ICS 35.020
I642

T/ SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/ SIA 005—2018

个人金融短信处理、传送、监控及管理技术规范

Technical specification for personal financial Short Message Service（SMS） processing, transmission, monitoring and management

2018–6–20 发布　　2018–7–20 实施

中国软件行业协会　发 布

目次

前　言

本标准按照GB/T 1.1-2009 给出的规则起草。

本标准由中国软件行业协会提出并归口。

本标准起草单位：中国信息协会、中国社会经济系统分析研究会、联动优势科技有限公司、北京软件和信息服务业协会、中国建设银行青岛市分行、交通银行股份有限公司、上海浦东发展银行股份有限公司郑州分行。

本标准主要起草人：方亚南、付晓宇、周德铭、朱玉、张伟毅、张耀、陈超峰、张毅、龙飞、李建民、于乐、邢皓、李卉、卢光明、崔洪清、高强、王荣凯、张然、高睿泽、冯伟睿、张钹。

本标准为首次制定。

个人金融短信处理、传送、监控及管理技术规范

1 范围

本标准对个人金融短信的提供方、服务方、监管方，提出了处理、传送、监控及管理过程中的安全技术管理的要求。

本标准适用于规范各类组织的个人金融短信处理活动，也适用于主管监管部门、第三方评估机构等组织对个人金融短信处理活动进行监督、管理和评估。

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。

《中华人民共和国电子签名法》

中国人民银行金融消费者权益保护实施办法银发〔2016〕314号

GB/T 15278-1994 信息处理 数据加密 物理层互操作性要求

GB/T20270-2006 信息安全技术网络基础安全技术要求

GB/T 20988-2007 信息安全技术信息系统灾难恢复规范

GB/T20273-2006 信息安全技术数据库管理系统安全技术要求

GB/T20009-2005 信息安全技术数据库管理系统安全评估准则

GB/T 22080 信息技术信息安全管理体系要求

GB/T 22081 信息技术信息安全管理实用规则

GB/Z 20985 信息技术安全技术信息安全事件管理指南

JR/T 0098.8-2012 中国金融移动支付检测规范第8部分：个人金融信息保护

T/SIA 001-2017 企业个人信息安全管理规范

3 术语、定义和缩略图

3.1 术语和定义

T/SIA 001-2017 中界定的以及下列术语和定义适用于本文件。

3.1.1

金融机构 Financial institution

从事金融服务业有关的金融中介机构，包括银行、证券公司、保险公司、信托投资公司、基金管理公司、第三方支付公司、互联网金融机构、金融租赁公司、财务公司及其他从事金融服务的机构。

3.1.2

个人金融信息 Personal financial information

金融机构通过开展业务或者其他渠道获取、加工和保存的与金融相关的个人信息，包括账户信息、金融交易信息及其他反映特定个人某些情况的信息。

a)个人账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等；

b)个人金融交易信息，包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人金融信息和用户在通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人金融信息等；

c）在与个人建立业务关系过程中获取、保存的其它个人金融信息。

3.1.3

个人金融信息主体 Personal financial information subject

可通过个人金融信息识别的特定的自然人，以下简称用户。

3.1.4

个人金融信息管理者 Personal financial information manager

获得个人金融信息主体同意和授权，基于合法、正当、必要的目的，决定个人金融信息处理方式，实际控制个人金融信息的企业。

3.1.5

个人金融短信 Personal financial short message

金融机构利用电信短消息功能向其用户手机发送的和该用户相关的账户变动情况、身份验证信息、业务通知信息等个人金融信息内容的短信息。

3.1.6

密钥管理 Key management

国家相关部门允许使用的密钥管理办法。

3.1.7

监控管理平台 Monitoring and management platform

监控管理内容包括但不限于：类别、格式、流量、报警信息、发送结果、违法信息结果。管理内容包括但不限于：互动管理、格式审查、安全审查、发送管理、风险分析、报警管理。

3.1.8

状态报告 Status report

短消息传送给电信运营商短信发送网关之后，短信发送网关返回的短消息发送结果报告。

3.2 缩略语

3.2.1

ISMS Information Security Management System 信息安全管理体系

3.2.2

PISMS Personal Information Security Management System 个人信息安全管理体系

3.2.3

ITSS Information Technology Service Standards 信息技术服务标准

3.2.4

WORM Write Once, Read Many 一次写入，多次读取的数据存储功能

4 基本要求

4.1 原则

a)目的明确原则。处理个人金融信息具有合法、正当、必要的目的，不扩大使用范围，不在个人金融信息主体不知情的情况下改变处理个人金融信息的目的；

b)安全保障原则。采取适当的、与个人金融信息遭受损害的可能性和严重性相适应的管理措施和技术手段保护个人金融信息，防止未经授权的检索、披露及丢失、泄露、损毁和篡改个人金融信息；

