Study on Cross-Border Interoperability of eSignatures

(CROBIES)

Common Supervision Model of Practices of Certification Service Providers issuing Qualified Certificates

A report to the European Commission

from SEALED, time.lex and Siemens

DRAFT FOR CONSULTATION

Please send your comments no later than the 30th of April 2010 to

Editing company: SEALED sprl,
VAT : BE 0876.866.142 – RPM: Tournai
12, rue de la Paix, B-7500 Tournai
olivier.delos@sealed.be, sylvie.lacroix@sealed.be

Date: 29/03/2010
Version: 1.0

Document information

Title:	CROBIES Work Package 1 **Common Supervision Model of Practices of Certification Service Providers issuing Qualified Certificates**
Project reference:	CROBIES
Document archival code:	INFSO-CROBIES-DFC-WP1-SEALED-29032010_v1.0

Version control

Version	Date	Description / Status	Responsible
V1.0	29/03/2010	Final draft for consultation	ODO, SLR

References

Ref.	Title
[1]	The European Directive 1999/93/EC of the European Parliament and the Council of the 13 December 1999 on a Community framework for electronic signatures. O.J. L 13, 19.1.200, p.12.
[2]	Study on the standardisation aspects of eSignature. A study for the European Commission (DG Information Society and Media) by SEALED, DLA Piper and Across communications, 22/11/2007.
[3]	Commission Decision 2003/511/EC "on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the EP and the Council". OJ L 175 15.7.2003, p.45.
[4]	**EESSI Mandate M279**, *Mandate to CEN, CENELEC and ETSI in support of a European legal framework for electronic signatures*, European Commission, 1998.
[5]	**EESSI mandate M290,** *Mandate addressed to CEN, CENELEC and ETSI in support of the European legal framework for electronic signatures- Phase 2: Implementation of the work programme resulting from mandate M279 and presented in Section 8.3 of the (draft) report prepared by EESSI*, European Commission, 1999.
[6]	**Mandate M460**, Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to electronic signatures, 7 January 2010.
[7]	Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on an ***Action Plan*** *on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market*, **COM(2008)798** of 28.11.08.
[8]	Directive 2006/123/EC of the European Parliament and Council of 12.12.06 on services in the internal market, OJ L376 of 27.12.06
[9]	Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. OJ L 299 of 14.11.2009, p. 18.
[10]	Study on the European Federated Validation Services. Framework contract ENTR/05/58-SECURITY, SC N°14 – Completion of the framework for signature validation services. February 2010 reports.

Definitions and Acronyms

Please refer to the Head Document for definitions and acronyms used throughout the present report.

Table of Contents

Common Supervision Model of Practices of Certification Service Providers issuing Qualified Certificates

1 Introduction

The present report proposes a common model, criteria and practices that could be used by Member States' bodies in charge of the supervision or voluntary accreditation of CSPs issuing QCs. The model can, and ideally should, be extended to the supervision and 'voluntary accreditation' of other types of certification service providers providing services ancillary to electronic signatures (e.g., provision of non-qualified certificates, time-stamping services, long term archiving, registered electronic mail, extended validation services).

The report is the result of Work Package 1 of the CROBIES study and aims at providing recommendations on how to further improve the trustworthiness of the supervision (accreditation) systems of CSPs in Member States. It proposes to establish a common model of supervision and voluntary accreditation of certification services ancillary to electronic signatures to enhance the interoperability, cross-border use and mutual recognition of electronic signatures and of added-value certification services either supporting or employing electronic signatures.

CROBIES

The CROBIES study looks at eSignature interoperability in general, but specifically in the context of cross-border use. While considering a consistent global and long term approach in proposed improvements at the legal, technical and trust levels, CROBIES is also focusing on quick wins that could substantially improve the interoperability of electronic signatures. These include most notably the establishment of a community framework for national Trusted Lists of supervised/accredited CSPs, input to the standardisation efforts in the field of electronic signatures and in particular in relation to certificate profiles, SSCD profiles and signature implementation guidance, and the proposal for a common model for CSP supervision and accreditation systems. This latter topic is addressed by the present CROBIES Work Package 1 report.

The global overview of the CROBIES study and of its approach is to be found in the "Head Document" of the study. The study is part of the *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market* adopted by the European Commission on 28.11.2008[1] [7] which aims at facilitating the provision of cross-border public services in an electronic environment.

[1] COM(2008) 798, http://ec.europa.eu/information_society/policy/esignature/action_plan/index_en.htm

2 Background information on the Supervision of CSPs

2.1 Supervision and Accreditation as defined in the eSignature Directive 1999/93/EC

2.1.1 Certification Service Providers

Article 2.11 of Directive 1999/93/EC on a Community framework for electronic signatures [1] (here after referred to as "Directive 1999/93/EC") defines a 'certification-service-provider' (CSP) as "*an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures*". When further refining this definition of a CSP, and taking into account recital (9) of Directive 1999/93/EC[2], one can identify the following categories of CSPs:

- CSPs issuing qualified certificates;
- CSPs issuing non-qualified certificates;
- CSPs providing other (ancillary) services related to electronic signatures such as:
    - CSPs providing services supporting electronic signatures, e.g.:
        - Provision of time stamping services
        - Provision of eSignature generation services
        - Provision of eSignature validation services
        - Provision of (long term) archiving services
    - CSPs providing services employing electronic signatures, e.g.:
        - Provision of registered electronic mail
        - Etc.

2.1.2 Appropriate supervision system

Article 3.3 of Directive 1999/93/EC requires that "*Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public*".

How the supervision system is established is left to the Member States. Recital (13) of Directive 1999/93/EC [1] states that "*the Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme*".

[2] *"(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, timestamping services, directory services, computing services or consultancy services related to electronic signatures;"*

2.1.3 Voluntary accreditation

While an "appropriate" system of supervision is mandatory for certification service providers issuing qualified certificates to the public and when established in a Member State, a 'voluntary accreditation' may be applied by any type of certification service provider. Directive 1999/93/EC defines the voluntary accreditation in its Article 2.13 as "*any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body*".

Article 3.2 of Directive 1999/93/EC requires that "*Without prejudice to the provisions of paragraph 1 [Member States shall not make the provision of certification services subject to prior authorisation], Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive*".

Article 7.1.a of Directive 1999/93/EC states that "*Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification service provider established in a third country are recognised as legally equivalent to certificates issued by a certification service provider established within the Community if: (a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State*".

A CSP issuing qualified certificates (to the public) must be supervised by the Member State (administration) in which it is established, if it is established in a Member State. Such a mandatory supervision of qualified certificates issued by certification services from supervised certification service providers provides assurance to relying parties that a claimed qualified certificate is in compliance with the provisions laid down in this Directive. A CSP issuing qualified certificates and established or not in a Member State may, on a voluntary basis, be accredited in any Member State in which a 'voluntary accreditation' system has been established. When not established in a Member State, such a voluntary accreditation is one of the applicable mechanisms for third country CSPs to have their qualified certificates issued to the public recognised as legally equivalent to qualified certificates issued by a certification service provider established within the Community (as foreseen in Article 7.1.a of Directive 1999/93/EC).

With regards to voluntary accreditation, the following principles from recitals (4) and (11) to (13) of Directive 1999/93/EC apply:

- ***Divergent rules*** *with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States* ***may create a significant barrier*** *to the use of electronic communications and electronic commerce* [1, consideration (4)];

- *Voluntary accreditation schemes* ***aiming at an enhanced level*** *of service-provision may offer certification service providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers* [1, consideration (11)];

- *Certification service providers should be left* ***free to adhere to and benefit from*** *such accreditation schemes* [1, consideration (11)]; *Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes* [1, consideration (12)]; *this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme* [1, consideration (13)];

- *It should be ensured that such accreditation schemes* ***do not reduce competition*** *for certification services* [1, consideration (12)];

2.1.4 Notification and Data Protection

Article 11 (**Notification**) of Directive 1999/93/EC states that:

1) *Member States shall notify to the Commission and the other Member States the following:*
    a. *information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);*
    b. *the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);*
    c. *the names and addresses of all accredited national certification service providers.*
2) *Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.*

Finally, Article 8.1 of Directive 1999/93/EC requires that "*Member States shall ensure that certification-service providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*".

2.2 Importance of the provision of information on supervised or accredited CSPs issuing QCs

Directive 1999/93/EC [1] requires Member States to implement *appropriate* supervision systems allowing for supervision of CSPs which are established on its territory and issue qualified certificates to the public (see article 3.3, recital (13), article 8.1, and 11 of [1]). But it does not specify how this has to be done.

