

# ISO/IEC 24727-2:2008-10 (E)

## Identification cards - Integrated circuit card programming interfaces - Part 2: Generic card interface

---

<b>Contents</b>		<b>Page</b>
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>Abbreviated terms .....</b>	<b>2</b>
<b>5</b>	<b>Organization for interoperability .....</b>	<b>2</b>
<b>5.1</b>	<b>Command-response pairs for interoperability .....</b>	<b>2</b>
<b>5.1.1</b>	<b>Command and response encoding .....</b>	<b>2</b>
<b>5.1.2</b>	<b>Class byte .....</b>	<b>3</b>
<b>5.1.3</b>	<b>Instruction byte .....</b>	<b>3</b>
<b>5.1.4</b>	<b>File descriptor byte .....</b>	<b>5</b>
<b>5.2</b>	<b>Card states for interoperability .....</b>	<b>6</b>
<b>5.3</b>	<b>Status words for interoperability .....</b>	<b>7</b>
<b>5.4</b>	<b>Data structures for interoperability .....</b>	<b>8</b>
<b>5.5</b>	<b>Card-applications for interoperability .....</b>	<b>9</b>
<b>5.5.1</b>	<b>Alpha card-application .....</b>	<b>9</b>
<b>5.5.2</b>	<b>Cryptographic information application .....</b>	<b>9</b>
<b>6</b>	<b>Capability descriptions .....</b>	<b>10</b>
<b>6.1</b>	<b>Card capability description (CCD) .....</b>	<b>10</b>
<b>6.2</b>	<b>Application capability description (ACD) .....</b>	<b>11</b>
<b>6.3</b>	<b>Procedural elements .....</b>	<b>11</b>
<b>6.3.1</b>	<b>Model of computation for procedural elements .....</b>	<b>12</b>
<b>6.3.2</b>	<b>Use of procedural elements .....</b>	<b>12</b>
<b>6.4</b>	<b>Determining the value of capability descriptions .....</b>	<b>13</b>
<b>6.4.1</b>	<b>General principle .....</b>	<b>13</b>
<b>6.4.2</b>	<b>Determining the value of the CCD .....</b>	<b>13</b>
<b>6.4.3</b>	<b>Determining the value of an ACD .....</b>	<b>13</b>
<b>Annex A (informative) Profiles for the cryptographic information application on the generic card interface .....</b>		<b>14</b>
<b>A.1</b>	<b>Profile A .....</b>	<b>14</b>
<b>A.1.1</b>	<b>EF.CIAInfo .....</b>	<b>14</b>
<b>A.1.2</b>	<b>EF.OD .....</b>	<b>14</b>
<b>A.1.3</b>	<b>EF.PrKD .....</b>	<b>14</b>
<b>A.1.4</b>	<b>EF.PuKD .....</b>	<b>14</b>
<b>A.1.5</b>	<b>EF.SKD .....</b>	<b>15</b>
<b>A.1.6</b>	<b>EF.CD .....</b>	<b>15</b>
<b>A.1.7</b>	<b>EF.AOD .....</b>	<b>15</b>
<b>A.1.8</b>	<b>EF.DCOD .....</b>	<b>15</b>
<b>Annex B (informative) Instances of profile A .....</b>		<b>16</b>
<b>B.1</b>	<b>eSign K Specification .....</b>	<b>16</b>
<b>Annex C (normative) Cryptographic information application for card-application service description .....</b>		<b>23</b>

<b>Annex D (informative) Example of cryptographic information application for card-application service description .....</b>	<b>28</b>
<b>Annex E (informative) DID Discovery .....</b>	<b>33</b>
<b>Bibliography .....</b>	<b>35</b>