



NSAI
Standards

Standard Recommendation
S.R. CWA 14167-4:2004

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

S.R. CWA 14167-4:2004

Incorporating amendments/corrigenda issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces:
CWA 14167-2:2002

This document is based on:
CWA 14167-4:2004
CWA 14167-2:2002

Published:
19 May, 2004
24 May, 2002

This document was published
under the authority of the NSAI
and comes into effect on:
24 September, 2011

ICS number:
03.120.20
35.040

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

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

S.R. CWA 14167-4:2004

CWA 14167-4:2004 (E)

—— 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).

S.R. CWA 14167-4:2004

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

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

S.R. CWA 14167-4:2004

CWA 14167-4:2004 (E)

—— this page has intentionally been left blank ——

CWA 14167-4:2004 (E)

Revision History

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

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

S.R. CWA 14167-4:2004

CWA 14167-4:2004 (E)

—— this page has intentionally been left blank ——

CWA 14167-4:2004 (E)

Table of Contents

Foreword	3
Revision History	6
Table of Contents	8
List of Tables	11
Conventions and Terminology	13
Conventions	13
Terminology	13
Document Organisation	16
1 Introduction	17
1.1 Identification	17
1.2 Protection Profile Overview	17
2 TOE Description	19
2.1 TOE Roles	20
2.2 TOE Usage	20
3 TOE Security Environment	23
3.1 Assets to protect	23
3.2 Assumptions	23
3.3 Threats to Security	25
3.4 Organisational Security Policies	27
4 Security Objectives	28
4.1 Security Objectives for the TOE	28
4.2 Security Objectives for the Environment	29
5 IT Security Requirements	31
5.1 TOE Security Functional Requirements	31
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
5.2 TOE Security Assurance Requirements	44
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
5.3 Security Requirements for the IT Environment	54
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 (FTP)	56

S.R. CWA 14167-4:2004

CWA 14167-4:2004 (E)

	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

S.R. CWA 14167-4:2004

CWA 14167-4:2004 (E)

—— 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 is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- Looking for additional Standards? Visit Intertek Inform Infostore
 - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-