The reliability of the so-called "qualified electronic signatures" (i.e. "*advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device*" as defined in [1, Article 5.1]) relies by definition on the reliability of qualified certificates (QCs) and hence on the reliability of the applicable *appropriate* supervision system.

Qualified electronic signatures (QES) are granted legal equivalence to handwritten signatures without giving the relying parties the right to contest this equivalence based on an alleged inadequate supervision scheme. The assumption of legal reliability of supervision schemes is thus clearly present in the Directive. Challenging this assumption would imply that relying parties would have the right to question the adequacy of supervision systems, and thus of the legal value of qualified signatures. This would run contrary to the letter and spirit of the Directive: it would undermine the cross border value of qualified electronic signatures, as any relying party would always be able to argue that the quality of supervision in another Member State might be *inappropriate*.

This relationship between supervision and the legal value of certificates and signatures highlights the need for information on which CSPs are supervised in Member States.

In the absence of supervisory bodies, any CSP would be able to claim that a certificate would be qualified, without any possibility of verifying this claim. Since qualified electronic signatures are automatically declared legally equivalent to handwritten signatures, this would create a system based largely on fiction: qualified electronic signatures are considered trustworthy, because they meet a number of requirements including the use of a qualified certificate, which is trustworthy because it is issued by a CSP issuing QCs, who is trustworthy simply because he says so in the certificate. Clearly, this approach of self-declared trustworthiness would not be likely to create a significant degree of trust in CSPs, and in particular in foreign CSPs, issuing issued QCs.

If it were not for the role of a supervisory body to ensure, as a third party with a governmental mandate, that QCs issued by a CSP established in its territory indeed meet the requirements of Directive 1999/93/EC, no relying party would ever be able to accept foreign signatures (including qualified electronic signatures) without assessing for itself whether the issuing CSP is in compliance with the requirements of Directive 1999/93/EC. This would of course not be feasible.

Thus, the Directive creates a clear tiered trust system: qualified certificates inherit trust from the CSP issuing QCs, who inherits trust from the supervision system. This trust system is logical and complete, on one condition: that the relying party can indeed assess whether or not the supervision status of a CSP service issuing QC is in fact available and acceptable.

In practice, until end of 2009, in the absence of a coherent strategy for presenting supervised CSPs issuing QCs at a European level, relying parties who required the use of qualified certificates encountered a very difficult task in assessing whether a received claimed qualified certificate was issued by a supervised CSP issuing QCs. This was a result of the insufficient or inconsistent information provided at the time by MS's on the supervision or voluntary accreditation status of CSPs issuing QCs. The Directive provides the qualified electronic signature with a specific legal value, however, in the absence of information about the supervised or voluntary accredited CSPs issuing QCs, in the form of a "trusted list" the relying party could not know if a signature is really qualified without investing unreasonable auditing resources. The recent Commission Decision 2009/767/EC [9], to the content of which CROBIES WP2 brought a significant contribution, establishes a legal basis and a common template for Member States national trusted lists of supervised or accredited CSPs. With regards to CSPs issuing QCs, those Trusted Lists ensure that services from those CSP's issuing QCs that are listed in the Trusted List are by definition supervised, thus the QCs issued by those services are trustworthy, and thus the legal value of qualified signatures supported by such QCs can no longer be reasonably contested by any relying party.

2.3 Possible extension of the supervision model towards provision of other certification services than issuing qualified certificates

With regards to Article 2.11, and recital (9), Directive 1999/93/EC [1] does not apply only to certification service providers issuing certificates but to "*any entity or legal or natural person who provides other services related to electronic signatures*". This may encompass but not be limited to, e.g., the provision of registration services, time-stamping services, directory services, long term archiving services, electronic registered mail, validation services,

provision of electronic signature software, hardware including SSCDs[3], and computing services or consultancy services related to electronic signatures.

While it may be clear that the basic principles of Directive 1999/93/EC can be derived as applicable to all such other types of services ancillary to electronic signatures, the Directive lacks specific requirements applicable to those services as it mainly focuses on requirements for the issuance of qualified certificates.

It is noticeable however that the standardisation framework associated with Directive 1999/93/EC includes some documents specifically addressing technical and practice specifications for some of these services (e.g. time-stamping services), but it does not cover all of them and requires some improvements and rationalisation[4].

The CROBIES study approach relies on the strong belief that it is only through the establishment of sound, closely mapped and consistent legal, standardisation and trust frameworks covering all types of electronic signature products and ancillary (trusted) services that interoperability issues of electronic signatures could be efficiently tackled and (cross-border) successful implementations of electronic signatures could be facilitated[5].

The 'legal framework improvement' track in the context of improving the existing eSignature legal framework is recommended to be addressed by extending Directive 1999/93/EC to cover legal requirements on all types of products and services ancillary to electronic signatures (i.e. not limited to the sole provision of (qualified) certificates) and by extending accordingly the current formal "new approach-like" mapping between legal requirements and "generally recognised standards"[6].

The 'standardisation framework improvement' track is to be addressed by Mandate M460 [6] aiming for a recast of the existing electronic signature standardisation framework around the rationalisation of the standardisation of (i) technical specifications and policy requirements, (ii) conformity assessment guidance (CAG) and (iii) implementation guidance and support facilitating the adoption of those standards by the market.

It is expected that on the basis of (i) and (ii), one could derive a common model for establishing "appropriate" supervision systems and voluntary accreditation systems. This would address one aspect of the improvement of the eSignature trust framework and would further facilitate the cross-border recognition of supervised or voluntarily accredited certification services other than issuing qualified certificates. Those two action items, trusted lists and a common model for supervision and accreditation systems are the main aspects of the 'trust framework improvement track'.

The 'common model for establishing "appropriate" supervision systems and voluntary accreditation systems' proposed in this CROBIES WP1 deliverable is based on the principle that MS supervision systems could rely on the extended legal framework, mapped to the recast and generally recognised standardised specifications & policy requirements and standardised CAG covering all types of products, certification services (e.g. provision of certificates, provision of timestamping services, provision of archiving services) and their related trust tokens (e.g. respectively digital certificates, time-stamp tokens, archives) to build up their national supervision and voluntary accreditation systems.

[3] Regarding SSCDs, this will also be specifically treated in WP4.
[4] See Mandate M460 [6] and other CROBIES deliverables.
[5] This belief has been recently further illustrated and confirmed in a closely related study, namely the EFVS study [10].
[6] See CROBIES Head Document and EFVS study reports [10].

Chapter 3 highlights the benefits and significant positive impacts that a common model for supervision systems and voluntary accreditation systems may have on the supervisory and accreditation bodies as well as on the market. It also provides a general overview of the proposed model.

Chapter 4 describes the proposed model into details while Chapter 5 gives some recommendations for the possible next steps towards a potential adoption and implementation of such a proposed model.

3 Common model for supervision / accreditation systems related to the provision of certification services

3.1 Introduction

Despite the fact that MS have the freedom to decide what they consider to be an *appropriate* supervision under Directive 1999/93/EC [1] for CSPs issuing QCs, creating a reference model for supervision (and for voluntary accreditation systems) of CSPs, whatever the type of services they provide, could have a **significant positive impact**, in particular for other services than issuing QCs, on the interoperable, cross-border use and mutual recognition of those services and hence electronic signatures supported by such services[7], namely:

- With regards to CSP not issuing QCs but providing services ancillary to electronic signatures a common model for supervision (respectively 'voluntary accreditation') relying on a common set of standards would be a sound basis for an improved interoperability, cross-border usage and mutual recognition of such services within the Community and towards third countries or international organisations;

- With regards to CSP issuing QCs, such a common model would serve as reference for Member States not yet having a supervision or accreditation system in place and willing to establish one (e.g. because no CSP issuing QC is active yet on their market, or because those countries are new comers in the EU);

- With regards to CSP issuing QCs, such a common model would serve as a reference model for negotiation of bilateral or multilateral recognition agreements between the Community and third countries or international organisation for the recognition of the legal equivalence of certificates issued by third country CSPs;

- With regards to CSP issuing QCs, such a common model could serve as a reference model for a Member State assessing its own existing supervision (or respectively 'voluntary accreditation') system, when applicable.

A key success factor and pre-condition for significant positive impact is that the various types and even sub-types of certification service ancillary to electronic signatures (including issuance of digital certificates) are precisely and unambiguously defined and the provision of such services clearly and unambiguously identified against one of such types or sub-types. This should of course be consistently implemented in all relevant frameworks, i.e. legal, technical/standardisation and trust frameworks.

[7] Note that the impact of such a model would obviously differ depending on a service.

