

# ISO/IEC 7816-15:2004-01 (E)

## Identification cards - Integrated circuit cards with contacts - Part 15: Cryptographic information application

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>2</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>2</b>
<b>4</b>	<b>Symbols and abbreviated terms .....</b>	<b>5</b>
4.1	Symbols .....	5
4.2	Abbreviated terms .....	6
<b>5</b>	<b>Conventions .....</b>	<b>7</b>
<b>6</b>	<b>Cryptographic information objects .....</b>	<b>7</b>
6.1	Introduction .....	7
6.2	CIO classes .....	7
6.3	Attributes .....	8
6.4	Access restrictions .....	8
<b>7</b>	<b>CIO files .....</b>	<b>8</b>
7.1	Overview .....	8
7.2	IC card requirements .....	8
7.3	Card file structure .....	9
7.4	EF.DIR .....	9
7.5	Contents of DF.CIA .....	10
<b>8</b>	<b>Information syntax in ASN.1 .....</b>	<b>13</b>
8.1	Guidelines and encoding conventions .....	13
8.2	Basic ASN.1 defined types .....	13
8.3	The CIOChoice type .....	22
8.4	Private key information objects .....	23
8.6	Secret key information objects .....	27
8.7	Certificate information objects .....	27
8.8	Data container information objects .....	30
8.9	Authentication information objects .....	31
8.10	The cryptographic information file, EF.CIAInfo .....	35
<b>Annex A (normative) ASN.1 module .....</b>		<b>38</b>
<b>Annex B (informative) CIA example for cards with digital signature and authentication functionality .....</b>		<b>52</b>
<b>Annex C (informative) Example topologies .....</b>		<b>55</b>
<b>Annex D (informative) Examples of CIO values and their encodings .....</b>		<b>57</b>
<b>Bibliography .....</b>		<b>70</b>