



Common Solution Model

Draft Report on proposal for a common certificate validation model (D2.4)

Draft Report on proposal for an organisational structure (D2.5)

Draft Report on proposal for a legal framework (D2.6)

Study on European Federated Validation Service (EFVS): Analysis and Assessment

September 2009



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

Author: 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 aims to assess the feasibility of specific measures to ensure the availability of a European scale federated electronic signature verification functionality. The preceding report analysed a set of existing signature verification solutions, along with the currently existing framework for signature verification.

In this report, we examine the consequences of the existing different signature verification solutions, and present a European level approach to address the remaining issues. This approach is mainly based on leveraging the e-signatures work that is currently already being done at the European level. It envisages that the outcomes of this pilot can be brought to a fully functional stage, firstly by completing the framework for signature and certificate verification, and secondly by examining how a more permanent governance infrastructure could be derived from the PEPPOL model.

In relation to the completion of the framework for signature and certificate verification, a significant amount of work is currently already being done in the context of the CROBIES study in relation to qualified certificates and signatures based on qualified certificates, which will impact in particular 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. To also facilitate signature verification for signatures based on non-qualified certificates, additional standardisation efforts will likely be required, including for:

- The establishment of certificate and signature quality criteria (cf. the BBS and FBCA policies), building on ETSI TS 101 456 and TS 102 042;
- The formalisation of common policy requirements, building on ETSI-102-038 and 102-041;
- Harmonised interface implementations of the XKMS v2 and OASIS-DSS protocols.

It is foreseen that the mandate to be given to European standardisation bodies in the framework of the CROBIES study will include the revision and completion of this framework, in as far as needed.

In relation to the required governance infrastructure, it is clear that a federation between validation authorities requires coordination, and thus the establishment of a governance model through a body that would ensure that the same norms are applied by all VAs and that these are implemented and respected harmoniously. There is however no need per se for this body to be created or controlled by the European Commission. A governance body could also be created as a non-profit sector association, or it could be built on existing bodies which already have a certain trust model in place. The main requirement is that this body would be able to coordinate the (voluntary) acceptance and implementation of a common set of policies, standards and protocols.

Collectively, this approach should facilitate the functioning of the European e-signatures market, and optimally leverages the work that is already being done through existing initiatives, including most notably the CROBIES study, the PEPPOL project, and the existing key solutions @firma, the BBS VA and e-Notarius.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
1 DOCUMENTS	6
1.1 APPLICABLE DOCUMENTS	6
1.2 REFERENCE DOCUMENTS	6
1.3 ACRONYMS	7
2 INTRODUCTION	8
2.1 THE EFVS STUDY	8
2.2 GOALS OF THE PRESENT REPORT – MOVING TOWARDS A COMMON EUROPEAN SIGNATURE VERIFICATION FUNCTIONALITY WITHIN PUBLIC SECTOR APPLICATIONS	9
3 COMMON SOLUTION MODEL	11
3.1 COMMON CERTIFICATE VALIDATION MODEL	11
3.1.1 SCOPE OF THE ENVISAGED SOLUTION	11
3.1.1.1 Certificate Validation	11
3.1.1.2 Signature Validation	13
3.1.1.3 Liability	13
3.1.1.4 Additional services	14
3.1.2 ADDRESSING THE VALIDATION OF QUALIFIED CERTIFICATES AND VERIFICATION OF SIGNATURES BASED ON QUALIFIED CERTIFICATES	15
3.1.2.1 Introduction	15
3.1.2.2 VA trustworthiness in a cross border context	15
3.1.2.3 VA services	17
3.1.2.4 VA protocols	18
3.1.3 ADDRESSING THE VALIDATION OF NON-QUALIFIED CERTIFICATES AND VERIFICATION OF SIGNATURES BASED ON NON-QUALIFIED CERTIFICATES	19
3.1.3.1 Introduction	19
3.1.3.2 VA trustworthiness in a cross border context	19
3.1.3.3 VA services	21
3.1.3.4 VA protocols	21
3.1.4 ADDITIONAL SERVICES	22
3.1.4.1 Semantic services	22
3.1.4.1.1 Introduction	22
3.1.4.1.2 Service description	22
3.1.4.1.3 Protocol	23
3.1.4.2 Time stamping services	23
3.1.4.2.1 Introduction	23
3.1.4.2.2 Service description	24
3.1.4.2.3 Protocol	25
3.1.4.3 Historical Validation	25
3.1.4.3.1 Introduction	25
3.1.4.3.2 Service description	25
3.1.4.3.3 Protocol	25
3.2 ORGANISATIONAL STRUCTURE	26

3.2.1	ROLES AND RESPONSIBILITIES IN THE FEDERATION – THE CONCEPTUAL MODEL	26	
3.2.2	PHASING APPROACH AND THE ROLE OF EXISTING EUROPEAN INITIATIVES	28	
3.2.2.1	Federated certificate and signature verification – the PEPPOL approach	28	
3.2.2.2	From PEPPOL pilot to a fully operational federation	31	
3.2.3	GAPS TO BE FILLED – ANTICIPATED NORMS AND STANDARDISATION WORK	32	
3.2.3.1	Gaps in a federated signature verification model	32	
3.2.3.2	The 'additional services': semantics and time based services	33	
3.2.3.2.1	Semantics, identity management and STORK		33
3.2.3.2.2	Time stamping, historical validation and trusted service providers		34
3.3	LEGAL FRAMEWORK	35	
3.3.1	THE VA-CUSTOMER RELATIONSHIP	35	
3.3.2	THE VA-CA RELATIONSHIP	37	
3.3.3	THE FEDERATED DIMENSION	38	

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY
[AD2]	Project Management and Quality Plan (EFVS SC14 PMQP)

1.2 Reference Documents

[RD1]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML
[RD2]	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 ¹
CRL	C ertificate R evocation L ist
CSP	C ertificate S ervice P rovider ¹
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 E uropean S ervices to public A ministrations, B usinesses and C itizens
OCSP	O ne 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 A dvanced E lectronic S ignature
XKMS	X ml K ey M anagement S pecification
XML	e X tensible M arkup L anguage
XML-DSIG	X ML D igital S ignature

¹ It should be noted that in this report, the notion 'Certification Service Provider' or 'CSP' is used as defined in the Signatures Directive, namely as a "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures". The notion 'Certification Authority' or 'CA' is used as a subclass of CSPs, specifically as a CSP issuing signature certificates to the signatories. The latter notion is not defined by the Directive.

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 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 [RD1]), 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, if needed.

As a first step in the EFVS Study, information has been collected on twenty-two 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, 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 preceding report, which showed that signature validation solutions currently have two options for creating trust at a cross border level.

The first option, as demonstrated by @firma 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 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 CAs issuing qualified certificates to the public. 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.

2.2 Goals of the present report – moving towards a common European signature verification functionality within public sector applications

The preceding report analysed a set of existing signature verification solutions, along with the currently existing framework for signature verification, in order to determine if further European initiatives might be needed to facilitate cross border signature verification, specifically in the context of eGovernment applications, and to determine which restrictions played a role in this respect.

One of the key findings was the fundamental difference between signatures based on qualified certificates and those based on non-qualified certificates, as noted above: in the former case, cross border trust can largely be achieved by ensuring that the existing legal framework (and the related trust model) is properly implemented, whereas in the second case more fundamental gaps still exist. In both cases, a need exists for better semantic harmonisation and for a clearer framework for ensuring the long term-validity of electronic signatures, including through the use of time stamping services.

In this report, we will examine the consequences of these different approaches, and will present a European level proposal to address the remaining issues. This will be done in three sections:

- **Section 3.1 - Proposal for a common certificate validation:** in this first section, we examine how cross border certificate validation can be facilitated, and in relation to this, how electronic signatures based on these certificates can be more easily verified. This section will thus establish a first conceptual model for European signature verification services. As noted above, a number of different issues need to be addressed in this section, including particularly:
 - *The scope of the proposed solution*, where we indicate which services we feel need to be addressed at a European level. As required by the specifications of the study, the validation of signature certificates is a minimum requirement, but obviously a number of related questions need to be addressed as well, including specifically signature verification as a whole, liability of the validation service provider, and additional services which may be required to attach consequences to the signature, including semantic services and historical verification services.
 - *Addressing qualified certificates and signatures based on qualified certificates:* as noted above, the Directive has already provided a viable trust model for this type of certificates and signatures, and the main challenge is thus to address how this can be put to effect.
 - *Addressing non-qualified certificates and signatures based on non-qualified certificates:* in this case, no effective trust model exists yet, and thus more fundamental thinking will be needed to examine how this can be resolved.
 - *Additional services – semantics, time-stamping and historical verification:* while the validity of a signature could be determined based on the aforementioned services alone, in practice the recipients may have a hard time to rely on electronic signatures from an unknown origin unless other issues are addressed, specifically semantics (who or what is the signatory?), time-stamping (trusted signature date) and historical verification (was the signature valid at the time of signing, rather than at the time of verification?). These issues will be examined separately, since they are relevant regardless of whether qualified or non-qualified certificates are used.
- **Section 3.2 - Proposal for an organisational structure:** a high-level proposal will be presented on how this envisaged functionality could be implemented from an organisational perspective, i.e. which entities and infrastructures (governance structure) would need to be implemented at a European, national and/or local level, and how they should interconnect from a technical perspective. The role of existing European initiatives – most notably PEPOL and STORK – will also be examined.
- **Section 3.3 - Proposal for a legal framework:** similarly, we will address how this organisational structure should be organised from a legal perspective, including the need for acceptance of specific

norms and standards, and the need for effective contractual frameworks. We will base this work on the assumption that the eSignatures Directive will remain in effect for the foreseeable future.

