

**CEN**

**CWA 14167-4**

**WORKSHOP**

May 2004

**AGREEMENT**

---

ICS 03.120.20; 35.040

Supersedes CWA 14167-2:2002

English version

## Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

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

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



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

**Management Centre: rue de Stassart, 36 B-1050 Brussels**

— this page has intentionally been left blank —

## Foreword

This 'Cryptographic Module for CSP Signing Operations - Protection Profile' (CMCSO-PP) is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) Electronic Signatures (E-SIGN) workshop. The document represents the CEN/ISSS workshop agreement (CWA) on trustworthy systems area D2.

The document is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The document has been prepared as a Protection Profile (PP) following the rules and formats of ISO 15408, as known as the Common Criteria version 2.1 [2] [3] [4].

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document [5].

This document has been originally prepared as a single Protection Profile and approved as CWA 14167-2:2002. Afterward, while reviewing this Protection Profile for the evaluation, in order to make it conformant to the Common Criteria 2.1, two Protection Profiles have been created for the same TOE, one including the mandatory function of key backup and the other excluding this function:

- Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP), version 0.28; CWA 14167-2:2004.
- Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP), version 0.28; CWA 14167-4:2004 (this document).

The Protection Profile with the key backup function (CMCSOB-PP) keeps the original part number (Part 2). The PP without the key backup function (CMCSO-PP) gets a new part number (Part 4).

The two Protection Profiles (CMCSOB-PP and CMCSO-PP) v. 0.28 have been both successfully evaluated and certified.

This document is part of the CWA 14167 that consists of the following parts:

- Part 1: System Security Requirements;
- Part 2: Cryptographic Module for CSP Signing Operations with Backup – Protection Profile (CMCSOB-PP);
- Part 3: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP);
- Part 4: Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP).

## **CWA 14167-4:2004 (E)**

This document supersedes CWA 14167-2:2002.

The document containing the Protection Profile v. 0.28 successfully evaluated is dated 27 October 2003. That document has been updated as follows:

- modified the CEN document identifier as described above;
- removed the "draft" indication;
- updated the fields "General Status" and "Version Number" in the "1.1 Identification" section;
- modified this Foreword.

The outcome of these updates constitutes the document dated 12 January 2004 and ready for the CEN workshop voting.

After the approval by CEN workshop that document has been updated as follows:

- updated the last sentence included in the text box on the cover page;
- updated the CWA's definition in the "Terminology" section;
- modified this Foreword.

The outcome of these updates constitutes the present document, dated 02 March 2004 and ready for the official publication by CEN and DCSSI.

**This version of this CWA 14167-2:2004 was published on 2004-05-19.**

Correspondence and comments to this Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP) should be referred to:

### **CONTACT ADDRESS**

**CEN/ISSS WS/E-Sign Project Team D2**  
**Project Team Chairman: Hans Nilsson**  
**Email [hans@hansnilsson.se](mailto:hans@hansnilsson.se)**

After CWA approval the contact address will be:

*CEN/ISSS Secretariat*  
*Rue de Stassart 36*  
*1050 Brussels, Belgium*

*Tel* +32 2 550 0813  
*Fax* +32 2 550 0966

*Email* [iss@cenorm.be](mailto:iss@cenorm.be)

