

ISO/IEC 9797-1:2011-03 (E)

Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and notation	3
5	Requirements	4
6	Model for MAC algorithms	5
6.1	General	5
6.2	Step 1 (key derivation)	6
6.2.1	General	6
6.2.2	Key Derivation Method 1	6
6.2.3	Key Derivation Method 2	7
6.3	Step 2 (padding)	7
6.3.1	General	7
6.3.2	Padding Method 1	7
6.3.3	Padding Method 2	7
6.3.4	Padding Method 3	7
6.3.5	Padding Method 4	8
6.4	Step 3 (splitting)	8
6.5	Step 4 (iteration)	8
6.6	Step 5 (final iteration)	8
6.6.1	General	8
6.6.2	Final iteration 1	8
6.6.3	Final iteration 2	8
6.6.4	Final iteration 3	9
6.7	Step 6 (output transformation)	9
6.7.1	General	9
6.7.2	Output Transformation 1	9
6.7.3	Output Transformation 2	9
6.7.4	Output Transformation 3	9
6.8	Step 7 (truncation)	9
7	MAC algorithms	9
7.1	General	9
7.2	MAC Algorithm 1	10
7.3	MAC Algorithm 2	10
7.4	MAC Algorithm 3	11
7.5	MAC Algorithm 4	12
7.6	MAC Algorithm 5	13
7.7	MAC Algorithm 6	14
Annex A (normative)	Object identifiers	16

Annex B (informative) Examples	19
B.1 General	19
B.2 MAC Algorithm 1	20
B.3 MAC Algorithm 2	22
B.4 MAC Algorithm 3	23
B.5 MAC Algorithm 4	24
B.6 MAC Algorithm 5	26
B.6.1 Examples of MAC generation process	26
B.6.2 AES using a 128-bit key	27
B.6.3 AES using a 192-bit key	27
B.6.4 AES using a 256-bit key	27
B.6.5 Three-key triple DEA	28
B.6.6 Two-key triple DEA	28
B.7 MAC Algorithm 6	29
B.7.1 Examples of MAC generation process	29
B.7.2 AES using a 128-bit key	29
B.7.3 AES using a 192-bit key	29
B.7.4 AES using a 256-bit key	30
Annex C (informative) A security analysis of the MAC algorithms	31
C.1 General	31
C.2 Rationale	33
Annex D (informative) A comparison with previous MAC algorithm standards	38
Bibliography	39