DIN CEN/TS 15480-2:2012-09 (E)

Identification card systems - European Citizen Card - Part 2: Logical data structures and security services ; English version CEN/TS 15480-2:2012

Contents

Page

Foreword 4

1 Scope 5

2 Normative references 5

3 Terms and definitions 6

4 Abbreviations 7
4.1 Abbreviations 7
4.2 Coding conventions and notation 9

5 Data elements and data structures 10
5.1 Supported data Structures 10
5.2 Access to data structures 10
5.3 Answer to reset (ATR) / answer to select (ATS) 11
5.4 General architecture and file supported 15
5.5 Selection of data structures 16
5.6 Access to files 17

6 Basic card services 18
6.1 General 18
6.2 Identification 18
6.3 User verification 20
6.4 Device authentication 20
6.5 Digital signature 23
6.6 Client/Server Authentication 24
6.7 Encryption key decipherment 24

7 Extended card services 25
7.1 General 25
7.2 Biometrics - on card matching 25
7.3 Passive Authentication 25
7.4 Basic Access Control 25
7.5 Active Authentication 25
7.6 Extended Access Control 26
7.7 Role authentication 26
7.8 Restricted Identification (RI) 27
7.9 Age, Validity or Auxiliary Data Verification 28
7.10 Modular Enhanced Role Authentication (mERA) 28

Annex A (normative) Command set 29

A.1 CLASS byte coding 29
A.2 Command chaining mechanisms 29
A.3 Extended length mechanism 30
A.4 Logical channels 31
A.5 Short and extended length fields 31
A.6 Status words 31
A.7 Command set 32

Annex B (normative) Cryptographic Information Application 54

B.1 Description 54
B.2 CIA data organisation 63

Annex C (normative) Mandatory features 83

C.1 General 83
C.2 Data elements and data structures 83

DIN CEN/TS 15480-2 (DIN SPEC 91130-2):2012-09 CEN/TS 15480-2:2012 (E) C.3 Card services 84
C.4 Command set 84
C.5 Device Authentication and Key Derivation 85
C.6 Digital signature 85
C.7 Client/Server Authentication 86
C.8 Encryption Key Decipherment 86

Annex D (informative) Optional features 87

D.1 General 87
D.2 Data elements and data structures 87
D.3 Card services 88
D.4 Command set 88
D.5 Device Authentication and Key Derivation 89
D.6 Digital signature 89

Annex E (informative) Application Profiles 90

E.1 General 90
E.2 Application Profile 1: ICAO Application with EAC features 90
E.3 Application Profile 2: Travel Document Application 96
E.4 Application Profile 3: eID Application 101
E.5 Application Profile 4: Digital Signature Application 111
E.6 E.6 Application Profile 5: eServices Application using a trusted third party 121
E.7 Application Profile 6: Health Insurance Application 136
E.8 Application Profile 7: Combined eID and signature application 152
E.9 Application Profile 8: Multi-Service application 156

Annex F (informative) Access rules in expanded format 161

F.1 Object protection by access rules in expanded format 161
F.2 Access rules in expanded format 161
F.3 Security attribute referencing expanded format 162
F.4 Security attribute template for physical interfaces 163

Annex G (informative) Example of data structure: the Security Data Objects concept 164

G.1 SDO concept 164

Bibliography 176