Ultimately and in summary, the purpose of this report is to determine how the remaining technical and legal gaps could be addressed.

3 Common Solution Model

3.1 Common Certificate Validation Model

3.1.1 Scope of the envisaged solution

This chapter describes the scope of the envisaged solution of what should be offered in terms of services by the envisaged certificate and signature validation model. As noted in the specifications of the study, the validation of signature certificates is a minimum requirement, but obviously a number of related questions need to be addressed as well, including specifically signature verification as a whole, liability of the validation service provider, and additional services which may be required to attach consequences to the signature, including semantic services and historical verification services. Each of these aspects will be further discussed below. Collectively, they represent the 'functional specifications' that any model would need to be able to fulfil.

3.1.1.1 Certificate Validation

One of the main services a VA provides to its customers is a one-stop-shop for certificate validation. The complexity for an e-signatures application to establish relationships with every CA throughout the European Union is already difficult to manage in the context of qualified certificates, where 100s of technical CAs are issuing qualified certificates to the public are established. Outside this context, the complexity becomes even greater. The added value to e-signatures application owners of a VA for cost-effective certificate validation at the national level in the public sector has already been proven by the @firma Spanish project (see <http://www.epractice.eu/node/277227>).

The certificate validation process has to handle not only the verification of the validity period of the certificate and the revocation status of the certificate but also the complex and potentially resource intensive task of certificate validation against a chain of (possibly multiple) root certificates.

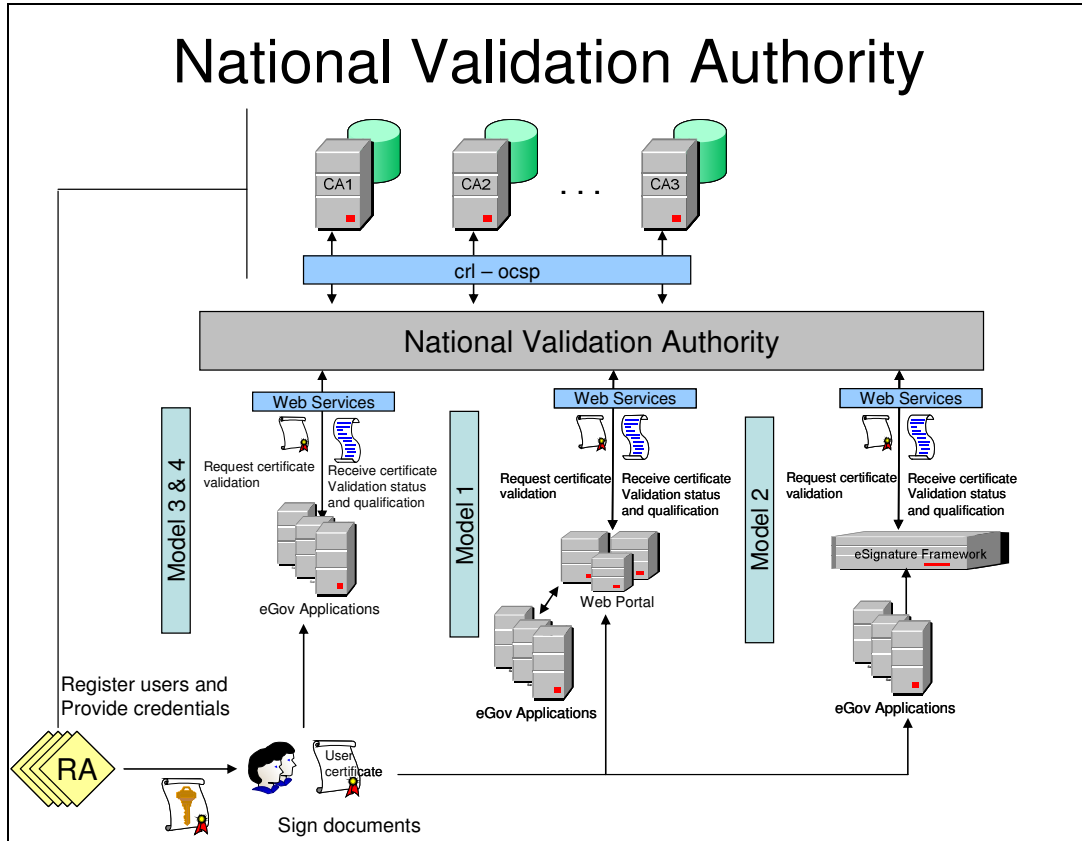
To achieve this goal, an e-signature application must be able either:

- To validate the certificate directly with the issuing CA, if it is known; in this case a VA is of course not necessary;
- To find the address of a VA that is capable of processing certificates issued by the CA referenced in the certificate; or
- To send the certificate validation request to a VA already known by the application and acting as a proxy that will retrieve the address of the target VA and will delegate the request to it. This could be a commercial or governmental VA at the National or European level.

This VA path discovery mechanism will be further detailed in the following sections (3.1.2.3 and 3.1.2.4) of this chapter.

The qualification of the certificate as indicated in the Qualify Certificate Statement or indicated in the certificate policy of the CA shall also be returned.

This approach depicted below has been already studied in the “Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications” [RD2]. A visual overview of the architecture is provided below, which was based on the concept of using national validation authorities. Obviously, as will be discussed later on, validation authorities do not need to be organised at the national level by definition.



In this figure, depending on the classification model of the applications:

- Applications can send their requests directly to the VA (Model 3&4) or
- Send their request to a Web Portal that will communicate with the VA (Model 1) or
- Use an eSignature framework that will communicate with the VA (Model2).

To create a federation of validation authorities, several important actions have to be realized:

- Establish trusted relationships (including in relation to liabilities) between the actors of the federation. This point will be discussed in the chapter 3.1.2.2 on VA trustworthiness in a cross border context **Error! Reference source not found.** and in the chapter 3.1.2.4 on VA protocols concerning Trust Service List integration.
- Communication protocols for VA-to-VA information exchange and communication protocols for e-signatures applications-to-VA information exchange must be defined and standardised. This point will be discussed in the 3.1.2.4 on VA protocols.

- The need for a viable governance model at the European level is addressed in the chapters 3.1.2.1 and 3.1.3.1.

3.1.1.2 Signature Validation

Signature validation is the second primary service a VA provides and can be included in the approach depicted above. The parsing and syntax checking of the signature and the mathematical verification of the signature can be delegated to a VA.

Generally, the delegation of this process to a validation authority requires the transfer of the whole document (including signature and possibly an existing Time Stamp Token) to the authority. This can be an issue to disclose the document when handling confidential/classified data. This problem can easily be addressed by calculating hash values of the signed document locally and only transferring the hash instead of the whole document, although in this case part of the process is of course no longer under the exclusive control of the VA. Certificate validation can be seen as a sub-process of the signature validation.

When present in the signature the Time Stamp Token must also be validated.

The aforementioned issue of VA path discovery is also valid for this process and will be further detailed in the following sections 3.1.2.3 and 3.1.2.4) of this chapter.

3.1.1.3 Liability

Apart from the technical functions of certificate validation and signature verification, it is clear that the envisaged validation authority will also need to accept certain responsibilities and liabilities for its services. The guarantees being offered will need to be sufficient to ensure that the service is a viable business prospect for the authority's customers.

From a practical perspective, at a minimum the validation authority will need to put in place agreements with its customers outlining its responsibilities and liabilities, which must comply with the provisions of the eSignatures Directive. In addition, these agreements will also need to cover the quality of the services, including e.g. availability (uptime), grace periods, guarantees in relation to applied CPSes, or use of validation protocols (CRLs may not be appropriate in some cases).

Secondly, the validation authority should implement specific agreements with the CAs to ensure that it can continue to offer the services as agreed with its customers (e.g. availability commitments on the VA side obviously need to be backed by availability commitments on the CA side, since the VA depends on the CAs infrastructure for this). These agreements need to include appropriate liability provisions to ensure that the VA can obtain suitable compensations from CAs that fail to meet their obligations, since this would likely also result in liability claims by the customers against the VA.

Finally, in a federated model that would allow national or (inter)regional VAs to delegate certain verification processes to peers in other countries, a legal framework needs to be established to govern the operation of the federation, including the responsibilities and liabilities of participating VAs, including of course an appropriate compensation model. All of these legal issues will be examined in more detail below.