c)诚信履行原则。按照收集时的承诺，或基于法定事由处理个人金融信息，在达到既定目的后不再继续处理个人金融信息；

d)责任明确原则。明确个人金融信息处理过程中的责任，采取相应的措施落实相关责任，并对个人金融信息处理过程进行记录以便于追溯。

e)隐私保护原则。通过技术手段、提供隐私保护服务功能、强化内部管理等办法充分保护用户的个人金融信息安全。

f)效率原则。指在规定的条件下和规定的时间内，通过技术手段保证个人金融短信处理各个环节连续提供服务。

g)可靠性原则。在主系统异常情况下，应及时切换到备用系统，确保个人金融短信处理各个环节连续提供服务。

h)信息共享原则。应建立统一的“黑名单”信息库，实现各金融机构之间的风险信息共享。

4.2 企业责任

4.2.1 法律责任

企业应承担的法律责任包括：

a)处理个人金融信息不得违反法律、法规；

b)发生重大安全事件时，应及时向相关监管机构报告；

c)在业务处理过程中，未做好风险防范工作，应承担相应的民事责任、刑事责任或行政责任。

4.2.2 管理责任

企业应承担的管理责任包括但不限于：

a)应建立有效的个人金融信息安全管理体系，落实个人金融信息管理责任；

b)应对个人金融信息处理过程采取必要、恰当的安全管理措施和技术手段，防止个人金融信息被滥用、篡改、泄露、损毁、丢失等，保证个人金融信息的完整性、准确性、可用性、保密性。

5 金融机构个人金融短信的生成与处理

5.1 个人金融短信的内容要求

5.1.1 内容合法

金融机构在生成个人金融短信时，应保证内容合法，不应包含敏感政治倾向、暴力倾向、不健康色彩的词或其它不文明用语。

5.1.2 隐私保护

金融机构在生成个人金融短信时，应注意用户的隐私保护，除必要情形外，不应出现用户姓名、证件号码、账户、余额等敏感信息。

5.2 个人金融短信分类

金融机构应根据个人金融短信来源、内容及风险级别等条件，对个人金融短信进行分类管理，不同分类的个人金融短信具有不同的信息编码格式及处理优先级。

5.2.1 警示类个人金融短信

警示类个人金融短信是金融机构向个人用户发送的、用于警示风险的个人金融短信。警示类个人金融短信有以下两种信息来源：

a)金融机构主动识别用户账户可疑的交易行为，生成警示个人金融短信发送给用户，向用户提醒风险。

b)监控管理平台通过数据分析，识别用户账户可疑行为并反馈给金融机构，金融机构根据反馈信息，采取适当的风控措施，包括发送警示个人金融短信或其他方式向用户提示风险等。

5.2.2 验证码类个人金融短信

验证码类个人金融短信是用户在金融机构注册、登录、交易时，金融机构向用户发送的用于验证用户身份的个人金融短信。

5.2.3 高风险交易类个人金融短信

高风险交易类个人金融短信是金融机构识别用户账户交易行为具有潜在风险,为保证金融安全，向用户发送的具有明显提示的个人金融短信。具有潜在风险的交易行为包括但不限于以下行为：

a)账户长时间沉默后的第一笔交易

b)按照国家反洗钱法规所规定的单笔大额交易

c)境内交易之后的境外第一笔交易

d)连续大额消费

e)极短时间内异地交易

f)短时间内大量交易次数

g)不符合用户过往习惯的交易

h)敏感时段的交易

i)敏感地域的交易

j)其它金融机构认定的异常交易

5.2.4 周期提醒类个人金融短信

金融机构应周期生成用户账户报告，通过个人金融短信发送给用户，保障用户账户安全，为保证用户及时了解账户情况，账户总结报告至少每月生成一次。金融机构应针对还款、逾期等情况周期生成提醒通知。

