



National Standards Authority of Ireland

## TECHNICAL GUIDE

I.S. CWA 14355:2004

ICS 03.160  
35.040  
35.100.05

National Standards  
Authority of Ireland  
Dublin 9  
Ireland

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

## GUIDELINES FOR THE IMPLEMENTATION OF SECURE SIGNATURE-CREATION DEVICES

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

*May 12, 2004*

NO COPYING WITHOUT NSAI  
PERMISSION EXCEPT AS  
PERMITTED BY COPYRIGHT  
LAW

© NSAI 2004

Price Code T

Údarás um Chaighdeán Náisiúnta na hÉireann



**CEN**

**CWA 14355**

**WORKSHOP**

March 2004

**AGREEMENT**

---

**ICS 03.160; 35.040; 35.100.05**

Supersedes CWA 14355:2002

English version

## **Guidelines for the implementation of Secure Signature-Creation Devices**

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**

**CWA 14355:2004 (E)**

## Contents

	page
Contents.....	2
Foreword .....	5
1    Scope.....	6
2    References.....	7
2.1    Normative references .....	7
2.2    Informative references.....	7
3    Terms and definitions, abbreviations .....	9
3.1    Terms and definitions .....	9
3.2    Abbreviations .....	9
3.3    Document conventions.....	11
4    SSCD-related provisions of the Directive .....	12
4.1    Relevant definitions .....	12
4.2    General provisions given as recitals.....	13
4.3    Technical aspects of provisions given in Annex III.....	14
4.4    SSCD-related provisions on qualified certificates and CSP .....	16
5    Explanatory amendments to CWA 14169 .....	17
5.1    General implementation guidelines .....	17
5.1.1    SSCD overview .....	17
5.1.2    SSCD Types.....	18
5.1.2.1    SSCD Type 1 .....	18
5.1.2.2    SSCD Type 2 .....	19
5.1.2.3    SSCD Type 3 .....	19
5.1.3    TOE vs. TOE IT-environment.....	20
5.1.3.1    SSCD Type 1 and SSDC Type 2 .....	20
5.1.3.2    All SSDC Types.....	20
5.2    Guidelines on specific matters of interest.....	21
5.2.1    Inter-TSF trusted channel (FTP_ITC) and trusted path (FTP_TRP).....	21
5.2.1.1    Reasoning for selection.....	21
5.2.1.2    Implementation examples .....	22
5.2.2    TOE Emanation (FPT_EMSEC).....	22
5.2.2.1    Reasoning for selection.....	22
5.2.2.2    Logical attacks .....	23
5.2.2.3    Leakage through radiation.....	23
5.2.2.4    Leakage during cryptographic operations, power attacks.....	23
5.2.2.5    Insertion of faults, fault analysis .....	23
5.2.3    Security function policies and roles (FDP_ACC, FDP_ACF) .....	24
5.2.3.1    SSCD Type 1 .....	24
5.2.3.2    SSCD Type 2 .....	25
5.2.3.3    SSCD Type 3 .....	26
5.2.4    Transition to operational state .....	27
5.2.5    Key destruction (FCS_CKM.4) .....	28
5.2.6    Authentication failure handling (FIA_AFL) .....	28
5.3    Requests for clarification .....	28
5.3.1    Status of the SSDC PPs.....	28
5.3.2    Key generation at the CSP .....	29
5.3.3    Usage for CSP signing .....	29
5.3.4    Key recovery, key escrow, shared secrets for SSDCs .....	29
5.3.5    Signature service provision .....	30
5.3.6    SVD export/import for Type 2 .....	30
5.3.7    Cryptographic attacks.....	30
5.3.8    Authentication and identification.....	30
5.3.9    Reasonably assured.....	30

