ICS 35.040
L 80

GM

中华人民共和国密码行业标准

GM/T 0074—2019

网上银行密码应用技术要求

Technical requirements on cryptographic application for internet banking

2019-07-12 发布　　2019-07-12 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：天地融科技股份有限公司、国民技术股份有限公司、北京信安世纪科技股份有限公司、北京数字认证股份有限公司、中钞研究院、银行卡检测中心、成都卫士通信息产业股份有限公司、北京华大智宝电子系统有限公司。

本标准起草人：李明、牟宁波、杨贤伟、李美祥、汪宗斌、林雪焰、李向锋、平庆瑞、汪小八、张文科、张立廷、陈跃、何智、史晓峰。

引　言

网上银行是指银行通过互联网向客户提供金融服务的业务。作为对银行传统渠道的一种补充，网上银行的开展可以极大地降低银行的经营成本，增加业务交易量并获得收益，同时也可以为客户提供更便捷和创新的银行服务。对用户而言，网上银行没有时间和空间的限制，节省用户的使用成本，满足多种形式的需求，具有良好的发展趋势。然而，由于互联网的开放性和固有缺陷，与传统服务渠道相比，网上银行存在更大的安全隐患和安全威胁。

密码技术作为信息安全核心防护手段，已广泛应用于网上银行的安全建设中。因此，从技术层面对网上银行系统中密码技术的设计、实现与使用进行要求，具有重大的现实意义。

本标准根据国内网上银行业务特点及密码应用功能需求，制定网上银行业务密码应用技术要求，以促进国内网上银行密码应用的技术规范化与健康发展。

网上银行密码应用技术要求

1 范围

本标准规定了密码技术在网上银行业务中应用的相关要求，包括密码算法、密钥管理、证书管理、安全通道、密码设备及数字签名六个方面。

本标准适用于指导网上银行业务中密码技术相关安全功能的设计、实现和使用，对于网上银行系统中密码子系统的测试、管理可参照使用。

手机银行等系统中相关部分内容也可以参照本标准。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的，凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GB/T 15843(所有部分) 信息技术 安全技术 实体鉴别

GB/T 19713 信息安全技术 公钥基础设施 在线证书状态协议

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 28447 信息安全技术 电子认证服务机构运营管理规范

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0018 密码设备应用接口规范

GM/T 0019 通用密码服务接口规范

GM/T 0021 动态口令密码应用技术规范

GM/T 0022 IPSec VPN 技术规范

GM/T 0023 IPSec VPN 网关产品规范

GM/T 0024 SSL VPN 技术规范

GM/T 0025 SSL VPN 网关产品规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0028 密码模块安全技术要求

GM/T 0029 签名验签服务器技术规范

GM/T 0030 服务器密码机技术规范

GM/T 0033 时间戳接口规范

GM/T 0034 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范

GM/T 0037　证书认证系统检测规范
GM/T 0038　证书认证密钥管理系统检测规范
GM/T 0039　密码模块安全检测要求
GM/T 0045　金融数据密码机技术规范
GM/T 0054　信息系统密码应用基本要求
GM/Z 4001　密码术语
JR/T 0068　网上银行系统信息安全通用规范

3　术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

网上银行　internet banking

商业银行等金融机构通过互联网向其客户提供各种金融业务的服务，简称“网银”。

3.2

真实性　authenticity

确保主体或资源的身份正是所声称的特性。真实性适用于用户、进程、系统和信息之类的实体。

3.3

客户端　client

为网上银行客户提供人机交互功能的程序，以及提供必需功能的组件，包括但不限于：可执行文件、控件、静态链接库、动态链接库等。

3.4

密码设备　cryptographic device

能够独立完成密码服务功能的设备。

3.5

服务端　server

网上银行系统中，金融业务服务的提供端。

4　缩略语

下列缩略语适用于本文件。

CSP　微软密码服务接口(Cryptographic Service Provider)
IPSEC　IP 安全协议(Internet Protocol Security)
OTP　一次性密码(One Time Password)
PKCS　公钥密码标准(Public Key Cryptography Standards)
SSL　安全套接字层(Secure Socket Layer)
TLS　传输层安全(Transfer Layer Secure)
VPN　虚拟专用网络(Virtual Private Network)
WTLS　无线安全传输层(Wireless Transport Layer Security)

