

中华人民共和国通信行业标准

YD/T 2671-2013

分权模式（金库模式） 客户信息安全保护技术要求

Privilege-divided model (JinKu-model) customer information
security protection technical specification

2013-10-17 发布

2014-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 分权模式管控原则	2
5.1 基本原则	2
5.2 管控对象	2
6 分权模式实现方式	2
6.1 实现架构	2
6.2 触发方式	2
6.3 授权方式	3
7 分权模式实现流程	4
7.1 远程授权	4
7.2 现场授权	5
7.3 自动授权	6
8 关键系统分权模式管控要求	7
8.1 管控范围	7
8.2 通信网及网管支撑关键系统管理规则	7
8.3 业务支撑关键系统管理规则	10
8.4 业务平台关键系统管理规则	11
9 分权模式实施要求	12
9.1 实施要求	12
9.2 审计要求	12
9.3 其他要求	12

前 言

本标准按照 GB/T1.1-2009 给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国移动通信集团公司、中国移动通信集团设计院有限公司。

本标准主要起草人：李 跃、张 滨、赵 刚、冯运波、刘利军、秦邱川、陈云超、张 琳、杜雪涛、任兰芳、柏洪涛。

分权模式（金库模式）客户信息安全保护技术要求

1 范围

本标准定义了利用分权模式（金库模式）进行客户信息安全保护的实施要求。

本标准适用于通信网及网管支撑系统中MSC/VLR/ MGW、HLR、WAP网关、网管客户支撑系统、信令监测系统等关键系统，业务支撑系统中BOSS、经分、CRM等关键系统，以及业务系统中定位业务平台等涉及敏感客户信息的关键系统。

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，仅所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。

- 中华人民共和国国务院令第291号 《中华人民共和国电信条例》
- 中华人民共和国信息产业部令第36号 《电信服务规范》
- 中华人民共和国信息产业部令第7号 《电信用户申诉处理暂行办法》

3 术语和定义

下列术语和定义适用于本文件。

3.1

分权模式（金库模式）

对于涉及到客户敏感信息的高风险操作，强制要求必须由两人或以上有相应权限的员工共同协作完成操作，防止部分拥有高权限账号的操作人员滥用权限违规获取、篡改相关信息，通过相互监督、利益制约确保高风险操作和高价值信息的安全性，也称为“双人操作”或“多人操作”模式。

4 缩略语

下列缩略语适用于本文件。

BSS/OSS	Business Support System/ Operations Support System	业务支撑系统/运营支撑系统
CRM	Customer Relationship Management	客户关系管理
EOMS	Electric Operation Maintenance System	电子运维系统
HLR	Home Location Register	用户归属位置寄存器
MGW	Media GateWay	媒体网关
MSC	Mobile Switching Center	移动交换中心
VLR	Visitor Location Register	访问用户位置寄存器
WAP	Wireless Application Protocol	无线应用协议

5 分权模式管控原则

5.1 基本原则

对涉及客户资料、订购关系、位置信息、客户通话详单等高价值信息的关键系统的高风险操作，进行分权模式管控，用以保护客户信息安全。

分权模式的实施应遵循如下基本原则：

- 1) 聚焦关键系统、聚焦高风险操作、聚焦高价值信息；
- 2) 敏感操作，多人完成，分权制衡；
- 3) 授权不操作，操作不授权。

5.2 管控对象

分权模式的管控对象为关键系统的高风险操作：

- a) 关键系统：存储客户资料、订购关系、位置信息、客户通话详单等高价值信息的系统，如BSS/OSS/经分/网管系统等；
- b) 高风险操作：可能对高价值信息产生安全隐患的操作，如批量查询、导出、变更和删除等。

6 分权模式实现方式

6.1 实现架构

在分权模式的实现中，集中的安全管控平台作为网管、业务支撑关键系统的统一运维入口，提供账号管理、认证管理、授权管理和审计管理的功能，如图1所示。

在集中的安全管控平台中含有一个分权管理模块，分权管理模块需要与集中安全管控平台的其他模块交换数据来实现分权管理所需的认证、授权等功能。当用户在应用系统进行关键操作时，业务功能触发分权管理模式并向分权管理模块发出请求，分权管理模块进行授权审批之后，用户方可根据审批结果访问或被拒绝访问敏感数据或文件。

