



NSAI
Standards

Irish Standard
I.S. EN 419212-5:2018

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService

I.S. EN 419212-5:2018

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:

EN 419212-5:2018

Published:

2018-04-04

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

2018-04-23

ICS number:

35.240.15

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

I.S. EN 419212-5:2018 is the adopted Irish version of the European Document EN 419212-5:2018, Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService

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

For relationships with other publications refer to the NSAI web store.

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

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 419212-5

April 2018

ICS 35.240.15

Supersedes EN 419212-1:2014, EN 419212-2:2014

English Version

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService

Interface applicative des éléments sécurisés pour les services électroniques d'identification, d'authentification et de confiance - Partie 5 : Services électroniques de confiance

Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste - Teil 5: Vertrauenswürdige elektronische Dienste

This European Standard was approved by CEN on 6 February 2017.

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, Serbia, 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: Rue de la Science 23, B-1040 Brussels

Contents

	Page
European foreword.....	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
4 Abbreviations and notation.....	6
5 Additional Service Selection.....	6
6 Client/Server Authentication	10
6.1 General.....	10
6.2 Client/Server protocols	10
6.3 Steps preceding the client/server authentication	11
6.4 Padding format	11
6.4.1 PKCS #1 v 1-5 Padding.....	11
6.4.2 PKCS #1 V 2.x (PSS) Padding.....	12
6.4.3 Building the DSI on ECDSA.....	13
6.5 Client/Server protocol	13
6.5.1 General.....	13
6.5.2 Step 1 — Read certificate	14
6.5.3 Step 2 — Set signing key for client/server internal authentication	15
6.5.4 Step 3 — Internal authentication	16
6.5.5 Client/Server authentication execution flow.....	18
6.5.6 Command data field for the client server authentication	19
7 Role Authentication.....	20
7.1 Role Authentication of the card	20
7.2 Role Authentication of the server	20
7.3 Symmetrical external authentication.....	20
7.3.1 Protocol	20
7.3.2 Description of the cryptographic mechanisms	24
7.3.3 Role description.....	25
7.4 Asymmetric external authentication	25
7.4.1 Protocol based on RSA.....	25
8 Symmetric key transmission between a remote server and the ICC.....	28
8.1 Steps preceding the key transport.....	28
8.2 Key encryption with RSA	28
8.2.1 General.....	28
8.2.2 PKCS#1 v1.5 padding	30
8.2.3 OAEP padding	30
8.2.4 Execution flow	31
8.3 Diffie-Hellman key exchange for key encipherment.....	33
8.3.1 General.....	33
8.3.2 Execution flow	35
9 Signature verification	37
9.1 General.....	37
9.2 Signature verification execution flow.....	37



This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- ④ Looking for additional Standards? Visit Intertek Inform Infostore
 - ④ Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-