**报告编号：2016-XX-XXXX-XX**

**中国移动集团浙江分公司“能力开放 平台”业务信息安全评估报告**

**系统名称： 能力开放平台**

**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](#_Toc470247750)

[二、 评估目的 3](#_Toc470247751)

[三、 评估内容 3](#_Toc470247752)

[四、 评估依据 4](#_Toc470247753)

[4.1 政策法规依据 4](#_Toc470247754)

[4.2 安全标准 4](#_Toc470247755)

[4.3 评估方式 5](#_Toc470247756)

[五、 评估组组成 5](#_Toc470247757)

[六、 评估时间 5](#_Toc470247758)

[七、 浙江移动信息安全管理总体情况 6](#_Toc470247759)

[八、 “能力开放平台”业务信息安全现状 6](#_Toc470247760)

[8.1业务基本情况 6](#_Toc470247761)

[8.2业务功能实现技术原理 6](#_Toc470247762)

[8.3业务相关信息安全管理和制度建设情况 7](#_Toc470247763)

[8.4业务安全保障措施 7](#_Toc470247764)

[九、 新技术新业务信息安全评估结果 8](#_Toc470247765)

[9.1“能力开放平台”业务管理体系评估结果 8](#_Toc470247766)

[9.2“能力开放平台”业务安全评估结果 8](#_Toc470247767)

[十、 整改建议 9](#_Toc470247768)

# 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）

# “能力开放平台”业务信息安全现状

## 8.1业务基本情况

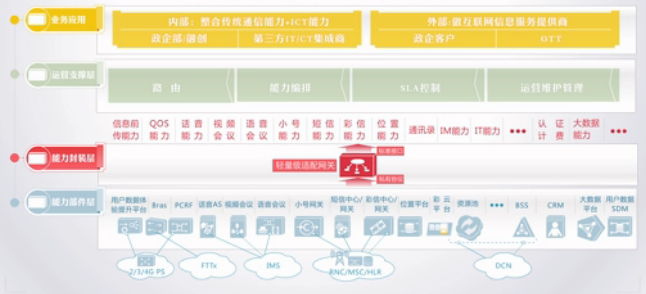
浙江移动“能力开放平台”中国移动面向互联网中小客户群体和企业群体开放的一项业务。“能力开放平台”基于“聚合开放”的理念，立足服务平台化，集合了基础通信、智能管道、大数据、运营支撑、IT等五大基础能力，为广大应用开发者提供一站式的标准化、规模化的开放能力服务。



“能力开放平台”通过对基础能力的组合应用，为各行各业提供语音、安全、认证及隐私小号等核心能力，现已产生了智慧乡村、数字快递、金融验真、远程排队等多个应用案例，并与新华网、阿里巴巴、京东、苏宁等知名企业签署了战略合作协议。截至2016年10月，平台合作伙伴已超过400家，API（应用程序编程接口）累计调用近20亿次，累计收入超过8000万元。目前已在信息通信业界初步形成生态效应，为“大众创业、万众创新”注入新活力。

## 8.2业务功能实现技术原理

“能力开放平台”针对现有移动网络中烟囱式建设的弊端而建立，如对接业务网络复杂，调用效率低、成本高。而能力开放平台则更加灵活。



1、基础能力从网元架构解耦出来并构成能力部件层；

2、能力封装层通过轻量级适配网关完成对宽带、核心网、BSS等能力的暴露；

3、运营支撑层对开放的能力进行编排和统一管理；

4、开放平台开放统一API接口,服务内外部用户

## 8.3业务相关信息安全管理和制度建设情况

“能力开放平台”是浙江移动已经正式商用的一项新技术新业务。评估中，浙江移动未能提供针对该“能力开放平台”业务制定的相关管理流程、管理规范等制度性文件；未见该业务信息安全应急预案或应急处理措施等制度条款，也未提供开展应急演练等工作的资料；未提供该业务人员开展信息安全培训方面的计划、总结或培训材料；未提供针对业务人员签署的信息安全承诺书、保密协议等材料，未提供针对业务维护人员的相关管理制度；未提供与合作单位在信息安全方面的协议条款或签署的信息安全责任书等资料。未提供业务上线前自评估报告。

