

# ISO/IEC 11770-4:2006-05 (E)

## Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>2</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>2</b>
<b>4</b>	<b>Symbols and notation .....</b>	<b>6</b>
<b>5</b>	<b>Requirements .....</b>	<b>8</b>
<b>6</b>	<b>Password-authenticated key agreement 9 6.1 Key Agreement Mechanism 1 .....</b>	<b>10</b>
6.1.1	Prior shared parameters .....	10
6.1.2	Functions .....	10
6.1.3	Key agreement operation .....	12
<b>6.2</b>	<b>Key Agreement Mechanism 2 .....</b>	<b>13</b>
6.2.1	Prior shared parameters .....	14
6.2.2	Functions .....	14
6.2.3	Key agreement operation .....	16
<b>6.3</b>	<b>Key Agreement Mechanism 3 .....</b>	<b>17</b>
6.3.1	Prior shared parameters .....	17
6.3.2	Functions .....	17
6.3.3	Key agreement operation .....	20
<b>7</b>	<b>Password-authenticated key retrieval .....</b>	<b>21</b>
<b>7.1</b>	<b>Key Retrieval Mechanism 1 .....</b>	<b>22</b>
7.1.1	Prior shared parameters .....	22
7.1.2	Functions .....	22
7.1.3	Key retrieval operation .....	23
<b>Annex A (normative) Functions for Data Type Conversion .....</b>		<b>24</b>
<b>Annex B (normative) ASN.1 Module .....</b>		<b>28</b>
<b>Annex C (informative) Guidance on Choice of Parameters .....</b>		<b>30</b>
<b>Bibliography .....</b>		<b>32</b>