

# ISO/IEC 9798-2:2008-12 (E)

## Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms

---

<b>Contents</b>		<b>Page</b>
<b>Foreword</b> .....		<b>iv</b>
<b>1</b> <b>Scope</b> .....		<b>1</b>
<b>2</b> <b>Normative references</b> .....		<b>1</b>
<b>3</b> <b>Terms and definitions</b> .....		<b>2</b>
<b>4</b> <b>Symbols and notation</b> .....		<b>3</b>
<b>5</b> <b>Requirements</b> .....		<b>3</b>
<b>6</b> <b>Mechanisms not involving a trusted third party</b> .....		<b>4</b>
<b>6.1</b> <b>Unilateral authentication</b> .....		<b>4</b>
<b>6.1.1</b> <b>Mechanism 1 -- One-pass authentication</b> .....		<b>5</b>
<b>6.1.2</b> <b>Mechanism 2 -- Two-pass authentication</b> .....		<b>5</b>
<b>6.2</b> <b>Mutual authentication</b> .....		<b>6</b>
<b>6.2.1</b> <b>Mechanism 3 -- Two-pass authentication</b> .....		<b>6</b>
<b>6.2.2</b> <b>Mechanism 4 -- Three-pass authentication</b> .....		<b>7</b>
<b>7</b> <b>Mechanisms involving a trusted third party</b> .....		<b>8</b>
<b>7.1</b> <b>Mechanism 5 -- Four-pass authentication</b> .....		<b>8</b>
<b>7.2</b> <b>Mechanism 6 -- Five-pass authentication</b> .....		<b>10</b>
<b>Annex A (normative) OIDs and ASN.1 syntax</b> .....		<b>12</b>
<b>Annex B (informative) Use of text fields</b> .....		<b>14</b>
<b>Annex C (informative) Properties of entity authentication mechanisms</b> .....		<b>15</b>
<b>Bibliography</b> .....		<b>16</b>