The proposed common model for supervision (and accreditation) of CSPs does not mean that Member States cannot raise the level of some requirements or increase the level of identified specifications for whatever general or specific application domains. However by doing so Member States should take into account the potential barriers, positive or negative consequences, this may create for their own national supervised or accredited services.

For the sake of readability and simplicity, the presentation of the next sections mainly focus on the supervision systems for evaluating compliance of CSPs issuing QCs with the provisions laid down in Directive 1999/93/EC but the common model for supervision of CSPs issuing QCs is designed in such a way that it can also be applied to all other types of CSPs providing services ancillary to electronic signatures and to "voluntary accreditation". Whether or not it is desirable to extend the proposed model to the supervision of CSP services other than the issuing of QCs and to voluntary accreditation systems is of course a policy decision. However, this paper takes the perspective that such an extension is desirable at least from an interoperability perspective (which is a key goal of CROBIES study). Whenever applicable and necessary, specific provisions for "voluntary accreditation systems" or for covering CSPs not issuing QCs will be explicitly provided.

This exercise is based on (i) the information received from Member States in the context of discussions on the Implementation of the Services Directive [8] and (ii) on information provided by Member States via FESA[8], in particular the replies to a FESA questionnaire on the issues of supervision and audit procedures, as well as (iii) on information on supervision/accreditation systems either publicly available (e.g. on Member States Supervisory Body websites) or directly provided by Member States.

3.2 Overview of a proposed common model for supervision and accreditation systems

As depicted in Figure 2 below, the following key categories of elements could be proposed for a common model for supervision and voluntary accreditation systems:

- The **initiation** step: This corresponds to the entrance on the market of the certification services of a new CSP and the means by which the Administration in charge of the supervision of such services becomes aware of the new CSP's services and starts to supervise the CSP[9]. With regards to the supervision of CSPs issuing QCs to the public, supervision by Member States is mandatory [1, art.3.3] for CSP_{QC} established on their territory but no prior authorisation can be imposed on the CSP [1, recital (10)]. Voluntary accreditation implies on the contrary an explicit application from a CSP to be assessed with regards to the provision of a specific certification service, after which and dependent on the result of the assessment, the CSP can evoke its status of accreditation (i.e. some prior action is needed from the CSP side contrary to supervision).

- The **compliance criteria**: This refers to the criteria against which the provision of certification services by a CSP will be assessed whether for supervision or accreditation purposes. It is likely that the criteria to be met will be the same for the provision of a specific type of service (e.g. provisions laid down in Directive 1999/93/EC for certification services issuing QC to the public) but will only differ between supervision and accreditation modes in the sense of "*voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-*

[8] FESA: Forum of European Supervision Authorities (www.fesa.eu).
[9] This can also apply to new services provided by an existing CSP.

service providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market" [1, recital (11)]. Those criteria should of course take into account specificities of the type of certification service to be assessed, be organized under the form of a check-list for the sake of facility for both the evaluated and the evaluator, be publicly available, based on standards and supported by a (national) legal framework.

- The **supervision (respectively accreditation) process**: This refers to the way both supervision and voluntary accreditation are organised and processed. This covers rules and processes for the designation of evaluators (supervision) and auditors (accreditation), the guidance and related rules to be observed by evaluators and auditors when conducting assessments, the overall evaluation/audit process with regards to the parties involved (e.g. the Member State Supervisory or Accreditation Body, the evaluators/auditors, the assessed party), and specific characteristics with regards to the supervision/accreditation process, like the frequency of controls/audits, the depth of such controls/audits, the associated fees, and the procedures related to complaints from either the market or the assessed CSPs.

- The **responsibilities and liabilities** for each of the involved parties taking part in the supervision or accreditation of certification services ancillary to electronic signatures.

Common model overview for supervision/accreditation of CSPs

Supervision systems	Accreditation systems

• Initiation
• Compliance criteria
(e.g. For CSP_{QC} meeting requirements from Directive 1999/93/EC)
  • Under the form of a Checklist
  • Publicly available
  • Standards based
  • Legal basis
• Supervision process
  • Evaluators designation process
  • Evaluation guidance
  • Evaluation process flow
  • Evaluation Process features
  • Frequency
  • Depth
  • Fees
  • Complaint procedures
• Responsibilities & liabilities
	• Initiation
	• Compliance criteria
	(e.g. For CSP_{QC} meeting requirements from Directive 1999/93/EC)
	  • Under the form of a Checklist
	  • Publicly available
	  • Standards based
	  • Legal basis
	• Accreditation process
	  • Auditors designation process
	  • Audit guidance
	  • Audit process flow
	  • Audit Process features
	  • Frequency
	  • Depth
	  • Fees
	  • Complaint procedures
	• Responsibilities & liabilities

Figure 1

The next section will further describe the details for each of these elements as part of the recommendations for a common supervision (respectively accreditation) model.

4 The proposed common model for supervision and accreditation systems in detail

4.1 Initiation

4.1.1 Supervision Initiation

On the one hand, with regards to the supervision and accreditation of CSPs (whatever certification service is provided), according to Directive 1999/93/EC, there must be no prior authorisation or any assimilated barrier to the entrance of certification services on the internal market; "*certification-service-providers should be free to provide their services without prior authorization; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect*" [1, recital (10)].

On the other hand, there is an obligation for Member States to appropriately supervise CSPs issuing QCs [1, art. 3.3] with the aim to provide assurance that they are meeting the provisions laid down in Directive 1999/93/EC. This obligations applies naturally from the day those services are entering the internal market.

In order to avoid or at least to mitigate the significant risk of entrance in the market of a non compliant CSP issuing QC, and hence to facilitate the initiation of supervision, a notification by CSPs (subject to supervision) of the start of their activities to relevant Member State's administration could be considered keeping in mind that this notification must not be an implicit way of implementing a prior authorisation mechanism.

This notification, whatever the size of the requested information aiming to support the supervision process by the Supervisory Body, does not contradict Directive 1999/93/EC provisions provided that it serves merely to support the assessment of compliance with the requirements imposed by the Directive with respect to CSPs issuing QCs, and that the CSP would not be prohibited to provide its certification services even when not providing such notification information, or providing incomplete information or even when providing not enough or unsatisfactory evidence of meeting the supervision criteria and requirements. This does not present specific trust problems, since the status of a CSP issuing QCs can be determined through the Supervisory Body (primarily via the trust list), and in the absence of a valid notification, the Supervisory Body will be unable to confirm the CSP's status towards this parties, thus significantly impairing its business potential. Therefore, in practical terms, there is a very strong incentive for CSPs to file complete and timely notifications to the Supervisory Bodies.

This notification should occur in a *reasonable* timeframe before or at the start of the certification services provision subject to supervision without being disproportionate compared to the amount of information reasonably required to support the assessment of compliance with the provisions laid down in Directive 1999/93/EC on which Member State's supervision system is based.

This principle of notification is of crucial importance both for the CSP willing to provide such certification services being subject to supervision and the Supervisory Bodies:

- Publication of the list of required information will help CSPs to meet the supervision criteria and requirements (in particular when a self-assessment is reasonably required as part of the notification information); and

- Supervisory Bodies would get information allowing and facilitating their supervision obligation at the time of CSP entrance into the market or even some time prior such entrance with the aim of mitigating risks and protect consumers against non-compliant CSPs issuing QCs entering the market.

Considering the significant trust impact of the provision of such trusted third party services that are certification services ancillary to electronic signatures, it is recommended to require the provision to the Supervisory Body of the following set of information and documents together with the notification of start of the provision of certification services subject to supervision:

- **Administrative and identification information** related to the CSP being either a public entity or a legal or natural person, when it is established in accordance with the national law: this includes but may not be limited to the name of the CSP, company information as registered in accordance with national laws, organization and company structure, capital, balance sheet and annual reports, contact information, etc.

- **Information on the basis of which it is possible to assess whether the certification services (e.g. issuing qualified certificates) meet the provisions laid down in Directive 1999/93/EC,** potentially completed by national provisions when applicable. This should include information allowing an assessment of the factual, technical, security, personnel and organizational qualifications of the CSP service to which the supervision system applies. As further explained in the present section of the report, this information is recommended to be organized around the following two components:

    - The **Full Certification Practices Statement** (Full CPS) describing the practices the CSP employs in providing its certification services;

    - The CSP **Self-Assessment** of compliance with the supervision criteria.

The most appropriate and standardised way to structure the CPS information is defined in RFC 3647.