5.2.5 一般交易类个人金融短信

一般交易类个人金融短信是指金融机构未发现异常的用户交易，向用户发送的包括该次交易信息的个人金融短信。

5.2.6 交互类个人金融短信

交互类个人金融短信是金融机构与用户交互而发送的个人金融短信。从交互源头区分，又可分为主动交互、被动交互两类。

a)主动交互类：指金融机构主动向用户推送的，并与用户产生信息交互的个人金融短信。如金融机构主动向用户发送分期说明，要求用户回复；用户回复分3期；金融机构对用户分期进行处理并向用户通知分期成功，每期还款额度等。

b)被动交互类：指用户主动通过上行信息与银行产生交互的个人金融短信。如用户向金融机构发送上行指令，要求查询余额；金融机构收到上行指令，查询到用户的余额信息，生成个人金融短信，发送给用户。

5.2.7 用户关怀类个人金融短信

用户关怀类个人金融短信是金融机构发送给用户的业务介绍、产品介绍、用户关怀、营销等信息。

5.3 个人金融短信格式

5.3.1 基本格式

5.3.1.1 个人金融短信分类

个人金融短信格式中需包含个人金融短信分类，个人金融短信分类的详细说明见《个人金融短信分类》章节。

5.3.1.2 个人金融短信编码

个人金融短信编码是个人金融短信发送处理平台为每个个人用户手机号生成的连续、唯一的编码，用户可根据个人金融短信内容中该编码的连续性判断个人金融短信来源的合法性，防范如伪基站、改号软件等假冒金融机构发送虚假短信欺诈等风险。

5.3.1.3 个人金融短信溯源

金融机构在生成和传送个人金融短信时，应在处理的各个环节保留日志，确保每条个人金融短信能够溯源。

5.3.1.4 个人金融短信正文

个人金融短信正文中应包含个人金融短信签名和要发送给用户的正文内容。个人金融短信签名是包含在个人金融短信正文内，采用“【XXXX】”格式标识个人金融短信发送者的身份。

5.3.1.5 有效期

金融机构应在个人金融短信传输报文中包含个人金融短信的有效期，超过有效期的个人金融短信不再发送给用户。

5.3.1.6 上下文关联字串

上下文关联字串是指个人金融短信中头部和尾部包含的各一段4-6位符号串（以下简称关联串，由数字、字母任意混合组成），每条个人金融短信中的头部的关联串，必须与该用户的上一条信息的尾部关联串相同，每条个人金融短信的尾部的关联串，与下一条该用户的个人金融信息的头部的关联串相同。用户可以很方便地根据个人金融短信内容中头、尾关联串的一致性，判断个人金融短信来源的合法性，防范如伪基站、改号软件等假冒金融机构发送虚假短信欺诈等风险。该信息是金融机构生成个人金融信息时的可选项。

