



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

WORKSHOP AGREEMENT

CWA 14172-5

November 2001

ICS 35.040; 35.240.50; 35.240.60

EESSI Conformity Assessment Guidance - Part 5: Secure Signature
Creation Devices

This CEN Workshop Agreement can in no way be held as being an official standard
as developed by CEN National Members.

© 2001 CEN

All rights of exploitation in any form and by any means reserved world-wide for
CEN National Members

Ref. No CWA 14172-5:2001 E

Contents

	page
Contents.....	2
Foreword.....	3
1 Scope.....	4
2 Definitions and abbreviations	5
2.1 Definitions.....	5
2.2 Abbreviations.....	5
3 Guidance on conformity assessment of Secure Signature Creation Devices	6
3.1 Introduction.....	6
3.2 Introduction to conformity assessment of SSCDs.....	6
3.3 Guidance on organisational structure of SSCD conformity assessment.....	7
3.4 Guidance on the process of confirming SSCD conformity	8
3.5 Guidance on maintaining approval	8
Annex 1 References and bibliography.....	10

Foreword

Successful implementation of the European Directive 1999/93/EC on a Community framework for electronic signatures requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products. Therefore, the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players: the European Electronic Signature Standardisation Initiative (EESSI).

In July 1999, EESSI delivered its initial recommendations in the EESSI Expert Report. The report contained an overview of the requirements for standards-related activities, as well as a work programme to meet these requirements. A work repartition was drawn up, allocating between CEN/ISSS and ETSI the standardisation activities. The work was carried out by CEN/ISSS in the E-SIGN project and by ETSI SEC in the ESI WG. The results are documented in a series of CEN Workshop Agreements (CWA) and ETSI standards.

The production of this CEN Workshop Agreement (CWA) was formally agreed at the Kick-Off meeting of the CEN/ISSS Electronic Signatures Workshop (WS/E-SIGN) on 16-17 December 1999, in response to the initial work plan of the European Electronic Signature Standardization Initiative (EESSI).

This CWA has been developed through the collaboration of a number of contributing partners in the E-SIGN Workshop, gathering a wide mix of interests, representing different sectors of industry (manufacturers, end-users, service providers, legal experts, academia, accreditation bodies, standardization organisations and national standards bodies) as well as representatives of the national public and European authorities.

The present CWA has received the support of representatives of these sectors. A list of company experts who have supported the document's contents may be obtained from the CEN/ISSS Secretariat.

The final review/endorsement round for this CWA was started on 2001-09-04 and was successfully closed at the Workshop's plenary meeting on 2001-10-03. The final text of this CWA was submitted to CEN for publication on 2001-10-05.

This CWA has been issued in five parts:

- Part 1 - General
- Part 2 - Certification Authority services and processes
- Part 3 - Trustworthy systems managing certificates for electronic signatures
- Part 4 - Signature creation applications and procedures for electronic signature verification
- Part 5 - Secure signature creation devices.

This series of documents provides guidance on conformity assessment against the requirements specified in the other Workshop Agreements and the ETSI standard concerning services, processes, systems and products related to electronic signatures. The present document is intended to be applicable to later versions of the related documents should they be revised after its publication, unless a later version of it is produced which conflicts with this statement, in which case the latest version shall apply.

1 Scope

This document provides guidance on conformity assessment of Secure Signature Creation Devices against the specification CWA 14168 “Secure Electronic Signature Devices, version EAL4” or CWA 14169 “Secure Electronic Signature Devices, version EAL4+”. The guidance is intended for use by designated bodies, assessors, evaluators and manufacturers.

2 Definitions and abbreviations

2.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Process	<i>A series of procedures and actions that have to be conducted in order to manage and enable the provision of an electronic trust Service.</i>
Product	<i>A good (hardware, software, or both) which performs against a particular specification and which can contribute towards the construction of a System built to fulfil a particular, service-focused function.</i>
Service	<i>The carrying-out of a function (or a series of functions) that provides a definable benefit to an end user. In the context of this document we are concerned primarily with electronic trust services, such as those associated with (Digital) Certificate Management.</i>
System	<i>The composition of Information Technology products and components (both hardware and software, and including processors, storage, networks, telecommunications, etc.) organised to support the provision of a particular electronic trust Service. This requires that the system be specifically, configured, integrated, installed in a physical environment and operated according to defined Processes.</i>

2.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CC	Common Criteria for Information Technology Security Evaluation
CC MRA	Common Criteria Mutual Recognition Arrangement
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CWA	CEN Workshop Agreement
E-SIGN	CEN/ISSS Electronic Signatures project
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standardization Institute
ETSI SEC	ETSI Security Technical Committee
ETSI SEC ESI	ETSI SEC Electronic Signatures and Infrastructures
EU	European Union
ISO	International Organization for Standardization
SSCD	Secure Signature Creation Device
TOE	Target of Evaluation
WG	Working Group within ETSI SEC ESI

3 Guidance on conformity assessment of Secure Signature Creation Devices

3.1 Introduction

This chapter provides guidance on conformity assessment of Secure Signature Creation Devices against the specifications CWA 14168 “Secure Electronic Signature Devices, version EAL4” or CWA 14169 “Secure Electronic Signature Devices, version EAL4+”. The guidance is intended for use by designated bodies, assessors, evaluators and manufacturers.

