that would be involved. It is therefore not surprising that most applications support only a limited set of signature solutions, which (almost) invariably are issued exclusively in the application owner's country. This is after all the only way that application owners can ensure that the signatures meet their requirements.

Supervision and accreditation schemes can play a major enabling role in managing the signature solutions supported in an application. However, it is important to recognise the fundamental differences between the goals and impact of both.

Article 3 of the Directive prohibits submitting the access to the market of certification services to any form of prior authorization (explicitly or via a "de facto" system). On the other hand the Directive requests the Member States to set up an appropriate system for the supervision of CSPs issuing qualified certificates to the public. The exact procedures for becoming supervised vary from country to country: in some countries, a mere notification is sufficient, whereas in others more in-depths assessments and verification procedures are required. None the less, the result is conceptually the same: qualified certificates are considered to meet certain requirements established in the Directive, and are legally equivalent.

¹¹⁷ In addition, there is of course also the crucial question of whether they are capable of identifying the signatory with a sufficient degree of certainty. However, as this is a question related to identity management, this will not be examined in detail in the present report.

This quality should make the qualified status a useful instrument to create interoperability. In practice, the possibility of recognising foreign qualified certificates as such is limited, due to the fact that lists of supervised CSPs are not always clearly and uniformly made available by the supervisory bodies. This specific issue will be addressed by a Commission Decision currently under consideration in the framework of the implementation of the Services Directive, which will require the Member States to ensure that such lists are made available in a common format. At that point, the interoperability (or rather, the practical cross border acceptability) of qualified certificates can be expected to benefit greatly. Until this time however, application owners have only limited possibilities of assessing the reliability of foreign qualified certificates, and interoperability is thus hampered.

Article 3 of the Directive also mentions the possibility to establish voluntary accreditation schemes. The objective of these schemes is to provide service providers with a possibility to obtain a quality label for their services. These voluntary accreditation schemes exist in roughly half of the surveyed countries (as noted above), and they are sometimes organised by the private sector (for example in the UK).

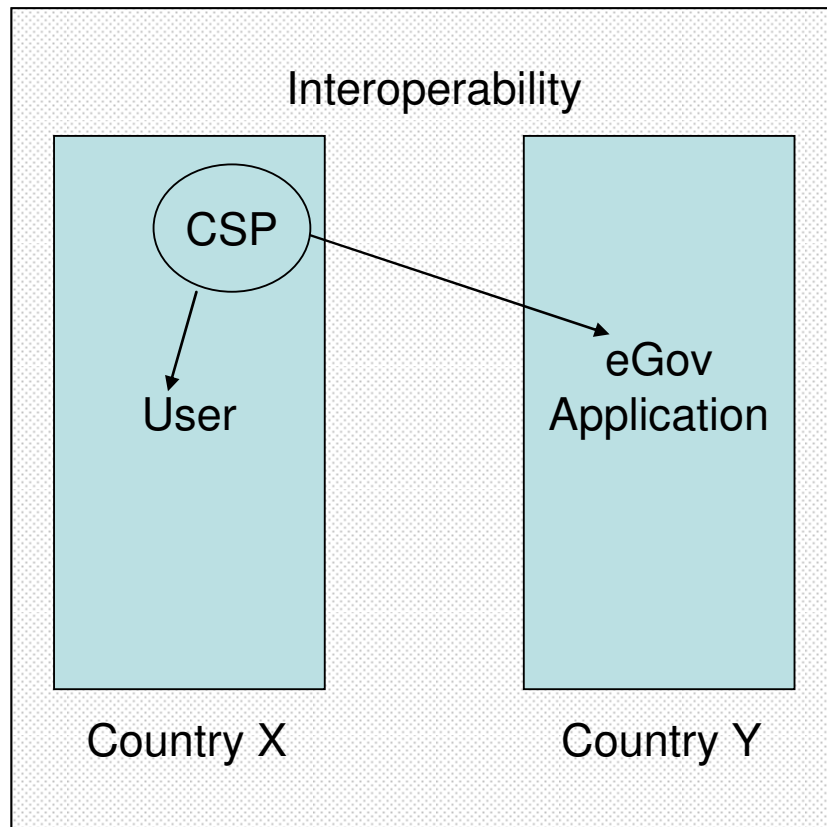
Obviously, and as envisaged by the Directive, these accreditation schemes are a purely national matter, with specific requirements and goals of the accreditation schemes varying quite broadly. This is not problematic as such, since voluntary accreditation was always conceived in the Directive as tool to enhance the level of service-provision (enhanced levels of trust, security and quality, as noted in recital 11 to the Directive), and not as a tool to support interoperability. However, the voluntary nature of accreditation schemes has always been stressed as a vital characteristic distinguishing them from prior authorization schemes, and that same recital 11 also noted that CSPs “should be left free to adhere to and benefit from such accreditation schemes”.

Various country profiles show that governments also use these accreditation schemes as a basis for determining the acceptability of an electronic signature in an eGovernment context. While it can still be argued that such accreditation schemes are still voluntary (in the sense that CSPs can choose to enter the general market for signature services without accreditation), it is clear that this depends entirely of how one defines the market. If the accreditation is mandatory in order to access the “market” for eGovernment applications, then the practical result can be the creation of new national barriers, as a CSP wishing to offer its services in larger markets (such as e.g. Germany, France or Spain) could find itself obliged to seek local accreditation or risk being kept out of the market for the simple reason that its signature solutions are not universally usable (being excluded from use in public sector applications).

One of the discussions is whether these practices are compliant with Art. 3.7 of the Directive (the so-called “public sector” clause), which allows Member States to “*make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens*”. In cases where accreditation has become a de facto requirement for the use of eSignatures in a given country’s eGovernment applications, it is questionable whether this restriction has still been observed. If the requirement to seek accreditation results in an obstacle to cross-border services for citizens, the public sector clause has clearly been violated. Given the considerations above, it seems that some countries have not respected the last restriction in the eGovernment/eSignature regulations.

5.2.2 Interoperability, specifically at the cross border level

One of the key questions raised in the application descriptions was the cross border accessibility of the application. The purpose was to ascertain whether applications could be used by non-nationals, and specifically whether this could be done without having to acquire signature solutions from another country, which would be an interoperability barrier. It is however important to distinguish the different components to this issue.



At the European level, full interoperability means that an eGovernment application of a given Member State should accept any (valid) electronic signatures sent by any natural or legal person from any other Member State even if the signature is created using credentials (certificates) issued by non-national Certification Service Providers (CSPs). Due to the issues mentioned above – the technical differences between signature solutions and the difficulty of determining the trustworthiness of foreign signatures – full interoperability currently does not exist in Europe. As many applications rely only on CSPs accredited by their own national accreditation body¹¹⁸ or with which they are sufficiently familiar, full interoperability would mean that either its own national accreditation body must be able to accredit non-national CSPs

¹¹⁸ The public or private body charged with the elaboration of, and supervision of compliance with, rights and obligations specific to the provision of certification services (cfr [RD3](#), Art 2 §13),

or that multilateral agreements must be established between accreditation Bodies from various Member States.

As mentioned above, many applications currently rely only on CSPs accredited by their own national accreditation authority. The application profiles show that they often claim to be open for cross-border use on this basis, meaning that non-nationals are expected to first apply for credentials from one of the accredited CSPs. Where qualified certificates are concerned, this means that non-nationals must physically appear in the country where the application is deployed. Obviously, while there is a theoretical possibility to use the application in this case, these circumstances can hardly be considered as ideal.

