

# ISO/IEC 11770-1:2010-12 (E)

## Information technology - Security techniques - Key management - Part 1: Framework

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>3</b>	<b>Symbols and abbreviated terms .....</b>	<b>6</b>
3.1	Symbols .....	6
3.2	Abbreviated terms .....	6
<b>4</b>	<b>General model of key management .....</b>	<b>6</b>
4.1	General .....	6
4.2	Protection of keys .....	7
4.2.1	General aspects of key management .....	7
4.2.2	Protection by cryptographic techniques .....	7
4.2.3	Protection by non-cryptographic techniques .....	7
4.2.4	Protection by physical means .....	7
4.2.5	Protection by organisational means .....	8
4.3	Generic key life cycle model .....	8
4.3.1	Key life cycle definitions .....	8
4.3.2	Transitions between key states .....	9
4.3.3	Transitions, services and keys .....	10
<b>5</b>	<b>Basic concepts of key management .....</b>	<b>10</b>
5.1	Key management services .....	10
5.1.1	Summary of key management services .....	10
5.1.2	Generate-Key (key generation) .....	12
5.1.3	Register-Key (key registration) .....	12
5.1.4	Create-Key-Certificate (key certification) .....	12
5.1.5	Distribute-Key (key distribution) .....	12
5.1.6	Install-Key (key installation) .....	12
5.1.7	Store-key (key storage) .....	12
5.1.8	Derive-Key (key derivation) .....	13
5.1.9	Archive-Key (key archiving) .....	13
5.1.10	Revoke-Key (key revocation) .....	13
5.1.11	Deregister-Key (key deregistration) .....	13
5.1.12	Destroy-Key (key destruction) .....	13
5.2	Support services .....	13
5.2.1	Key management facility services .....	13
5.2.2	User-oriented services .....	14
<b>6</b>	<b>Conceptual models for key distribution for two entities .....</b>	<b>14</b>
6.1	Introduction to key distribution .....	14
6.2	Key distribution between two communicating entities .....	14
6.3	Key distribution within one domain .....	15
6.4	Key distribution between two domains .....	16
<b>7</b>	<b>Specific service providers .....</b>	<b>18</b>
Annex A (informative)	Threats to key management .....	19

<b>Annex B (informative) Key management information objects .....</b>	<b>20</b>
<b>Annex C (informative) Classes of cryptographic applications .....</b>	<b>21</b>
<b>Annex D (informative) Certificate lifecycle management .....</b>	<b>23</b>
<b>Bibliography .....</b>	<b>30</b>