ISO/IEC 19772:2009-02 (E)

Information technology - Security techniques - Authenticated encryption

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols (and abbreviated terms) 3

5 Requirements 4

6 Authenticated encryption mechanism 1 (OCB 2.0) 4
6.1 Introduction 4
6.2 Specific notation 4
6.3 Specific requirements 5
6.4 Definition of function M2 5
6.5 Definition of function M3 5
6.6 Definition of function J 6
6.7 Encryption procedure 6
6.8 Decryption procedure 7

7 Authenticated encryption mechanism 2 (Key Wrap) 7
7.1 Introduction 7
7.2 Specific notation 8
7.3 Specific requirements 8
7.4 Encryption procedure 8
7.5 Decryption procedure 9

8 Authenticated encryption mechanism 3 (CCM) 9
8.1 Introduction 9
8.2 Specific notation 9
8.3 Specific requirements 10
8.4 Encryption procedure 10
8.5 Decryption procedure 12

9 Authenticated encryption mechanism 4 (EAX) 13
9.1 Introduction 13
9.2 Specific notation 13
9.3 Specific requirements 13
9.4 Definition of function M 13
9.5 Encryption procedure 14
9.6 Decryption procedure 14

10 Authenticated encryption mechanism 5 (Encrypt-then-MAC) 15
10.1 Introduction 15
10.2 Specific notation 15
10.3 Specific requirements 15
10.4 Encryption procedure 16
10.5 Decryption procedure 16

11 Authenticated encryption mechanism 6 (GCM) 16
11.1 Introduction 16
11.2 Specific notation 17
11.3 Specific requirements 17
11.4 Definition of multiplication operation 18
11.5 Definition of function G 18
11.6 Encryption procedure 18
11.7 Decryption procedure 19

Annex A (informative) Guidance on use of the mechanisms 20

A.1 Introduction 20
A.2 Selection of mechanism 20
A.3 Mechanism 1 (OCB 2.0) 21
A.4 Mechanism 2 (Key Wrap) 21
A.5 Mechanism 3 (CCM) 21
A.6 Mechanism 4 (EAX) 21
A.7 Mechanism 5 (Encrypt-then-MAC) 22
A.8 Mechanism 6 (GCM) 22

Annex B (informative) Examples 23

B.1 Introduction 23
B.2 Mechanism 1 (OCB 2.0) 23
B.3 Mechanism 2 (Key Wrap) 24
B.4 Mechanism 3 (CCM) 24
B.5 Mechanism 4 (EAX) 25
B.6 Mechanism 5 (Encrypt-then-MAC) 26
B.7 Mechanism 6 (GCM) 26

Annex C (normative) ASN.1 module 28

C.1 Formal definition 28
C.2 Use of subsequent object identifiers 28

Bibliography 29