Analysis and Assessment of the solutions

Draft Report on analysis and assessment of similarities and differences (D2.1)

Draft Report on impact on interoperability (D2.2)

Draft Report on addressing legal and trust issues in an EU level validation platform (D2.3)

Study on European Federated Validation Service (EFVS): Feasibility and Global Implementation Plan

September 2009

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

Authors: Hans Graux (time.lex), Christian Staffe (Siemens)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°14

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://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/7764

© European Communities, 2009

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

Executive summary

The European Federated Validation Service (EFVS) Study was initiated by IDABC in order to assess the feasibility of specific measures to ensure the availability of a European scale federated electronic signature verification functionality. As a first step in the EFVS Study, information has been collected on twenty-two existing solutions that already provide all or some of the functionalities associated with European signature verification functionality, or that could provide valuable insights on how such an EFVS could be organised. This has been done by drafting standardised profiles of the identified solutions, focusing specifically on how each of these solutions (a) determine the validity of signature certificates; (b) verify electronic signatures created using these certificates; and (c) provide specific guarantees to their customers on the outcomes of these processes. The solution profiles have been further analysed in the present report, which is logically structured as follows:

Section 3.1 - Analysis and assessment of similarities and differences: in this section, we have examined the collected information as bundled in the solution profiles. Based on a functional comparison table, we indicated which services are provided by each examined solution, and identified the solutions that most closely or completely meet the relevance requirements as stated above. On the basis of this table, four so-called key solutions were chosen, which offered the main functionalities sought for in a validation solution: validation of certificates, verification of signatures, and assuming liability towards the end user. These key solutions were the @firma platform, the BBS Validation Authority, the A-SIT Signature Verification Service (SVS) and e-Notarius.

Each of these four key solutions were then analysed in detail, including in particular the scope of the solutions (including business considerations), their technical approach, and the legal model behind it. While the emphasis of the analysis was on the key solutions, useful inputs from other profiles were identified and considered as well.

Section 3.2 - Impact on interoperability: in the second phase, three different analyses were performed:

- Interoperability needs analysis: firstly, a conceptual analysis was done, examining what the legal and technical challenges are, addressing in particular (a) functional requirements (what do we want to enable), (b) technical requirements (what are the technical issues to be resolved) and (c) legal requirements (legal/policy issues).
- Observed interoperability approach analysis, consisting of a mapping of the aforementioned conceptual model to the key solutions: how do they answer the requirements defined above, and if they don't, what are the main barriers?
- Interoperability gap analysis, consisting of an analysis of the remaining gaps and what would conceptually be needed to get to the goal defined above (in the Interoperability needs analysis).

The analysis showed that the solutions currently have two options for creating trust at a cross border level. The first option, as demonstrated by @firma, SVS and e-Notarius, is to leverage the existing trust model that has been created by the eSignatures Directive, which created the concept of the qualified certificate and made this subject to national supervision. This means that qualified certificates can benefit from an inherent trust, caused by a common legal framework (the Directive and its national transposition) which is enforced (at least in theory) by a comparable supervision regime. None the less, this option is not currently used in practice: neither @firma, SVS nor e-Notarius supports foreign qualified certificates. One of the key reasons – but not the only one – for this issue is the lack of a trustworthy source to identify CSPs issuing qualified certificates. This question is however already being addressed in the context of the CROBIES study.

The second option is demonstrated by the BBS model, which consists of operating largely on the basis of a contractual framework, which does not depend on the European regulatory framework and its trust model, and can thus also be applied outside the context of qualified certificates. In this case, the validation authority defines its own norms and standards, which it applies to any number of chosen CA's, and which it offers to its clients in accordance with their needs. This has the advantage of being applicable internationally (since there is no need to link explicitly to European rules and standards), but it also puts much more effort and responsibility with the validation authority as a single source of trust (a one stop shop for technical and legal guarantees). From an interoperability perspective, this option also creates the risk that different validation authorities apply different norms and standards, meaning that service providers will not be able to easily compare guarantees offered by different validation authorities.

These different options must be taken into account when choosing an appropriate road forward.

Section 3.3 - Addressing legal and trust issues in an EU level validation platform: based on this analysis, we have examined if and how further initiatives could be taken at the European level to facilitate the verification of signatures. The choices that should be made differ substantially depending on the scope of the envisaged outcome.

Current initiatives have focused largely on facilitating (or rather enabling) the cross-border verification of qualified signatures, and signatures based on qualified certificates. After examining current interoperability efforts, it is our finding that validation authorities will not require significant further assistance to serve the needs of this market segment, provided that the currently ongoing efforts, specifically in the context of the CROBIES study are successfully finalised and implemented (including most notably the establishment of national trusted lists of supervised CSPs (to be coordinated at the EU level), standardisation efforts in relation to certificate profiles, SSCD profiles and signature formats, and the establishment of supervision criteria). In this segment, there does not appear to be a manifest need or advantage for the Commission to establish a validation authority, as ongoing initiatives (including currently existing validation authorities) appear to be substantially capable of addressing market needs, and the liability risk for the Commission may be disproportionate to any advantages created in the market, should it choose to develop its own validation authority.

In contrast, these considerations do not hold equally true for signatures which do not rely on qualified certificates. In this market segment, there is no existing trust framework in many Member States that can be leveraged, since the Directive does not impose any supervision obligation for such certificates, nor are there specific quality criteria in place to determine the reliability of nonqualified certificates or signatures (although some have implemented voluntary accreditation schemes). In this area, validation authorities could certainly prove to be useful, as a way of locally assessing the compliance of CAs with specific norms and providing guarantees in this regard. However, the framework for doing so (including the question of which norms to apply to determine the trustworthiness of certificates) is still largely unavailable, and in this area Commission initiatives could still play a significant role, either by filling the remaining gaps, or by participating directly in the market, provided that this would not impede the proper functioning and development of the common market for such services. Several scenarios can be envisaged in this respect, which will be further examined in the following reports.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

1 DOCUMENTS 7

1.1 Applicable Documents 7

1.2 Reference Documents 7

1.3 Acronyms 8

2 INTRODUCTION 9

2.1 The EFVS Study 9

2.2 Goals of the present report - analysis and assessment of existing validation solutions and validation needs 11

3 ANALYSIS AND ASSESSMENT 13

3.1 Analysis and assessment of similarities and differences 13
3.1.1 Functional comparison 13
3.1.2 Solution analysis 18
3.1.2.1 Scope of the solution 18
3.1.2.1.1 Geographical scope 19
3.1.2.1.2 Sector scope 20
3.1.2.1.3 Business model 22
3.1.2.1.4 Actual use 24
3.1.2.2 Technical approach 26
3.1.2.2.1 Technical operation 26
3.1.2.2.2 Certificate validation approach 28
3.1.2.2.3 Signature verification approach 30
3.1.2.2.4 Logging/auditing 31
3.1.2.3 Legal approach 34
3.1.2.3.1 Relationship with the CAs and relying parties 34
3.1.2.3.2 Criteria for the assessment of certificate quality 37
3.1.2.3.3 Criteria for determining legal signature value 41
3.1.2.3.4 Liability/responsibility model 44
3.1.2.3.5 International legal model 47

3.2 Impact on interoperability 49
3.2.1 Technical Interoperability problems 49

3.2.1.1 Trustworthiness of CAs 49

3.2.1.2 Semantic interpretation of certificate fields 49

3.2.1.3 Incompatible use of identifiers 50

3.2.1.4 Signature Type 50

3.2.1.5 Dedicated Interface requirements 50

3.2.1.6 Signature format 50

3.2.1.7 Certificate Validation protocol 51

3.2.2 Legal interoperability problems 51

3.2.2.1 National perspective - trustworthiness of CA 51

3.2.2.2 Security levels – legal qualification of signature types 51

3.2.2.3 eSignature Directive compliance – prior authorisation and the public sector clause 51

3.2.2.4 National rules on identifiers 52

3.2.2.5 Responsibility and liability 52

3.2.3 Observed Interoperability approach analysis 53

3.2.4 Interoperability gap analysis 55

3.3 Addressing legal and trust issues in an EU level validation platform 56

3.3.1 Summary of main needs 56

3.3.1.1 Definition of the service 56

3.3.1.2 Quality of the service: certificate and signature 57

3.3.1.3 Legal value of the signature 58

3.3.1.4 Responsibility and liability of the validation authority 60

3.3.1.4.1 Liability under the Directive 60

3.3.1.4.2 The need for an authority? 63

3.3.1.4.3 The impact of federation 64

3.3.2 Description of main regulatory restrictions 67

3.3.2.1 Liability towards users of a validation authority 67

3.3.2.2 Market access and internal market limitations 68

3.3.3 Provisional findings on the high level framework to be established for validation services 71

1 Documents

1.1 Applicable Documents

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

1.2 Reference Documents

[RD1]	Project Management and Quality Plan (EFVS SC14 PMQP)
[RD2]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD3]	Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications http://ec.europa.eu/idabc/en/document/6485/5938

1.3 Acronyms

CA	**C**ertification **A**uthority
CRL	**C**ertificate **R**evocation **L**ist
CSP	**C**ertificate **S**ervice **P**rovider
DSS	**D**igital **S**ignature **S**ervices
DVCS	**D**ata **V**alidation and **C**ertification **S**erver
EFVS	**E**uropean **F**ederated **V**alidation **S**ervice
IDABC	**I**nteroperable **D**elivery of European Services to public **A**dministrations, **B**usinesses and **C**itizens
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol
PKCS	**P**ublic-**K**ey **C**ryptography **S**tandards
PKI	**P**ublic **K**ey **I**nfrastructure
SCVP	**S**erver-based **C**ertificate **V**alidation **P**rotocol
TTP	**T**rusted **T**hird **P**arty
TSA	**T**ime **S**tamping **A**uthority
TSL	**T**rust-service **S**tatus **L**ist
TST	**T**ime **S**tamp **T**oken
VA	**V**alidation **A**uthority
XAdES	**X**ML **Ad**vanced **E**lectronic **S**ignature
XKMS	**X**ml **K**ey **M**anagement **S**pecification
XML	e**X**tensible **M**arkup **L**anguage
XML-DSIG	**XML** **D**igital **Sig**nature

2 Introduction

2.1 The EFVS Study

The European Federated Validation Service (EFVS) Study was initiated by IDABC in order to assess the feasibility of specific measures to ensure the availability of a European scale federated electronic signature verification functionality. The outcome could take the form of a specific supporting service to be controlled by the European Commission or of a framework set up or coordinated by the European Commission allowing existing signature verification services to interconnect and offer their services more easily, at a minimum at the European level.

The specific road to be chosen will be determined in the course of the Study, depending on the current status of the market, possibilities available to the Commission within the existing legal framework (and specifically of the Directive on a Community Framework for electronic signatures [RD2]), and the need and potential benefits of each possible approach. It is foreseen that the Study will also establish an implementation plan for any actions to be proposed at the Commission level.

As a first step in the EFVS Study, information has been collected on existing solutions that already perform all or some of the functionalities associated with European signature verification functionality, or that could provide valuable insights on how such an EFVS could be organised. This has been done by drafting standardised profiles of the identified solutions, which have been preselected by the Study Team on the basis of the functionalities that they would need to be able to provide. These functionalities have been defined by the Study Team on the basis of the study specifications, which noted the following requirements with regard to the desired EFVS functionality:

> *"A solution is needed that would be beneficial in terms of trust in electronic transactions performed in eGovernment or eBusiness applications, and in terms of the technical validation of the exchanged eSignatures. The European Federated Validation Service would constitute such a trusted platform and authority that would provide trust in cross-border transactions involving the usage of eSignatures.*
>
> *Cross-border recognition of nationally issued digital signatures for security of data exchange requires interoperability at legal, operational and technical levels. The framework for a European Federated Validation Service will provide a necessary tool for the establishment of Trust between different CAs and for the technical validation of eSignatures."*

This description emphasises that the desired outcome is not merely intended to facilitate the technical validation of signature certificates, but also to establish trust in electronic signatures in a broader sense. The EFVS functionality should enable the recognition of signatures, regardless of the country of establishment of the CA.

At a high level, there are a number of services that could be offered by an EFVS. For the purposes of the present Study, three types of services in relation to electronic signatures were considered to be essential for any validation solution to be examined in the course of the Study:

- Firstly, the **validation of the authenticity and integrity of the signature certificate**, notably by verifying the CA's signature on the signature certificate, the validity and non-revocation of the certificate.

In addition to this mostly technical component, users of the service should have some form of guarantee with regard to the quality of the signature certificates being used, typically in the form of minimal standards that are common to all CAs supported by the validation solution.

- Secondly, the technical **verification of the signature**, keeping into account the multitude of formats and algorithms that may be in use. Again, users of the service should have some form of guarantee with regard to the quality of the signature as a whole, typically in the form of minimal standards that are common to all CAs supported by the validation solution..
- Finally, the solution should provide the users with specific **guarantees with regard to the trustworthiness and legal reliability of the electronic signature**, i.e. assessing the legal value of the signature and providing an acceptable liability model that allows the relying party to rely legally on this statement. It is this last quality which distinguishes a (purely technical) validation *service* from a validation *authority*.

Thus, for the purposes of this study, a validation authority is defined as a CSP offering these three basic services in relation to signature solutions issued by independent CAs.

Other services can also be a part of signature verification services, including most notably semantic services (e.g. checking the identity, legal capacity or location of the signatory) and services related to the long term validity of the signature (e.g. archiving of the signature/signed document, maintenance of the signature/document format, and time stamping to allow checking whether a signature was valid at a certain point in time, regardless of its current status). These additional services can however be considered as added value services, whereas the 'basic services' in the list above are considered to be crucial.

Twenty-two validation solutions were examined in the first phase of this study, mostly to collect information on whether they provided some or all of the aforementioned services, and if so, how. Four categories of information were collected for each of the identified solutions, specifically in relation to:

- Functional characteristics, i.e. what does it do?
- Technical characteristics, i.e. how does it work?
- Legal characteristics, i.e. what guarantees does the relying party have?
- Organisational characteristics, i.e. how is it organised?

In addition, the solution providers were asked to identify any issues that they were currently unable to assess in a satisfactory manner, or to indicate any barriers to deploying their activities on the European or broader international scale. This has resulted in the twenty-two solution profiles (Deliverable 1.2 of the Study) which have been created as a first outcome of the Study, and which will be examined further in the present report.

2.2 Goals of the present report - analysis and assessment of existing validation solutions and validation needs

It was expected that very few of the twenty-two examined validation solutions would offer all of the services mentioned in the introduction above. None the less, even solutions which were more rudimentary in scope or in nature (including a number of relatively simple certificate validation services) could still contain useful background information. However, given the more ambitious goals of the Study as stated above, it is not useful or necessary to comprehensively analyse such solutions.

Therefore, the analysis and assessment chapter is logically structured as follows:

- **Section 3.1 - Analysis and assessment of similarities and differences**: this section will examine the collected information as bundled in the solution profiles (Deliverable 1.2 of the Study), and will contain most notably the following sections:
  - *Functional comparison table*, where we indicate which services are provided by each examined solution, and identify the solutions that most closely or completely meet the relevance requirements as stated above. The analysis report will thereafter focus particularly on those solutions, examining these key solutions in detail, and including a summary paragraph that briefly mentions any other solutions that may have provided other useful inputs or insights.
  - *Solution analysis*: this section is divided into thematic subsections identifying the main approaches seen in our key solutions, along with advantages and disadvantages. As noted above, instructive elements from other solutions will be summarily identified separately. The subsections correspond to the structure of the questionnaire, and will cover in particular the scope of the solution (including business considerations), its technical approach, and the legal model behind it. On the basis of this analysis, the key inputs collected via the profiles will be well mapped and assessed.
- **Section 3.2 - Impact on interoperability**: the next phase will logically consist of defining (a) the interoperability problems that need to be resolved, (b) identifying how our key models address these (if they do), and (c) looking at the gaps to be filled. Thus, there will be three subsections:
  - *Interoperability needs analysis*: a conceptual analytic effort, examining what the legal and technical challenges are, addressing in particular (a) functional requirements (what do we want to enable), (b) technical requirements (what are the technical issues to be resolved) and (c) legal requirements (legal/policy issues).
  - *Observed interoperability approach analysis*, consisting of a mapping of the aforementioned conceptual model to the key solutions: how do they answer the requirements defined above, and if they don't, what are the main barriers?
  - *Interoperability gap analysis*, consisting of an analysis of the remaining gaps and what would conceptually be needed to get to the goal defined above (in the *Interoperability needs analysis*). Key inputs from other projects (such as CROBIES, STORK, and PEPPOL) will be identified and taken into account to determine how/if they are handling these issues.
- **Section 3.3 - Addressing legal and trust issues in an EU level validation platform**: finally, this third section will set out a trust/legal strategy for handling those issues, in three parts: (a) summarising the main needs above; (b) describing the main regulatory restrictions as imposed by the eSignatures Directive; and (c) proposing a high level framework for validation services addressing the gaps above. This section will then serve as an outline/design restriction for creating European signature verification functionality.

