



NSAI
Standards

Irish Standard
I.S. EN 419251-3:2013

Security requirements for device for authentication - Part 3: Additional functionality for security targets

I.S. EN 419251-3:2013

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 419251-3:2013

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

ICS 35.240.15

English Version

Security requirements for device for authentication - Part 3: Additional functionality for security targets

Profils de protection pour dispositif d'authentification -
Partie 3: Fonctionnalités additionnelles

Sicherheitsanforderungen für Geräte zur Authentisierung -
Teil 3: Zusätzliche Funktionalitäten für Sicherheitsziele

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.....	7
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.....	10
6.4 Required non-TOE Hardware and Software.....	10
6.5 Protection Profile Usage.....	10
6.6 Groups.....	10
6.6.1 General	10
6.6.2 Main groups.....	10
6.6.3 Environment groups	11
6.7 Configurations.....	13
6.7.1 General	13
6.7.2 Rules.....	13
6.7.3 Possible Configurations	14
6.8 TOE Environment.....	15
6.8.1 Overall view	15
6.8.2 Personalisation application	16
6.8.3 Administration application	17
6.8.4 Authentication application.....	18
6.8.5 Verifier	19
6.8.6 Key Generator	19
6.8.7 Certification Authority.....	20
6.8.8 Examples of applications.....	20
6.9 Life Cycle.....	22
6.9.1 Overview.....	22
6.9.2 Pre-Personalisation phase.....	23
6.9.3 Personalisation phase	23
6.9.4 Usage phase.....	24
7 Security problem definition	26
7.1 Assets.....	26
7.1.1 General	26
7.1.2 Core group.....	26
7.1.3 KeyGen group	26
7.1.4 Admin group.....	27
7.2 Users.....	27
7.2.1 Core group.....	27
7.2.2 KeyImp group.....	28

7.2.3	KeyGen group	28
7.2.4	Admin group.....	28
7.3	Threats.....	28
7.3.1	General	28
7.3.2	Core group.....	29
7.3.3	KeyGen group	30
7.3.4	Admin group.....	30
7.4	Organisational security policies.....	30
7.4.1	Core group.....	30
7.4.2	KeyGen group	31
7.4.3	Admin group.....	31
7.5	Assumptions	31
7.5.1	Core group.....	31
7.5.2	KeyGen group	32
7.5.3	Admin group.....	32
8	Security objectives.....	32
8.1	General – Transfer of sensitive data	32
8.2	Security objectives for the TOE.....	33
8.2.1	Core group.....	33
8.2.2	KeyImp group	34
8.2.3	KeyGen group	34
8.2.4	Admin group.....	34
8.2.5	Untrusted PersoAppli.....	35
8.2.6	Untrusted AuthAppli	35
8.2.7	Untrusted Verifier	35
8.2.8	Untrusted CA.....	35
8.2.9	Untrusted AdminAppli.....	35
8.3	Security objectives for the operational environment.....	36
8.3.1	Core group.....	36
8.3.2	KeyImp group	36
8.3.3	Admin group.....	37
8.3.4	Trusted PersoAppli	37
8.3.5	Trusted AuthAppli	37
8.3.6	Trusted Verifier.....	37
8.3.7	Trusted CA.....	37
8.3.8	Trusted AdminAppli	37
8.4	Rationale for Security objectives.....	38
9	Extended component definition – Definition of the Family FCS_RNG.....	43
10	Security requirements.....	43
10.1	General	43
10.2	Introduction	44
10.2.1	Subjects Objects and security attributes	44
10.2.2	Operations	45
10.3	Security functional requirements	46
10.3.1	General	46
10.3.2	Core group.....	47
10.3.3	KeyImp group	55
10.3.4	KeyGen group	58
10.3.5	Admin group.....	61
10.3.6	Untrusted PersoAppli.....	65
10.3.7	Untrusted AuthAppli	66
10.3.8	Untrusted Verifier	66
10.3.9	Untrusted CA.....	67
10.3.10	Untrusted AdminAppli.....	68
10.4	Security assurance requirements.....	68
10.5	SFR / Security objectives.....	69
10.6	SFR Dependencies	74
10.7	Rationale for the Assurance Requirements	76

Bibliography	78
Index	79

Figures

Figure 1 — TOE Security Features	15
Figure 2 — Personalisation application environment	16
Figure 3 — Administration application environment.....	17
Figure 4 — Authentication application environment.....	18
Figure 5 — TOE Life Cycle	22

Tables

Table 1 — Basic configurations.....	14
Table 2 — IdTrusted configurations	14
Table 3 — Protection of sensitive data	33
Table 4 — Security objectives vs problem definition rationale.....	38
Table 5 — Security attributes.....	45
Table 6 — Core security attributes.....	50
Table 7 — Core operations.....	50
Table 8 — Core security attributes – Operation.....	51
Table 9 — Core security attributes - initial value.....	52
Table 10 — Core security attributes – Updates	53
Table 11 — TSF data – updates	53
Table 12 — KeyImp security attributes.....	55
Table 13 — KeyImp security attributes - operations.....	56
Table 14 — KeyImp security attributes – update authorised roles.....	57
Table 15 — KeyImp security attributes – update values	58
Table 16 — KeyGen operations	59
Table 17 — KeyGen security attributes	59
Table 18 — KeyGen operation rules	60
Table 19 — KeyGen security attributes – update authorised roles.....	60
Table 20 — KeyGen security attributes – initial values	61
Table 21 — KeyGen security attributes – update values.....	61
Table 22 — Admin security attributes – update authorised roles.....	64
Table 23 — Admin security attributes – initial values	64
Table 24 — Admin security attributes – update values	64
Table 25 — Admin TSF data – operations.....	65
Table 26 — SFR vs Security objectives rationale	69
Table 27 — SFR dependencies	74

Foreword

This document (EN 419251-3:2013) 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*;
- EN 419251-3, *Security requirements for device for authentication — Part 3: Additional functionality for security targets* (the present document).

The present document was submitted to the Enquiry under the reference prEN 16248-3.

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.

1 Scope

This European Standard contains packages that define security requirements for an authentication device. This document is Part 3. Part 1 and Part 2 are Protection Profiles – PP– based on the packages defined in this document. Packages contained in this document can be added in a Security Target –ST– claiming PP of Part 1 or Part 2.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10181-2:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework*

ISO/IEC 15408-1:2009¹⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2¹⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3¹⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Conformance

3.1 CC Conformance Claim

These packages are CC Part 2 extended and CC Part 3 conformant and written according to ISO/IEC 15408-1, -2, -3 and ISO/IEC 18045.

3.2 PP Claim

These packages do not claim conformance to any other Protection Profile.

3.3 Package Claim

The evaluation assurance level for these packages is EAL4-augmented with the assurance components AVA_VAN.5 and ALC_DVS.2.

3.4 Conformance Rationale

Since these packages do not claim conformance to any other protection profile, no rationale is necessary here.

1) ISO/IEC 15408-1, -2 and -3 respectively correspond to *Common Criteria for Information Technology Security Evaluation*, Parts 1, 2 and 3.

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](#)
-