

ISO/IEC 7816-8:2016-11 (E)

Identification cards - Integrated circuit cards - Part 8: Commands and mechanisms for security operations

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	2
5	Interindustry commands for security operations	3
5.1	General	3
5.2	generate asymmetric key pair command	3
5.3	perform security operation command	7
5.3.1	General	7
5.3.2	compute cryptographic checksum operation	10
5.3.3	compute digital signature operation	10
5.3.4	hash operation	11
5.3.5	verify cryptographic checksum operation	11
5.3.6	verify digital signature operation	11
5.3.7	verify certificate operation	12
5.3.8	encipher operation	13
5.3.9	decipher operation	13
Annex A (informative) Examples of operations related to digital signature		14
Annex B (informative) Examples of certificates interpreted by the card		20
Annex C (informative) Examples of asymmetric key transfer		25
Annex D (informative) Alternatives to achieve the reversible change of security context		28
Annex E (informative) Example of uses for generate asymmetric key pair command		30
Bibliography		36