3.1.1.4 Additional services

As additional services that can be offered in the future, it could be envisaged that VAs would provide X509 v3 certificate holder information extraction and semantic processing to ensure that the different certificate profiles can be mapped against a European Standard. Depending on the success of standardisation effort of the certificate profile at the EU level (including via the ongoing CROBIES study), the need for such services must be re-evaluated. The @firma example has shown that this is a crucial question to be resolved, in which validation authorities can offer a real added value. This issue will be further examined below.

The possibility to perform a historical validation of the certificate and the signature is a second additional service to be considered. Ideally, this should be a core service of any validation authority, as the end user's interest is usually not in determining whether the signature is valid now, but rather whether it was valid at the time of signing (since it is the latter question which determines the value of the signature). This process will thus allow the application to check the validity of a certificate or a signature at a given time in the past.

Depending on the usage of this service, this may require a change in the CAs' practices: if a VA is presented with a document signed two years ago using a certificate that expired last year, then only the CAs resources would allow the VA to determine whether the signature was originally valid. There is currently however no complete European legal framework for authoritative time based services, which makes it very difficult to operate those services at a cross border level. For this reason, this specific service has for now been labelled as an additional value service, although it is clear that this gap will need to be addressed at the European level at some point. Similarly, time stamping services should also be considered as a significant independent service which requires a completion of the European framework.

3.1.2 Addressing the validation of qualified certificates and verification of signatures based on qualified certificates

3.1.2.1 Introduction

Firstly, we will examine the issues to be resolved in order to create the functionalities described above in relation to qualified certificates and signatures based on qualified certificates (including qualified signatures, i.e. advanced signatures based on qualified certificates which have been created using secure signature creation devices, in the terms of the Signatures Directive).

As was already noted above, there is a much smaller need for validation authorities in this field, because the basic building blocks (including qualified certificates, secure signature creation devices (SSCDs), and especially the trust model based on national supervision schemes) has already been defined in a relatively homogeneous way at the European level via the Directive. Admittedly, there is the practical problem that the provisions of the Directive are sometimes interpreted in a slightly different way, including e.g. the supervision criteria which are applied in practice by supervisory bodies, or the processes that a signature creation device must undergo before it can be considered an SSCD. However, validation authorities are not strictly necessary to address these problems, and indeed may not be able to offer a satisfactory response in some cases. For instance, in relation to the concept of an SSCD, a validation authority would be able to make a statement whether a device is considered an SSCD in a specific country, but not necessarily whether this would be a valid statement in all Member States. This is an issue that should be addressed by examining and updating the standardisation framework that has been put in place to support the correct implementation of the Signatures Directive, as is currently ongoing in the context of the CROBIES study (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).

This is however not to say that validation authorities could not offer any benefits in relation to these types of certificates and signatures. As we saw in the previous report, all of the examined key solutions (@firma, BBS and e-Notarius) addressed these types of signatures as well. While this is currently largely justified because the aforementioned standardisation framework has not been finalised and implemented yet, several advantages of these services are likely to remain in the future. This includes their services in relation to semantic interpretation of the certificates and historical verification, but also the assurance to end users that they have a single point of contact (a one stop shop) for their verification needs, which will accept responsibility and liability towards the end user (even if only in the interim, i.e. with the possibility for the validation authority to obtain compensation for any errors committed by the CA). In short, while there may not be a technical or legal need for validation authorities in this specific niche once the aforementioned standardisation work is completed and fully implemented; there may still be a significant business advantage for e-signatures application owners to having them and being able to delegate to them.

In that respect, it is useful to reflect on how a validation authority could operate at the European level within this segment of the market, either as an interim solution (until the ongoing standardisation work is taken up) or as a service provider offering added value services. This question will be examined below.

3.1.2.2 VA trustworthiness in a cross border context

In order for a validation authority to offer its services in a cross border context, it needs to perform a number of functions. These will be briefly discussed in the section below.

- *Trustworthiness of the CAs and the role of supervision/accreditation*

A first role that any VA needs to be able to play is to ensure the trustworthiness of any CAs supported by the VA. In the current niche of qualified certificates and signatures based on these, this question is rather simple: the VA must be able to determine whether the used certificated is indeed qualified or not. If the VA is asked to verify a complete signature, it must in addition be able to determine whether an SSCD was used, so that the VA's customer can determine whether the signature can be considered a qualified signature.

Currently, it is difficult for VAs to offer this service, since no overview exists of CSPs issuing qualified certificates to the public, or whether or not these certificates are supported by SSCDs. However, this issue is expected to be resolved by the end of 2009 through the establishment of a trusted list of such CSPs, which will be managed nationally. Since these lists will be created, published and maintained in accordance with a European standard, it should be relatively easy for VAs to implement support for such certificates.

- *The question of liability towards the end users*

As was already noted in the previous report, validation authorities established in any Member State are required under the Signatures Directive to accept certain liabilities for their services if they choose to offer certain guarantees related to qualified signature certificates, as determined by article 6.1 of the Directive, which states that the CSP (i.e. the validation authority) *"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."

Of course, it is possible (and even desirable) for the VA to offer additional guarantees in relation to the services that it provides to ensure that they become an attractive and realistic business proposition, as will be described below, but the liabilities above are adequate from the perspective of the Signatures Directive.

- *Quality of the services towards the end users*

Apart from the aforementioned liabilities, end users may have a need for specific guarantees, specifically in relation to the quality of the services. Relevant questions may include availability (uptime), grace periods, guarantees in relation to applied CPSEs, or use of validation protocols (CRLs may not be appropriate in some cases). These will likely need to be addressed in specific agreements.

- *Relations with CA*

To ensure that the VA can provide these services, it may need to implement specific agreements with the CAs. As was noted by the example of e-Notarius in Poland, such agreements may not be strictly necessary when the supported CAs offer sufficient public resources to validate certificates (e.g. sufficiently up to date CRLs or publicly accessible OCSP responders), but this will not always be the case, and CAs may require compensation from the VAs before allowing them to use their services.

In this case, the VA may need to implement specific agreements with the CAs to address these questions, again including questions of availability (uptime) of validation solutions, guarantees in relation to applied policies, or in some cases (as e.g. witnessed by the BBS example in the previous report) equitable revenue sharing agreements. Given that the continuity of the VAs services also depends on the continuity of the CAs services, the latter may be a crucial element to ensure the long term viability of the VA, as CAs may refuse cooperation with VAs that use up significant resources without reasonable compensation.

Theoretically, all of these services can be offered by individual and unconnected VAs, and indeed all of the examined key solutions in the previous report operate in isolation (i.e. without linking to any peers, specifically other VAs). However, this presents serious scaling problems in relation to most of the issues above:

- To implement support for CAs established in other Member States, trusted lists from these Member States have to be integrated. It itself, this should not offer significant difficulties, since these lists will be created at the national level on the authority of the Member States, making them conceptually the most reliable sources available to the VAs, irrespective of which country they originate from.
- However, once this is done, VAs will also need to accept liability in relation to the validation services they offer. While they will be able to obtain compensation for any errors committed by third parties (e.g. supervisory bodies or the CAs), they may be reticent to assume first line liability, given the potentially daunting scale of these liabilities and the potential difficulty of obtaining compensations at an EU level.
- Obviously, the same applies in relation to any guarantees offered to the end users and their impact on relations with the CAs: if end users want specific guarantees (e.g. availability of the services), then VAs will need to obtain appropriate guarantees as well. This may be difficult to arrange at a cross border level, if the VA would actually be required to conclude suitable agreements with all relevant CAs (or at least the ones that it chooses to support).

For this reason, a federated approach that allows national or (inter)regional VAs to delegate certain verification processes to peers in other countries (which would then accept responsibility and liability for this) may be more suitable to address scaling questions. The impact of this model will be discussed below.

3.1.2.3 VA services

As discussed above, any VA should offer as a minimum certificate validation and signature verification services. There are a few particularities when offering these services in the market segments of qualified certificates and signatures based on these certificates, which will be further discussed below.

- Certificate Validation

In addition to the problems described above (trustworthiness, liability...), this model raises the two additional questions of (a) Addressing: where can I find a suitable VA and (b) Binding: how can I call the VA, and which protocols should I use.

One way of solving these problems could be to leverage the concept of trusted list to include VAs and VA services. In this model, VAs would be defined as additional TSPs and VA services as TSP services. However, this does not yet solve the problem of finding the VA(s) supporting the CA. In the PEPPOL approach, it is envisaged to create a TSL that describes a national VS/VA (as TSP) by its service supply points (the address where one can establish the appropriate way to query the XKMS responder that supports all the CAs for this country, or rather those CAs which are compliant to the PEPPOL policy. For individual CAs, PEPPOL plans to rely on the official TSLs from Member States (when available), in addition to possible other CAs evaluated as being sufficiently trusted. In the meantime PEPPOL will implement national TSLs containing only the CAs participating to the initial pilot phases.