5　概述

网上银行密码应用技术体系是基于密码技术建立的安全服务体系，利用密码技术支撑真实性、机密

性、完整性和抗抵赖等特性，形成对网上银行系统与业务的安全支撑，以保护其应用安全及运行安全。以密码算法、密钥管理、数字证书、安全通道、数字签名等密码技术为基础的密码设备为网上银行业务系统的提供了安全保障，进而支撑网上银行业务安全展开。密码应用技术对网上银行业务的支撑如图1所示。

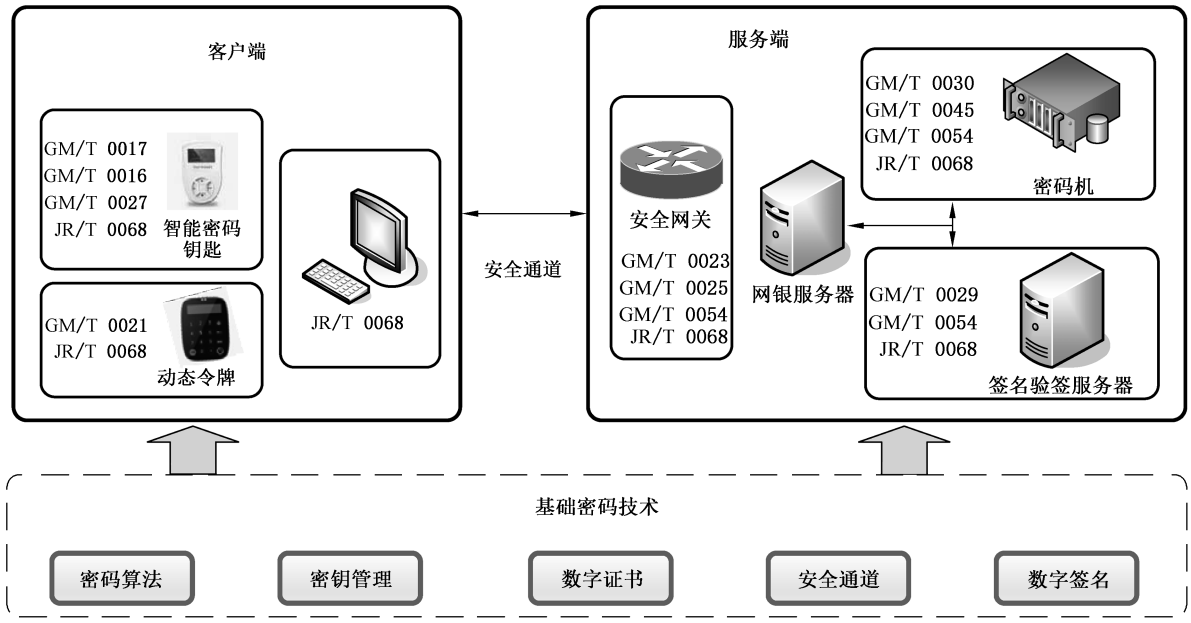

图1　密码应用技术对网上银行业务支撑示意图

网上银行系统应符合JR/T 0068的相关要求，具体实施方面，应遵循GM/T 0054中对等级保护不同等级的信息系统安全要求，结合网上银行系统的实际情况，选择相应级别的密码设备。示例参见附录A。

6　网上银行业务密码应用需求

6.1　查询业务

查询业务主要包括公共信息查询和与个人客户或企业客户的账户信息查询。

对于公共信息，可以不经过身份鉴别直接查询。对于与客户身份相关的账户信息查询，客户要先通过身份鉴别后才能查询。网银系统与客户的通讯中应保持查询结果的机密性和完整性。

6.2　资金变动业务

客户在办理资金变动业务前必须经过身份鉴别，只有账户的真正所有者才能操作账户资金。

在资金变动类业务中，资金在个人或企业名下封闭流动的（比如投资理财、定活互转等），操作中身份认证要求相对宽松，但像转账汇款、网上支付等资金流出的操作，每一次操作都需要进行客户身份鉴别。

除身份鉴别外，网银系统需要保证客户操作的机密性、完整性和抗抵赖性，并保持操作记录的可审计性。

6.3　签约业务

签约业务根据内容的不同，会有选择地使用身份鉴别方式，比如柜面实名、智能密码钥匙数字签名

等。网银系统要保证客户操作的机密性、完整性和抗抵赖性，并保持操作记录的可审计性。

6.4 其他业务

在以上三类业务之外，网银还提供一系列其他服务，比如保险业务、信用卡申请、操作员日志查询等。根据业务内容的不同，网银系统有选择性的使用身份鉴别方式，同时要保证客户操作的机密性、完整性和抗抵赖性，并保持记录的可审计性。

