

ISO/IEC 29167-21:2026-03 (E)

Information technology - Automatic identification and data capture techniques - Part 21: Crypto suite SIMON security services for air interface communications

Contents

Page

- Foreword..... v
- Introduction..... vi
- 1 Scope..... 1
- 2 Normative references..... 1
- 3 Terms, definitions, symbols and abbreviated terms..... 1
 - 3.1 Terms and definitions..... 1
 - 3.2 Symbols..... 2
 - 3.3 Abbreviated terms..... 3
- 4 Conformance..... 3
 - 4.1 Air interface protocol specific information..... 3
 - 4.2 Interrogator conformance and obligations..... 3
 - 4.3 Tag conformance and obligations..... 4
- 5 Overview of the SIMON crypto suite..... 4
- 6 Parameter and variable descriptions..... 4
- 7 Crypto suite state diagram..... 5
- 8 Initialization and resetting..... 6
- 9 Authentication..... 6
 - 9.1 General..... 6
 - 9.2 Message and response formatting..... 7
 - 9.3 Tag authentication (AuthMethod “00”)..... 7
 - 9.3.1 General..... 7
 - 9.3.2 TAM1 message..... 7
 - 9.3.3 Intermediate Tag processing..... 8
 - 9.3.4 TAM1 response..... 8
 - 9.3.5 Final Interrogator processing..... 8
 - 9.4 Interrogator authentication (AuthMethod “01”)..... 9
 - 9.4.1 General..... 9
 - 9.4.2 IAM1 message..... 9
 - 9.4.3 Intermediate Tag processing #1..... 10
 - 9.4.4 IAM1 response..... 10
 - 9.4.5 Intermediate Interrogator processing..... 10
 - 9.4.6 IAM2 message..... 10
 - 9.4.7 Intermediate Tag processing #2..... 11
 - 9.4.8 IAM2 response..... 11
 - 9.4.9 Final Interrogator processing..... 11
 - 9.5 Mutual authentication (AuthMethod “10”)..... 12
 - 9.5.1 General..... 12
 - 9.5.2 MAM1 message..... 12
 - 9.5.3 Intermediate Tag processing #1..... 13
 - 9.5.4 MAM1 response..... 13
 - 9.5.5 Intermediate Interrogator processing..... 14
 - 9.5.6 MAM2 message..... 14
 - 9.5.7 Intermediate Tag processing #2..... 14
 - 9.5.8 MAM2 response..... 15
 - 9.5.9 Final Interrogator processing..... 15

- 10 Communication** **16**
- 10.1 General 16
- 10.2 Message and response formatting 16
- 10.3 Transforming a payload prior to encapsulation 17
 - 10.3.1 General 17
 - 10.3.2 Encapsulating an Interrogator command 18
 - 10.3.3 Cryptographically protecting a Tag reply 19
- 10.4 Processing an encapsulated or cryptographically-protected reply 20
 - 10.4.1 General 20
 - 10.4.2 Recovering an encapsulated Interrogator command 21
 - 10.4.3 Recovering a cryptographically-protected Tag response 22
- 11 Key table and key update** **22**
- Annex A (normative) Crypto suite state transitions** **23**
- Annex B (normative) Errors and error handling** **24**
- Annex C (normative) Description of SIMON and SILC v3** **25**
- Annex D (informative) Test vectors** **29**
- Annex E (normative) Protocol specific information** **40**
- Bibliography** **43**