ISO/IEC 13888-3:2009-12 (E)

Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 1

5 Requirements 2

6 Trusted Third Party involvement 3

7 Digital signatures 3

8 Use of non-repudiation tokens with and without delivery authorities 4

9 Evidence produced by the end entities 4
9.1 General 4
9.2 Non-repudiation of origin 5
9.2.1 Non-repudiation of origin (NRO) token 5
9.2.2 Mechanism for non-repudiation of origin 6
9.3 Non-repudiation of delivery 6
9.3.1 Non-repudiation of delivery (NRD) token 6
9.3.2 Mechanism for non-repudiation for delivery 8

10 Evidence produced by a Delivery Authority 8
10.1 General 8
10.2 Non-repudiation of submission 9
10.2.1 Non-repudiation of submission (NRS) token 9
10.2.2 Mechanism for non-repudiation of submission 10
10.3 Non-repudiation of transport 10
10.3.1 Non-repudiation of transport (NRT) token 10
10.3.2 Mechanism for non-repudiation of transport 11
11 Mechanisms to ensure that a NR token was signed before a time t 12
11.1 General 12
11.2 Mechanism using a Time-stamping service 12
11.3 Mechanism using a Time-marking service 12

Bibliography 14