Unless expressly stated to refer to only one of these two CWAs all guidance in this part of the present document refers equally to either of them: the common way to refer to both within the present document is by use of the expression “CWA 14168/14169”.

This chapter is composed of five sections:

- Section 3.1, Introduction; is an overview of the guidance and explains the numbering of guidance and the use of the terminology concerning requirements.
- Section 3.2, Introduction to conformity assessment of SSCDs; explains the background of CWA 14168/14169 and the requirements for SSCDs in Directive 1999/93/EC regarding their conformity assessment by designated bodies.
- Section 3.3, provides guidance on organisational structure of SSCD conformity assessment based on the decision of the European Commission concerning minimum requirements for designated bodies. In addition, this section provides guidance on co-operation between designated bodies.
- Section 3.4, provides guidance on the process of evaluating and confirming conformity of SSCDs.
- Section 3.5, provides guidance on maintaining approval of an SSCD in case the SSCD is subject to changes (modifications, amendments, new versions).

To uniquely identify the guidance elements within the series of guidance documents, each element is numbered **G.<guidance document Part number>.<sequence number>**. The part number of this document is 5.

The term “shall” is used throughout the guidance in this chapter to indicate those provisions which, reflecting the requirements of Directive 1999/93/EC, Decision C(2000) 3179, or CWA 14168/14169, are mandatory. The term “should” is used to indicate those provisions that, although they constitute guidance for the application of the requirements, are expected to be adopted by designated bodies, assessors, evaluators and manufacturers of SSCDs. Any variation from the guidance should be an exception. Such variations should only be permitted on a case-by-case basis after it has been demonstrated that the exception meets the relevant requirements and the intent of this guidance in an equivalent way.

3.2 Introduction to conformity assessment of SSCDs

CWA 14168/14169 defines the Protection Profile for Secure Signature Creation Devices (SSCD) based on the essential requirements specified in Annex III of the European Directive 1999/93/EC on a Community framework for electronic signatures. The Protection Profile defines the security requirements of an SSCD for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. The SSCD represents the Target of Evaluation (TOE). The TOE may implement additional functions and security requirements for editing and displaying the data to be signed, but these additional functions and security requirements are not the subject of the Protection Profile.

The Protection Profile in CWA 14168/14169 follows the rules and formats of ISO 15408: 1999 (also known as the Common Criteria version 2.1).

According to Article 3 paragraph 4 of the Directive, appropriate public or private bodies designated by Member States shall determine the conformity of SSCDs with the requirements laid down in Annex III of the

Directive. Designated bodies should use CWA 14168/14169 as the basis for confirming that SSCDs meet the requirements. The confirmation that the requirements have been met is called “approval” in this publication.

This publication specifies guidance, the observance of which is intended to ensure that designated bodies and their evaluators and assessors operate in a consistent and reliable manner, thereby facilitating the widespread acceptance of their approvals on a national and international basis. This publication should serve as a foundation for the recognition of national systems in the interests of international trade.

3.3 Guidance on organisational structure of SSCD conformity assessment

G.5.1 The following document, prepared within the “Article 9 Committee”, has been issued by the European Commission and contains requirements for designated bodies:

Decision 2000/709/EC “Commission Decision 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.”

Designated bodies performing approval of SSCDs on the basis of CWA 14168/14169 shall comply with these Minimum Criteria. A designated body should be considered fulfilling the Minimum Criteria if it complies with the requirements of the standard EN 45011:1998.

G.5.2 The Minimum Criteria require independence of designated bodies of parties involved in designing, manufacturing, supplying, installing and maintaining SSCDs or Certification Authorities issuing certificates to the public and authorised representatives of any such parties. Such independence is a requirement of EN 45011:1998.

G.5.3 Designated bodies should independently confirm the validity of evaluation results. This independence should be maintained whether the evaluation facility is part of the same organisation as the designated body or whether the evaluation facility is an external body.

G.5.4 Evaluation facilities deployed by designated bodies for the assessment of TOE against CWA 14168/14169 should comply with the requirements of the following standard:

- EN ISO/IEC 17025: 1999 “General requirements for the competence of calibration and testing laboratories.”