Ultimately and in summary, the purpose of this report is threefold:

- Assessing the collected solution profiles and assessing the services they provide;
- Identifying the issues to be resolved at the European level and determining if and how the solution profiles are capable of handling these;
- Proposing a framework to address any remaining gaps in order to create the envisaged European federated signature verification functionality.

The results will be taken as a key input for the following phase, examining if and how this framework could be created in practice.

3 Analysis and Assessment

3.1 Analysis and assessment of similarities and differences

As noted above, this section will examine the collected information as bundled in the solution profiles, and will contain two key sections:

- *A functional comparison table*, where we indicate which services are provided by each examined solution, and identify the solutions that most closely or completely meet the relevance requirements as stated above. The analysis report will thereafter focus particularly on those solutions, examining these key solutions in detail, and including a summary paragraph that briefly mentions any other solutions that may have provided other useful inputs or insights.
- *Solution analysis*: this section is divided into thematic subsections identifying the main approaches seen in our key solutions, along with advantages and disadvantages. As noted above, instructive elements from other solutions will be summarily identified separately. The subsections correspond to the structure of the questionnaire, and will cover in particular the scope of the solution (including business considerations), its technical approach, and the legal model behind it. On the basis of this analysis, the key inputs collected via the profiles will be well mapped and assessed.

3.1.1 Functional comparison

The purpose of this chapter is to indicate which services are provided by each of the key solutions in terms of certificate validation, signature verification, time stamping, semantic services, liability…

As a first step in addressing this issue, the table below provides an overview of all of the solution profiles collected in the course of the study, and indicates for each of the solutions which type of functionalities they support. This table is the basis for the selection of the most promising key solutions, which will be further examined in detail. A description of each of the functionalities as they are understood for the purposes of this table is included below the table.

	Common certificate quality requirements	Certificate verification component	Common signature quality requirements	Signature verification component	Guarantee & liability model	Time stamping services	Long term validity assurance	Semantic services	Customisation at client's request
@firma	✓[1]	✓	✓[1]	✓	✓	✓		✓	
BBS	✓	✓	✓	✓	✓	✓			✓
CertiVer		✓							
CNUE	✓	✓	✓	✓					
CoreStreet		✓							
Cryptolog		✓		✓		✓	✓		✓
e-App									
e-Notarius	✓[1]	✓	✓[1]	✓	✓	✓			
FBCA	✓		✓						
GTA	✓		✓		✓				
Infocert	✓	✓	✓	✓		✓			
MOA-SP	✓[1]	✓	✓[1]	✓				✓	
PEPPOL	✓	(✓)[2]	✓	(✓)[2]					
Polito	✓		✓						
Signicat		✓		✓					
Safelayer – TrustedX	✓	✓	✓	✓		✓	✓	✓	✓
SPES	✓		✓	(✓)[3]					
Austria SVS	✓[1]	✓	✓[1]	✓	✓			✓	
TACAR	✓		✓						
TrustWeaver		✓		✓		✓			

[1] The solution is capable of determining and stating whether a certificate is qualified or not for the supported CSPs, and whether the resulting signature can be considered qualified or not, which can be considered as de facto quality requirements. For @firma and e-Notarius, only CSPs issuing qualified certificates are presently supported.

[2] Currently being implemented as a part of the PEPPOL pilot, but not yet available.

[3] Only available as a client component

Tumbleweed		✓							
VPS-Governikus	✓	✓	✓	✓		✓	✓		✓

Functionality	***Description***
Common certificate quality requirements	The solution provider has defined specific requirements in relation to the quality of the signature certificates which can be validated through the service, in a way that allows the end user to know whether these have been observed. Examples include the definition of a common policy (possibly comprising multiple levels) to indicate what measures participating CSPs take before issuing certificates to the public (e.g. requirements for registration or security of the CSPs facilities). For the purposes of this study, the ability to distinguish qualified and nonqualified certificates is considered a form of common certificate quality requirements, as indicated in the table above.
Certificate verification component	The solution provider offers a mechanism to verify signature certificates, in particular to check their validity, most commonly via OCSP, CRLs / delta-CRLs and/or LDAP.
Common signature quality requirements	The solution provider has defined specific requirements in relation to the quality of the signatures which can be validated through the service, in a way that allows the end user to know whether these have been observed. Examples include the requirement of observing common standards in relation to signature formats or algorithms to be used to ensure that they are sufficiently trustworthy. For the purposes of this study, the ability to distinguish qualified from nonqualified signatures is considered a form of common signature quality requirements, as indicated in the table above.
Signature verification component	The solution provider offers a mechanism to verify signatures, in particular to check their conformity with the aforementioned requirements.
Guarantee & liability model	The solution provider offers clear guarantees to the end users and accepts some degree of liability for this.
Time stamping services	The solution provider offers time stamping services as a part of the solution.
Long term validity assurance	The solution provider offers services intended to ensure that certificates and/or certificates can be verified over an extended period of time, including in particular after the signature certificate has expired.
Semantic services	The solution provider offers services intended to clarify who/what the signatory is, i.e. any assistance in interpreting the content or meaning of the certificate or signature, or the authorisation of the signatory.
Customisation at client's request	The solution provider customises the service at the client's request, e.g. by integrating specific signature quality requirements.

As seen in the table above, the main solutions meeting our predefined requirements for a signature verification service (covering the first five columns in the table) are @firma, BBS, SVS and e-Notarius.

We recognise of course that other solutions which did not meet all five predefined requirements none the less offer features that could be very useful to address current European eSignature verification shortcomings. Most notable among these were the solutions offered by Cryptolog, Safelayer-TrustedX, VPS-Governikus, PEPPOL, CNUE, and the Austrian MOA-SP open source software.

For the PEPPOL solution, the main reasons for not being retained as a key solution were the fact that it is envisaged to operate as a pilot project (and thus is unlikely to implementing a definitive liability model), and that it currently has no functioning implementation yet.

Similarly, while the CNUE solution is operational in a pilot configuration, it has several central characteristics which make it hard to compare with the other solutions. Firstly, it is used exclusively between notaries public, i.e. in a context where a prior trust already exists, since all members are a part of the same (or substantially similar) professional group. Secondly, the solution is coordinated by a central body (the CNUE), which can mediate between the stakeholders to ensure that the necessary preconditions for trust are met and enforced in practice. Finally, it leverages the specific relationship which exists between participating CAs and national professional organisations of notaries public: only CAs that have a pre-existing relationship with such national organisations can participate in the solution. For this reason, the CNUE solution will not be examined further as one of the key solutions in this Study.

For the other four solutions which were not retained, the main reason lies in the scope of the present study. These specific solutions are among the most technically advanced in the study. This is specifically visible for the Safelayer –TrustedX solution, which offers every functionality examined, but also for the others, which each offer certain important features. None the less, they were not retained as key solutions due to the fact that this study aims to examine solutions that could operate in a cross border eGovernment perspective. Defining a responsibility/liability model is crucial for this. It is not sufficient that a verification solution can provide a technically valid result; the user of that solution must also be able to rely on it.

This is however not an element that is offered by these four solutions. In each case, the solution is a technical one: customers (including public administrations) are free to acquire the necessary licenses to use the solutions, to integrate them into their own application, and to configure them at their own responsibility. This last element is crucial: the final responsibility for deciding whether or not a signature is trustworthy remains fully with the end user. In some cases – including e.g. the VPS-Governikus solution and the Austrian MOA-SP approach, certain default settings are offered (in the former case relating to German accredited/supervised CPSs[4], in the latter case to Austrian ones). However, in both of those cases it is the user of the solution that accepts any risks. The usability of the solution comes from the fact that they are all supervised within their own countries, and not because of any quality guarantees that the solution developer offers. Trust is thus obtained from the supervision/accreditation of the CAs, and not from any guarantees from the solution provider. It is this last element which distinguishes a validation authority from a validation service: a service can technically function without a liability model, but does not solve the fundamental trust issue that currently exists in the context of public sector processes.

In relation to Cryptolog, these considerations were also clearly communicated in the profile itself, which stressed that it is not a validation authority as such (encompassing a liability model and specific quality requirements proposed by Cryptolog), but rather a platform that others can implement to create their own validation authorities on the basis of any requirements desired by the customer. As such, it is extremely useful as a conceptual model to address interoperability issues, but less instructive in relation to the issues related to liability and quality requirements. This same sentiment was also reflected in the Safelayer TrustedX profile, which noted that it could offer any required technical functionality, including the capability of interconnecting with other validation solutions, but which also stressed that "*(i)t is up to the product operator/service provider to decide which CAs are going to be recognized or not. As stated in previous sections, the trust and policy*

[4] More accurately: by default the solution supports all German accredited/qualified CAs, the so-called V-PKI CAs (a special PKI used by the German administration) and CAs operating in Switzerland, and one Swiss CA which also uses Governikus

management that the product offers facilitates managing CAs with different legal value." Trust is thus a supported feature of the package, but the final decisions must be made by the end users themselves.

The same difficulty is also observed to a certain extent in the Austrian MOA-SP open source software: it is not envisaged to be a validation authority that assumes specific liabilities toward the end user. As noted above however, the default configuration of the software already has integrated support for Austrian CSPs that issue qualified or nonqualified signature certificates, meaning that by default, it does come with a de facto qualitative framework behind it. In addition, the solution is open source and could integrate the European trusted list of CSPs issuing qualified certificates from all other Member States when it becomes available by the end of the year.

For the Governikus solution, which is the technical basis on which PEPPOL is currently being built, the situation is much the same: a user of VPS/Governikus (e.g. an eGovernment application) would be able to install the components required for signature validation locally, and use the software to verify any of the supported signature types. The default installation covers all German CAs accredited/qualified CAs, the V-PKI CAs, and one Swiss CA (due to the fact that this CA also uses Governikus, which allows it to connect directly to other Governikus users; this feature will be further discussed in the sections below). If that user wants to integrate more CAs (e.g. unsupervised/unaccredited ones), they could configure that themselves as well, as with the Austrian approach, and again at their own responsibility.

In the following sections, for each aspect to be analysed we will look at the four identified key solutions in detail. If other solutions have approaches that are particularly noteworthy, instructive or useful as a model at the European level (including specifically CNUE, Cryptolog, MOA-SP, Governikus, TrustedX and PEPPOL), this will be separately mentioned in a summary paragraph.

3.1.2 Solution analysis

This section is divided into thematic subsections corresponding to the structure of the questionnaire and identifying the main approaches seen in our key solutions, along with advantages and disadvantages. When applicable, a short paragraph entitled 'Other noteworthy approaches' identifying usable elements from other solutions will be added.

3.1.2.1 Scope of the solution

A first question relates to the precise scope of the service. Some of the examined solutions presently only cover a specific region or a specific sector, both of which are important questions when assessing their relevance as models for a European approach. A solution which is only offered in a single region with a single legal framework or technical context effectively will have less interoperability issues to overcome. From that perspective, solutions which have a cross border scope (covering several Member States or even non-European countries) are inherently more interesting. The same consideration applies in relation to any sector based limitations: if a solution is only offered in a specific environment (e.g. by notaries public, as was the case for the aforementioned CNUE solution), it is likely to leverage the specific conditions that exist in that sector (e.g. the presence of a central coordinating body), which may be difficult to replicate outside that context.

The issue of scope is however not limited to the region and context in which the solutions are offered. Two other crucial questions that will be examined are the business model being used (is the solution a for-profit model, non-profit and/or funded by public resources) and to what extent the solution is used in practice (i.e. high volume versus low volume; fully operational services versus pilot implementations). Both elements are relevant to determine to what extent they can be replicated in a different context, and how this should be addressed.

3.1.2.1.1 Geographical scope

a. Observed approach in the key solutions

@firma approach	
Observed approach	*The scope of the solution is clearly national (targeting eGovernment applications mainly) as all CAs need to be supervised/accredited by the Spanish supervisory authority.*
Assessment	*The national focus finds its reasons in the difficulty of ensuring the trustworthiness of foreign CSPs.*

BBS approach	
Observed approach	*No geographical limitation applies. BBS offers the solution internationally. Supported CAs originate from multiple Member States and EEA countries, as well as GlobalSign.*
Assessment	*No strict reliance on national laws, standards or framework; thus, there are no geographical restrictions.*

SVS approach	
Observed approach	*The scope of the solution is mainly national: three out of four supported CAs are Austria. However, the EuroPKI Certification Authority is also supported.*
Assessment	*The solution is technically flexible enough to support virtually any CA, provided that a trust anchor can be registered.*

e-Notarius approach	
Observed approach	*Only Polish CSPs issuing qualified certificates are currently supported by e-Notarius, although CSPs from other MS have been integrated in a demo environment. This demo environment also interoperates with a Russian DVCS (Data Validation and Certification Server).*
Assessment	*The main operational service needs to focus on Polish CSPs, due to the need to assess and ensure the trustworthiness of the CSPs. If a European trusted list would be available, then this would help to address this issue.*

b. Other noteworthy approaches

No other solutions are significantly notable in this respect.

c. Summary conclusions

Of the four key solutions, two (@firma and e-Notarius) have an exclusive link to their respective countries of origins. For both of these, one of the decisive factors is the fact that the services need to provide certain assurances in relation to the supported CSPs, and that it is difficult to provide such assurances in relation to foreign CSPs, at least without engaging in extensive prior auditing.

This last consideration is also the reason why geographical restrictions are less relevant for the BBS solution, as CSPs are integrated upon clients' request after undergoing checks to ensure they meet the standards and policies adopted by the BBS Validation Authority. In that respect, location of the supported CSPs is not a relevant factor. The same holds more or less true for the SVS solution, where the decision to integrate a CA is made by the operator of the solution (A-SIT, in this case), based on an examination of the CP/CPS of the CA in question.

Geographical scope is thus clearly linked to the (in)ability of successfully addressing the trustworthiness of foreign CSPs.

3.1.2.1.2 Sector scope

a. Observed approach in the key solutions

@firma approach	
Observed approach	*The solution is primarily dedicated to public administration*
Assessment	*This restriction is not inherent to any technical or conceptual aspect of the solution itself.*

BBS approach	
Observed approach	*No restriction in sector scope; the service is available to any relying party that establishes a prior business agreement with BBS.*
Assessment	*No element of the service is dependent on any link with a specific sector or application field.*

SVS approach	
Observed approach	*No restriction in sector scope; the service is available to any relying party without restriction.*
Assessment	*No element of the service is dependent on any link with a specific sector or application field.*

e-Notarius approach	
Observed approach	*No restriction in sector scope; the service is available to any relying party that establishes a prior business agreement with e-Notarius. In addition, non-commercial use is free of charge (via https only in this case).*
Assessment	*No element of the service is dependent on any link with a specific sector or application field.*

b. *Other noteworthy approaches*

Most of the studies solutions are not inherently restricted to a specific sector or application field, but there are some exceptions, including notably:

- Academic solutions such as the Polito EuroPKI Top Level Certification Authority and the TACAR (TERENA Academic CA Repository). In the former case, the academic aspect is merely the main focus of the solution; in the latter part it is part of the common policy of TACAR (i.e. CAs without a link to the academic community cannot become a part of the repository).
- The CNUE solution, which is used exclusively between notaries public, as was noted above. In the case of CNUE, this is essential since it is the CNUE (*Conseil des Notariats de l'Union Européenne – Council of the Notariats of the European Union*) which coordinates the solution and thus insures the trustworthiness of the CAs, inter alia by ensuring that only CAs that have a pre-existing relationship with national notarial organisations can participate in the solution.
- The e-App solution, which is only used in relation to electronic apostilles, i.e. electronic documents issued by notaries in certain countries. In this case, the limitation to a specific sector is also quite important, since signed e-apostilles are validated through electronic registers (e-Registers) which are managed at a national level by the competent notarial body. In a direct sense, trust in the document is inherited from these registers, and not so much from the signature itself.

