

# 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

---

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