5.3.2 警示类个人金融短信格式

a)警示类个人金融短信正文中应添加显著的警示标识，用于提醒用户。

b)警示类个人金融短信正文中应添加紧急止损方式说明（如回复某个指令可即时冻结该个人账户），使用户在紧急情况（如盗刷）下避免损失继续扩大。

c)警示类个人金融短信正文中应添加紧急联络方式，该联络方式要求金融机构安排专职人员24小时值守，使用户在紧急情况下能迅速与金融机构取得联系。

5.3.3 验证码类个人金融短信格式

a)验证码类个人金融短信正文中应明确验证码发送方。

b)验证码类个人金融短信正文中应明确提示用户防范风险，包括但不限于提醒用户不能将验证码告知他人、在指定的时间内、渠道上使用该验证码等。

5.3.4 高风险交易类个人金融短信格式

参见5.3.2警示类格式。

5.3.5 周期提醒类个人金融短信格式

周期提醒类个人金融短信中应包含用户在当前报告周期中的账户总体变动及余额情况。

5.3.6 一般交易类个人金融短信格式

一般交易类个人金融短信中应包含用户交易时间、交易商户、交易金额等情况。

5.3.7 交互类个人金融短信格式

交互类个人金融短信中应包含交互标识，保证交互内容可识别。

5.3.8 用户关怀类个人金融短信格式

用户关怀类个人金融短信包含金融机构对用户的节假日关怀问候、金融理财产品推荐等内容。

5.4 个人金融短信退订

其它类型的个人金融短信可由金融机构根据自身业务情况自行处理。

5.4.1 可退订个人金融短信类型

为避免垃圾个人金融短信骚扰，部分类型个人金融短信中应包含退订个人金融短信的方式说明，退订说明中应明确该类型个人金融短信的退订方式。

a)周期提醒类

b)主动交互类

c)用户关怀类

5.4.2 不可退订个人金融短信类型

为保障用户账户安全，避免金融风险，部分类型个人金融短信不应提供退订功能。

a)警示类

b)高风险交易类

5.4.3 其他类型个人金融短信

用户退订时可按照个人金融短信分类退订，金融机构不应向用户发送已退订分类的个人金融短信。

5.5 信息反馈接收和处理

5.5.1 状态报告接收与处理

金融机构应提供状态报告接收的接口，接收监控管理平台发送的状态报告。金融机构应根据状态报告进行风险分析。

5.5.2 用户上行个人金融短信接收与处理

金融机构应提供上行个人金融短信接收的接口，接收监控管理平台发送的上行个人金融短信。金融机构应正确处理用户上行的退订信息。金融机构应及时处理用户上行的应急止损请求。

5.5.3 监控管理平台上传的风险提示信息接收与处理

金融机构应提供风险提示接收的接口，接收监控管理平台发送的风险提示。金融机构应对监控管理平台发送的风险提示进行跟踪、处理，防范可能的金融风险。

6 金融机构与监控管理平台间的信息传输

6.1 传输安全

6.1.1 传输加密

金融机构与监控管理平台间的信息应加密传输。加密标准应遵循《信息处理 数据加密 物理层互操作性要求》（GB/T 15278-1994）。

6.1.2 身份认证

金融机构与监控管理平台之间的信息交互应进行身份认证。身份认证包括但不限于用户密码认证。

6.1.3 网络安全

金融机构与监控管理平台之间的网络安全应遵循《信息安全技术网络基础安全技术要求》（GB/T 20270-2006）。

6.2 传输连续性

金融机构与监控管理平台之间的信息交互应具备断点续传功能，在传输中断后，从中断处续传消息，保证消息的完整性。金融机构与监控管理平台之间的信息交互应具备超时重发功能，在消息超时后进行重发，避免消息丢失。

