Study on Cross-Border Interoperability of eSignatures

(CROBIES)

Framework for Interoperable Secure Signature Creation Devices

A report to the European Commission from SEALED, time.lex and Siemens

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.

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
sylvie.lacroix@sealed.be, olivier.delos@sealed.be

Date: 29/03/2010
Version: 1.0

Document information

Title:	CROBIES Work Package 4 **Framework for Interoperable** **Secure Signature Creation Devices**
Project reference:	CROBIES
Document archival code:	INFSO-CROBIES-DFC-WP4-SEALED-29032010_v1.0

Version control

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

Definitions and Acronyms

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

References

Reference	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]	Commission Decision 2000/709/EC of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (notified under document number C(2000) 3179) (Text with EEA relevance)
[5]	CWA 14169: secure signature-creation devices. NB. The version of CWA 14169 from 2004 supersedes the version from March 2002. Nevertheless CD 20033/511/EC refers to the 2002 version. Where applicable, the present document precise the version it refers to.
[6]	FESA letter, dated 2008-06-24 to the European Commission on Generally Recognised Standards for Electronic Signature Products in accordance with the eSignature Directive [1].
[7]	FESA Public Statement on Server Based Signature Services – 20051027.
[8]	CWA 14355 (March 2004 – superseding CWA 15355 March 2002): Guidelines for the implementation of Secure Signature-Creation Devices.
[9]	CWA 14890 (EN), "Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements, Part 2: Additional Services.
[10]	CWA 14170, "Security Requirements for Signature Creation Applications".
[11]	ETSI TS 102 176-1 "Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms"
[12]	ETSI TS 102 176-2: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature

	creation devices"
[13]	CWA 14172-5 2004 EESSI conformity assessment guidance - part 5 : secure signature creation devices
[14]	BSI Technical Guideline TR-03110 "Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) Version 2.01.
[15]	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.
[16]	Common Criteria for Information Technology Security Evaluation (multi-parts 1/3). Current version is version 3.1, July 2009. The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA).See http://www.commoncriteriaportal.org/.
[17]	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.
[18]	CWA 14167 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures.

Table of Contents

1 INTRODUCTION 4

2 EXECUTIVE SUMMARY 4

3 THE LEGAL FRAMEWORK AND ASSOCIATED BUSINESS MODEL 9

3.1 THE LEGAL FRAMEWORK 9
3.2 THE SSCD CONFORMITY ASSESSMENT "BUSINESS MODEL" 10

4 INTEROPERABILITY ISSUES 12

4.1 LEGAL UNCERTAINTIES AROUND CONFORMITY ASSESSMENTS 12
4.1.1 Problem statement 12
4.1.2 Different degrees of legal certainty 13
4.1.3 Implications on SSCD cross-border recognition 17
4.2 TRUST IN THE SSCD'S CONFORMITY ASSESSMENT PROCESSES 21
4.3 LEGAL UNCERTAINTY OF GENERALLY RECOGNISED STANDARDS 23
4.4 POTENTIAL LEGAL DISCREPANCIES IN MEMBER STATES 25
4.5 NO LEGAL OBLIGATION BEYOND SSCD'S BOUNDARIES 25
4.6 THE STANDARDISATION FRAMEWORK RELATED ISSUES 28
4.6.1 The Standardization framework 28
4.6.2 CWA 14169 issues 29
4.6.3 CWA 14169 up-date 38
4.6.4 Conformity assessment guidelines issues 39

5 SYNTHESIS ON THE CURRENT LANDSCAPE 40

5.1 SSCD CROSS-BORDER RECOGNITION 40
5.2 STANDARDISATION FRAMEWORK SUSTAINING TECHNICAL INTEROPERABILITY OF (DIFFERENT TYPES) OF SSCDS AND GUARANTEEING CROSS-BORDER RECOGNITION 41

6 FRAMEWORKS IMPROVEMENTS FOR INTEROPERATION OF SSCDS 42

6.1 INTRODUCTION 42
6.2 THE LEGAL FRAMEWORK IMPROVEMENTS 43
6.3 THE TRUST FRAMEWORK IMPROVEMENTS 46
6.4 THE STANDARDIZATION FRAMEWORK CLARIFICATION AND ENHANCEMENT 49
6.5 STEPWISE APPROACH TO REACH THE PROPOSED OBJECTIVES 52

Framework for interoperable SSCDs

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.

The CROBIES Study concentrates in particular on the following aspects through related work packages and their associated reports:

WP1. The proposal for a common model for supervision and accreditation systems of certification service providers (CSPs) issuing QCs (and other services ancillary to electronic signatures);

WP2. The establishment of a "Trusted List of supervised/accredited Certification Service Providers" (in particular issuing QCs);

WP3. Interoperable profiles of qualified certificates issued by supervised/accredited CSPs in Member States;

WP4. A proposed framework for interoperable Secure Signature Creation Devices (SSCDs); and

WP5. A proposed model for providing guidelines and guidance for cross-border and interoperable implementation of electronic signatures.

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] which aims at facilitating the provision of cross-border public services in an electronic environment. Readers are suggested to read this Head Document prior to reading the present report.

1 Introduction

The present Work Package 4 report of the CROBIES study analyses the framework **for interoperable Secure Signature Creation Devices (SSCDs)** establishing what should be the ideal context for interoperable SSCDs, that should be based on the legal framework, the existing standards, protection profile, ISO 15408's Common Criteria certification model, in coherence with the findings of the other Work Packages of the CROBIES study.

2 Executive Summary

SSCDs in the global context of eSignatures

As they are defined and ruled by Directive 1999/93/EC *on a Community Framework for Electronic Signatures*, the use of SSCDs is mainly relevant in the support of the creation of Advanced Electronic Signatures which are based on a qualified certificate (hereafter $AdES_{QC}$) leading to the implementation of electronic signatures that meet the requirements of

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

Art. 5.1 (hereafter Qualified Electronic Signatures or QES), deemed to be equivalent to handwritten signatures. In this context, SSCDs are most of the time provided jointly with qualified certificates (QC) by Certification Service Providers (CSP) issuing such QC. The content of these QC should clearly indicate the fact that they are certifying a public key (signature verification data) associated to a private key (signature creation data) that is protected and managed by an SSCD which complies with provisions laid down in Directive 1999/93/EC and in particular its Annex III on SSCDs. In order to facilitate the validation and usage of interoperable and cross-border QES, the common profile for QC should contain a clear machine readable statement claiming that the private key associated with the public key in the certificate resides within an SSCD (see CROBIES WP3 for further details) and when QC from supervised/accredited certification services are lacking such information, Trusted Lists for supervised/accredited certification service providers[2] shall, indicate whether or not those QC are delivered to a public key associated with a private key residing in an SSCD. Such claims are deemed to be guaranteed by CSPs issuing QCs and supervised/accredited by Member States' relevant supervisory/accreditation bodies.

As a consequence, in the context of validation of QES, it is likely to be the case that relying parties do not need to validate the fact that the signature has been created by an SSCD beyond the validation of the certificate itself and/or the associated Trusted List, given that the certificate itself should already indicate conclusively if an SSCD was in fact used.

However, there might be cases where the SSCD status of a signature creation device has to be validated independently of the validation of a qualified certificate (e.g. when a signatory wishes to acquire a device such as a HSM to support its (non)qualified certificate independently of the provision of the certificate by the CSP). For those cases, and for CSPs for which SSCD status validation remains a crucial obligation it is necessary to have an interoperable Secure Signature Creation Devices (SSCDs) framework enabling a mutual recognition of SSCDs on a European level.

Problem statement

Directive 1999/93/EC [1], in its article 2.6, defines an SSCD as "*a signature-creation device which meets the requirements laid down in Annex III*".

This Directive also states that conformity assessments can be positively provided by appropriate (i.e. complying with the provisions of Decision 2000/709/EC [4]) public or private bodies designated by Member States (hereafter Designated Bodies or DBs). Such a determination of conformity by a DB of an SSCD with the requirements laid down in Annex III of [1] shall be recognised by all Member States.

Additionally the European Commission has published as Generally Recognized Standard in Decision 2003/511/EC [3] the reference to Protection Profiles (PP) of the CEN Workshop Agreement (CWA) 14169 (version dated 2002), which provide "*presumption of compliance to Annex III"* to devices meeting (or evaluated conform to) one of these PPs.

However, as analysed in the present WP4, two linked issues impede cross-border recognition of SSCD:

- the cross-border recognition of SSCD's conformity assessments,

[2] 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.

- the way SSCD's boundaries are considered in the evaluation of SSCD may result in ambiguity about the scope of the conformity assessments.

The tools one can rely upon in order to tackle these issues, i.e. the legal framework and the standards, disserve enhancements.

Legal value of SSCD conformity assessments

There are three legal issues impeding the cross-border recognition of SSCD's conformity assessments:

1. What is the legal value of a self-declaration or any other type of compliance assessment that is not delivered by a DB? Nothing in Directive 1999/93/EC [1] prevents a self-declaration of conformity by the SSCD provider, or indicates that these should have no legal value. However, some Member State legislations only recognise determination of conformity made by a Designated Body, and this does not appear to be an infringement of the European legal framework established by the eSignatures Directive [1]: the relevant provisions of the Directive are ambiguous, and can certainly be interpreted as requiring formal conformity assessments by a DB before a signature creation device can be considered an SSCD. *(Note however that at least one MS does not recognize peer DBs without a mutual assessment, which seems to be contrary to the spirit and possibly the letter of the Directive, and which harms interoperability).*

2. There is no obligation for a Member State to set-up a Designated Body and nothing obliges existing Designated Bodies to publish lists of SSCDs. As a result:

- many Member States do not have a Designated Body and rely on their peers, but as nothing obliges DBs to publish lists of SSCDs it is difficult for peers and relying parties to verify the status of a particular device;

- SSCD lists (templates) are not harmonised, when they exist.

3. The status of any kind of "certification" against Protection Profiles (PP) is uncertain:

- If not approved by a Designated Body, a certificate of conformity (or its legal value) may be questioned. International mutual recognition agreements on certification help a lot but they do not all[3] tackle the SSCD issue and not all Member States are participating to such agreements. Therefore, at present these mutual recognition agreements do not provide a conclusive answer to an international (or at least European) recognition of SSCD certification against a PP should even it be published as a generally recognised standard in [3].

- The CWA 14169:2002 mentioned in decision 2003/511/EC [3] is perceived as out-dated (a 2004 more recent version exists and in theory CWAs are valid for 3 years with one possible renewal for 3 years), and in addition this 2002 document is not correct[4]. The issues on the content lie in a number of small errors found after the

[3] Only Common Criteria specifically addresses SSCDs with ad-hoc PPs, but unfortunately the CCRA agreement [16] seems not covering the EAL4+ level characterising these PPs. Only the SOGIS MRA appears to cover these Common Criteria PPs.

[4] One shall note that the CEN is well aware of the issues discussed in this study and already started to consider updating CWA 14169 towards a European Norm (EN). This work will be finalised in collaboration with the EC in the framework of the standardisation Mandate M460 on electronic signatures [15] and the possible up-date of Decision 2003/511/EC [3].

evaluation of the Protection Profiles according to the Common Criteria for Information technology Security Evaluation (CC) certification process [16]. The document has been up-dated accordingly (CWA14169, version 2004), but this superseding version, dated from 2004 is about to expire. In addition, both versions contain obsolete references. In order to circumvent the fact that the document mentioned in decision 2003/511/EC is out-dated, the CEN/ISSS Forum (as it then was) decided a long time ago that CEN will retain the relevant CWAs as publications as long as the Commission Decision applies. Unfortunately, this validity extension of version 2002 seems not having been "officialised" or published and hardly brings more legal certainty to the document; in particular it seems to apply to the 2004 version of the document (i.e. not referred under [3]), as this is the sole version published on the CEN portal, and if this decision applies to the 2002 version, this does not solve the issues on the content that lead to the revision of the document after its evaluation. What is the legal value of an assessment against an obsolete (but legally recognised) document or to an updated version but not referred to in [3] (knowing that a CC certification is only possible against the 2004 version of the document)? To a large extent, this is an open question, creating legal uncertainty.

➔ Immediate actions on up-date of both the PPs and Decision 2003/511/EC are strongly recommended, as well as longer term actions on clarification of the legal value of conformity assessments (while considering Member States existing legislations).

SSCD's boundaries consideration in the evaluation of the SSCD

SSCD is essentially the device handling the private key in such a way that Advanced eSignature (AdES) requirements are guaranteed. But SSCD is not always the sole element implied in the AdES creation. The following elements -not necessarily considered as part of the target of evaluation in the conformity assessment- must be considered as being in the immediate environment of the SSCD:

- the Secure Creation Application (SCA),
- the Human Interface (HI) for input of the signatory authentication data (SAD) or the display of data to be signed (DTBS)

The PP requires that the "SSCD allows" for the establishment of a Trusted path and a Trusted channel with these elements up to the signatory for secure transmission of SAD and DTBS, respectively.

These requirements represent strong constraints on elements in the immediate environment of the SSCD. However, there are no legal obligations on these elements (such as compulsory "certified as secure" SCA or "certified secure" device reader). In fact, recital 15 of the eSignatures Directive [1] explicitly indicates that Annex III "does not cover the entire system environment in which such devices operate". Moreover, except with the use of additional PP (e.g. similar to PACE [14] for RF devices), nothing prevents a signatory to use his SSCD in an insecure environment, and there is no way for an AdES verifier to have any clue on the quality of this environment.

➔ An up-date of CWA 14169 (if not otherwise specified hereafter, "CWA 14169" relates to the 2004 version) including additional PP(s) is strongly recommended, if it is considered that the links between the SSCD and its environment must be reinforced (but this should not lead to slowdown the market by adding unreachable requirements on the environment) and this should be tailored according to the signing environments.

Another consequence of CWA 14169 requirements is that, according to certain interpretations, they simply put aside devices other than smart-cards from being recognized as SSCD.

➔ An up-date of CWA 14169 through the addition of appropriate PP(s) is strongly recommended to also cater for the recognition of a broader range of SSCDs in order to be more in line with market expectations ([2]).

As a conclusion, the first stepwise realisations leading to a common interoperable framework for SSCDs seem to be (i) an agreement on the acceptable origin and type of conformity assessment of SSCD, (ii) the clarification on the status of recast generally recognised standards, as well as (iii) a common understanding on how to deal with the boundaries of an SSCD. This should be followed by the adoption of a common template for the publication of SSCD status information for signature creation devices.

3 The legal framework and associated business model

3.1 The legal framework

As per Directive 1999/93/EC [1; Art.2.4 to 2.6] a secure-signature-creation device (SSCD) means a "*configured software or hardware used to implement the signature-creation data* (i.e. "*unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature*") *which meets the requirements laid down in Annex III*". Annex III of the eSignature Directive covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures as follows [1]:

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

As stated in *recital (15)* of Directive 1999/93/EC [1], "*Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient*".

Article 3.4 of Directive 1999/93/EC [1] states that "*the conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated*". The Commission has, through Decision 2000/709/EC[5] [4], established criteria to which Member States must refer to determine how a body can be designated. According to this Decision [4], the designated bodies are free to establish conformity assessment according to

[5] Through Commission Decision 2000/709/EC of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (notified under document number C(2000) 3179) (Text with EEA relevance**)** (2000/709/EC) [4].

their own criteria but they must be transparent in their conformity assessment practices and are liable for their activities.

Furthermore, Article 3.4 of Directive 1999/93/EC [1] adds that "*a determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph* [those abovementioned bodies designated by Member States] *shall be recognised by all Member States*".