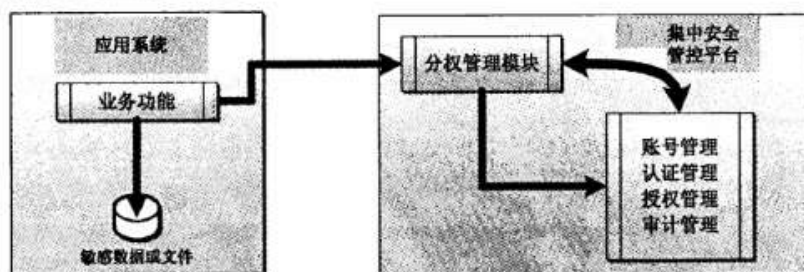


图1 分权模式实现架构

6.2 触发方式

6.2.1 基于业务操作触发

基于业务操作的触发方式是指当用户对敏感信息进行高风险操作时，触发分权模式，主要有如下两种类型：

- a) 基于图形界面访问触发

对通过图形界面访问敏感数据的操作，通过进行应用系统改造，增加分权模式控制点，当对应敏感操作的菜单或按钮被点击时，触发分权审批。

b) 基于命令行访问触发

对通过命令行访问敏感数据的操作，通过在系统中增加分权模式控制点，当敏感指令执行时，触发分权审批。

6.2.2 基于账号登录触发

基于账号登录触发方式是指当拥有高风险操作权限的账号通过系统登录时，触发分权审批。

6.2.3 基于准实时行为审计触发

对于无法做到基于业务操作和账号登录方式触发分权审批的系统，通过基于准实时行为审计进行分权模式管控。

准实时行为审计功能要求日志审计系统在24小时内对高风险操作日志进行筛选和稽核分析，并自动完成高风险操作与工单信息的匹配。对于无工单的高风险操作，触发分权告警。

在实施中，应优先采用基于业务操作和基于账号登录的分权模式触发方式，在无法实现上述两种方式的情况下，采用准实时行为审计方式作为补充。

6.3 授权方式

分权模式授权方式包括人工授权和自动授权两种方式。

人工授权方式包含如下两种场景：

a) 现场授权：分权模式触发后，授权人员通过输入认证凭据（如密码、证书、令牌和指纹等），现场完成授权。

b) 远程授权：分权模式触发后，系统向授权人员发送申请短信，短信内容应包含操作员账号、操作类型、操作对象和操作原因等信息。授权人员回复审批结果后，操作员根据审核结果继续或终止本次操作。

自动授权方式是指分权模式触发后，操作员输入本次操作的工单号或要查询的手机号，系统通过与工单系统的联动，实时对本次操作手机号和工单中授权的手机号进行比对，根据比对结果，继续或终止本次操作。

6.3.1 远程授权

集中安全管控平台应支持将操作人员发起的操作请求通过短信方式发送给授权人，授权人转发短信授权码或直接回复短信网关进行二次授权，并由集中安全管控平台提供短信授权码或回复结果的认证鉴权服务；

集中安全管控平台应确保生成的短信密码与操作人员、授权人、当次授权对应关系的唯一性。

6.3.2 现场授权

应用系统或集中安全管控平台应提供强认证信息输入界面，并应支持主账号密码、短信密码、动态令牌码、硬件证书、指纹中的一种或多种；

应用系统或集中安全管控平台应支持将操作人员、授权人的认证信息封装成授权请求发送给集中安全管控平台认证模块；

集中安全管控平台应确保生成的强认证信息与操作人员、授权人、当次授权对应关系的唯一性；

授权过程应该充分考虑安全性要求，存放和传输过程都应该加密；

授权过程中返回错误提示信息应明确告知是操作人员身份验证错误还是协同操作人授权失败。

6.3.3 自动授权

应用系统或集中安全管控平台应提供工单号输入界面, 并支持通过接口将请求转发给集中安全管控平台分权管理模块;

集中安全管控平台应支持调用工单系统的查询接口, 并根据返回信息解析、存储详细工单信息, 包括但不限于操作人信息、访问场景、访问方式、访问时间范围等信息; 有条件可以选择实现基于时间和内容的自动匹配;

在申请工单的有效时间内(操作时间段或非关闭状态), 集中安全管控平台应支持在有效期内不重复发起工单查询请求;

集中安全管控平台应确保生成的工单信息与操作人员、当次授权对应关系的唯一性;

授权过程应该充分考虑安全性要求, 存放和传输过程都应该加密;

授权过程中返回错误提示信息应明确告知是操作人员身份验证错误还是工单匹配失败。

7 分权模式实现流程

7.1 远程授权

远程授权可以采用短信方式, 授权人通过短信完成实时授权, 其中操作人与授权人的对应关系需要在分权管理模块上来维护, 并由集中安全管控平台提供短信认证鉴权服务, 如图2所示。