6.3 单点接入

监控管理平台应向金融机构提供统一的与中国移动、中国电信、中国联通三大运营商对接的入口，方便金融机构接入。

7 监控管理平台个人金融短信处理及性能

7.1 功能类

7.1.1 格式审查

监控管理平台在处理金融机构发送的个人金融短信时，应进行格式审查。格式错误的个人金融短信应通知金融机构，不进行发送。格式审查包括但不限于：

a)分类审查

b)编码审查

c)签名审查

7.1.2 黑名单过滤

监控管理平台在处理金融机构发送的个人金融短信时，应进行黑名单过滤。在黑名单中的手机号码应反馈给金融机构，不进行发送。

7.1.3 敏感词过滤

监控管理平台在处理金融机构发送的个人金融短信时，应进行敏感词过滤。包含敏感词的个人金融短信应反馈给金融机构，不进行发送，必要时进行报警处理。

7.1.4 过期检测

监控管理平台应具备个人金融短信过期检测的功能，已过有效期的个人金融短信应反馈给金融机构，不进行发送。

7.1.5 长个人金融短信拆分

监控管理平台应具备长个人金融短信拆分功能，对超长的个人金融短信进行拆分后发送的能力。

7.1.6 个人金融短信路由

监控管理平台应具备个人金融短信路由选择功能，对手机号码进行路由选择，将个人金融短信发送到相应的运营商或国外运营商。

7.1.7 状态报告处理

a)监控管理平台应提供接口，接收电信运营商短信网关返回的个人金融短信状态报告。

b)监控管理平台应将状态报告结果返回给金融机构。

c)监控管理平台应对状态报告结果进行实时分析，识别风险交易，向金融机构发送风险提示。

d)监控管理平台对按规定时间未收到状态报告返回的个人金融短信进行相应处理，包括但不限于重发、通知金融机构等措施。

7.1.8 上行个人金融短信处理

a)监控管理平台应提供接口，接收电信运营商短信网关发出的上行信息。

b)监控管理平台应根据相应业务规则，将上行个人金融短信路由到对应的金融机构。

7.2 非功能类

7.2.1 处理性能

a)监控管理平台的性能指标应满足金融机构个人金融短信发送的要求，单机构不应低于3000条/秒，监控管理平台总处理性能不应低于15000条/秒。

b)监控管理平台应及时对金融机构、电信运营商短信网关的请求进行应答，平均应答时间不超过50毫秒，最大响应时间不超过3秒。

c)监控管理平台应具备异常状况下的消息缓存能力，当遭遇网络、网关异常无法进行个人金融短信发送时，系统应能缓存金融机构的个人金融短信，并在有效期内，异常情况恢复后可以继续下发。缓存数量及缓存有效期均可由平台管理员设置。

d)监控管理平台应及时处理消息，在正常情况下，每条消息在监控管理平台停留的时间不应超过1秒。

e)监控管理平台应具备流量控制功能，向电信运营商短信网关发送个人金融短信的速度不应超过网关的限定值。

7.2.4 平台可用性

a)应用软件可用性。监控管理平台应用软件应采用分布式、高可用性架构部署，任意节点故障不应影响监控管理平台整体的可用性，整体可用性至少应达到99.99%

b)通道可用性。监控管理平台应提供备用通道，在主通道故障时，及时切换至备用通道。

7.2.5 平台处理能力扩容

a)监控管理平台应提供平滑的扩容方案，在金融机构业务量增大的情况下，提升处理能力，保障业务的稳定性、连续性。

b)监控管理平台应提供应急扩容方案，应对突发的流量洪峰。

7.2.6 平台容灾

监控管理平台应提供灾备方案，在系统、硬件、机房等故障时，为金融机构提供不间断发送个人金融短信的能力，保障金融机构业务的稳定性、连续性。容灾方案包括但不限于以下内容：

a)备用业务处理系统

b)备用网络

c)备用基础设置

d)数据备份系统

e)技术支持能力

f)运行维护管理能力

8 监控管理平台与电信运营商短信网关间信息传输

8.1 传输安全

8.1.1 传输加密

监控管理平台与电信运营商短信网关间的信息应加密传输。加密标准应遵循《信息处理 数据加密 物理层互操作性要求》（GB/T 15278-1994）。

8.1.2 身份认证

金融机构与监控管理平台之间的信息交互应进行身份认证。

8.1.3 网络安全

金融机构与监控管理平台之间的网络应遵循《信息安全技术网络基础安全技术要求》（GB/T 20270-2006）。

8.2 传输连续性

监控管理平台应采取技术手段，保证发送到用户手机上个人金融短信的编码连续性。监控管理平台与电信运营商短信网关的信息交互应具备断点续传功能，在传输中断后，从中断处续传消息，保证消息的完整性。监控管理平台与电信运营商短信网关的信息交互应具备超时重发功能，在消息超时后进行重发，避免消息丢失。

8.3 优先传输

监控管理平台应提供优先级功能，在收到高优先级消息时，插入当前消息的发送队列中，使高优先级消息能优先发送。高优先级的个人金融短信发送，有可能出现短信插队现象，导致破坏了短信编码的连续性，监控管理平台应在发送后续短信时重新编号，确保用户收到的个人金融短信编码的连续性。

8.4 运营商适配

监控管理平台应适配国内中国移动、中国联通、中国电信运营商及海外运营商。

9 电信运营商短信网关个人金融短信处理

9.1 格式审查

电信运营商短信网关在处理监控管理平台发送的的个人金融短信时，应进行格式审查。格式错误的个人金融短信应通知监控管理平台，不进行发送。格式审查包括但不限于签名审查，签名应符合《中华人民共和国电子签名法》。

