

ISO/IEC 29167-12:2015-05 (E)

Information technology - Automatic identification and data capture techniques - Part 12: Crypto suite ECC-DH security services for air interface communications

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Conformance	1
2.1	Claiming conformance	1
2.2	Interrogator conformance and obligations	1
2.3	Tag conformance and obligations	2
3	Normative references	2
4	Terms and definitions	2
5	Symbols and abbreviated terms	3
5.1	Symbols	3
5.2	Abbreviated terms	4
6	Introduction of the ECC-DH crypto suite	5
6.1	Core functionality	5
6.2	Design principles of the crypto suite	6
7	Parameter definitions	6
7.1	Elliptic curve parameters	6
7.2	Parameters of the EPIF Format	7
7.3	Random number generation	7
8	Crypto suite state diagram	7
9	Initialization and resetting	8
10	Tag Authentication	8
10.1	Introduction	8
10.2	Message and Response formatting	9
10.2.1	Concept	9
10.2.2	Description of Message and Response concept	9
10.2.3	Transmission order of the data	9
10.2.4	Parsing the Message	9
10.3	TAM1.0	10
10.3.1	TAM1.0 Message -- write certificate data	10
10.3.2	TAM1.0 Response	11
	status of write operation	11
10.3.3	Protection of certificate record	11
10.4	TAM1.1	11
10.4.1	TAM1.1 Message	11
	request certificate data	11
10.4.2	TAM1.1 Response	11

certificate data	11
10.5 TAM1.2	12
10.5.1 TAM1.2: Message	
send Interrogator challenge	12
10.5.2 TAM1.2 Response	
authentication result	12
10.6 TAM1.3	13
10.6.1 TAM1.3: Message	
request certificate data and send challenge	13
10.6.2 TAM1.3 Response	
certificate data and authentication result	13
11 Certificate memory	13
11.1 Concept	13
11.2 Certificate memory structure	14
11.3 Certificate record	15
11.4 Compressed X.509 certificate	15
11.5 X.509 certificate	17
11.6 Custom certificates	17
12 Tag authentication procedure	17
12.1 Processing steps	17
12.2 IChallenge generation and formatting	17
12.3 IChallenge examination	18
12.4 TResponse generation and formatting	18
12.5 TResponse examination	19
13 Communication	19
14 Key table and key update	20
Annex A (normative) Cryptographic suite State transition table	21
Annex B (normative) Error conditions and error handling	22
Annex C (normative) Cipher description	23
Annex D (informative) Examples ECC cryptographic protocol	25
Annex E (normative) Air Interface Protocol specific information	27
Annex F (normative) Reconstruction of X.509 Certificate	30
Bibliography	39