

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

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

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	2
3	Terms and definitions	2
4	Symbols and abbreviated terms	5
4.1	Symbols	5
4.2	Abbreviated terms	6
5	Conventions	7
6	Cryptographic information objects	7
6.1	Introduction	7
6.2	CIO classes	7
6.3	Attributes	8
6.4	Access restrictions	8
7	CIO files	8
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
8	Information syntax in ASN.1	13
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
Annex A (normative)	ASN.1 module	38
Annex B (informative)	CIA example for cards with digital signature and authentication functionality	52
Annex C (informative)	Example topologies	55
Annex D (informative)	Examples of CIO values and their encodings	57
Bibliography		70