Thus, for some solutions, the limitation to a specific sector is crucial for their viability.

c. *Summary conclusions*

Of our key solutions, only one is limited to a specific sector, as @firma is currently only used in Spanish eGovernment applications. This restriction in scope is however not related to technical necessity or to any dependence of the solution's trustworthiness on this sector. It appears instead to be due to a number of factors, including specifically the origin of the solution (as a project initiated by the regional government of Andalusia and currently operated by the Ministry of Presidency of Spain), and the need to manage liabilities in proportion to the public funding (i.e. since the service is operated by public resources, it is questionable whether it makes sense to also assume liabilities in the service of private sector applications without additional compensation).

The three remaining solutions are generic in scope, and can be applied to any sector. This appears to be the case in most of the examined solutions, with the exception of those mentioned above. Restrictions in scope to a specific sector appear to be mainly the consequence of:

- The need to assure trustworthiness, as is the case with e.g. CNUE, where the involvement of notariats is one of the main building blocks of the trust model;
- The need to control liabilities and financial risks in proportion to the business model, as is the case with e.g. @firma;
- The need to focus mainly or exclusively on the requirements of a specific sector which has created and controls the solution. This is the case to some extent with most sector-specific solutions, including all of the above (@firma, CNUE, TACAR, Polito, EuroPKI,...).

3.1.2.1.3 Business model

a. Observed approach in the key solutions

@firma approach	
Observed approach	*Non-profit solution financed by public funds*
Assessment	*The main reason for investment is the reduction of costs associated to the centralized development of validation services used by multiple eGovernment applications.*

BBS approach	
Observed approach	*Commercial for-profit model, on the basis of case-by-case business agreements with end users (transaction based, volume based or fixed). CAs are paid a fraction of the income, proportionate to their share of the number of certificates validated.*
Assessment	*Agreements are customised to adapt the required services, customisation, liabilities and cost model. The income sharing with CAs ensures that the BBS system is also attractive to them (which is necessary, since BBS requires prior agreements with the CAs).*

SVS approach	
Observed approach	*Non-profit solution operated by A-SIT, a registered non-profit association, in compliance with the principles of strict neutrality, free of instructions and economical independence.*
Assessment	*A-SIT is mainly funded by its members, the Federal Ministry of Finance, The Central Bank of the Republic of Austria and the University of Technology in Graz. The Signature Verification Service is free of charge. The underlying software may also be downloaded and used according to the Apache2-Licence ; thus service providers are free to create their own verification service based on the software and then charge for it.*

e-Notarius approach	
Observed approach	*Mainly commercial for-profit model, on the basis of case-by-case business agreements with end users (transaction based, volume based or fixed fee per month). A free service is available for non-commercial use.*
Assessment	*Commercial users and users who want to use other communication protocols than https (SOAP, API or any other protocol compliant with RFC 3029) will be charged for every issued verification attestation (verification certificate). Users may also buy predefined prepaid packets, which can be used within 2 years from the date of purchase. There is also an option with a monthly subscription payment, for users who want to have unlimited access to the Service.*

b. Other noteworthy approaches

No other solutions are significantly notable in this respect.

c. Summary conclusions

Of the four key solutions, two (BBS and e-Notarius) are commercial for-profit services which charge end users (relying parties) for validation, offering multiple payment models (per transaction, volume based or fixed fee). E-Notarius in addition offers a free service for non-commercial use.

The main difference between these solutions is the income sharing model employed by BBS, which concludes agreements with the participating CAs. This is not done by e-Notarius, which operates without such agreements (and thus without income sharing). This difference is to some extent enabled because e-Notarius focuses only on CSPs issuing qualified certificates whereas BBS is generic in scope (it uses its own multi-level policies, which encompass both qualified and non-qualified signature solutions). This is an important difference, since it means that e-Notarius does not need to perform any further assessments other than to ensure that the CSPs indeed comply with the requirements for issuing qualified certificates, which could be done relatively easily by checking the supervision status[5]. In BBS' case, this would not be sufficient since its classification model is more complicated and thus cannot rely solely on the supervised/unsupervised status. Since BBS needs to verify the practices adopted by each CA supported by its system, further interaction with the CA's is necessary. This difference in approach also means that BBS can apply its system internationally (since it is not dependant on the European notions of qualified certificates and the national supervision systems), which may be more complicated in the case of e-Notarius.

@firma and SVS in contrast are non-profit solutions. @firma is publicly funded, on the basis that the infrastructure is considered to offer substantial benefits to Spanish public services and to the Spanish businesses and citizens. SVS is operated by A-SIT, a non-profit association which also operates as an SSCD conformity assessment body in Austria.

In a broader perspective, all solution profiles show a strong link between business models and liability: as was to be logically expected, all solutions that assume any kind of liability have put in place a professional business model, either based on commercial agreements or on public funding. Several solutions have no business model to speak of, but these invariably disclaim any liability or are still in a pilot stage (i.e. they are funded as a project with business considerations to be worked out at a later stage).

If liability and responsibility is to be supported by a solution, the establishment of a credible business model (either based on commercial agreements or on public funding) is thus a key priority.

[5] At least in theory. At the time of writing (July 2009), no clear list of supervised issuers of qualified certificates exists yet at the European level, but it is expected that such a list will be created by the end of the year. Until that time, this information is not available in a trustworthy way, which explains to a large extent why the commercial service of eNotarius covers only Polish CSPs at this time: information on other Member States is simply not readily available.

3.1.2.1.4 Actual use

a. *Observed approach in the key solutions*

@firma approach	
Observed approach	*The @firma solution is fully operational and in active use since March 2006. It's being used by 339 eGovernment services with an average throughput of 900.000 transactions per month*
Assessment	*No additional comments.*

BBS approach	
Observed approach	*The BBS validation authority is fully operational and in active use. No exact volume data was provided, but the profile indicated that the volume was currently limited.*
Assessment	*No additional comments.*

SVS approach	
Observed approach	*The solution is operational and in production use. Typical usage figures are some tens to hundreds documents a day.*
Assessment	*No additional comments.*

e-Notarius approach	
Observed approach	*e-Notarius is fully operational and in active use. 250.000 proofs of verification have been delivered by the solution.*
Assessment	*No additional comments.*

b. *Other noteworthy approaches*

For many of the examined solutions, reliable usage figures were either unavailable or indicative of a limited uptake. Some notable exceptions existed, though:

- The VPS-Governikus solution, which is already deployed in most of the German Länder, which processes over 5.5 million signatures per month, and experts to surpass the 10 million mark in 2010.
- The CertiVer solution, which focuses exclusively on certificate validation, reported 60 million transactions per month (~720 million p.a.). It uses a pay-per-use for-profit model.
- The Cryptolog Serenity validation platform reports being used for up to 200 validations per second for one customer, but did not provide overall usage statistics. This platform can be either hosted by Cryptolog or installed locally (hence the unavailability of specific statistics).
- The TrustWeaver validation service has provided confidential usage figures, placing usage in the tens of millions of transactions per year. The service is for-profit and principally charges per transaction.

- The Tumbleweed validation authority, which reported usage of up to ~500 transactions per second at peak times.

c. Summary conclusions

With respect to the key solutions, the non-profit @firma appears to be the clear leader in uptake, with a likely driver being the fact that it is publicly funded. The two commercial solutions report smaller uptake.

However, when looking at the other solutions, it is clear that the for-profit nature of the solution is not the main determining factor. Solutions which have seen the most uptake in practice are often offered for profit, but they are tightly coupled with specific services that create clearly visible added value, while integrating the costs of the validation process into a more generic service. E.g. the TrustWeaver solution reported a substantial use of several tens of millions of transactions per year mainly through its use in e-invoicing, whereas the Tumbleweed authority has been taken up by the US Department of Defence, the UK National Health System and several financial institutions. Thus, actual uptake requires a clear link with specific services with a healthy use case.

In addition, it should be noted that some of the solutions are services which can be installed locally and operated without further knowledge of the solution owner. This is e.g. the case for the Austrian MOA-software, and for the TrustedX platform as well. Therefore, due to the fact that these are not offered as centralised validation authorities, no reliable statistics can be provided.

3.1.2.2 Technical approach

A second question relates to the technical approach of each solution. This includes mainly aspects related to the architecture, the respect of standards and the security.

The architecture plays an important role when it comes to the flexibility (how easily new services, new formats or new algorithms can be integrated) and scalability of the solution. When brought at a European level, scalability will become an even more important requirement as the number of users and transactions is likely to increase largely over time.

The respect of standards plays a key role in the technical interoperability and platform independence which are both very important aspects at the European level.

The last point focuses on the logging capabilities of the solution to be able to cope with auditing requirements in case of dispute.

3.1.2.2.1 Technical operation

a. *Observed approach in the key solutions*

@firma approach	
Observed approach	*The solution is broadly based on web services for both certificate validation and signature verification (based on OASIS WS-I Basic Profile v1.1)* *Web services access is secured by user/password or certificate (based on OASIS WS-Security standard).* *Data privacy is ensured at transport level using HTTPS* *Web service requests may be signed* *All web service responses are signed* *Certificate validation can also be requested following the OCSP protocol* *The solution is designed following a Service Oriented Architecture (SOA)* *Semantic services are offered through a dedicated web service* *Semantic information is returned to the caller following a normalized XML scheme* *Server-side signature service* *Time stamping service*
Assessment	*The solution has a strong technical background in terms of architecture, respect of standards, technical interoperability and security.* *Offering an OCSP service at the Validation Authority level is also interesting as it federates the OCSP services of the underlying CAs, providing a single point of access which is one of the core functionalities of a Validation Authority.*

BBS approach

Observed approach	*The solution is based on web services for both certificate validation and signature verification* *Web service access is secured at transport level (HTTPS) through client certificate* *Data privacy is ensured at transport level using HTTPS* *Web service requests may be signed* *All web service responses are signed* *A quality classification of certificates and signatures is defined and information is returned by the web service interfaces* *Currently no semantic services returned as normalized XML* *Web services are currently not following standards like XKMS or OASIS DSS*
Assessment	*The use of web services is going into the right direction but the lack of standard usages like OASIS DSS and the security at the transport level may appear as a drawback. Semantic services and their normalization is a key requirement to function at the European level and are not yet available.*

SVS approach	
Observed approach	*The solution is an implementation of the MOA-SP open source software, which can be implemented freely.* *The service provides a web front end where signed files can be uploaded.* *These files are being analyzed in a preliminary step in order to determine the file type. The next step invokes an appropriate plug-in that prepares the signed file for signature verification based on XML-DSig or on CMS. The following step involves the signature verification module, which is separately invoked for each signature. The final step encompassed collection and preparation of the results obtained from the validation module. The underlying certificate (including the chain up to a trusted root certificate) is also validated.* *Both OCSP and CRLs are supported. Which revocation information service is used depends on the certificate. The preferred order (if multiple revocation information services are available for a certain certificate) depends on the configuration of the verification service.* *The service supports enveloping, enveloped and detached signatures.* *Since the use of the service is free of charge, any citizen may use it to verify signed documents.* *The SSL protocol authenticates the server against the clients (browsers) and encrypts the connection used to upload the signed files for verification.*
Assessment	*The solution has a strong technical background in terms of architecture, respect of standards, technical interoperability and security.*

e-Notarius approach	
Observed approach	*Both certificate validation and signature verification services are provided as part of the DVCS protocol implemented by the solution* *Service requests may be signed*

	Service responses are signed *Time stamping services are also offered as part of the DVCS protocol*
Assessment	*This is the only solution providing both validation/verification services and time stamping services together using the DVCS protocol.*

b. Other noteworthy approaches

Cryptolog already offers a service of signature extension, which is interesting as this approach is (at best) only planned in most other solutions.

c. Summary conclusions

Most solutions offer the two basic services of certificate validation and signature verification. They rely generally on the use of web services to provide access to their services, which is probably the best choice as of today in terms of interoperability. Historical validation/verification is most of the time foreseen as future additional services but are already implemented by some solutions like MOA-SP/SVS, the VPS-Governikus platform and the Safelayer-TrustedX platform..

3.1.2.2.2 Certificate validation approach

a. Observed approach in the key solutions

@firma approach	
Observed approach	*Revocation status done through OCSP with fallback to CRL if unavailable. LDAP is also supported.* *All CRL/OCSP responses are signed* *No usage of XKMS*
Assessment	*No additional comments.*

BBS approach	
Observed approach	*Revocation status done through OCSP and distributed OCSP with fallback to CRL if unavailable* *Usage of XKMS is foreseen following PEPPOL deliverables*
Assessment	*No additional comments.*

SVS approach	
Observed approach	*Both OCSP and CRLs are supported. Which revocation information service is used depends on the certificate. The preferred order (if multiple revocation information*

	services are available for a certain certificate) depends on the configuration of the verification service. *If the certificate is properly referenced (by issuer and serial number for instance) and if there is a LDAP service configured the certificate is automatically retrieved from the directory service.*
Assessment	*No additional comments.*

e-Notarius approach	
Observed approach	*Revocation status done through OCSP, CRLs, LDAP or all of them* *Choice of method is configurable for each CA* *No usage of XKMS*
Assessment	*No additional comments.*

b. *Other noteworthy approaches*

The approach adopted by VPS-Governikus is specifically innovative with respect to certificate validation, as it uses an XKMS-responder relay interface to interconnect different instances of the Governikus platform. This server-side component named "OCSP/CRL Relay" is used by all other Governikus components as single point of entry for the verification of PKI-issued X509-Certificates based on the XKMS/XKISS protocol. Within the VPS/Governikus model, XMKS responders may be operated by administration branches running VPS/Governikus server instances, which are mostly operated by public administration data centres. One such instance is also operated by bos Bremen, the solution owner, as ASP, which is used by a number of other VPS/Governikus instances. VPS-Governikus users thus have a choice: they can rely strictly on CAs that they are familiar with themselves (e.g. because the CAs are established in their own country and known to be supervised and/or accredited), or alternatively they could choose to contact a trusted XMKS responder operated by another Governikus user if they don't know the CA locally. In that case, they would need to ensure themselves that they can trust the response from that responder. In addition to information that can be gathered by OCSP/CRL checks, this XKMS/XKISS responder is extensible so that it can deal with additional attributes concerning certificate and CSP quality.

Thus, provided that a trust model can be established between different Governikus operators, the Governikus model allows a federated validation service to be established. It is for this reason that the XKMS responder is one of the building blocks for the cross-border signature validation infrastructure to be supplied by the PEPPOL pilot project. As noted above however, it is up to the end users (i.e. the participants in such a federated model) to establish the necessary trust framework.

c. *Summary conclusions*

BBS is the only key solution planning to build on XKMS for certificate verification, whereas the others operate primarily on the basis of OCSP and CRLs.

