

ISO/IEC 19772:2020 (E)

Information security — Authenticated encryption

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols and abbreviated terms
5	Requirements
6	Authenticated encryption mechanism 2 (key wrap)
6.1	General
6.2	Specific notation
6.3	Specific requirements
6.4	Encryption procedure
6.5	Decryption procedure
7	Authenticated encryption mechanism 3 (CCM)
7.1	General
7.2	Specific notation
7.3	Specific requirements
7.4	Encryption procedure
7.5	Decryption procedure
8	Authenticated encryption mechanism 4 (EAX)
8.1	General
8.2	Specific notation
8.3	Specific requirements
8.4	Definition of function M
8.5	Encryption procedure
8.6	Decryption procedure
9	Authenticated encryption mechanism 5 (encrypt-then-MAC)
9.1	General
9.2	Specific notation
9.3	Specific requirements
9.4	Encryption procedure
9.5	Decryption procedure
10	Authenticated encryption mechanism 6 (GCM)
10.1	General
10.2	Specific notation
10.3	Specific requirements
10.4	Definition of multiplication operation •
10.5	Definition of function G
10.6	Encryption procedure
10.7	Decryption procedure
Annex A	(informative) Guidance on the use of the mechanisms
A.1	General

- A.2 Selection of mechanism
- A.3 Mechanism 2 (key wrap)
- A.4 Mechanism 3 (CCM)
- A.5 Mechanism 4 (EAX)
- A.6 Mechanism 5 (encrypt-then-MAC)
- A.7 Mechanism 6 (GCM)

Annex B (informative) Numerical examples

- B.1 General
- B.2 Mechanism 2 (key wrap)
- B.3 Mechanism 3 (CCM)
- B.4 Mechanism 4 (EAX)
- B.5 Mechanism 5 (encrypt-then-MAC)
- B.6 Mechanism 6 (GCM)

Annex C (normative) Object identifiers

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

Page count: 26