



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

---

# WORKSHOP AGREEMENT

**CWA 14172-1**

July 2001

---

ICS 35.040; 35.240.60

EESSI Conformity Assessment Guidance - Part 1: General

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 14172-1:2001 E**

---

# Contents

Contents.....	2
Foreword.....	3
1 Scope.....	4
2 Definitions and abbreviations .....	5
2.1 Definitions.....	5
2.2 Abbreviations.....	6
3 Guidance on conformity assessment .....	7
Annex 1 References and bibliography.....	8

---

## 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 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 Electronic Signatures Workshop (WS/E-SIGN) 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 2001-03-15 and was successfully closed at the Workshop's plenary meeting on 2001-04-04. The final text of this CWA was submitted to CEN for publication on 2001-05-09.

The purpose of this document is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures developed under the European Electronic Signature Standardisation Initiative (EESSI) by the CEN/ISSS Workshop on Electronic Signatures and the ETSI SEC ESI Working Group. The guidance is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to these standards.

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 the rationale for the guidance on conformity assessment concerning the following services, processes, systems and products related to electronic signatures:

- Certification Authority services and processes concerning public key infrastructure management, information security management, and organisational reliability related to the life-cycle management of Qualified Certificates (Work Area C - ETSI SEC ESI WG) - ref. standard ETSI TS 101 456 V1.1.1 (2000-12) – “Policy requirements for certification authorities issuing qualified certificates”;
- Trustworthy systems managing certificates for electronic signatures, Work Area D - E-Sign - ref. CWA 14167;
- Signature creation applications, Work Area G1 - E-SIGN - ref. CWA 14170;
- Procedures for electronic signature verification, Work Area G2 - E-SIGN - ref. CWA 14171;
- Secure Signature Creation Devices (Work Area F - E-SIGN) - ref. CWA 14168 and CWA 14169.

The present series of guidance documents is applicable to independent bodies, assessors, evaluators, and testing laboratories involved in assessing conformance to the standards resulting from these work areas, as identified above. It will serve also as helpful guidance to certification-service-providers, manufacturers and operators in the development of their services, processes, systems and products. The use of these documents is intended to achieve harmonisation of interpretations of the requirements specified in the standards listed in Annex I, section ‘References’, of this document.

---

## 2 Definitions and abbreviations

### 2.1 Definitions

For the purposes of the present series of guidance documents, the following terms and definitions apply:

- Designated Body** *Any public or private body appointed by a Member State in accordance with Article 3(4) of the European Directive 1999/93/EC to which the Member State delegates responsibility for the determination of conformance of SSCDs. Such bodies neither need be nor necessarily will be Certifiers (aka Certification Bodies) or would necessarily operate in strict accordance with the Common Criteria model.*
- Process** *A series of procedures and actions that have to be conducted in order to manage and enable the provision of an electronic trust **Service**.*
- Product** *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.*
- Service** *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.*
- System** *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**.*

## 2.2 Abbreviations

For the purposes of the present series of guidance documents, the following abbreviations apply:

<i>CA</i>	Certification Authority
<i>CC</i>	Common Criteria for Information Technology Security Evaluation
<i>CC MRA</i>	Common Criteria Mutual Recognition Arrangement
<i>CEN</i>	Comité Européen de Normalisation (European Committee for Standardization)
<i>CEN/ISSS</i>	CEN Information Society Standardization System
<i>CMM</i>	Capability Maturity Model for software processes
<i>CPS</i>	Certification Practice Statement
<i>CWA</i>	CEN Workshop Agreement
<i>E-SIGN</i>	CEN/ISSS Electronic Signatures project
<i>EESSI</i>	European Electronic Signature Standardization Initiative
<i>ETSI</i>	European Telecommunications Standardization Institute
<i>ETSI SEC</i>	ETSI Security Technical Committee
<i>ETSI SEC ESI</i>	ETSI SEC Electronic Signatures and Infrastructures
<i>EU</i>	European Union
<i>ISO</i>	International Organization for Standardization
<i>QCP</i>	Qualified Certificate Policy
<i>SPICE</i>	Software Process Improvement and Capability dEtermination
<i>SSCD</i>	Secure Signature Creation Device
<i>TOE</i>	Target of Evaluation
<i>TS</i>	Technical specification
<i>WA</i>	Work Area within E-SIGN (sometimes used as 'WA-x' to identify a specific WA)
<i>WG</i>	Working Group within ETSI SEC ESI

### 3 Guidance on conformity assessment

The guidance offered by this CWA relates to four distinct subjects, each the output of a specific CEN/ISSS E-Sign WA or ETSI SEC ESI WG. In addition it makes recommendations regarding the future inclusion of one subject area the results of which were not available in time for the conclusion of this issue of the present document.

Of the four subjects explicitly addressed, the requirements for each differ, since they address different parts of the span covered by services, processes, systems and products. It is therefore appropriate that each of these areas is allocated a whole section of this CWA to facilitate their reference and extraction for application.

