

# ISO 16609:2004-03 (E)

## Banking - Requirements for message authentication using symmetric techniques

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	2
4	Protection .....	4
4.1	Protection of authentication keys .....	4
4.2	Authentication elements .....	5
4.3	Detection of duplication or loss .....	5
5	Procedures for message authentication .....	6
5.1	Preliminaries .....	6
5.2	Message format .....	6
5.3	Key generation .....	6
5.4	MAC Generation .....	7
5.5	MAC placement .....	7
5.6	MAC checking .....	7
6	Approved MAC algorithms .....	7
6.1	Overview of ISO/IEC 9797-1 .....	7
6.2	Overview of ISO/IEC 9797-2 .....	9
6.3	Implementation recommendations .....	9
Annex A (normative) Approved block ciphers for message authentication .....		11
Annex B (informative) Message authentication for coded character sets .....		13
Annex C (informative) Examples of message authentication for coded characters sets .....		18
Annex D (informative) Framework for message authentication of standard telex formats .....		23
Annex E (informative) Protection against duplication and loss using MIDs .....		25
Annex F (informative) Deterministic (pseudo-random) bit generator .....		26
Annex G (informative) Session key derivation .....		27
Annex H (informative) General tutorial information .....		28
Bibliography .....		29