Among all surveyed applications, no application has been assessed as fully interoperable in the sense of the above definition. However, smaller scale forms of interoperability appear to have been achieved, in ways that were not yet the case in the previous edition of the study. These deserve further scrutiny.

5.2.2.1 True interoperability examples

The definition above referred to full interoperability as the capability of accepting any valid eSignature from another Member State. This is not yet currently a reality. Yet, some small examples exist where eGovernment services support signature solutions from another country. This is notably the case in Estonia, where the Company Registration Portal¹¹⁹ allows end users to establish a new company on-line. In addition to Estonian ID-card users, the portal is usable also to holders of a Portuguese, Belgian or Finnish ID-card or to holders of a Lithuanian Mobile-ID. Support for other cardholders is planned. The list is currently still limited due to the need to ensure the reliability of the signature solution and to eliminate technical issues, but cross border interoperability is a reality in this case. Similarly, as the Estonian CSP AS Sertifitseerimiskeskus is also active in the Lithuanian market (including through the Mobile-ID solution mentioned above), signatures from this CSP are also accepted in some Lithuanian eGovernment applications.

Similarly, some Austrian eGovernment applications (including the @-AVA-Online® eTendering Platform of the Austrian Federal Railways) have integrated a signature validation software module that allows signature solutions from other countries (notably eID cards from Belgium, Italy, and Slovenia) to be supported. Again, the list is currently limited and focused on relatively higher profile signature solution cases that are generally known to be trustworthy, but the fact that these examples exist shows that progress is indeed being made in the eSignature interoperability field.

Obviously, the currently ongoing initiatives – specifically in the context of the implementation of the Services Directive (the CROBIES study) and the PEPPOL large scale eProcurement pilot – can be expected to provide further good practice cases and thus contribute to these positive developments.

5.2.2.2 Cross border service provision – eSignatures as an export product

The examples above referred to concrete cases where foreign eSignature solutions were actively being supported by an application, and where interoperability was thus achieved. However, we are also seeing example cases where signature service providers from one Member State are exporting their products, services and/or know-how to other countries. Above, the example of Estonian CSP Sertifitseerimiskeskus offering its services in Lithuania – both through traditional certificates and through a mobile phone eSignature service - was already given. A second example was found in the recent introduction of the li.sign smart card in Liechtenstein. Here, the CSP issuing the qualified

¹¹⁹ <https://ettevotjaportaal.rik.ee/?chlang=eng>

certificates on the card is the FLZ Anstalt, a CSP from Liechtenstein, which is however a subsidiary institution of Austria CSP A-Trust. In both of these cases, the general know how of a high profile signature solution has been transplanted into another country's eGovernment context.

It should be stressed that these are of course not examples of interoperability, since they both relate to CSPs from one country who subsequently start offering their services in another country, rather than users from one country being able to use their signature solutions in another (although the latter is also possible to a certain extent in the Estonia/Lithuania case). None the less, they show that it is at least conceptually possible for services providers to develop their services across several countries. For completeness' sake however, it should also be noted that both examples relate to neighbouring countries which are thus more likely to have certain similarities in their cultural and legal attitudes towards electronic signatures, which in the case of Liechtenstein/Austria can be seen inter alia in the nearly completely identical legal framework. Such similarities do not exist between all European Member States, as could be seen in sections 4.1 and 4.2 of the report. Thus, similar eSignature export approaches are unlikely to be universally possible.

5.2.2.3 Interoperability and user groups

Finally, it should also be noted that for some applications, the importance of eSignature interoperability is not absolute. This has been witnessed inter alia in the eHealth and eJustice applications, where it was frequently seen that an application was accessible to anyone who was registered as a part of a profession in a given country (e.g. doctors registered as such with national health care departments, notaries public registered as such with their local organisations). In those cases, it should be stressed that the lack of interoperability with other solutions is meaningless if the application relate to a service which can only be provided by that user group. E.g. if patient files can only legally be accessed by health care professionals registered in a specific country, then it would be a meaningless exercise to build an application supporting this task with support for foreign eSignature solutions, as all persons who are entitled to use the application can easily obtain the appropriate credential.

In summary, cross border interoperability is an important factor in applications which are (or rather should be) open to end users from any country, such as e.g. eProcurement. Applications which are inherently only useful to end users in a specific country (which is frequently the case in strongly regulated professions, as can be seen in a number of eHealth and eJustice applications) benefit relatively little from such interoperability. This is of course not to say that eSignature interoperability is not important to the eHealth/eJustice sectors, but merely to clarify that it is important to assess on a case by case basis what the user base is, and to determine on the basis of this to what extent interoperability is beneficial or necessary.

5.2.3 Electronic signatures and the authentication of data and entities

A major and frequently recurring point of debate is the relationship between electronic signatures and authentication. In practice, it frequently occurs that a person is requested to authenticate himself in an e-government application, after which he may exchange certain documents freely and without any further technical steps. This method of proceeding (which is common in many countries, but which is particularly prevalent in e.g. the United Kingdom¹²⁰, the Netherlands¹²¹, Norway¹²² and Malta¹²³) is often signalled as an electronic signature, both by the national experts and by the public sector application owners. However, there is some debate as to whether or not such a process can be considered an electronic signature in the sense of the Directive .

A significant number of experts are of the opinion that this is the case. The reasoning behind this is typically twofold. First of all, it is clear that PKI processes are often¹²⁴ used to authenticate the user, with the same ultimate goal as a traditional username/password authentication process. Indeed, the identification of the signatory is one of the key benefits that an electronic signature offers over a hand written signature, since the use of a certificate allows the signatory to be identified (to the extent that the CA that issued the certificate is trusted, of course). Secondly, the Directive explicitly defines the electronic signature as 'data in electronic form which are attached to or logically associated with other electronic data *and which serve as a method of authentication*' (article 2.1, emphasis added). Thus, there is a legal basis for the link between authentication and e-signatures¹²⁵.

However, for the purposes of the present study, which focuses on the act of signing specific data and not on PKI processes in general, the 'authentication' process referred to in the Directive can in our view only refer to data authentication, understood as the corroboration that the origin and integrity of data is as claimed¹²⁶; and not to entity authentication¹²⁷.

We argue against the extension of the notion of a signature to include entity authentication processes, both for practical and for philosophical reasons. In legal practice, a signature has traditionally been only one of many ways in which a person can confirm his identity, express his consent, effect non-repudiation, and a myriad of other functions which are traditionally ascribed to signatures. The signature has been given a specific legal status in most jurisdictions, although other ways of obtaining the same legal result are usually (but not always) allowed. It is therefore not surprising that e-government applications would show the same degree of flexibility, and permit other solutions than

¹²⁰ Principally via the Government Gateway scheme; see <http://www.gateway.gov.uk/>

¹²¹ Principally via the DigiD scheme; see <http://www.digid.nl/>

¹²² Principally via the authentication solutions supported by the Alt-inn portal; see <http://www.altinn.no/>

¹²³ Principally via the eID solutions supported by the MyGov portal; see <http://www.mygov.mt>

¹²⁴ But not always; username/password systems are also in common use for lower security type applications.

