ISO 14906:2022-12 (E)

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

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Abbreviated terms 4

5 EFC application interface architecture 6
5.1 Relation to the DSRC communication architecture 6
5.2 Usage of DSRC application layer by the EFC application interface 8
5.3 Addressing of EFC attributes 8
5.3.1 Basic mechanism 8
5.3.2 Role of the Element Identifier (EID) 9
5.3.3 Multiple instances of Attributes 9
5.4 Addressing of components 10

6 EFC transaction model 11
6.1 General 11
6.2 Initialisation phase 11
6.2.1 Overview 11
6.2.2 EFC application-specific contents of the BST 12
6.2.3 EFC application-specific contents of the VST 13
6.3 Transaction phase 14

7 EFC functions 15
7.1 Overview and general concepts 15
7.1.1 EFC functions and service primitives 15
7.1.2 Overview of EFC functions 16
7.1.3 Handling of multiple instances 17
7.1.4 Security 19
7.2 EFC functions 22
7.2.1 General 22
7.2.2 GET_STAMPED 22
7.2.3 SET_STAMPED 23
7.2.4 GET_SECURE 24
7.2.5 SET_SECURE 25
7.2.6 GET_INSTANCE 25
7.2.7 SET_INSTANCE 26
7.2.8 GET_NONCE 27
7.2.9 SET_NONCE 28
7.2.10 TRANSFER_CHANNEL 28
7.2.11 COPY 29
7.2.12 SET_MMI 30
7.2.13 SUBTRACT 30
7.2.14 ADD 31
7.2.15 DEBIT 32

7.2.16 CREDIT 33
7.2.17 ECHO 34

8 EFC Attributes 34
8.1 General 34
8.2 Data group contract 36
8.3 Data group receipt 39
8.4 Data group vehicle 45
8.5 Data group equipment 50
8.6 Data group driver 52
8.7 Data group payment 54

Annex A (normative) EFC data type specifications 56

Annex B (informative) CARDME transaction 57

Annex C (informative) Examples of EFC transaction types 89

Annex D (informative) Mapping table from LatinAlphabetNo2, LatinCyrillicAlphabet, LatinGreekAlphabet and LatinAlphabetNo10 to LatinAlphabetNo1 101

Annex E (informative) Mapping table between EFC Vehicledata attribute and European registration certificate 102

Annex F (normative) Security calculations for DES 105

Annex G (informative) Security computation examples for DES 111

Annex H (normative) Security calculations for AES 114

Annex I (informative) Security computation examples for AES 119

Bibliography 121