

DIN CEN/TS 15480-3:2014-06 (E)

Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface; English version CEN/TS 15480-3:2014

Contents

Page

Foreword.....	5
1 Scope	7
2 Normative references	7
3 Terms and definitions	8
4 Symbols and abbreviations	8
5 ECC fitting in ISO/IEC 24727 model	10
5.1 ISO/IEC 24727 main features	10
5.2 General security issues – Applicable ISO/IEC 24727-4 Stack Configurations for the ECC environment	12
5.3 ECC-3 Middleware Architecture	16
5.3.1 General.....	16
5.3.2 Service Access Layer (SAL)	17
5.3.3 Generic Card Access Layer (GCAL)	17
5.3.4 Interface Device Layer and API (IFD API)	17
5.3.5 ECC-3 Stack Distribution and Connection Handling	17
5.3.6 Multi-stack composed configuration	20
5.3.7 A Web Service based architecture for ECC-3 framework.....	22
5.3.8 XML-based SAL interface	27
6 Card Discovery Mechanisms	28
6.1 General.....	28
6.2 Discovery decision tree	29
6.3 Migration path towards ECC and provision for legacy cards	29
6.3.1 General.....	29
6.3.2 Interoperable access to the Repository	30
6.4 Set of data for interoperability.....	30
6.5 Application and Card Capability Descriptors	31
6.6 ISO/IEC 7816-15 implementation.....	34
6.6.1 General.....	34
6.6.2 Profile designation within EF.DIR	34
6.6.3 ISO/IEC 24727-3 data structures mapping	35
6.6.4 ISO/IEC 24727-3 data structures storage onto the card	35
6.6.5 General discovery mechanism.....	37
6.7 Other data descriptor	39
7 Authentication protocols	39
7.1 General.....	39
7.2 Authentication Mechanisms based on ISO/IEC 24727 SAL-API	39
7.3 Asymmetric internal authentication.....	40
7.4 Asymmetric external authentication.....	40
7.5 Symmetric internal authentication.....	41
7.6 Symmetric external authentication	41
7.7 Mutual authentication with key establishment	41
7.8 Device authentication with non traceability.....	41
7.9 Key transport protocol based on RSA	41
7.10 Terminal Authentication.....	42
8 IFD-API Web Service Binding	42
9 Card-Info Structure — Introduction	42

10	XML-based Service Access Layer Interface	43
11	Federative Framework-wise Authenticate API	43
11.1	General	43
11.2	Authenticate method	44
11.3	Web Service Binding for Authenticate API	47
11.3.1	General	47
11.3.2	Authenticate.XSD definition	47
11.3.3	Authenticate.WSDL definition	48
Annex A	(informative) Interface Device Layer Architecture and Management.....	51
A.1	Scope	51
A.2	IFD-Layer Architecture.....	51
A.3	Resource Manager	52
A.3.1	General	52
A.3.2	IFD-Handlers	52
A.3.3	Card transactions	52
A.3.4	Application threads	52
A.4	Administrative functions	52
A.4.1	IFD-Handler related functions	52
A.4.2	Interface Device related functions.....	53
Annex B	(informative) IFD-API – C Language Binding.....	54
Annex C	(informative) SAL-API Post-issuance personalisation requests	60
C.1	General	60
C.2	Post-issuance personalisation requests	60
C.3	Canonical protocol	60
C.3.1	General	60
C.3.2	DataSetCreate	61
C.3.3	DSICreate.....	68
C.3.4	DIDCreate	70
C.3.5	DIDUpdate	71
C.3.6	CardApplicationServiceCreate.....	72
C.4	General recommendation and conclusion.....	74
Annex D	(informative) Additional features versus ISO/IEC 24727 (all parts).....	75
D.1	General	75
D.2	Discovery Mechanism.....	75
D.3	General Procedures (SAL).....	75
D.4	Architecture	77
D.5	Differences between IFD-API in ISO/IEC 24727-4 and ECC-3	77
D.5.1	More generale SlotCapabilityType.....	77
D.5.2	Transmit with support for batch processing	80
D.5.3	Additional error code for SignalEvent.....	82
Annex E	(informative) C-Language Binding for ExecuteSAL function	83
Annex F	(informative) Java-Language Binding for ExecuteSAL function	84
Annex G	(informative) Application Discovery Profile: card requirements to access/offer services in ISO/IEC 24727 framework.....	85
G.1	General	85
G.2	OID	85
G.3	General	85
G.4	interfaces / transport protocols	85
G.5	Data elements and data structures.....	86
G.6	Command set.....	88
G.7	Data structure of Card Applications	89
G.7.1	General	89
G.7.2	DF/ADF content	89

G.7.3	EF DCOD content.....	89
G.7.4	EF AOD content	90
G.7.5	EF SKD content.....	90
G.7.6	Ef PrKD content	90
Bibliography		91