

ISO/IEC 29167-13:2026-03 (E)

Information technology - Automatic identification and data capture techniques - Part 13: Crypto suite Grain-128A security services for air interface communications

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	1
4.1	Symbols	1
4.2	Abbreviated terms	2
5	Conformance	2
5.1	Air interface protocol specific information	2
5.2	Interrogator conformance and obligations	2
5.3	Tag conformance and obligations	2
6	Overview of the Grain-128A crypto suite	3
7	Parameter description	3
8	Crypto suite state diagram	4
9	Initialization and resetting	6
10	Authentication	7
10.1	General	7
10.2	Tag authentication	8
10.2.1	General	8
10.2.2	CryptoAuthCmd(TA.1 Payload for Tag CS)	8
10.2.3	CryptoAuthResp(TA.1 Payload for Interrogator CS)	9
10.2.4	Final interrogator processing	9
10.3	Interrogator authentication	9
10.3.1	General	9
10.3.2	CryptoAuthCmd(IA.1 Payload for Tag CS)	9
10.3.3	CryptoAuthResp(IA.1 Payload for Interrogator CS)	10
10.3.4	CryptoAuthCmd(IA.2 Payload for Tag CS)	10
10.3.5	CryptoAuthResp(IA.2 Payload for Interrogator CS)	10
10.4	Mutual authentication	11
10.4.1	General	11
10.4.2	CryptoAuthCmd (MA.1 Payload for Tag CS)	11
10.4.3	CryptoAuthResp(MA.1 Payload for Interrogator CS)	11
10.4.4	CryptoAuthCmd(MA.2 Payload for Tag CS)	11
10.4.5	CryptoAuthResp(MA.2 Payload for Interrogator CS)	12
10.4.6	Final interrogator processing	12
11	Communication	12
11.1	General	12
11.2	Authenticated communication	13

11.3	Secure authenticated communication	14
12	Key table and key update	15
	Annex A (normative) State transitions	16
	Annex B (normative) Error conditions and error handling	20
	Annex C (normative) Cipher description	21
	Annex D (informative) Test vectors	24
	Annex E (normative) Protocol specific information	31
	Bibliography	39