

ISO/IEC 13157-3:2016-04 (E)

Information technology - Telecommunications and information exchange between systems - NF C Security - Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM

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
6	Acronyms	2
7	General	2
8	Protocol Identifier (PID)	2
9	Primitives	2
9.1	Key agreement	3
9.1.1	Curve P- 256	3
9.1.2	EC Key Pair Generation Primitive	3
9.1.3	EC Public key validation	3
9.1.4	ECDH secret value derivation Primitive	3
9.1.5	Random nonces	3
9.2	Key Derivation Functions	3
9.2.1	KDF for the SSE	4
9.2.2	KDF for the SCH	4
9.3	Key Usage	4
9.4	Key Confirmation	4
9.4.1	Key confirmation tag generation	5
9.4.2	Key confirmation tag verification	5
9.5	Data Authenticated Encryption	5
9.5.1	Starting Variable (StartVar)	5
9.5.2	Additional Authenticated Data (AAD)	5
9.5.3	Generation-Encryption	5
9.5.4	Decryption-Verification	5
9.6	Data Integrity	6
9.7	Message Sequence Integrity	6
10	Data Conversions	6
11	SSE and SCH service invocation	6
12	SCH data exchange	6
12.1	Preparation	6
12.2	Data Exchange	7

12.2.1	Send	7
12.2.2	Receive	7
Annex A (normative)	Fields sizes	8