

ISO/IEC 13157-2:2016-04 (E)

Information technology - Telecommunications and information exchange between systems - NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Conformance	1
3	Normative references	1
4	Terms and definitions	2
5	Conventions and notations	2
5.1	Concatenation	2
5.2	Hexadecimal numbers	2
6	Acronyms	2
7	General	3
8	Protocol Identifier (PID)	3
9	Primitives	3
9.1	Key agreement	4
9.1.1	Curve P-192	4
9.1.2	EC Key Pair Generation Primitive	4
9.1.3	EC Public key validation	4
9.1.4	ECDH secret value derivation Primitive	4
9.1.5	Random nonces	4
9.2	Key Derivation Functions	5
9.2.1	KDF for the SSE	5
9.2.2	KDF for the SCH	5
9.3	Key Usage	5
9.4	Key Confirmation	6
9.4.1	Key confirmation tag generation	6
9.4.2	Key confirmation tag verification	6
9.5	Data Encryption	6
9.5.1	Initial value of counter (IV)	6
9.5.2	Encryption	6
9.5.3	Decryption	7
9.6	Data Integrity	7
9.6.1	Protect data integrity	7
9.6.2	Check data integrity	7
9.7	Message Sequence Integrity	7
10	Data Conversions	7
10.1	Integer-to-Octet-String Conversion	7
10.2	Octet-String-to-Integer Conversion	7
10.3	Point-to-Octet-String Conversion	8

10.4	Octet-String-to-Point Conversion	8
11	SSE and SCH service invocation	8
11.1	Pre-requisites	9
11.2	Key Agreement	10
11.2.1	Sender (A) Transformation	10
11.2.2	Recipient (B) Transformation	10
11.3	Key Derivation	11
11.3.1	Sender (A) Transformation	11
11.3.2	Recipient (B) Transformation	11
11.4	Key Confirmation	11
11.4.1	Sender (A) Transformation	11
11.4.2	Recipient (B) Transformation	12
12	SCH data exchange	12
12.1	Preparation	13
12.2	Data Exchange	13
12.2.1	Send	13
12.2.2	Receive	13
Annex A (normative) AES-XCBC-PRF-128 and AES-XCBC-MAC-96 algorithms		15
A.1	AES-XCBC-PRF-128	15
A.2	AES-XCBC-MAC-96	15
Annex B (normative) Fields sizes		16
Annex C (informative) Informative references		17