**报告编号：2016-XX-XXXX-XX**

**中国移动集团浙江分公司“和包·城市通”业务系统信息安全评估报告**

**系统名称： 和包城市通**

**委托单位： 中国移动集团浙江分公司**

国家计算机网络与信息安全管理中心

目录

[一、 概要 3](#_Toc470247934)

[二、 评估目的 3](#_Toc470247935)

[三、 评估内容 3](#_Toc470247936)

[四、 评估依据 4](#_Toc470247937)

[4.1 政策法规依据 4](#_Toc470247938)

[4.2 安全标准 4](#_Toc470247939)

[4.3 评估方式 5](#_Toc470247940)

[五、 评估组组成 5](#_Toc470247941)

[六、 评估时间 5](#_Toc470247942)

[七、 浙江移动信息安全管理总体情况 6](#_Toc470247943)

[八、 “和包•城市通”业务信息安全现状 6](#_Toc470247944)

[8.1业务基本情况 6](#_Toc470247945)

[8.2业务功能实现技术原理 6](#_Toc470247946)

[8.3业务相关信息安全管理和制度建设情况 9](#_Toc470247947)

[8.4业务安全保障措施 9](#_Toc470247948)

[九、 新技术新业务信息安全评估结果 10](#_Toc470247949)

[9.1“和包•城市通”业务管理体系评估结果 10](#_Toc470247950)

[9.2“和包•城市通”业务安全评估结果 11](#_Toc470247951)

[十、 整改建议 11](#_Toc470247952)

# 概要

2016年11月7日至11日，国家计算机网络与信息安全管理中心对中国移动集团浙江分公司（以下简称浙江移动）“和包”业务开展了信息安全现场评估工作。

此次信息安全评估主要内容包括管理体系评估、业务风险评估和信息安全保障能力评估三个部分。评估方法包括人员访谈、制度核实、业务功能演示、内容安全测试、测试验证、渗透测试等。

本报告主要给出“和包”业务的信息安全评估情况。

# 评估目的

为进一步提升浙江移动新技术新业务的信息安全防护和处置能力，依据新技术新业务信息安全评估相关政策文件，结合通信安全分级保护、风险评估的基本方法和标准，发现并找出新技术新业务相关的管理制度、业务流程、网络系统、服务器以及应用系统等方面存在的安全漏洞和隐患。目的是为企业健全互联网新技术新业务管理制度、完善业务流程、提早启动保障措施、加固系统和网络漏洞提供参考和依据，进而提高业务系统的安全防护水平，为业务的发展创造安全可靠的环境。

# 评估内容

浙江移动新技术新业务安全评估工作主要涉及管理、业务和信息安全保障等方面的安全因素。管理方面，主要采用访谈调研、相关文件查阅的方式，查找管理方面存在的漏洞；业务方面，主要采用人员访谈、功能演示、业务试用、流程梳理等方式，查找业务方面存在的漏洞或隐患；信息安全保障能力方面，主要通过内容测试、漏洞扫描、渗透测试等手段，查验现有信息安全技术保障措施是否满足基本要求。各方面的评估重点包括：

* 1. 管理体系方面：重点评估浙江移动对于各新技术新业务的信息安全管理体系和业务安全管理措施是否满足电信管理机构的安全管理要求，具体包括机构设置、管理制度、信息安全相关要求和技术标准以及具体执行情况；
  2. 业务风险方面：评估浙江移动新技术新业务的完整业务流程，结合业务功能属性及技术实现，包括内容发布审核、业务边界安全、权限管理、用户信息保护等，评估系统潜在的信息安全风险；
  3. 信息安全保障能力方面：评估浙江移动现有的安全措施、技术手段等信息安全保障能力是否能够有效控制业务信息安全风险。开展内容过滤机制测试；对业务系统、操作系统、网络设备进行安全检测；通过渗透测试查看系统安全防护情况等。
  4. 其他：评估与浙江移动新技术新业务相关系统的安全性。

