

# ISO/IEC 11770-6:2016-10 (E)

## Information technology - Security techniques - Key management - Part 6: Key derivation

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
<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 abbreviations .....</b>	<b>3</b>
4.1	Symbols .....	3
4.2	Abbreviations .....	4
4.3	Notation .....	4
<b>5</b>	<b>Key derivation techniques .....</b>	<b>4</b>
5.1	Model .....	4
5.2	Types of key derivation function .....	5
5.3	Relationship to key management life cycle .....	6
5.4	Use of a key derivation function .....	6
<b>6</b>	<b>One-step key derivation functions .....</b>	<b>6</b>
6.1	General .....	6
6.2	One-step key derivation function 1 (OKDF1) .....	7
6.2.1	General .....	7
6.2.2	Requirements for use .....	7
6.2.3	Operation of function .....	7
6.3	One-step key derivation function 2 (OKDF2) .....	8
6.3.1	General .....	8
6.3.2	Requirements for use .....	8
6.3.3	Operation of function .....	8
6.4	One-step key derivation function 3 (OKDF3) .....	9
6.4.1	General .....	9
6.4.2	Requirements for use .....	9
6.4.3	Operation of function .....	9
6.5	One-step key derivation function 4 (OKDF4) .....	9
6.5.1	General .....	9
6.5.2	Requirements for use .....	10
6.5.3	Operation of function .....	10
6.6	One-step key derivation function 5 (OKDF5) .....	10
6.6.1	General .....	10
6.6.2	Requirements for use .....	11
6.6.3	Operation of function .....	11
6.7	One-step key derivation function 6 (OKDF6) .....	11
6.7.1	General .....	11
6.7.2	Requirements for use .....	12
6.7.3	Operation of function .....	12
<b>7</b>	<b>Two-step key derivation functions .....</b>	<b>12</b>
7.1	General .....	12
7.2	Key extraction function .....	13

7.2.1	Key extraction function 1 (KTF1) .....	13
7.3	Key expansion functions .....	14
7.3.1	Key expansion function 1 (KPF1) .....	14
7.3.2	Key expansion function 2 (KPF2) .....	15
7.3.3	Key expansion function 3 (KPF3) .....	16
7.3.4	Key expansion function 4 (KPF4) .....	17
7.4	Two-step KDFs .....	18
7.4.1	Two-step key derivation function 1 (TKDF1) .....	18
7.4.2	Two-step key derivation function 2 (TKDF2) .....	18
7.4.3	Two-step key derivation function 3 (TKDF3) .....	19
7.4.4	Two-step key derivation function 4 (TKDF4) .....	19
Annex A (normative) Object identifiers .....		20
Annex B (informative) Guidance on use .....		21
Bibliography .....		23