G.5.5 Designated bodies should form an association to achieve the following objectives:

- a) Setting up and maintenance of co-operation to enable equivalence of evaluation, reporting and approval of Secure Signature Creation Devices throughout the EU.
- b) Providing a forum for identification of any problems of interpretation in the evaluation requirements and consultation with appropriate bodies to enable resolution.
- c) Contributing towards the maintenance of the existing standard and the preparation of revised and new standards for Secure Signature Creation Devices.
- d) Contributing to the evolution, maintenance and preparation of evaluation methods.
- e) Facilitating co-operation amongst its members without inhibiting fair and open competition between them.
- f) Providing public workshops or open meetings from time to time to facilitate the promulgation of the association’s work and to promote dialogue with manufacturers and users of SSCDs.

G.5.6 Designated bodies should make use of any interpretation material regarding the application of the CC, as and when it may become available, e.g. from the CC Editorial Board or similar bodies (such work was developed to support the mutual recognition of ITSEC and CC evaluations, under the title 'Joint Interpretation Library').

3.4 Guidance on the process of confirming SSCD conformity

G.5.7 Designated bodies should operate a scheme for the evaluation and approval of SSCDs against the requirements of CWA 14168/14169. In addition to the requirements of EN 45011: 1998, the scheme should contain the following provisions:

- a) Before accepting an application for evaluation and approval, the designated body should obtain information on a possible existing approval issued by another designated body. In the case that the SSCD has been already approved, the designated body should inform the applicant that additional approval is not required under the rules of the EU.
- b) Before accepting an application for evaluation and approval, the designated body should determine whether the SSCD would in principle be conforming to the requirements.
- c) The applicant is responsible for the preparation of the Security Target of the SSCD. Neither the designated body nor the evaluation facility should be involved in the preparation of the Security Target.
- d) The designated body should monitor all evaluations in a manner appropriate to the assurance level. Periodic meetings should be held with the evaluation facility as appropriate.
- e) The designated body should assess all evaluation results.
- f) The evaluation facility should document the observations in a final evaluation report, stating the degree to which the evaluation criteria and security functionality have or have not been met, with supporting evidence. The evaluation report is released to the designated body.
- g) The designated body should first review the evaluation report to determine whether it provides a basis for the assessment report. If applicable, the designated body should obtain additional information and evidence from the evaluation facility. The designated body should document the results of the review of the evaluation report and accompanying evidence in an assessment report. The assessment report should provide a statement on the level of conformity of the TOE with its Security Target. In addition, the assessment report should confirm the assurance level and identify any vulnerability in the TOE.
- h) The approval should confirm that the TOE meets its Security Target to the claimed level of assurance. The approval should not endorse the SSCD in any other respects.
- i) The designated body should require the holder of the approval to report to it any change of the approved SSCD, for consideration whether approval can be maintained.

G.5.8 Under the existing "Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security", participating Certification/Validating Bodies recognise Common Criteria certificates which any other participant in the CC MRA has issued. Designated bodies participating in the CC MRA should distinguish between formal CC evaluation and certification of a SSCD and issuing an approval, i.e. a statement that the SSCD conforms specifically to the requirements laid down in Annex III of Directive 1999/93/EC. This implies that a certificate issued by a participant in the CC MRA 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.

3.5 Guidance on maintaining approval

G.5.9 The approval awarded after the evaluation of the TOE is valid only for the specific version of the SSCD. SSCDs will be subject to changes (modifications, amendments, new versions) that could affect their security-relevant characteristics. The designated body should offer a scheme for maintaining approval without requiring that SSCDs be always formally re-evaluated. The scheme for maintaining approval should contain the following provisions:

- a) Organisations that design and manufacture (or control the design and manufacturing of) SSCDs can participate in the scheme. Participation is voluntary and can commence at any moment desired. Participation should not be made a prerequisite to applications for approval of SSCDs.
- b) The scheme should require that the organisation implements a documented management system for quality assurance of the design and manufacturing operations of SSCDs. A quality system that is in

accordance with ISO 9001 will satisfy the general requirements for such operations. The designated body may formulate additional requirements specific to the design and manufacturing of SSCDs. The formulation and interpretation of such additional requirements should be co-ordinated within the association of designated bodies recommended in G.5.4 above.