# 评估依据

## 4.1 政策法规依据

《基础电信企业信息安全责任管理办法（试行）》

《互联网新技术新业务信息安全评估管理办法（试行）》

《关于开展基础电信企业网络与信息安全责任考核有关工作指导》

《互联网用户账号名称管理规定》

## 4.2 安全标准

《互联网新技术新业务安全评估指南》（征求意见稿）

《电信网和互联网安全防护管理指南》

《电信网和互联网安全风险评估实施指南》

《电信网和互联网灾难备份及恢复实施指南》

《电信网和互联网物理环境安全等级保护要求》

《电信网和互联网物理环境安全等级保护检测要求》

《电信网和互联网管理安全等级保护要求》

《电信网和互联网管理安全等级保护检测要求》

《2016年省级基础电信企业网络与信息安全工作考核要点与评分标准》

## 4.3 评估方式

本次信息安全评估的主要方式有：人员访谈、文档材料核查、业务功能验证、内容安全测试和安全测评。

人员访谈从被评估方的业务人员和部门领导直接获取企业信息安全管理、业务应用及平台安全、安全保障措施等方面的现状。

文档材料核查主要是指对企业信息安全、业务安全等相关制度的制定情况进行核实。

业务功能验证通过检查业务功能和流程，对业务应用和系统平台潜在的安全风险做出判断。

内容安全测试主要用于评估企业内容安全相关的保障能力，包括违法不良样本的识别检测、传播扩散控制等方面。

安全测评主要针对业务平台安全和数据安全，涉及漏洞分析、渗透测试等技术手段。

# 评估组组成

|  |  |  |
| --- | --- | --- |
| **姓名** | **职称/职务** | **职责** |
| 王红兵 | 首席工程师 | 评估组长 |
| 张 琳 | 工程师 | 评估测试 |
| 刘 洋 | 工程师 | 评估测试 |
| 贾芳姝 | 工程师 | 评估测试 |
| 郑晓天 | 工程师 | 评估测试 |
| 祝旭晨 | 工程师 | 评估测试 |

# 评估时间

评估时间：2016年11月7日至11日

综合数据分析时间：2016年11月14日至2016年12月2日

评估报告生成时间：2016年12月2日

# 浙江移动信息安全管理总体情况

（空）

# “和包•城市通”业务信息安全现状

## 8.1业务基本情况

中国移动的“和包”业务，是中国移动面向个人和企业客户提供的一项综合性移动支付业务，支持线上支付，如互联网购物、充话费、生活缴费等，也支持线下支付，如在便利店、商场、公交、地铁等特约商家线下消费。

本次评估中，浙江移动提供的“和包•城市通”业务，是中国移动“和包”  
业务的一个“模块”，用户注册开通业务后才可显示该功能模块。“和包•城市通”是浙江移动与本地市民卡公司合作推广的一项便民业务，针对持NFC手机和NFC-SIM卡的用户，通过“和包”实现刷卡功能。如同将城市一卡通装进手机里，实现通过手机客户端空中开户、空中充值、数据查询等功能，充值支付等功能通过中国移动“和包收银台”实现。

业务核心功能包括：空中充值，通过“和包收银台”使用银行卡或和包账户为市民卡充值；交易记录查询，可以查询消费记录、充值记录等；余额查询，查询市民卡余额；商户网点，可按照类别、关键字查询充值网点和商户网点。

“和包•城市通”业务系统由浙江融创信息产业有限公司开发，14年7月在杭州正式上线，现已在温州、绍兴、杭州、玉环4个城市部署业务，用户数量达到2万人。

## 8.2业务功能实现技术原理

浙江移动建设了“中国移动浙江公司手机支付业务平台”，以中国移动集团的统一手机支付账户为账户核心，同时考虑与本地或全网的银行合作，以浙江省的自有业务和合作业务为支付目标，以深度开展支付消费业务为目的，为用户提供多样化个性化支付服务。通过手机支付平台，用户可随时、随地、随意的对移动各种自营业务进行缴费，并且使用各种其他支付类业务，如手机彩票、手机支付水电气费、手机公交车刷卡、手机购买电影票、手机超市刷卡、手机购买各种小额商品等。手机支付业务平台中心平台位于湖南，各个省建设各自的省平台与中心平台连接，为各个省用户提供接入中心平台的途径，同时省平台对本省商户、POS设备及合作银行进行管理。省平台建设内容包括省手机支付服务平台和省POS服务平台两部分。同时需要建设省公司密钥管理中心。



