ISO/IEC 7816-8:2004-06 (E)

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

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviations and notation 2

5 Interindustry commands for cryptographic operations 2
5.1 GENERATE ASYMMETRIC KEY PAIR command 2
5.2 PERFORM SECURITY OPERATION command 5
5.3 COMPUTE CRYPTOGRAPHIC CHECKSUM operation 6
5.4 COMPUTE DIGITAL SIGNATURE operation 6
5.5 HASH operation 7
5.6 VERIFY CRYPTOGRAPHIC CHECKSUM operation 8
5.7 VERIFY DIGITAL SIGNATURE operation 8
5.8 VERIFY CERTIFICATE operation 9
5.9 ENCIPHER operation 9
5.10 DECIPHER operation 10

Annex A (informative) Examples of operations related to digital signature 11

Annex B (informative) Examples of certificates interpreted by the card 14

Annex C (informative) Examples of asymmetric key import/export 16

Bibliography 19