ISO/TS 24534-5:2008-02 (E)

Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 5: Secure communications using symmetrical techniques

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 2

3 Terms and definitions 2

4 Symbols and abbreviations 8

5 System communications concept 9
5.1 General 9
5.2 Overview 9
5.2.1 Vehicle registration identification 9
5.2.2 System concept and supported interfaces 10
5.2.3 Roles involved 11
5.2.4 The communications context for reading 11
5.2.5 The communications context for writing 12
5.2.6 Service levels supported 12
5.3 Security services 13
5.3.1 Assumptions 13
5.3.2 Entity authentication while reading ERI data 13
5.3.3 Confidentiality while reading ERI data 13
5.3.4 Keys for authentication and confidentiality 14
5.3.5 Access control to ERI data 14
5.4 Communication architecture description 14
5.4.1 Overall communication concept for identifying vehicles 14
5.4.2 Overall communication concept for remote access 15
5.4.3 The onboard communication 15
5.5 Interfaces 16
5.5.1 The short-range air interface 16
5.5.2 The onboard interface with the ERT 17

6 Interface requirements 17
6.1 Overview 17
6.2 Abstract transaction definitions 18
6.2.1 Transaction overview 18
6.2.2 Session phases 18
6.2.3 ERI transactions and protocol data units 19
6.2.4 Mutual authentication 1 20
6.2.5 Mutual authentication 2 20
6.2.6 Get secret key ERI data 21
6.2.7 Set secret key ERI data 22
6.2.8 Commissioning secret key ERT 23
6.2.9 Decommissioning secret key ERT 23
6.2.10 Update access control list 24
6.2.11 Get ciphertext access control list entry 25

6.2.12 End of Session 26
6.3 The onboard interface to the ERT 26
6.3.1 General ERT interface requirements 26
6.3.2 An ISO 14443 interface 27
6.4 The short-range air interface 27
6.4.1 General short-range air interface requirements 27
6.4.2 The use of the DRSC application layer protocol 27
6.4.3 Lower layers 29
6.5 Remote access interface 29

Annex A (normative) ASN.1 module definitions 30

Annex B (informative) Operational scenarios 33

Annex C (normative) PICS pro forma 36

Bibliography 38