In addition, the Commission has, in accordance with the procedure laid down in Article 9, established and published reference numbers of generally recognised standards for electronic-signature products in the *Official Journal of the European Communities* through Commission Decision 2003/511/EC [3]. As per Article 3.5 of Directive 1999/93/EC [1], "*Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards*". For electronic signature products that Member States shall presume to be in compliance with the requirements laid down in Annex III to Directive 1999/93/EC, the generally recognised standard is CWA 14169 (March 2002): secure signature-creation devices [5].

3.2 The SSCD conformity assessment "business model"

As stated in the previous section, the main legal requirements ruling and driving trust in SSCDs are essentially based on:

- Directive 1999/93/EC [1], and in particular its recital (15), Art. 2.4 to 2.6, Art. 3.4, 3.5 and of course Annex III;

- Decision 2003/511/EC [3] referring to CWA 14169 as the generally recognised standard related to Annex III compliance; and

- Decision 2000/709/EC [4] on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3.4 of Directive 1999/93/EC.

These documents provide criteria on the basis of which compliance statements can be made. They are the following:

- Requirements given by Directive 1999/93/EC itself and in particular in its Annex III [1];

- Requirements from the associated generally recognised standard as published in Commission Decision 2003/511/EC [3], i.e. CWA 14169:2002 [5];

The first category fixes the basis level for meeting Directive 1999/93/EC requirements with regards to SSCD.

Excepting self-declaration, the finding of compliance against CWA 14169:2004 [5] (correcting version 2002) which actually is made of a set of three Common Criteria Certified Protection Profiles**,** generally takes the form of a Common Criteria

Certificate, which is also recognised under two international agreements, the Common Criteria Recognition Agreement (CCRA) [6] and the SOGIS MRA[7].

One can identify three potential tracks for SSCD recognition in function of the following **three types of compliance statements**:

- ***Declaration of compliance***: a signature creation device can be declared by its manufacturer as an SSCD on the mere basis that it complies with the requirements of Directive 1999/93/EC and specifically its Annex III, irrespective of whether any determination of conformity was made by a designated body, and irrespective of whether any statement is made on compliance with CWA 14169;

- ***Certification of compliance against CWA 14169***: a signature creation device can be certified as an SSCD on the basis that it was assessed to be compliant with CWA 14169, irrespective of whether this was assessed by a designated body;

- ***Determination of conformity by a Member State Designated Body***: a signature creation device can be considered an SSCD on the basis that it was determined to meet the requirements of Annex III of Directive 1999/93/EC by a Designated Body operating under the conditions established by its applicable law, which must meet the requirements of Commission Decision 2000/709/EC.

It is important at this stage to distinguish the roles of Designated Bodies and Certification Bodies. The Designated Body is liable for SSCD determination of conformity, and for this purpose, is responsible for the potential set-up of "determination of conformity schemes" conducting evaluation activities. One of the most obvious schemes is the certification process under which one or more

[6] The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA). See http://www.commoncriteriaportal.org/ for further information. Note that recast of CWA 14169:2004 PPs is likely to take into account the updates recently made in CC according to its newly published July 2009 3.1 version.
In the context of an international recognition of CC certificates, an arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of PPs based on the CC. As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org. The CCRA logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

[7] In the context of European recognition of ITSEC/CC certificates, the SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective on 03 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all Evaluation Assurance Levels (EAL 1 – EAL 7). The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

certification bodies are mandated to perform the assessment of the devices on behalf of the DB. The Designated Body may be a Certification Body itself, or it may delegate the certification process to another party. Certification Bodies under most of the schemes are dully-licensed laboratories.

To these three types of SSCD compliance statement, relying parties have two additional ways of obtaining an SSCD compliance statement, which are in fact variations of the three above mentioned scenarios:

- The SSCD status can be **derived from the certificates and/or from the supervision or accreditation status list of certification services having issued those qualified certificates.** For Qualified Certificate, the support of the certificate by an SSCD is ascertained either by a (machine readable) statement in the qualified certificate itself and by a confirmation of this support in the associated Trusted List [17]. In this case, the content of the certificate or of the Trusted List can be considered a form of declaration of compliance by the issuing CSP. In cases where the supervisory or accreditation body actually verifies or guarantees the status of an SSCD, the content of the Trusted List may be considered a declaration of compliance from that body.

- Secondly, it is possible that the status of an SSCD is disputed and becomes the subject of a court ruling at the national level, where the judgment ultimately confirms an SSCD conformity independently of the recognition track. In this case, the ruling itself (and the expert testimony on which the ruling would likely be based) could be considered a form of declaration of compliance that can no longer be disputed for that specific case outside of further legal proceedings. However, it should be noted that this option of a court ruling confirming the conformity is largely theoretical at this time, as no cases addressing this issue are known to us.

The main difference between each of these tracks for conformity assessment lies in the legal certainty that they offer, and thus in the burden of proof if they are disputed. As a consequence, the different ways of establishing compliance with the Directive and combination thereof may lead to different rates of acceptation as detailed below in section “Legal uncertainties around conformity assessments”.

4 Interoperability issues

4.1 Legal uncertainties around conformity assessments

4.1.1 **Problem statement**

Directive 1999/93/EC [1] is not very clear on ***whether SSCD conformity assessments are legally required*** and in particular, whether ***conformity assessment by a Designated Body is legally necessary or not***. The Directive says that a determination of conformity made by a Designated Body (DB) shall be recognised by all Member States (Art. 3.4). This provision results in the equivalence of conformity assessments performed by any DB: all Member States are required to accept the outcome of such an assessment as being valid, thus resulting in the unambiguous status of an SSCD within all of the Member States. However, this does not address the question of whether those assessments are a necessary precondition in order for a signature creation device to be accepted as an SSCD.

As there is no obligation for a Member State to have a Designated Body[8], besides the "automatic" recognition of SSCD whose conformity with Annex III of Directive 1999/93/EC is determined by designated bodies, it is not clear whether SSCD whose conformity with Annex III is established by *other entities* must/can be accepted/rejected, even in the case where this conformity with Annex III is made against generally recognised standards published in Commission Decision 2003/511/EC [3]. Depending on the ***origin of the conformity assessment,*** which kind of conformity declaration is thus acceptable? What would be the level of recognition of an SSCD certified by a third party (not being a designated body)? What would be the level of recognition of an SSCD whose conformity to Annex III of Directive [1] is self-claimed by the supplier? One can only say that it is likely to be the case that a conformity assessment against those generally recognised standards will have more chance to be recognised than a conformity assessment against other criteria, as per Article 3.5 of Directive 1999/93/EC [1]. In all cases, if a final judgment in Court confirms SSCD conformity to a device – independently of the recognition track –, this shall lead to a non deniable recognition. However, depending on the Court (local or European) and the nature of the judgement, the cross-border recognition may be limited in scope (e.g. to a certain country and/or product).

Due to the fact that there is no obligation for a Member State to have a Designated Body, it is hard to imagine that other sources of conformity declaration are not legally acceptable under Directive 1999/93/EC. However, the legal certainty of the declarations (i.e. the likelihood that the declarations will be upheld as meeting the legal requirements of the Directive) certainly differs depending on their source, with certain forms of declaration (e.g. self-declarations by the supplier) being noticeably more vulnerable to legal challenges than others (e.g. conformity findings by a DB). This issue is examined in the next section.

4.1.2 **Different degrees of legal certainty**

The strongest legal certainty is obviously afforded by a formal determination of conformity by a DB. As noted in Article 3.4 of the Directive, such determinations "shall be recognised by all Member States". This means that the only possibilities to

[8] Article 3.4 of Directive 1999/93/EC [1], states that "*The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. [...]*. Recital (15) states that: *[...]; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient"*. The Directive does not contain a direct obligation for each Member State to designate a suitable body. Art.3.4 indeed says that criteria should be established to determine if a body is suitable to act as a SSCD conformity assessment body (which was done through Decision 2000/709/EC of November 2000 [4]), but it does not contain an actual legal obligation to designate them. Similarly, recital (15) of the Directive indeed states that bodies must be designated, but it does not say that each Member State must do this; only that the Member States and the Commission have to act swiftly to make sure that suitable bodies are designated. Therefore, one can also read this as a "collective obligation", i.e. an obligation on the Member States and the Commission to ensure that suitable bodies are designated in at least one or some Member States; it is thus not necessary to designate a body in each Member State (which would be an individual obligation, as it is the case for instance with the supervision).

Since determinations of conformity are supposed to be valid across borders, a limited number of bodies would probably be enough to serve the needs of the EU market; one Designated Body would theoretically be sufficient. This is also the interpretation that Prof. Jos Dumortier presented in the ELSIGN study in 2004 (http://www.ec.europa.eu/idabc/servlets/Doc?id=29484) and which has never been disputed either by the Commission or by the Member States, so there seems to be some consensus on this point.

challenge such determinations (and thus the status of an SSCD) relate to material/procedural errors (e.g. the DB was provided with inaccurate information by the issuing CSP or misjudged this information) or to challenges of the legal framework itself (e.g. the DB does not meet the requirements of the Directive or of Decision 2000/709/EC). In either case, the burden of proof lies entirely with the party disputing the status of the SSCD.

In all other cases, no legal presumption of compliance exists, and general rules of evidence apply. While no recorded cases of such proceedings appear to be available, in civil proceedings, the absence of legal presumptions means that it is up to a party making a claim to provide adequate evidence of that claim. If the status of an SSCD is challenged by the relying party and the signatory initiates legal proceedings, in the absence of a formal determination of conformity it will need to provide any other proof it may have, and the value of this proof will then be appreciated by the judge against applicable (national) law. In countries where a conformity finding by a DB is not formally required, a certification of compliance against CWA 14169 by a neutral body will likely be considered highly persuasive, although the judge is not bound by it and the opposing party may provide counterevidence showing that e.g. mistakes were made by the neutral body. Similarly, information included on the national trusted list in relation to the SSCD status will likely be considered authoritative (but not necessarily binding). A simple claim of conformity by the CSP (or indeed by the signatory itself) will in that respect also be admissible, but will likely have only a limited evidentiary weight. At any rate, the judge will need to motivate his or her decision, indicating why the proof was considered as adequate or inadequate to meet the requirements of national law.

In case of contrary evidences (e.g. the signatory relies on a claim of conformity by the CSP which is only briefly substantiated, while the relying party disputes this on the basis of similar arguments from its security experts), the judge will likely appoint an expert to weigh the arguments against the requirements of the Directive to make his ruling. Thus, in the absence of formal determinations of conformity by a DB, legal uncertainties exist and each party carries the burden of the proof for the claims that it makes; neither can benefit from any presumption.

Obviously, and as noted above, this only applies in cases where the national law doesn't explicitly require formal determinations of conformity by a competent DB; if a determination from a DB is legally required, then the parties only need to show whether or not this determination is available, or alternatively they can request the local court to seek a preliminary ruling regarding the correctness of the local transposition of the eSignatures Directive from the European Court of Justice. So far, this has not happened.

As a matter of nuance, one could add that a ruling from a national court on the status of an SSCD may thereafter get force of precedent. Generally, common law systems attach a binding force of precedent to rulings of higher courts, meaning that the burden of proof would lie on the party not supported by the ruling to show why a new dispute on the same SSCD is different. Continental law systems generally do not recognise binding force of precedent (with limited exceptions which differ from country to country), and will typically consider earlier rulings to be authoritative, but not binding. Thus, earlier rulings from a court on the status of an SSCD are certainly authoritative, but do not necessarily provide certainty or have any value in another jurisdiction (i.e. in another Member State).

As summarised in Figure 1 below, different levels obtained by combining the types of compliance statements with the categories of criteria will each give a certain level of

risk in the context of legal presumption of compliance and a level of risk with regards to the assurance of technical compliance. Indeed, meeting requirements from Annex III of Directive 1999/93/EC is enough to be recognised as an SSCD but this may be hard to prove by the SSCD supplier when not using specific criteria and/or a specific assessment methodology to support such a statement, while meeting compliance with requirements from the associated generally recognised standard as published in Commission Decision 2003/511/EC [3], i.e. CWA 14169 [5], gives according to Article 3.5 of Directive 1999/93/EC a legal presumption of compliance with the requirements of Annex III in the whole Community.

A certification by a third party gives of course some more credibility and basis for recognition in particular when such certifying parties are using recognised evaluation and assessment methodologies as those based on Common Criteria.

From a legal compliance perspective, the level of risk can be associated consequently as illustrated in Figure 1 below.

Type of compliance statement	Compliance criteria	Legal compliance risks
Self-declaration	Annex III of Directive 1999/93/EC	HIGH Compliance can be challenged, and may thereafter be hard to prove (by the signatory or its CSP or its device provider)
	Generally recognised standard	
Certification of compliance	Any certificate against standard, or any other technical doc., that can pretend to offer compliance with Annex III. Common Criteria certificate (certifying conformity to Generally recognised standard. Note here that only CWA14169:2004 is applicable for CC Certification)	MEDIUM Presumption of compliance according to art 3.5 of Directive 1999/93/EC where compliance is shown
Determination of conformity by a Designated Body	Annex III	LOW Recognition of compliance is ensured according to Article 3.4 of Directive 1999/93/EC and not cannot be challenged by third party[9] (liability for this statement is on the Designated Body)
	Generally recognised standard	
Supervision/Accreditation of certification services issuing qualified certificates	Member State's supervision/accreditation system	Presumption of compliance (liability for this statement is on the CSP, liability for controlling the CSP is on the Supervision/Accreditation body)

Figure 1: SSCD conformity assessment business model

As was noted above, qualified certificates should in principle contain statement on the SSCD status of the signature device as well; however, in the current state of play, it does not follow that the trusted lists managed by national supervisory bodies can be used as a conclusive way to resolve the question of whether a signature creation

[9] Except in relation to material/procedural errors or to challenges of the legal framework itself, as noted above.

device can be accepted as an SSCD across all Member States. This is due to the fact that Member States can freely determine the key characteristics which decide the meaning of the supervision/accreditation schemes, specifically the adoption of the terms of an appropriate supervision scheme (and voluntary accreditation schemes if desired), and any need to undergo formal SSCD assessment by a DB. As a result, the meaning of the SSCD status on a supervision body's trusted list may vary from one Member State to the next.

As an example, in Member State A the inclusion of a qualified certificate supported by an SSCD on a trusted list managed by the national supervisory body may simply mean that the CSP has declared that the signature creation device was certified as an SSCD by the supplier or by an independent laboratory (not a DB), whereas in Member State B this inclusion may mean that an SSCD has undergone formal assessment by a DB.

Thus, the supervision/accreditation schemes which are created and applied at the national level (and the resulting trusted lists) can only be interpreted as an affirmation that the signature creation device is considered to be an SSCD under national law, as verified under the rules of the national supervision/accreditation system. In contrast, it does not mean that this affirmation is legally indisputable across the EU. The SSCD status on a trusted list would only be valid across the EU if there would be a consensus on the exact requirement for a qualification as an SSCD (i.e. what type of assessment is needed). As long as there is no consensus on this question, the impact of the SSCD status as indicated in the trusted list is not conclusive.

For this reason, the supervision/accreditation of qualified certificates has been placed separately from the three other scenarios in the above table: while it *could* become a conclusive factor resulting in complete certainty on the SSCD status in the future if a consensus was reached on the type of assessment required under the Directive, this is presently not the case. Therefore, its value varies from country to country: in a highly flexible Member State that accepts self-declarations from the supplier, inclusion on a trusted list will likely be sufficient to recognise a device as an SSCD; in Member States with a rigid system (e.g. requiring determination by a DB) the inclusion on a trusted list is meaningless unless the relying party knows that the list was created in a Member State with a similar interpretation. Therefore, the legal impact of the supervision/accreditation scheme cannot be determined in general terms.