— this page has intentionally been left blank —

This document is a preview generated by EVS

## Revision History

### PRE-RELEASE HISTORY FOR EDITORIAL TRACKING ONLY, REPLACE FOR FINAL PP

<b>v0.04</b>	17.04.01	initial draft for Brussels kick-off meeting
<b>v0.05</b>	27.04.01	PP-skeleton resulting from kick-off meeting
<b>v0.06</b>	09.05.01	extension of skeleton
<b>v0.07</b>	11.05.01	inclusion of SFR and operations (pre-Munich meeting version)
<b>v0.08</b>	28.05.01	inclusion of Munich-meeting discussions (editing in parallel sections)
<b>v0.09</b>	03.06.01	combination of the sections to single document
<b>v0.10</b>	13.06.01	inclusion of the revised sections 2 and 3
<b>v0.11</b>	14.06.01	incorporated telephone conference results
<b>v0.12</b>	21.06.01	added SFR/SAR as generated/mapped via Sparta-tool data files version distributed for workshop comments at Sophia Antipolis meeting
<b>v0.13</b>	07.08.01	comments on v0.12 incorporate including Helmut's revisions
<b>v0.14</b>	13.08.01	revisions during Brussels D2 meeting
<b>v0.15</b>	20.08.01	incorporated comments and Brussels D2 meeting results "for public comments version" to be distributed
<b>v0.16</b>	27.08.01	Version distributed for public comments.
<b>v.017</b>	03.10.01	Version including changes according to comments and Milano meeting
<b>v.018</b>	08.11.01	minor editorial changes, "list of approved algorithms and parameters" defined under terminology
<b>v.019</b>	28.02.02	Changes according to the findings of CWA evaluator checks
<b>v0.20</b>	16.07.02	Crypto-user is replaced by Auditor in the application notes to the audit functions, rationale for O.Control_Service updated.
<b>v0.21</b>	31.01.03	Changes according to the findings of evaluation report
<b>v0.22</b>	25.02.03	Changes due to the comments of the expert group
<b>v0.23</b>	08.05.03	Backup case removed, CSP-SCD export is not allowed at any time
<b>v0.25</b>	03.06.03	Changes due to public comments in ESIGN workshop
<b>v0.26</b>	04.09.03	Changes due to the findings of evaluation report
<b>v0.27</b>	07.10.03	Editorial changes due to the evaluator's remarks
<b>v0.28</b>	27.10.03	Editorial changes due to the evaluator's remarks

— this page has intentionally been left blank —

# Table of Contents

Foreword	3
Revision History	6
Table of Contents	8
List of Tables	11
Conventions and Terminology	13
<b>Conventions</b>	<b>13</b>
<b>Terminology</b>	<b>13</b>
Document Organisation	16
1 Introduction	17
<b>1.1 Identification</b>	<b>17</b>
<b>1.2 Protection Profile Overview</b>	<b>17</b>
2 TOE Description	19
<b>2.1 TOE Roles</b>	<b>20</b>
<b>2.2 TOE Usage</b>	<b>20</b>
3 TOE Security Environment	23
<b>3.1 Assets to protect</b>	<b>23</b>
<b>3.2 Assumptions</b>	<b>23</b>
<b>3.3 Threats to Security</b>	<b>25</b>
<b>3.4 Organisational Security Policies</b>	<b>27</b>
4 Security Objectives	28
<b>4.1 Security Objectives for the TOE</b>	<b>28</b>
<b>4.2 Security Objectives for the Environment</b>	<b>29</b>
5 IT Security Requirements	31
<b>5.1 TOE Security Functional Requirements</b>	<b>31</b>
5.1.1 Security audit (FAU)	31
5.1.2 Cryptographic support (FCS)	33
5.1.3 User data protection (FDP)	34
5.1.4 Identification and authentication (FIA)	37
5.1.5 Security management (FMT)	38
5.1.6 Protection of the TOE Security Functions (FPT)	40
5.1.7 Trusted path (FTP)	43
<b>5.2 TOE Security Assurance Requirements</b>	<b>44</b>
5.2.1 Configuration management (ACM)	44
5.2.2 Delivery and operation (ADO)	45
5.2.3 Development (ADV)	46
5.2.4 Guidance documents (AGD)	49
5.2.5 Life cycle support (ALC)	50
5.2.6 Tests (ATE)	51
5.2.7 Vulnerability assessment (AVA)	52
<b>5.3 Security Requirements for the IT Environment</b>	<b>54</b>
5.3.1 Security audit (FAU)	54
5.3.2 User data protection (FDP)	54
5.3.3 Identification and authentication (FIA)	55
5.3.4 Trusted path (FPT)	56