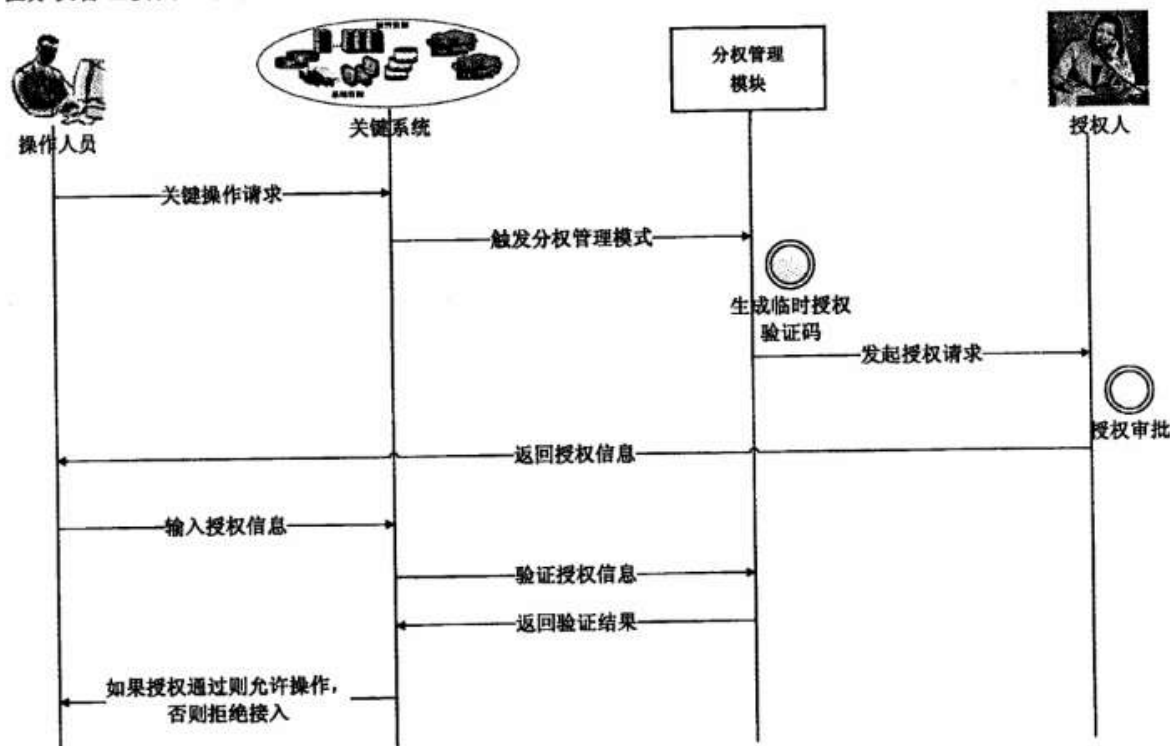


图2 远程授权模式实现流程

远程授权的实现详细流程如下:

- 当应用系统触发分权模式管理流程时, 通过接口将操作请求转发给分权管理模块;
- 分权管理模块根据操作请求, 找到授权人, 生成临时授权验证码及操作请求;
- 分权管理模块将临时授权验证码及操作请求通过短信方式发送到授权人的手机号码上;

d) 当授权人审批通过后, 可以将短信密码直接转发给当前业务操作人员, 业务操作人员在系统的密码输入界面输入收到的短信密码, 进行授权码鉴别; 或由授权人通过短信网关回复审批通过或拒绝给应用系统, 如果采用此方式, 不需要操作人员再次输入临时授权验证码;

e) 业务系统调用分权管理模块的鉴别服务, 当验证通过后, 允许当前操作人员继续此业务操作, 否则阻止此业务操作;

f) 本次分权管理模式操作完成后, 应用系统需要将操作日志发送给集中安全管控平台审计中心。

7.2 现场授权

现场授权模式需要授权人在现场, 采用主账号密码、硬件证书、动态令牌或指纹等方式进行, 授权人通过现场输入主账号密码、插入硬件证书、提供当前动态令牌码或按指纹等完成实时授权, 其中操作人与授权人的对应关系需要在分权管理模块上来实现, 并由集中安全管控平台提供主账号密码认证鉴权服务或相应其他强认证服务。现场授权模式实现流程如图3所示。