- Signature Verification

The same questions raised by the certificate validation service apply here, and they can be solved in much the same way, by including the signature verification service as a service provided by the VA in a TSL.

As described later in the additional services chapter, time stamping is also of great importance, so verification of signature formats like C/XAdES-T should be provided as well.

3.1.2.4 VA protocols

To be interoperable at a European level, the different services must rely as much as possible on existing standards: certificate validation can be offered e.g. through OCSP and/or XKMS; whereas signature verification can be offered through e.g. OASIS-DSS (the latter of which was supported by @firma and planned by BBS). In addition, eNotarius makes use of the DVCS protocol which has the advantage of being able to encapsulate in a single protocol a certificate validation service, a signature verification service and time stamping services.

3.1.3 Addressing the validation of non-qualified certificates and verification of signatures based on non-qualified certificates

3.1.3.1 Introduction

The description above addressed the market segment for qualified certificates and signatures based on such certificates, and discussed which particular issues would need to be addressed for VAs to operate at the European level in this specific segment. As was shown, the approach does not need to be overly complicated, and indeed the functioning of this market segment does not depend on the existence of validation authorities since a trust model is already present in the Directive and implemented in all of the Member States. The same is however not true for non-qualified signature certificates.

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 non-qualified certificates or signatures. In this area, validation authorities could thus 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 in 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.

Below, we will examine how this could be addressed.

3.1.3.2 VA trustworthiness in a cross border context

Many of the functions to be performed by a VA in relation to non-qualified certificates and signatures based on such certificates are the same as discussed above in relation to qualified certificates, but there are also a number of important differences. The section below will focus on these differences.

- *Trustworthiness of the CAs and the role of supervision/accreditation*

Obviously, this first question is the most fundamental one: in relation to non-qualified certificates, there are no quality criteria to be applied (comparable to the definition of qualified certificates in the Directive), and there is no supervision/accreditation scheme being operated in the Member States.

If this issue is to be resolved, we will need to examine how quality criteria could be established and harmonised at the European level. Such harmonisation is necessary: if all VAs would be allowed to establish their own norms (as has currently been done by BBS and the US FBCA), this risks further market segmentation and precludes the establishment of any federated or otherwise decentralised validation schemes. This is a situation that must be avoided. It should thus be established to what extent the Directive allows the creation of such a normative framework, and what aspects should be covered by it.

A second and equally complex problem is determining a CA's compliance with this framework. For qualified certificates, the mechanism used for this task is the network of national supervisory bodies, whose efforts will soon be summarised in national trusted lists, which will then be coordinated at the European level. This approach could of course be applied to non-qualified certificates as well, at least in theory: in that case, existing supervisory bodies would expand the scope of their supervision tasks (or new supervisory bodies would be created), and extend their current trusted lists (or offer new ones) that provide an overview of each CA's compliance with the normative framework. Alternatively, the normative framework could be implemented nationally as an accreditation scheme, which would again allow the resulting output to be taken up in the existing trusted lists. However, this raises the fundamental problem that there is no legal basis for this effort in the Signatures Directive, and the Member States and national supervisory bodies can be anticipated to be highly reluctant to voluntarily accept this task. Thus, this approach is likely to require a revision of the Signatures Directive, limiting its appeal for the future. Alternative mechanisms should therefore be considered.

The main possibility in this respect appears to be the solution adopted by BBS (the only examined key solution which also integrated nonqualified certificates in its validation authority): allowing the VAs themselves to assess compliance with the specific standards, and requiring them to accept responsibility and liability in this regard. Of course, this still implies that a common normative framework is reached, and furthermore that VAs can be established which are willing to conduct compliance assessments and (above all) accept liability in case of problems. Certificate and signature liability could then be addressed through a federated model, in which VAs would conduct assessments locally and assume liabilities for the covered CAs, and in which they would form a trusted network with their peers that assume similar responsibilities to other CAs. The basis for trust would in this case be purely contractual.

- *The question of liability towards the end users*

As was already noted in the previous report, the mandatory liability regime created by the Directive applies only in relation to qualified signature certificates, as determined by article 6.1 of the Directive. If the guarantees provided by a validation authority do not relate to qualified certificates, then the authority is free to determine which guarantees it offers to its customers, e.g. via specific contracts or via general terms and conditions. Again, it is desirable for the VA to offer additional guarantees in relation to the services that it provides to ensure that they become an attractive and realistic business proposition, as will be described below. In a federated model, the VA must additionally ensure that the guarantees it offers towards the end users are backed by suitable agreements with its peers.

- *Quality of the services towards the end users*

There are no additional issues above those already identified above in relation to qualified certificates, although it bears repeating that again, federation would require the VA to ensure that the guarantees it offers towards the end users are backed by suitable agreements with its peers.

- *Relations with CA*

Again, the VA may need to implement specific agreements with the CAs to address a number of questions, including in relation to availability (uptime) of validation solutions, guarantees in relation to applied policies, or in some cases (as e.g. witnessed by the BBS example in the previous report) equitable revenue sharing agreements. There is no fundamental difference here with the situation for qualified certificates.

If a federated approach is used that allows national or (inter)regional VAs to delegate certain verification processes to peers in other countries (which would then accept responsibility and liability for this), a framework

needs to be established for the federation as well, which contains specific obligations for each of the participating VAs. The impact of this model will be discussed below.

3.1.3.3 VA services

In relation to the key services to be offered by the VA - certificate validation and signature verification at a minimum – the change of market segment has no specific impact on the required functionalities as such: the basic approach remains the same, as do the main difficulties, namely establishing lists of reliable VAs and identifying a suitable VA for unknown CAs.

3.1.3.4 VA protocols

Again, the change of market segment has no real bearing on the protocols to be used. The use of existing standards (XKMS and OASIS-DSS, for instance) remains advisable. Below, we will examine which practices could be followed in this respect.

3.1.4 Additional services

In addition to the certificate and signature verification functionalities discussed above, VAs may also offer certain additional services to e-signatures application owners that go beyond the simple verification of electronic signatures at the current moment. These relate to semantic services (determining who or what the signatory is) and time based services, including time stamping and historical validation. These services have been labelled as 'additional services' because they are not strictly necessary to determine whether or not a signature is valid at the present time. However, in many cases that is not the (only) question being raised by e-signature application owners, and for this reason, it is worth examining which role VAs could play in this respect.

Since these issues are largely identical for (signatures based on) qualified and non-qualified certificates, this distinction will not be made systematically in the section below.

3.1.4.1 Semantic services

3.1.4.1.1 Introduction

The first question relates to determining who or what the signatory is. While it is certainly possible to determine whether or not a certificate and/or a signature are valid without making statements on the identity or the authorisations of the signatory, VA's services may be of relatively little value to an e-signatures application owner if semantic aspects are not dealt with. Without semantic services, an e-signatures application owner may be able to get a declaration that a signature is valid, but without any information on who the signature can be ascribed to. This implies that the application owner will need to examine the signature certificate being used to extract the information itself, which is not very cost-effective and would face the problem of having to parse fields used differently by different CAs. It would therefore be useful if the question of semantic services could be addressed centrally by the VAs as well.

3.1.4.1.2 Service description

Certain standards already exist that impact semantic harmonisation to a certain extent, including ETSI TS 101 862 (Qualified Certificate Profile) and TS 102 280 (X.509 v3 Certificate Profile for Certificates Issued to Natural Persons), in particular through their relative harmonisation of the Subject field. However, in practice these are implemented by different CAs in a diverging manner. It is therefore unsurprising that some key solutions, including e.g. @firma, have implemented specific services within the VA to ensure that the application owners do not need to concern themselves with the differences between existing CA certificates. In the case of the @firma VA, it maps the different implementations to a common XML based format, which is used in communication with the application owners, as noted in its profile: *"in addition to the validation services, an interpretation service of the X509 v3 certificate attributes and the extensions is in place. The service extracts all the certificate related information to a normalized XML form, which it then sends to the application relying on the certificate, so that a mapping of the individual certificate profile to a XML scheme is performed by the VA. For instance, all subject related-information, issuer data and related information, type of certificate, key usage, etc from a X509 file can be normalised and sent back to the customer every time the certificate is validated."* In this way, semantic differences can be bridged.

To some extent, the issue of identifying the signatory in a more harmonised manner will be addressed by the currently ongoing CROBIES work surrounding the "Common Minimum Requirements for a Qualified Certificate

Profile supporting Qualified Electronic Signatures”; however, the efforts in this field do not relate primarily to questions of identity management as applied to the signatory but rather to the content and structure of the certificate as a whole. 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. It should be kept in mind however that this work is only envisaged to directly impact qualified certificates, and that the serialNumber as such may not be a directly usable resource to any given e-signatures application.

In this respect, the CROBIES work provides a crucial input to resolve semantic issues related to the identity and capacity of the signatory, and the @firma example provides a good practice case of the output that could be expected. What is still lacking is the connection between the two, i.e. the possibility of taking the serialNumber (and any other information which may be present in the signature certificate), and using this as a resource to create a harmonised identity profile, e.g. in the form of an XML scheme as with @firma. This is where other initiatives such as the STORK pilot may become relevant. This interaction will be discussed in section 3.2 below.