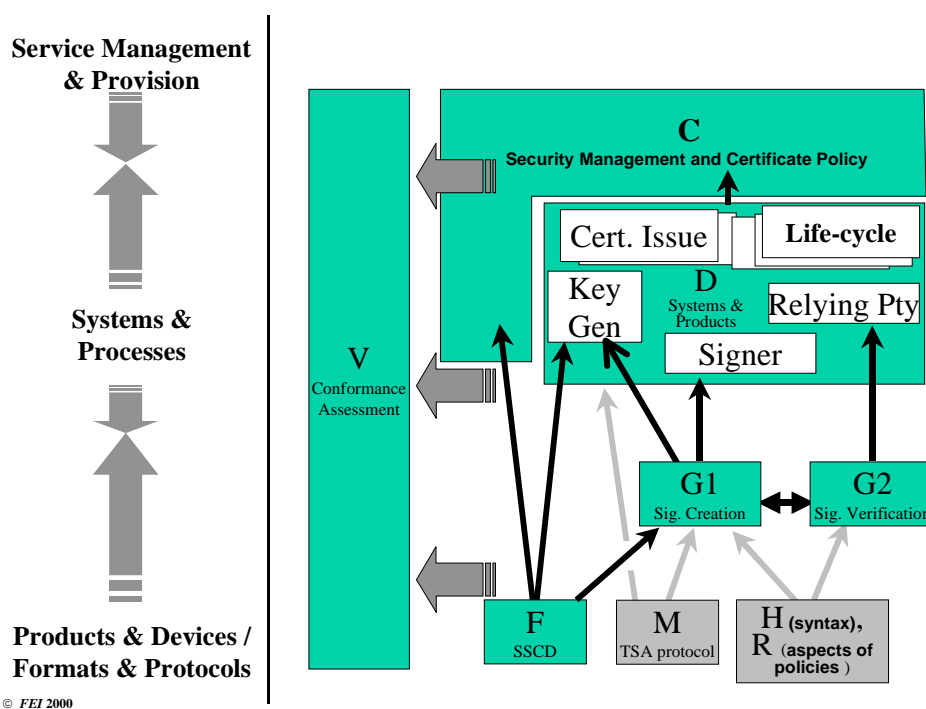
Since the ultimate focus of the EESSI programme is upon the provision of electronic trust services, the individual parts in this series of guidance documents are presented in the following additional parts:

- Part 2 - Certification Authority services and processes (Work Area 'C');
- Part 3 - Trustworthy systems managing certificates for electronic signatures (Work Area 'D');
- Part 4 (1) - Signature creation applications (Work Area 'G1');
- Part 4 (2) - Procedures for electronic signature verification (Work Area 'G2');
- Part 5 - Secure Signature Creation Devices (Work Area 'F').

in this order.

Quite apart from the sequencing implied by adopting a top-down approach, this order also reflects the actual relationships and dependencies between the different areas. One of the principles behind this conformance assessment guidance is that one specific set of guidance can support a previously defined guidance set. Thus, an assessor or evaluator addressing one of these areas should find it natural that, when a lower-level area is referenced, that area is addressed in a subsequent section.

The relationships and dependencies on which this ordering is based are shown in the following figure, those areas shown in colour being the ones within the scope of this CWA (i.e. Work Areas H, M and R are excluded).



---

## Annex 1 References and bibliography

### References

The following normative documents contain 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 14167	<i>Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures</i>
CWA 14168	<i>Secure Electronic Signature Devices, version EAL4</i>
CWA 14169	<i>Secure Electronic Signature Devices, version EAL4+</i>
CWA 14170	<i>Security Requirements for Signature Creation Applications</i>
CWA 14171	<i>Procedures for Electronic Signature Verification</i>
ETSI TS 101 456 V1.1.1 (2000-12)	<i>Policy requirements for certification authorities issuing qualified certificates</i>

### Bibliography

The following material provides supporting information.

- BSI IT-Grundschutzhandbuch "Bundesamt für Sicherheit in der Informationstechnik - IT-Grundschutzhandbuch Standard-Sicherheitsmaßnahmen", January 2000.
- C(2000) 3179 def. "Decision of the Commission of 06/11/2000 concerning 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 of 13 December 1999 on a Community framework for electronic signatures"
- 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
- CMM: "The Capability Maturity Model: Guidelines for Improving the Software Process", Carnegie Mellon University, Software Engineering Institute (Principal Contributors and Editors: Mark C. Paulk, Charles V. Weber, Bill Curtis, and Mary Beth Chrissis), ISBN 0-201-54664-7, Addison-Wesley Publishing Company, Reading, MA, 1995.
- 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 45014:1998: "General Criteria for Suppliers Declaration of Conformity (supersedes EN 45014:1989)" (ISO/IEC Guide 22:1996)
- 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."
- FIPS 140-1 "Security Requirements for Cryptographic Modules", January 1994.
- 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."
- ISO/IEC TR 15504:1998: "Information technology - Software process assessment" (9 parts), SPICE.
- RFC 2527 "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework", March 1999."