CEN

WORKSHOP

AGREEMENT

CWA 14167-3

May 2004

ICS 03.120.20; 35.040

Supersedes CWA 14167-3:2003

English version

Cryptographic module for CSP key generation services protection profile CMCKG-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 14167-3:2004 E

—— this page has intentionally been left blank ——

Foreword

This 'Cryptographic Module for CSP Key Generation Services - Protection Profile' (CMCKG-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.

This document supersedes CWA 14167-3:2003.

The document has been prepared as a Protection Profile (PP) following the rules and formats of the Common Criteria version 2.1 [2] [3] [4]. This PP has not been evaluated.

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].

Correspondence and comments to this Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP) should be referred to:

CONTACT ADDRESS

CEN/ISSS WS/E-Sign Project Team Maintenance
Editor: Wolfgang Killmann
Email: Wolfgang.Killmann@t-systems.com

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

v0.01	17.12.01	initial draft
v0.02	15.01.02	second draft, includes drafts of chapter 3 to 5
v0.03	25.01.02	third draft, includes discussion of the Barcelona meeting
v0.04 - v0.06		working drafts
v0.07	24.07.02	draft for public comments
v0.08	13.09.02	draft with changes according to public comments
v0.09	03.06.03	editorial changes due to maintenance, adoption to draft PP CMCSO and PP CMCSOB for compatibility
v010	21.11.03	changes due to maintenance, adoption to draft PP CMCSO and PP CMCSOB for compatibility
v011	28.01.04	typos corrected, some adoption to draft PP CMCSO and PP CMCSOB for compatibility
v012	12.02.04	editorial refinements according to received comments

—— this page has intentionally been left blank ——

Table of Contents

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.

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)

Certification generation application (CGA) means a collection of application elements which requests the SVD from the device generating the SCD/SVD pair for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair, if the requested SVD has not been generated by the SCD/SVD generation device yet. The CGA verifies the authenticity of the SVD by means of

(a) the SSCD proof of correspondence between SCD and SVD and
(b) checking the sender and integrity of the received SVD.

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).