



NSAI
Standards

Irish Standard Recommendation
S.R. CEN/TS 419221-2:2016

Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup

S.R. CEN/TS 419221-2:2016

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/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:

CEN/TS 419221-2:2016

Published:

2016-07-20

This document was published under the authority of the NSAI and comes into effect on:

2016-08-07

ICS number:

35.040

35.240.30

NOTE: If blank see CEN/CENELEC cover page

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

National Foreword

S.R. CEN/TS 419221-2:2016 is the adopted Irish version of the European Document CEN/TS 419221-2:2016, Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

CEN/TS 419221-2

July 2016

ICS 35.240.30; 35.040

Supersedes CWA 14167-2:2004

English Version

**Protection Profiles for TSP cryptographic modules - Part 2:
Cryptographic module for CSP signing operations with
backup**

Profils de protection pour modules cryptographiques
utilisés par les prestataires de services de confiance -
Partie 2 : Module cryptographique utilisé par le
prestataire de services de certification pour les
opérations de signature avec sauvegarde

Schutzprofile für kryptographische Module von
vertrauenswürdigen Dienstleistern - Teil 2:
Schutzprofil für CSP Signieroperationen mit Sicherung

This Technical Specification (CEN/TS) was approved by CEN on 8 May 2016 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents	Page
European foreword.....	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
4 PP Introduction.....	6
4.1 General.....	6
4.2 PP Reference.....	6
4.3 Protection Profile Overview.....	7
4.4 TOE Overview	8
4.4.1 TOE type	8
4.4.2 TOE Roles	9
4.4.3 Usage and major security features of the TOE.....	9
4.4.4 Available non-TOE hardware/software/firmware.....	11
5 Conformance Claim	11
5.1 CC Conformance Claim	11
5.2 PP Claim.....	11
5.3 Conformance Rationale.....	11
5.4 Conformance Statement	12
6 Security Problem Definition.....	12
6.1 Assets.....	12
6.1.1 General.....	12
6.1.2 TOE services.....	12
6.1.3 TOE Data.....	12
6.2 Threats.....	14
6.2.1 General.....	14
6.2.2 Threat agents.....	14
6.2.3 Threats description.....	15
6.2.4 Threats vs Threat agents.....	17
6.3 Organizational Security Policies.....	18
6.4 Assumptions.....	18
7 Security Objectives	19
7.1 General.....	19
7.2 Security Objectives for the TOE.....	19
7.3 Security Objectives for the Operational Environment	21
8 Extended Components Definitions	22
8.1 Extended Component Definitions	22
8.1.1 Family FCS_RND	22
8.1.2 Family FDP_BKP.....	23
9 Security Requirements.....	25
9.1 General.....	25
9.2 Subjects, objects, security attributes and operations	25
9.2.1 General.....	25

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](#)
-