It should be emphasized that the above table is logical and sound, but may not directly be applied at the national level in all Member States. E.g. if a Member State has implemented regulations that clearly require a conformity determination from a designated body before an SSCD can be recognized as such, then the legal value of any other track (including the self-declaration and certificate options in the table above) is virtually non-existent within that country. Such a strict interpretation of the Directive cannot be a priori recognized as an infringement of art 3.4 of the Directive, since it is not explicitly contrary to it. Thus, the absence of a European consensus on the need for a formal conformity assessment by a DB has a strongly negative impact on the cross-border recognition of SSCDs: in the absence of such a consensus, Member States choose their own interpretations, leaving issuers of signature creation devices in legal uncertainty, as well as the end users and relying parties.

4.1.3 **Implications on SSCD cross-border recognition**

4.1.3.1 Designated Body according to the Directive, art 3.4

As previously stated, Member States are not required under Directive 1999/93/EC [1] to establish a Designated Body. However, even if one Designated Body would theoretically be sufficient to serve the needs of the eSignatures market, it is difficult to imagine that "one" Designated Body would agree to endorse alone the responsibilities of SSCD conformity determination for the whole of the Community, since that Body would then carry the responsibility (and liability) for the determination of conformity for a very large number of SSCDs. The practical barriers – in terms of manpower and resources required, in addition to insurance requirements to cover liabilities for all assessed devices – may be prohibitive to offer such services in a financially viable manner. The current situation is not that extreme, as at the moment of edition of the present document, twelve Member States do have a Designated Body, in the sense of Art 3.4 of the Directive. These bodies can be private or public, and for two countries there is more than one single Designated Body. It is worth to note that at least four (4) Member States (Belgium, France, Italy and Romania) explicitly state acceptance of attestations provided by Designated Bodies from foreign countries. Only a few of these Designated Bodies provide lists of SSCDs that are publicly available, such as Austria, France, Germany or Italy.

However, when a Designated Body determines that an SSCD conforms to Annex III of Directive 1999/93/EC, the procedure, form and consequences of such a determination are not fixed (e.g. does the Designated Body issue statements and/or list(s) of "approved" SSCD?). As a consequence, a Member State wishing to rely on another Member State to endorse the recognised SSCDs in that Member State might have no formal tool to do so (e.g. a published list of SSCDs for which a Designated Body have made a determination of conformity). **The issue today is** thus that consistency between the available lists and other relevant publication's sites is not straightforward. As an example, at the moment of writing of the present document, one can find seven (7) SSCDs conformity certificates listed on the French Designated Body website (DCSSI[10]), one of which is established against CC. On the CC portal, this product certificate cannot be found, although another product certified by the DCSSI – not listed on the French site – can be found. This highlights the difficulties for Relying Parties to find accurate information on SSCD status. Hopefully, no automated process such as the one required for eSignatures validation is required for SSCD, but this non-harmonisation of information remains an issue.

4.1.3.2 Various Member States' position regarding conformity assessments

The need for conformity assessments varies; not all Member States take the same position in relation to this issue. The purpose here is not an exhaustive legal review of each and every Member State's legislations, but rather the identification of **potential legal discrepancies** between Member States that might impede cross-border interoperability. Some countries have interpreted Directive 1999/93/EC very strictly by stating that SSCD conformity assessments by designated bodies are required, or otherwise they cannot consider a device to be an SSCD (e.g. Germany). Other Member States consider that no formal assessment is required to determine that an SSCD complies with Annex III (e.g. Belgium). These two examples are further illustrated below, knowing that the 27 Member States have positions between these two extremes.

[10] http://www.ssi.gouv.fr/site_documents/certifconforme/index.html

Germany: a strict interpretation example

The present illustration overviews the German Regulation on eSignatures, on the basis of the Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations and the Ordinance on Electronic Signatures.[11]

Foreign SSCDs are considered to be legally equivalent to SSCDs that have undergone a conformity assessment by a designated body in Germany, provided that it has been established in a MS or EEA country that they meet the requirements of the Directive [Sig G, section23, §3, first sentence].

SSCDs that have not undergone a formal conformity assessment by a designated by in Germany thus need to comply with the Directive, and with the provisions of the Ordinance, stating that:

> "The security of foreign electronic signatures shall be deemed equivalent […] if the competent authority has established that the security requirements for certification service providers and products for qualified electronic signatures, the evaluation modalities for certification service providers and products for qualified electronic signatures as well as the requirements for the evaluation and certification bodies […] offer equivalent security.
> In order to establish equivalent security, the competent authority may agree with the competent foreign body on the recognition procedures unless otherwise provided in bilateral or multilateral agreements".

The competent authority mentioned above is the Bundesnetzagentur. It seems that BNA practice is that equivalent security is not to be assessed on a per-case basis but regarding the whole system in one country. Equivalent (provable!) security could only be established by showing compliance with evaluation levels or something similar[12], so that in the end only a very similar system to the German one could probably be accepted without major difficulties (if only for formal reasons). I.e. Germany evaluates if a Designated Body's processes are equivalent to theirs (which is based on a two-step process explained below), and an SSCD's inclusion on a list then demonstrates that it has passed this process. This is a difficult system to apply in practice, because it does not scale well: if all Member States would act so, they would all need to establish their own processes, and then start determining if all other Member States' systems were equivalent. This difficulty may be alleviated by recognition arrangements provided in bilateral or multilateral agreements; SOGIS MRA or CCRA e.g. might be used for this purpose (see also next section "Trust in the SSCD's conformity assessment processes").

As noted above, equivalence is measured against the processes that the Ordinance requires for "German" SSCDs; i.e. in a 2 steps process:

---

[11] The authors thank M. Hajo Bickenbach for his collaboration in this section. The English version of these documents used for the elaboration of this section were the following ones: Law Governing Framework Conditions for Electronic Signatures (Signatures Law - SigG) of 16 May 2001 - (unofficial consolidated version) - http://www.bundesnetzagentur.de/media/archive/3612.pdf ; and Ordinance on Electronic Signatures (Signatures Ordinance – SigV) of 16 November 2001 - http://www.bundesnetzagentur.de/media/archive/3613.pdf

[12] This interpretation is based on the inputs provided by M. Bickenbach; however, there cannot be a conclusive statement on how this system functions in practice, as no system outside of Germany has been assessed to be equivalent yet, and no SSCD has been published by the Bundesnetzagentur as being acceptable without a German conformity assessment finding by a German designated body.

- First an evaluation of the product, either via:
    - The evaluation of products for qualified electronic signatures on the basis of the Common Criteria for Information Technology Security Evaluation (Federal Gazette 1999 p. 1945 – ISO/IEC 15408) or the Information Technology Security Evaluation Criteria (ITSEC – Joint Ministerial Bulletin of 8 August 1992 p. 545) in the version currently in force. The evaluation must cover at least evaluation level CC EAL 4 or ITSEC E 3 for secure signature creation devices.
    - Or by meeting the associated generally recognized standard i.e. CWA14169;

- And then a confirmation by a "confirmation body" (i.e. the Designated body in the sense of the Directive [1]).

This requirement could be contrary to the provisions of Directive 1999/93/EC, which does not impose such technical requirements.

In addition, the establishment of equivalence by the Bundesnetzagentur might be seen as an infringement of article 3.4 of Directive 1999/93/EC; *"A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States."* Germany (or any other country) may check whether foreign bodies are those referred by the Directive, i.e. that these bodies comply with decision 2000/709/EC, and under this decision the bodies must be *"transparent in its conformity assessment practices"*, but this does not allow a country to judge the practices and criteria of another country. The principle in Directive 1999/93/EC is indeed that Member States have no right to determine if the foreign findings of conformity are 'adequate' according to their own rules, so if this is how the Bundesnetzagentur interprets it, then that seems like a significant issue.

Finally, one can note that there are no foreign products listed in the lists on the Bundesnetzagentur website, or any products assessed by non-German Designated Bodies; however there is no need to be listed on the German list to be recognised (as per the art. 23 in the German law). One can argue that this might result in marketing difficulties, since potential German users of SSCDs will likely look towards the Bundesnetzagentur for guidance to determine which SSCDs are acceptable under German law: but that problem may not be limited to Germany, since no Member State is currently able to provide a comprehensive overview of all European SSCDs.

There is finally another concept in the German regulation to be underlined, the Signature Application Component (quite similar to the SCA presented in the present document), for which declaration of conformity is also required (at least for CSPs). However, although the Signature Application Component and SSCD are interfacing during a Signature Process, nothing binds the recognition of a particular SSCD with the recognition of a particular Signature Application Component.

Belgium: a flexible interpretation example

This illustration is based on the Belgian case. Belgium has not included an obligation of a conformity assessment in their rules: an SSCD needs to comply with Annex III, but no formal assessment is required to determine this.

Implications

The German case shows an approach where there is a national legal requirement for SSCD assessment by a Designated Body. Germany is not the sole country[13] with such an approach. One can also observe cases, like Hungary e.g., that requires Certification of electronic signature products (these include signature-creation devices). In Hungary, by the Act on Electronic Signatures No 35 of 2001, SSCDs must be compliant with criteria determined in current relevant standards and deliverables, as determined and published by the notified designated bodies[14]. These bodies do not evaluate signature products themselves; rather they check the existence of evidences in the certificate issued by a (foreign) ITSEF laboratory whether the TOE meets the specific criteria of CWA 14169. Austria also explicitly mentions specific items that need to be evaluated, such as the evaluation of chip cards, of components used for hash calculation, of secure viewing and PIN entry.

In total, for seven (7) countries, a certification of conformity is clearly required (in most of the cases against the generally recognised standard CWA 14169), **being confirmed by a Designated Body determination of conformity or not. A few other countries**, like Belgium, **do not necessarily require a conformity assessment** (for example, in the Czech Republic the Ministry of Interior *only* formally verifies the information provided in relation to an SSCD to determine if a given SSCD is applicable for usage in the Czech Republic).

The stricter interpretation (requirement for SSCD assessment by a Designated Body) does not seem to be a very pragmatic attitude, simply because many countries have not designated conformity assessment bodies, meaning that a limited number of designated bodies would need to carry the burden for the European SSCD market, and that political difficulties may arise (e.g. because a national eID card from a country without a designated body would need to be assessed in another country). However, it is not strictly contrary to the Directive (i.e. it is not 'legally wrong'), at least until a clarification on the exact interpretation of the Directive would be given. In addition, it should be emphasized that strict interpretations (like requiring determinations of conformity by designated bodies or requiring a certification of conformity) have the clear advantage of leaving less room for discussions and thus making the cross-border recognition more straightforward.

It seems to be more logical to take the flexible approach, and to argue that issuers of SSCDs should be able to make the determination themselves, and that the benefit of formal assessments is the removal of doubt. This is more pragmatic, and also more in line with current approaches to standardisation (like the New Approach directives: self declaration of compliance, with the possibility of disputes, rather than requiring prior conformity checks). However there is of course a risk involved, since there is less legal certainty this way: if a claimed SSCD is later found not to comply with Annex III, then that could cause significant problems (especially in relation to the

[13] This information is based amongst other on the collection and assessment of the current situation and position of the 27 EU Member States, as well as Iceland and Finland and other EEA countries. They were asked to answer the following questions:

1. Please provide information on the notified bodies referred to in Art. 3.4 of the e-Signature Directive (name, address, URL).
2. Please indicate whether the supervision scheme and/or national legislation require compliance to specific SSCD criteria, and/or certification.
3. Are these criteria/requirements based on compliance with (non) EU standardisation deliverables? Which ones?

[14] There are 2 DBs in Hungary. They are both notified to the Commission as required under article 11, 1, b) of the Directive.

legal value of any signatures created using such a device in procedures that required the use of a qualified signature). There is no clear answer about what happens in case of a conflict between these different interpretations of the need for a determination of conformity: e.g. a service provider only wants to accept qualified signatures, and refuses to accept signatures created using an SSCD for which no conformity determination exists. There are no real rules to determine who needs to take the initiative in this case: the question is then whether there is a negative obligation on the service provider (proving that the device is not compliant) or a positive obligation on the issuer (proving that it is compliant).

Due to the fact that there is no obligation for a Member State to have a Designated Body, it is hard to imagine that other sources of conformity declaration are not legally acceptable under Directive 1999/93/EC. However, as the Directive 1999/93/EC also allows stricter interpretations, (at least until there will be a European Court of Justice ruling to clarify this issue), if self-declarations do have a legal value, one encounters a problem of recognition in countries where self-declarations for SSCD are not admitted (in particular where a certification or a determination by a DB is required).

The study team would suggest the EC to provide some clarification on the legal value of the different levels of SSCD conformity assessments. Member States' existing regulations shall be considered carefully before this clarification to ensure that the spirit and the letter of the internal market provisions of the Directive are respected fully.

4.2 Trust in the SSCD's conformity assessment processes

International agreements do exist in order to ensure trust in evaluation/certification processes and in related bodies as well as to guarantee the mutual recognition of the resulting certificates thanks to recognition Agreements of IT security certificates - as far as such certificates are based on ITSEC or CC.

These agreements would clearly help to enhance trust in DB's practices, for what regards the determinations made by a designated body and, since we do not have a firm answer on the legal value of certification other than determinations made by a designated body, they would also help to improve the legal standing of conformity assessments made by other bodies.

1. European Recognition of ITSEC/CC – Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden, Switzerland and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement. Version 3 of the SOGIS MRA was expected to be approved in 2009.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

The SOGIS MRA agreement covers thus ITSEC and CC certification levels up to EAL7 and thus provides recognition of certification against CWA 14169. At the moment of edition of the present study, only the 9 above mentioned EU Members States were members. It would be interesting to have more Member States in these agreements.

2. International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

Common Criteria Recognition Arrangements (CCRA) for Common Criteria (CC)[15] ensures trust in evaluation/certification processes and bodies in the community of countries having signed such arrangements. For what concerns SSCD in particular, CWA 14169 is a (set of) Protection Profile(s) (PP[16]) built and evaluated against Common Criteria (ISO/IEC 15408). The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

The arrangement caters for mutual recognition of certificate up to level 4. The SSCD profile required by CWA 14169 however is EAL4 + (i.e. EAL4 augmented). As noted above, it is questionable whether this level is fully covered by the Arrangement or not. However, looking the Certificates issued under CCRA, one read that the

[15] The arrangement caters for mutual recognition of certificate up to level 4. One also reads in SSCD certificates that it also covers the recognition of CC PPs (see e.g. BSI-PP-0005-2002). The SSCD profile required by the generally recognised standard is EAL4 + (i.e. EAL4 augmented). It is questionable whether this level is fully covered by the Arrangement or not, i.e. whether EAL4+ can be considered to be a sublevel which is still a part of the 'main level' of EAL4, or whether it should be considered to be a higher level. Arguments in favour of both interpretations exist; on the one hand, CC Part 3 explicitly defines only 7 assurance levels and no sublevels (i.e. no EAL4+), and on the basis of this it can be argued that the CCRA should cover any variations on EAL1 to EAL4 as well. One also note in the CCRA arrangement that the "The assurance package confirmed should distinguish between Common Criteria Evaluation Assurance Level Part 3 « conformant » and Common Criteria Evaluation Assurance Level Part 3 « augmented ». Augmentation should be designated by a plus, (e.g., EAL 3 +) ». This way of working – whereby the augmented status is merely interpreted as a variation of the primary level - can be seen as a way to have the EAL4+ level covered in the CCRA. However, both logically and legally this is somewhat questionable, since such variations are not necessarily known to the Participants in the CCRA, and it may be difficult to argue credibly that they have agreed to accept variations on the base profiles of CC Part 3 without knowing what these are. In addition, in relation to the scope of the CCRA, article 2 explicitly states that extensions of the CCRA's scope are possible "by adding other assurance levels *or components*" (emphasis added). This seems to imply that any components added to the four first base EAL levels would also need to be agreed explicitly. A clarification is needed from CC in this respect, and also with respect to the potential impact that the exceptions provision of the CCRA (article 3) could have on the cross border value of CC-compliant SSCDs, given that a specific Community regulatory framework exists, one could argue to pre-empt the binding applicability of the CCRA. As noted in the CCRA, recognition of CC-compliant SSCDs (up to level 4 as specified in the CCRA) would not be mandatory for the participants if this would be contrary to Community regulations. Since Community regulations refer to generally recognised standard, which have been set at EAL4+ rather than EAL4, it could be argued that there are thus two reasons why the CCRA's binding recognition rules do not apply in a satisfactory manner: on the one hand its inherent limitation to EAL4, and on the other hand the existence of a European framework that only requires EAL4+ before recognition becomes mandatory.

