

ISO/IEC TS 29167-15:2017-09 (E)

Information technology - Automatic identification and data capture techniques - Part 15: Crypto suite XOR security services for air interface communications

Contents	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms, definitions, symbols and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Symbols and abbreviated terms	2
3.2.1 Symbols	2
3.2.2 Abbreviated terms	2
4 Conformance	3
4.1 Claiming conformance	3
4.2 Interrogator conformance and obligations	3
4.3 Tag conformance and obligations	3
5 Cipher introduction	3
6 Parameter definitions	4
7 State diagram	5
8 Initialization and resetting	5
9 Authentication	6
9.1 General	6
9.2 Authentication procedure	6
9.2.1 Protocol requirements	6
9.2.2 Procedure	6
10 Secure communication (optional)	8
11 Key update (optional)	9
Annex A (normative) State transition tables	10
Annex B (normative) Error codes and error handling	11
Annex C (informative) Cipher Description	12
Annex D (informative) Test vectors	13
Annex E (normative) Protocol specific	14
Annex F (normative) Authentication procedure pseudo-code	18
Annex G (informative) Security considerations	21
Bibliography	22