3.1.4.1.3 Protocol

Specific web services could be used to return semantic information but some protocols like OCSP (like done by the CertiVeR solution) and XKMS (like Governikus/PEPPOL did with XKMS v2) can also be extended.

At a high level, three elements are needed which are so far still lacking:

- Firstly, a common certificate profile containing sufficient identification information. This is currently already being established within the framework of the CROBIES study, albeit only in relation to qualified certificates. A similar approach would also be needed for non-qualified certificates.
- Secondly, a common identity profile, as is currently being used by @firma in the form of a standardised XML scheme. Where the identity information contained in the certificate is sufficiently complete, creating the corresponding XML file will be trivial. However, given that the ETSI TS 102 280 standards requires only *commonName* or *surName&givenName* to be present and leaves all other attributes (*domainComponent*, *countryName*, *serialNumber*, *title*, *organizationName*, *organizationalUnitName*, *stateOrProvinceName*, and *localityName*).as optional, this information may not be sufficient to allow an adequately complete XML file to be created.
- Thirdly, a framework for creating such XML files in a trusted fashion, e.g. through the intervention of VAs, as in the case of @firma. Since the VA will already be trusted by the e-signatures application owner, this would also be a suitable point to establish trust in the identity management component of electronic signatures.

3.1.4.2 Time stamping services

3.1.4.2.1 Introduction

Many handwritten documents with a legal scope do not only contain the signature of the owner, but also the date on which the document is claimed to have been signed. The date is as important as the signature in many cases (contracts, orders, patents... are a few typical examples). However, the date specified inside the document can clearly not be trusted as such. The owner can always antedate the document in an attempt to claim that he was in possession of or has sent the document before the actual date. This is why some services require such paper documents to be sent by registered mail, with post offices acting as a Trusted Third Party that postmarks the document.

Electronically signing a document does not inherently bring any proof of the actual date and time that the document was signed: if validation takes place some time after signature creation, it is possible that the certificate has been compromised, revoked or otherwise became invalid, notwithstanding its validity at the time of signing. This can be avoided by using trusted time-stamping services provided by a trusted third party acting as a Time Stamping Authority. Trusted time-stamping is the process of securely associating a trusted time to a document in such a way that the signature cannot be disputed later, even by the signatory of the document, provided that the integrity of the Time Stamping Authority is not compromised.

Trusted Time-stamping services can be used to support:

- Authenticity: the time provided by the timestamp can be trusted and is not refutable
- Integrity: the timestamp is protected against tampering without detection
- Timeliness: the time of the digital signature is in fact the actual time
- Legal recognition and non-repudiation

Timestamp creation firstly relies on the acquisition of an accurate trusted time from a trusted entity like a national measurement institute (for instance the Royal Observatory of the Army in the @firma solution). Successful timestamp verification will ensure that neither the initial document nor the timestamp has been changed in any way and that the timestamp was indeed issued by the trusted third party.

Even if time stamping verification services are considered here as an additional service of a validation authority, it needs to be taken into account from a legal and technical perspective in the framework of a European federated service. The lack of a clear legal framework timestamps complicates issues surrounding the long term validity of electronic signatures.. The promotion of signature formats including timestamps like XADES/CADES-T and their integration as a service of any CA or VA is therefore advisable. However, a clear European framework for such services is still missing, leading Member States to implement their own and diverging rules, presenting interoperability risks. Among the key solution profiles, @firma is the only non commercial solution providing time stamping verification services.

From an organisational point of view, Timestamp Authorities operate at the same level as Certificate Service Providers and require a very similar legal framework. When verifying timestamps, one needs to trust the Time Stamping Authority and have access to its public key. Without a central Validation Authority, this leads to the same full mesh problem between applications and TSAs. Fortunately, TSAs can already be defined in the envisaged Trust-service Status List using the specific service type identifier "Time-stamp Authority" as defined in [RD4], which should diminish at least the problem of discovery.

3.1.4.2.2 Service description

The Validation Authority does not need to provide any explicit time stamping services. Indeed, the timestamp creation can be handled by the application itself by directly contacting a Time Stamp Authority to generate a signature including a timestamp. It's also not essential for a Validation Authority to provide an explicit (separate) timestamp verification service, as this verification process should be a part of the general signature verification process. As such, time stamping can be considered an 'added value service' for validation authorities.

3.1.4.2.3 Protocol

The most common timestamp protocol is described in the ETSI TS 101 861: "Time stamping profile", a profile of the "RFC 3161 – Internet X509 Public Key Infrastructure Time-Stamp Protocol" standard which has been augmented by the ANSI ASC X9.95 Standard. Timestamp renewal is described in RFC 4998. There is also the ISO/IEC 18014 standard. Both the OASIS DSS and the DVCS protocol can be used to support time stamping services.

The minimum recommended protocols for generating signatures including timestamps are C/XADES-T (or any higher level extension like –C, –X, –X-L, –A). Other additional services may however lead to the recommendation of a higher level of signature.

3.1.4.3 Historical Validation

3.1.4.3.1 Introduction

Time stamping as described above referred to the specific service offered by a trusted service provider in which a particular piece of data is signed to link it to a specific moment in time (e.g. to attest to the fact that the signature was already present on that piece of data was valid at the moment of time stamping). Historical validation however refers to a different situation, namely the situation in which a service provider allows the validity of a signature to be checked for a significant amount of time after its creation, without necessarily resorting to time stamping. A typical example would be a VA that receives a signature which was created two years ago using a certificate that expired one year ago, and that would try to determine the validity of the signature at the time of creation (i.e. two years ago) based on its records of valid certificates at that time, such as e.g. archived CRLs.

As such, historical validation does not require a VA, and can also be offered directly by a CA. However, the intervention of a VA is possible, as in the Austrian SVS/MOA solutions, which support historical validation by default.

3.1.4.3.2 Service description

As noted above, the basic service consists of determining whether a signature was valid at some point in history. The VA (or CA, as the case may be) receives the signature, certificate and desired validation time as inputs, and attempts to determine whether the signature was valid at the specified moment in time. Obviously, OSCP lookups are pointless for this service when the certificate is no longer valid; historical validation either needs to rely on archived CRL information or on any time stamps that may have been applied to the signature at an earlier moment in time.

3.1.4.3.3 Protocol

Protocols generally provide an optional field to specify the date and time that the client wants the server to perform the validation / verification. When such a field is provided, the server will attempt to perform the verification at the time specified in the request instead of using a time defined by the server policy (usually the time when the request is being handled by the server). For instance, one can find the field "validationTime" in the SCVP protocol or the <UseVerificationTime> of the OASIS DSS protocol.

3.2 Organisational Structure

Based on the functional requirements in section 3.1, in this second part of the report we will present a high-level proposal on how this envisaged functionality could be implemented from an organisational perspective, i.e. which entities and infrastructures (governance structure) would need to be implemented at a European, national and/or local level, and how they should interconnect from a technical perspective. The role of existing European initiatives – most notably PEPPOL and STORK – in providing parts of the puzzle will also be examined.

3.2.1 Roles and responsibilities in the federation – the conceptual model

Broadly speaking, three major roles need to be distinguished in a federated signature verification model:

- Firstly, the CAs that issue signature certificates to the public. Their main role is putting the basic infrastructure to create electronic signatures in the hands of their customers, providing the basic building blocks for the validation of the certificates that they issue, and observing applicable European rules standards to the extent required by the Signatures Directive.
- Secondly, the VAs that will assume responsibility for signature verification (and thus also certificate validation) towards their customers. They will typically be able to validate signatures created using a certain number of certificates from a certain number of CAs themselves, and for other CAs they will have to rely on resources offered by their peers in a federated model.
- Thirdly, the operator of the federation, who puts in place common rules that the VAs within the federation will observe, and who will provide access to certain common resources, including an overview of VAs that can be contacted for specific CAs (i.e. VA discovery). It is not envisaged that the operator will act as a VA itself, since this would compromise its neutrality.

From a functional perspective, an application owner in this model could still choose not to work with VAs at all, and simply implement support for any number of CAs that it considers to be sufficiently trustworthy directly in its application. This will likely become gradually easier in the future due to the ongoing standardisation work within the CROBIES study, at least in relation to qualified certificates and signatures based on these. However, an application owner could also choose to work with a VA, either to simplify its implementation work (since it would then only need to be able to communicate with a single VA rather than a multitude of CAs), to increase the amount of CAs that it could support (and thus increase its potential user base and business case), or to rely on any added value services provided by the VA (like semantic interoperability or historical validation).