不同业务类型的安全性要求对应表如表1所示。

表1 网上银行业务密码应用需求

安全性要求	身份鉴别	机密性	完整性	抗抵赖	核验审计
查询业务	对公、个人	对公、个人	对公、个人	—	—
资金变动业务	对公、个人	对公、个人	对公、个人	对公、个人	对公、个人
签约业务	对公、个人	对公、个人	对公、个人	对公、个人	对公、个人
其他业务	对公、个人	对公、个人	对公、个人	对公、个人	对公、个人

7 网上银行密码应用技术要求

7.1 密码功能要求

7.1.1 身份鉴别

客户在进行账户操作前(账户查询、转账等)，须向系统表明身份，在资金变动类交易过程中也需要向系统再次确认自己的身份。网上银行常用的客户身份鉴别方法包括且不限于用户名与静态密码、动态密码(OTP令牌、短信、动态口令卡等)、智能密码钥匙、生物特征等其中的一种或多种的组合。

客户在提交身份鉴别信息登录系统时，系统要保证信息的机密性与安全性，防止第三方窃取相关信息后冒充客户登录。

客户在交易过程中进行的身份鉴别，除要保证身份鉴别信息的机密性与安全性，还应保证身份鉴别信息的完整性、不可抵赖性和可审计性。

为保证身份鉴别的安全性，在GB/T 15843的基础上应采用GB/T 32918、GB/T 32905、GB/T 32907或国家密码主管部门认可的密码算法。

7.1.2 数据机密性要求

客户与网银系统间交互的数据需要加密传输，以保证数据内容机密性，包括且不限于登录信息、交易信息、签约信息以及网银系统内存储的数据等，防止客户电脑上的恶意程序或传输过程中的第三方窥测。

为保证数据机密性，应对其进行加密处理，根据应用场景采用GB/T 32918、GB/T 32907或国家密码主管部门认可的密码算法，其中，使用GB/T 32918时，应遵循GB/T 35275或GB/T 35276。

7.1.3 数据完整性要求

客户与网银系统间交互的数据要进行完整性校验，以防止第三方修改。需要进行完整性校验的数据包括且不限于：客户从本地发送至网银系统的登录数据、交易申请数据以及签约数据等，网银系统发送至客户本地的登录结果、查询结果、交易结果以及签约结果等。

为保证数据的完整性，应对其进行数字签名、杂凑或其他类似的处理，根据应用场景采用

GB/T 32918、GB/T 32905、GB/T 32907，或国家密码主管部门认可的密码算法，其中，使用GB/T 32918时，应遵循GB/T 35275或GB/T 35276。

7.1.4 抗抵赖性要求

客户登录网银系统后进行的交易、签约等活动，要求银行和客户双方都不能抵赖：客户不能否认自己操作的转账记录或签约记录等，银行也不能否认自身已经完成的转账、签约等各项操作。

为保证双方动作的抗抵赖性，应对活动信息进行数字签名，根据应用场景采用GB/T 32918或国家密码主管部门认可的密码算法。

7.1.5 核验审计要求

核验审计主要包括事中核验审计与事后核验审计两方面：事中核验审计是在客户操作网银系统过程中核验或审计客户的身份与权限是否合法，主要包括系统登录、交易中的身份认证及权限核对等；事后核验审计是对于网银系统后台存储的交易数据，核验或审计是否正确等。

为保证核验审计的可操作性以及安全性，审计前宜对审计目标中的姓名、账号、金额等关键字段进行加密或屏蔽。若采用加密的方式，根据实际情况应采用GB/T 32918、GB/T 32905、GB/T 32907，或国家密码主管部门认可的密码算法。

7.2 密钥管理要求

7.2.1 概述

密码算法在网上银行的身份鉴别、通信加密、核验审计、数据机密性、数据完整性、抗抵赖以及安全通道建立等方面发挥着重大作用，相应的密钥管理是网上银行系统运行管理的基础。

密钥管理应遵循GM/T 0054的要求。除特定场景的密钥管理应遵循相关标准外（比如证书中的认证密钥管理应遵循GM/T 0038），用户使用的智能密码钥匙中的业务密钥以及系统管理员密钥等常用的密钥管理要求见7.2.2～7.2.6。

