ISO/IEC 7816-8:2021 (E)

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

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Interindustry commands for security operations

- 5.1 General
- 5.2 Generate asymmetric key pair command
- 5.3 Perform security operation command
- 5.3.1 General
- 5.3.2 Compute cryptographic checksum operation
- 5.3.3 Compute digital signature operation
- 5.3.4 Hash operation
- 5.3.5 Verify cryptographic checksum operation
- 5.3.6 Verify digital signature operation
- 5.3.7 Verify certificate operation
- 5.3.8 Encipher operation
- 5.3.9 Decipher operation

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

- A.1 General
- A.2 Sequences of commands for managing a security environment
- A.3 Sequences of commands for digital signature computation
- A.4 Sequences of commands for digital signature verification
- A.5 CHA-Certificate Holder Authorization Data Object (CHA-DO)
- A.6 Compute digital signature with two subsequent signature commands
- A.7 Sequence of commands for self-descriptive card verifiable certificate verification

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

- B.1 General
- B.2 Data objects for card-verifiable certificates
- B.3 Self-descriptive card-verifiable certificates
- B.4 Non-self-descriptive card-verifiable certificates
- B.5 Self-descriptive card verifiable certificates
- B.5.1 General
- B.5.2 Certificate profile identifier
- B.5.3 Certification authority reference
- B.5.4 Public key
- B.5.5 Certificate holder reference
- B.5.6 Certificate holder authorization template
- B.5.7 Certificate effective date
- B.5.8 Certificate expiration date
- B.5.9 Certificate extension
- B.5.10 Digital signature (ECDSA)

Annex C (informative) Examples of asymmetric key transfer

C.1 Usage of the GET DATA command for public key export
C.2 Usage of the put data command for private key import
C.2.1 Example for referencing the corresponding private key
C.2.2 Example of private key import under secure conditions

Annex D (informative) Alternatives to achieve the reversible change of security context

Annex E (informative) Examples of uses for generate asymmetric key pair command

E.1 General
E.2 Example of uses for the generate asymmetric key pair command with key pair generation
E.3 Example of uses for the generate asymmetric key pair command with access to an existing public key, key reference in data field
E.4 Examples with access to an existing public key, key reference in P2

Page count: 35