9.2 黑名单过滤

电信运营商短信网关在处理监控管理平台发送的个人金融短信时，应进行黑名单过滤。在黑名单中的手机号码应反馈给监控管理平台，不进行发送。

9.3 敏感词过滤

电信运营商短信网关在处理监控管理平台发送的个人金融短信时，应进行敏感词过滤。包含敏感词的个人金融短信应反馈给监控管理平台，不进行发送，必要时进行报警处理。

9.4 个人金融短信发送

电信运营商短信网关应及时将个人金融短信发送到用户手机。如遇用户未开机、不在服务区等情况，电信运营商短信网关至少应将个人金融短信缓存48小时，48小时候如仍未发送成功，则返回相应的状态报告。

9.5 状态报告生成

a)电信运营商短信网关在将个人金融短信发送给用户手机后，应及时生成状态报告，并将状态报告反馈给监控管理平台。

b)电信运营商短信网关如未成功发送个人金融短信给用户（如空号、敏感词等），应及时生成相应的状态报告，并将状态报告反馈给监控管理平台。

c)电信运营商短信网关如未成功反馈状态报给监控管理平台，应周期性尝试重发。尝试时间应不少于24小时，重试间隔应不大于30分钟。

9.6 上行个人金融短信处理

电信运营商短信网关在收到用户上行个人金融短信时，应及时将上行个人金融短信发送到监控管理平台，必要时进行长个人金融短信拆分处理。电信运营商短信网关如未成功反馈状态报给监控管理平台，应周期性尝试重发。尝试时间应不少于24小时，重试间隔应不大于30分钟。

10 个人金融短信存储

参照《金融行业信息系统信息安全等级保护实施指引》（JRT0071-2012），个人金融信息应存储于专用的数据库内，并制定数据存储架构安全规则和管理规范，包括数据访问控制规则、数据存储转移安全规则、数据存储完整性和多副本一致性管理规则、重要数据加密规则等。并采取措施确保个人金融信息的完整性、准确性、可用性、保密性，避免个人金融信息的滥用、篡改或丢失。

10.1 存储安全

10.1.1 备份与恢复

通过执行定期的数据复制、备份和恢复，实现对存储数据的冗余性管理，保护数据的有效性。应满足《信息系统灾难恢复规范》（GB/T 20988-2007）中灾难恢复等级第六级要求。

a)应支持自动备份、手动备份、增量备份、全备份、同步备份、异步备份、本地备份、异地备份。

b)应支持卷镜像和快照的方式提供数据的备份与恢复功能。

c)应支持通过远程复制的方式提供数据的备份与恢复功能。

d)应制定对不同一致性水平要求的冗余数据提供不同等级的安全保护机制。

e)应具备数据副本存储的多种压缩策略和实现机制，并确保压缩数据副本的完整性和可用性。

10.1.2 访问控制

基于金融机构数据存储安全需求建立数据访问控制机制，防止对存储数据的未授权访问风险。应满足《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2006）中的第五级访问验证保护级要求。

a)应为存储系统安全管理员提供操作员标识与鉴别策略、数据访问控制策略，及其相关的操作规程。

b)应利用数据存储访问控制模块实施用户标识与鉴别策略、数据访问控制策略，并实现相关安全控制措施。

c)应提供访问控制时效的管理和验证，以及接入数据存储的合法性和安全性认证。

d)应提供主动防御机制或措施，如基于用户行为或设备行为安全分析机制。

10.1.3 防病毒

应支持防病毒软件扫描，防止系统或文件被病毒感染。

10.1.4 磁盘阵列数据安全机制

应支持通过配置RAID5保障存储数据的可靠性。

10.1.5 存储容量

系统的数据存储容量应满足对金融信息保存的时限要求。并提供数据存储剩余空间预警机制，当剩余存储空间低于阈值时进行告警。在存储空间达到预警指标时，能够采用自动转储等方式将数据备份到其他存储空间。

