National Standards Authority of Ireland

TECHNICAL GUIDE

I.S. CWA 14172-7:2004

ICS 35.040
35.240.60

EESSI CONFORMITY ASSESSMENT GUIDANCE - PART 7: CRYPTOGRAPHIC MODULES USED BY CERTIFICATION SERVICE PROVIDERS FOR SIGNING OPERATIONS AND KEY GENERATION SERVICES

National Standards
Authority of Ireland
Dublin 9
Ireland

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

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

May 12, 2004

Price Code F

Údarás um Chaighdeáin Náisiúnta na hÉireann

CEN

WORKSHOP

AGREEMENT

CWA 14172-7

March 2004

ICS 35.040; 35.240.60

English version

EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services

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 14172-7:2004 E

Contents

Foreword

Successful implementation of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures requires standards for services, processes, systems and products related to electronic signatures as well as guidance for conformity assessment of such services, processes, systems and products.

In 1999 the European ICT Standards Board, with the support of the European Commission, undertook an initiative bringing together industry and public authorities, experts and other market players, to create the European Electronic Signature Standardisation Initiative (EESSI).

Within this framework the Comité Européen de Normalisation / Information Society Standardisation System (CEN/ISSS) and the European Telecommunications Standards Institute / Electronic Signatures and Infrastructures (ETSI/ESI) were entrusted with the execution of a work programme to develop generally recognised standards to support the implementation of Directive 1999/93/EC and development of a European electronic signature infrastructure.

The CEN/ISSS Workshop on electronic signatures (WS/E-SIGN) resulted in a set of deliverables, CEN Workshop Agreements (CWA), which contributed towards those generally recognised standards. The present document is one such CWA.

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables.

This CWA is provided as a series of discrete documents, each a part of the overall CWA, the present part being Part 7, Cryptographic modules used by Certification Service Providers for signing operations and key generation services, providing guidance on conformity assessment of cryptographic modules.

Details of all applicable parts can be found in Part 1.

This version of this CWA Part was published in 2004-03.

A list of the individuals and organizations which supported the technical consensus represented by this CEN Workshop Agreement is available to purchasers from the CEN Central Secretariat.

1 Scope

This document provides guidance on conformity assessment of cryptographic modules used by CSPs for signing operations and key generation services against the following standards:

- CWA 14167-2 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)";
- CWA 14167-3 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)";
- CWA 14167-4 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations — Protection Profile (CMCSO-PP)".

The guidance is intended for use by certification bodies, evaluators, assessors and manufacturers.