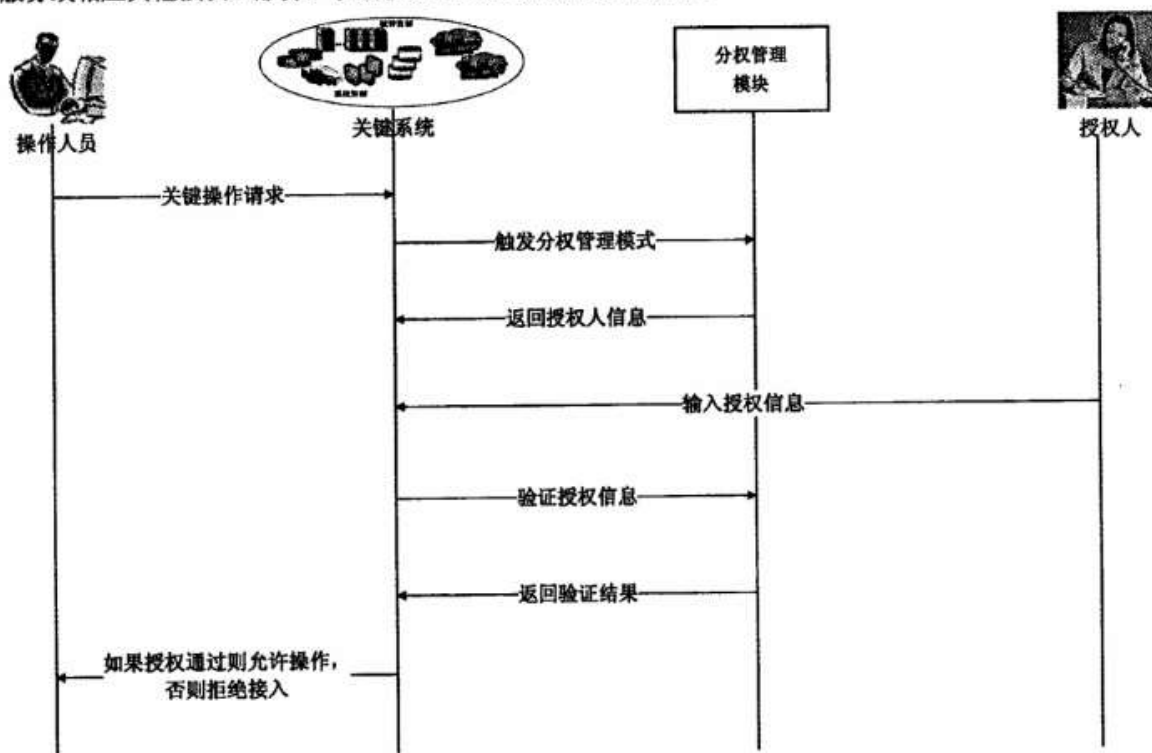


图3 现场授权模式实现流程

现场授权的实现详细流程如下:

- 当应用系统触发分权管理模式管理流程时, 通过接口将操作请求转发给分权管理模块;
- 分权管理模块根据应用系统发来的请求, 找到对应的授权人, 并向应用系统返回授权人信息;
- 应用系统弹出主账号密码、短信密码或动态令牌码输入窗口, 或弹出要求插入硬件证书、指纹的提醒信息;
- 应用系统将对主账号密码、动态令牌码、证书或指纹等信息通过集中安全管控平台认证接口转发到集中安全管控平台认证中心;

e) 集中安全管控平台验证通过后, 反馈鉴权结果给应用系统, 允许当前操作人员继续此业务操作, 否则阻止此业务操作;

f) 本次分权模式操作完成后, 应用系统需要将操作日志发送给集中安全管控平台审计中心。

7.3 自动授权

自动授权模式需要和工单系统进行联动, 一般适用于单条记录或频率比较高业务办理场景。当操作人员发起关键业务办理操作请求时, 需要在应用系统上输入审批通过后的工单号, 分权管理模块根据工单号访问工单系统进行工单的有效性验证, 并需要确认操作时间在工单的有效期内。自动授权模式实现流程如图4所示。

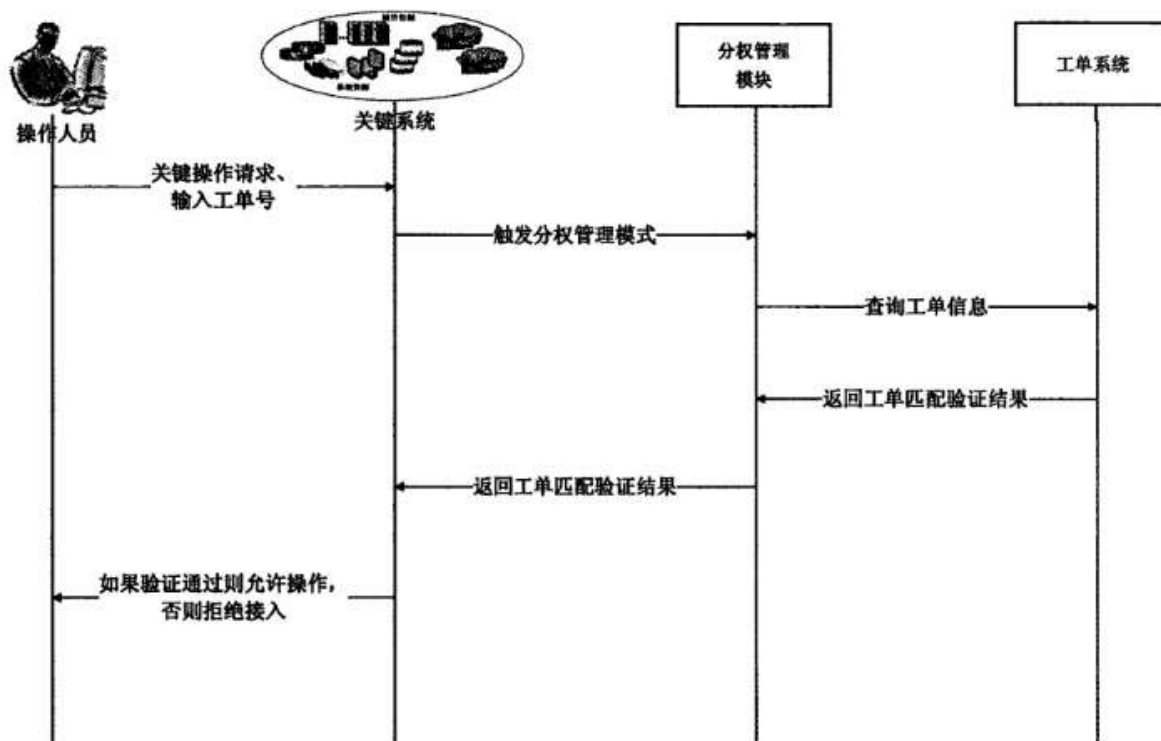


图4 自动授权模式实现流程

自动授权模式的实现详细流程如下:

- a) 操作人员发起敏感数据查询、下载请求并输入本次操作的工单号;
- b) 触发分权模式管理流程时, 通过接口将操作请求转发给分权管理模块;
- c) 分权管理模块实时查询工单系统并返回工单有效性的验证结果, 有条件可以选择实现基于时间和内容的自动匹配;
- d) 工单匹配验证通过后, 允许当前操作人员继续此系统资源操作, 否则阻止此操作;
- e) 本次分权模式操作完成后, 集中安全管控平台门户或堡垒系统需要将操作日志发送给集中安全管控平台审计中心;
- f) 集中安全管控平台审计中心需要针对工单信息以及操作内容进行事后匹配审核, 针对工单与操作不匹配的操作行为生成专门的统计报表。

8 关键系统分权模式管控要求

8.1 管控范围

分权模式需管控的关键系统、高风险操作的范围包括见表1。

表1 分权模式需管控的关键系统、敏感信息和对应的高风险操作

类别	关键系统	敏感信息	对应高风险操作
业务支撑系统	BSS/OSS	集团客户资料、个人客户资料、VIP客户资料、详单、账单、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息、资源数据、积分数据	1. 通过数据库工具访问数据库表； 2. 登录主机获取文件； 3. 无密码查询客户详单； 4. 导出/批量导出客户详单；
	CRM	集团客户资料、个人客户资料、VIP客户资料、各类特殊名单、用户密码、详单、账单、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息、资源数据、积分数据	5. 批量查询/导出/变更客户资料； 6. 批量为客户开通/变更业务； 7. 批量为客户变更账户余额； 8. 变更客户积分信息
	经分	集团客户资料、个人客户资料、各类特殊名单、详单、账单、客户消费信息、基本业务订购关系、增值业务（含数据业务）订购关系、增值业务信息、统计报表、渠道及合作伙伴资料、资源数据	1. 批量查询/导出客户资料； 2. 导出经营分析统计报表；
通信网及网管支撑系统	MSC/VLR/MGW	客户位置信息	1. 查询客户位置信息
	HLR	客户位置信息、鉴权信息	1. 查询客户位置信息
	WAP网关	用户上网记录、彩信记录	1. 查询用户上网记录
	网管（客户支撑系统）	位置信息、通信记录	1. 查询客户位置信息 2. 查询客户通信记录
	网管（信令监测系统）	位置信息（准实时）、通话记录（主被叫号码、通话时间）	1. 查询客户位置信息； 2. 查询/导出客户通信记录；
业务平台	重要业务平台	位置信息、订购关系、好友名单、通信录等	1. 用户位置即时定位查询； 2. 导出用户订购关系； 3. 导出好友名单、通信录等

8.2 通信网及网管支撑关键系统管理规则

8.2.1 MSC/VLR/MGW

MSC/VLR/MGW负责所有的呼叫控制信令和承载话务，是交换网的核心网元，其维护操作主要是由系统维护人员通过命令行方式进行的。

MSC/VLR/MGW存储的敏感客户信息主要为客户位置信息。

MSC/VLR/MGW的敏感客户信息获取途径，主要为通过登录网元，使用命令行方式对客户信息进行查询。

方式1：如果网元支持基于特定操作的授权，应仅将位置信息查询操作权限赋予个别特权账号，特权账号在集中安全管控平台系统登入时触发分权模式审批。

方式2：禁止系统维护人员直接访问网元进行客户位置信息查询操作，统一通过网管客户支撑系统查询，在网管客户支撑系统上进行分权模式管控。

方式3: 梳理各设备厂商网元的位置信息查询操作指令, 在通过集中安全管控平台系统操作敏感指令时触发分权模式审批。

8.2.2 HLR

HLR向MSC/VLR/MGW提供路由信息和用户管理信息, 包括用户状态、用户位置、用户签约信息等, 其维护操作主要是由系统维护人员通过命令行方式进行。

HLR存储的敏感客户信息主要为客户位置信息和用户鉴权信息。(注: 鉴权信息已经加密, 无需纳入分权管控。)

HLR的敏感客户信息获取途径, 主要为通过登录网元, 使用命令行方式对客户信息进行查询。

针对HLR的客户位置信息查询操作, 应选择如下方式实现分权管控:

方式1: 禁止系统维护人员直接访问网元进行客户位置信息查询操作, 统一通过网管客户支撑系统查询, 在网管客户支撑系统上进行分权模式管控。

方式2: 如果网元支持基于特定操作的授权, 应仅将位置信息查询操作权限赋予个别特权账号, 特权账号在集中安全管控平台系统登入时触发分权模式审批。

方式3: 梳理各设备厂商网元的位置信息查询操作指令, 在通过集中安全管控平台系统操作敏感指令时触发分权模式审批。

8.2.3 WAP 网关

WAP网关主要功能是实现WAP协议栈与Internet协议栈之间协议的转换, 支持手机使用互联网业务, 其维护操作主要有两种方式, 一是通过系统图形界面进行维护, 二是通过登录主机以命令行方式进行维护。