If the application owner would decide to call upon the services of a VA, it would conclude a suitable agreement with a chosen VA, outlining the specific services to be provided. While VAs could be organised at the national level, this is certainly not required. VAs could be established along national lines, but also on a regional or interregional basis (e.g. a VA covering all or several Scandinavian, Baltic or Germanic countries), or even on a sectoral basis (e.g. a VA covering CAs which are directly controlled by public administrations, or which are active exclusively in e-invoicing, e-health or e-justice). From the application owner's perspective, the only relevant question is whether the VA covers its anticipated customer base, either because the VA has direct agreements in place with the relevant CAs, or because it is a part of a federation that includes these CAs. Inversely, from the VA's perspective, their coverage of CAs will be dictated by the potential market that they see for their validation services, which could be driven by commercial considerations (as e.g. seen in the BBS key solution), public

benefit (as e.g. seen in the @firma key solution), or a mixture of both (as e.g. seen in the CNUE solution for European notaries, which could also be an interesting model for e.g. an e-health or e-justice VA).

What is however crucial is that the VAs operate on a common basis, allowing application owners to use a single interface to communicate with any VA, and allowing the VAs to interconnect to each other in a federated model. This requires coordination between the VAs, and thus the establishment of a governance model through a body that would ensure that the same norms are applied by all VAs and that these are implemented and respected harmoniously. Ideally, there should be only one federation at the European level, since the existence of multiple federations would again risk fragmenting the market.

However, while a single body would need to take control over the coordination of this federation, there is no need per se for this body to be created or controlled by the European Commission. A model in which the CSP sector itself takes charge of this coordinating role indeed seems to be preferable to ensure that the approach is optimally aligned with market realities and to minimise the risk of unnecessary market distortions. An analogy could be made in this respect to the governance model behind the Single Euro Payments Area (SEPA), a framework to ensure that any electronic payments within the Eurozone can be treated as domestic, by requiring all payment processors to apply common procedures and standards. While a regulatory framework was established at the European level (notably through the Payments Services Directive²), governance is in the hands of the European Payments Council (EPC³), which consists of European banks and banking associations. Thus, SEPA is driven by common European norms, but governed by the sector itself. A similar initiative could prove to be a suitable model for European signature validation services, provided that common pitfalls in relation to sector driven support, sufficient harmonisation and sufficient resources can be avoided.

Such a governance body could thus be created as a non-profit sector association, much as the EPC, or it could be built on existing bodies which already have a certain trust model in place, such as e.g. the European Chambers of Commerce (EuroChambres)⁴. The main requirement is that this body would be able to coordinate the (voluntary) acceptance and implementation of a common set of policies, standards and protocols.

In the section above, a number of existing gaps have already been identified (e.g. in relation to the reliability of nonqualified signature certificates, or the implementation of certificate/signature verification protocols), along with several possible solutions that have currently already been implemented (e.g. @firma, BBS, e-Notarius) or are being piloted at the European level (most notably through PEPPOL). Below, we will examine the resources that are thus already available and which could be leveraged to create such a federated model.

² Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC Text with EEA relevance, see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:HTML>

³ See <http://www.europeanpaymentscouncil.eu/>

⁴ See <http://www.eurochambres.eu>

3.2.2 Phasing approach and the role of existing European initiatives

The approach proposed above is not new, and aspects of this strategy are currently already being explored through the PEPPOL project. It is instructive in that respect to examine the high level approach taken by this project and subsequently to examine how this model could be integrated into the structure described above.

3.2.2.1 Federated certificate and signature verification – the PEPPOL approach

The PEPPOL project⁵ aims to create a pilot implementation that permits e-procurement across multiple participating Member States, by proposing a coherent solution to most of the technical, legal and operational problems encountered in this process. As can be expected, one of the components of the PEPPOL project – WP1 – examines the issue of cross border e-signature use and verification.

Broadly summarised⁶, PEPPOL foresees the implementation in a pilot form of a federated certificate validation model, based on the VPS/Governikus solution which is already in active use in Germany, in which contracting authorities (i.e. the 'customers of the VAs') would be able to verify signatures by:

- Directly verifying the signature itself if the CA is known (i.e. no validation authority is needed in this case).
- Contacting a VA for the validation of the signature certificate (but not the signature as a whole). In this case, PEPPOL will rely on responders implementing the XKMS v2 protocol. PEPPOL will provide a harmonised interface for this implementation to avoid implementation discrepancies.
- Contacting a VA for the verification of the signature as a whole. In this case, PEPPOL could rely on responders implementing the OASIS-DSS protocol; however, there is no commitment yet to implement this aspect within PEPPOL. .

With regard to federation, it is important to note that only a single VA needs to be known to the customer in the Governikus/PEPPOL model. If the CA is not known to the VA being contacted, XMKS requests can be chained to other VAs for resolution; i.e. XMKS responders will operate in a federated model. This is however not the case with OASIS-DSS responders: while they can also use the federated XKMS model to validate a signature certificate, signature verification as such is handled locally and OASIS-DSS requests are not chained to other responders. The VA that was originally contacted by the contracting authority always signs its response itself even when XKMS chaining was used, so that the contracting authority only has to establish trust with one VA (although it may choose to support more if desired).

Other noteworthy building blocks to be implemented in a pilot form by PEPPOL include specifically:

- The definition of quality level criteria for signature certificates and electronic signatures, which consider:
 - The quality of the certificate (including e.g. the supervised/accredited status)

⁵ See <http://www.peppol.eu/>

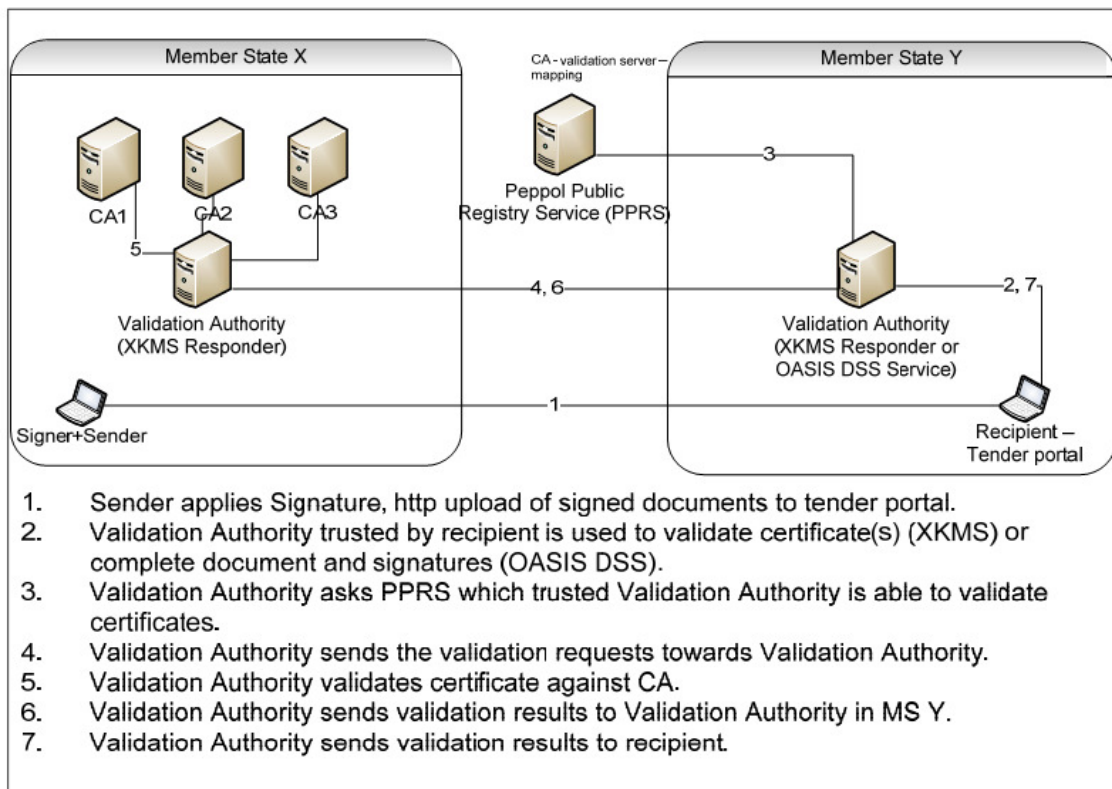
⁶ See <http://www.peppol.eu/deliverables/wp-1> for more details and specific deliverables

- Assurances related to this claimed quality (i.e. the extent to which this status has been independently corroborated)
- Cryptographic quality of the signature, based on algorithm and bit length

These criteria were based on the approach used by the BBS key solution mentioned above.

- The promotion of signature policies as a way for the VA's customer (i.e. the contracting authority in the PEPPOL project) to define and communicate its requirements in relation to:
 - The authorization and commitment implied by a signature or a set of signatures;
 - The application of signatures in e-procurement processes – the documents that should be signed and at what stages of the process;
 - Signature validation policies that specify the required quality levels and approval status (e.g. qualified) for eID and e-signatures, the validation process, and other requirements imposed on the actors.
- The support for Trusted Lists, specifically through the PEPPOL Public Registry Service (PPRS), a list containing trusted VA services based on the ETSI TS 102 231 standard. Authenticity of the list will be assured by means of an electronic signature from the TSL issuer. Public keys of TSL issuers will be published on PEPPOL web sites. The trusted lists can be used directly by relying parties in some cases (if they feel this is adequate), and will otherwise be available to validation services (XMKS or OASIS-DSS) as a trusted resource to identify CAs.

