

# ISO/IEC 13888-2:2010-12 (E)

## Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques

---

<b>Contents</b>		<b>Page</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>1</b>
<b>4</b>	<b>Symbols and abbreviated terms .....</b>	<b>3</b>
<b>5</b>	<b>Notation .....</b>	<b>3</b>
<b>6</b>	<b>Requirements .....</b>	<b>4</b>
<b>7</b>	<b>Secure envelopes .....</b>	<b>5</b>
<b>8</b>	<b>Generation and verification of non-repudiation tokens .....</b>	<b>5</b>
<b>8.1</b>	<b>Creation of tokens by the TTP .....</b>	<b>5</b>
<b>8.2</b>	<b>Data items used in the non-repudiation mechanisms .....</b>	<b>5</b>
<b>8.3</b>	<b>Non-repudiation tokens .....</b>	<b>6</b>
<b>8.4</b>	<b>Verification of tokens by the TTP .....</b>	<b>7</b>
<b>9</b>	<b>Specific non-repudiation mechanisms .....</b>	<b>8</b>
<b>9.1</b>	<b>Mechanisms for non-repudiation .....</b>	<b>8</b>
<b>9.2</b>	<b>Mechanism for non-repudiation of origin .....</b>	<b>8</b>
<b>9.3</b>	<b>Mechanism for non-repudiation of delivery .....</b>	<b>9</b>
<b>9.4</b>	<b>Mechanism for obtaining a time stamping token .....</b>	<b>10</b>
<b>Annex A (informative) Examples of specific non-repudiation mechanisms .....</b>		<b>11</b>
<b>A.1</b>	<b>Examples of non-repudiation mechanisms of origin and delivery .....</b>	<b>11</b>
<b>A.2</b>	<b>Mechanism M1: Mandatory NRO, optional NRD .....</b>	<b>11</b>
<b>A.3</b>	<b>Mechanism M2: Mandatory NRO, mandatory NRD .....</b>	<b>13</b>
<b>A.4</b>	<b>Mechanism M3: Mandatory NRO and NRD with intermediary TTP .....</b>	<b>14</b>
<b>Bibliography .....</b>		<b>17</b>