WAP网关存储的敏感客户信息主要为用户上传记录。

WAP网关的敏感客户信息获取途径, 主要为通过系统维护界面菜单查询用户上传记录和通过后台直接登入系统主机读取日志文件方式。

针对采取图形界面方式获取敏感客户信息的维护方式, 无法在集中安全管控平台系统上实现该业务操作的管控, 应选择如下方式实现分权管控:

方式1: 禁止系统维护人员使用WAP网关直接进行查询, 统一通过网管客户支撑系统查询, 在网管客户支撑系统上进行分权模式管控。

方式2: 如果WAP网关支持基于特定操作的授权, 应仅将上网记录查询权限赋予个别特权账号, 特权账号在集中安全管控平台系统登入时应触发分权模式审批。

方式3: 通过日志审计系统收集WAP网关操作日志, 并与EOMS工单系统联动, 进行准实时(24小时)自动审计和比对, 如果发现无工单的敏感操作, 及时进行告警。

针对通过后台直接登入系统主机读取日志文件方式获取敏感客户信息, 应选择如下方式实现分权管控:

方式1: 仅将日志文件的读取权限赋予个别特权账号, 特权账号在集中安全管控平台系统登入时触发分权模式审批。

方式2: 针对WAP网关的日志文件的读取指令, 通过集中安全管控平台系统实现指令级分权模式审批。

8.2.4 网管客户支撑系统

网管客户支撑系统（网管客户支撑系统包括网络投诉综合处理平台、客户投诉处理平台、客户服务支撑系统等）通过整合投诉处理过程涉及的各个环节，集成各类分散的投诉处理支撑系统，为客服和网络维护部门提供快速处理网络类投诉的功能，其操作主要通过应用图形界面进行。

网管客户支撑系统的数据均来源于其他设备和支撑系统，涉及处理客户投诉相关的敏感信息，主要有客户位置信息和通信记录。

网管客户支撑系统的敏感客户信息获取途径，主要为通过系统应用界面菜单查询客户位置信息和通信记录。

由于网管客户支撑系统是采取图形界面方式获取敏感客户信息，而通常查询操作请求都有客户投诉工单作为依据，可以由网管客户支撑系统自身进行系统改造，采用如下方式实现分权管控：

方式1：通过和EOMS工单系统联动，针对客户位置信息和通信记录的查询操作，由网管客户支撑系统以基于工单的自动授权方式触发分权模式审批。

方式2：针对无EOMS工单的客户位置信息和通信记录的查询操作，由网管客户支撑系统以远程或现场人工授权方式触发分权模式审批。

8.2.5 信令监测系统

信令监测系统的主要功能是通过整理、分析和统计采集到的信令消息数据，详细反映全网的各种呼叫接续过程以及位置更新、漫游、鉴权等移动性信令信息，其维护操作主要有两种方式，一是通过系统图形界面方式，二是通过登录主机以命令行方式。

信令监测系统存储的敏感客户信息主要为客户位置信息和通信记录。

信令监测系统的敏感客户信息获取途径，主要为通过系统维护界面菜单或通过后台直接登入系统操作数据库查询用户位置信息和通信记录。

针对通过图形界面获取敏感客户信息的维护方式，如果信令监测系统可以进行改造，应采用如下实现分权管控：

方式1：通过和EOMS工单系统联动，针对客户位置信息和通信记录的查询操作，由信令监测系统以基于工单的自动授权方式完成分权模式审批。

方式2：针对无EOMS工单的客户位置信息和通信记录的查询操作，由信令监测系统以远程或现场人工授权方式触发分权模式审批。

如果信令监测系统无法进行改造，应采用如下实现分权管控：

方式1：仅将客户位置信息和通信记录查询权限赋予个别特权账号，特权账号在集中安全管控平台系统登入时应触发分权模式审批。

针对通过后台直接登入数据库的敏感客户信息获取方式，应选择如下方式实现分权管控：

方式1：仅将获取客户位置信息和通信记录的权限赋予个别特权账号，特权账号在集中安全管控平台系统登入时触发分权模式审批。

方式2：针对获取客户位置信息和通信记录的指令，通过集中安全管控平台系统实现指令级分权模式审批。

8.3 业务支撑关键系统管理规则

8.3.1 CRM 系统

CRM系统实现了对客户资料、通话详单等的管理和展现功能,存放了包括个人客户资料、集团客户资料、VIP客户资料、详单、账单、客户消费信息、基本业务订购关系、增值业务(含数据业务)订购关系、增值业务信息、资源数据、用户积分在内的敏感信息。

CRM系统中的敏感数据,主要通过以下方式接触和获取:

- a) 后台人员使用数据库客户端工具访问CRM系统敏感数据库表(比如客户资料、订购关系等);
- b) 后台人员使用系统账号,通过FTP、TELNET等方式远程登录CRM系统主机获取数据文件(比如客户资料、订购关系等);
- c) 通过CRM前台,在不验证用户密码的情况下查询用户详单;
- d) 通过CRM前台,在查询出客户通话详单之后,单个导出/批量导出客户通话详单;
- e) 通过CRM前台批量查询/导出/变更个人或集团客户资料;
- f) 通过CRM前台批量为客户开通/变更服务、增值产品等业务;
- g) 通过CRM前台,使用批量缴费或调账方式批量为客户变更账户余额;
- h) 通过CRM前台变更客户积分信息。