¹²⁵ This perspective is also taken in the paper 'Regulating a European eID – A preliminary study on a regulatory framework for entity authentication and a pan European electronic ID for the Porvoo e-ID Group' by Thomas Myhr. See [http://www.fineid.fi/vrk/fineid/files.nsf/files/7431D844D1C359F9C225711F004553CB/\\$file/Thomas_Myhr_report.pdf](http://www.fineid.fi/vrk/fineid/files.nsf/files/7431D844D1C359F9C225711F004553CB/$file/Thomas_Myhr_report.pdf)

¹²⁶ See inter alia the Modinis eIDM Glossary, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc#4_5_1_Data_authentication

¹²⁷ See also the ELSIGN Study (The Legal and Market Aspects of Electronic Signatures report) in this regard. See http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation/

electronic signatures to serve the same function. This does not mean in our opinion that such other solutions can be readily considered to be signatures.

Indeed, if entity authentication could be said to be a form of signature on the grounds that it can obtain similar results, the traditional value attached to signatures in many legal frameworks would be in peril. After all, if one can be said to have electronically 'signed' a document after suitably secure electronic entity authentication, then it seems one must also accept that a paper document should be considered 'signed' if a person has merely handed it in after authenticating himself in another suitable fashion (e.g. after ID card verification, or simply after visual identification by someone familiar with the provider of the paper document). Paper documents should by this logic be considered 'signed', even if there is ostensibly no signature attached to the document. This is not the case: both in the paper and in the electronic context (as witnessed by the definition of the electronic signature in the Directive), a signature is always 'attached to or logically associated with' the signed document. The latter element should therefore be the deciding factor when determining whether an electronic signature in the sense of the Directive is used: whether or not the authentication information was attached to or logically associated with specific other data by the signatory with a view of signing it.

These considerations should of course not be interpreted to mean that entity authentication should not be considered as an invalid operating method in e-government applications, or indeed that we would consider it to be somehow inadequate or less suitable than an electronic signature. As in any other legal field, a signature has its purposes and its uses in e-government, but it should never be considered to be a requirement when a different solution offers the necessary guarantees. We merely wish to emphasise that in cases of pure entity authentication, we find that no signature is actually used, and that applications using purely entity authentication are therefore strictly speaking out of scope for this study.

This is also the opinion that was held tacitly or explicitly by most of the national correspondents and national experts. As a global indicator of this fact, we can refer to the tables in sections 4.1.7 and 4.1.8, which deal respectively with multi- and single factor authentication. The former list is quite short, and the latter nearly empty. None the less, it is clear that these solutions are highly common in most countries. Their systematic underreporting seems to be indicative of the fact that these solutions are indeed not seen in most cases as electronic signatures but as entity authentication tools.

Thus, the main driver behind entity authentication as a proxy for electronic signatures seems to be user friendliness and flexibility, rather than any philosophical or political preference. It has been noted by several experts that entity authentication is retained as a proxy for electronic signatures for the simple reason that it is considered 'good enough' in terms of safety and reliability, and that additional requirements would encumber the underlying processes excessively in a manner that would offer little added value.

5.3 Identified interoperability issues

The overview and analysis above has revealed the following interoperability issues. The objective of this list is to provide a first basis for a discussion in the perspective of future European strategies in this area..

5.3.1 National perspective in choosing signature solutions

5.3.1.1 Issue

It was already noted in the previous edition of the study that most of the surveyed countries, as far as they have adopted electronic signatures in their e-government applications, have organised this feature without taking into account electronic signatures solutions issued by CSPs in other countries. The regulatory, technical and organisational framework is always organised from a strictly national perspective. In most of the cases this national perspective is implicit. The application presumes that the user is a national living on the country's territory. In addition to all other kinds of practical obstacles that prevent other users to access and actually use the application, electronic signatures can in this way become an additional barrier.

5.3.1.2 Impact assessment

The impact of this issue is clear: when an application allows only signature solutions issued in the application owner's country, then the application is de facto only accessible across borders if end users obtain the appropriate credentials, which will frequently (but not always) mean physically going to the country in question to obtain this credential and/or to undergo any required registrations (e.g. in cases where the certificate needs to contain a national identifier). In practice, the application will typically be unusable across borders.

It was anticipated in the previous edition of the study that this strictly national perspective of most of the e-signature applications in the e-government sphere could be a temporary issue. Priority is first given to e-signature features for the large majority of the users. Serving more marginal categories, such as the occasional users from other countries, is not considered as a first priority. In addition, two years ago signature interoperability means (including cross border signature validation solutions) were not yet at a very advanced stage.

This has changed somewhat in the meantime, and in the section above we already noted some (very) limited interoperability initiatives reaching the deployment phase. We mentioned already the example of Estonia, where the Company Registration Portal¹²⁸ allows signatures created by Estonian ID-card users, but also a Portuguese, Belgian or Finnish ID-card or to holders of a Lithuanian Mobile-ID. In addition, some Austrian eGovernment applications (including the @-AVA-Online® eTendering Platform of the Austrian Federal Railways) have integrated a signature validation software module that allows signature solutions from other countries (notably eID cards from Belgium, Italy, and Slovenia) to be supported. In both cases, the list is currently limited and focused on relatively higher profile signature

¹²⁸ <https://ettevotjaportaal.rik.ee/?chlang=eng>

solution that are generally known to be trustworthy, but the fact that these examples exist shows that progress is indeed being made in the eSignature interoperability field.

5.3.1.3 Potential solutions and ongoing initiatives

The examples above show that some administrations are already working on the integration of foreign signature solutions, with a logical initial focus on signature solutions which are relatively known as secure, meaning in practice mostly official eID card based signatures. One of the key drivers behind this is of course the approaching implementation deadline of the Services Directive¹²⁹ and the end of 2009, which requires Member States to implement so called points of single contact (article 6 of the Services Directive). Through these points of single contact, service providers covered by this Directive should be able to complete electronically and at a distance:

(a) all procedures and formalities needed for access to his service activities, in particular, all declarations, notifications or applications necessary for authorisation from the competent authorities, including applications for inclusion in a register, a roll or a database, or for registration with a professional body or association;

(b) any applications for authorisation needed to exercise his service activities.

In many countries, this will imply the use of electronic signatures, and thus interoperability with foreign eSignature solutions. No doubt this has driven awareness of the importance of eSignature interoperability and spurred interest in working on this issue.

In addition, several high profile pilot projects are currently ongoing which are also examining the issue of signature interoperability, with the main example being the PEPPOL large scale pilot on cross border eProcurement¹³⁰. This pilot builds on the existing infrastructure and experiences gained at the national level in Germany, including notably through the VPS/Governikus signature validation platform approach¹³¹, which ensures that German signature solutions can already be validated with relative ease. These currently ongoing initiatives can be expected to provide further good practice cases and thus contribute to these positive developments.

Thus, there seems to have been a positive shift in the attitudes towards foreign signature solutions, in the sense that there is a strong awareness that a purely national focus on eSignature issues is not longer sufficient. None the less, there are substantial barriers still to be overcome before full eSignature interoperability becomes a reality. These will be further examined below.