> Note: While it is true that RFC 3647 is mainly oriented to the provision of certifications services issuing digital certificates in the context of a Public Key Infrastructure (PKI), the structure (table of contents) of the information to be provided in a CPS can be easily adapted and standardised[10] to any type of certification service ancillary to electronic signatures in the sense of Directive 1999/93/EC [1, art. 2.11, recital(9)], e.g. Time-Stamping Practices Statement, (Long Term) Archiving Practices Statement, Signature Validation Services Practice Statements. In the remaining of the text, unless specifically specified, the term CPS will be used to cover all types of Practices Statements related to the provision of services ancillary to electronic signatures.

Since a detailed CPS may contain sensitive details of its system, a CSP may elect not to publish its entire CPS. It may instead opt to publish a so-called CPS Summary. The CPS Summary would contain only those non-sensitive provisions on CSP's practices from the Full

[10] Such a standardization effort is clearly recommended and expected to be addressed in the context of Mandate M460 on the rationalization of the eSignature standardization framework [6].

CPS that the CSP considers to be relevant to the participants in the provision of certification services and in particular with the aim to convince relying parties of their trustworthiness.

In the context of the supervision of certification services (in particular those services issuing QCs to the public), the required notification information should include the disclosure to the Supervisory Body of the Full CPS.

For the sake of clarity, the Full CPS should be structured in compliance with RFC 3647 when certification services are related to the provision of qualified or non-qualified certificates and even when related to the provision of certification services ancillary to electronic signatures, to the extent feasible and applicable with regards to the standardized table of content provided by RFC 3647.

The Full CPS will cover the provision of practices statements on the following topics[11]:

1. **Global overview** of the infrastructure supporting the provision of certification services (e.g. a PKI in the context of issuing digital certificates), including the description of the component services and participants active in the provision of those services as well as subscribers and relying parties, the description of the appropriate and prohibited usage of the certification services results (e.g. digital certificates, timestamps, etc.) and the rules for administrating and managing policy and practices documentation related to the provision of the certification services;

2. **Publication and repository responsibilities**: describing the entities responsible for operating repositories in the context of the provision of certification services, the type of information that is published in those repositories, time and frequency of publications and access control on those repositories;

3. **Identification and authentication rules** for subscribers and providers of component services in the context of the provision of the certification services: This describes the procedures used to authenticate the identity and/or other attributes of an end-user certification service applicant prior service issuance. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to operate in or interoperate with the CSP. It also addresses naming practices.

4. **Certification Service Output (CSO)[12] life-cycle operational requirements**: This part describes requirements imposed upon the CSP and the entities providing component services as part of the CSP certification service with respect to the life-cycle of the CSO (e.g. digital certificate, timestamp token, long term archive, etc.) when applicable. This covers application for a CSO, application processing, issuance, acceptance, renewal, and when applicable, modification, suspension and revocation, status service, end of subscription, archiving, auditing, escrow and recovery.

5. **Facility, management and operational controls**: This component describes non-technical security controls (i.e. physical, procedural, and personnel controls, as well

[11] Please refer to RFC 3647 for more detailed information on the set of provisions which are here after categorized in nine primary components as outlined in the CPS framework as defined in RFC 3647 (http://www.ietf.org/rfc/rfc3647.txt).

[12] The Certification Service Output (CSO) is here defined as a physical or binary (logical) object or service output generated or issued as a result of the use of a Certification Service ancillary to electronic signatures provided by a CSP as defined by Art. 2.11 of Directive 1999/93/EC.

as audit logging procedures, records archival, compromise and disaster recovery) used by the CSP to securely perform its services and focusing description on critical component services and security tasks. It also covers provisions to ensure proper termination of the whole or part of its component services. These non-technical security controls are critical to trusting the CSO since lack of security may compromise CSP operations.

6. **Technical security controls**: This component is used to define the security measures taken by the CSP to protect its cryptographic keys and activation data, to impose constraints on repositories, subscribers, provider of certification services components and other participants to protect their private keys, activation data for their private keys, and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel. This component also describes other technical security controls used by the CSP to perform securely the key operations of its provision of certification services. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology), computer, network and operational security controls.

7. **Content description and profiles for CSO**: This component is used to describe the format, content description and profile of CSOs (e.g. certificate, CRL and/or OCSP profiles in the context of CSPs issuing (qualified) certificates).

8. **Compliance audit and other assessments**: This component addresses the following:

    - The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment;
    - Frequency of compliance audit or other assessment for each entity that must be assessed pursuant to its practices requirements, or the circumstances that will trigger an assessment;
    - The identity and/or qualifications of the personnel performing the audit or other assessment.
    - The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.
    - Actions taken as a result of deficiencies found during the assessment;
    - Who is entitled to see results of an assessment, who provides them, and how they are communicated.

9. **Information on other business and legal matters**: This component covers general business and legal matters like fees and refund policy, financial responsibility, confidentiality of business information, privacy of personal information, IPRs, representations and warranties, disclaimer of warranties and limitation of liability, indemnities, term and termination, individual notices and communication with participants, amendments, dispute resolution and governing law, etc.

In terms of documents, the provision of the full CPS is expected to include, but not limited to, the following documents:

- The ***CPS Summary*** providing the public statements on the practices the CSP employs in providing its certification services and covering all the above nine components;

- This CPS Summary should be **completed by all CSP internal documents providing detailed description on practices related to the above nine components**. This should include but not be limited to the following list of typical CSP internal and sensitive documents providing detailed information on the basis of which an assessment can be initiated:

    - **CSO Policies** (e.g. Certificate Policies – CP, Timestamping Policies, etc.) specify general rules used by the CSP for the issuance of the CSO (e.g. qualified certificates). The purpose of each of these CSO Policies is to establish what Participants (CSP, and/or component services providers) within the Certification Services Infrastructure must do in the context of requesting, issuing, managing and using the specific type of CSO described in the related CSO Policy. The set of rules, requirements and definitions stated within a CSO Policy is determining the level of security reached by the associated CSO type.

    - **CSP Managerial Body** (often called Policy Approval Authority) related documents, i.e. statutes, governance rules and the review process for practices related documents (i.e. Full CPS and associated component documents)

    - **Certification Service Disclosure Statement**: This document that should also be available independently to subscribers and relying parties describes the key subscriber and relying party oriented information about the certification services. This relates to the PKI Disclosure statement or the Time-Stamping Disclosure statement with regards to the provision of certificates and timestamp tokens respectively but this concept can be extended to any provision of certification services.

    - **Risk assessments and inventory of assets**: A risk assessment has to be carried out in the context of the provision of certification services that are subject to supervision in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures. This risk analysis shall be done with the full support and collaboration of all component services providers and shall be regularly reviewed and revised if necessary. This should include an inventory of all information assets and classification for the protection requirements to those assets consistent with the risk analysis.

    - **Security policies**: This should include, but not be limited to, access control security policies for secure areas on Certification Services Infrastructure (CSI) secure sites and premises, physical an environmental security policies, information security policies, CSI system security policy and CSI personnel security policy.

    - **Incident Management and Compromise Handling procedures** as part of a more complete document named "**Service Level Management**"

    - **Disaster Recovery, Business Continuity and Termination plans**

    - **CSI Operations Management procedures** aiming to demonstrate that the CSI system components are secure and correctly operated, with minimal risk of failure.

- **CSI System Access Management procedures** aiming to demonstrate that CSI system access is limited to properly authorised individuals in accordance with the System Access Management provisions and security policies.

- **Trustworthy system deployment and maintenance procedures**

- **Contractual agreements**: including
  - General terms and conditions applicable to Subscribers and Relying Parties;
  - Specific contractual agreement with Subscribers;
  - Contractual agreements with all external organizations supporting the provision of certification services through the provision of component services.

  Those contractual agreements should include, either directly or by reference, all obligations of such entities, including the applicable policies and practices.

- **Keys and activation data lifecycle management document:** This information component should provide the description of the trustworthy process and systems for the generation of CSP private keys, activation data and certificates (and those of any component service active in the CSI to operate and support the certification services), and for their life cycle management, according to documented procedures.

- **CSI Hardware Security Modules (HSM) life cycle management:** This information component should provide the description of the life cycle management procedures related to the CSI HSMs. Those detailed life cycle management rules and procedures should be consistent with and ensure the related statement made in the CPS and applicable CSO Policies.

- **Procedure for clock synchronization with UTC** (when applicable)

- **Recording rules and procedures:** This component should provide information on how it is ensured that all relevant information concerning the operations of the CSP certification services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings.