5.3.10	Management of security function behaviour (FMT_MOF.1).....	30
5.3.11	Emanation Security (FPT_EMSEC) vs. Unobservability (FPR_UNO) .....	31
6	Relation of SSCD PP to other standards.....	32
6.1	Overview of related protection profiles .....	32
6.1.1	SSCD PP.....	32
6.1.2	Eurosmart PP9911 (software and hardware) relying on PP9806 (hardware) .....	32
6.1.3	Eurosmart PP0002 "Smart Card IC Platform Protection Profile" .....	33
6.1.4	Eurosmart PP0010 "Smart Card IC with Multi-Application Secure Platform" .....	33
6.1.5	The NIST SC-user group PP-document (Version 3.0) .....	33
6.2	Evaluation aspects of SSCD as HW-SW combination.....	34
6.2.1	Requirements for hardware components .....	34
6.2.2	Division of SSCD into different components .....	35
6.2.2.1	Hardware platform.....	35
6.2.2.2	Operating system .....	35
6.2.2.3	SSCD application .....	36
6.2.3	Evaluation of the SSCD as composite device .....	36
6.2.3.1	Case 1 – Evaluation of the SSCD as an integral product.....	37
6.2.3.2	Case 2 - Evaluation of the SSCD using hardware evaluation results .....	37
6.2.3.3	Case 3 - Evaluation of the SSCD using results of hardware and operating system evaluation .....	38
7	General Platform Implementation Guidelines .....	39
7.1	SSCD and the Qualified Certificate .....	39
7.1.1	SSCD-indicator in the certificate .....	39
7.1.2	Trusted channel to the CGA.....	40
7.1.3	Certificate distribution.....	40
7.2	Implementation of SCA and SSCD .....	40
7.2.1	Class 1 SCS – SCA and SSCD share a computing engine .....	41
7.2.2	Class 2 SCS – SCA and SSCD on separate computing engines .....	41
7.3	Display limitations .....	41
7.3.1	Display message (DM) device.....	41
7.3.2	Display hash (DH) device .....	42
7.4	Use cases.....	42
7.4.1	Class 1DM System .....	42
7.4.2	Class 2DM System .....	42
7.4.3	Class 1DH System .....	42
7.4.4	Class 2DH System .....	43
8	Implementation guidelines for smartcards .....	44
8.1	SSCD platform functions .....	44
8.1.1	Personalisation .....	44
8.1.2	User authentication .....	44
8.1.3	Trusted channels and trusted path.....	44
8.2	SSCD environment.....	45
9	Implementation guidelines for mobile phones .....	46
9.1	Usage considerations .....	46
9.1.1	Displaying the complete message on the phone.....	46
9.1.2	Displaying only a hash value on the phone .....	46
9.2	SSCD platform functions .....	47
9.2.1	Personalisation .....	47
9.2.2	User authentication .....	47
9.2.3	Trusted channels and trusted path.....	47
9.3	SSCD environment.....	48
10	Implementation guidelines for PDA .....	49
10.1	Computing engine choices .....	49
10.1.1	Single Computing engine .....	49
10.1.2	Separate Computing engines.....	49
10.2	Display considerations.....	49
10.2.1	Display Message device.....	49
10.2.2	Display Hash device .....	49
10.3	User intentions.....	50

**CWA 14355:2004 (E)**

10.4	SSCD platform functions .....	50
10.4.1	Personalisation .....	50
10.4.2	User Authentication .....	50
10.4.3	Trusted Paths and Channels .....	50
11	Implementation guidelines for PCs .....	52
11.1	Computing engine choices .....	52
11.1.1	Single Computing engine .....	52
11.1.2	Separate Computing engines .....	52
11.2	Display considerations .....	52
11.2.1	Display Message device .....	52
11.2.2	Display Hash device .....	52
11.3	User intentions .....	53
11.4	SSCD platform functions .....	53
11.4.1	Personalisation .....	53
11.4.2	User Authentication .....	53
11.4.3	Trusted Paths and Channels .....	53
12	Signing Services .....	55
<b>Annex I (informative) Comparison of Protection Profiles .....</b>		56
AI.1	Security Objectives comparison .....	56
AI.1.1	SSCD vs. Eurosmart PP0010 .....	57
AI.1.1.1	Scope of TOE .....	57
AI.1.1.2	Comparison of security objectives .....	57
AI.1.2	SSCD vs. Eurosmart PP0002 .....	58
AI.1.2.1	Scope of TOE .....	58
AI.1.2.2	Comparison of security objectives .....	59
AI.1.3	SSCD vs. SCSUG .....	59
AI.1.3.1	Scope of TOE .....	59
AI.1.3.2	Comparison of security objectives .....	59
AI.2	Functional Security Requirements comparison .....	61
AI.2.1	FAU Security audit .....	61
AI.2.2	FCS Cryptographic support .....	62
AI.2.3	FDP User data protection .....	63
AI.2.4	FIA Identification and authentication .....	64
AI.2.5	FMT Security management .....	65
AI.2.6	FPR Privacy .....	66
AI.2.7	FPT Protection of the TSF .....	67
AI.2.8	FRU Resource utilisation .....	68
AI.2.9	FTP Trusted path/channels .....	68



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