

DIN EN 419212-4:2016-11 (E)

Application Interface for Secure Elements for Electronic Identification,
Authentication and Trusted Services - Part 4: Privacy specific Protocols; English
version FprEN 419212-4:2016

Contents	Page
European foreword.....	4
Introduction	5
1 Scope	6
2 Normative references.....	6
3 Privacy Context functions	6
3.1 Introduction	6
3.2 Auxiliary Data Comparison.....	7
3.2.1 General.....	7
3.2.2 Presentation of the auxiliary data	7
Table 1 — Reference device authentication scheme mEAC	8
3.2.3 Age Verification	10
Table 2 — COMPARE operation — command APDU	10
Table 3 — COMPARE operation — response	10
3.2.4 Document Validation	10
Table 4 — COMPARE operation — command APDU	11
Table 5 — COMPARE operation — response	11
3.3 Restricted Identification.....	11
3.3.1 General.....	11
Table 6 — General command sequence for Restricted Identification	13
3.3.2 Command APDU for Step RI:1	15
Table 7 — Step RI:1 of Restricted Identification — command APDU	15
Table 8 — Step RI:1 of Restricted Identification — response APDU.....	15
3.3.3 Command APDU for Step RI:2	16
Table 9 — Step RI:2 of Restricted Identification — command APDU	16
Table 10 — Coding of CAPDU Tag 'AX'	16
Table 11 — Step RI:2 of Restricted Identification — response APDU	16
4 e-Services with trusted third party protocol	17
4.1 General.....	17
4.2 Architecture	17
Figure 1 — eServices with trusted third party - Architecture.....	18
4.3 Enhanced Role Authentication (ERA) protocol.....	18
Figure 2 — eServices with trusted third party - Protocol flow [TR03110P2#2.3.6].....	19
4.4 Authentication flow steps	20
4.4.1 General.....	20
Table 12 — Privacy preserving scheme	20
4.4.2 Step 1: Service selection	21

4.4.3	Step 2: User consent.....	22
4.4.4	Step 3 User authentication to the SP.....	22
4.4.5	Step 4 Access to the service (or go to next steps).....	22
4.4.6	Step 5 Request for attributes (OPT).....	22
4.4.7	Step 6 Restoration of security context (OPT)	22
4.4.8	Step 7 User authentication to the AP (OPT)	22
4.4.9	Step 8 Reading and providing attribute requested (OPT)	22
4.4.10	Step 9 Restoration of security context (OPT)	22
4.4.11	Step 10 Ask access to the service (OPT)	22
4.4.12	Step 11 Verification of attributes by the SP (OPT)	22
4.4.13	Step 12 Grant access to the service (OPT)	22
	Bibliography	23