ISO/IEC 20009-2:2013-12 (E)

Information technology - Security techniques - Anonymous entity authentication - Part 2: Mechanisms based on signatures using a group public key

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 3

5 General model and requirements 4

6 Key generation process 5

7 Mechanisms without an online TTP 6
7.1 Introduction 6
7.2 Unilateral anonymous authentication 7
7.3 Mutual anonymous authentication 9
7.4 Unilateral-anonymous mutual authentication 12
7.5 Mutual anonymous authentication with binding-property 15
7.6 Unilateral-anonymous mutual authentication with binding-property 21

8 Mechanisms involving an online TTP 28
8.1 Introduction 28
8.2 Unilateral anonymous authentication 28
8.3 Mutual anonymous authentication 31
8.4 Unilateral-anonymous mutual authentication 35

9 The group membership opening process 44
9.1 General 44
9.2 The evidence evaluation process 45

10 The group signature linking process 45
10.1 General 45
10.2 Linking process with opener 45
10.3 Linking process with linking key 46
10.4 Linking process with linking base 46

Annex A (normative)Objectidentifiers 47

Annex B (informative) Information on mechanisms with binding-property 49

Bibliography 51