图1 系统平台结构图

1、省手机支付服务平台。主要功能包括负责本地业务平台、本地商户系统、本地金融机构的接入；负责本省商户、金融机构的管理；提供支付交易转发功能。



图2 省手机支付服务平台功能架构图

2、省POS服务平台。实现对POS终端的接入以及管理功能，支撑现场支付业务；主要包括POSP和POS终端管理平台两个功能模块，POSP实现手机支付的交易功能以及和交易相关的交易监控、密钥管理等功能，POS终端管理平台实现对POS终端的管理、监控以及相关的统计分析功能。



图3 省POS服务平台功能架构图

3、对外部系统连接。

（1）省手机支付服务平台。与中心手机支付平台的接口连接，实现和中心手机支付平台的交互，完成消费、对帐等接口功能；与本地金融机构连接，实现本地银联等金融机构的连接，开通资金进出通道；与商户平台接口：实现本地商户的接入，为商户提供支付功能。

（2）省POS服务平台。与POS终端的连接，实现POS终端到省POS服务平台的管理及交易接口连接；与中心POS服务平台的连接，实现多个POS服务平台间的连接，完成交易上送；与中心手机支付服务平台的连接：实现机构信息以及商户信息的同步以及交易上送功能。

（3）省手机支付业务运营管理平台。实现对省手机支付的业务运营管理，报表分析等功能。



图4 业务运营支撑平台的功能框架图

## 8.3业务相关信息安全管理和制度建设情况

“和包•城市通”业务系统由浙江融创信息产业有限公司开发和维护。系统开发过程中，浙江移动对开发人员及所属公司有明确的信息安全要求。目前运维人员共3人，保证7\*24小时响应，针对运维人员制定有运维手册。

“和包•城市通”相关业务人员在开展业务前进行过网络与信息安全方面的培训。针对业务人员制定有业务操作手册。

评估访谈中，未见针对该业务建立的业务管理流程或规范性的文件，也未见针对该业务系统制定的信息安全应急管理措施，未见针对业务人员签署的网络与信息安全责任书或承诺书，未见业务人员签署的保密协议等文件。

