

ISO/IEC 13157-4:2016-06 (E)

Information technology - Telecommunications and information exchange between systems - NFC Security - Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Conformance	1
3	Normative references	1
4	Terms and definitions	1
5	Conventions and notations	3
6	Acronyms	3
7	General	4
8	Fields and PDUs for NEAU-A	5
8.1	Protocol Identifier (PID)	5
8.2	NFC-SEC-PDUs	5
8.3	TTP involving	6
8.3.1	TTP policy and field	6
8.3.2	TTP policy negotiation	6
8.4	Entity identifiers	7
8.5	Cert field	7
8.6	Res field	7
9	Primitives	8
9.1	General requirements	8
9.2	Entity authentication	9
9.2.1	Mechanisms	9
9.2.2	EC curve	10
9.2.3	ECDSA	10
9.2.4	Certificate validation	12
9.3	Key agreement	13
9.4	Key confirmation	13
9.5	Key Derivation Function (KDF)	13
10	NEAU-A mechanism	13
10.1	Entity authentication involving a TTP	13
10.1.1	Protocol overview	13
10.1.2	Preparation	14
10.1.3	Sender (A) transformation	14
10.1.4	Recipient (B) transformation	16
10.1.5	TTP transformation	17
10.2	Entity authentication without involving a TTP	17
10.2.1	Protocol overview	17
10.2.2	Preparation	17

10.2.3	Sender (A) transformation	18
10.2.4	Recipient (B) transformation	19
10.3	Key derivation	20
10.3.1	Sender (A)	20
10.3.2	Recipient (B)	20
11	Data Authenticated Encryption in SCH	20
Annex A (normative) UDP Port 5111 and TAEP		21
A.1	UDP and port 5111	21
A.1.1	UDP	21
A.1.2	Port 5111	21
A.2	TAEP	22
A.2.1	TAEP packet format	22
A.2.2	TAEP_REQ and TAEP_RES format	22
Annex B (informative) ECDSA test vectors		24
Bibliography		27