10.2 存储架构

应考虑金融机构的数据量增长、数据存储安全需求和合规性要求，制定适当的存储架构，以实现对存储数据的有效保护。

a)应建立可伸缩的分布式数据存储架构，满足数据量持续增长、数据快速读写需求。

b)应具备数据存储跨机柜、跨机房容错部署能力。

c)应提供分层的数据存储加密架构，满足应用层、操作系统层、存储层等层次数据存储加密要求。

10.3 数据完整性

应对存储的数据进行完整性保护具备如下功能：

a)应提供对存储内的数据检测是否存在完整性错误的功能；

b)在检测到数据存在完整性错误时，应能提供必要的恢复措施；

c)可支持WORM功能，应提供对于数据一次写入多次读取功能。

10.4 数据保密性

应对存储的数据的保密性进行保护，要求包含以下内容：

a)应支持通过符合国家规定的加密产品对存储的数据进行加密；

b)应对数据采用非明文存储或其他安全存储机制，保证数据即使被窃取也无法利用：

c)口令、密钥等信息不应明文存储在本地，须加密保护；对数据的访问应有认证、授权或加解密机制，对于认证凭据的安全存储，在不需要还原明文的场景下，应使用不可逆算法加密；

d)不应在URL、日志、错误消息、调试信息中暴露口令、密钥、银行账号、会话标识符等信息。

10.5 数据时效性

对金融监控管理平台管理员的要求：

a)个人金融短信保存期限应为实现目的所必需的最短时间。

b)超出上述个人金融短信保存期限后，应对金融信息进行删除或匿名化处理。

10.6 去标识化处理

应对个人敏感信息的存储采用假名化、碎片化、加密、加噪等技术脱敏后存储。

10.7 分离、索引、独立加密保存

应将个人金融短信处理中涉及的相关信息分割为三个部分独立加密存储，这三个部分分别是手机号、发送的短信内容、外围信息（短信类别、发送时间等）。三个部分的信息应采用不同的加密解密密钥体系，各部分信息之间应采用统一的编码进行索引关联。以保证某个部分的信息被窃取时，窃取者无法获得完整的信息。

11 监控管理平台监控

11.1 监控管理平台监控通知方式

应支持邮件、个人金融短信、语音拨号和桌面等多种报警方式，确保管理员可以及

时掌握系统的运行情况。

11.2 IT资源监控

11.2.1 服务器监控

可实时监控服务器CPU利用率、内存利用率、磁盘利用率、进程状态、带宽容量和应用程序的性能等，并确保主服务器出现故障时自动切换到备用服务器。

11.2.2 网络监控

可监控网络系统的硬件、软件及其系统中的数据等，不应因偶然的或者恶意的原因而遭受到破坏、更改、泄露，及时报警以保证系统连续可靠正常地运行，网络服务不中断。

11.2.3 中间件监控

可监控Weblogic、MQ等中间件的配置信息管理、故障监控、性能监控等，及时报警以确保中间件持续稳定运行。

11.2.4 应用软件监控

可实时监控和掌握应用软件内存利用率、磁盘利用率和应用程序的性能等，及时报警以确保应用软件稳定运行。

11.2.5 数据库监控

可监控请求数、连接数、最大事务执行时间、恶意的SQL注入行为、非法的业务登录、高危的SQL操作和过量的数据下载等，及时报警以确保数据库连续稳定运行。

11.3 业务监控

11.3.1 业务流量监控

应具备监控个人金融短信实时发送量的功能。

11.3.2 发送状态监控

可以监控如下的发送状态：

a)发送无响应

b)发送成功无回执

c)网关响应失败

d)通道连接异常等

11.4 操作行为监控

应建设统一的运维管理平台，实现对人员、设备、操作的统一管理，及运维管理的白盒透明化，实现认证、权限、审计、口令等操作的集中管理，最终形成一个完整安全的运维监控管理。并将各项运维管理规章制度以可监控的方式进行管理落地。

11.5 用户风险监控

11.5.1 个人金融短信查询

监控管理平台应提供：

a)监管方、发送方、风控平台等多方查询。

b)手机号、时间、个人金融短信内容关键字等多种查询方式。

c)用户通过上行指令方式获取近期发送的个人金融短信。

11.5.2 高风险交易监控

特征符合5.2.3的高风险交易，应向监管机构、用户、金融机构预警。

11.5.3 状态报告风险监控

应对状态报告进行分析，并根据情况向金融机构端发送风险警示信息，如高风险交易未如期返回状态报告等。

11.5.4 综合数据监控

可通过数据特征、行为预测模型、实时风控、用户风险评级、用户风险画像、风控策略等大数据支撑服务对交易做出智能风险判断，并作出实时风险反馈。

a)数据特征提取。可按照账户级别（高风险、一般风险）、发送状态（发送成功、发送失败、发送异常、停机等）、状态报告（正常、异常、可疑）、交易类别、交易行为（电子大额交易关机、境外交易、连续多次交易、非归属地刷卡、睡眠卡唤醒等）、历史交易数据（金融机构内部数据和外部数据）等数据标签进行归属分类。