¹²⁹ Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market; see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT>

¹³⁰ See <http://www.peppol.eu/>

¹³¹ See www.virtuelle-poststelle-bund.de, <http://www.bos-bremen.de/de/produkte/governikus/229415/>, and http://www.bsi.bund.de/fachthem/vps/common_vps.htm

5.3.2 Legal framework is based on concepts that are unique to a specific country

5.3.2.1 Issue

In sections 4.2.1. and 4.2.2. we examined the applicable legal frameworks in each of the surveyed countries, specifically as they related to eGovernment applications. This allowed us to identify some examples of terminological or real difference, where national laws established concepts which have no clear meaning at the European level, including (as noted above):

- Bulgarian law, which uses a definition of electronic signatures that corresponds substantially to the meaning of 'advanced electronic signature' under the Directive. The EDESA provides an alternative definition of the 'advanced electronic signature', which is in fact similar to that of the so-called qualified electronic signature. Finally, the EDESA introduced the concept of a universal electronic signature (UES), a type of advanced electronic signature (in the sense of the Directive) which is supported by a qualified certificate issued by a CSP registered in Bulgaria. The UES is the only type of electronic signature which has the effect of a handwritten signature in respect to everyone under Bulgarian law, unlike the basic and the advanced electronic signature which have such an effect only between private persons. In practice the UES is commonly required for the eGovernment needs. The UES is thus a uniquely Bulgarian concept.
- In the context of Croatian law, the advanced electronic signature is defined as being based on a qualified certificate.
- French law relies on a specific and comprehensive reference framework, rather than on the concept of qualified certificates/signatures. French CSPs can choose to be evaluated against the requirements of the "Référentiel Intersectoriel de Sécurité" (RGS), part of which was previously called PRIS (Politique de Référencement InterSectorielle, version 2). The RGS aims to define requirements applying to a series of security functions in information systems. It is mandatory for public agencies and for their service providers. Three levels of security are defined for each service: middle (*), strong/standard (**), and strengthened (***). CSPs/CAs may make use of this qualification among public or private application promoters, thus ensuring that the reference framework acts as a voluntary accreditation scheme. To be referenced, the CSP must be first be qualified for a service and for a security level, and secondly the certificate profile must be compliant with the one defined to ensure the interoperability with all online services requiring such type of certificates. The certificates issued for signature purposes at high signature*** level allow a signature to be obtained that is presumed to be reliable, within the scope of the eSignatures Directive, corresponding to the European ETSI and CEN standards which technically reflect the requirements of the European Directive on electronic signatures.
- Lithuanian law relies on the concept of the 'secure eSignature', which is identical to the notion of "advanced eSignature" used by the eSignatures Directive.
- Polish law is currently under revision. Among other points, it is being considered to introduce the term of advanced electronic signature, in the same sense as defined in the Directive. Current Polish law instead relies on the term 'secure electronic signature', corresponding roughly to an advanced signature created using an SSCD. Separate from this initiative, current draft regulations with regard to the planned Polish eID card envisage that the card will support so-called 'personal signatures', a new concept to be introduced. As personal signatures are

currently planned to be considered legally equivalent to hand written signatures, the European equivalent term would appear to be a qualified signature.

- Finally, Slovak law defines only the electronic signature based on asymmetric cryptography (digital signature) and does not define the technologically neutral electronic signature as defined in Art. 2.1 of the Directive. The advanced electronic signature according to the Directive was transposed into the Slovak legal system as an “electronic signature” (much as in Bulgaria) and the qualified electronic signature according to Art. 5.1 of Directive was transposed into the Slovak legal system as “guaranteed electronic signature (zaručený elektronický podpis - ZEP)”.

5.3.2.2 Impact assessment

As long as these are purely terminological issues, this situation may prove to be slightly confusing but ultimately harmless, since signature interoperability will ultimately require that solutions are implemented which automatically assess the adequacy of a signature, and end users will never be expected to actually familiarise themselves with these national concepts anyway. However, if these categories take up such a fundamental role in eGovernment processes that it becomes impossible or unreasonably complex to determine whether a foreign signature meets the applicable requirements, there is a real risk of these diverging concepts becoming a barrier to cross border interoperability. This can in particular be the case when national laws require the use of a signature type which is unknown at the European level. This issue will be examined further below.

5.3.2.3 Potential solutions and ongoing initiatives

There is no objection against the creation of specific national concepts, and in some cases (like e.g. the French Intersectorial Reference Framework (*Référentiel Intersectoriel de Sécurité*) they can be considered as highly developed and useful examples of a voluntary accreditation scheme. However, national policy makers must be aware that national signature concepts (or national accreditation schemes) can also become interoperability barriers when national policies and laws become too strongly linked to these concepts and schemes, to the extent that foreign signature solutions can no longer enter the market. In that respect, policy makers must make sure that their national regulatory concepts and schemes do not create interoperability barriers towards foreign eSignature solutions. This is not merely a matter of principle, as adverse policies could also be contrary to the eSignature Directive’s rules in relation to prior authorization and the public sector clause (article 3.7). This issue will be further examined below.

5.3.3 Legal framework contains requirements that cannot be met by foreign solutions

5.3.3.1 Issue

Sections 4.2.1. and 4.2.2. contained some examples of national eSignature/eGovernment regulations aimed towards facilitating national interoperability (i.e. information exchange between services within a country) and/or improving the quality of service, but which may none the less result in interoperability barriers at the European level. As already referenced above, it will be recalled that examples of this include:

- **Bulgaria:** The Bulgarian eGovernment Act provides the possibility for the addressees of eGovernment services to make electronic statements and to send them electronically. Pursuant to Bulgaria law the state and municipal authorities are not only obliged to accept electronic documents signed with a universal electronic signature (UES) and submitted electronically but also to issue official administrative documents in electronic form if such documents are requested by citizen or representative of a legal entity. These documents also must be signed with UES. As was noted above however, the UES is a type of advanced electronic signature which is supported by a qualified certificate issued by a CSP registered in Bulgaria. Thus, non-Bulgarian signatures typically will not qualify for this status. Given that the UES is commonly required in eGovernment applications, this may be a legal interoperability barrier.
- **Czech Republic:** the eSignatures Act states that in the public sector an advanced electronic signature based on a qualified certificate issued by an accredited CSP must be used. For the communication with the public administration the certificate has to contain a social security number. This identifier is stored in the information system of the state social assistance managed by the Ministry of Labour and Social Affairs. Obviously, foreign certificates will not contain a social security number, meaning that foreign signature solutions will generally not be able to meet this requirement.
- **Italy:** the Code of the digital administration (Article 65) requires that all requests and declarations sent to public authorities are valid if:
 - They are signed with a digital signature whose certificate has been issued by an accredited certification-service-provider;
 - When the user is identified and authenticated through the use of the EIC or the national service card;
 - When the user is identified and authenticated through other systems adopted at the local level.

All of these options however rely on the use of local solutions: CSPs accredited in Italy, Italian smart cards, or systems used by local Italian administrations. Again, foreign signature solutions therefore appear to be excluded.

It should be stressed that the approaches above all serve the legitimate purpose of ensuring the reliability of electronic signatures being used (in all three countries), and of being able to easily identify the signatory in an automated fashion that allows the development of advanced eGovernment services (in the Czech Republic, where the social security number enables this).

In addition, it should be pointed out that these situations in which national solutions are strongly favoured or even supported exclusively are not at all exceptional. The reason that the examples above are mentioned is that their general eGovernment laws are more explicit in this respect. In many other countries (e.g. those using eID cards as listed above) the situation is highly similar, but not enforced through horizontal eGovernment regulations (as with the example above), but rather through vertical (application or sector specific) regulations, e.g. a public procurement act requiring that a national eID card is used.

