

# ISO/IEC 29167-19:2019-06 (E)

## Information technology - Automatic identification and data capture techniques - Part 19: Crypto suite RAMON security services for air interface communications

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Conformance .....	2
4.1	Claiming conformance .....	2
4.2	Interrogator conformance and obligations .....	2
4.3	Tag conformance and obligations .....	2
5	Symbols and abbreviated terms .....	3
5.1	Symbols .....	3
5.2	Abbreviated terms .....	3
5.3	Notation .....	4
6	Crypto suite introduction .....	5
6.1	Overview .....	5
6.2	Authentication protocols .....	6
6.2.1	Tag identification .....	6
6.2.2	Symmetric mutual authentication .....	7
6.3	Send sequence counter .....	8
6.4	Session key derivation .....	9
6.4.1	General .....	9
6.4.2	KDF in counter mode .....	9
6.4.3	Key derivation scheme .....	10
6.5	IID, SID, used keys and their personalization .....	11
6.6	Key table .....	13
7	Parameter definitions .....	14
8	State diagrams .....	14
8.1	General .....	14
8.2	State diagram and transitions for Tag identification .....	15
8.2.1	General .....	15
8.2.2	Partial result mode .....	15
8.2.3	Complete result mode .....	16
8.3	State diagram and transitions for mutual authentication .....	17
8.3.1	General .....	17
8.3.2	Partial result mode .....	17
8.3.3	Complete result mode .....	18
8.3.4	Combination of complete and partial result mode .....	19
9	Initialization and resetting .....	20
10	Identification and authentication .....	20
10.1	Tag identification .....	20

10.1.1	General .....	20
10.1.2	Partial result mode .....	20
10.1.3	Complete result mode .....	20
10.2	Mutual authentication .....	21
10.2.1	General .....	21
10.2.2	Partial result mode .....	21
10.2.3	Complete result mode .....	22
10.3	The Authenticate command .....	23
10.3.1	General .....	23
10.3.2	Message formats for Tag identification .....	23
10.3.3	Message formats for Mutual Authentication .....	24
10.4	Authentication response .....	25
10.4.1	General .....	25
10.4.2	Response formats for Tag identification .....	25
10.4.3	Response formats for mutual authentication .....	26
10.4.4	Authentication error response .....	28
10.5	Determination of result modes .....	29
11	Secure communication .....	30
11.1	General .....	30
11.2	Secure communication command .....	30
11.3	Secure Communication response .....	31
11.3.1	General .....	31
11.3.2	Secure communication error response .....	31
11.4	Encoding of Read and Write commands for secure communication .....	31
11.5	Application of secure messaging primitives .....	32
11.5.1	General .....	32
11.5.2	Secure Communication command messages .....	33
11.5.3	Secure Communication response messages .....	34
11.5.4	Explanation of cipher block chaining mode .....	37
11.6	Padding for Symmetric Encryption .....	38
Annex A	(informative) State transition tables .....	39
Annex B	(informative) Error codes and error handling .....	42
Annex C	(normative) Cipher description .....	43
Annex D	(informative) Test vectors .....	53
Annex E	(informative) Protocol specifics .....	56
Annex F	(informative) Non-traceable and integrity-protected Tag identification .....	64
Annex G	(normative) Description of the TLV record .....	67
Annex H	(informative) Memory Organization for Secure UHF Tags .....	72
Bibliography	.....	76