[16] The PP is *a generic* Security Target (ST) that needs to be instantiated under particular STs, device per device, when the evaluation/certification is performed.

arrangement includes the PP. Does this include a PP above EAL4 (such as SSCD PP which is EAL4+)? A clarification is needed.

Regarding CCRA, as of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org. At the moment of edition of the present study, only 12 EU Members States were thus members. It would be interesting to have more Member States in these agreements.

CCRA and SOGIS MRAs are efficient tools for SSCD certification cross-border recognition between signatory Member States; however, outside of this scope, the agreement unfortunately has no legal value. It would be interesting to involve more Member States as signatories in these agreements to improve the cross border standing of PP compliance assessments. It is worth noting that CWA 14172 [13] aims to guide SSCD conformity assessment also encourages Members States to sign such international arrangements in order to enhance the cross-border recognition of SSCD conformity determination made by Designated Bodies. In addition, if both organisations were publishing the list of certified SSCDs in the same (to be harmonised) way as the Member States DBs, this would greatly help in the interoperability. The study team suggest work is carried on the harmonisation of such publication, as a proposal to be discussed between Member States and these organisations.

Finally, it should be noted that the CCRA and SOGIS RA are agreements between the contracting parties, rather than treaties or other formal international agreements in the sense of international law. They are thus not formally legally binding.

One shall also mention the International Accreditation Forum (IAF), which is a global association of Accreditation Bodies, Certification Body Associations and other organisations involved in conformity assessment activities in a variety of fields including management systems, products, services and personnel (www.iaf.nu), thanks to which the recognition of product certificates is given and has not to be questioned. There seems that nothing specific regarding SSCD Certificates does exist at this stage, however their website announces a liaison with the CEN.

4.3 Legal uncertainty of Generally Recognised Standards

Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets generally recognised standards for electronic-signature products in the *Official Journal of the European Communities* standards [1, art 3.5]. For SSCDs in particular, Member States shall presume that there is compliance with the requirements laid down in Annex III when an SSCD complies with CWA 14169 (March 2002) [5]. There is however no obligation to follow a generally recognised standard like CWA 14169; e.g. if the conformity of an SSCD is assessed by a designated body according to Article 3(4) of the Directive under other criteria, the conformity should not be questioned.

However, some issues have already been identified in [2]; generally speaking, the (majority of) standards referenced in the Official Journal are "harmonised standards", in the sense of European Norms (ENs). Decision 2003/511/EC [3] on the publication of reference numbers for electronic signature products, however, does not refer to harmonised standards but to "Generally Recognised Standards" (GRS) which are CEN Workshop Agreements or CWAs[17]. Indeed, CWAs have been issued in the context of the European Electronic Signature Standardisation Initiative (EESSI) to support Directive 1999/93/EC because this type of documents is faster to issue than ENs. In the context of EESSI, it was a requirement not to wait for an EN in order to enable and support the market as soon as possible. Note, however, that CWA 14169 referenced by the Decision 2003/511/EC has been superseded by its 2004 version which is currently updated and under the process of becoming EN.

Nevertheless, there exists a general uncertainty as to the "legal value" of CWAs, their effects in the internal market and the impact they have (or should have) on public authorities, regulators and justices, market operators and end-users.

In addition, Decision 2003/511/EC makes use of direct and dated references (stating the number and date of the CWAs in question). Those of course have been updated from that time while the Annex of the Decision did not, assuming backward compatibility of current versions. Maintaining direct dated references to standards in regulatory texts could thus cause market uncertainty if the published standards do not reflect "the state of the art" or cannot be adopted or integrated in common applications (see [2] and [6]). The publication of dated versions of the generally recognised standards, may lead to confusion when those versions become updated and/or obsolete (knowing that an obsolete document may in addition impede trust in the SSCD).

In particular, CWA 14169:2002 mentioned in decision 2003/511/EC is perceived as out-dated (in theory CWAs are valid for 3 years with one possible renewal for 3 years), and even worse the document is not correct. The issues on the content lie in a number of small errors found after the evaluation of the Protection Profiles according to The Common Criteria (CC) for Information technology Security Evaluation certification process. The document has been up-dated accordingly (14169:2004), but this superseding version, dated from 2004 is about to expire. In addition, both versions refer to obsolete references. In order to circumvent the fact that the document mentioned in decision 2003/511/EC is out-dated, the CEN/ISSS Forum (as it then was) took a long time ago the conscious decision that CEN will retain the relevant CWAs as publications as long as the Commission Decision applies. So renewal is automatic (source, CEN). Unfortunately, no public statement is available on this which hardly brings more legal certainty to the document; in particular it seems to apply to the 2004 version of the document (i.e. not referred un the Decision), as this is the sole version published on the CEN portal, and if this decision applies to the 2002 version, this does not solve the issues on the content that lead to the revision of the document after its evaluation. What is the legal value of an assessment against an obsolete (but legally recognised) document (knowing that a CC certification is only possible against the 2004 version of the document)?

The publication of dated versions of the generally recognized standards versus non-dated version is a topic to be discussed under the Directive [1] Article 9 Committee;

[17] **CEN Workshop Agreements –** The referenced standards do not have the nature of *harmonised standards* (ENs) but are CEN Workshop Agreements (CWAs) adopted by CEN. These are new deliverables of flexible standards-making procedures followed by CEN.

both solutions offer pros and cons. The objective is to avoid ambiguity on device conformity because of confusion around the validity of the GRS at the moment of its certification.

4.4 Potential legal discrepancies in Member States

Directive 1999/93/EC [1], in its recital (20), states that *"Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of handwritten signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be* ***regarded as legally equivalent to handwritten*** *signatures* ***only if the requirements for handwritten signatures are fulfilled****".*

In order to prevent legal discrepancies, besides the fact that Directive 1999/93/EC explicitly sought "Harmonized criteria", the "non-discrimination" principle should be applicable, both for the interpretation on "who" should be a trusted entity to determine SSCD conformity with requirements from Annex III of Directive 1999/93/EC, as well as for the criteria used to assess this conformity. But this will not solve the interoperability issues linked to the possible interpretations of handwritten signature in the Member States, and although harmonised criteria are sought for electronic signatures, national requirements on signature may induce **specific criteria** for SSCD that could raise interoperability issues; e.g. a Member State can define a handwritten signature as exclusively linked to a human being. This is not an infringement of the Directive [1] but may creates interoperability issues with a Member State that has ruled that moral persons also have the right to create Qualified signatures. Such interpretations may also lead to refuse a device offering a certain degree of automation of signatures (e.g. mass-signature processes that do not require the implication of the human-being, as it is required for ***hand***written signatures).

4.5 No legal obligation beyond SSCD's boundaries

The conformity assessment criteria are naturally highly dependent on the SSCD concept itself, which is sometimes questioned (as it appeared in the survey performed within the Electronic Signature Standardisation Study [2]). This is true even for determination of conformity made by Designated Bodies, although those bodies are (i) liable (making that relying parties have the possibility to turn against an identified party, i.e. the designated body in case of litigation), *and* (ii) shall not be questioned by (other) Member States as per [1]. The difficulty stems from setting-up the ***boundaries of the SSCD*** (determining where to start and where to stop the conformity assessment).

An SSCD is essentially the device handling the private key in such a way that Advanced eSignature (AdES) requirements are guaranteed. The SSCD is not always the sole element implied in the AdES creation. The following elements, not necessarily part of the SSCD, must be considered as being in the immediate environment of the SSCD:

- the Secure Creation Application (SCA), and if not provided by the SCA,
- the human interface (HI) for input of the signatory authentication data (SAD) or display of data to be signed (DTBS)

The SSCD is thus a part of the signature creation environment such as represented in Figure 2 below.

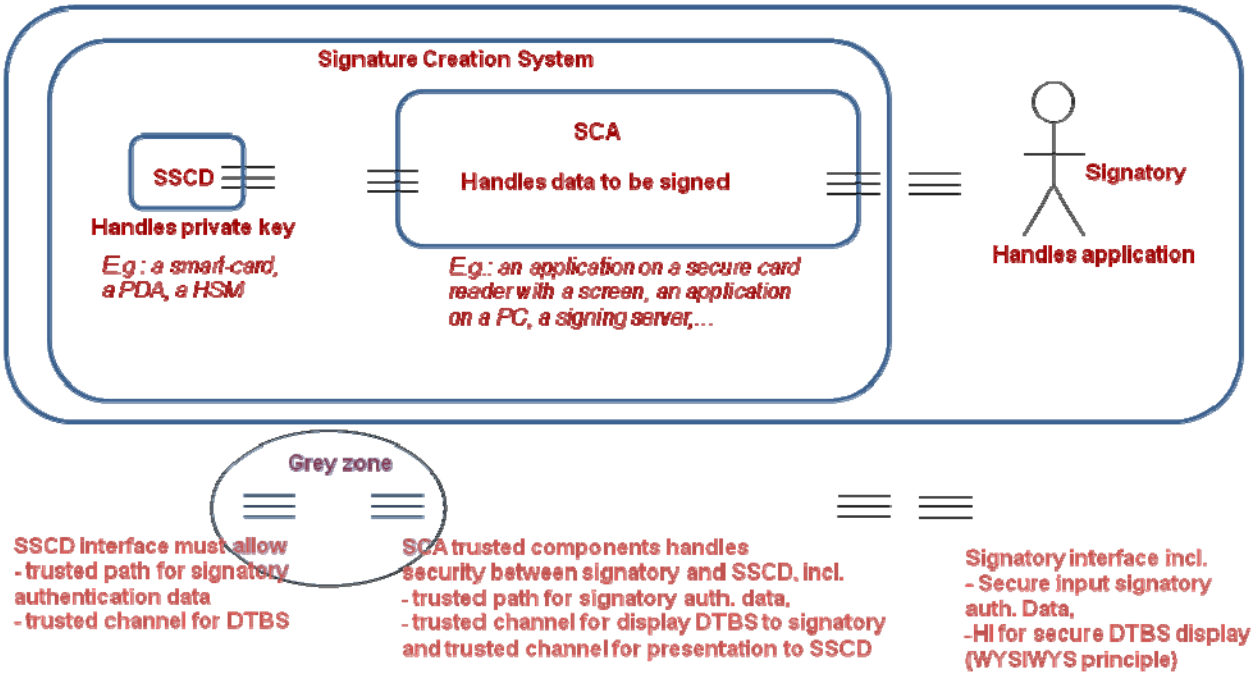

Figure 2: SSCD in Signature creation environment

As per Directive 1999/93/EC [1], Annex III covers requirements for secure signature-creation devices to ensure the functionality of AdES. By definition, SSCD means configured software or hardware used to implement the *signature-creation data*. Beside SSCD one can identify other hardware or software used during the creation of electronic signatures, falling under the scope of 'electronic-signature products' such as defined in Directive [1] art 2.12 "*hardware or software, or relevant components thereof, which are intended to be used […] for the creation or verification of electronic signatures*". A SCA, although not defined as such[18], is such an electronic-signature product implied in the AdES creation. There is a distinction between the "crypto device" (SSCD) and the application making use of this crypto device. Clearly there must be an interface between the two and there are a number of security requirements regarding the application component at least for secure handling and management of this interface.

The sole control on the private key (*the signature creation data*) by the signatory and the protection of the DTBS are important security requirements in AdES concept[19] that certainly needs to be covered by the SSCD in particular, and by the whole signature creation environment in general. Some questions may arise from the following sentence within the Directive recital (15); *"Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate"*. Although this recital states the obvious for all-purpose computers (an all-

[18] Although SCA is not a concept defined as such in the Directive, it appears in the standardization landscape (see below, especially in CWA 14170).

[19] item (c) of AdES definition: "*AdES is created using means that the signatory can maintain under his sole control*" and item (d) linking the AdES to the data to which it belongs.

purpose computer cannot be secured completely), this sentence induces trust issues because it is seen by some stakeholders as a possible gap in the control by the signatory (e.g. for smart-cards based SSCD, would the smart-card readers be kept outside the scope of the evaluation, this might cause a security issue regarding the control on the PIN code).

As far as SSCD only are concerned, the risk to impede the sole control is rather limited as long as Annex III requirements are fulfilled. Independently of the environment in which such devices operate,

Annex III §1 requires that:

> *(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;*
>
> *(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;*
>
> *(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.*

These conditions are sufficient to guarantee the sole control on the signature creation data by the signatory. They must be fulfilled up to the SSCD's boundaries (per CWA 14169, the SSCD must allow for the creation of a trusted path between the signatory and the SSCD in order to insure the secure transfer of the signatory authentication data (e.g. a PIN code) to the SSCD, potentially through the SCA and/or the Human Interface (if not provided by the SCA).).

Annex III §2 requires that:

> *Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.*

This condition on the DTBS protection must be fulfilled up to the SSCD's boundaries (per CWA 14169, the SSCD must allow for the creation of a trusted channel up to the signatory for secure display of DTBS, for secure transfer of DTBS from the SCA and for the output of the signature to the SCA).

The issue is that these conditions shall be "maintained" beyond the SSCD when it does not implement the SCA or the HI. The requirements on Trusted Path and Trusted Chanel represent strong constraints on elements in the immediate environment of the SSCD**. However, there are no legal obligations on these elements** (such as obligation to work with "certified as secure" SCA or with secure SSCD reader). An SSCD used with an unsecure SCA will not lead to a secure AdES (since the AdES security will rely on the SSCD security including its boundaries, e.g. in particular the SCA, AND the rest of the signature creation environment).

However, regarding the SSCD definition and the legal requirements on SSCD, the generally recognised standard CWA 14169 is sufficient[20] for legal presumption of

[20] Nevertheless, this does not prevent the use of complementary guidance for the conformity assessments of a SSCD. In particular, the EESSI work that has been performed around the Directive is not limited to CWA 14169. The way this standardization landscape, encompassing CWA 14169,

compliance with Directive 1999/93/EC (and shall not be questioned regarding its status of conformity assessment criteria, as per article 3.5 of [1] & Decision 2003/511/EC [3]). The way these requirements are fulfilled up to the SSCD boundaries is under the responsibility of the bodies in charge of the SSCD conformance assessment. Beyond the SSCD interfaces, the SSCD security *shall* not be challenged. In particular, as per articles 3.4 of [1] it *must* not be challenged when the determination of conformity is made by a Designated Body (that is liable for this).

