



**NSAI**  
Standards

Irish Standard  
I.S. EN 419212-4:2018

# Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols

I.S. EN 419212-4:2018

*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 419212-4:2018

*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 419212-4:2018 is the adopted Irish version of the European Document EN 419212-4:2018, Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols

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 419212-4**

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 4: Privacy specific Protocols**

Interface applicative des éléments sécurisés pour les services électroniques d'identification, d'authentification et de confiance - Partie 4 : Protocoles spécifiques à la protection de la vie privée

Anwendungsschnittstelle für sichere Elemente zur elektronischen Identifikation, Authentisierung und für vertrauenswürdige Dienste - Teil 4: Datenschutzspezifische Protokolle

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
<b>European foreword.....</b>	<b>3</b>
<b>Introduction .....</b>	<b>4</b>
<b>1 Scope.....</b>	<b>5</b>
<b>2 Normative references.....</b>	<b>5</b>
<b>3 Introduction.....</b>	<b>5</b>
<b>3.1 General.....</b>	<b>5</b>
<b>3.2 Auxiliary Data Comparison.....</b>	<b>6</b>
<b>3.2.1 General.....</b>	<b>6</b>
<b>3.2.2 Presentation of the auxiliary data .....</b>	<b>6</b>
<b>3.2.3 Age Verification .....</b>	<b>9</b>
<b>3.2.4 Document Validation .....</b>	<b>10</b>
<b>3.3 Restricted Identification.....</b>	<b>10</b>
<b>3.3.1 General.....</b>	<b>10</b>
<b>3.3.2 Command APDU for Step RI:1 .....</b>	<b>14</b>
<b>3.3.3 Command APDU for Step RI:2 .....</b>	<b>15</b>
<b>4 e-Services with trusted third party protocol .....</b>	<b>16</b>
<b>4.1 General.....</b>	<b>16</b>
<b>4.2 Architecture .....</b>	<b>16</b>
<b>4.3 Enhanced Role Authentication (ERA) protocol .....</b>	<b>18</b>
<b>4.4 Authentication flow steps .....</b>	<b>19</b>
<b>4.4.1 General.....</b>	<b>19</b>
<b>4.4.2 Step 1: Service selection .....</b>	<b>21</b>
<b>4.4.3 Step 2: User consent .....</b>	<b>21</b>
<b>4.4.4 Step 3 User authentication to the SP .....</b>	<b>21</b>
<b>4.4.5 Step 4 Access to the service (or go to next steps) .....</b>	<b>21</b>
<b>4.4.6 Step 5 Request for attributes (OPT) .....</b>	<b>21</b>
<b>4.4.7 Step 6 Restoration of security context (OPT).....</b>	<b>21</b>
<b>4.4.8 Step 7 User authentication to the AP (OPT).....</b>	<b>21</b>
<b>4.4.9 Step 8 Reading and providing attribute requested (OPT) .....</b>	<b>21</b>
<b>4.4.10 Step 9 Restoration of security context (OPT).....</b>	<b>21</b>
<b>4.4.11 Step 10 Ask access to the service (OPT).....</b>	<b>21</b>
<b>4.4.12 Step 11 Verification of attributes by the SP (OPT) .....</b>	<b>21</b>
<b>4.4.13 Step 12 Grant access to the service (OPT).....</b>	<b>21</b>
<b>Bibliography.....</b>	<b>22</b>



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
-