3.1.2.2.3 Signature verification approach

a. Observed approach in the key solutions

@firma approach	
Observed approach	*Signature verification is based on OASIS DSS standard* *Support for detached, enveloped and enveloping signatures* *Support for multiple signatures (independent, co-signed and counter-signed)* *Supported signature formats are:* *PKCS#7, CMS, CADES-BES, -T, -C, -X, -XL, -A* *XMLDsig, XADES-BES, -T, -EPES, -C, -X, -XL, -A* *PDF and ODF*
Assessment	*The solution is very complete in terms of signature verification support and based on open standards*

BBS approach	
Observed approach	*OASIS DSS is not currently used for signature verification but is foreseen.* *Support for detached, enveloped and enveloping signatures* *Support for multiple signatures (independent, co-signed and counter-signed)* *Supported signature formats are:* *PKCS#7, CMS, XML, PDF, XAdES, CAdES*
Assessment	*No additional comments.*

SVS approach	
Observed approach	*Validation through a web front end where signed files can be uploaded. These files are then analyzed in a preliminary step in order to determine the file type. The next step invokes an appropriate plug-in that prepares the signed file for signature verification based on XML-DSig or on CMS. The following step involves the signature verification module, which is separately invoked for each signature. The final step encompassed collection and preparation of the results obtained from the validation module.* *Support for detached, enveloped and enveloping signatures* *Support for multiple signatures which may be independent, wrapped or countersigned.* *Supported signature formats are:* *PKCS#7, CMS, XAdES BES based XML-Signatures and Austrian PDF-AS signatures*
Assessment	*No additional comments.*

e-Notarius approach	
Observed approach	*Signature verification is part of the DVCS protocol* *Support for detached, enveloped and enveloping signatures* *Support for multiple signatures* *Supported signature formats are:* *PKCS#7, CMS, XML, PDF, XAdES, CAdES* *SDOC and SignPro (linked to Sigillum CA)* *ZEP (linked to EVPU CA)*
Assessment	*Some non standard formats related to specific CAs are supported by e-Notarius.*

b. Other noteworthy approaches

Signature validation on the basis of OASIS-DSS was originally also planned to be examined in the PEPPOL project. However, due to organisational reasons, there is presently only a commitment to examine XKMS-implementations as described above (provided by BOS (Bremen Online Services), who is also the owner of the Governikus solution). There is at present no commitment yet in PEPPOL to implement the OASIS DSS service/interface, although this may change in the future.

c. Summary conclusions

The main standard signature formats are supported. E-Notarius supports some non standard formats related to specific CAs which could lead to some interoperability problems at the European level.

Support for ODF is not common, especially in commercial solutions where PDF is preferred.

3.1.2.2.4 Logging/auditing

a. Observed approach in the key solutions

@firma approach	
Observed approach	*The following is systematically logged in the system:* • *All traffic (requests and responses) of the services* • *All communication (CRL downloading, OCSP requests) with the related CAs* • *Configuration and management actions (like the inclusion of a new certificate)* • *Business and error alarms reported by the monitoring system* *All logs are signed every day to guarantee the integrity and authenticity of the information stored in the log files* *Information related to a particular transaction can be aggregated into a PDF or Excel file*

Assessment	*The logging system is particularly complete and covers almost all parts of the system that could be analysed in case of audit of a particular transaction*

BBS approach	
Observed approach	*The following is systematically logged in the system:* • *All traffic (requests and responses) of the services* • *All communication (CRL downloading, OCSP requests) with the related CAs* • *Configuration and management actions (like the inclusion of a new CA)*
Assessment	*No further comments*

SVS approach	
Observed approach	*Depending on the configured log level all steps are logged, including:* • *parsing of the document* • *identification of the file type* • *invocation of the verification module and downloads like certificates (LDAP), OCSP or CRLs.* *The auditing depends on the internal practices of the provider operating the service. Usually, users do not have access to logs.*
Assessment	*No further comments*

e-Notarius approach	
Observed approach	*The following is systematically logged in the system:* • *All traffic (requests and responses) of the services* • *All communication (CRL downloading, OCSP requests) with the related CAs* • *Time Stamp requests to the TSA* • *Usage of service private key for signing responses*
Assessment	*No further comments*

b. Other noteworthy approaches

The most sophisticated logging approach was found with the Safelayer-TrustedX platform, which incorporates a central logs and audits management system for any events generated by all of the platform's service components. The system log can be extended to external log modules. The TrustedX log information can be accessed by external applications for auditing or monitoring purposes or by its own GUI console. In addition, the TrustedX platform integrates of-the-shell an authorization and control access system that enforces authorization policies to any entity/user that accesses TrustedX services. In particular, the access to auditing information is also controlled by the system and reporting can be tailored as a per user granularity.

c. Summary conclusions

Most solutions have a logging system; some offer the logs on requests and sometimes filtered by transaction. It is rare that logs can be accessed directly online by customers.

3.1.2.3 Legal approach

In addition to the technical issues, the examined solutions also have to be able to provide an workable response to the legal issues they are confronted with, most notably with regard to their relationship with the CAs and the relying parties, the criteria they use to determine the quality of the certificate and the signature (including the importance of European concepts such as qualified certificates, supervision, accreditation, and so-called qualified signatures), and whether or not they accept any responsibility towards the end user. The latter element is the criterion that is sometimes referred to (including e.g. in the profiles of BBS, Cryptolog and TrustedX) to distinguish between validation services (a technical concept) and validation authorities (a service with legal value). To address the cross border interoperability challenges, the remaining trust issues need to be resolved, and the question of responsibilities and liabilities is primordial in this respect.

3.1.2.3.1 Relationship with the CAs and relying parties

a. *Observed approach in the key solutions*

@firma approach	
Observed approach	*@firma focuses on CAs issuing qualified certificates which are supervised in Spain, meaning that its relationship is mostly built on the pre-existing supervision model (which exists in all Member States). None the less, a separate contract with @firma is required to regulate SLA. However, this contract does not include compensation for the CAs (although they are free to engage in contracts with the relying parties using @firma's services.* *As regards the relying parties (which are only public services with @firma), regional or local administrations must sign bilateral agreements with @firma to address mainly the following aspects:* • *Services to be offered by the VA* • *The customer's obligations, conditions and terms of the services* • *@firma´s liability, security/ operational/ technical polices and also the Service Level Agreement for the services.*
Assessment	*@firma thus relies on a dual contractual framework, both with CAs and relying parties, predominantly to define the services to be provided by @firma and the liabilities that it will assume. Economic considerations are not regulated, as @firma is funded with public resources.*

BBS approach	
Observed approach	*The BBS requires contracts with the CAs and the relying parties.* *CAs need to conclude an agreement to ensure that handling the CA is not a violation of the existing policies, that BBS' qualification levels can be applied correctly (see below), and that and a compensation model is put in place in which BBS compensates the CA for the use of its validation facilities, if required.* *Relying parties must conclude agreements to address mainly the following points:* • *The services to be offered by the VA (including the integration of specific CAs if needed).* • *Quality requirements with regard to certificates and electronic signatures (i.e. the requirements the VA should apply to determine whether or not a signature should be considered valid for the customer's purposes). The customer can override these requirements by specifying alternative requirements in requests. The solution is able to utilise back-office rule-sets specific to each relying party. Thus meta responses combining both validation and quality is offered via a "Trusted"/"Not Trusted" response flag .* • *BBS's liability for its services; exact levels of liability vary from agreement to agreement, depending on the levels of services and needs of the customer, but the liability provisions of the eSignatures Directive are always respected in cases where qualified certificates are concerned.* *•The cost model/business model (i.e. costs per transaction, volume based or fixed pri* • *Services to be offered by the VA* • *The customer's obligations, conditions and terms of the services* • *@firma´s liability, security/ operational/ technical polices and also the Service Level Agreement for the services.*
Assessment	*BBS thus relies on a dual contractual framework, both with CAs and relying parties. As with @firma, these serve to define the services to be provided by BBS (including specific customisations) and the liabilities that each party will assume, but they also define the compensations to be paid by relying parties to BBS in compensation for the service, and by BBS to the CAs for the use of their validation facilities.*

SVS approach	
Observed approach	*CA integration policies are decided solely by the operator (A-SIT) at its own discretion, based on the CP/CPS of the CA in question. Other implementations of the MOA-SP software might make other choices, depending on their preferences.*
Assessment	*The solution provider does not specifically regulate its relationship with the CAs.*

e-Notarius approach	
Observed approach	*e-Notarius presently focuses on CAs issuing qualified certificates which are supervised in Poland, meaning that its relationship is mostly built on the pre-existing supervision model (which exists in all Member States). No separate contract or compensation is arranged with the CAs.*

	The relying parties using the e-Notarius service provided by General Certification Authority CERTUM have to conclude a contract with Unizeto Technologies SA first, at least for commercial use (non-commercial use does not require a contract).
Assessment	*e-Notarius requires commercial users of the service to conclude a prior contract first, but does not specifically regulate its relationship with the CAs.*

b. Other noteworthy approaches

Most alternative approaches relied on variations of the above, including specifically:

- Approaches that required only declarations of compliance from the CAs, and had no agreements with end users in place. This was used mainly by solutions that merely disseminate information regarding compliance with one or more common policies, such as e.g. the TACAR CA repository, which additionally requires personal interviews between the solution owners and TACAR representatives;
- Approaches that required declarations of compliance backed by independent audits, such as e.g. the US FBCA, which requires participating CA to obtain an audit certificate showing compliance with specific levels of the FBCA's policies.

Obviously, in solutions that are intended to be implemented locally by the user (including Cryptolog, VPS-Governikus, MOA and TrustedX), the relationship between the solution provider and the CAs is an irrelevant issue, in the sense that these solutions require the end user (i.e. the entity implementing the platform locally) to obtain any needed guarantees from the CA's themselves; the solutions in this case *support* a trust relationship between the user of the system and the CA, but do not *create* it. As indicated in the TrustedX solution profile:

> *The legal requirements that a CA needs to meet must be established by the operator/user of the solution based on TrustedX. From the product perspective, TrustedX allows implementing the required security policies regarding certification validation and digital signature, among others, and offers the possibility to manage the level of trust of each CA, and in general of each trust entity like VAs or TSAs.*

It should be noted however that some of these solutions by default are delivered with integrated support for supervised and/or accredited CSPs from the solution provider's country of establishment, but it remains up to the user of the solution to decide whether he/she wishes to rely on this.

c. Summary conclusions

A clear distinction needs to be made between the relationship between the solution and the CA on the one side, and the relationship between the CA and the relying parties (the end users of the solution). In both cases, most but not all solutions have specific agreements in place to regulate this relationship.

With regard to the relationship between the solution provider and the CA, the main purpose is to clarify if/how the CA meets the solution provider's requirements, including an assessment of the CA's compliance with specific standards or norms, if applicable, which may require audits by the solution provider or by an independent body. Guarantees will typically be requested from the CA, notably a guarantee that the CA will remain compliant with these requirements, or that it will inform the solution owner of any changes that may impact this compliance. In a limited number of cases, compensation between the solution provider and the CA will also be regulated, as the solution provider will often require the use of the CA's verification facilities (OCSP lookups or CRL integration). As noted above, in some cases (like e.g. e-Notarius or the SVS service) no specific agreement is implemented in this regard.

With regard to the relationship between the solution provider and the relying party, the main purpose is to clarify the scope of the services offered by the solution provider (including service levels and customisation, if applicable), and in particular which responsibilities and liabilities (if any) are assumed by the solution provider in respect to the service. Finally, the compensation of the solution provider is usually contractually arranged. Again, exceptions to the rule exist where no agreement exists between the solution provider and the end users, but this occurs exclusively in cases where the solution provider accepts no liabilities, and in particular when the solution essentially consists of the dissemination of information regarding CA practices which the end user can then choose to rely on at his own risk.

3.1.2.3.2 Criteria for the assessment of certificate quality

a. Observed approach in the key solutions

@firma approach	
Observed approach	*@firma supports exclusively[6] the verification of qualified certificates, which are supervised in Spain by the Ministry of Industry. Thus, all supported certificates meet the requirements for qualified certificates as defined in the eSignatures Directive. The @firma Validation Practice Statement identifies all supported CAs, and end users may choose which ones they wish to accept for their applications.*
Assessment	*No separate quality framework has been implemented; the main purpose of @firma in relation to the verification of certificates is to confirm that the certificates are covered by the quality requirements defined by the Directive (or rather the Spanish transposition thereof). Similar approaches could be applied in any Member State.*

BBS approach	
Observed approach	*BBS has defined its own system of six levels of reliability, which are assessed per CA depending on the applicable certificate policy, and assigned to the combination of CA and policy. One element to be considered is assessment of compliance with national or international legislation, e.g. that requirements for qualified certificates/ signatures are met. The current system is mainly based on assurances provided by the CA together with assessment of accreditation/supervision status provided by national authorities (these are required for certificates to reach level 4 or above). The VA has two quality levels for qualified certificates, level 5 and 6, respectively without and with use of SSCD. A signature produced by the use of a certificate at level 6 will be identified as a qualified signature, provided also that the cryptographic quality fulfils the requirements of the customer in that specific case.* *Since most legislations only allow certificates issued to natural persons to be marked as qualified, certificates issued to legal entities cannot be assigned level 5*

[6] In a few cases @firma also supports non-qualified certificates such as certificates for automatic signatures processes in machines as used by many applications of the country, but these are in the process of being recognised as qualified, following a recent Spanish bill on eGovernment.

	or 6 (the qualified levels), no matter their inherent quality. *BBS reserves the right to suspend or degrade a CA whose certificates must be considered unreliable due to weaknesses in the quality of the hash algorithm and size of the key pair used by the CA to sign certificates; thus, the policy of the CA is not the only deciding factor.* *The solution is able to utilise back-office rule-sets specific to each relying party. Thus meta responses combining both validation and quality is offered via a "Trusted"/"Not Trusted" response flag .*
Assessment	*A multilevel framework has thus been created autonomously by BBS, which takes into account European concepts such as qualified certificates and national supervision but which does not depend on them. This has the advantage of offering a system that meets European needs (including the need to identify qualified signatures when necessary) and that can still function at an international level as well. Acceptance of this framework is settled through the specific agreements BBS puts in place with the relying parties, where they can specify which types of signatures (or certificates) they consider to be acceptable in their applications.*

SVS approach	
Observed approach	*In the case of SVS, the solution operator decides on what basis it chooses to support certificates from any given CA. Certificate policies are not automatically checked but certificate policy statements and key usage attributes are shown to the user. Furthermore the solution is able to determine and distinguish between qualified and non-qualified signature certificates (by evaluating QC statements). Finally the specific certificate is being evaluated with regard to the Austrian concept of official signatures. Official signatures are based on advanced or qualified certificates containing a special object identifier as a private extension. Official signatures are used to sign official documents issued by authorities.*
Assessment	*The SVS solution is highly flexible, in the sense that the solution provider can integrate any CAs it chooses, and communicates the aforementioned information to the end user so that he can make a decision on whether the signature is trustworthy.*

e-Notarius approach	
Observed approach	*Like @firma, e-Notarius supports exclusively the verification of qualified certificates, in the case of e-Notarius on the basis of supervision in Poland by the Minister of the Economy. Thus, all supported certificates meet the requirements for qualified certificates as defined in the eSignatures Directive. The @firma CPS stipulates the relevant policies.*
Assessment	*No separate quality framework has been implemented; the main purpose of e-Notarius in relation to the verification of certificates is to confirm that the certificates are covered by the quality requirements defined by the Directive (or rather the Polish transposition thereof). Similar approaches could be applied in any Member State.*

b. Other noteworthy approaches

Most solutions have implemented similar approaches, either by relying on a single policy specifying certain high-level requirements to be observed by CAs to ensure the quality of the certificate (although generally not in as detailed a fashion as the BBS approach, a variation of which will also be implemented in the course of the PEPPOL pilot) or by simply relying on the existing concepts of qualified/nonqualified certificates, like @firma and e-Notarius. In that respect, this distinction between qualified and nonqualified certificates seems to function as a de facto seal of quality for signature certificates, as the main criterion with European regulatory support in the eSignatures Directive.

In this respect, it is also worth noting summarily that the national supervision schemes for qualified certificates will be one of the main building blocks for the initiatives currently ongoing in the context of the CROBIES project. One of the outputs of this project is a draft Decision which will require Member States to put in place homogenic trusted lists of qualified CAs, made available in a common format. In this way, it will become easier for relying parties to assess whether or not a specific certificate is indeed qualified, by checking whether the issuing CA is included on the trusted list of its country of establishment. Obviously, once compiled these lists will also be a very useful resource for validation solution providers, as it can act as a de facto basis for establishing trust in foreign solutions.

