

ISO 14906:2018 (E)

Electronic fee collection — Application interface definition for dedicated short-range communication

Contents

| | |
|---------|--|
| | Foreword |
| | Introduction |
| 1 | Scope |
| 2 | Normative references |
| 3 | Terms and definitions |
| 4 | Abbreviated terms |
| 5 | EFC application interface architecture |
| 5.1 | Relation to the DSRC communication architecture |
| 5.2 | Usage of DSRC application layer by the EFC application interface |
| 5.3 | Addressing of EFC attributes |
| 5.3.1 | Basic mechanism |
| 5.3.2 | Role of the EID |
| 5.3.3 | Multiple Instances of Attributes |
| 5.4 | Addressing of components |
| 6 | EFC Transaction Model |
| 6.1 | General |
| 6.2 | Initialisation Phase |
| 6.2.1 | Overview |
| 6.2.2 | EFC application-specific contents of the BST |
| 6.2.3 | EFC application-specific contents of the VST |
| 6.3 | Transaction phase |
| 7 | EFC functions |
| 7.1 | Overview and general concepts |
| 7.1.1 | EFC functions and service primitives |
| 7.1.2 | Overview of EFC functions |
| 7.1.3 | Handling of multiple instances |
| 7.1.4 | Security |
| 7.1.4.1 | General |
| 7.1.4.2 | Use of access credentials and authenticators |
| 7.1.4.3 | Principle of Access Credentials |
| 7.1.4.4 | Access Credentials with DES |
| 7.1.4.5 | Access Credentials with AES |
| 7.1.4.6 | Authenticator with DES |
| 7.1.4.7 | Authenticator with AES |
| 7.2 | EFC functions |
| 7.2.1 | General |
| 7.2.2 | GET_STAMPED |
| 7.2.3 | SET_STAMPED |
| 7.2.4 | GET_SECURE |
| 7.2.5 | SET_SECURE |
| 7.2.6 | GET_INSTANCE |
| 7.2.7 | SET_INSTANCE |
| 7.2.8 | GET_NONCE |
| 7.2.9 | SET_NONCE |
| 7.2.10 | TRANSFER_CHANNEL |

- 7.2.11 COPY
- 7.2.12 SET_MMI
- 7.2.13 SUBTRACT
- 7.2.14 ADD
- 7.2.15 DEBIT
- 7.2.16 CREDIT
- 7.2.17 ECHO

8 EFC Attributes

- 8.1 General
- 8.2 Data group CONTRACT
- 8.3 Data group RECEIPT
- 8.4 Data group VEHICLE
- 8.5 Data group EQUIPMENT
- 8.6 Data group DRIVER
- 8.7 Data group PAYMENT

Annex A (normative) EFC data type specifications

Annex B (informative) CARDME transaction

- B.1 General
- B.2 Overview
- B.2.1 The four phases
 - B.2.1.1 General
 - B.2.1.2 Initialisation — Say Hello
 - B.2.1.3 Presentation - Read OBE Data
 - B.2.1.4 Receipt — Write New OBE Data
 - B.2.1.5 Tracking and Closing — End the Transaction
- B.3 CARDME transaction phases
 - B.3.1 Overview
 - B.3.2 Initialisation Phase
 - B.3.3 Presentation Phase
 - B.3.3.1 General
 - B.3.3.2 Account and contract information
 - B.3.3.3 Information about the last passage
 - B.3.3.4 Vehicle classification information
 - B.3.3.5 Security related information
 - B.3.4 Optional Presentation Phase
 - B.3.5 Receipt Phase
 - B.3.6 Tracking and Closing Phases
- B.4 Bit-level specification
 - B.4.1 General
 - B.4.2 Initialisation
 - B.4.2.1 Initialisation request (BST)
 - B.4.2.2 Private window request
 - B.4.2.3 Private window allocation
 - B.4.2.4 Initialisation response (VST)
 - B.4.3 Presentation
 - B.4.3.1 Presentation request
 - B.4.3.2 Presentation response
 - B.4.4 Optional presentation
 - B.4.4.1 Optional presentation request
 - B.4.4.2 Optional presentation response
 - B.4.5 Receipt
 - B.4.5.1 Set receipt request
 - B.4.5.2 Set receipt response
 - B.4.6 Tracking and closing
 - B.4.6.1 Tracking request (ECHO.request)
 - B.4.6.2 Tracking response (ECHO.response)
 - B.4.6.3 Closing

Annex C (informative) Examples of EFC transaction types

- C.1 General
- C.2 Read only EFC transaction

- C.3 Read and write EFC transaction
- C.4 EFC purse transaction using the DEBIT function
- C.5 On-board account transaction using ICC and the TRANSFER_CHANNEL function
- C.5.1 General
- C.5.2 Overview
- C.5.2.1 General
- C.5.2.2 Preparation phase
- C.5.2.3 Initialisation phase
- C.5.2.4 Presentation phase
- C.5.2.5 Receipt phase
- C.5.2.6 Tracking and Closing phase
- C.5.3 Transaction using an ICC
- C.6 Multiple contracts EFC transactions
- C.6.1 General
- C.6.2 Case 1: Closed System Exit, National Post Paid Subscription
- C.6.3 Case 2: Closed System Exit, Local Debiting Account (Success)
- C.6.4 Case 3: Closed System Exit, Local Debiting Account (Failure)
- C.6.5 Case 4: CheckPoint

Annex D (normative) Mapping table from LatinAlphabetNo2 & 5 to LatinAlphabetNo1

Annex E (informative) Mapping table between EFC Vehicledata attribute and European registration certificate

Annex F (normative) Security calculations for DES

- F.1 General
- F.2 Attribute authenticator
- F.2.1 General
- F.2.2 Authenticator using the attribute PaymentMeans
- F.3 Calculation of Access Credentials
- F.4 Key derivation
- F.4.1 General
- F.4.2 Calculation of derived Authentication Key
- F.4.3 Calculation of the Access Key

Annex G (informative) Security computation examples for DES

- G.1 General
- G.2 Computation of Attribute Authenticator
- G.3 Computation of Access Credentials
- G.4 Key derivation
- G.4.1 Authenticator Key
- G.4.2 Access Credentials Key

Annex H (normative) Security calculations for AES

- H.1 General
- H.2 Attribute authenticator
- H.2.1 General
- H.3 Calculation of Access Credentials
- H.4 Key derivation
- H.4.1 General
- H.4.2 Calculation of a derived Authentication Key
- H.4.3 Calculation of a derived Access Key

Annex I (informative) Security computation examples for AES

- I.1 General
- I.2 Computation of Attribute Authenticator
- I.3 Computation of Access Credentials
- I.4 Key derivation
- I.4.1 Authentication Key
- I.4.2 Access Credentials Key