

ISO/IEC 29167-16:2022-11 (E)

Information technology - Automatic identification and data capture techniques - Part 16: Crypto suite ECDSA-ECDH security services for air interface communications

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Symbols and abbreviated terms	2
4.1	Symbols	2
4.2	Abbreviated terms	2
5	Conformance	3
5.1	Claiming conformance	3
5.2	Interrogator conformance and obligations	4
5.3	Tag conformance and obligations	4
6	Cipher introduction	4
7	Parameter definitions	4
7.1	Parameter definitions	4
7.2	Certificate format	5
8	State diagram	6
9	Initialization and resetting	6
10	Authentication	7
10.1	General	7
10.2	Authenticate message	7
10.2.1	Message in Authenticate command and reply	7
10.2.2	Authenticate(MAM1.1 Message)	8
10.2.3	MAM1.1 Response	9
10.2.4	Authenticate(MAM1.2 Message)	9
10.2.5	MAM1.2 Response	10
10.3	Authentication procedure	11
10.3.1	Protocol requirements	11
10.3.2	Procedure	11
11	Communication	13
11.1	Authenticate communication	13
11.2	Secure communication	13
Annex A (normative) State transition table		15
Annex B (normative) Error codes and error handling		16
Annex C (normative) Cipher description		17

Annex D (informative) Test vectors	18
Annex E (normative) Protocol specific operation	23
Annex F (normative) Protocol message's fragmentation and defragmentation	27
Annex G (informative) Examples of ECC parameters	28
Annex H (normative) TTP involving	29
Bibliography	31