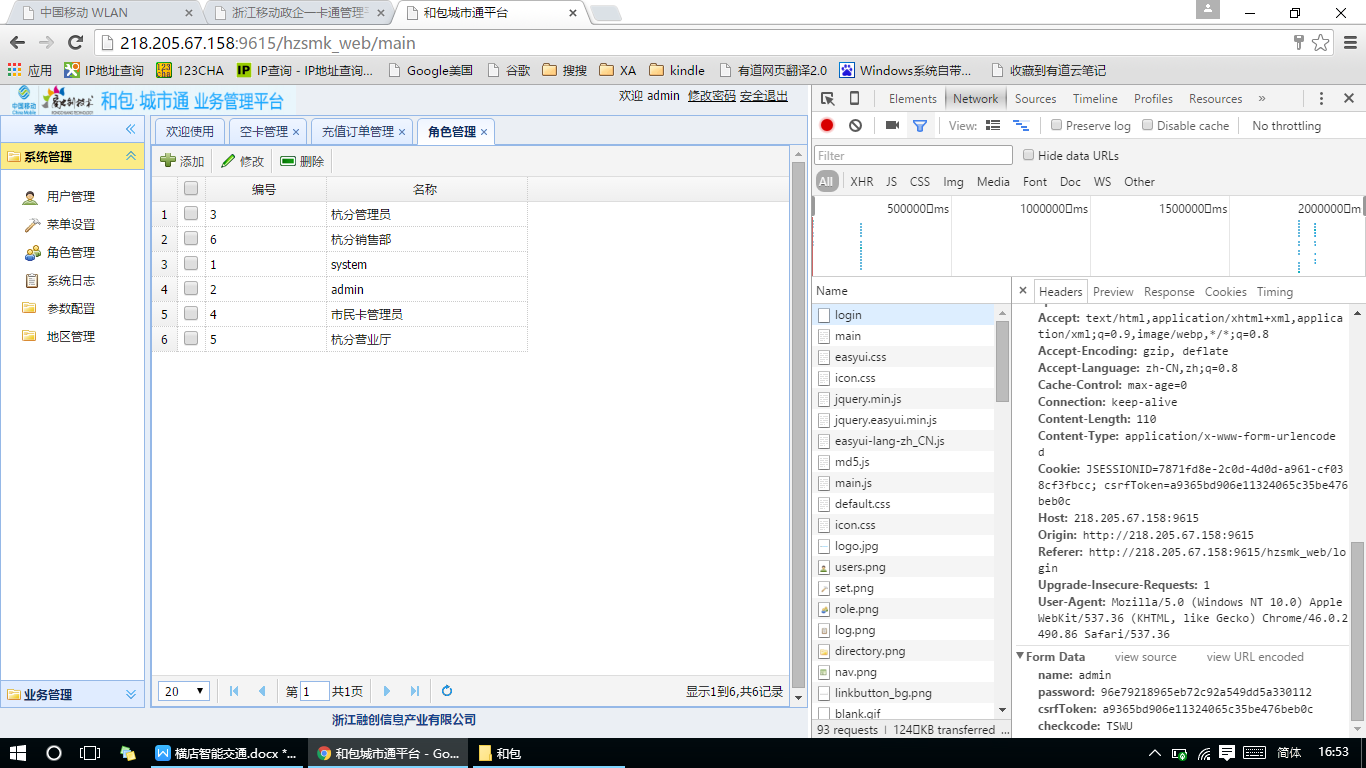
## 8.4业务安全保障措施

评估访谈中，浙江移动未能提供针对“和包·城市通”业务建立的业务管理流程、管理规范等文件或文档，未能提供该业务系统的信息安全应急管理措施。

1、帐号管理

手机客户端用户为中国移动和包业务用户，注册过程需要手机号注册。

城市通业务管理平台为不同权限用户设置了不同账户级别，包括管理员账户和普通账户。账户登录过程对帐号、密码等数据进行了加密传输，但对账户密码未设置强度要求，也没有错误登录次数限制。账户密码要求每2个月更换，设置有会话失效机制，限时30分钟。