- c) Assessment to verify compliance with the quality assurance requirements is the responsibility of the designated body that issued the approval of the SSCD(s) in question. In order to avoid duplication of assessments, the designated body may accept either or all of the following:
 - i) existing ISO 9001 certification of the design and manufacturing organisation where the certifier is accredited to EN 45012. In this case, the designated body should not duplicate assessments against ISO 9001, but should assess the requirements specific to the design and manufacturing of SSCDs.
 - ii) existing certification of the design and manufacturing organisation by another designated body under the scheme for maintaining approval of SSCDs.
- d) The process for conducting assessment of quality assurance management systems should be based on the provisions of ISO 10011-1:1990.
- e) The designated body should carry out periodic surveillance and reassessment at sufficiently close intervals to verify that the certificated design and manufacturing organisations continue to comply with the requirements. In most cases it is unlikely that a period greater than one year for periodic surveillance would be satisfactory.
- f) The designated body should have clear procedures laying down the circumstances and conditions in which the certification of the design and manufacturing organisation will be maintained. If on surveillance or reassessment nonconformities are found to exist, the design and manufacturing organisation should effectively correct such nonconformities within a time agreed. If correction is not made within the time agreed, certification should be reduced, suspended or withdrawn. The time allowed to implement corrective action should be consistent with the severity of the nonconformity and the risk to the assurance of SSCDs meeting specified requirements.
- g) The designated body should approve any new version of the SSCD without formal re-evaluation whilst the design and manufacturing organisation holds a valid certificate under the scheme for maintaining approval, subject to the following:
 - i) the design and manufacturing organisation presents to the designated body a security impact analysis providing evidence that the changes to the SSCD have been designed and implemented in accordance with the procedures of the certified quality assurance management system,
 - ii) there are no outstanding nonconformities with the certified quality assurance management system.

G.5.10 Designated bodies offering a scheme as described in guidance G.5.8 above should comply with the requirements of the standard EN 45012:1998.

G.5.11 In case the design and manufacturing organisation does not hold a valid certificate issued under a scheme as meant in G.5.8 above, the designated body should ensure formal re-evaluation of approved SSCDs that have been changed. The re-evaluation should take the extent of the changes of the SSCDs into account; the evaluation effort may be adjusted accordingly.

Annex 1 References and bibliography

References

The following normative document contains provisions that, through reference in this text, constitute provisions of this CWA. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this CWA are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

CWA 14168	<i>Secure Electronic Signature Devices, version EAL4</i>
CWA 14169	<i>Secure Electronic Signature Devices, version EAL4+</i>

Bibliography

The following material provides supporting information:

- BSI IT-Grundschutzhandbuch "Bundesamt für Sicherheit in der Informationstechnik - IT-Grundschutzhandbuch Standard-Sicherheitsmaßnahmen", January 2000.
- CC MRA: 1998 "Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security", 5 October 1998
- CCIMB-99-031 "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model", Version 2.1, August 1999
- CCIMB-99-032 "Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements", Version 2.1, August 1999
- CCIMB-99-033 "Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements", Version 2.1, August 1999
- Decision 2000/709/EC "Commission Decision 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"
- Directive 1999/93/EC "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures"
- EA-4/06 "Interpretation of Accreditation Requirements in ISO/IEC Guide 25 and EN 45001", October 1993 (previously EAL-G5).
- EA-6/01 "EA Guidelines on the Application of EN 45011", June 1999
- EA-7/01 "EA Guidelines on the Application of EN 45012", February 1998.
- EA-7/03 "EA Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems", February 2000.
- EN 45010:1998: "General Requirements for Assessment and Accreditation of Certification/Registration Bodies" (ISO/IEC Guide 61:1996)
- EN 45011:1998: "General Requirements for Bodies Operating Product Certification Systems" (ISO/IEC Guide 65:1996)
- EN 45012:1998: "General Requirements for Bodies Operating Assessment and Certification/Registration of Quality Systems" (ISO/IEC Guide 62:1996)
- EN 45020:1998: "Standardization and Related Activities - General Vocabulary; Corrected 1998-02-26" (ISO/IEC Guide 2:1996)

- EN ISO/IEC 17025: 1999 "General requirements for the competence of calibration and testing laboratories."
- ISO 9000:2000: "Quality management systems - Fundamentals and vocabulary."
- ISO 9000-3:1997: "Quality management and quality assurance standards - Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software."
- ISO 9001:2000: "Quality management systems - Requirements."
- ISO 9004:2000: "Quality management systems - Guidelines for performance improvements."
- ISO 10011-1:1990 "Guidelines for auditing quality systems - Part 1: Auditing."
- ISO 10011-2:1991 "Guidelines for auditing quality systems - Part 2: Qualification criteria for quality system auditors."
- ISO 10011-3:1991 "Guidelines for auditing quality systems - Part 3: Management of audit programmes."
- ISO 15408-1:1999 "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model"
- ISO 15408-2:1999 "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements"
- ISO 15408-3:1999 "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements"
- ISO/IEC 17799:2000: "Information technology -- Code of practice for information security management."