DIN EN 419212-4:2018-06 (E)

Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols; English version EN 419212-4:2018

Contents

Page

European foreword ... 3

Introduction ... 4

1 Scope ... 5

2 Normative references ... 5

3 Introduction ... 5
3.1 General ... 5
3.2 Auxiliary Data Comparison ... 6
3.2.1 General ... 6
3.2.2 Presentation of the auxiliary data ... 6
3.2.3 Age Verification ... 9
3.2.4 Document Validation ... 10
3.3 Restricted Identification ... 10
3.3.1 General ... 10
3.3.2 Command APDU for Step RI:1 ... 14
3.3.3 Command APDU for Step RI:2 ... 15

4 e-Services with trusted third party protocol ... 16
4.1 General ... 16
4.2 Architecture ... 16
4.3 Enhanced Role Authentication (ERA) protocol ... 18
4.4 Authentication flow steps ... 19
4.4.1 General ... 19
4.4.2 Step 1: Service selection ... 21
4.4.3 Step 2: User consent ... 21
4.4.4 Step 3 User authentication to the SP ... 21
4.4.5 Step 4 Access to the service (or go to next steps) ... 21
4.4.6 Step 5 Request for attributes (OPT) ... 21
4.4.7 Step 6 Restoration of security context (OPT) ... 21
4.4.8 Step 7 User authentication to the AP (OPT) ... 21
4.4.9 Step 8 Reading and providing attribute requested (OPT) ... 21
4.4.10 Step 9 Restoration of security context (OPT) ... 21
4.4.11 Step 10 Ask access to the service (OPT) ... 21
4.4.12 Step 11 Verification of attributes by the SP (OPT) ... 21
4.4.13 Step 12 Grant access to the service (OPT) ... 21

Bibliography ... 22