

ICS 35.240.40
CCS A 11



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 27929-2025

Replacing GB/T 27929-2011

**Financial services - Requirements for message authentication
using symmetric techniques**

金融服务 采用对称加密技术进行报文鉴别的要求

(English Translation)

Issued on: June 30, 2025

Implemented on: October 1, 2025

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

- Preface
- 1 Scope
- 2 Normative references
- 3 Terms and Definitions
- 4 General Principles
 - 4.1 Protection of Authentication Keys
 - 4.2 Message Authentication Elements
 - 4.3 Detection of duplicate, lost or out-of-sequence messages
- 5 Message Authentication Process
 - 5.1 MAC Generation
 - 5.2 MAC Location
 - 5.3 MAC Verification
 - 5.4 Message Authentication Mechanism Based on GB/T 15852
 - 5.4.1 Overview
 - 5.4.2 Message Authentication Mechanism Based on GB/T 15852.1
 - 5.4.3 Message Authentication Mechanism Based on GB/T 15852.2
 - 5.4.4 Message Authentication Mechanism Based on GB/T 15852.3
 - 5.4.5 Implementation Recommendation
- Appendix A (Informative) Using MIDs to Prevent Duplication and Loss
 - A.1 Purpose
 - A.2 Preventing Duplication
 - A.2.1 Duplicate Messages
 - A.2.2 Multi-party processing
 - A.2.3 Include identity
 - A.3 Loss Detection
- Appendix B (Informative) General Guidance Information
- Reference

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents"

Drafting.

This document replaces GB/T 27929-2011 "Requirements for message authentication using symmetric encryption technology in banking services" and Compared with GB/T 27929-2011, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

a) The terms "authentication", "authentication algorithm", "authentication element", "deviation", "cryptanalysis", "data integrity", "data source authentication", "decryption", etc. have been deleted.

"Secret", "Separator", "Hexadecimal Number", "Message Body", "Current Random Number" (see 3.2, 3.3, 3.4, 3.8, 3.10, 2011 Edition) 3.11, 3.13, 3.14, 3.15, 3.17, 3.23, 3.24), added the term "generalized hash function" (see 3.16), changed the term "message Definition of "Message Authentication Code (MAC) Algorithm" (see 3.9 and 3.10, 3.19 and 3.20 of the 2011 Edition);

b) Deleted the requirements for the preparation phase of the message authentication process, message format, and key generation (see 5.1 to 5.3 of the 2011 edition);

c) Added SM4 and AES algorithms (see 5.4.2), and deleted the DEA algorithm (see 6.1.4 of the 2011 edition);

d) Added SM3, RIPEMD-160, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384 and SHA3-512 algorithms (see 5.4.3), SHA-1 and RIPEMD-128 algorithm (see 6.2 of the 2011 edition);

e) Added UMAC, Poly1305-AES and GMAC algorithms (see 5.4.4).

This document is modified to adopt ISO 16609:2022 "Requirements for message authentication using symmetric cryptographic techniques in financial services".

This document has the following structural adjustments compared to ISO 16609:2022.

--- The fifth paragraph of 5.3 corresponds to the fifth paragraph of the introduction to ISO 16609:2022.

The technical differences between this document and ISO 16609:2022 and their reasons are as follows.

--- The term "check code" in ISO 16609:2022 has been deleted because the text does not contain any relevant content about check code;

--- Change ISO 8583-1 to ISO 8583 (see Chapter 3). ISO 8583-1 has been replaced by ISO 8583;

--- Change ISO 11568-1 and ISO 11568-2 to ISO 11568 (see 4.1). ISO 11568-1 and ISO 11568-2 have been ISO 11568 replaced;

---Changed TDEA to the algorithm name 3DES that conforms to my country's usage habits, added MAC algorithm 7 (TrCBC) and MAC Algorithm 8 (CBCR) (see 5.4.2) to correspond to GB/T 15852.1-2020.

The following editorial changes have been made to this document.

--- Replace ISO/IEC 9797 (all parts) with the informative reference GB/T 15852 (all parts);

--- Deleted the informative reference to NISTSP800-107 in Note 2 of Table 2 of ISO 16609:2022.

1 Scope

This document establishes the methods used to protect the integrity of financial services business messages or stored data and to verify that messages originate from authorized sources.

The process is independent of the transport process used. Approved block cipher algorithms that support message authentication code (MAC) calculations are also provided.

The authentication methods defined in this document apply to data stored in coded character sets or binary form and to data formatted and transmitted.

message.

This document applies to symmetric algorithms where the sender and receiver use the same key and does not specify how to generate the shared key.

Use does not prevent internal fraud at the sender and receiver, or forgery of the MAC by the receiver.

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.

ISO 8583 Financial-transaction-card-originated messages—Note. GB/T 15150-1994 Bank Card Interchange Message Specification for Financial Transaction Content (ISO 8583:1987, IDT) Note. GB/T 27909.1-2011 Banking Key Management (Retail) Part 1: General Principles (ISO 11568-1:2005, MOD) GB/T 27909.2-2011 Banking Key Management (Retail) Part 2: Symmetric Cryptography and Key Management and Lifecycle (ISO 11568-2:2005, MOD) GB/T 27909.3-2011 Banking Key Management (Retail) Part 3: Asymmetric Cryptography Systems and Key Management and Lifecycle (ISO

11568-4:2007,MOD)

3 Terms and Definitions

For the purposes of this document, the terms and definitions defined in ISO 8583 and the following apply.

algorithm

A mathematical procedure or rule to be followed in calculation to obtain a specified result.

authenticationkey

The encryption key used in the authentication process.

beneficiary

The final party to whom funds are transferred as a credit or payment.

Note: There may be more than one beneficiary.