4.6 The standardisation framework related issues

4.6.1 The Standardization framework

A series of CEN and ETSI deliverables related to SSCDs and their management were produced in the direct following of the directive and the edition of CWA 14169, or more recently. It is important to approach this standardisation work globally, as we are going to see that although CWA 14169 is the sole document referred as generally recognised standard in Decision 2003/511/EC [3] for what regards SSCDs, this CWA needs the support of other technical documents for different reasons explained in the next section. The most relevant standard and technical documents are listed below (the list does not pretend to be exhaustive; such a global inventory shall be part of the standardisation Mandate M460 on electronic signatures [15]. Some of the documents have expired; their up-date will also be part of the standardisation Mandate M460):

1. CWA 14355 [8]: These guidelines for the implementation of Secure Signature-Creation Devices are an informative reference of CWA 14169. This document provides guidelines addressing **the boundary between the Target of Evaluation (TOE) and its immediate environment**, i.e. the interface between them. The purpose of CWA 14355 is to extend the previous work towards defining guidelines on implementing SSCDs in specific platforms (such as smart cards, PCs, PDAs and mobile phones) and in specific environments (such as public terminals or secured environments). This CWA is intended for use by both legal and technical experts in the area of electronic signatures, as well as designers of systems and products in this area. CWA 14355 goes beyond CWA 14169 (technology neutral and limited to generic SSCD), provides samples and derives findings for different types of platforms (e.g. Smart-Cards, PDA).

2. EN 14890 [9] “Application Interface for smart cards used as Secure Signature Creation Devices” deals with the key issue of enabling interoperability, so that smart cards from different manufacturers can interact with different kind of signature creation applications.

3. CWA 14170 [10] “Security Requirements for Signature Creation Applications”, describes the signature creation process and defines a Signature Creation System (SCS) as consisting of a Signature Creation Application (SCA) and a Secure Signature Creation Device (SSCD).

---

supports the SSCD cross-border recognition is crucial and is studied in the “The standardisation framework related issues” section of the present document.

4. ETSI TS 102 176-1 [11] “Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”.

5. ETSI TS 102 176-2 [12] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices”.

6. CWA 14172-5 [13] 2004 EESSI conformity assessment guidance - part 5 : “secure signature creation devices”.

7. BSI Technical Guideline TR-03110 [14] “Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) Version 2.01

8. ETSI SR 002 176 Algorithms and Parameters for Secure Electronic Signatures[21]

4.6.2 **CWA 14169 issues**

CWA 14169:2002 mentioned in decision 2003/511/EC is out-dated and not correct (see ad-hoc section “***Legal uncertainty of Generally Recognised Standards***”). The **references** found in both versions of CWA 14169 (the version referred by 2003/511/EC as well as its up-date from 2004) are **obsolete** and sometimes inexistent.

In particular, CWA 14169 uses a normative reference (in the three PPs in its Annexes) to an inexistent list known as “*the list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the ‘Electronic Signature Committee’ in the Directive* »,reference itself disregarded further in the text with the following recommendation « *The security target writer should instead consult [ALGO], the national certification body and the designated body according to the Directive 1999/93/EC, article 3, paragraph 4, for advice which algorithms and parameters that are approved to fulfill the protection profile*.” where [ALGO] is ETSI SR 002 176 and “instead” means “*instead of the list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the ‘Electronic Signature Committee’ in the Directive* ”.

Because of this confusion, each country may establish its own criteria and there is a risk that Directive 1999/93/EC [1] article 3.5 cannot be followed anymore (i.e. presumption of compliance with Annex III) (see also [6]).

[21] The so-called Algo Paper (ETSI SR 002 176) was created by a group of experts under the mandate of the European Electronic Signature Standardisation Initiative (EESSI) Steering Group. No formal mandate from Article 9 Committee according to procedures conformant to Article 10 of Directive 1999/93/EC was ever granted to the production of this document. It received some acceptance by Member States (e.g. used by AT) but (to be confirmed) was never endorsed formally by the Article 9 Committee except through the fact that it is a normative reference for CWA 14167 enlisted by CD 2003/511/EC as approved by the Article 9 Committee. Note that in itself the ETSI SR 002 176 document has no formal value as it is a “Special Report” (SR) and not a standardisation deliverable as such.

CWA 14169 uses an informative reference to CWA 14355 that is also on the point to expire.

4.6.2.1 The need for guidance on conformity assessment

CWA 14169 is built under a technology-neutral approach that has solely been based on the requirements that are defined by Directive 1999/93/EC. In theory, CWA 14169 contains the necessary criteria to cover the SSCD concept as defined by Directive 1999/93/EC [1] by defining Common Criteria Protection Profiles (PP) to evaluate SSCDs (here after SSCD PP) as Target of Evaluation (TOE) reaching CC EAL4+ security level. The PP is a *generic* Security Target (ST) that needs to be instantiated device per device when a certification is to be performed. This is the controversial part of the certification process, as the way a certification against CWA 14169 is performed is left to the certification body (cfr here below). In order to avoid discussions / interpretation that may appear at this stage, guidance on appropriate conformity assessment practices could help in sustaining cross-border recognition.

As already stated, participation of more Member States in international arrangements such as SOGIS MRA or CCRA, may help in this issue, since they bring mutual recognition that pre-empts the questioning of the certification process.

4.6.2.2 SSCD is not the sole element to consider for secure eSignature

An important aspect influencing the SSCD PPs is that the scope of Annex III – and thus the scope of conformity assessment carried out by designated bodies – is limited to the SSCD. As already explained, the SSCD has to operate in an environment whose security is out of scope of CWA 14169; the conformity of an SSCD with regards to Annex III of Directive 1999/93/EC stops at the boundaries of the SSCD. Discussions / interpretation may appear and a clear positioning of SSCD and thus of CWA 14169 with regards to other eSignature products (e.g. such as the SCA defined in standard CWA 14170) could help in sustaining cross-border recognition. In particular the way the "trusted path"[22] for user data authentication is maintained beyond the SSCD if the human interface is not provided by the target of evaluation (see hereafter).

CWA 14169 itself states: *"To cope with the requirements defined in Annex III of the EU Directive, security requirements have to be specified and fulfilled* ***also*** *for elements which represent components or mechanisms within the immediate environment of the SSCD. Such components or mechanisms shall be clearly identified during the evaluation process".* This precaution may alleviate the fears raised by the sentence in the Directive [1] *"Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate"*. It copes with the fact that Annex III induces some sort of requirements in

[22] 'Trusted path' provides a means for users to perform functions through an assured direct interaction with the TOE (Target of Evaluation) Security Functions. Trusted path is usually desired for user actions such as initial identification and/or authentication, but may also be desired at other times during a user's session. Trusted path exchanges may be initiated by a user or the TSF. User responses via the trusted path are guaranteed to be protected from modification by or disclosure to untrusted applications [8].

the application interface. Common Criteria does provide means to express requirements to be fulfilled by the target of evaluation (TOE) AND to express requirements that need to be fulfilled by the TOE environment (the product certificate issued by a product certification body usually lists these environmental requirements as obligations under which the product certificate is valid). However, the TOE is the SSCD, i.e. the device handling the signature creation device and although an implementer may decide to include additional elements such as display elements, Input/Output elements, or document generation into the evaluation process to increase his customers' confidence in the product, ***this is not a requirement that can be derived from Directive 1999/93/EC.***

For what regards the limit of the SSCD, CWA 14169 page 4, clearly shows that the boundaries of "immediate environment" of the SSCD depend on the implementation. Although the functionality of the SSCD to be evaluated is the handling of the SCD, the assessment might thus encompass diverse elements, in particular for what regards the interactions with the SCA when the SCA is not part of the TOE and with the Human Interface (HI) (if not provided by SCA), which is always considered as the "immediate environment".

In order to have a sharpened idea on what must be exactly considered, one needs to analyse further the technical details provided in CWA 14169. Page 170, e.g., further describes the limits of the TOE (description of an SSCD type3).

> The TOE is an SSCD according to Directive 1999/93/EC [1]. […]. An SSCD is configured software or hardware used to implement the signature-creation data (SCD). The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:
> (1) to generate the SCD and the correspondent signature-verification data (SVD) and
> (2) to create qualified electronic signatures
> (a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function may either be provided by the TOE itself or by **appropriate environment**
> (b) using appropriate hash functions that are, […], agreed as suitable for qualified electronic signatures
> (c) after **appropriate authentication of the signatory** by the TOE.
> (d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable […].
>
> The TOE implements all IT security functionalities which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control. The TOE may provide an interface for user authentication by its own **or** implements **IT measures to support** a **trusted path to a trusted human interface device** (i.e. *by a trusted human interface device connected via a trusted **channel** with the TOE. The human interface device is used for the input of VAD (verification authentication data) for authentication by knowledge or for the generation of VAD for authentication by biometric characteristics. The TOE holds RAD (reference authentication data) to check the provided VAD. The human interface implies appropriate hardware. The second approach allows to reduce the TOE hardware to a minimum e. g. a smart card.)*

At this stage already, one can see that it is not easy to map the here above concepts with the legal requirements. The words "appropriate" leave indeed some room for interpretation. Although the evaluation of such interpretation is precisely the role of the evaluator, there is thus no straight mapping with the directive.

Regarding the "or measures to support a trusted path" (or secure channel), one has to further seek the details in CWA 14169:

> In addition to the functions of the SSCD, the TOE may implement the signature-creation application (SCA). The SCA presents the data to be signed (DTBS) to the signatory and prepares the DTBS-representation the signatory wishes to sign for performing the cryptographic function of the signature. But this PP assumes the SCA as environment of the TOE because the PP describes the SCD-related security objectives and requirements, whereas the SCA does not

implement the SCD. If a SSCD implements a SCA than it will fulfil the security objective and requirements for the TOE, as well as for the SCA as specific TOE environment in the actual PP.

If the SCA / HI are not implemented by the SSCD, as shown in the next figure inspired from figures 1 and 2 in CWA14169, annex3, CWA 14169 calls for:

- a Trusted Path (i.e. a secure communication path enabling data integrity and confidentiality for the transfer of the authentication data) between the SSCD and the signatory, i.e. up-to the HI, via the SCA if it is not part of the TOE. If the SSCD must allow for this trusted path on his side, the SCA, being outside the scope of the SSCD evaluation, is expected to provide the dual part of the duty.

- a Trusted Channel (i.e. a secure communication channel enabling the mutual authentication of two connected end-points and data integrity and confidentiality) between the SCA (if it is not part of the TOE and the SSCD) for what regards the input of DTBS on one hand, and the output of the signature on the other hand. It also calls for such a secure channel for the presentation of the DTBS to the signatory through the HI. If the SSCD must allow for this trusted channel on his side, the SCA/HI, being outside the scope of the SSCD evaluation, is expected to provide the dual part of the duty.

The use cases page 42 from CWA 14355 [8] and Table 17 of page 35 from CWA 14170 [10] confirms these interpretations of CWA 14169 (namely in its page 186[23] [5]).

[23] From CWA 14169, page 186 one reads:
The TSF (TOE Security Function) **shall allow**
[1. Identification of the user by means of TSF
2. Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE.
3. Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import.]
on behalf of the user to be performed before the user is authenticated.

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Where
FTP_TRP.1.1/ TOE: The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2/ TOE: The TSF shall permit [selection: the TSF, local users] to initiate communication via the trusted path.
FTP_TRP.1.3/ TOE: The TSF **shall require** the use of the trusted path for [selection: initial user authentication] [assignment: other services for which trusted path is required].
FTP_ITC.1.1/ DTBS import: The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ DTBS import: The TSF shall permit the SCA to initiate communication via the trusted channel.
FTP_ITC.1.3/ DTBS import: The TSF or the SCA shall initiate communication via the trusted channel for signing DTBS-representation.

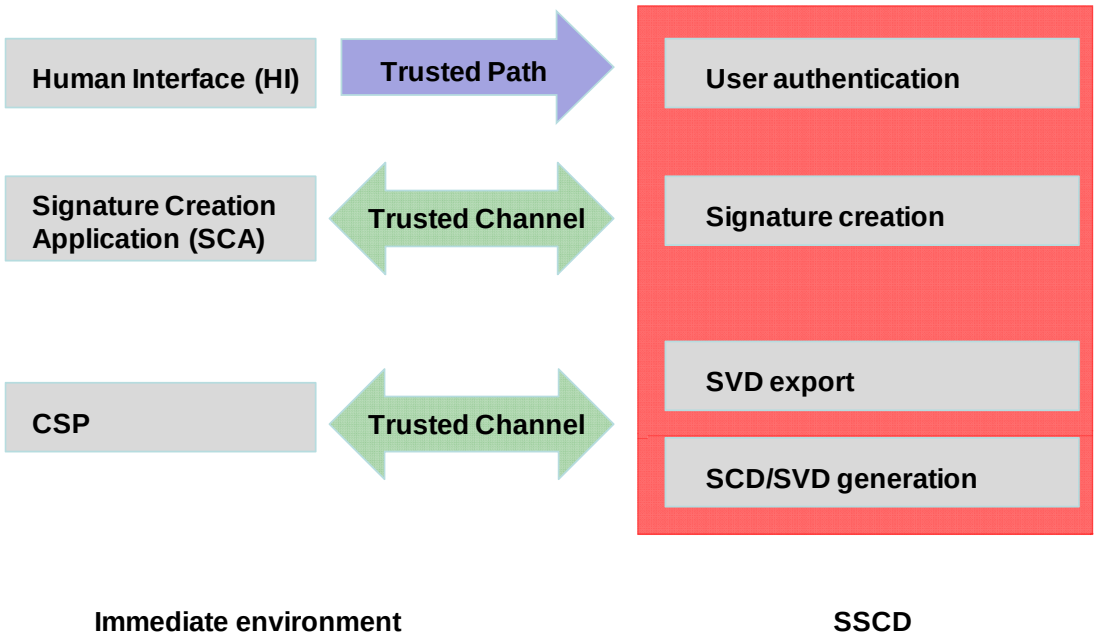

Figure 3

These requirements on Trusted Path and Trusted Channel represent strong constraints on elements in the immediate environment of the SSCD. **Fulfilment of these requirements can only be assessed by evaluating the whole system**, including communication between the signatory and the signature creation device.

In particular, CWA 14169 makes the **assumption** in page 175 that the signatory uses **only** a **trustworthy** SCA (and trustworthy CA, which is obviously the case for CSP issuing Qualified certificates). But as already said, if the SCA is not implemented by the SSCD, it is outside the scope of the SSCD conformity assessment **and there are no legal obligations on these elements** (such as obligation to work with a "trustworthy" SCA or with a "trustworthy" SSCD reader). The sole « obligation » would come from CWA14169, pp189-190 in particular where one read « *FTP_TRP.1.3/ TOE: The TSF **shall require** the use of the trusted path […]* ".

This shows that the boundaries of the TOE are not easy to define. In which cases and to which extent is it thus necessary to consider elements ranging from keyboard to screen, SSCD readers (for smart-cards in particular), middleware to access and manage the Secure Creation Data, amongst other as « trustworthy » for claiming to meet the requirements of a Secure Signature Creation Device? What are the technical guidelines, criteria for this purpose?

CWAs 14355 [8] and 14170 [10] help in this exercise (although confusion also arises from the standards themselves; e.g. the definitions of "Trusted Path" in CWA 14169, CWA 14170 and CWA 14355 are not easily comparable. Each document is obviously correct regarding the generic ISO definitions of Trusted Path, but since those deliverables concern closely linked signature products, and since the boundaries thereof are a touchy part of the security evaluation process, a very clear positioning is necessary *(still keeping in mind the "legal" definition of the SSCD limited to handling private keys)).* A clear positioning of CWA 14169 with regards to these other documents, in particular on the way the trusted paths and trusted channels are maintained if the human interface and/or the SCA are not provided by the Target Of Evaluation (TOE) is desirable.