- The **complete description of the CSI technical, physical and logical infrastructure**, including:
  - The complete (technical, logical, physical) description of the entire CSI.
  - Detailed description of implemented CSI computer, life cycle and network security controls details
  - Detailed description of all secure sites and premises used by the CSP to provide its certification services, including, per site, a detailed description of physical security, infrastructure and network security, procedural security, physical and logical access control
  - Description on how all communications between CSP's certification services components regarding any phase of the life cycle of the CSOs are secured to ensure confidentiality, mutual authentication and secure logging/auditing.

- **Trusted personnel related information and documentation**, including, job descriptions, CVs, signed contractual agreements (including NDA and signed "non-conflict of interest" statement), recruitment rules, (re-)trainings processes, tasks allocation rules and processes.

- **Operational procedures and guidelines** for **all CSI Participants** for the provision of component services or parts of component services as part of the provision of the CSP certification service (other than Subscribers, i.e. for CSP issuing certificates; security officers such as Registration Authority, Central Registration Authority, Suspension & Revocation Authority, Certification Authority, (S)SCD Officers, ...).

Besides the classical administrative and identification information related to the CSP, and the Full CPS structured information, yet another significant piece of information is recommended to be required from the CSP in the context of the initiation phase of the supervision of the CSP's certification services, namely the **Self-Assessment of compliance against supervision criteria**. The self-assessment of compliance could be based on a check-list organised according to the following template:

- One entry (row) per supervision criteria to be met;
- The following columns per entry:
  - Identification number of the supervision criteria
  - Title of the supervision criteria
  - Reference(s) to explanations and detailed information about the supervision criteria specifications and requirements
  - Indication on the severity of the criteria (e.g. based on a three-value metric like the classic "low", "medium", "high")
  - Self-evaluation of compliance with the supervision criteria according to a three-value metrics: "green" (fully compliant), "orange" (partially compliant), "red" (not compliant)
  - Free text field allowing the CSP to provide results of the self-assessment with regards to the supervision criteria and arguments with regards to the self-evaluation value (green, orange or red). This can include references to annexed documentation (e.g. components of the Full CPS).
  - Free text field allowing the Supervisory Body to comment CSP's self-evaluation of the supervision criteria and when applicable to require corrective measures.

On the start of activities of a CSP issuing QC into the market, it is however the responsibility and obligation of the Supervisory Body to implement its appropriate supervision system and to perform the appropriate controls foreseen in its supervision system upon reception of a notification of the provision of certification services subject to supervision. When notification information is inexistent, incomplete, insufficient or not satisfactory with regards to compliance with the supervision criteria, and when the consecutive supervision control (after the start by the CSP of the issuing QC activities) reveals that the CSP fails to comply with the supervision criteria, it is up to the Supervisory Body to take the appropriate measures to enforce corrective actions on the CSP or require the cessation of the related activities in accordance with national legislation.

The described set of notification information should actually be considered as advantageous for the CSP as the communication of a clear list of obligations for the business of CSPs issuing QCs, namely the supervision criteria, have to be clear and known in advance hence he has the ability to perform, before starting its activities, a self-assessment on the basis of a check-list. This offers the CSP the advantage of a better preparation, from earliest stages of the conception, building and implementation of the certification services issuing QSs and allowing CSP to maximise the chance for successful supervision.

4.1.2 Accreditation Initiation

When considering certification services ancillary to electronic signatures (including issuance of digital certificates), voluntary accreditation as defined in Directive 1999/93/EC is the sole accreditation type considered here. Whenever the term “accreditation” is used in this report, it is meant to be “voluntary accreditation” as defined in article 2.13 of Directive 1999/93/EC. Accordingly, accreditation implies a confirmation of compliance (namely with rights and obligations specific to the provision of certification services) to be granted upon request by the concerned CSP, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to declare its compliance with the accreditation scheme until it has received the decision by the body.

Consequently, the accreditation initiation should consist in an application for a certification service to be granted with an accredited status resulting from the successful audit of the certification services against accreditation criteria. This accreditation application is to be submitted by the CSP to the Member State's Accreditation Body[13].

Similarly to the reasoning developed in the previous section, it is recommended to organise the accreditation initiation under the form of an accreditation application requiring the provision by the CSP of classical administrative and identification information about itself, of the Full CPS and of a self-assessment of compliance with accreditation criteria on the basis of a check-list to be filled in.

4.1.3 Summary

Supervision Initiation:

No prior authorisation to the provision of certification services subject to supervision (e.g. issuing of QCs) but notification of the provision of certification services. Information to be provided together with the notification includes classic administrative and identification information about the CSP, the Full CPS and a self-assessment of compliance with supervision criteria on the basis of a check-list to be filled in.

Accreditation Initiation:

Voluntary accreditation implies on the contrary an explicit application from a CSP to be assessed with regards to the provision of a specific certification service, after which and dependent on the result of the assessment, the CSP can evoke its status of accreditation (i.e. some prior action is needed from the CSP side contrary to supervision). Such accreditation must voluntarily be applied for by a CSP by submitting an application form to the Member State Accreditation Body together with the provision of classic administrative and identification information about the CSP, of the Full CPS and of a self-assessment of compliance with accreditation criteria on the basis of a check-list to be filled in.

[13] Note that nothing precludes the Supervisory Body and the Accreditation Body to be distinct entities or a single and same entity.

4.2 Compliance Criteria

4.2.1 Supervision Criteria

4.2.1.1 Organised per certification service type

When considering supervision of certification service providers for compliance with the provisions laid down in Directive 1999/93/EC and when considering the broad meaning of the definition of 'certification-service-provider', supervision criteria should naturally be organised per type of certification services while it is expected that certain criteria and requirements will be common to all certification service activities or to groups of them. Without being exhaustive, the list of types of certification service activities should include at least the following:

1. Certification services issuing certificates:
   a. Certification services issuing qualified certificates
   b. Certification services issuing non-qualified certificates
2. Certification services other than issuing certificates but ancillary to electronic signatures:
   a. Services supporting electronic signatures
      i. Time stamping services
      ii. Electronic signature generation services
      iii. Electronic signature validation services
      iv. (Long term) Archiving services
   b. Services employing electronic signatures
      i. Provisioning of electronic registered mail services
      ii. Additional services to be identified

Furthermore, besides criteria common to all components of a certification service, within each of these categories of certification service activities, the supervision criteria can further be organised per component service.

In the context of the provision of supervision status of supervised certification services, there is a need for further specifying some of the above listed categories in order to further facilitate the comparison between different sub-categories of certification services. For example the provision of non-qualified certificates can be organised around specific levels of security/quality of digital certificates such as the NCP+, NCP, and LCP levels from ETSI TS 102 042[14], or around other levels being defined in the context of PEPPOL, STORK and other initiatives. There is a need for rationalisation in the context of the ranking of such digital certificate issuing certification services to align them with eIdentification levels (often not relying solely on the use of digital certificates) and with levels to be defined for Advanced Electronic Signatures as defined by Directive 1999/93/EC[15].

4.2.1.2 Standards based criteria

The business model adopted by the policy makers in Directive 1999/93/EC was to link the publication of some standards to a legal presumption of conformity with some legal

[14] ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

[15] Please refer to CROBIES deliverable WP5-2 for a proposed "Quality Classification Scheme for eSignature (elements)".

requirements of this Directive. Decision 2003/511/EC is the current instrument to implement such a link. It specifically focuses however on only one part of the elements covered by the definition of an "electronic signature product" (Directive 1999/93/EC, Article 2.11[16]). It only covers those product elements related to the Certification Service Providers issuing (qualified) certificates (with reference of Article 3.5 presumed compliance with Annex II.f) and Secure Signature Creation Devices (with reference of Article 3.5 presumed compliance with Annex III) through the referencing to respectively three "generally recognised standards" which are CEN Common Workshop Agreements (CWA) (i.e. CWA 14167-1:2003, CWA 14167-2:2003, CWA 14169:2002).

When considering those CWAs, one can consider that this business model has finally succeeded since both the market (i.e. the CSPs issuing QCs) and the Member States Supervisory Bodies are relying on those referenced deliverables and on the other standardisation deliverables that have been further developed around them and included by reference (either normative or informative). Indeed most of these CSPs issuing QCs, when not all, are using or are at least compliant with updated versions of the published generally recognised standards (CWA 14167 1-2, CWA 14169) and even more often to informatively or normatively referenced in those published standards (such as ETSI TS 101 456, ETSI TS 101 862, ETSI 102 176-1/2). This is mainly because the Member States' administration in charge of supervising their national certification services issuing QCs have organised their supervision criteria on the basis of those CEN and ETSI standards, notably through their participation to the Article 9 Committee and through the Forum of European Supervisory Authorities for Electronic Signatures (FESA).