5.3.3.2 Impact assessment

In these cases, regulations may result in an impossibility of using foreign signature solutions. It should be stressed however that this is only the case if the regulations explicitly contain a requirement to use a specific solution as a precondition for specific service, and not if they merely support the use of a national solution. The distinction is important: there is no objection to establishing an approach to eSignature (including the use of specific identifiers or a voluntary accreditation scheme) with a view of ensuring that these solutions are easily identifiable to end users as a good option or with a view of ensuring a higher quality of service. However, when the approach results in the strict or de facto exclusion of foreign signature solutions, this can present a real problem.

In those cases, such restrictions must be considered as applications of Article 3.7 of the eSignatures Directive (the so-called public sector clause), which allows Member States to “make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.” In cases where cross-border services for citizens are legally made impossible or unreasonably complicated (e.g. because they de facto have only the option of acquiring a signature solution issued in another Member State), then the regulatory restrictions appear to be in violation of the public sector clause.

The same considerations apply *mutatis mutandis* to accreditation schemes. Various country profiles show that governments also use these accreditation schemes as a basis for determining the acceptability of an electronic signature in an eGovernment context. It was already observed above that the question of whether or not these schemes can still be considered voluntary often depends entirely of how one defines the applicable market. If the accreditation is mandatory in order to access the “market” for eGovernment applications, then the practical result can be the creation of new national barriers, as a CSP wishing to offer its services in larger markets (such as e.g. Germany, France or Spain) could find itself obliged to seek local accreditation or risk being kept out of the market for the simple reason that its signature solutions are not universally usable (being excluded from use in public sector applications). This was clearly not the intent of accreditation schemes, and usage of voluntary accreditation schemes to artificially restrict access to eGovernment applications through legal means would be contrary to the eSignatures Directive.

5.3.3.3 Potential solutions and ongoing initiatives

Member States should be aware of the letter and spirit of the public sector clause, and especially the limitation that additional requirements may not constitute an obstacle to cross border services for citizens. It should be noted that the systematic use of voluntary accreditation schemes to can also be a

violation of the public sector clause. It should therefore be ensured that regulations at the national level do not needlessly establish such barriers. Member States must be aware of the fact that the principles of non-discrimination and equivalence to handwritten signatures should also apply to eGovernment applications, unless the public sector clause allows them to decide otherwise.

Obviously, it should be recognised that the elimination of such regulatory barriers is not a solution to all eSignature interoperability barriers, and it is clear that regulations are only one small piece of the puzzle. However, Member States should be aware that regulatory restrictions may in time become part of the problem, when technical and organisational interoperability solutions have been developed. For this reason, it appears to be prudent to recommend national policy makers to examine whether their legal frameworks are sufficiently adapted to support cross border signature interoperability solutions such as those already deployed in Estonia and Austria, or piloted by the PEPPOL project amongst others.

5.3.4 Interpretation of the European legal framework

5.3.4.1 Issue

The eSignatures Directive can be credited with the creation of the basic regulatory framework for the use of electronic signatures at the European level. It has established many of the main building blocks, but it can also be noted that some concepts leave a margin of interpretation that results in cross border interoperability barriers.

The primary example identified in this study is the conceptual confusion behind qualified certificates. In the Directive, a 'certificate' in general is linked to a *person*, whereas the 'qualified certificate' refers to the *signatory*. The notion of a person is not defined in the Directive, but due to its frequent references in several provisions to 'legal or natural persons', it is generally accepted that this concept covers legal persons (most notably companies) as well. In contrast, the notion of signatory is defined in Article 2.3 as "a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents." This has caused much debate as to whether a qualified certificate can be issued to legal persons.

It was noted in section 4.2.3 that differences in interpretation exist between the Member States with respect to the question of whether qualified certificates can be issued directly to legal persons without identifying a specific natural person as the authorised certificate holder. This will create a very real interoperability barrier in the future, especially in the context of the Services Directive, where it can be anticipated that e.g. an Estonian company will use a qualified signature solution (or more accurately, a digital stamping solution) issued by an Estonian CSP to meet the requirements of a country whose laws require the use of a qualified signature. While the company's signature will be considered a legally valid signature under Estonian law, this may not be the case in other countries that do not acknowledge the concept of a qualified signature created directly by a company. This is an issue that would need to be clarified at the European level.

Other examples of differing interpretations exist as well. To some extent these are simply due to the margin of appreciation left by the Directive, and therefore do not (or rather should not) create specific

interoperability concerns. The question of supervision of CSPs issuing qualified certificates to the public is one example in this respect: while a supervision regime has been established in each country, the exact modalities (and the resulting real reliability) of these regimes vary substantially. In principle this is not a problem: the Directive merely requires that supervision regimes must be 'appropriate' (article 3.3 of the Directive), without specifying the criteria to determine when a regime should be considered as such. While it is clear that the cross border validity of qualified signatures can a priori not be challenged on the basis that a foreign supervisory regime has not been found 'appropriate', it goes without saying that the cross border trustworthiness of supervision regimes could benefit from an improved exchange of best practices or more tangible guidelines.

A third and more significant example of differing interpretations can be found in the concept of secure signature creation devices (SSCDs), defined in the Directive as a signature-creation device which meets the requirements laid down in Annex III to the Directive. The different interpretations in this case relate to the provision of Article 3.4, stating that "*the conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States.*" Some Member States (e.g. Germany) have interpreted this provision to mean that a formal assessment process is always necessary to determine whether the requirements of Annex III have been met (e.g. because the requirements of Commission Decision 2003/511/EC¹³² have been met), whereas other countries (e.g. Belgium) consider that such an assessment could serve to remove any doubt but is not strictly required.

Up to this point, there have been relatively few discussions on this point, given that there was a multitude of other blocking factors stopping the effective cross border interoperability of electronic signatures. However, as other issues are increasingly being addressed, this is likely to surface as another point of discussion, specifically because market distortions can occur if these differences in interpretation remain. After all, if these different requirements in relation to an SSCD are tolerated, then an entrepreneur who wishes to establish a CSP using SSCDs for signature creation will likely choose to set up his operations in which lengthy and costly assessments are not needed, and thereafter claim that his solution meets national requirements and should therefore be accepted at the European level. While this is not harmful with respect to interoperability, this seems undesirable from an internal market perspective.

5.3.4.2 Impact assessment

The different impacts of these interpretations have been outlined briefly above:

- For the qualified certificate issue, real problems may occur in the sense that signatures which are recognised as being qualified signatures in one country may not be given the same status in the next. This is a fundamental problem, given that the improved legal reliability and interoperability status is one of the advantages that a qualified signature is supposed to enjoy. It is also worth repeating that this is an important issue in the context of the Services Directive, where companies can be expected to be a large part of the target group of service providers who are supposed to benefit from the implementation work.

¹³² Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council

- For the supervision issue, if the differences in supervision criteria are too great, then this may impact the credibility of the supervision system, and thus of the trust model behind the Directive. While this is not a strictly legal interoperability barrier, de facto trust concerns can play a substantial disruptive role.
- Finally, for the notion of SSCDs, it is not impossible that the legal value of existing signature solutions will be challenged in the future based on the diverging interpretations on the necessity of conformity findings.

Thus, there is a real interoperability threat connected to these diverging interpretations.