2、日志留存

管理员日志信息永久留存。

3、数据备份

每月对业务数据进行备份，一般包括应用程序数据、配置数据、用户注册开卡信息、用户行为日志、管理员行为日志等。

# 新技术新业务信息安全评估结果

## 9.1“和包•城市通”业务管理体系评估结果

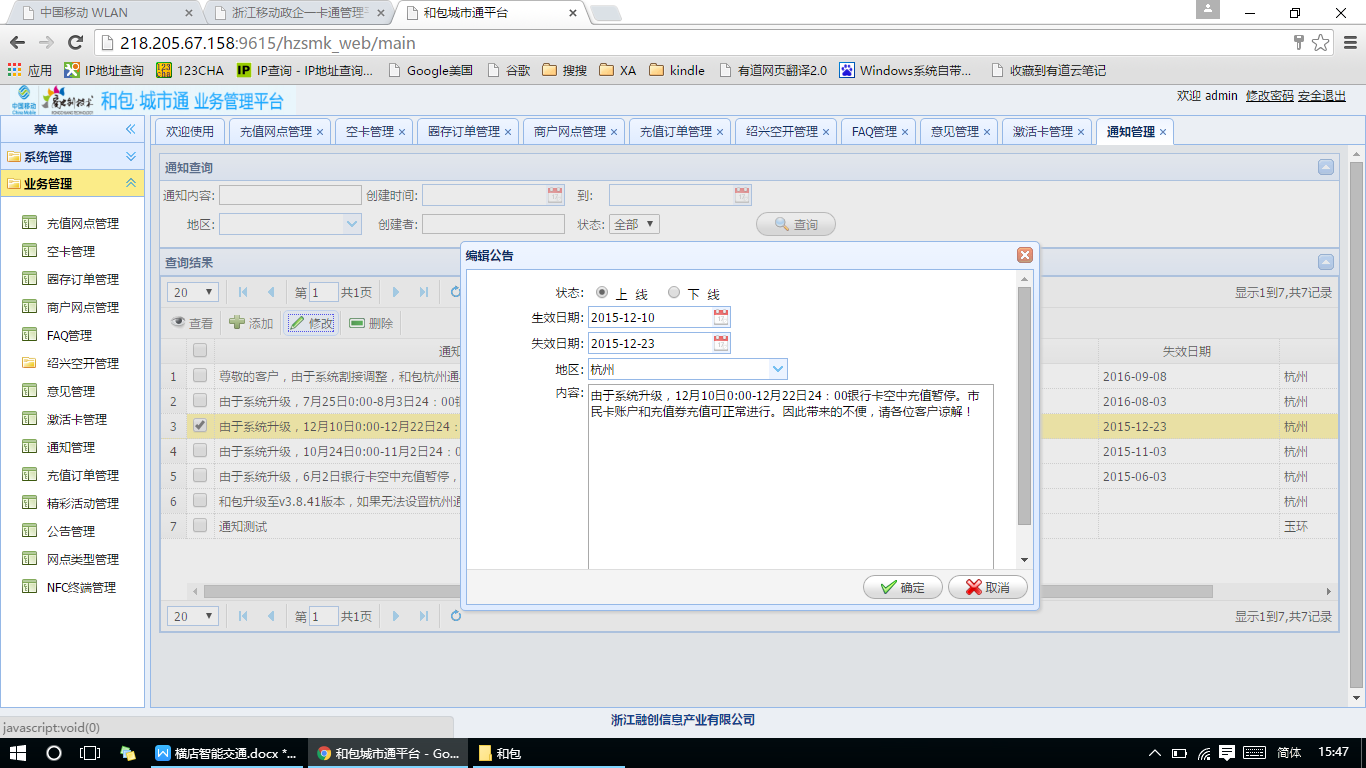
浙江移动制定有《中国移动浙江公司互联网新技术新业务信息安全评估管理细则》，对新技术新业务信息安全评估的组织、实施及整改工作做出一系列具体的要求和规范。在业务上线前开展了自评估，并进行了整改。

但评估中，浙江移动未能提供针对“和包•城市通”业务建立的业务管理流程或规范性的文件，也未见针对该业务系统制定的信息安全应急管理措施，未见针对业务人员签署的网络与信息安全责任书、承诺书，保密协议等文件。建议后续建立或完善业务相关管理规范，建立应急处置机制，完善对业务人员的信息安全管理。

## 9.2“和包•城市通”业务安全评估结果

城市通业务管理平台账户登录过程对帐号、密码等数据进行了加密传输，登录过程无需手机验证，账户密码定期更改，设置有会话失效机制，但对账户密码未作强度要求，没有错误登录次数限制，登录错误提示信息未作模糊处理。账户登录日志信息永久留存。

业务用户不能发布信息，业务管理平台可向用户推送文字、图片等信息，用户不能拒绝。发布信息过程具备先审后发机制，无信息自动过滤机制，设置有人工审核员1名。



# 整改建议

1. 管理体系方面

* 建议建立完善业务相关管理规范，完善对业务人员网络与信息安全的具体要求，完善对业务人员的保密要求。
* 建议建立好业务应急处置机制。

2. 业务安全方面

* 建议对业务管理平台账户登录过程设置错误登录次数限制，对登录错误提示信息作模糊处理。
* 建议对业务管理平台账户密码强度进行强制性要求。