7.2.2 密钥生成

密钥生成应遵循随机生成原则，所采用的随机数为密码设备产生的真随机数，应满足GB/T 32915的要求。

密钥文档资料保存期限应不低于记录对象的生命周期。

7.2.3 密钥存储

密钥在未受保护的环境中不得以明文的方式存储。密钥的存储安全可以用安全硬件保证，也可以用加密算法保证。

对于受知识分割或双重控制等安全机制保护的密钥，不同部分应保存在不同地点，并且不能由一个人保管。

7.2.4 密钥使用

密钥使用应该按照密钥正确用途进行使用。例如：在进行身份鉴别、保证信息的数据完整性和抗抵赖时使用签名密钥，在保证信息的机密性时使用加密密钥。不同用途的密钥不能混用。

7.2.5 密钥备份和恢复

设备内部的工作密钥可以在本设备的安全区域进行备份，当设备检测到工作密钥被非法更改时，设

备应对密钥进行恢复操作。密钥工作及存储的安全区域禁止提供外部访问接口，防止密钥泄露。

需要对密钥进行外部备份时，应采用安全硬件进行保护，或将密钥加密后以密文形式导出，不得以明文方式直接导出。

7.2.6 密钥撤销与存档

失效、作废或泄漏的密钥应及时更新，原密钥可以归档但不应再使用。

7.3 证书管理要求

7.3.1 概述

网上银行业务使用的数字证书，主要指最终用户用以完成身份认证、安全通信和交易签名的数字证书。

证书认证系统和相关的密钥管理系统建设应遵循 GM/T 0028、GM/T 0034、GM/T 0037、GM/T 0038、GM/T 0039、GM/T 0054 和 GB/T 28447 等相关标准要求。

证书格式应遵循 GB/T 20518 和 GM/T 0015。

在线证书状态服务应符合 GB/T 19713。

7.3.2 证书生命周期管理

证书生命周期包括以下阶段：

a) 证书申请：网上银行客户申请证书时，银行对用户提交的申请信息及身份信息进行审核，确认其是否完整、真实、有效；

b) 证书下载：证书下载过程中，智能密码钥匙内部生成非对称密钥对的私钥应全程受智能密码钥匙保护；外部导入的密钥对应当加密保护，避免私钥泄露；

c) 证书更新：在证书即将到期的情况下，网上银行客户可以办理证书更新。更新证书时，应更换密钥对，并吊销旧证书和密钥，在吊销列表中需包含旧证书序列号；

d) 证书吊销：在证书丢失、损坏等情况下，网上银行客户可以办理证书吊销。

7.4 通道安全要求

网上银行的客户端与后台系统之间，以及网上银行后台与其他第三方系统间的连接，应遵循 GM/T 0054的要求采用安全通道的方式对通讯数据进行保护。

安全通道应该使用加密算法和安全协议保护客户端与服务器之间所有的连接，保证传输数据的机密性和完整性，例如，使用 SSL/TLS、IPSEC 和 WTLS 协议。

采用 SSL/TLS 协议的安全产品应符合 GM/T 0024，SSL VPN 网关产品应符合 GM/T 0025。

采用 IPSec 协议的安全产品应符合 GM/T 0022，IPSec VPN 网关产品应符合 GM/T 0023。

7.5 密码设备要求

7.5.1 密码功能要求

网上银行系统使用的各类设备，包含以下部分或全部典型密码功能的属密码设备范畴，应满足 GM/T 0054 所要求的安全等级：

a) 产生随机数：生成指定长度的随机序列；

b) 密钥生成：生成指定算法类型和长度的密钥；

c) 非对称密码运算：公钥运算、私钥运算、数字签名和签名验证；

d) 对称密码运算：单包或多包数据加密、解密；

e) 密码杂凑运算：单包或多包密码杂凑生成；
f) 消息鉴别码运算：单包或多包消息鉴别码生成、验证；
g) 证书运算：提供证书验证、证书解析等功能；
h) 密钥与证书管理：各种密钥的导入、导出、备份、恢复；公钥证书的导入、导出、备份、恢复；
i) 正确性自检：密码模块或功能正确性自动检测。

7.5.2 接口要求

智能密码钥匙设备的接口应满足 GM/T 0016，服务类密码设备的接口应满足 GM/T 0018，其他密码设备服务接口应支持 GM/T 0019，在使用其他规范时（如 CSP、PKCS#11 等），底层算法、功能等方面的实现应遵循相关标准要求。