5.3.4.3 Potential solutions and ongoing initiatives

Most of the issues outlined above are already known, and are being addressed to some extent by existing initiatives, most notably in the context of the supporting initiatives accompanying the national implementation work of the Services Directive, specifically through the CROBIES study. These efforts include the establishment of national trusted lists of supervised CSPs (to be coordinated at the EU level) and the establishment of supervision criteria.

The latter action will obviously have a positive impact on the diverging supervision regimes that currently exist, whereas the former (national trusted lists) will have an indirect impact on the qualified certificate and SSCD issues. The current proposal for the national trusted lists envisage the possibility for including qualified certificates issued to legal persons on this list and marking them as such, so that recipients of signatures created using such signatures will be able to identify them as originating from a legal person. Similarly, the trusted list will contain an indication of whether or not the certificate is considered to be supported by an SSCD under the national interpretation of the Directive.

However, it is clear that this approach is not intended to address the two fundamental questions:

- Can a legal entity obtain a qualified certificate, and thus create qualified signatures?
- Is it necessary for a signature creation device to undergo a conformity assessment before it can be considered an SSCD?

With regard to the first question, the trusted list approach allows the recipient to determine whether the signature was created by a legal person, but still leaves the issue of the legal value of such a signature open to national conflicts. This may not be a crucial point in circumstances where a qualified signature or an advanced signature based on a qualified certificate is not legally required, but can prove to be decisive in applications where these are in fact mandatory.

Similarly, the trusted list will allow a recipient to obtain an answer to the question if the signature creation device is considered to be an SSCD in the issuer's country, but not necessarily if this is adequate from his own country's regulatory perspective. This need not be an interoperability issue as long as Member States would agree to respect each other's interpretation of the notion of an SSCD, i.e. Member States accept that a signature creation device can be considered an SSCD if it can be considered as such in the country of establishment of the issuer; but there appears to be little legal basis for such a flexible attitude, which would in addition creation internal market concerns, as noted above.

Fundamentally, the two questions of qualified certificates issued to legal persons and of the need for a conformity assessment for SSCDs can only definitively be settled through an official European ruling on the correct interpretation of the Directive, e.g. from the Court of Justice.

5.3.5 European framework implicitly favours certain types of signatures

5.3.5.1 Issue

While this issue has not been acknowledged with explicitly so far, it is clear that most of the comments above pertain specifically to signatures based on qualified certificates (i.e. advanced signatures based on qualified certificates and qualified certificates). The reason for this is that the current trust model of the Directive is substantially linked to this concept: trust in the signatures can be determined due to the fact that qualified certificates share common requirements (Annex I of the Directive), as do the CSPs issuing such certificates to the public (Annex II of the Directive), and compliance is supervised by specific supervisory bodies with a national mandate under Article 3.3. The system is admittedly imperfect, notably due to the fact that it is currently still hard to determine if a CSP is in fact supervised (due to the current lack of harmonised national lists of supervised CSPs) and how reliable this supervision scheme is; but both of these elements are currently being worked on in the course of the aforementioned CROBIES initiative. Once finalised, the trust model behind signatures based on qualified certificates will thus be relatively comprehensive and complete.

However, this progress is not as meaningful for other electronic signatures, specifically advanced signatures which are not based on qualified signatures or basic ('simple') signatures. In this case, the building blocks are fundamentally different: there are no common criteria to determine their reliability, no requirements in relation to CSPs (insofar as CSPs are involved, which is not necessarily the case for simple signatures), and no supervision model to ascertain whether such requirements are followed. While accreditation schemes fill this trust void to a certain extent, such schemes are currently established at the national level and offer little opportunity for cross border interoperability.

5.3.5.2 Impact assessment

Realistically, it is clear that little progress has been made in relation to the interoperability of signatures which are not based on qualified signatures, and that no short term progress can be foreseen, due to the fact that the aforementioned basic building blocks to establish trust are missing. Barring further initiatives at the European or otherwise cross border level, it seems doubtful that any large scale interoperability is possible for these signature types in the short term.

5.3.5.3 Potential solutions and ongoing initiatives

The main way of addressing this issue is to ensure that the building blocks which exist for qualified certificates (requirements in relation to certificates and CSPs, and the assessment of compliance with these requirements) are given a reasonable equivalent in the nonqualified sphere.

This issue is currently being examined further in the context of the ongoing European Federated Validation Service (EFVS) study, and will not be dealt with in this report in detail. Broadly speaking

however, it is clear that there is a need for a more comprehensive normative framework for these types of signatures to define the applicable requirements (if desired by distinguishing multiple tiers/levels of these requirements), and for a governance framework to ensure that compliance with these requirements can be verified at the cross border level, e.g. through validation services or through a more systematic use of the voluntary accreditation model.

5.3.6 Incompleteness of the European legal framework

5.3.6.1 Issue

This study focuses on one specific type of trusted third party (TTP) service, namely that of electronic signatures, and other TTP services are out of scope of this study. None the less, it is worth referring to the analysis in section 4.2.2 and 4.2.3, which noted that some countries have opted not to address the issue of electronic signatures in isolation, but have instead considered that it would be advisable to place this in a broader framework of certification services regulations. Examples included:

- The recently revised Slovakian regulatory framework, with other examples including the German, Estonian and Czech legal framework (all of which include provisions in relation to e.g. timestamping, in the German and Czech case even defining qualified timestamping). The Slovak regulatory framework in addition contains provisions for an archive electronic signature and an accreditation for long term electronic document storage. Finally, the reforms also created so called mandate certificates (certificates for the people with special position, such as judges, notaries, lawyers, solicitors etc.). The mandate certificate allows to determine the legal capacity in which a person is signing a document. The law introduced also the obligation of certification holder or the company or organisation that represents to notify to the CSP any change of his legal capacity and subsequently to apply for revocation of the mandate's certificate. An obligation was also introduced to state a birth number in qualified certificates that will be used in contact with public state administrative bodies. Thus, issues of identity management have also been addressed to some extent by these reforms.
- The same can be seen in Finland, where ongoing regulatory reforms envisage establishing a legal framework for electronic (entity) authentication, noting that the use of PKI certificates for authentication has remained in a legislative "no-man's-land". The proposal intends to clarify roles, requirements and obligations for all organisations that are and will offer services for strong electronic authentication, in the same model as has been already implemented for Qualified Certificate Service Providers.
- Other countries like Italy can similarly look back on a long tradition of regulation supported by clear technical standards, including in relation to e.g. electronic registered mail.

In these countries, electronic signatures were seen as implicitly linked to other TTP services which would be necessary to unlock the full potential of electronic signatures. These national regulations in relation to time stamping, long term archiving, electronic registered mail, identity management and authorisations seem to indicate that there is a certain normative gap to be filled, in the sense that each of these services would require a legal framework to ensure their trustworthiness to end users. On the other hand, the fact that these initiatives are taken at a strictly national level means that there is a risk of disparities emerging in the European market.

5.3.6.2 Impact assessment

It should be stressed again that TTP services other than electronic signature are strictly speaking out of scope of this study. None the less, all of these examples of TTP services are also linked to the use and value of electronic signatures. E.g. time stamping can be a useful tool to determine at which time the validity of a document was assessed and confirmed; electronic archiving can ensure that the integrity and authenticity of a signed document can be determined even when the validity of the signature can no longer be determined; and the issue of identity management is crucial to be able to link the signature to the signatory. However, all of these services lack a European framework, and in some cases national regulations are stepping in to fill the gap. This creates a risk of interoperability gaps when national regulations begin to diverge.

