

ISO/IEC 29167-17:2015-06 (E)

Information technology - Automatic identification and data capture techniques - Part 17: Crypto suite crypt toGPS security services for air interface communications

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Conformance	1
2.1	Claiming conformance	1
2.2	Interrogator conformance and obligations	1
2.3	Tag conformance and obligations	1
3	Normative references	2
4	Terms and definitions	2
5	Symbols and abbreviated terms	5
5.1	Symbols	5
5.2	Abbreviated terms	6
6	Cipher introduction	6
7	Parameter definitions	7
8	State diagram	8
9	Initialization and resetting	8
10	Authentication	9
10.1	Introduction	9
10.2	Tag authentication: CCR variant (Method "00" = TAM1)	10
10.3	Tag authentication: NTS variant (Method "01" = TAM2)	12
10.3.1	CCR variant (Method "00" = TAM1)	15
10.3.2	NTS variant (Method "01" = TAM2)	19
11	Communication	23
12	Key table and key update	23
Annex A (normative) State transition tables		24
Annex B (normative) Error codes and error handling		25
Annex C (normative) Cipher description		27
Annex D (informative) Test vectors		28
Annex E (normative) Protocol specific		35
Bibliography		38