Globally, the functionality of the PEPPOL pilot can be represented as below (taken from the PEPPOL solution profile, and provided by the PEPPOL consortium):



Thus, the main requirements imposed by the federated model proposed above are present: the possibility of federated certificate validation and signature verification through VAs based on common standards (XKMS and OASIS-DSS), harmonised implementation of these standards, common quality requirements for certificates and signatures, and a centralised service for the discovery of trusted CAs and VAs through the PPRS. The PEPPOL model appears to be a solid working basis to implement the federated model.

This is not to say that no further gaps will need to be addressed, though. These will be addressed in the section below.

3.2.2.2 From PEPPOL pilot to a fully operational federation

As a pilot implementation, it is clear that not all issues will be handled definitively within the pilot, and that certain changes would still be required before arriving at a fully operational federation, in particular in relation to the governance model. These changes relate mainly to the following:

- The model which we outlined above requires a centralised governance body, which would supplant the role of the PEPPOL Consortium in the PEPPOL pilot. This governance body will assume several responsibilities, including the management of the TSL (the PPRS in the PEPPOL nomenclature), the conclusion of agreements with unsupervised/unaccredited CAs⁷, and to enforce the common standards and implementations on the participating VAs.
- The creation of a liability model for the federation: the VAs need to be able to interact and trust each other, which means that they need to accept responsibility (and thus liability) when interacting, specifically through the use of XKMS chaining.
- A business model needs to be established for the federation. For individual VAs, this can be left to their own discretion. As was already noted above, it is possible for some VAs to operate on a commercial basis, others as public services, and yet others as a mixed model. However, when VAs interact (e.g. through XKMS chaining) an arrangement for compensation is needed to cover any liabilities, and this will need to be coordinated at the federation's level. In addition, the governance body itself must be funded as well, which will likely imply contributions from the VAs.
- Obviously, the PEPPOL deliverables would need to be formalised as well so that they can be applied consistently throughout the federation. It should be noted that this does not necessarily require formal standardisation (e.g. through CEN or ETSI); the main requirement is that common agreements exist and are applied (and enforced) within the federation. These relate notably to common policy requirements – PEPPOL does not (at least not at this stage) define complete, comprehensive signature policies that are given unique references – and implementations of the XKMS and OASIS-DSS protocols.

⁷ As noted in the PEPPOL solution profile, it is envisaged that the trusted list to be used by PEPPOL will be based on the European coordination of national supervision/accreditation lists, which means that in practice the list will only cover CAs issuing qualified certificates or which are accredited/supervised for other reasons. For the inclusion of other CAs (e.g. CAs issuing nonqualified certificates which are not supervised or accredited in their Member State of establishment), PEPPOL will “consider the use of the professional services offered by Validation Authorities like DNV. In this case the PEPPOL Consortium will sign an agreement with such VA in order to verify if a CSP, not included in any voluntary supervision/accreditation MS's schema, possesses the PEPPOL Policy requirements. In a positive case the VA signs an agreement with the investigated CSP. This way, the legal trustworthiness (legal recognition) is based on a contractual level. Such CSPs will be identified as Contractual accepted CSP (CCSP). As in the previous case, if the CCSP provides qualified certificates, it will be addressed as CQCSP.” Thus, extension of the TSL to unsupervised and unaccredited CAs will be handled centrally.

3.2.3 Gaps to be filled – anticipated norms and standardisation work

3.2.3.1 Gaps in a federated signature verification model

From a standardisation perspective, as was noted above, a significant amount of work is currently already being done in the context of the CROBIES study in relation to qualified certificates and signatures based on qualified certificates, which will impact in particular 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.

As noted above however, additional standardisation efforts will likely be required, including for:

- The establishment of certificate and signature quality criteria (cf. the BBS and FBCA policies), building on ETSI TS 101 456 and TS 102 042.
- The formalisation of common policy requirements, building on ETSI-102-038 and ETSI-102-041;
- Harmonised interface implementations of the XMKS v2 and OASIS-DSS protocols (likely a direct formalisation of the output of PEPPOL)
- The creation of a trusted list for VA discovery, based on ETSI TS 102 231.

The efforts above should cover the basic services of certificate validation and signature verification. However, semantic and time based services would not yet be covered by the federation at that point. While not within the direct scope of this work, below we will discuss briefly how this could be addressed.

3.2.3.2 The ‘additional services’: semantics and time based services

3.2.3.2.1 Semantics, identity management and STORK

As was noted above, without semantic services, an e-signatures application owner may be able to get a declaration that a signature is valid, but without any information on who the signature can be ascribed to. This implies that the application owner will need to examine the signature certificate being used to extract the information itself, which is not very cost-effective. It would therefore be useful if the question of semantic services could be addressed by the VAs as well.

Good practices exist in this respect, including e.g. the examined key solution @firma, which maps the different certificate profile implementations to a common XML based format, which is used in communication with the application owners. In this way, the signature verification VA can also be used to perform an identity management related task, based on the same infrastructure.

It is interesting to note that there are significant similarities between the federated signature verification approach described above (based on a series of national, regional or sector specific VAs that interact with a number of CAs that are relevant to their domain) and one of the conceptual models behind the STORK pilot⁸. While STORK focuses on interoperable identity management and not on e-signature interoperability, one of the components of STORK intends to explore e-signature validation to a limited extent as well.

Building on the recommendations of the 2007 IDABC Study on eID interoperability for PEGS⁹, the logic behind the currently envisaged STORK model is to build on local (typically national) Pan-European Proxy Services (PEPS) that are interconnected in a federated model, and which would be able to connect directly other PEPS in other Member States, or directly to identity providers in countries that rely on a middleware approach without implementing PEPS portals. Generally speaking, in this model Service Providers (SP) would pass a certificate validation request to its local PEPS, which would redirect this request to the PEPS of the Member State in which the issuing CA is established (or directly to an Identity Provider (IP) if that Member State is a middleware country). The targeted IP then issues a certificate validation response which will be re-routed back to the initiating SP.

It is clear that the function of the PEPS is very similar to that of the VAs in the model discussed above, and the same implementation approach could therefore conceptually be followed. In addition, this would also offer an opportunity to address identity management issues in a more systematic way, since this is within the remit of the STORK pilot (but not of PEPPOL). Specifically, one might imagine that it would be possible for the PEPS to build on the infrastructure and functionality offered by the VAs in the PEPPOL model, and to enrich this by adding a component that is comparable to the @firma approach, in which different certificate profile implementations are mapped by the local PEPS to a common XML based format, which could then be resigned by the PEPS. The coordination of this work across these different initiatives (notable between STORK and PEPPOL) would ensure that a single common approach and a single set of standards is taken up at the European level.

As was noted above, the currently ongoing CROBIES work provides a crucial input for qualified certificates, since it will result in a harmonised serialNumber becoming a mandatory component of qualified signature certificates, which could prove to be a vital component for the STORK model to link the e-signature verification

⁸ See <http://www.eid-stork.eu/>

⁹ See <http://ec.europa.eu/idabc/en/document/6484/5644>

functionality to the identity management issue. In this way, it seems possible to use the federation signature verification model as a method to addressing some of the existing identity management questions, at least insofar as PKI based signatures are used.

3.2.3.2.2 Time stamping, historical validation and trusted service providers

The OASIS-DSS protocol can be used to support time stamping services, and certain standards are already in place at the European level in relation to time stamping protocol, specifically ETSI TS 101 861: "Time stamping profile", a profile of the "RFC 3161 – Internet X509 Public Key Infrastructure Time-Stamp Protocol" standard which has been augmented by the ANSI ASC X9.95 standard. None the less, time stamping is not currently envisaged to be a mandatory part of the PEPPOL project, nor is it dealt with by the model proposed above.

From PEPPOL's perspective, it notes that: *"PEPPOL WP1 recommends as the main solution that if a time stamp from the sender is included with a signature, this should be generated locally by use of a system clock or another correct time source. TSA services should not be used by the sender. This relies on an assumption that no formal requirement exists for sending side TSA time stamps. PEPPOL WP1 is not aware of any such requirement."*

The receiving side will typically obtain time stamps (from TSA or system clock whatever is considered necessary) to embed in more elaborate SDO structures such as XAdES [ETSI-101-903] or CAdES [ETSI-101-733] or in archival records for the signed documents. This is considered outside the scope of PEPPOL and TSA services will not be offered by PEPPOL for the pilots. There may however be mandatory requirements for use of a TSA (e.g. Italy). In such cases, the receiver will select a TSA service that is known and regarded as trusted by the receiver."¹⁰ In summary, signing parties would be allowed to use time stamps within their signatures, and relying parties would be able to apply their own time stamps after receipt of a signature, but no binding obligations are imposed by the signature validation model adopted by PEPPOL.