7.5.3 安全要求

7.5.3.1 通用要求

网上银行系统使用的密码设备，应使用获得国家密码主管部门认定型号的商用密码产品，并在使用过程中，保证私钥和对称密钥不以明文形态出现在密码设备外。

7.5.3.2 服务端密码设备安全要求

网上银行系统使用的服务端密码设备，除了满足密码设备通用安全要求外，还应满足 JR/T 0068 中服务器端安全功能要求。其中签名验签服务器应满足 GM/T 0029，服务器密码机应满足 GM/T 0030，金融数据密码机应满足 GM/T 0045。

7.5.3.3 客户端密码设备安全要求

7.5.3.3.1 整体要求

客户端安全应遵循 JR/T 0068 要求。

7.5.3.3.2 智能密码钥匙

网上银行系统使用的智能密码钥匙密码设备，除了满足密码设备通用安全要求外，还应符合 GM/T 0027、JR/T 0068 中关于智能密码钥匙的相关要求，其接口应满足 GM/T 0016，处理的数据格式应满足 GM/T 0017。

智能密码钥匙工作时应当与客户端或后台建立安全通道，防止业务数据被监听或篡改。

7.5.3.3.3 动态口令终端

网上银行系统使用的动态口令终端密码设备，应满足 GM/T 0021、JR/T 0068 中关于 OTP 令牌 、动态密码卡以及手机短信动态密码等相关要求。

7.5.3.3.4 新型/专用客户端

对于新出现或专用的客户端密码设备，可参照本标准的要求，保证客户端密码设备自身安全机制的可靠性以及其所保护信息的安全性。

对于将上述两种或多种客户端密码设备功能集成在一起的多功能客户端密码设备，如带动态口令功能的智能密码钥匙，或者带智能密码钥匙功能的互联网支付终端等，其每项功能应当符合相应功能类型单个密码终端产品的安全要求。

7.6 数字签名要求

数字签名格式应符合 GB/T 35276 的要求，数字签名封装格式应符合 GB/T 35275 的要求，用于制作数字签名的智能密码钥匙或其他安全设备应符合 GM/T 0016 的要求，用于制作服务端数字签名的设备应符合 GM/T 0018 或 GM/T 0029 的要求。

对交易时间或时效性有要求的业务，应使用时间戳保证交易时间的准确性，其接口应符合GM/T 0033。

附 录 A
（资料性附录）
等级保护第三级网上银行系统建设示例

GM/T 0054 对信息系统建设中的密码应用相关内容提出了要求，网上银行系统建设涉及的安全功能以及密码产品的安全等级选择，应满足 GM/T 0054 的要求。本标准结合 GM/T 0054 的规定，以等级保护第三级网上银行系统，明确物理环境、网络、业务、管理等密码方面的安全要求。详细内容见表 A.1。

表 A.1 等级保护第三级网上银行系统密码应用技术要求

指标			要求
技术要求	物理和环境安全	身份鉴别	对于机房、研发等重点场所使用门禁卡等身份识别设备进行出入人员身份管理
		电子门禁记录数据完整性	对电子门禁的进出记录进行数字签名或计算 MAC，防止修改
		视频记录数据完整性	对监控记录进行数字签名或计算 MAC，防止修改
		密码模块实现	宜优先选用符合 GM/T 0028 三级密码模块标准的门禁系统及视频监控系统进行物理环境安全建设
	网络和通信安全	身份鉴别	客户接入网银系统服务时，客户与网银系统双方进身份认证并建立安全通道，通过安全通道传输数据，保证身份认证的可信以及通信内容的机密性与完整性。建立安全通道的智能密码钥匙、安全控件、安全网关等产品由网银系统统一管理。其中数字证书相关内容应满足 7.3 的要求
		访问控制信息完整性	
		通信数据完整性	
		通信数据机密性	
		集中管理通道安全	
		密码模块实现	在满足 7.4 要求的基础上，宜优先选用符合GM/T 0028三级密码模块标准的智能密码钥匙、安全网关等产品
	设备和计算安全	身份鉴别	网银系统的管理员、操作员等不同用户，每个用户都应有自己唯一的身份标识，PIN 码定期更换且有一定的强度要求
		访问控制信息完整性	使用 MAC 或数字签名等密码技术保证系统配置、状态控制、日常维护等操作过程中系统控制信息的完整性
		敏感标记的完整性	系统的配置信息、应用信息等重要资源的敏感标记 采用 MAC 或数字签名等密码技术保证标记的完整性
		日志记录完整性	系统日志采用 MAC 或数字签名等密码技术保证完整性
		远程管理身份证鉴别信息机密性	系统采用远程登录的方式进行配置管理时，要保证身份鉴别信息的机密性，不能被伪造或重放
		重要程序或文件完整性	采用基于加密机、智能密码钥匙等安全设备作为信任根的信任链，实现对客户端、系统功能、数据文件、管理配置等程序和文件的完整性保护
		密码模块实现	宜优先选用符合 GM/T 0028 三级密码模块标准的智能密码钥匙、加密机、验签服务器等产品