Another interesting approach is the one taken by the Safelayer-TrustedX platform. When validating digital certificates and signatures, TrustedX determines the level of trust of the certificate based on the diagnostic of the underlying certificate chain. This diagnosis is expressed using LoA levels as decimal values (i.e. 0-3) and LoA labels as strings (i.e. Government, Corporative, Finance, etc...). Thus, applications can avoid any indication of complexity associated with the signature's trust (certificates, CRLs, OCSPs, etc.) and simply and exclusively focus on a decimal value and text string. The basis for determining the trust level of the certificate or the signature is the OMB/NIST Level of Assurance classification[7].

The main other noteworthy approach that is also worth identifying here is the US FBCA (Federal Bridge Certification Authority). The FBCA is not an autonomous service as such, but rather consists of a framework of specific norms and standards to determine the reliability of CAs, based on a standardized methodology for assessing compliance with these norms and standards, and a cross-certification platform allowing CAs to cross-certify with the U.S. Federal PKI Architecture at seven pre-defined assurance levels, formalised in the FBCA Certificate Policy[8], ranging from 'Rudimentary' to 'High'[9]. The approach is comparable to that of the BBS, although it is somewhat more holistic, since the policy covers all aspects related to the operation of the CA (including e.g. financial reserves, physical security of the facility, etc.), depending on the level of assurance required.

The approach is of particular interest because it constitutes a form of multi-level assurance policy with governmental backing, as opposed to the strictly contractual approach which BBS must apply (given that the European regulatory framework is less fine grained in this respect). Obviously, European concepts such as qualified certificates or supervision are not relevant in a US concept and therefore not considered in the FBCA policy.

[7] See http://csrc.nist.gov/drivers/documents/m04-04.pdf

[8] See http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[9] Exact requirements for each of these levels can be found at http://www.cio.gov/fpkipa/drilldown_fpkipa.cfm?action=pa_mappingmatrices

c. Summary conclusions

Most solutions thus only have two major options open to them:

Firstly, they can choose to rely on quality criteria with specific regulatory backing. As seen above, in Europe this implies relying on the distinction between qualified and nonqualified certificates, as defined in the Directive. While not particularly fine grained, it does have the advantage of legal certainty, as issuers of qualified certificates are supervised in their countries of establishment, meaning that there is a certain implied quality guarantee, which appears to be a suitable basis for building trust.

In addition, it is relatively easy to assert trust in this criterion on a cross border level, since the trust is derived from governmental supervision which is (in principle and at least from a legal perspective) equivalent in all Member States. The main complexity is that currently no clear overview exists at the European level of supervised CSPs issuing qualified certificates, which is one of the main reasons why both @firma and e-Notarius currently limit their services to CAs established in their own countries. However, this problem is being addressed by the CROBIES study and is expected to be resolved by the end of this year, and in this respect it is interesting to note that both @firma and e-Notarius mention the possibility of integrating CAs on these trusted lists in their respective validation solutions.

However, as noted above, even if this integration of foreign CAs were to be done, there is still the issue that non-European CAs would be hard to integrate into this model, and that the two-tier quality classification (qualified or not) may not be particularly satisfactory from a commercial perspective, as end users may have more specific desires. In that respect, the US approach of defining a global policy covering multiple tiers is an interesting example of a governmentally supported multi-level approach.

The second option is of course not to rely on certificate quality criteria with specific regulatory backing, and to define one’s own policies which are then voluntarily (typically contractually) accepted by the users of the validation solution. This is the approach which is used by BBS, as described above, and has the merit of being able to make the quality classifications arbitrarily refined (i.e. to whatever extent is considered useful by the solution provider, or more typically by its customers). It is interesting to note however that especially relatively simple European verification solutions which offer only one certificate quality level frequently do not rely on the notions of qualified or nonqualified signatures, e.g. the academic solutions TACAR and Polito. In a sense this is not surprising: in a number of use cases qualified certificates are not required, because simpler signature solutions with lesser guarantees are perfectly suitable and substantially cheaper to acquire. For these use cases, it makes relatively little sense to implement verification solutions that apply the distinction between qualified and nonqualified certificates when qualified certificates are not used in practice.

3.1.2.3.3 Criteria for determining legal signature value

a. *Observed approach in the key solutions*

@firma approach	
Observed approach	*Based on the @firma Validation Practice Statement, end users can see which CAs are supported, and whether they use SSCDs or not. On the basis of this, end users can decide whether they will accept only qualified signatures, or also advanced signatures based on qualified certificates. Other than that, @firma does not make a further classification of the type of the crypto or hash algorithms used by the application. All the standards and algorithms supported by @firma are supposed to equally provide the same overall signature quality since they follow the recommendations provided by the National Interoperability Framework and the guidelines of the National Center for Cryptology, in addition to what is available according to the state-of-the-art of the technology.*
Assessment	*As in relation to certificate quality, no separate quality framework has been implemented; the main purpose of @firma in relation to the verification of signatures is to allow the end users to confirm whether the signatures are qualified or advanced based on qualified certificates.*

BBS approach	
Observed approach	*As was also the case for certificate quality, BBS has defined its own algorithm for determining the reliability of electronic signatures. Based on certificate quality (six levels as defined above), hash algorithm quality, and public key algorithm / key size, the signature quality level is calculated as follows:* *Signature quality = certificate quality + hash algorithm quality + public key algorithm and key size quality* *Values for hash algorithm quality, public key algorithm and key size quality are set by BBS. This algorithm is amended as follows:* • *If any quality parameter is 0, signature quality is set to 0 regardless of the values of the other two quality parameters. The signature is considered too weak to be trusted.* • *If certificate quality level is 6, and both other quality parameters have value 1 or higher, the signature quality shall be set to 20. This value thus indicates a qualified signature according to the EU Directive.*
Assessment	*A multilevel framework has thus been created autonomously by BBS, which takes into account the technical characteristics of the signature as well, and is more fine-grained than the standard distinction between qualified and non-qualified signatures. Acceptance of this framework is settled through the specific agreements BBS puts in place with the relying parties, where they can specify which types of signatures (or certificates) they consider to be acceptable in their applications.*

SVS approach	
Observed approach	*The solution is able to distinguish between qualified and non-qualified certificates,*

	and can also identify Austrian official signatures. There are two degrees of validity provided by the system: trusted and not trusted. Since certificate policies are not explicitly evaluated possible restrictions are not taken into account.
Assessment	*No separate quality framework has been implemented; the solution allows the end users to confirm whether the signatures are qualified or official.*

e-Notarius approach	
Observed approach	*Like @firma, e-Notarius allows the user to determine whether a signature is qualified or not, but makes no further classification based on the type of the crypto or hash algorithms used by the application.*
Assessment	*As in relation to certificate quality, no separate quality framework has been implemented; the main purpose of e-Notarius in relation to the verification of signatures is to allow the end users to confirm whether the signatures are qualified or advanced based on qualified certificates.*

b. Other noteworthy approaches

The Safelayer TrustedX uses an approach that is fairly comparable to the BBS system: once the end user has decided which CAs to accept, he can define policies to specify the certificate validation mechanism (CRL, OCSP or other), check the certificate policy (i.e. to force qualified certificates), the signature policy or the cryptographic algorithms. Additional controls, like the role of the signer, commitment and places of signature can also be checked. Taking into account the aforementioned OMB/NIST LoA levels, TrustedX extends this concept to digital signatures in order to classify the perceived trust and reliability of the signatures. TrustedX validation and verification policies can be configured to summarize signature trust and reliability in four levels: level 0, for low assurance, level 1, for intermediate assurance, level 2, for high assurance, and level 3, for very high assurance. For instance, qualified signatures are usually at level 3. Of course, it remains up to the end user to decide which ratings to assign to which signature solutions.

c. Summary conclusions

With regard to the legal value of electronic signatures, the European regulatory framework makes only one crucial assertion, which is that advanced signatures based on qualified certificates and created using secure signature creation devices (commonly referred to as qualified signatures) are legally equivalent to hand-written signatures. From that perspective, it is not surprising that each of the key solutions above support the functionality of distinguishing qualified and non-qualified signatures.

Apart from that fact, however, answers on the legal value of an electronic signature cannot be made in general terms, i.e. by the solution provider based on generic criteria. The only functionality the solution provider can offer (in addition to distinguishing qualified from nonqualified signatures) is the ability of matching a signature's characteristics against a signature validation policy[10] required in agreement with the solution's end user. Deciding the legal effect of this signature is however the task of the end user itself, and the solution provider cannot resolve this question. The main added value of offering multiple additional levels of signatures (as is e.g. done by BBS) is therefore offering a standardised 'menu' of predefined signature verification policies from which the end user can choose, if desired. However, this does not mean that the solution provider makes assertions on the legal value of the signature in the sense of its ability to meet the end user's legal needs.

[10] Defined in RFC3125 as "a set of rules for the creation and validation of an electronic signature, under which the validity of signature can be determined."; see http://tools.ietf.org/html/rfc3125

3.1.2.3.4 Liability/responsibility model

a. Observed approach in the key solutions

@firma approach	
Observed approach	*The terms and conditions of @firma´s liability are determined in the general agreements with the customers that establish the responsibility of the VA for providing accurate validation information about the status of the qualified certificates and the results of the verification processes of digital signatures. @firma is at the same time covered by the liability contracts signed with the CAs which basically follow the provisions of the eSignatures Directive for CAs and make all of them responsible for providing accurate and up-to-date revocation information.*
Assessment	*@firma positions itself as an intermediary service, which is responsible for passing on accurate validation information as provided by the CAs to the end users. If inaccurate information is provided by the CAs, @firma has reserved the right to recover any damages from the CAs.* *@firma does not consider itself to be liable or responsible for the quality of the qualified certificates or signatures covered by the VA. The quality of the certificates is assessed by the national accreditation/supervision body.*

BBS approach	
Observed approach	*Provisions with regard to the liability of the VA are addressed both in the agreements with the CAs and with the customers.* *In the relation with CAs, specific provisions are needed as final liability lies with them (i.e. the VA assumes interim liability towards its customers insofar as this is legally required and contractually agreed with the customers, but it should be able to obtain compensation from the CAs if there was no material error on the VA's part). In this way, the VA transfers final liability to the CAs (or other information providers) if an erroneous answer from the VA is caused by erroneous information from such actors. To accomplish this, the VA will in most cases need agreements with the CAs and other information providers, as relying on general statements in a CA's policy is too ambiguous and too risky.* *In relation with the customers, the VA assumes responsibility insofar as legally required and insofar as this is demanded by the customer. The VA should ideally provide a one-stop shopping service, where all relevant liabilities related to certificate/signature verification are taken on by the VA. However, the VA's liabilities must be clearly stated and accepted by its customers, and the cost to a customer may depend on the level of risk that the VA takes with respect to the customer. Thus, liability towards the customer can be customized, depending on the requirements and willingness to compensate for this necessity on the customer's side.*
Assessment	*BBS positions itself as an intermediary service, which is responsible for passing on accurate validation information as provided by the CAs to the end users. If inaccurate information is provided by the CAs, BBS has reserved the right to recover any damages from the CAs.* *As a commercial service, BBS' willingness to assume liability towards the end user*

	depends on the specific guarantees sought by the end user, and the resulting compensation paid. BBS can thus operate as a one-stop shop, provided that this is desired (and paid for) by the end user.

SVS approach	
Observed approach	*SVS relies on the general liability provisions of the eSignatures Act and the Civil Code, and offers/requires no specific additional guarantees from end users/CAs.*
Assessment	*No further comments.*

e-Notarius approach	
Observed approach	*As noted above, while e-Notarius has business agreements with the relying parties (end users), it does not put in place agreements with the CAs. In relation to the end users, e-Notarius' liability is specified in its CPS, and its liability is guaranteed in accordance with the regulations for the Polish Act for qualified CSPs.*
Assessment	*e-Notarius relies on the general liability provisions of the eSignatures Act in Poland, and has not acquired specific additional guarantees from the CAs.*

b. Other noteworthy approaches

No individual noteworthy approaches stand out; however, it should be noted that there appears to be much reticence to accept specific responsibilities and liabilities, and much unclarity as regards the application of the eSignatures Directive's provisions on liability in relation to verification services.

One interesting contribution was provided in the Cryptolog profile however, which noted that *"[w]e believe a clear difference should be made between:*

- *A signature verification platform*
- *A signature verification service*
- *A signature verification authority*

The way we view this difference is the following:

- *A signature verification platform provides a "technical service". It takes as input a signature verification policy and a signed document and provides a technical answer.*
- *A signature verification service is an instance of a signature verification platform together with a given signature verification policy. In that case, questions regarding "quality", "reliability" and "legal value" of the signature make sense, as they depend on the parameters on the signature policy. However, the answer is still technical.*
- *A signature verification authority is a signature verification service that will take universal liability on top of the technical validation answer. While we have nothing against such an authority, we believe it is not strictly needed. Indeed, one could provide means to extend the signature regularly in order to ensure that it will always be (re)verifiable by any third party (this is the approach taken by our solution). In that*

> *case, there is no need of "trust" (in the Trust Service Provider – TSP) sense. Rather, the service is technical."*

This is ultimately the approach taken by a number of technical verification platforms which an end user can implement and configure locally, making his own choices and assuming full responsibility for this. The same applies e.g. also to the Austrian MOA software modules, the Governikus platform and the TrustedX platform. The later noted in this respect:

> *Safelayer only guarantees that the product will work according to technical specifications described in the instructions manuals and under the terms described in the licence agreement. Safelayer also guarantees the product interoperability and assurance through interoperability reports, and Quality and Common Criteria certifications.*

With respect to trusting certificates and signatures however, "*the relationship with the relying parties and CAs has to be established by the operator/user of the solution based on TrustedX. From the technical perspective, TrustedX facilitates the implementation of established agreements, providing a powerful and flexible policy based system.*"

c. Summary conclusions

As witnessed in the four key solutions, the approaches to liability differ in important nuances. While @firma clearly profiles itself as an intermediary between the end user and the CA (with the latter always bearing ultimate responsibility), it has none the less put in place specific agreements to make this matter explicit.

The BBS solution takes a similar approach, requiring contracts with the supported CAs "*as relying on general statements in a CA's policy is too ambiguous and too risky."* Unlike the @firma approach, BBS is willing to profile itself as the sole point of responsibility, provided of course that the customer pays for this service (which is of course a possibility that @firma does not have, being a publicly funded solution.

Finally, SVS and e-Notarius seem to take a similar approach by profiling themselves as an intermediary, but without relying on specific agreements with the CAs. Rather, they depend on the standard liability provisions contained in the Directive and the applicable transpositions thereof.

Globally, there is much uncertainty as regards the application of the eSignatures Directive's provisions on liability in relation to signature verification services, an issue which will be explored further in the sections below. In addition, as seen in the contribution from Cryptolog quoted above, there is even some question whether validation authorities (i.e. authorities assuming liability towards the end users[11]) are really necessary, and whether purely technical services (preferably offered by the original CA) would not also be adequate.

