

# ISO/IEC 13157-1:2010-04 (E)

## Information technology - Telecommunications and information exchange between systems - NFC Security - Part 1: NFC-SEC NFCIP-1 security services and protocol

---

<b>Contents</b>		<b>Page</b>
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	Representation of numbers .....	2
5.2	Names .....	3
6	Acronyms .....	3
7	General .....	4
8	Services .....	4
8.1	Shared Secret Service (SSE) .....	4
8.2	Secure Channel Service (SCH) .....	5
9	Protocol Mechanisms .....	5
9.1	Key agreement .....	5
9.2	Key confirmation .....	5
9.3	PDU security .....	5
9.4	Termination .....	5
10	States and Sub-states .....	6
11	NFC-SEC-PDUs .....	7
11.1	Secure Exchange Protocol (SEP) .....	7
11.2	Protocol Identifier (PID) .....	8
11.3	NFC-SEC Payload .....	8
11.4	Terminate (TMN) .....	8
11.5	Error (ERROR) .....	8
12	Protocol Rules .....	8
12.1	Protocol and Service Errors .....	8
12.2	Interworking Rules .....	9
12.3	Sequence Integrity .....	9
12.4	Cryptographic Processing .....	9
Annex A (normative) Protocol Machine Specification .....		10
(NFCIP-1) .....		15