However even if *based* on the CEN and ETSI current standards organised around the generally recognised standards, the effective criteria used by national supervision systems can significantly differ from one Member State to another. There are of course criteria that are common to all supervision systems but there is no ***reference*** set of criteria and no ***reference*** set of conformity assessment guidance with regards to these criteria on the basis of which supervision criteria could be based.

This lack of reference sets is actually not a real issue under the current legal framework of Directive 1999/93/EC, in the specific area of CSPs issuing QCs since Member States are free to decide how they ensure the supervision of compliance with the provisions laid down in this Directive.

Nevertheless, for reasons explained in section 3.1, i.e. to facilitate trust of those services throughout the EU and to serve as reference:

- for Member States not yet having a supervision system in place and willing to establish one (including for CSPs issuing QCs);
- for negotiation of bilateral or multilateral recognition agreements between the Community and third countries or international organisation for the recognition of the legal equivalence of certificates issued by third country CSPs as qualified certificates [1, Art. 7.2];
- for a Member State assessing its own existing supervision system, when applicable;
- to all Member States with regards to the supervision of CSP not issuing QC but providing services ancillary to electronic signatures, allowing a sound basis for an improved interoperability, cross-border usage and mutual recognition of such services within the Community and towards third countries or international organisations;

[16] Directive 1999/93/EC, Article 2.12: 'electronic-signature product' means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures.

The establishment of a **reference set of supervision criteria** could be valuable to support the interoperability and cross-border use of electronic signatures.

However, the establishment of such a **reference set of supervision criteria** cannot be envisaged without taking into consideration the whole set of improvements required with regards to the Legal, Technical, Trust frameworks and the mapping mechanisms and measures implemented between them. This is further illustrated in Figure 3 below:

- The CROBIES team **recommends extending the scope of the EU legal electronic signature framework to integrate specific requirements on the provision of certification services ancillary to electronic signatures**. Directive 1999/93/EC, and in particular its general principles, applies to all types of certification service providers and to certification services ancillary to electronic signatures [1, Art. 2.11, recital (9)]. However its detailed requirements and annexes focus on one specific type of CSP, the one issuing QCs. This lack of detailed requirements for other types of certification services ancillary to electronic signatures has lead some Member States to establish national laws and regulations on the provision of such services. E.g. Italy, Germany and Hungary have national laws on the provision of time-stamping services in particular when supporting (qualified) electronic signatures. Divergences in such national laws may rapidly create new barriers to the interoperable and cross-border use of electronic signatures: to have a long term electronic signatures equivalent to hand written signature valid in the Union, it may be required to implement as many time-stamp tokens as there are divergent national regulations in the EU. Establishing a common framework for legal requirements applicable to all types of certification services would be an essential action with regards to the facilitation of the interoperability and cross-border use of electronic signatures beyond QES and $AdES_{QC}$. Similarly defining levels of advanced electronic signatures and associated certification security/quality/policy levels for supporting digital certificates is equally important. The identification and definition of the certification services, their component services and the associated categorisation in terms of security/quality/policy levels would be a critical starting point for establishing a common framework for legal requirements for those services. The legal effect and value of the resulting certification services outputs should also be carefully defined and clarified.

- The CROBIES team furthermore **recommends extending the scope of the EU legal electronic signature framework to achieving a better mapping** between the legal requirements of the framework (also extended to all eSignature products/services categories) and the rationalised eSignature standardisation framework. This includes **updating Decision 2003/511/EC.**

- **The existing European eSignature standardisation framework should be improved and rationalised**: The current state of the European standardisation on eSignature relates to the legal requirements of the Directive and stems from the EESSI, the *European Electronic Signature Standardization Initiative* [4],[5]. It also covers ancillary services to eSignature. The 2007 study on the standardisation aspects of eSignature [2] concluded that the current multiplicity of standardisation deliverables together with the lack of usage guidelines, the difficulty of access and lack of business orientation is detrimental to the interoperability of eSignature, and formulated a number of recommendations to mitigate this. Furthermore, the fact that EESSI ended its activities immediately after the publication of its work did not contribute towards the take-up of the existing standardisation deliverables by the industry. A new mandate M460 [6] has been issued to the ESOs aiming to update the

existing European eSignature standardisation deliverables[17] in order to create a **rationalised eSignature standardisation framework**. Such a rationalisation supports the realisation of the items of the Action Plan COM(2008)798 *on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market* [7]. This mandate should result in structuring the existing and to-be-developed standardisation deliverables according to a simple and straightforward numbering of four standards series covering respectively (i) CSP certification services issuing digital certificates (qualified and non-qualified), (ii) SSCDs, (iii) creation/verification of electronic signatures, and (iv) Certification services other than issuing digital certificates. This shall reflect the new architecture of the European eSignature standardisation framework to be structured per eSignature product/service categories and providing the associated technical/policy requirements and specifications, the related Conformity Assessment Guidance (CAG), and the implementation guidelines.

- In the context of the rationalisation of the eSignature standards, standardisation deliverables should be structured into four European Electronic Signature Standards (EESS) series from which **reference supervision criteria** as well as the **reference Conformity Assessment Guidance** should be derived and standardised.

Reference supervision criteria in line with eSignature frameworks review

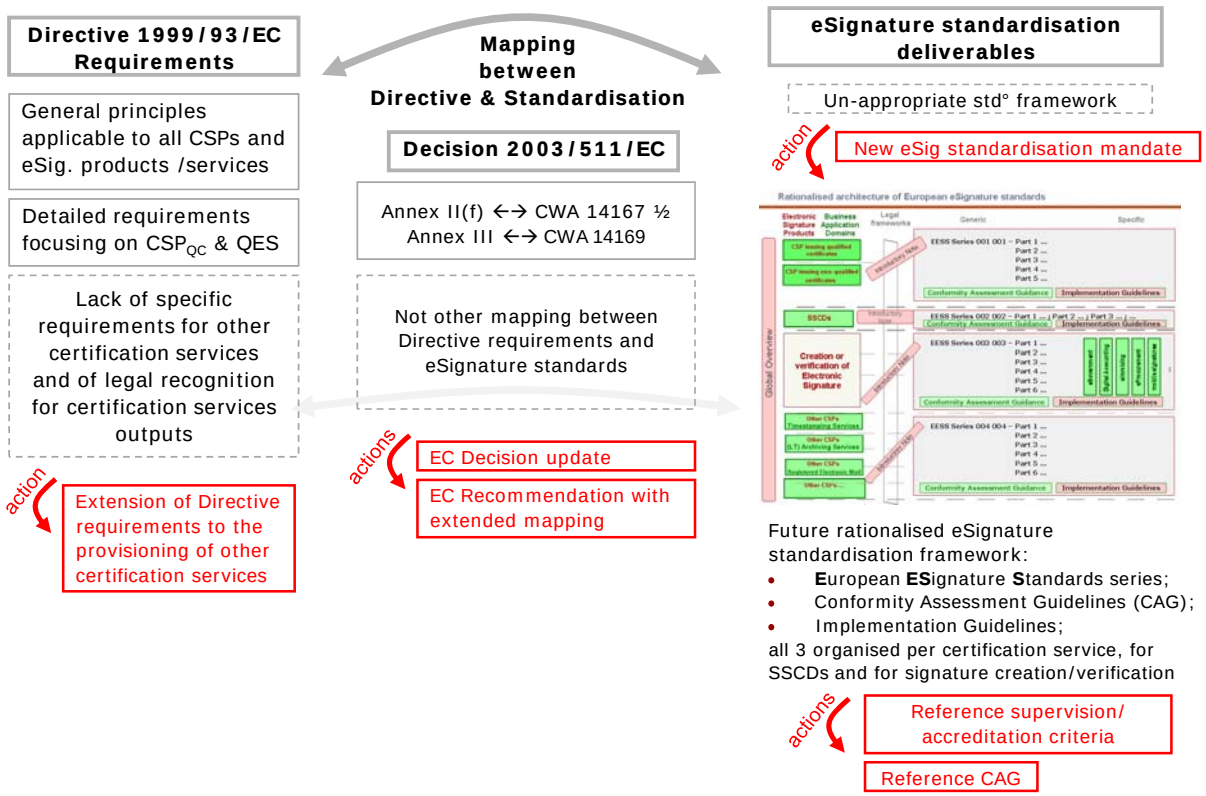


Figure 2

[17] The expression **standardisation deliverable** is used in this document as a generic reference to standardisation documents, be they established standards such as official EN or ISO norms, or less formal consensus specifications such as CWA, TS, TR or Request for Comments (RFC).

