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

Ref. No.:CWA 14167-2:2004 E

—— 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*

—— this page has intentionally been left blank ——

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 support is mandatory in this version CMCSOB-PP
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

—— this page has intentionally been left blank ——

Table of Contents

—— this page has intentionally been left blank ——

List of Tables

—— 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.

Backup means export of the CSP-SCD, the TSF data and the system data (backup data) sufficient to recreate the state of the TOE at the time the backup was created. Note that backup is the only function which is allowed to export CSP-SCD and only if backup package is implemented.

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.

Restore means import of the backup data to recreate the state of the TOE at the time the backup was created.

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)

Split knowledge procedure for key import is a process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key.

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.

Document Organisation

Section 1 provides the introductory material for the Protection Profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

1 Introduction

This section provides document management and overview information that is required to carry out protection profile registry. Therefore, section 1.1 “Identification” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Section 1.2 “Protection Profile Overview” summarises the PP in narrative form. As such, the section gives an overview to the potential user to decide whether the PP is of interest. It is usable as stand-alone abstract in PP catalogues and registers.

1.1 Identification

Title:	Cryptographic Module for CSP Signing Operations with backup – Protection Profile
Authors:	Wolfgang Killmann, Helmut Kurth, Herbert Leitold, Hans Nilsson
Vetting Status:	
CC Version:	2.1 Final (including final interpretations)
General Status:	Evaluated and certified
Version Number:	0.28
Registration:	
Keywords:	cryptographic module, CSP signing device, qualified certificate signing, certificate status information signing

The following final interpretation of the CCIMB related to APE criteria in CC part 3 [4] and the CEM [8] were taken into account: 008, 013, 019, 043, 049, 051, 058, 064, 065, 084, 085, 098, 138.

1.2 Protection Profile Overview

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], referred to as the ‘Directive’ in the remainder of the PP, states in Annex II that:

- *Certification-service-providers must:*
  - *(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;*
  - *(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;*

In the supporting ETSI Technical Specification "Policy Requirements for Certification Authorities (CA) [1] issuing Qualified Certificates" (ETSI TS 101 456) [6], it is stated that

- *The CA shall ensure that CA keys are generated in accordance with industry standards, and*

[1] **Note: In the remainder of this PP the term ‘Certificate Service Provider (CSP)’ is used instead of the commonly used term ‘Certification Authority (CA)’, as the former is employed by the Directive [1] this PP aims to support.**