

ISO/IEC 29167-10:2017-09 (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	1
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	Introduction of the AES-128 crypto suite	6
6	Parameter definitions	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)	13
9.4.1	General	13
9.4.2	TAM1 Message	13
9.4.3	TAM1 Response	14
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	20
9.5	Interrogator authentication (Method "01" = IAM)	21
9.5.1	General	21
9.5.2	IAM1 Message	21
9.5.3	IAM1 Response	22
9.5.4	Final Interrogator processing IAM1	22
9.5.5	IAM2 Message	22
9.5.6	IAM2 Response	23
9.5.7	Final Interrogator processing IAM2	23
9.5.8	IAM3 Message	23
9.5.9	IAM3 Response	28
9.5.10	Final Interrogator processing IAM3	29
9.6	Mutual authentication (Method "10" = MAM)	29
9.6.1	General	29
9.6.2	MAM1 Message	29
9.6.3	MAM1 Response	30
9.6.4	Final Interrogator processing MAM1	30

9.6.5	MAM2 Message	30
9.6.6	MAM2 Response	31
9.6.7	Final Interrogator processing MAM2	31
10	Communication	31
11	Key Table and KeyUpdate	31
	Annex A (normative) Crypto suite state transition table	34
	Annex B (normative) Error conditions and error handling	35
	Annex C (normative) Cipher description	36
	Annex D (informative) Test vectors	40
	Annex E (normative) Protocol specific information	41
	Annex F (informative) Examples	49
	Bibliography	58