The **reference supervision criteria** and the **reference Conformity Assessment Guidelines** should be derived from the results of the above-described actions and they should also become part of the rationalised standardisation framework. They should be implemented and organised in such a way that they can provide a real alternative to non-European evaluation schemes like for example "WebTrust for CA" in the context of certification services issuing digital certificates.

Member States would then be free to choose but it would be recommended to adapt or establish their own supervision model around those standardised reference criteria and conformity assessment guidance as a common minimum set of requirements.

Moreover, Member States' national Trusted List of supervised/accredited CSPs, established in compliance to the common template defined in Commission Decision 2009/767/EC, allows Member States not only to provide information on the supervision/accreditation status of CSPs issuing QCs (mandatory part of the Trusted Lists) but also to provide, on a voluntary basis, supervision/accreditation status information about any other type of certification service from CSPs provided a supervision / voluntary accreditation scheme is established under their jurisdiction.

4.2.2 Accreditation Criteria

With regards to the assessment of compliance with the provision laid down in Directive 1999/93/EC for CSP issuing QCs, accreditation criteria will be equivalent to supervision criteria in the sense that supervision must already ensure such a compliance of the supervised certification service issuing QCs.

Supervision and accreditation schemes are unlikely to differ on those compliance criteria rather, they will diverge on the expected level of service provision in terms of higher/lower levels of trust, security and quality that would be demanded by the market from some accredited services. The enhanced/inferior levels of trust, security and quality can be materialised in one of both of the following tracks:

- Higher/lower trust, security and/or quality levels to be reached on a per criteria basis, when applicable and relevant (on top of the intrinsic compliance criteria common to the supervision scheme);

- Higher/lower targets with regards to the assessment process features, namely the frequency of the assessment, the depth and guidance rules of the controls.

Similarly to 'reference supervision criteria', 'reference accreditation criteria' are recommended to be derived from the rationalised European eSignatures standardisation framework mentioned above.

4.2.3 Summary

Reference supervision/accreditation criteria are recommended to be provided under the form of a check-list allowing a certification service provider to perform a self-assessment with regards to the compliance of their certification services with supervision/accreditation criteria.

The establishment of a **reference set of supervision criteria** for compliance of certification services (e.g. issuing QCs) with provisions laid down in Directive 1999/93/EC should take into consideration the whole set of improvements required with regards to the Legal,

Technical/Standardisation, and Trust frameworks as well as the efficient mapping between them:

- ***Legal framework***: Extension of the existing EU eSignature legal framework in order to integrate specific requirements on the provision of certification services other than those of issuing qualified certificates but ancillary to electronic signatures;

- ***Technical/Standardisation framework***: Realisation of a rationalised eSignature standardisation framework around
  - **E**uropean **E**lectronic **S**ignature **S**tandards (EESS) series;
  - Conformity Assessment Guidelines (CAG);
  - Implementation Guidelines;

  all three organised for each certification service type, for SSCDs and for signature creation/verification.

- ***Trust framework***: A common template for Member States' national Trusted Lists of supervised/accredited CSP covering, as per CD 2009/767/EC, all types of certification services ancillary to electronic signatures.

- An improved ***formal mapping*** between an extendedEU legal eSignature framework (including extended legal requirements for CSPs) on the one side and eSignature standards on the other side. This would include the update of Decision 2003/511/EC.

The **reference supervision/accreditation compliance criteria** and the **reference Conformity Assessment Guidance** should be derived from and standardised in accordance with the results of those above described actions and in particular from and as part of the rationalised standardisation framework in the context of mandate M460. These two documents should be public and should be implemented and organised in a way providing an alternative to similar non-European evaluation schemes like for example "WebTrust for CA" for digital certificates.

4.3 Supervision and Accreditation processes

4.3.1 Evaluators/Auditors designation process and evaluation/audit guidance

Member States may decide how they ensure the supervision of compliance with the provisions laid down in Directive 1999/93/EC. The Directive does not preclude the establishment of private-sector-based supervision systems [1, recital (13)]. Some Member States rely on evaluators/auditors from their internal staff while others rely on externalisation using one of the two following designation models:

- Evaluation and respectively audits are performed by own personnel of the Supervisory Body and Accreditation Body.

- Supervisory Body and/or Accreditation Body relies on external evaluators/auditors to perform the effective evaluation/audits.

The proposed common supervision/accreditation model allows for both designation modes. In both modes however, the rules and criteria to determine whether an evaluator/auditor should be designated should be established on the basis of best practices and international standards. The proposed common supervision/accreditation model recommends that rules and guidance for the performance of evaluation and audit should be established on the basis

of best practices and international standards like e.g. ISO 19011[18] setting forth guidelines for quality management systems auditing, the relevant ISO 17000[19] series of standards and guides, the harmonised EN 45000[20] series of European standards for the accreditation of certification bodies, and/or more specifically with regards to evaluation of CSPs issuing QCs, the relevant parts of CWA 14172 series[21] and ETSI TR 102 437[22].

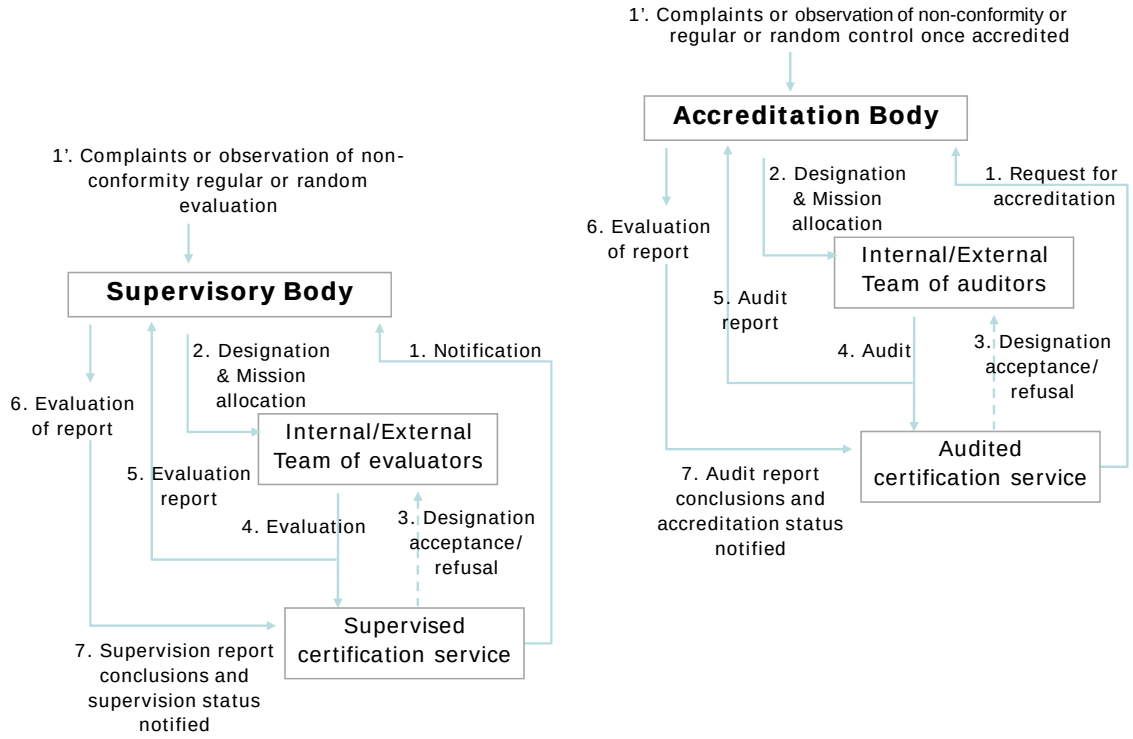
It is recommended that the previously identified action aiming to establish a reference Conformity Assessment Guidance as part of the rationalisation of the eSignature standardisation framework should take into account and cover rules and guidance for the designation of evaluators/auditors and for the execution of the evaluation/audits.

4.3.2 Evaluation/Audit process flow

Irrespective of the use of internal or external evaluators/auditors, it is expected that the supervision/accreditation shall remain under the final control, authority and responsibility of the Member State Supervisory/Accreditation Body.