This appears to be the rational approach, due to the fact that a legal framework for time stamping services is currently largely missing at the European level, leading certain Member States to implement their own legal frameworks, including e.g. through the definition of qualified time stamping services (e.g. in Germany¹¹). Thus, there is no common regulatory ground for the creation or use of time stamping services. As a result, while the aforementioned standards exist, the legal effect of using these services – or of other trusted service providers, like electronic registered mail, electronic archiving and conversion to electronic formats – is not presently regulated. This would likely require a new legal framework to be established. While the Signatures Directive would allow the Commission to publish reference numbers of generally recognised standards for electronic-signature products (through article 9), this would not result in any clear or harmonised legal effect in the Member States. For this, new regulatory initiatives in relation to trusted service providers may be required, building on the framework of the Signatures Directive. However, this particular question is out of scope of the present study.

¹⁰ See <http://www.peppol.eu/deliverables/wp-1/d1-1-part-4-architecture-and-trust-models>, p. 35

¹¹ So-called *Zertifizierungsdiensteanbieter für das Ausstellen von qualifizierten Zeitstempeln* ; see http://www.bundesnetzagentur.de/enid/8887695e47bd1de945d089eac9d5b9d1,0/Elektronische_Signatur/Zertifizierungsdiensteanbieter_ph.html

3.3 Legal framework

Finally, in this last section, we examine the legal framework that would be required to implement such a federated signature verification infrastructure. Building on the observations in the preceding sections, three different legal relationships need to be examined in more detail to determine how a federated validation structure could operate:

- The relationship between the validation authority and its customers
- The relationship between the validation authority and the CAs
- The relationship between validation authorities in a federated model

As has already been noted above, strictly speaking only the first relationship requires a specific legal framework in order to operate a validation authority: validation authorities can operate in isolation outside of any federation (as demonstrated by all of the key solutions), and it is technically possible for a validation authority to operate without a prior agreement with the CAs using their publicly available resources (as demonstrated by e.g. e-Notarius). However, without a federation, validation authorities carry a very significant responsibility and risk, and may have a hard time scaling their operations. Similarly, without agreements with the CAs, VAs are dependent on the goodwill of the CAs to continue their operation and may not be able to offer their customers much guarantees in relation to the quality of their services. Therefore, all three relationships should be considered. Below, we will assess which aspects should be covered at a minimum.

3.3.1 The VA-customer relationship

This relationship is the cornerstone of the VA's business viability. In order to operate successfully, the following points will need to be settled at a minimum:

- The services to be provided must be clearly defined. These should include:
 - The identification of supported CAs
 - The identification of supported standards and protocols
 - The identification of the provided services (at a minimum certificate validation and signature verification; but possibly also semantic services and historical verification of signatures, or other added value services)
 - Identification of the criteria used to classify certificates and/or signatures, and the way in which this classification is communicated. As seen in the key solutions, this can be fairly simple (e.g. signature is qualified or nonqualified; the certificate used is qualified or nonqualified), fairly elaborate (as with the BBS solution: 7 quality default quality levels for certificates, and a specific algorithm to calculate signature quality), or even fully customised (customers may choose which specific CAs are considered acceptable; this is supported by both @firma and BBS)
- Access and use conditions, including specifically the way in which the service can be used by the customer (typically web services, occasionally also secure websites, or software components to be installed locally)

- Quality of service, including guarantees in relation to availability (uptime), permissible grace periods, guarantees in relation to the supported CA's CPSes, or use of validation protocols (CRLs may not be appropriate in some cases), insofar as these are not covered by the criteria used to classify certificates and/or signatures as noted above.
- Liabilities: the validation authority should define clearly which guarantees it offers to its customers. These could take the form of universal guarantees (applicable to any certificate or signature verified through the service) or be tiered depending on the quality of the certificate or signature (e.g. guarantees offered in relation to qualified certificates should cover all aspects mentioned in article 6 of the Directive, whereas in relation to nonqualified certificates lesser guarantees are offered). Guarantees and liabilities should be defined in relation to certificates, signatures, services provided by the validation authority, supported CAs, and quality of service.

With regard to the business model, it is clear that a validation authority will need to derive some form of income from its activities to cover its liabilities; if it accepts no liabilities, then it is not considered a validation authority for the purposes of this study. Typically, this income will be provided by the customers, which may be legal entities (including private businesses or public administrations) or natural persons, and income will be calculated based on any model deemed sufficient by the validation authority (including transaction based, volume based or fixed fee per month). Alternatively, as was seen in the @firma example, the authority can be publicly funded. This is of course an equally legitimate choice, although the use of public funds will typically imply a limitation in the scope of its customer based and/or services (in the case of @firma a focus on Spanish public sector applications). From an interoperability perspective this is largely immaterial; the business model is a pure business choice.

If a federated model is applied, the observations above remain entirely valid. The main impact however is that certain elements need to be harmonised between the participants in the federation, such as e.g. common services, common criteria used to classify certificates and/or signatures, common communication protocols, and a business model that allows the participants in the federation to interact. This question will be examined in the sections below, dealing with the federated dimension (section 3.3.3.).

3.3.2 The VA-CA relationship

This second relationship is crucial to put in place a business that is sustainable for the validation authority and reliable for the authority's customer. As was already briefly noted above, a VA could choose to operate without formalising its agreement with any supported CAs, simply by relying on publicly available resources, including notably publicly accessible OCSP/LDAP/CRLs and published CPSes, but this is a relatively high risk proposition. There is no guarantee that these resources will remain accessible to the VA, and furthermore customers may be reluctant to trust a VA that has not obtained any commitments or guarantees from the CAs in respect to their services. In that respect, a formalisation of the relationship between the VA and the CAs seems necessary.

In order to operate successfully, the VA principally needs to ensure that any guarantees it offers to its own customers need to be mirrored by an equivalent obligation on the part of the CA, which would thus include the following points:

- The VA needs to obtain guarantees with regard to the certificate validation resources offered by the CA (OCSP, CRL, LDAP...) and the protocols that can be used to access these. If historical verification is required, this must also be established.
- The VA needs to obtain guarantees that the assertions it will make to its own customers in relation to the criteria used to classify certificates and/or signatures are accurate. This could be done by obtaining representations of compliance from the CAs, or by more direct means including audits conducted by the VA itself or by third parties. Obviously, in relation to qualified certificates, it would typically be sufficient for the CA to declare that the information included in the trusted list established by the competent supervisory body is accurate.
- The VA needs to stipulate how it will use the validation facilities of the CA, and to what extent, including guarantees in relation to availability (uptime). This may imply that a revenue sharing agreement is put in place, in which the CA is compensated appropriately and proportionately for the use of its services.
- Finally, in relation to liabilities, the VA will need to ensure that the CA assumes responsibility and liability for its compliance with these requirements, so that the VA can obtain compensation from any offense by a CA that results in the VA being held accountable by its own customers. In addition, the VA may choose to require specific insurance or solvency guarantees of the CA to ensure that it can meet its obligations, and should require the CA to notify the VA of any changes in its policies or practices that may impact the agreement.

In a federated model, most of these elements can be left at the discretion of each VA in the federation, as their main goal is to protect the individual VA against liability claims based on difficulties within the CA. While the VA's need to assume certain responsibilities towards each other, it is not strictly necessary that they organise themselves in an identical manner. The main requirement is that it is clear for each participant in the federation which guarantees can be provided in relation to any given CA.

3.3.3 The federated dimension

Finally, we need to consider the legal requirements introduced through the federated dimension. Supposing that a federation of VAs were to be established at the European level, then it is clear that they would need to put in place a legal framework to govern their cooperation, rights and obligations. At a minimum, this would include the following:

- Common norms and standards to be applied by the VAs to classify certificates and/or signatures;
- Common communication protocols to be used between the VAs to validate certificates;
- Compensations to be paid between participating VAs for the use of their validation services;
- Guarantees to be provided by the VAs to ensure their solvency and accountability;
- Quality of service, including guarantees in relation to availability (uptime);
- Liabilities to be accepted by the VAs in relation to each other, either in the form of universal guarantees (applicable to any certificate or signature verified through the service) or tiered depending on the quality of the certificate or signature (e.g. guarantees offered in relation to qualified certificates should cover all aspects mentioned in article 6 of the Directive, whereas in relation to nonqualified certificates lesser guarantees are offered). Guarantees and liabilities should be defined in relation to certificates, signatures, services provided by the validation authority, supported CAs, and quality of service.

This could be organised by creating a central framework agreement, managed by a central governance body at the European level, to which new VAs could voluntarily accede by declaring their compliance with all of the elements above. This body would need to manage the standards, norms and protocols to be applied by the VAs in the federation, and could be contractually accorded additional powers to ensure the functioning of the federation, including e.g. powers of auditing and mediation or arbitration in case of conflicts. In addition, it could make available standardised agreements to govern the aforementioned relations (VA-customer and VA-CA) to ensure homogeneity between the VAs practices. In this way, responsibilities and liabilities of all stakeholders in the model could be coordinated and harmonised in an efficient way.