[11] More accurately defined in RFC3125 as "entities that help to build trust relationships between the signer and verifier", including Signature Policy Issuers, but also other more generic service providers such as CAs, RAs, Repository Authorities, Time-Stamping Authorities, OCSP responders, and Attribute Authorities. See http://tools.ietf.org/html/rfc3125

3.1.2.3.5 International legal model

a. Observed approach in the key solutions

@firma approach	
Observed approach	*@firma presently does not have an international model in place, since it currently focuses exclusively on Spanish CSPs issuing qualified certificates. However, as noted above, the reason for this focus is that these certificates offer some guarantee of quality due to the supervision/accreditation model implemented in Spain and in all other Member States. Thus, the model could be extended to other European CSPs issuing qualified certificates to the public.*
Assessment	*The approach could be extended across Europe, although it may be difficult to do so based on entirely the same model as has been applied so far, since @firma currently requires contracts with each of the CSPs. To apply this approach across Europe, @firma would either have to obtain similar agreements with each CSP directly, abandon this requirement altogether, or find a way to implement this approach in a federated model (i.e. by having similar solutions to the @firma one established in other MS, which apply the same or similar agreements with their national CSPs).* *From a broader international perspective (i.e. outside the EU), the current dependence on European concepts of qualified certificates and supervision means that interoperability possibilities are limited.*

BBS approach	
Observed approach	*As noted above, while BBS uses European concepts such as qualified certificates and supervision, these are not required to apply its solution, since it is largely based on contracts. Thus, the service can (and does) operate in a broad international context, including outside of the EU.*
Assessment	*No additional comments.*

SVS approach	
Observed approach	*As noted above, decisions to support specific CAs are made autonomously by the solution provider. Thus, the service could operate in a broad international context, including outside of the EU (although presently, it doesn't).*
Assessment	*No additional comments.*

e-Notarius approach	
Observed approach	*Like @firma, e-Notarius presently does not have an international model in place in its commercial service, since it currently focuses exclusively on Polish CSPs issuing qualified certificates. However, as noted above, the reason for this focus is that these certificates offer some guarantee of quality due to the supervision/accreditation model implemented in Poland and in all other Member States. Thus, the model could be extended to other European CSPs issuing*

	qualified certificates to the public. In addition, it should be noted that the demo service operated by e-Notarius also interoperates with a Russian DVCS (Data Validation and Certification Server).
Assessment	*The approach could be extended across Europe with relative ease, provided that e-Notarius could get an overview of European CSPs issuing qualified certificates to the public, as is currently being established in the context of the implementation of the Services Directive. As shown through the demo service, interoperability with countries operating under comparable frameworks is also possible, although in this case the non-European CSPs would need to become accredited as issuers of qualified certificates under the conditions defined by the Directive, and e-Notarius would likely need to offer the necessary guarantees before this could be done.*

b. Other noteworthy approaches

In relation to the other examined solutions, the US FBCA solution is again an interesting example of an alternative approach, as it explicitly allows for the cross-certification with other bridges, subject to some additional requirements. The list of current cross-certified entities presently includes two bridges: the CertiPath Bridge and the SAFE-Biopharma Bridge. In addition, the terms of the FBCA allow it is cross-certify with non-U.S. based PKIs as well. However, applications from non-US organisations, countries or sub-federal entities of a country would only be considered if there are "*reasonable expectations from a US Federal Government entity that it would benefit from being able to do PKI-based transactions interactions with the applicant entity, and/or where it would be in the interest of the U.S. Federal Government's international relations to cross-certify*."

Among the technical solutions examined, the TrustedX platform offers the broadest interconnectivity possibilities, not being inherently linked to the European context, and by offering the possibility of connecting with any other type of island of trust, whether in a hierarchical or crossed/federated model. TrustedX can be configured to interoperate with VAs provided by CAs as well as with global VAs and Validation Platforms. In fact, TrustedX has been configured to use the @firma key solution by default.

c. Summary conclusions

In summary, a clear distinction must be made between solutions that rely on the European concepts of qualified certificates and supervision, and those which operate mainly or exclusively on a contractual basis. The former can typically operate with greater ease within Europe, given that they derive a substantial part of their trustworthiness from existing government controlled supervision schemes, but have a harder time extending beyond a strictly European perspective. Inversely, contractual frameworks have no such restriction, but require agreements to be put in place with each participants, or accept an inordinate liability towards the end users. Thus, there is a trade-off to be made here, with no clear superior choice.

3.2 Impact on interoperability

The overview in section 3.1 examined the main approaches taken by the signature verification solutions to overcome specific parts of the interoperability challenges. In this chapter, we will attempt to address these challenges more systematically, specifically by addressing the following points:

- Identifying the interoperability challenges that need to be resolved
- Identifying how our key models address these (if they do)
- Identifying the gaps to be filled to achieve European electronic signature interoperability

3.2.1 Technical Interoperability problems

The technical problems listed in this chapter have been considered as barriers for the cross border recognition of eSignatures in the European Union. These problems have been identified in the “Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications” RD3. In this section, only a summary overview is provided, and we refer to the “RD3” documents for more details.

3.2.1.1 Trustworthiness of CAs

Determining the trustworthiness of a CA is a complex process: one must assess assurance levels, certificate policies and certification practice statements; conduct annual audits; establish qualification agreements (SLA, QoS …), etc.

To determine the CA trustworthiness in the validation process it is required to:

- Asses that the CA is trustworthy, and that the quality of the certificate is acceptable in relation to its intended use;
- Be capable of validation of the CA’s signature on the certificate. This requires a trusted copy of the CA’s own public key, which may be either directly available, or which may be obtained from further certificates in a certificate chain.

The situation of a European level eGovernment application can become quickly unmanageable: even if we consider that the application has to support a relatively modest number of e.g. 3 CAs per Member State, then this still implies that a relationship with more than 80 CAs must be managed. In reality, the number can be expected to be substantially larger than this.

3.2.1.2 Semantic interpretation of certificate fields

There is a lack of consistency in the semantic interpretation of certificate fields within various digital certificate implementations. Not all European CSP give the same meaning to the same certificate fields. Therefore, it is currently up to each application or national framework to develop:

- Ad-hoc parsing by “certificate type”,
- Specific OCSP/CRL connections,

- Ad-hoc syntax and semantic checks of certificates

The management problem (i.e. the scaling issue) is the same as the one described in the "Trustworthiness of CA" chapter. It will become quickly a nightmare for an eGovernment application to maintain specific semantic interpretation of fields for each supported European CA.

3.2.1.3 Incompatible use of identifiers

This issue identified by the aforementioned study concerned signatures based on certificates where the application requires the certificate to contain a specific National/Sectoral/Regional unique number.

If the expected identifier is not found in the certificate, applications simply stop their processing and reject the signature request. This is a clear barrier against the cross border interoperability.

This interoperability issue is the consequence of a design decision of the eGovernment applications owner. It cannot be solved by a VA but by modifying the design of the concerned applications. Therefore **it is out of scope** of this analysis. For completeness' sake, it should be added that this issue is addressed to some extent within the CROBIES study surrounding the "Common Minimum Requirements for a Qualified Certificate Profile supporting Qualified Electronic Signatures". As such, the CROBIES work is aimed at establishing a better and more harmonised implementation of the aforementioned TS 102 280 standard. One of the main expected impacts will be the mandatory use of a harmonised serialNumber within the Subject field of the certificate, which should ensure that at least a basic resource is available to unambiguously identify signatories.

3.2.1.4 Signature Type

Establishing when a signature can be accepted as a Qualified Signature is difficult in practice. This is caused by the fact that Qualified Certificates Statements "qCStatements extension" as defined in the RFC 3739 is optional and not (yet) systematically used. Perhaps more importantly, there is no clear way at this time to establish if the signature creation device that was used by the signatory can be considered an SSCD in the sense of the Signatures Directive. Thus, especially at a cross border level, it is very complicated to identify qualified signatures as such. Again, this issue is being addressed within the context of the CROBIES study, specifically the aforementioned efforts related to the establishment of national trusted lists of supervised CAs issuing qualified certificates to the public. The resulting national lists should prove a highly useful resource in addressing this issue.

3.2.1.5 Dedicated Interface requirements

Another factor identified by the aforementioned study which is limiting interoperability at the technical level is applications requiring specific non-standardised interfaces to be installed on the user's workstation prior to sign a document.

Here we don't talk about the middleware necessary to 'drive' the token containing the credentials necessary for the signature (e.g. smartcard driver) but a client signing tool to be installed on the user workstation.

This interoperability issue is the consequence of a design decision of the eGovernment applications owner. It cannot be solved by a VA but by modifying the design of the concerned applications. Therefore **it is out of scope** of this analysis.

3.2.1.6 Signature format

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

Anyway, even if this exchange of documents has not yet been deemed necessary by application providers surveyed in the "Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications" RD3, it seems obvious that it will be more and more frequently requested in the future. It was recommended in “RD3” to promote the use of international standards like CAdES or XAdES, but it is be also recommended to support documents with multiple signature formats. This issue is also being examined within the context of the CROBIES study, specifically by examining the possibility of harmonising existing signature formats for the public sector.

3.2.1.7 Certificate Validation protocol

Not all the validation protocols are supported by surveyed eGovernment applications in the “Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications” RD3 study. Some applications support only CRLs while others support only OCSP.

Among surveyed CSPs in Europe, not all have deployed an OCSP responder. eGovernment applications supporting only OCSP cannot verify the validity of the certificate issued by a CSP which has only deployed CRLs. It is clear that this issue needs to be addressed by validation authorities.

3.2.2 Legal interoperability problems

As with the technical problems listed above, legal issues have also been identified in the “Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications” [RD3]. Again, we will provide a summary overview of the identified issues below, in order to determine in a second stage if and how these issues have been addressed by the key solutions.

3.2.2.1 National perspective - trustworthiness of CA

The issuing of determining the trustworthiness of CAs is of course not purely technical in nature. Most countries, as far as they have adopted electronic signatures in their e-government applications, have organised this without taking into account electronic signatures created by companies and individuals from 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. Serving more marginal categories, such as the occasional users from other countries, is not considered as a first priority.

3.2.2.2 Security levels – legal qualification of signature types

For similar applications, Member States don’t necessarily require the same type of electronic signature. It is perfectly possible that a similar application in one Member State is only based on user-id/password protection while another Member State requires qualified electronic signatures for the same type of transaction. This presents a dual risk: on the one hand, it is possible that eventually every company and individual in every Member State will need to have a complete set of electronic signature facilities (at least including a qualified electronic signature facility), and on the other hand, it is necessary for service providers to be able to determine the legal qualification of signature types from foreign users.

3.2.2.3 eSignature Directive compliance – prior authorisation and the public sector clause

Many Member States require end users to use signature certificates issued by a limited set of certification service providers (e.g. CSPs which are supervised, accredited or otherwise 'recognised' in that country). It is questionable whether this is compliant with Article 3.1 of the European Directive 1999/93/EC, since this could be construed as a requirement which is "de facto" equivalent to a prior authorisation. If these restrictions are to be seen as an application of the "public sector clause" (Art. 3.7) of the Directive permitting the introduction of additional requirements for signatures used in the public sector, then it seems questionable whether this is a defendable interpretation.

This interoperability issue is the consequence of a design decision of the eGovernment application owner. It cannot directly be solved by a VA; however, the availability of VAs that can provide assertions on the reliability and value of foreign signature types may induce eGovernment application owners to eliminate such restrictions. The issue is **out of scope** of this analysis.

3.2.2.4 National rules on identifiers

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). The current national rules in this domain don't take into account processing by public authorities or service providers of other Member States.

Solutions have to be developed in the framework of e-ID interoperability. These will most probably include legislative amendments in some of the surveyed countries.

Again, this interoperability issue is the consequence of a design decision of the eGovernment application owner. It cannot be solved by a VA but by modifying the design of the concerned applications. Therefore **it is out of scope** of this analysis.

3.2.2.5 Responsibility and liability

One of the main reasons why foreign signatures cannot easily be accepted in eGovernment applications is the current impossibility of obtaining sufficient guarantees with regard to the reliability and value of such signatures, backed by an entity willing to take responsibility and liability for making assertions related to this point. Of course, this is the entire point of utilising a VA.

3.2.3 Observed Interoperability approach analysis

This part will analyze if the key solutions answer the issues summarily outlined above.

Concerning the technical issues questions are:

1. Concerning the **Trustworthiness of CA** at the technical level: Is this problem solved by the key solutions? The answer is "Yes" for all the solutions because by nature this is one of the main functions of a Validation Authority".
2. Concerning **Semantic interpretation of certificate fields**: Do the key solutions provide a interface to return to the caller the semantic interpretation of certificate fields?
3. Concerning the **Signature Type**: How do the key solutions handle the quality of the certificate/signature?
4. Concerning the Signature format: Do the key solutions support international standard formats and are they able to manage documents with multiple signature formats.
5. Concerning the **Certificate Validation protocol**: Do the key solutions provide an interface to the caller that is independent of the protocol used by the VA to validate the certificate with the CA (OCSP/CRL/LDAP). The answer is "Yes" for all the solutions because by nature this is one of the main function of a Validation Authority".

The following table gives an answer to these questions.

	Trustworthiness of CA[12]	**Semantic interpretation of certificate fields**	**Signature Type**	**Signature format**	**Certificate Validation protocol**
@firma	Yes at the National level (See Relationship with the CAs and relying parties)	Yes	Yes: By associating a profile by application (i.e Application can request to reject the validation when the certificate is not qualified).	Yes (See Signature verification approach)	Yes: By web service interface or OCSP responder.
BBS	Yes at the international level	No	Yes: the validation request returns	Yes (See Signature	Yes: By web service interface

[12] Trustworthiness of CA at the European level will be achieved to some extent by the publication of TSL list of supervised TSP by country by the end of 2009.

	Trustworthiness of CA[12]	Semantic interpretation of certificate fields	Signature Type	Signature format	Certificate Validation protocol
	(See Relationship with the CAs and relying parties)		the classification.	verification approach)	
SVS	Yes for supported CAs (chosen at the solution provider's discretion) (See Relationship with the CAs and relying parties)	No	Yes: key characteristics of the signature are communicated to the end user	Yes (See Signature verification approach)	Yes: through OCSP/CRLs.
e-Notarius	Yes at the National level (See Relationship with the CAs and relying parties)	No	Yes: when adding new CA the quality is configured in the system.	Yes (See Signature verification approach)	Yes: part of the DVCS protocol.

Table 1: Interoperability issues resolution by key solutions

Concerning the legal issues, the key questions are:

1. Concerning the **trustworthiness of the CA** at the legal level: can the solutions provide an answer to the question whether or not the certificates issued by supported CAs can be considered reliable according to the criteria established in agreement with the user of the solution's services?
2. Concerning the **legal qualification of signature types**: can the solutions make a statement on the legal qualification of the signature being presented, which means specifically that qualified and non-qualified signatures can be readily distinguished?
3. Concerning **responsibility and liability**: do the solutions accept responsibility and liability for making assertions on the reliability and value of supported signatures, backed a credible liability model?

Obviously, the answer is affirmative for all of the key solutions, since these are the criteria that were used to select the key solutions from all the examined validation solutions. However, it should be noted that only BBS and SVS have a cross-border interoperability scope; @firma and e-Notarius work on an exclusively national level and support only qualified certificates. The main reason for this is precisely that this allows them to leverage existing national trust structures related to those certificates. The key challenge to be addressed is precisely how such services could support other certificates (for which no such implied trust model exists) outside of a purely national context.

3.2.4 Interoperability gap analysis

In this section, we will attempt to identify what specific issues have not yet been addressed, and what would conceptually be needed to get to the goal defined above. Key inputs from other projects will also be taken into consideration to detect how/if they are handling these issues.

At the technical level almost all our key solutions contain answers to the issues indentified in the “Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications” RD3.

The exceptions are semantic issues, which are not covered by BBS and e-Notarius. Without this function, each eGovernment application needs to obtain the knowledge of the semantic behind fields (they need to extract the information) of all certificates they process.

Concerning the possible interoperability between any EU Member States’ VAs, our key solutions indicated the lack of:

- An appropriate EU legal framework for VA services. What is the definition of a VA, what are VA services, what is the liability model for the VA, what is the supervision/accreditation scheme, …To some extent this issue is addressed by the general rules of the Signatures Directive, but this impact is largely limited to qualified certificates and signatures based on these.
- An appropriate EU legal framework for Time Stamping services. Some Member states have created their own supervision and/or accreditation scheme but due to the lack of an EU supervision/accreditation scheme, the cross-border interoperability is very difficult, meaning that end users must assess the validity and value of foreign time stamping services on a case by case basis.
- Standardisation for VA-to-VA communication protocols, if a federation were to be created. Some VAs have developed their own web service interface specifications, whereas other VAs use existing protocol like DVCS, OASIS-DSS or XKMS.

3.3 Addressing legal and trust issues in an EU level validation platform

In this section, we will examine how the trust/legal issues identified above could be addressed by a platform operating at the European level, including the main restrictions if the European Commission would like to operate such a platform itself. Obviously, the provisions of the Signatures Directive will play a crucial role in addressing these issues. The end result should be a proposal for a high level framework for European signature verification services, including the role that the European Commission could play in this respect.

3.3.1 Summary of main needs

Firstly, we need to examine what the main legal and trust issues are in a European signature verification context, i.e. the specific issues that need to be addressed by any signature verification service provider. This will establish the basic requirements that need to be addressed by any forthcoming European initiative.