In this perspective, technical guidelines such as Password Authenticated Connection Establishment (PACE [14]), for RFIDs (secure mutual authentication between a signature device and the terminal in which it operates) specifically define the securisation of the interaction between the signature terminal (and thus (part of) the SCA) and the S(S)CD. The positioning of such guidelines as regard to CWAs 14169 and 14170 is also desirable (as well as any PACE-like Password-Authenticated Key Exchange Protocols allowing two parties to establish a secure channel that would be envisaged for contact cards). As an illustration, for the provision of a trusted channel, CWA 14355 provides the example of using ADPU ISO 7816 commands for smart-cards. These commands ensures integrity and confidentiality of data transferred to the SSCD (note that this is not sufficient for the trusted channel as required by CWA 14169 where in addition a mutual authentication must be provided (FTP_ICT p47)). Anyway, in all cases, implementing ADPU has an impact on the middleware (even if basic and limited to libraries). Going beyond that, and ensuring compliance with CWA 14169 by means of a PACE-like protocol would even more impact the SCA.

Note that even if CWA 14169's Trusted path requirement (FTP_TRP referred here above) has been said to be the blocking point for applying SSCD-PP for major Citizen Card roll-outs, one would like to end this long section on SSCD's boundaries with a pragmatic highlight: SSCD and SCA are two different signatures products. The conformity assessment of the first one shall not be impacted by questions on the second. One might be tempted to go even more beyond the scope of the SSCD alone and impose a Secure SCA, and/or a Secure SSCD reader and/or a Secure protocol between the SSCD and the Signature Terminal, such as Password-Authenticated Key Exchange Protocols, in order to cater for a globally Secure Signature Creation. However, except with the use of additional PP (such as PACE making that only "PACE-like authorised" terminals would be able to generate a Signature with the SSCD), nothing prevents a signatory to use his SSCD on an "unsecure" environment, and there is no way for an AdES verifier to have any clue on the quality of this environment.

Is it reasonable to force all SCAs to be "trustworthy" (as per assumption in the PPs) or to force the signatory to work in "secure only" environment in all and every cases? This risks slowing down the market of eSignatures applications and does not appear to have a legal basis in the Directive, thus possibly infringing on its internal market provisions. Also, the signatory must have the liberty to sign in the environment of his choice and to decide whether his PC or his application is appropriate for signatures purposes and trustworthy, at his own risk. In addition, legally speaking meeting the requirements of CWA 14169 is sufficient to qualify as an SSCD. Beyond this, the maintenance / extension of the trusted path up-to the signatory, potentially via a SCA, is not required by the Directive. So, if PACE-similar protocols are envisaged to build additional PPs to the current CWA 14169 ones, one shall clearly specify in which condition that kind of PP would apply. A distinction shall be made between environment controlled by the signatories (e.g. home, office) and open environments (e.g. public locket). **Indeed, the demarcation between the SSCD and its immediate environment is a matter of risk assessment and a pragmatic approach may, depending on the environment, put additional requirements on procedure and policies to strengthen technical requirements.** For example, if open environments (such as public kiosk at an administration's desk, e.g.) certainly call for very secure signatures process (because users must trust an application on which they have no control and because many people access the same application), one can expect a better control on the environment by the signatory working at home or at the office (in these cases, the signatories, or its employer, have the opportunity to secure the environment). The requirements on the SCA shall be tailored according

to the environment. As advised in CWA 14170, page 16, in some cases procedural methods will perfectly compensate the fact that the SCA is not “assessed as being trustworthy” nor bound to the SSCD by any imposed protocol, alleviating such constraints on the SCA.

4.6.2.3 Multi-keys on a single SSCD might not be supported, although this is a real business need

CWA 14169 contains three PPs for SSCD:

- SSCD Type 1 - generation of the Signature Creation and Verification Data (SCD & SCV);
- SSCD Type 2 – signature generation (to be used in combination with an SSCD Type 1 from which keys are imported);
- SSCD Type 3 - has the functions of SSCD type 1 and type 2.

Both SSCD Type 2 and Type 3 state: "**The destruction of the SCD (private key) is mandatory before the TOE load (type 2) / generate (Type 3) a new pair SCD/SCV**".

This means which one cannot have a SSCD (smartcard, token, HSM) with two (or more) key pair referring two different qualified certificates (e.g. using a SCD -referring to a personal qualified certificate- and using another SCD (referring to a business qualified certificate). Such a person, with 2 Q_certificates, must have two different SSCDs.

There is a need for a protection profile to evaluate multikey SSCD.

Of course, this means also that one cannot use these profiles to evaluate a multikey HSM to be used as SSCD in compliance with a common protection profile which complies the requirements laid down in Annex III to Directive 1999/93/EC (see also below).

4.6.2.4 Types of SSCD “eligible” devices might be too restricted to smart-cards

There are in theory many ways software, hardware or procedural to implement a SSCDs. CWA 14169 consistently refers to an *abstract* category of Signature Creation Devices, of which smart cards would be just a special case. However the fulfilment of trusted path and trusted channel requirements seems by far more complex for central signing server and/or devices such as HSM than for smartcard. In particular, the end-user authentication toward the SCD might be more complex for devices where the private key is not directly in the hand of the signatory. This is actually closely linked to the interpretation of the AdES “sole control” requirement and may lead to national interpretations on the way the “Sole Control” can be provided.

1. Can a **Signing Server** (using adequate protection for the private keys stored on it) be claimed to meet the requirements of a Secure Signature Creation Device?

CWA 14355 [8] says regarding Signing Services:

> “*It is quite possible to design a Signing Service system where the SCD of all users are held in a large SSCD to which many users can connect. One instance would be an Internet site that signs messages for the signatory when presented with the message and proper user authentication.*

This design is not prohibited by the Directive [nor by CWA 14169] and is technically possible. The output of the current workgroup however does not address the serious technical issues that this type of design will present.

Firstly, the [CWA 14169 SSCD PP] is not appropriate for the SSCD that the signing service would use. A new PP is required to address the concerns of proper separation of SCD information, user authorization, user intentions and message display.

Another major problem that the signing service must solve is the creation of the trusted path between the user and the SCA and the trusted path[24] *between the SCA and the SSCD. For the Signing Service, the trusted path may very well have to be established over the public Internet. In addition the ability to properly obtain the user's consent to use the SCD would require a trusted path between the SSCD and the current platform where the user is residing.*

These problems are not technically infeasible to solve; however with the current generations of hardware and software the choices will be limited".

A Signing Server can be made to provide the same hardware/software protection as other secure devices. There are some differences, e.g. the owner of a key cannot physically protect a Signing Server "device" and a Signing Server in a network has a different vulnerability than an off-line device. Some types of Verification Authentication Data that may be acceptable for cards (e.g. PIN) are weak in a network environment, but if the authentication requirements are set too high they greatly reduce the advantages of server-based signing.

Basically, still according to [8] an additional PP with a particular focus on the Trusted Channel, seems to be necessary.

In addition, a Signing Server would also typically not be personalized (e.g. usable by only one user) as it is required by CWA 141969 (see above), but should serve a set of users. The possibility to have several SCD&SCV on one SSCD is a strong requirement from the market (e.g. public administrations may not want to provide a smartcard (and readers) to all civil servants and may prefer to use a multikey / mutli-users signing server).

This is another reason to call for a protection profile to evaluate multikey SSCD.

2. Can a **Hardware Security Module (HSM)** be claimed to meet the requirements of a Secure Signature Creation Device?

There are very few recognised HSM's. However, as already stated, all is matter of risk assessment and a pragmatic approach may put additional requirements on procedure and policies to strengthen technical requirements. In the case of HSMs, it is likely to be the case that the modules are placed in secure room; restricting the access to the room to authorized person(s) is a procedure participating to the establishment of a Trusted Path.

It is worth to note that CWA 14167 [18] has a larger view than CWA 14169 and allows for the use of HSM for CSPs' signatures (in particular for the issuance of qualified certificates). One cannot imagine that such HSMs used by CSPs would be less secure than SSCDs used by end-users! HSMs are thus devices that might be recognised as SSCD, provided that the ad-hoc technical and procedural security is in

[24] CWA 14355 states « trusted path », one feels however that it should be "trusted channel" instead (unless this concerns the continuation of the previous Trusted Path up to the SSCD).

place. However, a HSM manufacturer claimed that he submitted an HSM evaluation to one of the Member States Certification Body and were told that it could not be accepted because “an HSM could not be certified against CWA 14169” (or, at least, the Certification Body did not believe it could).

3. Beyond Signing Server or HSM, does CWA 14169 support **other devices than smart-cards**?

If it is not the case, this needs to be motivated (in particular a clarification of the reason(s) why a HSM can be accepted under CWA 14167 and not under CWA 14169). A clarification of CWA 14355 proposing several other devices as candidates for SSCD is desirable. It is worth to note that even if diverse technologies, such as mobile technologies, e.g., are endorsed within CWA 14355, the standardisation landscape seems far more complete for smart-cards based SSCD.

If it appears that CWA 14169 cannot allow for the certification of other than smart-cards devices, one shall assess whether other standardisation documents / deliverables exist and make sure that they cover all potential business needs (e.g. signing servers, HSMs, …) as well as diverse other (new) technologies endorsement, and one shall determine if it is relevant to define additional PP(s) within CWA 14169 to cater for this need.

Finally, without presuming the existence of gaps in the existing PPs, it shall be noted that in some cases, the combination of more than one PPs may be required to sustain the evaluation of new types of SSCD (e.g. such as it might be the case for signing servers, as proposed above), however the evaluation is made (and thus paid) per PP. The evaluation may rapidly become unaffordable for suppliers when more than one PP need to be combined for covering the evaluation of a device.

4.6.2.5 The need for batch signatures

Does CWA 14169 allow batch of signatures? Can a device supporting **automated signature** (without a human intervention for each single signature) be claimed to meet the requirements of a Secure Signature Creation Device?

Is the concept of sole control impeded by signature creation automation? The provision of a PIN code (in the sense of **P**ersonal) is not possible anymore, how can a similar level of control on the key be achieved? Are there criteria for assessing such level of control?

How to interprets the CWA 14169 requirement on trusted path (“the TSF shall require the use of the trusted path for [selection: initial user authentication] [assignment: other services for which trusted path is required]”)? Does it allow limiting the user authentication to the initial authentication only, while subsequent signatures might occur without the tangible commitment of the signatory?

If CWA 14169 does not allow automation of signatures, would it be conceivable to have a PP covering this need?

4.6.3 **CWA 14169 up-date**[25]

CEN TC 224 in charge of the signature standards within CEN is well aware of most of the issues mentioned in the previous section "**CWA 14169 issues**". There is an up-date plan, started months ago, for CWA 14169 and related standards. This work will be conducted in harmony with mandate M460 to European Standardisation Organisations on the rationalised framework for the standardisation of eSignature [15]. In particular, CWA 14169 shall become a EN norm. End 2009, it has been accepted by TC224 to split the future EN 14169 into 6 parts:

I. - One introductory part followed by five PPs[26].

II. Protection Profiles for Secure Signature Creation Device Part 2: Device with key generation

III. Protection Profiles for Secure Signature Creation Device Part 3: Device with key import

IV. Protection Profiles for Secure Signature Creation Device Part 4: Extension for device with key generation and trusted channel to certificate generation application

V. Protection Profiles for Secure Signature Creation Device Part 5: Extension for device with key generation and trusted channel to signature creation application

VI. Protection Profiles for Secure Signature Creation Device Part 6: Extension for device with key import and trusted channel to signature creation application

The CEN/TC224 is also working on other PPs related to e-signature:

1) Protection Profile - Authentication Device (PKI based). The Target of Evaluation (TOE) considered in this Protection Profile (PP) is hardware device (such as, for example, a smart card or USB token) allowing its legitimate holder to authenticate himself/herself, using asymmetric cryptographic techniques when accessing an on-line service.

This PP is aimed at being usable with PP-SSCD. Combined with PP-SSCD one can imagine that this PP might open the door the other than smart-cards devices.

2) Protection Profiles for signature-creation and signature-verification applications (SCA/SVA). The PPs for signature-creation / verification applications will allow to evaluate and certify the security and conformance to the security requirements understood for a Signature Creation Application, working in conjunction with a SSCD suitable for the production / verification of `Qualified

[25] The authors thanks the CEN TC 224 representative, M. Lescribaa, for the inputs to this section

[26] The main argument for splitting the content is that the protection profiles shall be certified and certification bodies prefer to have one protection profile per document. The second argument is to have different timing deadlines for the different parts, e.g. part 2 is more advanced than the other parts. Part 1 is added, as the terminology is common to all parts.

electronic signatures' in accordance with the requirements of Directive 1999/93/EC [1].

It seems that two PPs will be proposed to be designed subject to the approval process as applicable in TC 224 and according to the draft specifications below:

PP-SCA
This PP defines the security requirements for a Signature Creation Application (SCA).
The SCA runs on an Operating System of a Personal Computer (PC), or another electronic machine. The SCA is connected to an SSCD, which actually computes the electronic signature, as recommended by the European Directive for Electronic Signatures. The SCA applies a signature policy to generate attributes that are added to the signature to enable a future verification of the signature. The main functions of the SCA are: importing the document to be signed, checking the document format, providing the ability to display this document to the signer, and upon the signer's decision, hash the document to generate the Data To Be Signed (DTBS) including attributes according to the selected signature policy, send the DTBS representation to the SSCD, and retrieve the signature from the SSCD. Additionally, the SCA will check that the document format is compatible with its display ability. The signer shall be able to select a signature key with its corresponding certificate and a signature policy.

PP-SVA
This PP defines the security requirements for a Signature Verification Application (SVA). The SVA runs on an Operating System of Personal Computer (PC), or another electronic machine.
The SVA applies a signature policy to verify whether the signature is valid and if the signature corresponds to the signed document. The main functions of the SVA are: importing the signed document, verifying the signed document according to the signature policy including verification of the validity of the signer's certificate, providing the verification results, checking the document format, providing the ability to display the document, and providing the ability to display the relevant contents of the signer's certificate. Additionally, the SVA checks that the document format is compatible with its display ability. The verifier shall be able to select a signature policy for verification.

These PP's shall be compatible with each other, i.e. a Security Target shall be able to claim conformance to both PP.

The proposed Protection Profiles are to cover and reflect the latest advances in standardization in the framework of Directive 1999/93/EC, ranging from the evaluation and certification criteria, to the environmental assumptions that must be fulfilled by the SCA/SVA. At this stage, it is however difficult to say to which extent those PPs to be produced will be "based" on CWA 14170 and CWA 14171, as there are still discussions among experts to define the exact number and scope of PPs needed.

Another objective is to complete the EN 14890 series of standards by including one or more protocols of the Password-based Authenticated Key Exchange Family for a transaction leading to the generation of a secure electronic signature by the card and where appropriate, in a contactless environment or other contexts respective.

One also notes that CWAs 14167, 14170 and 14355 have also been assigned by CEN to CEN/TC224 for their conversion as EN, presuming that these important deliverables to be used with CWA 14169, will be up-dated. One trust this will answer the requests evoked along the present document.