Specifically in relation to identity management, we saw earlier that electronic signatures are frequently linked to national unique identifiers. They are used to initiate the process for the application of a certificate or inserted in the subject field of the certificate. The processing of these unique identifiers is sometimes strictly regulated (e.g. reserved for designated authorities or service providers), and current national rules in this domain generally do not take into account data processing by public authorities or service providers of other Member States. Solutions will have to be developed in the framework of e-ID interoperability. This may include legislative amendments in some of the surveyed countries.

5.3.6.3 Potential solutions and ongoing initiatives

Due to the large number of TTP services, a large number of European initiatives is potentially relevant. The STORK pilot project will obviously provide useful inputs on addressing identity management issues at a cross border level. Similarly, the CROBIES study will touch on this issue through the "Common Minimum Requirements for a Qualified Certificate Profile supporting Qualified Electronic Signatures"; however, the efforts in this field do not relate primarily to questions of identity management as applied to the signatory but rather to the content and structure of the certificate as a whole. Within the context of the EFVS study, it will also be examined to what extent existing validation services address these points, and what European initiatives (if any) might be needed to support these services.

5.3.7 Prevalence of ad-hoc solutions with limited interoperability perspectives

5.3.7.1 Issue

Not all Member States have adopted a general all-encompassing central strategy with regard to electronic signatures in e-government applications. There are many ad-hoc solutions and regulations in this domain, especially in countries which do not favour strong PKI based approaches. This fragmentation can possibly hinder future interoperability initiatives.

5.3.7.2 Impact assessment

This might be a temporary issue. In most of the surveyed countries the sectoral “ad hoc” approach seems to be a first phase in the development of transactional e-government services. Sectoral “ad hoc” solutions are implemented because there is not yet a clear strategy on the national level.

However, as was noted above, it’s also clear that for some applications the importance of eSignature interoperability is not absolute. In those cases, it should be stressed that the lack of interoperability with other solutions is meaningless if the envisaged user group can easily gain access to the appropriate signature solutions. Cross border interoperability is an important factor in applications which are (or rather should be) open to end users from any country, such as e.g. eProcurement. Applications which are inherently only useful to end users in a specific country (which is frequently the case in strongly regulated professions, as can be seen in a number of eHealth and eJustice applications) benefit relatively little from such interoperability. This is of course not to say that eSignature interoperability is not important to the eHealth/eJustice sectors, but merely to clarify that it is important to assess on a case by case basis what the user base is, and to determine on the basis of this to what extent interoperability is beneficial or necessary.

5.3.7.3 Potential solution and ongoing initiatives.

In our opinion, no corrective action in this regard is necessary. While it is true that national diversity between e-government applications currently exists and will likely continue to exist for some time, it is important to note that all Member States acknowledge that a lack of interoperability in ‘open applications’ (i.e. those which should be accessible to a broad user group covering multiple countries) is a serious handicap that needs to be eliminated. In short, while the existence of ad hoc solutions can be a barrier to cross border interoperability, Member States are by and large acting to remedy this situation, so that no further action seems necessary.

5.3.8 Incompatible use of certificate attributes

5.3.8.1 Issue

This issue concerns signatures based on certificates where the application requires the certificate to contain a specific attribute. In the previous study, the problem was already identified as “Incompatible use of identifiers” which could be National/Sectoral/Regional unique number.

The issue can be considered as more important today. Indeed, the new sectoral applications considered above, especially in the eHealth and eJustice sectors, often require the signature certificate to contain a specific attribute allowing the identification of the role of the signatory (e.g. nurse, doctor, judge, lawyer, notary ...).

This new application requirement imposes, by essence, new barriers to the interoperability of eSignatures. Mainly for two reasons: first because there is no standardisation on the attribute which might be used by application to identify the role of the signer, and secondly because there is no standardisation on the values that such attributes may contain. Regarding the values of these attributes, the language is again another barrier. Indeed, is “lawyer” equivalent to “advocaat” or “Rechtsanwalt”?

Finland “eResept”

“The VALVIRA certificate contains the medical professionals TERHIKKI register number and an extension describing the cardholder’s professional role. “

Germany “Electronic input into the register of companies using the German EGVP system”
“Attribute “notary”“

Hungary “Electronic Company Register”
“The certificate includes: the name of the signer, **the title of the signer (e.g. lawyer, judge)**, in case of lawyers it contains the **regional chamber of lawyers**, and the **registration number of the lawyer within that chamber**, the name of any organization they are affiliated with country and locality codes. “

Turkey “National Judiciary Network Project”
“National register number in the signature certificate is used to determine the signatory’s role. “

5.3.8.2 Impact assessment

The incompatible use of certificate attributes, being either a unique identifier or role identifier, is definitely an interoperability problem for the affected applications.

Nevertheless the analysis of the survey has found 69 applications that make use of eSignatures. Among these 69 applications 15 require a unique identifier to be present in the certificate and among these 15 only 2 applications have been assessed as opened to non-national persons.

5.3.8.3 Potential solution and ongoing initiatives

This issue concerns signatures based on certificates where the application requires that a specific field of the certificate contains a specific National/Sectoral/Regional unique number because there is a clear need for applications to identify the signatory of a document.

Similarly, other applications require the certificate to contain an indication about the signer’s role (lawyer, doctor ...).

The easiest and most often used way to achieve this identification is to insert a unique identifier / role identifier in the certificate, but this has a great impact on the possible interoperability of the application.

In the paper-based world, identification data on official documents (e.g. tax declaration, prescriptions ...) are part of the document itself (specific fields) and are certainly not deduced from the handwritten signature. Why should this be different in the electronic world?

In order to avoid building barriers to interoperability, policy makers in the Member States should carefully assess whether there is any need for the mandatory use of specific fields/values in the certificates, and what the interoperability impact of their design decisions will be.

5.3.9 Signature Type enforcement

5.3.9.1 Issue

Technically, there are two ways for the applications to verify that a Qualified Signature received is actually a Qualified Signature as such, i.e. based on a qualified certificate and created using a Secure Signature Creation Device (SSCD):

- Either because the application “knows” that the CSP provides only Qualified Signatures;
- Or because the certificate makes use of the “qCStatements extension” as defined in the RFC 3739.

5.3.9.2 Impact assessment

Among the surveyed applications which are requiring a Qualified Signature, half of them are enforcing this need by limiting the list of CSPs they are trusting as provider of Qualified Signature.

This way of working constitutes however a barrier to full European interoperability.

5.3.9.3 Potential solution and ongoing initiatives

We recommend that qualified certificates issued by European CSPs comply with the “Qualified Certificate profile”¹³³ and, in particular, make effective use of the Qualified Certificates Statements “qCStatements extension” as proposed by the ETSI Technical Specification. In addition, currently ongoing review efforts in the context of the ongoing CROBIES study should be carefully monitored, due to the impact that this work may have on the existing standardisation framework.

5.3.10 Signature format

5.3.10.1 Issue

As in the previous study, it appears that among the surveyed applications, many different types of signature formats have been found (PKCS#7, XMLDSig, XAdES, CAdES ...)