3.3.1.1 Definition of the service

As noted above, the main functions of a validation authority relate to:

- The capability of determining the validity of a signature certificate at the time of signature verification;
- Verifying the technical validity of the signature itself;
- Providing some assurance on the trustworthiness of the signature, in particular by providing certain guarantees in relation to the CA and thus at a minimum to the signature certificate. This may involve:
    - Confirmation that the certificate is qualified in the sense of the Signatures Directive
    - Confirmation that the signature is a qualified signature (legally equivalent to a hand written signature)
    - Confirmation that the signature meets requirements prescribed by the end user (which may include both of the above, but could also simply relate to e.g. the certificate originating from a set of pre-approved CSPs)
    - Creating a complete certificate chain (which is at any rate necessary up to a point that is recognised by the validation authority)
    - Classifying the certificate or the signature as a whole according to a criteria system developed by the validation authority.

In addition, some other services may be functionally necessary for the end user of the service, even though they do not strictly relate to the validity of the signature itself. These include the semantic services mentioned above (since even a valid signature is of little value to the relying party if he or she cannot determine who or what the signatory is), and the historical verification of signatures (since a signature may be verified a significant amount of time after which it is created). The latter two elements are still rather rarely found as services offered by signature validation authorities, but the set of functions above appears to be ubiquitous. It is clear that any European initiative will need to support these at a minimum.

3.3.1.2 Quality of the service: certificate and signature

From a trust perspective, one of the most complicated issues is determining the quality of the signature certificate being used and the signature created with this certificate. From a legal perspective, the European regulatory framework essentially offers only two major reference points: a signature certificate is either qualified or not qualified, and an electronic signature can be either qualified (or in strictly legal terms: an advanced signature created using a qualified certificate and a secure signature creation device or SSCD) or nonqualified. It is therefore not surprising that two of the key solutions use only this distinction, and cannot make any judgments on the quality of signatures that do not use qualified certificates (or on nonqualified certificates as such).

Strictly speaking this does not need to be a problem, especially in environments where qualified certificates are relatively abundant and commonly used. However, this description is certainly not applicable to the whole of the European market as it stands. In this respect, an acceptance that European validation authorities will only be able to make any statements in relation to the quality of qualified certificates and/or qualified signatures may be seen as being out of phase with market realities. It would be desirable for validation authorities to have a wider range of options open to them. It should be noted that this is not merely a matter of policy preference, but also of necessity, since most Member States have interpreted the notion of a qualified certificate to mean that it can only be issued to natural persons, and not to legal entities (with Spain being a notable exception in this regard). Thus, validation authorities that can only validate signatures based on qualified certificates are inherently limited to validating signatures created by natural persons, at least in most Member States. This may prove to be a significant restriction, especially considering the number of application fields (like procurements, taxation, invoicing etc.) where signatures from companies may constitute a majority.

Of course, the latter issue of validating signatures created on behalf of legal persons could also be resolved by alternative means, including by harmonising the semantics behind authorisations included in qualified certificates, i.e. making it easier for relying parties to determine whether a signature was created by a natural person acting on his own behalf, or rather on behalf of a legal entity, on the basis of specific attributes in the signature certificate. However, this would obviously require a certain degree of harmonisation in this field, and would require validation authorities to become much more deeply involved in semantic services, neither of which is a trivial task. Finally, since advanced signatures that do not rely on qualified certificates still occupy a very significant portion of the PKI market, it seems desirable to ensure that validation authorities are capable of serving this market as well.

To do so, validation authorities in Europe currently don’t have any alternative than to define their own reliability requirements, in the form of proprietary policies such as the one developed by BBS for its own clients. Of course, these policies do not have any binding legal value in their own right, but rely on purely contractual frameworks, i.e. it is up to the customers to define which signature certificates and signature requirements they deem to be adequate. The main risk from an interoperability perspective is that validation authorities would each opt to define slightly different and mutually incompatible policies, which may make it harder or even impossible for validation authorities to interoperate in a federated model, should they deem this desirable.

From that perspective, it is interesting to note that the US has addressed this issue by establishing its own assurance levels via the FBCA policy. In this way, the whole of the US could (but is not required to) apply these criteria to assess the reliability of specific CA services in a homogeneous way. This is certainly an approach that would offer clear benefits, provided of course that a federated European electronic signature validation solution would be considered desirable, and that it would be envisaged to also cover nonqualified signature certificates in this solution. Inversely, if the policy emphasis were to remain exclusively on qualified signature certificates, then the presently ongoing initiatives aiming to create national trusted list of supervised and accredited CSPs (to be coordinated also at the European level) are largely sufficient to address most of the trust issues. Obviously, in practice trust needs to be backed up by adequate liability arrangements. This specific issue will be examined separately below.

3.3.1.3 Legal value of the signature

The Signatures Directive's approach with regard to the legal value of electronic signatures is at the same time relatively simple and very nuanced, as captured in article 5 – legal effects of electronic signatures, which reads as follows:

> *1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:*
>
> *(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and*
>
> *(b) are admissible as evidence in legal proceedings.*
>
> *2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:*
>
> *- in electronic form, or*
>
> *- not based upon a qualified certificate, or*
>
> *- not based upon a qualified certificate issued by an accredited certification-service-provider, or*
>
> *- not created by a secure signature-creation device.*

This results in a situation where the legal value of a signature as described in par.1 (a qualified signature) can be summarised as being equal to that of a handwritten signature, whereas all electronic signatures can benefit from the non-discrimination rule of par.2, which essentially means that they cannot be summarily denied legal effectiveness on the grounds noted above. In practice, this means that only for qualified signatures the legal effect is universally and unambiguously clear; any other type of electronic signature may have its legal effect challenged on the basis that it does not sufficiently meet the basic requirements of a signature. This however should not be read to mean that only qualified signatures have a real purpose in the market: in practice, the legal frameworks in most Member States have only a limited number of legal actions that require a handwritten signature (which would thus typically need to be replaced by a qualified signature for undisputable legal certainty). Many actions do not require a signature at all, and can be easily replicated in an electronic context with more basic signature types.

The latter decision of accepting the legal validity of signatures other than qualified signatures is however not one that can be made in general terms, since it is dependent on the applicable legal framework (formalities may be more strict in some countries than others) and on the specific context (some transactions and some parties will require greater security than others). The main consequence of this diversity from the perspective of a validation authority is that it can only make two types of useful assertions to the user of such a service: either it can confirm that a signature is qualified (and therefore legally equivalent to a handwritten signature), or it can confirm the necessary characteristics of the certificate and signature to the end user. Either way, the ultimate decision of accepting whether or not the signature is legally capable of meeting the end user's needs remains with the end user itself (as even in the case of qualified signatures, other requirements may apply).

In that respect, as was already noted in section 3.1 above, the only functionality the solution provider can offer (in addition to distinguishing qualified from nonqualified signatures) is the ability of matching a signature's characteristics against a signature verification policy required in agreement with the solution's end user. Deciding the legal effect of this signature is however the task of the end user itself, and the solution provider cannot resolve this question. The main added value of offering multiple additional levels of signatures (as is e.g. done by BBS) is therefore offering a standardised 'menu' of predefined signature verification policies from which the end user can choose, if desired. However, this does not mean that the solution provider makes assertions on the legal value of the signature in the sense of its ability to meet the end user's legal needs.

From a European perspective, the question then remains the one noted above, which is whether it would be useful to formulate standardised European policies that would create additional levels of electronic signatures (other than qualified or nonqualified), in much the same way that the BBS solution has done from a commercial perspective, or that he FBCA has done with governmental backing. The purpose of such policies would not be to regulate the legal value of such signatures – this is already regulated by the Signatures Directive – but rather to ensure that the users of validation services (or indeed of signature services in general) have an easier option to identify the assurances linked to non-qualified electronic signatures. Thus, this is not a legal support measure, but it can nevertheless substantially facilitate the creation of trust.

3.3.1.4 Responsibility and liability of the validation authority

In this section, we will examine the question of which responsibility a validation authority needs to accept to offer the services identified above, and in relation to this question, whether or not a validation authority is necessary, and whether a federated validation authority (or more accurately a federated network of validation authorities) is a viable option.

3.3.1.4.1 Liability under the Directive

A first pressing issue is the question of liability: what are the liabilities a validation authority needs to accept under the Signatures Directive? This issue is regulated by article 6 of the Directive, the first paragraph[13] of which notes that:

> *1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:*
>
> > *(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;*
> >
> > *(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;*
> >
> > *(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;*
>
> *unless the certification-service-provider proves that he has not acted negligently.*

The question arises mostly in relation to the concept of “guaranteeing” a qualified certificate to the public, which causes the aforementioned liabilities to become applicable. This notion has already been subject to some discussions and some scrutiny, in particular in relation to two questions: does this question relate to *any* type of guarantee in relation to qualified certificate, and does a technical validation service type of guarantee in relation to qualified certificate, and does a any certificate validation service *by definition* result in such a guarantee?

The first question is caused by the simple fact that the Directive only refers to “guaranteeing a certificate” in two places: firstly in the liability provision above, and secondly in the provisions related to international aspects of electronic signatures. More specifically, article 7 of the Signatures Directive specifies when certificates issued by

[13] The second and third paragraphs of this article pertain respectively to the liabilities of CSPs issuing qualified certificates to the public in relation to revocation (par.2) and the possibility of indicating limitations of use (par.3) or value (par.4) in qualified certificates; these are of less direct importance from the perspective of the validation authority.

non-European CSPs can be considered legally equivalent to qualified certificates as defined in the Directive. As one of the options, article 7 notes the following:

> *"1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:*
>
> *[...]*
>
> *(b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; [...]"*

Thus, "guaranteeing a certificate" in the sense of article 7 relates to the situation where a European CSP warrants to third parties that the certificate is sufficiently reliable to be considered a qualified certificate in accordance with European norms. On this basis, it has been argued that the liability provision of article 6 in relation to guarantees *only* applies to the situation where a European CSP makes such a statement in relation to non-European certificates. While it seems logical that the notion has the same meaning in article 6 and 7, neither provision addresses the fundamental question of what it means to "guarantee a certificate".

This is precisely what the second question above refers to: does a certificate validation service *by definition* result in a guarantee? In other words, is it possible to offer a technical validation service in relation to qualified certificates that does not result in a guarantee (and thus potentially in liability, depending on the interpretation given to article 6)? The Directive is not clear on this issue.

If we look at the key solutions above, we see that the matter is also interpreted and handled in different ways. The @firma solution confirms that it considers itself liable as an intermediary service that provides guarantees to the end users, but adds that it puts agreements in place with the CAs and end users of the service to make this matter explicit. The BBS solution takes a similar approach, requiring contracts with the supported CAs "*as relying on general statements in a CA's policy is too ambiguous and too risky."* Unlike the @firma approach, BBS is willing to profile itself as the sole point of responsibility, provided of course that the customer pays for this service. e-Notarius' approach is more ambiguous, as it depends purely on the standard liability provisions contained in the Directive and the Polish transposition thereof in relation to the liabilities of CSPs issuing qualified certificates.

In contrast, in the section above we have also frequently made reference to validation solutions which take the position that they are not authorities, in the sense that their technologies must be installed and used by their customers on their own responsibility. This is the case i.a. for the Austrian MOA solution, the TrustedX platform, VPS-Governikus, and Cryptolog. All of these are advanced and flexible validation solutions which the end user can configure to support the validation of any signatures that they consider to be sufficiently trustworthy. However, none of the solution providers makes any statements on the reliability of individual CAs, nor do they accept specific liabilities in this respect. At least from the perspective of these solution providers, it is possible to offer certificate validation services without a guarantee in the sense of the Directive.

The issue of guarantees in terms of Article 6 of the Directive was also examined in the 2003 Study on The Legal and Market Aspects of Electronic Signatures[14], which noted that:

[14] See http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

> *"Certainly, the guarantee required will have to go beyond a simple recognition of the other CSP's public key, as it is the case in cross certification. In most cases, the guarantee will be provided in a contract between CSPs and subsequently communicated to the public through the certificate practice statement of the issuing provider of the Qualified Certificate. The guarantee should cover at least the items mentioned in paragraph (1) and (2) of Article 6. One case of guaranteeing a certificate is mentioned in Article 7.1(b) of the Directive (see further)."*

Thus, in this case, the guarantee was interpreted to take the form of a legal arrangement between CSPs, with guarantees in relation to non-European CSPs being considered an example. The simple technical recognition of another CSP's public key was not considered sufficient in this respect; an underlying legal commitment expressed in the form of an agreement or policy seems to be required.

The comment quoted above from the Cryptolog team seems to support this interpretation, as they noted that *"[w]e believe a clear difference should be made between:*

- *A signature verification platform*
- *A signature verification service*
- *A signature verification authority*

The way we view this difference is the following:

- *A signature verification platform provides a "technical service". It takes as input a signature verification policy and a signed document and provides a technical answer.*
- *A signature verification service is an instance of a signature verification platform together with a given signature verification policy. In that case, questions regarding "quality", "reliability" and "legal value" of the signature make sense, as they depend on the parameters on the signature policy. However, the answer is still technical.*
- *A signature verification authority is a signature verification service that will take universal liability on top of the technical validation answer. While we have nothing against such an authority, we believe it is not strictly needed. Indeed, one could provide means to extend the signature regularly in order to ensure that it will always be (re)verifiable by any third party (this is the approach taken by our solution). In that case, there is no need of "trust" (in the Trust Service Provider – TSP) sense. Rather, the service is technical."*

This interpretation (apart from the observations in relation to the need for a validation authority, which we will revisit below) is reconcilable with the opinion expressed above: the notion of "guaranteeing a certificate" does not attach itself automatically to any technical service related to a qualified certificate, including services aiming to confirm the validity of such certificates. Under this interpretation, there is only a "guarantee" (and thus liability) when the CSP offering the services in relation to such a certificate has put in place a legal framework in which it assumes responsibilities towards the end users themselves. Services which are provided on an 'as is' basis, without any assumed responsibilities or warranties provided, do not provide such guarantees or accept any liabilities. This would e.g. be the case for the Austrian SVS validation service, which does not claim to assume any liabilities towards the end user.

Of course, this is even more applicable to platforms which have to be installed and configured locally, like the MOA open source software, Cryptolog, TrustedX or Governikus. In each of these cases, the solution provider merely distributes a platform which the user can install at configure based on his own preferences. The solution providers (i.e. the vendors of the platform) do not offer specific guarantees in relation to the validation services performed thereafter. It is of course perfectly possible that the customers who install and configure such platforms then offer specific guarantees to their end users, which would make these customers into validation authorities themselves.

This is indeed a rather logical conclusion: purely technical validation services which disclaim any responsibilities towards the users do not accept any liabilities (neither under Article 6, nor independent from it), but also are of very limited use. Inversely, if a validation service provider does accept certain responsibilities and expresses commitments towards the end user, then liability attaches itself to the service provider. However, to address this specific issue article 6 of the Directive is not strictly necessary, since the guarantees and liabilities accepted by the validation service provider are then defined on a consensual basis. In that respect, it seems that general liability rules for certification services are sufficient, and article 6.1 does not appear to be linked by definition to validation services.

None the less, the question of liability is an element that needs to be strongly considered in a cross border context if eSignature interoperability in public sector applications is to be resolved: in order to be trustworthy, a model for the cross border verification of certificates or signatures needs to be able to accept certain liabilities. In a federated model, this means that service providers which delegate the verification of foreign certificates to other validation authorities in the country of origin must have a legal framework in place to make claims against these validation authorities; otherwise liability becomes unmanageable.

3.3.1.4.2 The need for an authority?

As was already noted above, a crucial question that needs to be examined is not only whether a validation authority is feasible and how, but also whether it is necessary. The Study [RD3] quoted above concluded that a validation authority - possibly in a federated form, i.e. a federated network of interconnected local validation authorities – would be beneficial and a suitable way to address the interoperability issues in relation to electronic signatures. This opinion is however not universally supported.

