

ISO/IEC 20009-3:2022-02 (E)

Information security - Anonymous entity authentication - Part 3: Mechanisms based on blind signatures

Contents		Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 General model and requirements	4
6 Unilateral anonymous authentication	5
6.1 General	5
6.2 Mechanism 1 — Two-pass unilateral anonymous authentication	5
6.2.1 General	5
6.2.2 Requirements	5
6.2.3 Domain parameters generation process	6
6.2.4 Key generation process	6
6.2.5 Credential issuance process	7
6.2.6 Authentication process	8
Annex A (normative) Object identifiers	10
Annex B (informative) Conversion functions	11
Annex C (informative) Group description	12
Annex D (informative) Special hash-functions	13
Annex E (informative) Security considerations	15
Bibliography	16