National Standards Authority of Ireland

STANDARD

I.S. CWA 14167-2:2004

ICS 03.120.20;
35.040

National Standards
Authority of Ireland
Dublin 9
Ireland

Tel: (01) 807 3800
Fax: (01) 807 3838

CRYPTOGRAPHIC MODULE FOR CSP SIGNING OPERATIONS WITH BACKUP - PROTECTION PROFILE - CMCSOB PP

This Irish Standard was published under the authority of the National Standards Authority of Ireland and comes into effect on:

July 23, 2004

Price Code Y

Údarás um Chaighdeáin Náisiúnta na hÉireann

CEN

WORKSHOP

AGREEMENT

CWA 14167-2

May 2004

ICS 03.120.20; 35.040

Supersedes CWA 14167-2:2002

English version

Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB 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 with Backup - Protection Profile' (CMCSOB-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 (this document);

- Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP), version 0.28; CWA 14167-4:2004.

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).

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 with Backup (CMCSOB-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 isss@cenorm.be