

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

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

---

<b>Contents</b>		<b>Page</b>
<b>Foreword</b>	.....	<b>iv</b>
<b>Introduction</b>	.....	<b>v</b>
<b>1 Scope</b>	.....	<b>1</b>
<b>2 Normative references</b>	.....	<b>1</b>
<b>3 Terms and definitions</b>	.....	<b>1</b>
<b>4 Symbols and abbreviated terms</b>	.....	<b>3</b>
<b>5 General model and requirements</b>	.....	<b>4</b>
<b>6 Unilateral anonymous authentication</b>	.....	<b>5</b>
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
<b>Annex A (normative) Object identifiers</b>	.....	<b>10</b>
<b>Annex B (informative) Conversion functions</b>	.....	<b>11</b>
<b>Annex C (informative) Group description</b>	.....	<b>12</b>
<b>Annex D (informative) Special hash-functions</b>	.....	<b>13</b>
<b>Annex E (informative) Security considerations</b>	.....	<b>15</b>
<b>Bibliography</b>	.....	<b>16</b>