ICS 35.240.40
CCS A 11

中华人民共和国国家标准

GB/T 27929—2025
代替 GB/T 27929—2011

金融服务　采用对称加密技术进行报文鉴别的要求

Financial services—Requirements for message authentication using symmetric techniques

（ISO 16609:2022,MOD）

2025-06-30 发布　　2025-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 27929—2011《银行业务　采用对称加密技术进行报文鉴别的要求》，与GB/T 27929—2011相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 删除了术语“鉴别”“鉴别算法”“鉴别元素”“偏差”“密码分析”“数据完整性”“数据源鉴别”“解密”“分隔符”“十六进制数”“报文正文”“当前随机数”（见2011年版的3.2、3.3、3.4、3.8、3.10、3.11、3.13、3.14、3.15、3.17、3.23、3.24），增加了术语“泛杂凑函数”（见3.16），更改了术语“报文鉴别码”“报文鉴别码（MAC）算法”的定义（见3.9和3.10，2011年版的3.19和3.20）；

b) 删除了报文鉴别过程的准备阶段、报文格式和密钥生成的要求（见2011年版的5.1～5.3）；

c) 增加了SM4和AES算法（见5.4.2），删除了DEA算法（见2011年版的6.1.4）；

d) 增加了SM3、RIPEMD-160、SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256、SHA3-224、SHA3-256、SHA3-384和SHA3-512算法（见5.4.3），删除了SHA-1和RIPEMD-128算法（见2011年版的6.2）；

e) 增加了UMAC、Poly1305-AES和GMAC算法（见5.4.4）。

本文件修改采用ISO 16609:2022《金融服务　采用对称加密技术进行报文鉴别的要求》。

本文件与ISO 16609:2022相比做了下述结构调整：

——5.3的第五段对应ISO 16609:2022中引言的第五段。

本文件与ISO 16609:2022的技术性差异及其原因如下：

——删除了ISO 16609:2022中的术语“校验码”，因为正文中未涉及校验码的相关内容；

——将ISO 8583-1更改为ISO 8583（见第3章），ISO 8583-1已被ISO 8583代替；

——将ISO 11568-1和ISO 11568-2更改为ISO 11568（见4.1），ISO 11568-1和ISO 11568-2已被ISO 11568代替；

——将TDEA更改为符合我国使用习惯的算法名称3DES，增加了MAC算法7（TrCBC）和MAC算法8（CBCR）（见5.4.2），以便与GB/T 15852.1—2020进行对应。

本文件做了下列编辑性改动：

——用资料性引用的GB/T 15852（所有部分）替换ISO/IEC 9797（所有部分）；

——删除了ISO 16609:2022的表2注2中对NIST SP 800-107的资料性引用。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中金金融认证中心有限公司、山东财经大学、山东科技大学、北京国家金融标准化研究院有限责任公司、中国银联股份有限公司、网联清算有限公司、清华大学。

本文件主要起草人：朱钢、谢宗晓、马春旺、李达、王自冲、李恩达、吴利东、董亚南、董坤祥、甄杰、周夕崇、谢彦丽、薄舜添、贺宇、汤洋、郭林、杨萌、夏泽宇。

本文件及其所代替文件的历次版本发布情况为：

——2011年首次发布为GB/T 27929—2011；

——本次为第一次修订。

金融服务　采用对称加密技术进行报文鉴别的要求

1　范围

本文件确立了用于保护金融服务业务报文或存储数据的完整性，以及验证报文来自已授权来源的过程，该过程与所使用的传输过程无关。也提供了已核准的支持报文鉴别码(MAC)计算的分组密码算法列表。本文件中定义的鉴别方法适用于以编码字符集或二进制形式存储的数据和格式化及传输的报文。

本文件适用于发送方和接收方采用相同密钥的对称算法，未规定生成共享密钥的方法。本文件的使用不能防止发送方和接收方的内部欺诈，或者接收方伪造 MAC。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

ISO 8583　金融交易卡原始报文　交换报文规范(Financial-transaction-card-originated messages—Interchange message specifications)

注：GB/T 15150—1994　产生报文的银行卡　交换报文规范　金融交易内容(ISO 8583:1987，IDT)

ISO 11568　金融服务　密钥管理(零售)[Financial services—Key management (retail)]

注：GB/T 27909.1—2011　银行业务　密钥管理(零售)　第 1 部分：一般原则(ISO 11568-1:2005，MOD)

GB/T 27909.2—2011　银行业务　密钥管理(零售)　第 2 部分：对称密码及其密钥管理和生命周期(ISO 11568-2:2005，MOD)

GB/T 27909.3—2011　银行业务　密钥管理(零售)　第 3 部分：非对称密码系统及其密钥管理和生命周期(ISO 11568-4:2007，MOD)

3　术语和定义

ISO 8583 界定的以及下列术语和定义适用于本文件。

3.1

算法　algorithm

为得到规定的结果而遵循的，用于计算的待定数学过程或数学规则。

3.2

鉴别密钥　authentication key

用于鉴别过程的加密密钥。

3.3

受益人　beneficiary

以贷记或支付方式被转账的最终方。

注：受益人有可能不止一人。