

ISO/IEC 13888-2:2010-12 (E)

Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques

Contents		Page
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	3
5	Notation	3
6	Requirements	4
7	Secure envelopes	5
8	Generation and verification of non-repudiation tokens	5
8.1	Creation of tokens by the TTP	5
8.2	Data items used in the non-repudiation mechanisms	5
8.3	Non-repudiation tokens	6
8.4	Verification of tokens by the TTP	7
9	Specific non-repudiation mechanisms	8
9.1	Mechanisms for non-repudiation	8
9.2	Mechanism for non-repudiation of origin	8
9.3	Mechanism for non-repudiation of delivery	9
9.4	Mechanism for obtaining a time stamping token	10
Annex A (informative) Examples of specific non-repudiation mechanisms		11
A.1	Examples of non-repudiation mechanisms of origin and delivery	11
A.2	Mechanism M1: Mandatory NRO, optional NRD	11
A.3	Mechanism M2: Mandatory NRO, mandatory NRD	13
A.4	Mechanism M3: Mandatory NRO and NRD with intermediary TTP	14
Bibliography		17