CRM系统应选择如下方式进行分权管控:

针对CRM系统的前台操作,通过对CRM系统的应用进行改造,选用如下方式实现分权管控:

方式1:通过工单系统联动,针对敏感操作,由CRM系统以基于工单的自动授权方式触发分权模式审批;

方式2:针对CRM系统未与工单系统联动的场景,由CRM以现场或远程人工授权方式触发分权模式审批。

针对CRM系统的后台操作,选用如下方式实现分权管控:

方式1:基于账号登录触发分权模式审批。将CRM系统对敏感信息表和文件的操作权限仅授予个别特权账号,禁止使用特权账号进行普通维护,在特权账号登录集中安全管控平台时,触发分权模式审批操作。

方式2:基于敏感操作指令触发分权模式审批。通过集中安全管控平台系统的堡垒主机,对用户的操作指令进行监控,在执行敏感操作指令时,触发分权模式审批操作。

8.3.2 BSS/OSS 系统

为了实现对用户的通话进行计费的功能,BSS/OSS系统存放了集团客户资料、个人客户资料、VIP客户资料、详单、账单、客户消费信息、基本业务订购关系、增值业务(含数据业务)订购关系、增值业务信息、资源数据、用户积分等敏感信息。

BSS/OSS系统中的用户通话详单、账单、积分等数据,主要用于CRM前台查询和经分系统的统计分析。BSS/OSS前台应用不涉及敏感信息的处理和展现,涉及敏感信息的主要是后台维护人员的日常维护操作。

BSS/OSS系统中的敏感数据,主要通过以下方式接触和获取:

- a) 后台维护人员使用数据库客户端工具访问BSS/OSS系统敏感数据库表(比如通话清单表等);

b) 后台维护人员使用系统维护账号, 通过FTP等方式远程登录BSS/OSS系统主机获取数据文件(比如用户通话详单等)。

BSS/OSS系统应选择如下两种方式进行分权管控:

方式1: 基于账号登录触发分权模式审批。将BSS/OSS系统对敏感信息表和文件的操作权限仅授予个别特权账号, 禁止使用特权账号进行普通维护, 在特权账号登录集中安全管控平台时, 触发分权模式审批操作。

方式2: 基于敏感操作指令触发分权模式审批。通过集中安全管控平台系统的堡垒主机, 对用户的操作指令进行监控, 在执行敏感操作指令时, 触发分权模式审批操作。

8.3.3 集中安全管控平台集中安全管控平台集中安全管控平台集中安全管控平台经分系统

经分系统主要用于对公司业务的经营分析和统计报表生成, 实现对市场营销、产品管理、客户管理、资源管理、供应商及合作伙伴管理等全面支撑。

为了实现对公司业务的运营分析, 经分系统存放了集团客户资料、个人客户资料、详单、账单、客户消费信息、积分信息、基本业务订购关系、增值业务订购关系、增值业务信息、统计报表、渠道及合作伙伴资料、资源数据等敏感信息。

经分系统中的敏感数据, 主要通过以下方式接触和获取:

- a) 后台维护人员使用数据库客户端工具访问经分系统敏感数据库表(比如用户资料表等);
- b) 后台维护人员使用系统维护账号, 通过FTP等方式远程登录经分系统主机获取数据文件(比如统计报表等);
- c) 用户通过访问经分系统页面, 查询或导出敏感的经营分析统计报表。

针对经分系统的前台操作, 通过对经分系统的应用进行改造, 当敏感操作发生时, 触发分权模式审批。

针对经分系统的后台操作, 选用如下方式实现分权管控:

方式1: 基于账号登录触发分权模式审批。将经分系统对敏感信息表和文件的操作权限仅授予个别特权账号, 禁止使用特权账号进行普通维护, 在特权账号登录集中安全管控平台时, 触发分权模式审批操作。

方式2: 基于敏感操作指令触发分权模式审批。通过集中安全管控平台系统的堡垒主机, 对用户的操作指令进行监控, 在执行敏感操作指令时, 触发分权模式审批操作。

8.4 业务平台关键系统管理规则

8.4.1 重要业务平台

业务平台存储的敏感客户信息主要为位置信息、订购关系、好友名单、通信录等, 其维护方式主要为通过系统维护界面或后台数据库命令访问相关数据。

业务平台敏感客户信息获取途径主要为维护人员通过后台方式, 利用系统维护界面或后台数据库命令访问相关数据, 进行查询用户位置、导出用户订购关系、导出好友名单、通信录等操作。

分权模式管控要求:

- a) 对于已纳入集中安全管控平台管理的业务平台, 通过集中安全管控平台基于账号或指令的方式实现分权模式管理。

b) 对于未纳入集中安全管控平台管理的业务平台, 建议参照上述系统的分权模式管理规则, 通过技术改造或管理要求实现分权控制。

9 分权模式实施要求

9.1 实施要求

a) 图形化操作接口分权模式实现要求

1) 对于能够进行分权模式改造的业务系统, 在系统中执行高风险操作时增加专门的控制点, 触发分权模式审批;

