This is a free page sample. Access the full version online.

NSAI Standards

Irish Standard
I.S. EN 419251-1:2013

Security requirements for device for authentication - Part 1: Protection profile for core functionality

© CEN 2013 No copying without NSAI permission except as permitted by copyright law.

This is a free page sample. Access the full version online.

I.S. EN 419251-1:2013

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 419251-1:2013

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

This is a free page sample. Access the full version online.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 419251-1

March 2013

ICS 35.240.15

English Version

Security requirements for device for authentication - Part 1: Protection profile for core functionality

Profils de protection pour dispositif d'authentification - Partie 1: Dispositif avec import de clés

Sicherheitsanforderungen für Geräte zur Authentisierung - Teil 1: Schutzprofil für Kernfunktionalitäten

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

© 2013 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN 419251-1:2013: E

This is a free page sample. Access the full version online.

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 10
6.4.1 E-government 10
6.4.2 Multiple applications 11
6.5 Required non-TOE Hardware and Software 11
6.6 Protection Profile Usage 11

7 TOE Environment 12
7.1 Overall view 12
7.2 Personalisation application 13
7.2.1 General 13
7.2.2 Functionalities 13
7.2.3 Communication 13
7.3 Authentication application 14
7.3.1 General 14
7.3.2 Functionalities 14
7.3.3 Communication 14
7.4 Verifier 15
7.4.1 Functionalities 15
7.4.2 Communication 15
7.5 Key Generator 15
7.5.1 Functionalities 15
7.5.2 Communication 15
7.6 Certification Authority — Functionalities 15

8 Life Cycle 16
8.1 Overview 16
8.2 Pre-Personalisation phase 17
8.3 Personalisation phase 18
8.3.1 General 18
8.3.2 Personalisation application 18
8.4 Usage phase — Authentication application 18
8.4.1 General 18
8.4.2 Verifier 19

9 Security problem definition 19

This is a free page sample. Access the full version online.

9.1 Assets ... 19
9.1.1 General ... 19
9.1.2 Assets protected by the TOE ... 19
9.1.3 Sensitive assets of the TOE ... 19
9.2 Users ... 20
9.3 Threats ... 21
9.4 Organisational security policies ... 22
9.4.1 Provided services ... 22
9.4.2 Other services ... 22
9.5 Assumptions ... 23

10 Security objectives ... 24
10.1 General ... 24
10.2 Security objectives for the TOE ... 24
10.2.1 Provided service ... 24
10.2.2 Authentication to the TOE ... 24
10.2.3 TOE management ... 24
10.3 Security objectives for the operational environment ... 25
10.4 Rationale for Security objectives ... 26

11 Extended component definition ... 30

12 Security requirements ... 30
12.1 General ... 30
12.2 Introduction ... 31
12.2.1 Subjects Objects and security attributes ... 31
12.2.2 Operations ... 31
12.3 Security functional requirements ... 32
12.3.1 General ... 32
12.3.2 Core ... 32
12.3.3 KeyImp ... 40
12.4 Security assurance requirements ... 43
12.5 SFR / Security objectives ... 43
12.6 SFR Dependencies ... 46
12.7 Rationale for the Assurance Requirements ... 48
12.7.1 EAL.4 methodically designed, tested, and reviewed ... 48
12.7.2 AVA_VAN.5 Advanced methodical vulnerability analysis ... 48
12.7.3 ALC_DVS.2 Sufficiency of security measures ... 48

Bibliography ... 49

Index ... 50

Figures

Figure 1 — TOE Security Features ... 12
Figure 2 — Personalisation application environment ... 13
Figure 3 — Authentication application environment ... 14
Figure 4 — TOE Life Cycle ... 16

Tables

Table 1 — Protection of sensitive data ... 24
Table 2 — Security objectives vs problem definition rationale ... 27
Table 3 — Security attributes ... 31
Table 4 — Core security attributes ... 35
Table 5 — Core operations ... 35
Table 6 — Core security attributes - Operation ... 36

This is a free page sample. Access the full version online.

Table 7 — Core security attributes - Initial value....37
Table 8 — Core security attributes – updates....38
Table 9 — TSF data – Updates....38
Table 10 — KeyImp security attributes....40
Table 11 — KeyImp security attributes - operations....41
Table 12 — KeyImp security attributes – update authorised roles....42
Table 13 — KeyImp security attributes – Update values....43
Table 14 — SFR vs Security objectives retionale....44
Table 15 — SFR dependencies....46

This is a free page sample. Access the full version online.

Foreword

This document (EN 419251-1:2013) 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* (the present document);

— 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 was submitted to the Enquiry under the reference prEN 16248-1.

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.

SAI GLOBAL

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