Because the surveyed applications are not the same as in the previous study, it is very difficult to state precisely, from a statistical point of view, if the situation is more or less homogeneous than 2 years ago on that topic.

However, it seems to be a trend whereby applications are requiring more and more XML signatures and/or PDF signatures.

¹³³ ETSI: “Qualified Certificate profile”, ETSI TS 101 862, V1.3.3, January 2006

5.3.10.2 Impact assessment

Having multiple signature formats in use across Europe does not constitute an interoperability barrier as soon as the signed documents do not need to be exchanged from an application to another.

Anyway, even if this exchange of document has not yet been deemed necessary by application providers, it seems obvious that it will be more and more requested in the future. At that time, making use of common formats (e.g. XAdES as proposed by ETSI) will become a necessity.

5.3.10.3 Potential solution and ongoing initiatives

To avoid issues linked to signature format recognition, we still recommend promoting the use of international standards. Moreover, this recommendation fits in the strategy of other important initiatives such as ETSI PLUGTEST™ which is focusing on XAdES Interoperability, the STORK large scale pilot, the PEPPOL project or the Cross Border Interoperability of eSignatures [CROBIES] study.

Today, three main signature formats are emerging:

- CAAdES (CMS Advanced Electronic Signature)¹³⁴: defines a number of Electronic Signature formats that build on CMS (RFC 3852) by adding signed and unsigned signature attributes , resulting in support for a number of variations in the signature contents and powerful processing requirements.
- XAdES (XML Advanced Electronic Signature)¹³⁵: set of extensions to XML-DSig¹³⁶ making it suitable for advanced electronic signature. While XML-DSig is general framework for digitally signing XML documents, XAdES specifies precise profiles of XML-DSig for use with qualified electronic signature in the meaning of European Union Directive 1999/93/EC. One important benefit from XAdES is that electronically signed documents can remain valid for long periods, even if underlying cryptographic algorithms are broken.
- PAdES (PDF Advanced Electronic Signatures)¹³⁷: defines the first of a series of profiles that describe how digital signatures in PDF can be used in a way that provide an Advanced Electronic Signature framework for the signing of electronic documents in PDF format.

5.3.11 Signature validation

¹³⁴ ETSI: “Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAAdES)”, ETSI TS 101 733, V1.7.3, January 2007

¹³⁵ ETSI: “XML Advanced Electronic Signatures (XAdES)”, ETSI TS 101 903, v1.3.2, March 2006

¹³⁶ W3C “XML-Signature Syntax and Processing”, W3C Recommendation, 12 February 2002
<http://www.w3.org/TR/xmlsig-core/>

¹³⁷ “Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1”, ETSI TS 102 778, V1.1.1, April 2009

5.3.11.1 Issue

Most of the surveyed applications rely on the validation mechanisms provided by the CSP they trust or on the validation mechanisms provided by their national framework. In any case, they typically are only able to validate signature that have been generated by CSPs from their own country.

In general, eGovernment applications have been developed in that way because no trust relationships exist with other CSPs but also because they want to limit the number of CSPs that they have to interact with.

The limited number of CSPs currently supported by eGovernment applications is a major barrier to interoperability. If every application would have to support all European established CSPs, the situation will quickly become unmanageable. Indeed, at the European level, if we consider an average of 3 CSPs per country, this would mean that every eGovernment application would have to manage relationships with more than 90 CSPs.

5.3.11.2 Impact assessment

The signature validation landscape has changed in Europe since 2007. Indeed, in the previous study, Spain was the only country to mention the existence of a validation service, called @firma.

But, among the surveyed applications of this study, 5 validation services were reported: @firma in Spain, e-Notarius in Poland, MOA-SP in Austria, VPS/Governikus in Germany and BBS in Norway.

We also know from the feasibility study on European Federated Validation Service (EFVS) that several other Validation Services are present on the European market.

This trend proves that the signature validation issue has been deemed as sufficiently important to be quickly tackled also for the eGovernment applications.

The usage of validation services in the Member States will partially solve the interoperability issue of signature validation, but still a mean to federate (i.e. interconnect) those services at the European level will be missing.

The preliminary conclusions of the EFVS feasibility study, whose goal was to address this signature validation interoperability issue, show that it will likely not be feasible for the European Union to set-up a Federation of Validation Services, and that alternative governance models will need to be explored.

5.3.11.3 Potential solution and ongoing initiatives

As stated above, even if the set-up of a Federation of Validation Services would be the solution to solve many of the eSignature validation issues, the EFVS feasibility study preliminary conclusions show that it will likely prove unmanageable to organise this under the responsibility of the European Commission.

Therefore, we seems advisable to assess whether the normative framework for Signature Validation Services is currently adequate, and to examine which further steps would be needed to conceptually permit service providers to operate signature validation services across the EU in a legally secure and interoperable manner.

5.3.12 Validation protocol

5.3.12.1 Issue

Validating an electronic certificate is a complex process. First, it must be checked if the certificate belongs to a trusted CSP (the whole certification chain has to be analysed), then the validity is verified (does the certificate expired?) and finally the status must be verified (is the certificate rejected?).

To achieve the certificate status check, the application can make use of different protocols: CRL (a red list of rejected/suspended certificates downloaded from the CSP's site), OCSP (a request certificate status is sent to the CSP which sends back a response of "current", "expired," or "unknown.").

SCVP (Server-based Certificate Validation Protocol) has been designed to make it easier to deploy PKI-enabled applications by delegating path discovery and/or validation processing to a server, and to allow central administration of validation policies within an organization.

Among surveyed applications, 58 applications have answered the question « What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP...) »:

- 29 are only supporting CRL as validation protocol,
- 22 support both CRLs and OCSP,
- 7 support only OCSP protocol.

None of the surveyed application support SCVP.

The responses are not surprising, as they fit perfectly with the validation protocols usually provided by CSPs.

5.3.12.2 Impact assessment

There is potentially an issue for the seven applications that only support OCSP as validation protocol. Indeed, not all CSPs presented in the various country profiles have set-up an OCSP responder. Many of the CSPs only provide a certificate validation mechanism based on CRLs.

Of course, the issue is more related to specific applications that have not been designed for interoperability and that only support validation protocols provided by the CSPs they trust. To achieve interoperability, eGovernment applications should support as many validation protocols as possible.

5.3.12.3 Potential solution and ongoing initiatives

The complexity for applications of supporting the validation protocol provided by the CSP they trust, will automatically disappear as soon as Validation Services will be made available to eGovernment applications.

Indeed, by using such a model, the whole validation process will be off-loaded to the Validation Service, eliminating the need for eGovernment applications to support multiple protocols.

5.3.13 Signature algorithm

5.3.13.1 Issue

Not all surveyed countries have the same security requirements in terms of signature algorithm. E.g. as of 1/1/2010, SHA-1 will no longer be allowed for hash functions in use with Qualified Certificates in Germany. The decision was made following the discovery of a security issue within SHA-1.

5.3.13.2 Impact assessment

This type of problem will not be seen at signature creation time. But if the signed document needs to be sent out to another country, then the latter might reject the signature because it was created in year X using a signature algorithm which was already no longer allowed in the country where the signature is now being validated.

5.3.13.3 Potential solution and ongoing initiatives

To address this issue, harmonisation work is needed at European level. At any rate, decisions to no longer allow one signature/digest algorithm due to security issues should be made collegially by all Member States.