ISO 16609:2022-08 (E)

Financial services - Requirements for message authentication using symmetric techniques

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Principles 3
4.1 Protection of authentication keys 3
4.2 Message authentication elements 3
4.3 Detection of duplication, loss or sequence errors 4

5 Procedures for message authentication 4
5.1 MAC generation 4
5.2 MAC placement 5
5.3 MAC verification 5
5.4 Approved authentication mechanisms based on the ISO/IEC 9797 series 5
5.4.1 General 5
5.4.2 Approved message authentication mechanisms based on ISO/IEC 9797-1 5
5.4.3 Approved message authentication mechanisms based on ISO/IEC 9797-2 6
5.4.4 Approved message authentication mechanisms based on ISO/IEC 9797-3 7
5.4.5 Implementation recommendations 8

Annex A (informative) Protection against duplication and loss using MIDs 9

Annex B (informative) General tutorial information 11

Bibliography 13