Typically, the supervision/accreditation process flow in place in most of the Member States in which a supervision/accreditation system is in place with regards to Directive 1999/93/EC and which is recommended as part of the proposed common supervision/accreditation model can be depicted as follows:

Evaluation/Audit process flow for the common supervision/accreditation model of CSPs



[18] ISO 19011: Guidelines for Quality and/or Environmental Management Systems Auditing.
[19] ISO 17000 series: Conformity assessment -- Vocabulary and general principles.
[20] EN 45000 series for the accreditation of certification bodies.
[21] CWA 14172 series: EESSI Conformity Assessment Guidance.
[22] ETSI TR 102 437 : Electronic Signatures and Infrastructures (ESI): Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)

Figure 3

1. Initiation: The process is initiated either through respectively a notification for supervision or a request for accreditation. Additionally, the evaluation/audit process can be triggered once the certification service being under supervision or accredited, either from a complaint, from an observation of non-conformity, on a random or regular basis by the Accreditation/Supervisory Body respectively (step 1' in Figure 4 below).

2. The next step consists in the designation of internal or external team of evaluators/auditors. It is however recommended that the common supervision/accreditation model will require the (active or passive) participation of a member of the Supervisory/Accreditation Body in the team of evaluators/auditors.

3. The controlled certification service should be authorised to accept or reject, with motivated reasons, the whole or part of the team of evaluators/auditors. In this latter case the Supervisory/Accreditation Body should propose the partial or complete replacement of the team.

4. The team of evaluators/auditors performs the evaluation/audit

5. The evaluation/audit report is provided to the Supervisory/Accreditation Body

6. The evaluation/audit report is evaluated by the Supervisory/Accreditation Body

7. Conclusions and potential recommendations and/or requests for corrective actions are communicated to the evaluated/audited certification service for implementation.

Once the certification service is either under supervision or accredited, it enters in a mode that allows the Supervisory/Accreditation Body to perform additional and/or successive controls as part of the "maintenance" of the supervision/accreditation process, on a random basis, on a regular basis or as triggered by complaints or notification of changes in certification service by the CSP.

The evaluation/audit conclusions can be of three natures:

- Passed: the evaluated/audited certification service is "under supervision" mode or respectively "accredited" and is granted to act accordingly.

- Failed without possible or implemented correction: then, in accordance with the national provisions, the certification service is required to be ceased, or it does not benefit from a qualified status, respectively an accredited status.

- Failed with possible implementation of corrections: Successful evaluation /accreditation status is conditioned to the implementation of corrective actions within a determined delay in function of the type and criticality of the correction(s).

When applicable, the Supervisory/Accreditation Body notify the European Commission (according to Directive 1999/93/EC [1, Art. 11] and/or Decision 2009/767/EC) and update its national Trusted List.

The recommendations expressed here are without prejudice to the Member State's Supervisory/Accreditation Body to rely on private-sector-based schemes.

4.3.3 Evaluation/Audit process features

4.3.3.1 Frequency

The frequency of supervision/accreditation regular controls varies from Member State to Member State between every year and every three years.

Additionally, an evaluation or audit control may be triggered whenever:

- A significant change in the certification practices requires, for whatever reason, to reconsider the supervision and/or accreditation status;
- A complaint is made about a non-conformity about a supervised/accredited certification service; or
- An observation of non-conformity is made about a supervised/accredited certification service.

The proposed common model for supervision/accreditation systems recommends that:

- A CSP issuing QCs self-assessment should submit annually to the relevant Member State administration;
- The frequency for evaluation/audit controls should preferably be annual or at least not exceed a three-year frequency;
- Additional evaluation or audit controls should be triggered for reasons the reasons listed above.

4.3.3.2 Depth

The proposed common model for supervision/accreditation systems recommends that accreditation audits should be organised as deep as necessary for each and every criteria that must be controlled according to the accreditation criteria and model.

The supervision controls are recommended:

- to be oriented primarily on those criteria for which the self-assessment provided by the CSP at initiation step for supervision or accreditation process indicates failure to comply or partial compliance with the corresponding criteria;
- to be selected on a the basis of a sampling method for the remaining criteria

4.3.3.3 Fees

The proposed common model recommends that determination of fees, when applicable, for supervision and accreditation controls be left open to the Member States. However supervision fees, when applicable, cannot be such that they could be considered as a "prior authorization" to the provisioning of certification services, where "*prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect*" [1, recital (10)].

4.3.3.4 Complaints procedures

The proposed common model recommends that complaints procedures be made publicly available by Member States Supervisory/Accreditation Bodies and appropriately processed both for market entities to complain against non-conformity of certification service(s) from supervised/accredited CSPs and for supervised/accredited CSPs with regards to issues related to the supervision/accreditation of one or several of its certification services.

4.3.4 Responsibilities and liabilities

The proposed common model recommends that clear determination of responsibilities and liabilities for each and every participant to the supervision/accreditation model for supervision/accreditation of certification services. This includes e.g. the Supervisory and Accreditation Bodies, the evaluated/audited certification service provider, the members of the team of evaluators/auditors.

National rules regarding liability should apply to all those participants, including certification-service-providers providing certification services to the public.

5 Conclusions and recommendations

The proposed common model for supervision/accreditation systems outlined in the present report relies on the implementation of a set of improvements required with regards to the Legal, Technical/Standardisation, and Trust frameworks as well as the realisation of an efficient mapping between them:

- ***Legal framework***: extension of the existing EU eSignature legal framework , in order to integrate specific requirements on certification services other than issuing qualified certificates but ancillary to electronic signatures;

- ***Technical/Standardisation framework***: Realisation of a rationalised eSignature standardisation framework around
  - **E**uropean **ES**ignature **S**tandards series;
  - Conformity Assessment Guidance (CAG);
  - Implementation Guidelines;

  all three organised for each certification service type, for SSCDs and for signature creation/verification.

- ***Trust framework***: The common template for Member States' national Trusted Lists of supervised/accredited CSP [9] covers all types of certification services ancillary to electronic signatures.

- An improved ***formal mapping*** between an EU eSignature legal framework extended to cover the legal requirements for CSPs ancillary to electronic signatures on the one side and standardisation deliverables on the other side (e.g. through an update of Commission Decision 2003/511/EC) for achieving a more complete, efficient and consistent mapping between Directive 1999/93/EC (and its potential extension) and the rationalised EU eSignature standardisation framework resulting from the execution of mandate M460 [6].

The **reference supervision/accreditation criteria** and the **reference Conformity Assessment Guidance** should be derived from and standardised on the basis of the results of those above described actions and in particular from and as part of the rationalised standardisation framework effort in executing mandate M460 [6]. Those two references should be implemented and organised in such a way that they can provide a real alternative

to similar non-European evaluation schemes like for example “WebTrust for CA” in the context of certification services issuing digital certificates.

Despite the fact that MS have the freedom to decide what they consider to be an appropriate supervision under Directive 1999/93/EC [1] for CSPs issuing QCs, creating a reference model for supervision (and hence for accreditation) of CSPs, whatever the type of services they provide, could have a **significant positive impact**, in particular for other services than issuing QCs, on the interoperable, cross-border use and mutual recognition of those services and hence electronic signatures supported by such services[23], namely:

- With regards to CSP not issuing QCs but providing services ancillary to electronic signatures a common model for supervision (respectively ‘voluntary accreditation’) relying on a common set of standardisation deliverables would be a sound basis for an improved interoperability, cross-border usage and mutual recognition of such services within the Community and towards third countries or international organisations;

- With regards to CSP issuing QCs, such a common model would serve as reference for Member States not yet having a supervision or accreditation system in place and willing to establish one (e.g. because no CSP issuing QC is active yet on their market, or because those countries are new comers in the EU Community)

- With regards to CSP issuing QCs, such a common model would serve as a reference model for negotiation of bilateral or multilateral recognition agreements between the Community and third countries or international organisation for the recognition of the legal equivalence of certificates issued by third country CSPs as qualified certificates

- With regards to CSP issuing QCs, such a common model could serve as a reference model for a Member State assessing its own existing supervision (or respectively ‘voluntary accreditation’) system, when applicable.

The proposed common model for supervision/accreditation of CSPs is without prejudice for a Member State to raise the level of some requirements or increasing the level of identified specifications for whatever general or specific application domain purposes. However by doing so Member States should take into account the potential barriers, positive or negative consequences or differences this may create for their own national supervised/accredited services.

It is **recommended** that the establishment of a common model for supervision and accreditation systems shall be taken into consideration by the Member States and in particular the Member States supervisory and accreditation bodies on the basis of the model proposed by this report. It is suggested that the Forum of European Supervisory Bodies (FESA) becomes an active organ and an effective representation of supervisory and accreditation bodies from at least all Member States. It is suggested that FESA Members will, if they decide such a goal would be desirable, to set-up a working group contributing actively on this work item and actively participating or at least liaising with ESO’s in the context of mandate M460 and its relevant working items.

[23] Note that the impact of such a model would obviously differ depending on a service.