

ISO/IEC 13157-2:2010-04 (E)

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

Contents		Page
Foreword		iv
Introduction		v
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
9.2	Key Derivation Functions	5
9.3	Key Usage	5
9.4	Key Confirmation	6
9.5	Data Encryption	6
9.6	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	9
11.3	Key Derivation	10
11.4	Key Confirmation	11
12	SCH data exchange	12
12.1	Preparation	12
12.2	Data Exchange	12
Annex A (normative) AES-XCBC-PRF-128 and AES-XCBC-MAC-96 algorithms		14
Annex B (normative) Fields sizes		15
Annex C (informative) Informative references		16