b)联合分析。应具备根据不同数据特征进行风险识别的功能。

c)风险反馈。应支持将联合分析后的风险识别结果向对应的金融机构预警、监管方报告并向用户发送警示信息提醒。

11.5.5 风险信息共享

打通金融机构、金融监管机构和监控管理平台的之间信息壁垒。个人金融短信监控管理平台应支持查询风险信息，风险信息包括但不限于：

a)金融机构在日常业务经营过程中发现的欺诈交易、违法违规交易等信息；

b)监管机构、公安机关和协会等提供或通报的风险信息；

c)黑名单信息；

d)监控管理平台通过大数据分析识别个人金融短信的风险信息；

12 监控管理平台的安全防护

应遵循GB/T 22080、GB/T 22081的一般方法，构建个人金融信息安全机制、策略。

12.1 安全边界

个人金融信息安全应与一般意义的信息安全的边界基本一致，主要包括：

a)实体安全：IT系统的场地、环境的安全；

b)基础平台安全：承载个人信息的各种基础平台安全；

1)网络及相关设备构成的基础平台安全；

2)承载各种应用、业务系统运行的底层系统平台安全；

3)应用系统支撑平台安全（数据库、中间件等）；

4)各种安全产品、技术等构成的平台安全等；

c)应用系统安全：各种管理、业务等应用系统安全；

d)个人金融信息数据库安全：个人金融信息数据库及各种相关信息安全；

e)数据传输安全：个人金融信息在传输过程中的安全；

f)接口安全：各种接入设备、终端安全；

g)运行安全：承载个人金融信息（及相关数据信息）系统运行的安全。

12.2 安全技术应用

个人金融信息安全应与一般意义的信息安全采用的安全技术策略基本一致：

a)应依据GB/T20273-2006、GB/T20009-2005，综合规划个人金融信息数据库相关信息安全；

b) 应基于12.1描述的安全边界，结合个人金融信息管理者的整体信息安全，统一、系统规划、模块化设计信息安全体系，特别考虑新技术应用可能产生的新的个人金融信息安全威胁；

c) 应在统一、系统规划、模块化设计基础上，基于个人金融信息管理者的实际需求，运用先进、成熟、安全、可靠的产品、技术、知识，构建金融信息安全体系，保证个人金融信息安全。

13 监控管理平台管理要求

13.1 监控管理平台运维要求

监控管理平台运维机构应遵照ITSS信息技术服务运行维护标准开展工作。

13.2 监控管理平台信息安全管理要求

运维机构应通过《信息技术 安全技术 信息安全管理体系要求》(GB/T 22080-2016)的认证，并按照建立、实施和文件化信息安全管理体系（ISMS）的要求，独立组织并实施安全控制。

13.3 操作行为管理

监控管理平台的运维机构应建立信息系统的运行与维护的操作准则，并及时跟踪、发现和解决异常的行为及可能导致的安全事故。应针对业务系统的日常操作行为，对操作权限进行控制和规范管理，如对文件的上传和下载、数据的查看范围进行权限界定。

应对不同角色的权限范围进行控制，风险指令进行控制隔离等，建立不同等级的操作授权规则。

13.4 人员管理

应明确与个人金融信息管理相关人员的权限、责任，关键岗位人员如：系统管理员、实际操作人员（业务、运营等）、数据库管理员等应通过背景审查。加强监督和管理，防范未经授权访问个人金融信息。

13.5 IT 环境安全管理

应在信息安全体系建设中，充分考虑个人金融信息及相关因素的特点，加强个人金融信息安全防护，预防安全隐患和安全威胁。如网络基础平台、系统平台、应用系统、安全系统、数据、机房环境等的安全，及信息交换中的安全防范、病毒预防和数据恢复、非传统信息安全等。