4.6.4 **Conformity assessment guidelines issues**

CWA 14172-5[27] [13] aims to provide guidance for SSCD conformity assessment. It introduces the concept of "SSCD approval"; ***"****Designated bodies participating in a*

[27] This CWA 14172-5 has been prepared with the Directive [1] art9 Committee.

mutual recognition agreement should distinguish between issuing an SSCD conformity certificate (voluntary product certification) and issuing an SSCD approval (a document of legal value in the EU stating that the SSCD conforms to the requirements laid down in Annex III of Directive 1999/93/EC). This implies that a certificate issued by e.g. a SOGIS-MRA or CCRA participant is not automatically an approval of the SSCD in question. Designated bodies should request applicants to present already existing evaluation and assessment reports and should decide independently on the basis of these reports whether the issuing of an approval is warranted without re-evaluation of the SSCD."

SSCD approval would lead to official / trusted lists of SSCDs. The concept of "approval" seems similar to the "determination of conformity" defined in the Directive [1]. A clarification on this affirmation is desirable. In addition, if such documents exist, they may be used as common template for the publication of information on SSCDs by the DBs.

However, CWA 14172-5 presumes that SSCD conformity certificate (even CWA 14169 based) might not have a "legal" value (only the "approval" by a Designated Body has a legal value). As far as the legal (un)certainty of SSCD conformity certificate is not clarified, these affirmations can be challenged.

There are other standards that might help the certification processes: ISO/IEC 15446 "Information Technology – Security techniques – Guide on the production of Protection Profiles (PP) and Security Targets (ST)" or ISO/IEC 15292 "Protection Profile registration procedures" or ISO/IEC 18045 "Methodology for IT security evaluation".

5 Synthesis on the current landscape

5.1 SSCD cross-border recognition

Evaluation or certification processes for SSCD are in place in most of the Member States. However the legal strength of the conformity assessment (and thus the cross-border recognition of SSCD) varies from countries to countries depending on their interpretation of the directive.

Designated Bodies exist in many Member States and when it is not the case, the related Member State may rely on Designated Bodies of other Member States which meet the requirements of Decision 2000/709/EC [4]. Frequently the determination of conformity by Designated Bodies is based on a 2-step process (like previously highlighted in the German case): (i) the product certification and (ii) the confirmation by the Designated Body. However, as stated in the introduction of the present document, there is no obligation to proceed in this way. Unfortunately, if some Member States publish lists of SSCDs benefiting from a determination of conformity, there are too few Member States doing this publication. These lists are not harmonised, sometimes difficult to find, sometimes difficult to read (e.g. it is not obvious to determine the type of conformity). An effort on clarification and the use of a common template is desirable. This could be (re-) enforced by Decision 2000/709/EC [4] that requires Designated Bodies to be transparent in their practises. Harmonisation with lists provided by CC or SOGIS is also desirable.

The international recognition of Designated Bodies seems to function quite correctly, although the previous section shows that some Member States lack of trust in the conformity assessment practices from others (may be because their practices are not

transparent enough) and thus require a mutual assessment of their assessment practices. Such a mutual assessment obligation infringes Directive 1999/93/EC [1] stating that SSCD determinations of conformity made by a Designated Body *shall* be recognized (provided that the Designated Body complies with Decision 2000/709/EC [4] – but this Decision [4] only requires good practices and does not impose the criteria to be observed for the determination of conformity). One can imagine that the realisations and clarifications that might result from the implementation of the CROBIES WP4 recommendations will help to enhance mutual trust between Designated Bodies. To this regards it's a pity to note that (too) few Member State Designated Bodies are affiliated to SOGIS MRA or CCRA (which are the most susceptible organisations to enhance cross-border recognition of SSCD certification of compliance). A hypothesis is that being a member requires a mutual assessment of the practices and this might be set to a (too) high level. An alternative explanation would be that Member States might simply not be aware of such arrangements.

CWA 14169 [5], as being referred to by Commission Decision 2003/511/EC [3] eases the interoperability, as a (CC) conformity certificate against CWA 14169 is sufficient for presuming compliance of a device with Annex III of Directive 1999/93/EC [1] (this would be further enhanced by an up-date of both the CWA and the Decision in order to have the accurate reference to the correct version in the Decision). As a consequence, conformity assessment criteria for secure signature creation devices in Member States are rather harmonized[28] and mostly based on CWA 14169. This emphases the utility of Decision 2003/511/EC [3], and one can affirm that the mechanisms of generally recognised standards support cross-border recognition. However the legal strength of a certificate against CWA 14169 not endorsed by a DB needs to be clarified.

5.2 Standardisation framework sustaining technical interoperability of (different types) of SSCDs and guaranteeing cross-border recognition

CWA 14169 already referred in Decision 2003/511/EC [3] was a good starting point to support an "*harmonised"* realisation of Directive 1999/93/EC in an implementation-independent manner, but it may be not sufficient to clearly identify technologies to be capable to perform secure electronic signatures, for the different reasons evoked in the previous sections, in particular the difficulty to set the boundaries of an SSCD.

CWA 14169 *might be* intrinsically sufficient to sustain an SSCD conformity assessment provided that:

- The Security Target (ST) instantiation is correctly performed. In particular, the implementation includes all necessary elements (such as, *if needed,* display elements or I/O elements) into the evaluation process to achieve his customers' confidence in the product with a special care on the boundaries between the SSCD and its environment. Assessing whether an SSCD fulfils these provisions is the role of the designated body. But nothing prevents to

[28] Most of the Member States (18) claim they rely on European Standards for assessing SSCDs conformity, 8 of them explicitly cite CWA 14169 (without specifying the version) or CC EAL4+ (i.e. indirectly CWA 14169), making that a total of 12 countries do rely on CWA 14169. Some countries in addition to European standards, also mention other criteria such as to US standards like FIPS. One country explicitly mentions CWA 14167 for HSM (and another one ETSI TS 101 456): this may be because they could not find another way to map HSM with SSCD requirements laid down in Directive 1999/93/EC [1].

further sustain the evaluation / certification of SSCDs by pointing additional guidelines for defining the ST.

- Correct (secure) algorithm & parameter are used in combination with CWA 14169 requirements. To this regards, the references used in the CWA need to be up-dated.

The Electronic Signature Standardisation Study [2] also showed that there is a very clear business need to address (central) signing servers, HSMs, automated signature, etc. Although whether or not current implementations of such signatures comply with the currently proposed CWA 14169 PPs, it seems that the extension of the SSCD general concept to **other types of devices than Smart-Cards is not very well covered** by the current standardisation framework and as indirect consequence, this narrows the SSCD concept down and excludes devices other than smart cards more or less explicitly. In addition, the support for multikey SSCD is lacking (even for smart-card devices).

It is also worth to mention that suppliers are sometimes reluctant to enter into a certification process because of the cost. If smart-card providers can easily find a business case thanks to the mass market linked to European Citizen eID cards, it is not likely to be the case for other suppliers. In addition, if it is needed to combine more than one PP to cover a particular product, this may rapidly reach high costs (in terms of resources, time and money). In this perspective, the proliferation of PPs should be avoided, if possible. As a matter of fact, the **technologies** that are **currently used** / **recognised** in Europe seem to be mostly smart-cards; many smart-cards can be found on the Designated Bodies' lists. A least one HSM is listed in the Italian list of SSCD, because certified under ITSEC E3 High (accepted in Italy besides CC EAL4+). Such as previously stated, the Return On Investment (ROI) regarding the costs of certification against CWA 14169 may not be relevant for HSM providers. No server based signature service evaluated as secure signature creation device could be found.

Finally, there is a market need for formal EN standards instead of CWAs. There is a plan within the CEN for this purpose. CWA 14169 in particular is proposed to become a EN. This is also a clear requirement as target results for the European eSignature standardisation rationalisation under Mandate M460 [15].

6 Frameworks improvements for interoperation of SSCDs

6.1 Introduction

In theory, SSCDs benefit from internal market provision, meaning that if they are recognized by one Member State Designated Body, they have to be accepted by all others. The processes used to perform the security evaluation through the Designated Body can be freely determined by the Member States (like for 'appropriate' supervision systems of CSPs issuing qualified certificates to the public), and are subject to the general framework of Decision 2000/709/EC [4] (e.g. requirements of transparency and non-discrimination). However, under the light of the questions and issues raised along the present document, one can point to some issues that need to be addressed as well in the associated SSCD recognition *"business model"* of Directive 1999/93/EC [1] as in the *"standardisation landscape"* related to SSCDs.

This section proposes different actions to address these issues. These proposals have to be seen as catering for the "ideal" situation and need to be confronted with the current situation in the EU Member States. Urgent tasks in matter of SSCD cross-border interoperability in the *clarification* of the legal framework, in the trustworthy framework and in the *maintenance* of the existing standardization framework (closely linked to the legal framework via Decision 2003/511/EC [3]) are identified, as well as other actions to be undertaken on a longer term, in particular the tasks related to the forthcoming mandate to European Standardisation Organisations on the rationalised framework for the standardisation of eSignature.

6.2 The legal framework improvements

Recommendation 1

1. The legal validity of conformity assessments should be clarified on the basis of the interpretation given on Figure 1 and in particular the following questions should be answered:

- What is the legal value of a self-claimed conformity assessment?
- What is the legal value of a certificate of conformity assessment not endorsed by a Designated Body?
- If a certificate of conformity assessment not endorsed by a Designated Body has no legal value, does it have a (legal) value when the certification is made against the generally recognised standard CWA 14169?

It seems to be more logical to take the flexible approach, and to argue that issuers of SSCDs should be able to make the determination themselves, and that the benefit of formal assessments is the removal of doubt. Under this interpretation, a self-claimed conformity assessment would create a (refutable) presumption of compliance with the requirements of Directive 1999/93/EC and specifically Annex III. This is more pragmatic, and also more in line with current approaches to standardisation (like the New Approach directives: self declaration of compliance, with the possibility of disputes, rather than requiring prior conformity checks).

However, it should be stressed that Directive 1999/93/EC [1] also allows stricter interpretations, at least until there would be a European level ruling to clarify this issue. In addition, it should be emphasized that less flexible, stricter interpretations (like requiring determinations of conformity by designated bodies) have the clear advantage of leaving less room for discussion and thus making the cross-border recognition more straightforward. In all cases, but particularly this case, the next recommendations are necessary.

Any decision must consider, on the one hand, the existing regulations in the Members States (see section "***Member States legal approach***"), knowing that some Member States require determination of conformity, and on the other hand the situation of the suppliers that should not be placed in a situation of facing prohibitive costs for certification. In other words, if measures were to be taken following this perspective, it shall be kept in mind that they need to stay appropriate and realistic for companies seeking to limit the costs of compliance measures; the accreditation and approval criteria of cryptographic software and hardware to be used for creating (and validating) signatures shall thus not be(come) too high.

To address this open question, the only conclusive option is to seek a binding opinion on the correct interpretation or clarification of Directive 1999/93/EC, and specifically on the question whether a Member State may make the cross border acceptance of a claimed SSCD subject to the requirement of a prior determination of conformity by a designated body, or whether more flexible mechanisms (such as self-declarations of compliance or independent Certification) are equally sufficient for claimed SSCDs to be entitled to a recognition as SSCDs in the sense of the Directive in all Member States. While it would be possible to resort to authoritative but non-binding opinions on this question (e.g. opinions issued by the European Commission), this would not eliminate the risk of such opinions being overruled at a later stage by the competent judicial body. Thus, seeking a binding interpretation on the matter seems to be the only way to definitively settle it[29] besides recast of the Directive.

[29] In this respect, the principal option would be to obtain a decision from the European Court of Justice. Two main avenues are available in this regard.
The first possibility would be to create a conflict between two diverging interpretations of Directive 1999/93/EC in relation to the SSCD concept, such as a case in which a service provider from Member State A refuses to recognise the status of a qualified signature created by a user in Member State B, on the grounds that Member State A requires SSCDs to undergo a conformity determination by a Designated Body, when this is not the case (and has not been done for that SSCD) in Member State B. The conflict would be brought before a national court, which would be requested by the parties to seek a preliminary ruling from the European Court of Justice on the matter (i.e. the Court of Justice would be asked to rule on the correct interpretation of the SSCD concept under the Directive). This ruling would be binding in the specific conflict itself, and would also be binding in any similar matters being raised in any other Member State at a later time (i.e. the question would not be open for re-discussion if other parties in other Member State would be confronted with the same problem). The main difficulty to apply this option would be the need to create a specific conflict (which would require at least one party willing to get directly involved), and the risk of the national judge refusing to ask for a preliminary ruling on the grounds that he or she feels that the (national) law is clear enough and in compliance with the Directive.

A second possibility exists that would avoid this risk, which is for the European Commission to choose a specific interpretation (for the purposes of the final goal, it is irrelevant which one it supports) and to initiate proceedings against a Member State that has chosen a different interpretation on the grounds of failure to fulfil an obligation under Community law. The end result would be the same: by ruling on the Member State's (non-)compliance with the Directive, the Court would de facto provide an interpretation on the SSCD concept and on the need for conformity determinations by designated bodies.

The main risk in either option would be that the Court would rule that Directive 1999/93/EC makes no statement on the need for formal determinations of conformity, and that this is a matter which Member States are free to interpret in their own transpositions. The result would be that there would still not be a homogeneous interpretation of the SSCD concept in Europe, which could continue to hinder interoperability in the future.

In this respect, the first option above (a preliminary ruling provoked by a conflict between two parties under separate laws) has the advantage of potentially offering an answer to this question as well, since it is likely that the Court would indicate whether it is sufficient that the SSCD is recognised as such under the laws of a specific Member State, or rather whether it must meet the requirements of the Member State in which it is used. In the former case, a SSCD that meets the requirements of a country with flexible rules (e.g. self-declaration is sufficient) would then need to be recognised as a SSCD in any Member State, whereas in the second case its status would vary from Member State to Member State, depending on the requirements in each MS, thus shifting the burden of taking the real decision on a "case per case" or "country per country" basis.

Recommendation 2

2. An update of Decision 2003/511/EC may be necessary, possibly in a stepwise approach.

As detailed in sections "***Legal uncertainty of Generally Recognised Standards***" and "**CWA 14169 issues**" the version of CWA 14169 mentioned in the decision, dated from 2002, is not usable. An urgent up-date of the Decision referring to an up-dated version of CWA14169 is needed[30]. The update of CWA 14169 (without prejudice of further required adaptations in the context of its transformation into EN and/or in the context of the M460mandate [15], see hereafter) would consider:

(1) Verification and correction of **CWA 14169** to match provisions of the applicable Common Criteria, and validation of the modified protection profiles from BSI.

(2) Remove the references (e.g. to CWA 14355) that are coming near to expiration, or up-date these referenced documents.

(3) That references to algorithms and parameters must be non ambiguous[31] (updating, adapting or deleting the current normative reference (in the three PP in Annexes) to the inexistent "list" known as "*the list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive* », reference itself disregarded in the text with the following recommendation: "The security target writer should instead consult [ALGO], the national certification body and the designated body according to the Directive 1999/93/EC, article 3, paragraph 4, for advice which algorithms and parameters that are approved to fulfil the protection profile." where [ALGO] is ETSI SR 002 176 and "instead" means "instead of the empty reference to the "list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive".

<u>The update of the CD requires:</u>

(1) Defining an adequate way to refer to applicable cryptographic algorithms since [ALGO] is obsolete and the "list" is inexistent. The difficulty is that referenced algorithms remain considered good till they are (on the point to be) broken by a hacker, i.e. the life expectancy on a decision of algorithm is impossible to guess – therefore, directly referencing algorithms in the

[30] The study team suggests undertaking a discussion on **maintaining direct dated references to standards in the Decision, assuming backward compatibility versus referring to non-dated document**, between the Article 9 Committee, the standardisation bodies and the EC. If this discussion in not possible in a short timeframe, this first Decision up-date should maintain direct dated version as it is the case now.

