ISO/IEC 25185-1:2016-01 (E)

Identification cards - Integrated circuit card authentication protocols - Part 1: Protocol for Lightweight Authentication of Identity

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Symbols and abbreviated terms 2

5 Data dictionary 3

6 Authentication Protocol Description 5
6.1 Step 1 -- INITIAL AUTHENTICATE command 6
6.2 Step 2 -- INITIAL AUTHENTICATE command evaluation 7
6.3 Step 3 -- INITIAL AUTHENTICATE response 7
6.4 Step 4 -- INITIAL AUTHENTICATE response evaluation 7
6.5 Step 5 -- FINAL AUTHENTICATE command 7
6.6 Step 6 -- FINAL AUTHENTICATE command evaluation 8
6.7 Step 7 -- FINAL AUTHENTICATE response 8
6.8 Step 8 -- FINAL AUTHENTICATE response evaluation 8

7 Application identification 9

8 Command set 9

9 Status bytes and error handling 9

10 Key diversification 10

11 Session key generation 10

12 Default mode 10

Annex A (normative) Test vectors 11

Annex B (informative) Key management policy 12

Annex C (informative) Keyset management 13

Annex D (informative) Reference implementation 14

Annex E (informative) Identity leakage considerations 15

Annex F (informative) Operational mode management 16

Annex G (informative) PLAID security features 17

Bibliography 20