

# ISO/IEC 13157-5:2016-06 (E)

## Information technology - Telecommunications and information exchange between systems - NFC Security - Part 5: NFC-SEC entity authentication and key agreement using symmetric cryptography

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Conformance .....	1
3	Normative references .....	1
4	Terms and definitions .....	1
5	Conventions and notations .....	2
6	Acronyms .....	3
7	General .....	3
8	Fields and PDUs for NEAU-S .....	4
8.1	Protocol Identifier (PID) .....	4
8.2	NFC-SEC-PDUs .....	4
8.3	Entity identifiers .....	4
9	Primitives .....	5
9.1	General requirements .....	5
9.2	Entity authentication .....	6
9.2.1	Mechanism .....	6
9.2.2	AES .....	6
9.2.3	Modes of operation .....	6
9.2.4	Message Authentication Code (MAC) .....	6
9.3	Key agreement .....	6
9.4	Key confirmation .....	6
9.4.1	Overview .....	6
9.4.2	Key confirmation tag generation .....	6
9.4.3	Key confirmation tag verification .....	6
9.5	Key Derivation Function (KDF) .....	7
9.5.1	Overview .....	7
9.5.2	KDF for MKA and KEIA .....	7
9.5.3	KDF for the shared secret Z .....	7
9.5.4	KDF for the SSE and SCH .....	7
9.6	Data authenticated encryption during authentication .....	8
9.6.1	Initial values (IV) .....	8
9.6.2	Additional Authenticated Data (AAD) .....	8
9.6.3	NEAU-S payload encryption and MAC generation .....	8
9.6.4	NEAU-S payload decryption and MAC verification .....	8
10	NEAU-S mechanism .....	9
10.1	Protocol overview .....	9
10.2	Preparation .....	9

<b>10.3</b>	<b>Sender (A) transformation .....</b>	<b>9</b>
<b>10.4</b>	<b>Recipient (B) transformation .....</b>	<b>10</b>
<b>11</b>	<b>Data Authenticated Encryption in SCH .....</b>	<b>11</b>