

ISO/IEC 9797-3:2011-11 (E)

Information technology - Security techniques - Message Authentication Codes (MACs) - Part 3: Mechanisms using a universal hash-function

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	2
5	General model	4
6	Mechanisms	5
6.1	Introduction	5
6.2	UMAC	5
6.2.1	Description of UMAC	5
6.2.2	Requirements	5
6.2.3	Notation and auxiliary functions	5
6.2.4	Key preprocessing	9
6.2.5	Message preprocessing	9
6.2.6	Message hashing	9
6.2.7	Layered hash-functions	10
6.2.8	Finalization	12
6.3	Badger	12
6.3.1	Description of Badger	12
6.3.2	Requirements	12
6.3.3	Notation and auxiliary functions	13
6.3.4	Key preprocessing	13
6.3.5	Message preprocessing	14
6.3.6	Message hashing	14
6.3.7	Finalization	16
6.4	Poly1305-AES	16
6.4.1	Description of Poly1305-AES	16
6.4.2	Requirements	16
6.4.3	Key preprocessing	16
6.4.4	Message preprocessing	16
6.4.5	Message hashing	17
6.4.6	Finalization	17
6.5	GMAC	18
6.5.1	Description of GMAC	18
6.5.2	Requirements	18
6.5.3	Notation and auxiliary functions	18
6.5.4	Key preprocessing	19
6.5.5	Message preprocessing	19
6.5.6	Message hashing	19
6.5.7	Finalization	19
Annex A (normative)	Object Identifiers	20

Annex B (informative) Test Vectors	22
Annex C (informative) Security Information	24
Bibliography	25