2) 对于无法改造的系统, 通过将特殊权限赋予个别账号, 在集中安全管控平台系统基于账号登录触发分权模式审批;

3) 对于无法梳理账号的情况, 基于准实时审计实现分权管控。

b) 命令行操作接口分权模式实现要求

1) 通过将特殊权限赋予个别账号, 在集中安全管控平台系统基于账号登录触发分权模式审批;

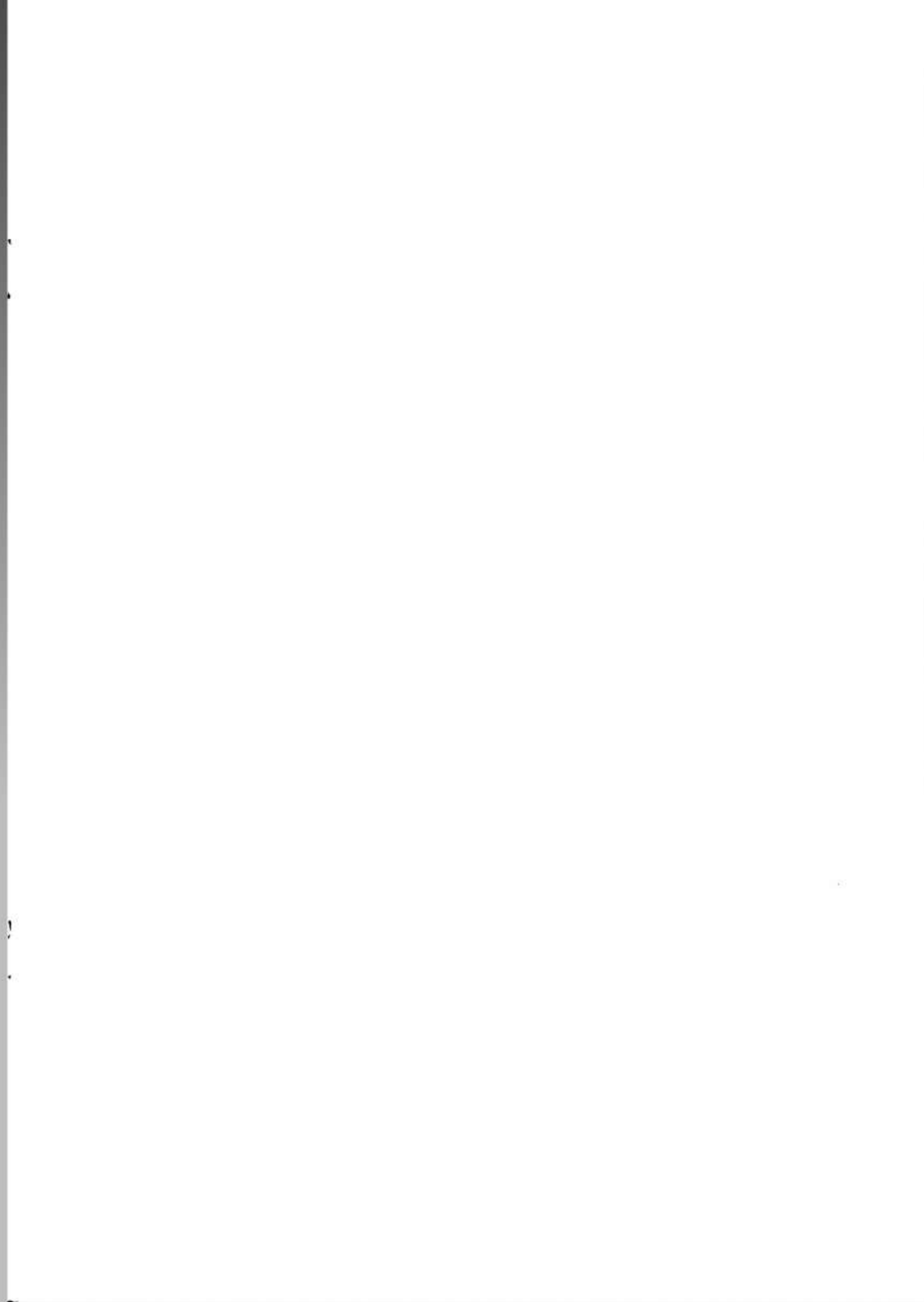
2) 对于无法梳理账号的情况, 在集中安全管控平台系统基于敏感指令触发分权模式审批。

9.2 审计要求

所有分权模式授权操作, 必须有完备的审计日志。集中安全管控平台日志审计系统应收集敏感信息的操作日志, 并设定相应的审计规则, 及时发现未执行分权模式审批的敏感操作, 并产生告警。

9.3 其他要求

实现分权管控的系统应提供分权模式切换开关, 以备在应急情况时, 不影响正常的生产、维护工作。



中华人民共和国
通信行业标准
分权模式（金库模式）客户信息安全保护技术要求
YD/T 2671-2013

*

人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100064
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2013年12月第1版
印张：1.25 2013年12月北京第1次印刷
字数：28千字

15115·365

定价：15元

本书如有印装质量问题，请与本社联系 电话：(010)81055492