

ISO/IEC 29167-10:2026-03 (E)

Information technology - Automatic identification and data capture techniques - Part 10: Crypto suite AES-128 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..... 2
 - 3.1 Terms and definitions..... 2
 - 3.2 Symbols..... 5
 - 3.3 Abbreviated terms..... 5
- 4 Conformance..... 6
 - 4.1 Air interface protocol specific information..... 6
 - 4.2 Interrogator conformance and obligations..... 6
 - 4.3 Tag conformance and obligations..... 6
- 5 Overview of the AES-128 crypto suite..... 7
- 6 Parameter description..... 7
- 7 Crypto suite state diagram..... 8
- 8 Initialization and resetting..... 9
- 9 Authentication..... 9
 - 9.1 General..... 9
 - 9.2 Adding custom data to authentication process..... 10
 - 9.3 Message and response formatting..... 12
 - 9.4 Tag authentication (Method “00” = TAM)..... 12
 - 9.4.1 General..... 12
 - 9.4.2 TAM1 Message..... 13
 - 9.4.3 TAM1 Response..... 13
 - 9.4.4 Final Interrogator processing TAM1..... 14
 - 9.4.5 TAM2 Message..... 14
 - 9.4.6 TAM2 Response..... 16
 - 9.4.7 Final Interrogator processing TAM2..... 19
 - 9.5 Interrogator authentication (Method “01” = IAM)..... 20
 - 9.5.1 General..... 20
 - 9.5.2 IAM1 Message..... 20
 - 9.5.3 IAM1 Response..... 20
 - 9.5.4 Final Interrogator processing IAM1..... 21
 - 9.5.5 IAM2 Message..... 21
 - 9.5.6 IAM2 Response..... 22
 - 9.5.7 Final Interrogator processing IAM2..... 22
 - 9.5.8 IAM3 Message..... 22
 - 9.5.9 IAM3 Response..... 27
 - 9.5.10 Final Interrogator processing IAM3..... 27
 - 9.6 Mutual authentication (Method “10” = MAM)..... 27
 - 9.6.1 General..... 27
 - 9.6.2 MAM1 Message..... 27
 - 9.6.3 MAM1 Response..... 28
 - 9.6.4 Final Interrogator processing MAM1..... 28

9.6.5	MAM2 Message.....	29
9.6.6	MAM2 Response.....	29
9.6.7	Final Interrogator processing MAM2.....	30
10	Communication.....	30
11	Key Table and KeyUpdate.....	30
Annex A	(normative) Crypto suite state transitions.....	32
Annex B	(normative) Error conditions and error handling.....	33
Annex C	(normative) Cipher description.....	34
Annex D	(informative) References for AES test vectors.....	38
Annex E	(normative) Protocol specific information.....	39
Annex F	(informative) Examples of <u>messages</u> and <u>responses</u> for the implementation of the TAM1, TAM2, MAM1 and MAM2.....	46
Bibliography	54