The comment from the Cryptolog team took the opposing position, noting that *“a signature verification authority is a signature verification service that will take universal liability on top of the technical validation answer. While we have nothing against such an authority, we believe it is not strictly needed. Indeed, one could provide means to extend the signature regularly in order to ensure that it will always be (re)verifiable by any third party (this is the approach taken by our solution). In that case, there is no need of “trust” (in the Trust Service Provider – TSP) sense. Rather, the service is technical.”*

In fact, there is no real conflict between these opinions. The original recommendation of working towards a validation authority was based on the situation as it exists today, and on the necessity to find a way to address the remaining gaps in e-signature interoperability. It is recognised that there are many ways to do this, which includes in particular improving signature standardisation and harmonisation efforts: if all CSPs could apply a systematic approach based on a limited amount of strictly observed standards, and uniform signature validation solutions were made easily accessible to all third parties, and remaining gaps (such as the lack of trusted lists of CSPs issuing qualified certificates and a clear overview of existing SSCDs) were filled, then validation authorities could likely be avoided, especially if the question of harmonised assurance levels was resolved (allowing third parties to easily determine what reliabilities they have without having to study a CPS in a potential unknown language), and (as noted by Cryptolog above) historical verification could be ensured by continuous resigning. In practice however, these issues have not been resolved, and will likely not be resolved for some time.

This should not been mistaken as a plea not to undertake the efforts above, and to simply focus on a (federated) validation authority instead. Indeed, many of these problems need to be addressed at any rate, with or without a validation authority. Ultimately, we feel that it is the market that will decide whether validation authorities offer any added value. Based on the existing solutions that have been identified and study – which are of course based on the currently existing situation in which the aforementioned gaps have not yet been addressed – the answer so far appears to be an (admittedly cautious) 'yes'. The main goal should be to put in place the building blocks that allow validation authorities to function more easily (i.e. to create a framework for validation services insofar as this is presently still missing), including by examining how the Commission could play an enabling role in this regard, for instance by implementing and disseminating good practices, and ensuring that the e-signatures market can take its natural course.

3.3.1.4.3 The impact of federation

Given the scope of the study, described as examining the possibility of a 'European Federated Validation Service', it needs to be considered to which extent federation of validation services is possible and desirable, what aspects could be federated, and what the impact of federation is on the conceptual model that could be applied. In this respect, the key solutions examined above do not offer much guidance, since none of them are federated in the sense that they rely on peers to perform their services.

As was noted above, the key services to be provided by a validation platform relate to the verification of certificates and signatures, and to the provision of legal assurances on the trustworthiness of the signature. Each of these services shows elements that could be implemented in a federated manner.

In relation to certificate verification, it is clear that verification authorities will typically rely on the verification mechanisms offered by the originating CSPs, typically by relying on OCSP lookups, LDAP or by integrating recent CRLs. This is indeed the approach that was also seen in each of the three key solutions. However, it should be noted that this should not be considered as federation, since the verification authorities in these cases do not rely on peers to provide the functionality. However, that does not mean that federated certificate verification has no use case or necessity. Indeed, one of the key questions that verification authorities need to face is precisely which verification resources are sufficiently reliable (Is the OCSP service operated by the competent CSP? Are CRLs acceptably up to date and authentic?). At the national/local level, these questions are still manageable, since the verification authority will likely be sufficiently familiar with local CSPs to determine which certificate verifications services are authentic, and whether or not they are reliable. On a cross border level, this is much less obvious.

To address this question, different options are available. As we saw in the BBS solution profile, one approach is to engage in direct contacts with the CSPs, and to ensure that the CSP itself commits to identifying the authoritative certificate verification mechanisms (location of recent CRLs, OCSP responder URL, ...), and that it provides sufficient guarantees for the reliability of these mechanisms. This is the logically simplest approach, but it is logistically complicated when CSPs from across the globe are integrated. From that perspective, it is not surprising that federated approaches exist as well.

The VPS-Governikus solution is the most direct example of this, as it has implemented support for the XKMS-responder relay interface to interconnect different instances of the Governikus platform. On the basis of this, as noted above, Governikus users have the possibility of choosing to trust XMKS responders operated by another Governikus user to validate certificates issued by CA's which they don't know locally. In this way, the Governikus model allows a federated validation service to be established.

So far however this model has not yet been tested in practice. The first operational implementations will be piloted in the course of the PEPPOL pilot project, as described in a separate solution profile. The PEPPOL approach will build on the Governikus experience to implement such a federated network. Once implemented, it is foreseen that users of the PEPPOL model will be able to call on local (trusted) validation services to verify certificates. If these are unable to make an assertion themselves, they may relay the request to another validation service as needed; it is not anticipated that more than one step is necessary. Upon receiving the response from any remote validation authority, the local authority service re-signs the response (and possibly adds information, e.g. on certificate quality) before returning the response to the caller. I.e., to the relying party it always looks like the local validation service answers, even when the request is chained. This XKMS approach is also envisaged to be integrated into the BBS model.

This is a useful way to apply federation to address the issue of determining the trustworthiness of certificate verification mechanisms being offered. However, it must also be acknowledged that there are two significant problems to be addressed as well:

- Firstly, federation (including through the use of XKMS responders) requires that a circle of trusted verification services (e.g. XKMS responders) is established. This means that a legal framework (regulatory or contractual) must be established between the participants, and that each of them can be held accountable for the services they provide. This is not trivial.
- Secondly, in order to gain the full advantage of such federated services, the verification authorities (e.g. XKMS responders) would need to be able to provide assertions on the quality of the certificates, including as a minimum whether or not they are qualified certificates, but also e.g. whether or not they are supported by SSCDs, and if any more complex quality determination systems are put in place (like the BBS or FBCA policies mentioned above), then these should also be presented. However, to be useful, these criteria would need to be harmonised, at a minimum at the European level. Again, this is not trivial.

In addition, depending on the scope of the envisaged federated validation solution, the efforts required to implement the above may be disproportionate. For instance, if the validation solution focuses only on qualified certificates, then the problems above will largely be addressed by the creation of a European trusted list of CSPs issuing qualified certificates to the public. In that scenario, the creation of a federation would thus not bring notable advantages to the table.

With regard to electronic signatures, the same observations largely apply: the key solutions do not use federation in a real sense, but examples of federated approaches still exist. The PEPPOL pilot, in addition to supporting XKMS responders for the verification of certificates, will also look into the possibility of implementing standardised OASIS-DSS responders for full signature verification. In a non federated model, the e-Notarius solution relies on the DVCS protocol, which could also be implemented in a federated manner.

This could be particularly beneficial in cases where signature formats vary, and only local solutions would be capable of verifying a signature or addressing questions of historical validity. But again, the same problems also need to be addressed: a legal framework needs to be established for signature verification, and uniform criteria need to be applied by each of the nodes in the federated network. Following on the recommendations of [RD3], it is interesting to note that the @firma solution recalled the possibility of addressing interoperability issues by establishing national (or regional) @firmas in the Member States, in which case the main issue to be addressed would be the creation of a trust framework between such authorities. Obviously, in that case the functionality would also be the same as with the national @firma solution, including the focus on qualified signature certificates.

Thus, it is clear that federation is a useful approach for certificate and signature verification, but likely only in the scenario that interoperability efforts will expand beyond the scope of qualified signature certificates, as in the latter case more cost effective solutions appear to be available and under development. Specifically, the problem of creating a suitable trusted framework between the participants in the federation (thus including a harmonised and enforceable liability framework) may prove to be very complicated: the nodes in the federation need to be able to cooperate in a trustworthy manner and as equals, while each end user of the federation (i.e. users trying to verify signatures and/or certificates via the federation) will only see a benefit to the system if the node they are contacting accepts full liability.

3.3.2 Description of main regulatory restrictions

To address the aforementioned issues at the European level, we need to examine if it would be possible to operate a federated European signature validation service in which the European Commission plays a central role. Two major issues need to be considered in particular: the liability provisions of the Directive and their applicability to signature validation services, and the impact of the market access and internal market articles on the permissibility of such a service.

3.3.2.1 Liability towards users of a validation authority

The liability provisions of the Directive and their impact on validation authorities was already discussed above in section 3.3.1.4.1. Briefly summarised, the main conclusion was that validation authorities established in any Member State would need to accept certain liabilities for their services if they choose to offer certain guarantees and expresses commitments towards the end user, in order to ensure that the service is usable in practice.

How does this affect a European Commission, should it choose to create a validation authority of its own or to operate a service to link existing authorities together in a federated model? The answer depends largely on the scope of the chosen approach.

Firstly, it should be stressed that the Signatures Directive requires Member States to establish a legal framework to govern the activities of CSPs established within their borders. This rule also applies to the liability provisions above: according to the Directive, the appropriate liability framework must be established by the Member States. As a result, the binding liability provisions of the Directive would only apply if the validation authority is an entity established within a Member State. The European Commission however at this stage lacks legal personality, and is not formally established within a Member State. There seems to be no reason in principle why a validation authority could not be established that would be subjected to an ad hoc legal framework (such as e.g. a Commission Decision), or at least to a legal framework that differs from the provisions of the Signatures Directive.

However, the impact of this consideration should not be overestimated, especially since the value of the services of a European entity would depend not on the applicability of the Directive but on the responsibilities and liabilities that it is willing and able to shoulder. In that respect, if the Commission would choose to organise an initiative to assist in the validation of electronic signatures, the assumption of certain responsibilities and liabilities may be a functional necessity and a prerequisite for its usefulness in the market. Compliance with the Directive's provisions in this regard thus seems necessary, even if it might be possible for the Commission to avoid this.

Secondly, however, it should be noted that responsibilities and liabilities to be assumed will depend greatly on the type of services to be organised at the European level. To illustrate this point, three possible scenarios can be provided by way of examples:

- If the Commission were to choose to implement a validation authority in the narrowest sense, i.e. a CSP that assumes responsibility for the verification of signatures and/or certificates towards end users, then liability would apply directly in accordance with the guarantees to be provided by the Commission.

- However, one could also envision the Commission acting as a central coordinator to interlink existing validation authorities together, i.e. a model in which the Commission acts as a ‘hub’ in a network in which a multitude of validation authorities would be the ‘nodes’. In this case, it is clear that a legal framework would still be needed that defines the rights and responsibilities (and thus liabilities) of each member of this network, including the Commission, but this could be organised in such a way that the Commission itself offers no guarantees in relation to the verification processes themselves. Whether this could be implemented in a way that makes liability noticeably lighter for the Commission is however questionable, given the crucial role that the Commission would then play as a trust enabler between existing validation authorities.
- Finally, the Commission might also opt to assume an enabling role towards the signature verification market without offering a validation authority itself or creating any specific infrastructure to support signature/certificate verification, e.g. by coordinating further standardisation work that is still needed, assisting in the homogeneous implementation of these standards (including e.g. by identifying and disseminating good practices, or more directly by developing and disseminating software components or reference implementations supporting generally recognised (European) standards under an accessible license that validation authorities would be free to re-use, or identifying validation authorities in the Member States to the public). In that way, the Commission could play a strong role in supporting this market, even going so far as to implement the necessary components (which it could also re-use internally towards its own Commission services), but without offering guarantees in relation to qualified certificates, and thus without the liability provisions of the Directive becoming applicable. In this hypothesis, liability could be made much lighter (or even virtually absent, depending how far the Commission would choose to go). This role has been explicitly foreseen in article 3.6 of the eSignatures Directive, in which Member States and the Commission are tasked with working together “to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer”. Thus, this is indeed a role that the Commission and Member States could jointly undertake.

While not exhaustive, the list above illustrates that the liability attached to any European level initiative will vary considerably depending on the choices to be made. A few general conclusions can already be drawn at this point:

- Firstly, it is clear that any infrastructure to be used in the verification of signatures or certificates (either in the form of a validation authority as such, or in the form of a central hub interlinking the services of validation authorities) will require considerable liabilities to be assumed by the Commission. This is a prerequisite for establishing trust in the infrastructure, and thus for its effective operation.
- Secondly, irrespective of the liability provisions of the Directive, avoiding liability altogether without critically impairing trust (as noted in the first bullet point above) may be unavoidable.
- Thirdly, it is also clear that there are still certain gaps that need to be filled in relation to the verification of electronic signatures and certificates which will not adequately be resolved by currently ongoing initiatives (including specifically in relation to nonqualified certificates, semantic harmonisation and time stamping / historical validation). It is at any rate possible and advisable for the Commission to play a strong supporting role in this respect, which could be done without substantial liability risks.

3.3.2.2 Market access and internal market limitations

In addition to liability, another difficult issue is whether or not the Commission could offer validation services without violating the market access and internal market clauses of the Directive, which state the following:

"Article 3 - Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. 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. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated.

A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

7. Member States may 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.

Article 4 - Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market."

The main concern in this regard would be that a European signature verification service would have an unfair advantage over other European CSPs (particularly private sector CSPs such as the aforementioned BBS and e-Notarius solutions) due to the fact that a Commission created or endorsed validation authority may be considered inherently more trustworthy by service providers, as its interpretation and implementation of European rules, norms and standards could be considered authoritative and therefore less likely to ever be disputed. This could result in a situation where a European validation authority could supplant other service providers, resulting in a de facto prior authorisation scheme (i.e. only the European validation authority would service the European market, or other validation authorities would only be able to operate if they have a trusted relationship with the European authority), or a de facto limitation on the free circulation of electronic signature products.

From a strictly legal perspective though, these objections do not appear to apply, principally because the clauses quoted above apply to the Member States and bar them to undertake specific actions that could negatively impact the development of the internal market. Under article 3 of the Directive, Member States may not impose prior authorisation schemes. However, as long as Member States do not choose to make collaboration with a European validation authority mandatory, this provision would not appear to apply. Even if a Member State would choose to take this option, then this would be a violation of the Directive by that Member State, not by the Commission. Similarly, the internal market provisions of article 4 require the Member States not to impede the free circulation of electronic signature products, but this does not apply to the Commission. Formally, the Signatures Directive thus does not appear to contain fundamental objections against the creation of a European validation authority.

However, it is of course intuitively clear that this doesn't imply that the Commission is free to impose restrictions to market access or to disrupt the free circulation of signature creation products. Rather, the main restriction in this regard are the institutional EU rules, including the Treaty on the European Union, which charge the Commission with ensuring that the provisions of this Treaty are applied. Measures which run contrary to this Treaty, including measures disrupting the free circulation of goods and services, are therefore not permissible on more fundamental grounds than the Directive. Any initiatives to be taken by the Commission must aim to ensure the proper functioning and development of the common market.

3.3.3 Provisional findings on the high level framework to be established for validation services

As was noted above, there are a multitude of options open to the Commission, depending on the envisaged scope of the envisaged verification solutions.

A main question in this regard is whether or not to focus exclusively on signatures based on qualified certificates. As was already noted above, significant efforts are currently already being undertaken to address the current existing problems in the market, including most notably the establishment of national trusted lists of supervised CSPs (to be coordinated at the EU level), standardisation efforts in relation to certificate profiles, SSCD profiles and signature formats, and the establishment of supervision criteria (all in the context of the CROBIES study). If successful and properly implemented, there does not appear to be a manifest need for the Commission to establish a validation authority focusing on this specific sector (qualified signatures and qualified certificates), as ongoing initiatives (including currently existing validation authorities) appear to be substantially capable of addressing market needs, and the liability risk for the Commission may be disproportionate to any advantages created in the market.

In contrast, this is not the case for signatures which do not rely on qualified certificates, where there is none the less also a clear need for interoperability. In this case, there is no existing trust framework in many Member States that can be leveraged, since the Directive does not impose any supervision obligation for such certificates (although some have implemented voluntary accreditation schemes), nor are there specific quality criteria in place to determine the reliability of nonqualified certificates or signatures. In this area, validation authorities could certainly prove to be useful, as a way of locally assessing the compliance of CAs with specific norms and providing guarantees in this regard. However, the framework for doing so (including the question of which norms to apply, cf. the criteria used by BBS and the US FBCA) is still largely unavailable, and in this area Commission initiatives could still play a significant role, either by filling the remaining gaps, or by participating directly in the market, provided that this would not impede the proper functioning and development of the common market for such services. Several scenarios can be envisaged in this respect, which will be further examined in the following reports.

Finally, it is also clear that semantic harmonisation and time stamping / historical verification are thus far insufficiently supported in the market. These are two areas which will certainly require further attention at the EU level.