



NSAI
Standards

Irish Standard
I.S. EN 419251-2:2013

Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application

I.S. EN 419251-2:2013

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard – national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation - recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces:

This document is based on:
EN 419251-2:2013

Published:
15 March, 2013

This document was published
under the authority of the NSAI
and comes into effect on:
15 March, 2013

ICS number:
35.240.15

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

EUROPEAN STANDARD

EN 419251-2

NORME EUROPÉENNE

EUROPÄISCHE NORM

March 2013

ICS 35.240.15

English Version

**Security requirements for device for authentication - Part 2:
Protection profile for extension for trusted channel to certificate
generation application**

Profils de protection pour dispositif d'authentification -
Partie 2: Dispositif avec import de clé, génération de clé et
administration; Communication sécurisée vers l'application
de génération de certificats et l'application d'administration

Sicherheitsanforderungen für Geräte zur Authentisierung -
Teil 2: Schutzprofil für Erweiterung für vertrauenswürdigen
Kanal zur Zertifikaterzeugungsanwendung

This European Standard was approved by CEN on 7 December 2012.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

	Page
Foreword.....	5
1 Scope.....	6
2 Normative references.....	6
3 Conformance.....	6
3.1 CC Conformance Claim	6
3.2 PP Claim	6
3.3 Package Claim.....	6
3.4 Conformance Rationale	6
3.5 Conformance Statement.....	6
4 Terms and definitions	7
5 Symbols and abbreviations	9
6 Overview of the target of evaluation	9
6.1 TOE Type	9
6.2 TOE Usage.....	9
6.3 Security Features of the TOE.....	9
6.4 Examples of applications.....	11
6.4.1 E-government.....	11
6.4.2 Multiple applications.....	11
6.5 Required non-TOE Hardware and Software	12
6.6 Protection Profile Usage.....	12
7 TOE Environment.....	13
7.1 Overall view	13
7.2 Personalisation application	14
7.2.1 General	14
7.2.2 Functionalities.....	14
7.2.3 Communication.....	14
7.3 Administration application	15
7.3.1 General	15
7.3.2 Functionalities.....	15
7.3.3 Communication.....	15
7.4 Authentication application.....	16
7.4.1 General	16
7.4.2 Functionalities.....	16
7.4.3 Communication.....	16
7.5 Verifier	17
7.5.1 Functionalities.....	17
7.5.2 Communication.....	17
7.6 Key Generator	17
7.6.1 Functionalities.....	17
7.6.2 Communication.....	17
7.7 Certification Authority.....	18
7.7.1 Functionalities.....	18
7.7.2 Communication.....	18
8 Life Cycle.....	19
8.1 Overview.....	19
8.2 Pre-Personalisation phase.....	20
8.3 Personalisation phase	20
8.3.1 General	20

8.3.2	Personalisation application	21
8.4	Usage phase	21
8.4.1	Authentication application	21
8.4.2	Administration application	22
8.4.3	Verifier	23
9	Security problem definition	23
9.1	Assets	23
9.1.1	General	23
9.1.2	Assets protected by the TOE	23
9.1.3	Sensitive assets of the TOE	23
9.2	Users	24
9.3	Threats	25
9.4	Organisational security policies	27
9.4.1	Provided services	27
9.4.2	Other services	27
9.5	Assumptions	28
10	Security objectives	29
10.1	General	29
10.2	Security objectives for the TOE	29
10.2.1	Provided service	29
10.2.2	Authentication to the TOE	29
10.2.3	TOE management	30
10.3	Security objectives for the operational environment	31
10.4	Rationale for Security objectives	33
11	Extended component definition – Definition of the Family FCS_RNG	38
12	Security requirements	39
12.1	General	39
12.2	Introduction	40
12.2.1	Subjects Objects and security attributes	40
12.2.2	Operations	40
12.3	Security functional requirements	41
12.3.1	General	41
12.3.2	Core	41
12.3.3	KeyImp	49
12.3.4	KeyGen	52
12.3.5	Admin	55
12.3.6	Untrusted CA	59
12.3.7	Untrusted AdminAppli	60
12.4	Security assurance requirements	61
12.5	SFR / Security objectives	61
12.6	SFR Dependencies	67
12.7	Rationale for the Assurance Requirements	69
	Bibliography	70
	Index	71

Figures

Figure 1 — TOE Security Features	13
Figure 2 — Personalisation application environment	14
Figure 3 — Administration application environment	15
Figure 4 — Authentication application environment	16
Figure 5 — TOE Life Cycle	19

Tables

Table 1 — protection of sensitive data	29
Table 2 — Security objectives vs problem definition rationale.....	34
Table 3 — Security attributes	40
Table 4 — Core security attributes	44
Table 5 — Core operations	44
Table 6 — Core security attributes - operation.....	46
Table 7 — Core security attributes - initial value.....	46
Table 8 — Core security attributes – updates.....	47
Table 9 — TSF data – updates	47
Table 10 — KeyImp security attributes.....	49
Table 11 — KeyImp security attributes - operations.....	50
Table 12 — KeyImp security attributes – update authorised roles.....	51
Table 13 — KeyImp security attributes – update values	52
Table 14 — KeyGen operations	53
Table 15 — KeyGen security attributes	53
Table 16 — KeyGen operation rules	54
Table 17 — KeyGen security attributes – update authorised roles	54
Table 18 — KeyGen security attributes – initial values	55
Table 19 — KeyGen security attributes – update values.....	55
Table 20 — Admin security attributes – update authorised roles.....	58
Table 21 — Admin security attributes – initial values	58
Table 22 — Admin security attributes – update values	58
Table 23 — Admin TSF data – operations.....	59
Table 24 — SFR vs Security objectives rationale	62
Table 25 — SFR dependencies	67

Foreword

This document (EN 419251-2:2013) has been prepared by Technical Committee CEN/TC 224 "Personal identification, electronic signature and cards and their related systems and operations", the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2013, and conflicting national standards shall be withdrawn at the latest by September 2013.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

EN 419251 contains the following parts:

- EN 419251-1, *Security requirements for device for authentication — Part 1: Protection profile for core functionality*;
- EN 419251-2, *Security requirements for device for authentication — Part 2: Protection profile for extension for trusted channel to certificate generation application* (the present document);
- EN 419251-3, *Security requirements for device for authentication — Part 3: Additional functionality for security targets*.

The present document was submitted to the Enquiry under the reference prEN 16248-2.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



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