



NSAI
Standards

Irish Standard Recommendation
S.R. CEN/TS 419221-3:2016

Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services

S.R. CEN/TS 419221-3:2016

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 419221-3:2016

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 419221-3:2016 is the adopted Irish version of the European Document CEN/TS 419221-3:2016, Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services

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 419221-3

July 2016

ICS 35.040; 35.240.30

Supersedes CWA 14167-3:2004

English Version

**Protection Profiles for TSP Cryptographic modules - Part
3: Cryptographic module for CSP key generation services**

Profils de protection pour modules cryptographiques
utilisés par les prestataires de services de confiance -
Partie 3 : Module cryptographique utilisé par le
prestataire de services de certification pour la
génération de clés

Schutzprofile für kryptographische Module von
vertrauenswürdigen Dienstleistern - Teil 3:
Kryptographisches Modul für CSP
Schlüsselgenerierungsdienste

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	3
0 Introduction	4
0.1 General	4
0.2 Document Structure	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 General	6
4.1 PP reference	6
4.2 TOE overview	6
4.2.1 TOE usage and major security features	6
4.2.2 TOE type	8
4.2.3 Available non-TOE hardware/firmware/software	8
5 Conformance Claims	8
5.1 CC conformance claim	8
5.2 PP claim	9
5.3 Conformance rationale	9
5.4 Conformance statement	9
6 Security Problem Definition	9
6.1 TOE assets	9
6.2 Threats	10
6.3 Organizational security policies	12
6.4 Assumptions	13
7 Security Objectives	13
7.1 General	13
7.2 Security objectives for the TOE	13
7.3 Security objectives for the operational environment	15
7.4 Security objectives rationale	16
8 Security Requirements	21
8.1 Security functional requirements	21
8.1.1 Subjects, objects, security attributes and operations	21
8.1.2 Security requirements operations	22
8.1.3 Security Audit (FAU)	23
8.1.4 Cryptographic Support (FCS)	24
8.1.5 User Data Protection (FDP)	25
8.1.6 Identification and Authentication (FIA)	28
8.1.7 Security Management (FMT)	29
8.1.8 Privacy (FPR)	30
8.1.9 Protection of the TSF (FPT)	31
8.1.10 Trusted path/channels (FTP)	33
8.2 Security assurance requirements	33
8.3 Security requirements rationale	34
8.3.1 Security functional requirements rationale	34
8.3.2 Security assurance requirements rationale	40
Bibliography	41

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](#)
-