	5.3.5	Non-IT requirements	56
6		Rationale	58
	6.1	Introduction	58
	6.2	Security Objectives Rationale	58
	6.2.1	Security Objectives Coverage	58
	6.2.2	Security Objectives Sufficiency	61
	6.3	Security Requirements Rationale	66
	6.3.1	Security Requirement Coverage	66
	6.3.2	Security Requirements Sufficiency	67
	6.4	Dependency Rationale	71
	6.4.1	Functional and Assurance Requirements Dependencies	71
	6.4.2	Justification of Unsupported Dependencies	74
	6.5	Security Requirements Grounding in Objectives	75
	6.6	Rationale for Extensions	79
	6.6.1	Rationale for Extension of Class FCS with Family FCS_RND	79
	6.7	Rationale for Assurance Level 4 Augmented	80
		References	82
		Appendix A - Acronyms	83

— this page has intentionally been left blank —

## List of Tables

Table 5.1 Assurance Requirements: EAL 4 augmented	44
Table 6-1 Security Environment to Security Objectives Mapping	58
Table 6-2 Tracing of Security Objectives to the TOE Security Environment	60
Table 6-3 Functional and Assurance Requirement to Security Objective Mapping	66
Table 6.4 Functional and Assurance Requirements Dependencies	71
Table 6-5 Requirements to Objectives Mapping	75

— this page has intentionally been left blank —

# Conventions and Terminology

## Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [2], Annex B “Specification of Protection Profiles”. Admissible cryptographic algorithms and parameters for algorithms are given in a separate document [5]. Therefore, the Protection Profile (PP) refers to [5].

## Terminology

**Administrator** means a CSP user role that performs TOE initialisation or other TOE administrative functions. These tasks are mapped to the Crypto-officer role of the TOE.

**Advanced electronic signature** (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using means that the signatory can maintain under his sole control, and
- (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

**Authentication data** is information used to verify the claimed identity of a user.

**Auditor** means a user exporting the TOE audit data and reviewing the audit data with tools in the TOE environment.

**CEN workshop agreement** (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN).

**Certificate** means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)

**CSP signature creation data** (CSP-SCD) means SCD which is used by the CSP, e.g. for the creation of advanced electronic signatures in qualified certificates or for signing certificate status information.

**CSP signature verification data** (CSP-SVD) means SVD which corresponds to the CSP-SCD and which is used to verify the advanced electronic signature in the qualified certificate or for signing certificate status information.

**Certification-service-provider** (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (defined in the Directive [1], article 2.11).

**Data to be signed** (DTBS) means the complete electronic data to be signed, such as QC content data or certificate status information.

**Data to be signed representation** (DTBS-representation) means the data sent to the TOE for signing and is

- (a) a hash-value of the DTBS or
- (b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
- (c) the DTBS itself.

The client indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the client. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.

**Digital signature** means data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO 7498-2]

**Directive** The Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1] is also referred to as the 'Directive' in the remainder of the PP.

**Dual person\_control** means a special form of access control of a task which requires two users with different identities to be authenticated and authorised to the defined roles at the time this task is to be performed.

**Hardware security module** (HSM) means the cryptographic module used to generate the advanced signature in qualified certificates and which represents the TOE.

**List of approved algorithms and parameters** means cryptographic algorithms and parameters published in [5] for electronic signatures, secure signature creation devices and trustworthy systems

**Reference authentication data** (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

**Qualified certificate** (QC) means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)

**Secure signature-creation device** (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).

**Side-channel** means illicit information flow in result of the physical behavior of the technical implementation of the TOE. Side-channels are but limited to interfaces not intended for data output like power consumption, timing of any signals and radiation. Side-channels might be enforced by influencing the TOE behavior from outside.

**Signature-creation data** (SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature. (defined in the Directive [1], article 2.4)

**Signature-verification data** (SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature. (defined in the Directive [1], article 2.7)

**SSCD provision service** means a service that prepares and provides a SSCD to subscribers.

**User** means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

**User data** means data created by and for the user that does not affect the operation of the TSF.

**Verification authentication data** (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.