表 A.1（续）

指标			要求
技术要求	应用和数据安全	身份鉴别	用户使用的智能密码钥匙、动态令牌等等密码设备进行用户身份鉴别
		访问控制	用户使用网上银行系统时，通过安全通道保护信息传输安全性的基础上，基于传输数据的 MAC 或数字签名等密码技术保证控制信息的完整性
		数据传输安全	用户使用网上银行系统时，客户端与后台建立安全通道，对业务数据进行保护
		数据存储安全	系统中用户资产信息等重要业务数据需要加密存储
		日志记录完整性	系统日志采用 MAC 或数字签名等密码技术保证完整性
		重要应用程序的加载和卸载	业务系统功能模块修改之前需要确认权限的正确有效
		密码模块实现	宜优先选用符合 GM/T 0028 三级密码模块标准的智能密码钥匙、动态令牌、加密机、验签服务器等产品
密钥管理	生成		在 7.2.2 的要求基础上，密钥生成设备应具备检查和剔除弱密钥的能力，系统应当生成密钥审计信息
	存储		在 7.2.3 的要求基础上，应具有密钥泄露时的应急处理和响应措施
	使用		在 7.2.4 的要求基础上，应有安全措施防止智能密码钥匙及加密机等密码设备中的密钥泄露或替换，并周期更新密钥
	分发		保证智能密码钥匙、加密机、签名验签服务器等密码设备的密钥分发过程安全
	导入与导出		保证智能密码钥匙、加密机、签名验签服务器等密码设备的密钥导入及导出的安全
	备份与恢复		在 7.2.5 的要求基础上，密钥的备份与恢复在记录操作时要生成审计信息
	归档		在 7.2.5 的要求基础上，归档密钥要生成审计信息并进行归档密钥备份
	销毁		在 7.2.5 的要求基础上，要明确密钥销毁措施
安全管理	制度	制定密码安全管理制度	制定涵盖物理和环境安全、网络和通讯安全、设备和计算机安全、应用和数据安全以及密钥管理方面的密码安全管理制度
		定期修订安全管理制度	密码安全管理制度能够根据执行过程中的实际效果反馈定期修订
		明确管理制度发布流程	有明确的管理制度发布流程
	人员	了解并遵守密码相关法律法规	网上银行系统相关工作人员要能准确了解并遵守密码相关法律法规
		正确使用密码相关产品	网上银行系统研发、操作、运维、管理、审计相关人员能够正确使用密码相关产品
		建立岗位责任及人员培训制度	对于密码设备操作、运维、管理、审计及密钥管理等相关岗位建立岗位责任制度

表 A.1（续）

指标			要求
安全管理	人员	建立关键岗位人员保密制度和调离制度	对于密钥管理、密钥操作、核验审计等关键岗位建立多人共管、互相制约的保密制度，相关人员须为正式在编员工，如有违规要有岗位调离机制
		设置密码管理和技术岗位并定期考核	设有密码设备操作、运维、管理、审计等岗位，并定期对工作内容进行考核
	实施	规划	网上银行系统的密码技术应用相关模块、设备、功能，应制定统一的实施规划，并组织专家评审
		建设	网上银行系统建设时，应有明确的实施方案，选用经国家密码管理部门核准的产品或密码服务
		运行	网上银行系统运行前应经密码测评机构进行安全评估；系统投入运行后应每年委托密码测评机构开展安全评估
	应急	应急预案	应制定网上银行业务应急预案
		事件处置	网上银行系统紧急情况发生时，应按照预案结合实际情况及时处理
		向有关主管部门上报处置情况	网上银行系统发生密码技术相关事故后及时向同级密码主管部门进行报告