[31] This is not only necessary for the SSCD support, but also for other eSignatures products and for the risk assessment of any eSignature validation processes. The reader will find more detail on the importance of cryptographic algorithms and parameters in WP5 of the CROBIES study.

Decision may lead to uncontrolled need for updates while an indirect reference to a standard may be more appropriate.

(2) To preserve existing implementations based on previous version of CWA 14169 (this question depends on decision to maintain direct dated reference or not).

NB. The updated CWA may actually have the form of CEN Technical Specifications because they would be most probably produced by the existing CEN TC224 instead of a CEN/ISSS workshop that would need to be set-up since the eSignature Workshop has ceased its activities.

(3) A coherent approach with M460 mandate to European Standardisation Organisations on the rationalised framework for the standardisation of eSignature [15]. In this perspective, as explained hereafter in the recommendations dedicated to CWA 14169, longer term actions are scheduled and should lead to a subsequent up-date of CWA 14169 that may or may not be linked to a subsequent Decision up-date, depending on the decision on dating the referred standards.

As already stated, regarding the SSCD definition and the legal requirements on SSCD, the generally recognised standard **CWA 14169 is the adequate document and is sufficient for presuming compliance with Directive 1999/93/EC.** Adding documents that are linked but not related to SSCD may only add confusion. Depending on the way to refer to applicable cryptographic algorithms, it might be possible to also refer to a document replacing "[ALGO]", provided that such document is kept up-to-date.

6.3 The trust framework improvements

Recommendation 3

3. It is important to make sure that Member States Designated Bodies are in place.

SSCDs recognized by one Member State Designated Body have to be accepted by all other Member States. There is however no obligation for all Member States to have a Designated Body. In order to have a legally enforced tool for SSCD recognition at least ONE Designated Body is sufficient, but ideally, all Member States should have a Designated Body. This does not require all Member States to have certification bodies, since Designated Bodies can subcontract the actual testing to some certification bodies in the SOGIS MRA or CCRA space. By this way, any SSCD provider would have the possibility to ask for determination of conformity in its own country. If the process of obtaining determinations of conformity by Designated Bodies could be made sufficiently simple, the aforementioned problem on the interpretation of the SSCD concept could also be addressed without a binding interpretation from the Court of Justice, i.e. by ensuring that all SSCDs with cross border ambitions could simply obtain the necessary determinations which cannot be disputed in other Member States.

Recommendation 4

4. Publication of the list of Designated Bodies by the EC.

In accordance with Article 11 of Directive 1999/93/EC [1], Member States shall notify to the Commission and the other Member States the names and addresses of the Designated Bodies referred to in Article 3(4); the publication, according to a common template, of the list of Designated Bodies by the EC would strongly help cross-border recognition of certificates of conformity issued and/or endorsed by these bodies.

Recommendation 5

5. Member States Designated Bodies must be transparent in their conformity assessment practices and Member States and for this purpose are encouraged to adhere to international agreements such as SOGIS MRA or CCR.

Transparency in conformity assessment is a legal requirement from Decision 2000/709/EC [4], but this is also an obvious requirement to strengthen the trust in the conformity assessment processes.

The present document identified SOGIS MRA and CCRA as solutions to the SSCD recognition problem. Member States should participate to international mutual recognition schemes, CCRA and/or SOGIS RA in particular, in order to enhance cross-border recognition of SSCDs.

However there is the issue that these arrangements apply to the Participants in the Arrangement, but not to non-signatories (e.g. article 18 of the CCRA). Thus the requirement to recognize certified SSCDs on the basis of the SOGIS MRA or CCRA would only apply to the Participants, but not to third parties (such as e.g. private party service providers). As a result, it is questionable whether the CCRA can thus offer a comprehensive solution to the SSCD recognition problem.

Another point related to CCRA requires a clarification from CC. It concerns the fact that the CCRA do cover fully the certification against SSCDs PPs[32].

One should also seek a clarification on the link between The International Accreditation Forum and the CEN. No SSCD certification under this forum could be established, but it might be interesting to know the status of this liaison in order to see to which extend a support to SSCD recognition could be established.

CWA 14172-5 proposes guidelines to sustain SSCD conformity assessment as well as many advices for DBs. A revision of this document is wished, in function of the clarification provided in Recommendation 1, with a particular focus on clarification on the concept of “approval” versus “determination of conformity by a DB”. This document has been prepared with the Article 9 Committee and shall be seen as a

[32] A clarification from CC is necessary on the fact that the CCRA covers the recognition the certification against the SSCD PPs, i.e. the level EAL4+ is covered by the arrangements

good start to harmonise the work of DBs (e.g. in the publication of information on SSCDs' status).

Recommendation 6

6. Member States Designated Bodies should provide **lists of approved SSCDs** to be used in the qualified electronic signature environment with a **sufficient level of trust**.

Official Member States lists of certified SSCDs with presumption of legal compliance would enhance cross-border interoperability by providing a straightforward tool for relying parties in assessing which devices are SSCDs.

The way these lists are established needs to be carefully thought out, and should consider the current reality that different levels of conformity assessment have a different legal value in the various Member States (cfr Recommendation 1). The lists may be organised in such a way that the SSCD conformity statement type and underlying criteria are clearly indicated (see Figure 1) or the lists may simply indicate that a certain device is an SSCD as per Directive 1999/93/EC [1]. However, while such a list is conceptually quite similar to the establishment of Trusted List of supervised or accredited CSPs [17], in the case of SSCD, a specific care should be given to liabilities for such a list. Indeed, Designated Bodies – when they exist – cannot act as the entities responsible for publishing all levels of SSCD conformity assessment declarations. If a Designated Body publishes self-declarations and / or SSCD certification statements, this could indeed be seen as an endorsement of these conformity assessments, which could create the risk of such publications being considered de-facto a "determination" of conformity by a Designated Body, which could cause liability risks for Designated Bodies that they are unlikely to be willing to readily assume. A simple "publication" without further assessment might not be affordable for Designated Bodies, since they are liable for the determination of conformity they make. Additionally, this could ruin the distinction between self-declaration, certification statement and determination of conformity by Designated Bodies by unifying them all under the sole "determination by a Designated Body" level. In some countries, this new "list" concept may be considered as a sufficient proof of compliance with the Directive's requirements, whereas others may continue to reject it on the basis that publication does not necessarily mean that any real determination of compliance has taken place. Thus, the interoperability issues may not be resolved if this system would be implemented without further supporting actions.

An alternative is to transfer the responsibility of publishing the lists of SSCD to the bodies in charge of the supervision systems mentioned in art 3.2 of the Directive.

However, this approach also offers a new risk, depending on how it is implemented: if the lists present a deep level of granularity providing very accurate detail on the level of the conformity assessment (i.e. on whether the conformity is self-declared, certified by an independent third party or determined by a Designated Body), then this list may offer a tool to Member States that only accept the determination by a Designated Body to close the door to otherwise recognised devices, even if they fulfil SSCD requirements of Directive 1999/93/EC, and even if they benefit from a legal recognition by above Recommendation 1. In other words, there is a risk that such an amendment of the list would turn it into a possible tool for supporting the rejection of

foreign signature solutions, since the list would provide clear information on whether SSCDs have undergone formal determinations (which so far has not been systematically available). This might even lead these Member States to question the CSPs trusted lists (for which an agreement in principle has been reached in the framework of the Services Directives) by requiring that a condition to be listed as a trusted CSPs would be to only use SSCD with a certain level of conformity assessment. This is not a wish.

At this stage, one can also ask the question of the relevance of a "central point" that would gather information about all SSCDs for which a determination of conformity exist under the form of a compiled list, and/or, similarly to the Trusted Lists [17], a list of links towards DB lists. Hopefully, no automated process such as required for eSignatures validation will be required for SSCDs. Rather, a harmonisation of the information might already enhance the cross-border recognition a little bit. Without being real "central" point, the CC lists of certified SSCDs is already an efficient tool. As already stated, if both CC and SOGIS were publishing the list of certified SSCDs in the same (to be harmonised) way as the Member States DBs, this would greatly help in the interoperability. The CROBIES study team suggests work is being carried on the harmonisation of such publication and discussed between Member States and these organisations.

6.4 The standardization framework clarification and enhancement

The most relevant standard and technical documents related to SSCD were considered for the high level assessment of the standardisation framework relevant to the present study. However, the recast of the EU eSignature standardisation model is a long-term task that goes beyond the present study. In particular the world wide inventory of all SSCD related standards and technical guidelines is a real need and is part of the M460 mandate to European Standardisation Organisations on the rationalisation of the eSignature standardisation framework [15].

The present section proposes different recommendations to be performed in this framework.

Several immediate actions are recommended in order to better support cross-border recognition.

Recommendation 7

7. Up-date CWA 14169 for the purpose of the urgent Decision up-date (i.e. Recommendation 2).

The update of CWA 14169 (without prejudice of further required adaptations in the context of its transformation into EN and/or in the context of the forthcoming mandate, see hereafter) should consider:

(1) Verification and correction of **CWA 14169** to match provisions of the applicable Common Criteria, and validation of the modified protection profiles from BSI.

(2) Remove the references that are coming near to expiration, or up-date these

referenced documents.

(3) That references to algorithms and parameters must be non ambiguous (updating, adapting or deleting the current normative reference (in the PPs in Annexes) to an inexistent "list" known as "*the list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive* », reference itself disregarded in the text with the following recommendation « *The security target writer should instead consult ETSI SR 002 176 [ALGO], the national certification body and the designated body according to the Directive 1999/93/EC, article 3, paragraph 4, for advice which algorithms and parameters that are approved to fulfill the protection profile*."). [ALGO] being itself obsolete).

Recommendation 8

8. A deep assessment of CWA 14169 is necessary as well as a clear positioning with regard to other related EESSI related technical documents.

As detailed in section "CWA 14169 issues", of the present document one faces three issues when defining a Security Target for certification against CWA 14169.

A CWA 14169 deep update shall tackle the following points (these points may already be addressed under the current work of the CEN TC 224 that should thus be highlighted in the following perspective):

1. A clear positioning, recast, scoping and/or harmonisation between the following documents, and alike, should be produced:
   - CWA 14169
   - CWAs 14170 and 14171
   - CWA 14355
   - CWA 14890
   - Password Authenticated Key exchange protocols and PACE-like PPs

2. Where relevant, a clear referencing towards other documents shall be maintained.

3. How to set the boundaries of the SSCD
   - A clear positioning of CWA 14169 with regards to other standards (e.g. CWA 14170) in particular on the way the trusted paths and trusted channels are maintained if the human interface and/or the SCA are not provided by the Target Of Evaluation (TOE) is desirable.
   - If additional PPs are envisaged to further secure the path between SSCD and SCA, one shall clearly specify in which condition these PPs applies. A distinction shall be made between environment controlled by the signatories (e.g. home, office) and open environments (e.g. public locket). In which cases and to which extent is it thus necessary to consider elements ranging from keyboard to screen, SSCD readers (for smart-cards in particular), middleware to access and manage the Secure Creation Data, amongst other as « trusted or « secure » for claiming to meet the requirements of a Secure Signature Creation Device? What are the technical guidelines, criteria for this purpose? CWA 14355 [8] provides guidelines addressing the boundary between the

TOE and its immediate environment. Is this document sufficient? Shouldn't it be up-dated to consider new types of PPs?

4. Cover the need for multikey SSCDs.

5. Cover the market need for other than smart-card SSCDs
   - Does CWA 14169 support other devices than smart-card devices? If not, this needs to be motivated (in particular a clarification of the reason(s) why a HSM can be certified conform against CWA 14167 and not against CWA 14169 and a clarification of CWA 14355 proposing several other devices as SSCD candidates are desirable). If it appears that CWA 14169 cannot allow for the certification of other than smart-cards devices, is it relevant to define additional PP(s) within CWA 14169 to cater for this need?
   - If CWA 14169 does not cater for other devices than smart-card devices needs, one shall assess whether other documents/deliverables exist and make sure that they cover all potential business needs (e.g. signing servers, HSMs, …) as well as diverse other (new) technologies endorsement.

6. Cover the need for batch signatures
   - Does CWA 14169 allow batch of signatures? How to interprets the CWA 14169 requirement on trusted path (the TSF shall require the use of the trusted path for [selection: initial user authentication] [assignment: other services for which trusted path is required])? Does it allow limiting the user authentication to the initial authentication, while subsequent signatures might occur without the tangible commitment of the signatory?
   - If CWA 14169 does not allow automation of signatures, would it be conceivable to have a PP covering this need?

7. CWA 14169 should become a European Norm (EN).

Recommendation 9

9. Need for conformity assessment guidelines
(This recommendation also sustains Recommendations 5 and 6).

CWA 14172-5 proposes guidelines to sustain SSCD conformity assessment as well as many advices for DBs. It might be a good tool to sustain cross-border recognition of SSCD listed by Designated Bodies. However, its underlying hypothesis needs to be verified under the light of Recommendation 1.

A clarification on the concept of "approval" found in CWA 14172-5 versus "determination of conformity by a DB" from the Directive is needed.

This document might also be used to propose a harmonised template for the publication of SSCD status list and to sustain Recommendation 6. To this regard, it may be interesting to define:
- the minimal set of information to be provided in such lists; type of PP against which the device is certified, name of certification body, date of expiration of the certificate, coordinates of the Designated Body, participation of this Body to international recognition agreements, …);
- the possible template for publication ;
- …

NB: this CWA 14172-5 document has been established with the Article 9 Committee. Its up-date should be done with the Article 9 Committee as it is mainly destined to Designated Bodies.

Recommendation 10

10. There is a need for real standards.

Regarding the legal uncertainty around the published generally recognised standards, some recommendation have been proposed in the eSignature Standardisation study [2], in particular the publication of non-dated document. It was also recommended to go further in the direction of EN norms rather than CWAs. The study on ES Standardisation mentioned the fact that there is a market demand for "real standard". This is true for SSCD standard(s) as well of course. However, it is worth to note that one of the CWAs, CWA 14890 has just became a EN; this alleviate the criticism over the legal uncertainty bound the fact that Decision 2003/511/EC does not refer to *"harmonized"* standards. However this CWA is not directly mentioned in Decision 2003/511/EC on the one hand, and one the other hand, it focuses on Smart-Card devices only.

The need for "real standard" is obvious for CWA 14169. Would ETSI TS 102 176-1 [11] "Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms" or any other document approved by the Article 9 Committee be also referred to in the update of Decision 2003/511/EC such as proposed above in other to cater for the [ALGO] requirement. Note that CROBIES WP5 is further addressing this particular issue.

6.5 Stepwise approach to reach the proposed objectives

Since many orientations depend on the legal status of the conformity assessment types, the first step is the clarification on these possible statuses. This should be done through Recommendation 1. If infringements to the Directive are suspected, they should be handled with the due diligence.

In parallel, the urgent tasks for the up-date of CWA 14169 identified under Recommendation 7 should be launched. This may immediately trigger Recommendation 2 enabling an up-date of the Decision 2003/511/EC [3].

Secondly, agreements with the Members States could be looked for, particularly on the way the information on SSCD –when it exists- should be presented in order to have a harmonised information sources, usable in a cross-border environment. This should be done through Recommendations 3 to 6.

The next steps should be performed as part of the M460 mandate to European Standardisation Organisations on the rationalisation of the eSignature standardisation framework [15] (in particular through Recommendations 8, 9 and 10 identified).