## 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“能力开放平台”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。

关于账户管理方面，账户登录过程对帐号、密码等数据明文传输，对账户密码强度作出强制要求，没有错误登录次数限制，登录错误信息作了模糊处理。业务收集了用户位置、通话记录、终端型号、使用的应用、上网记录等信息。

关于日志留存方面，业务日志信息存储3个月。

关于数据备份方面，业务数据每周进行备份，一般包括用户注册信息、用户行为日志、调用日志等，备份方式为双机热备份。

# 新技术新业务信息安全评估结果

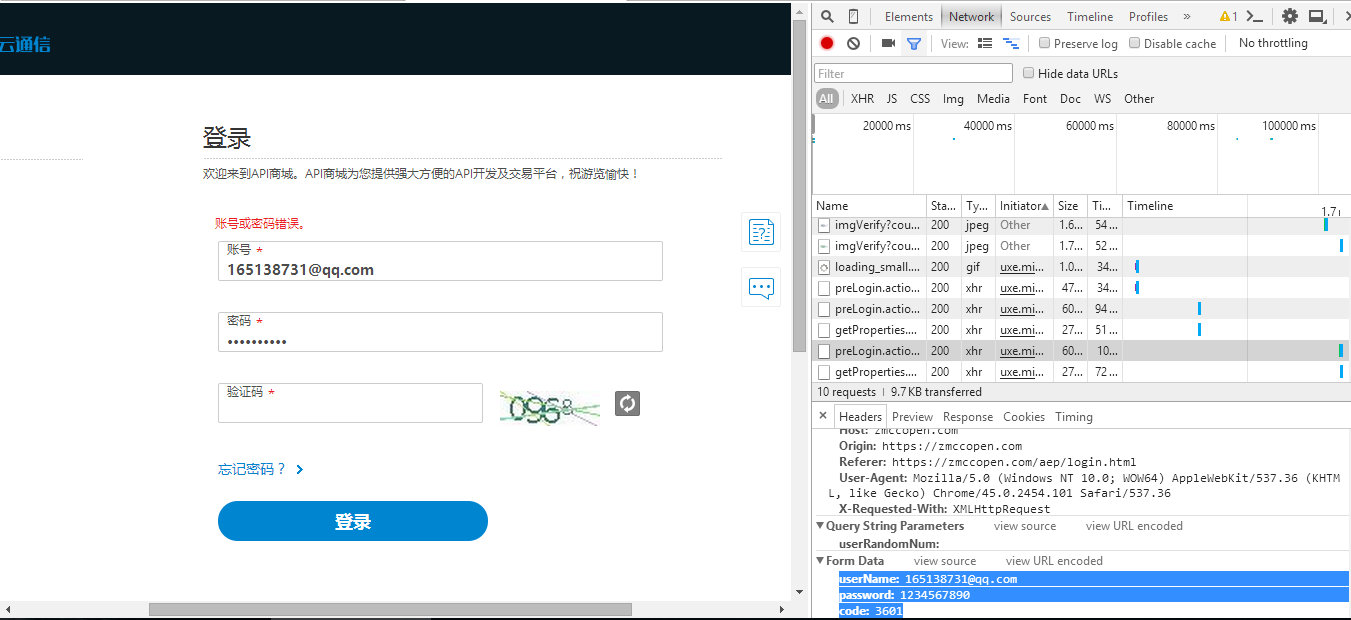
## 9.1“能力开放平台”业务管理体系评估结果

“能力开放平台”业务已正式商用。评估中浙江移动未能提供业务信息安全管理相关的一系列制度文件，建议浙江移动加强对新技术新业务的信息安全管理，履行好信息安全主体责任，落实好公司制定的《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》，开展好新技术新业务信息安全自评估工作。。

## 9.2“能力开放平台”业务安全评估结果

“能力开放平台”业务主要面向应用开发者，不具备信息发布功能，信息交互性较弱。业务通过大数据平台，集合了包括用户手机品牌、终端更换频次、用户消费水平、通话时长频度，在网时长、户籍地等等多维度信息，建议浙江移动加强对用户信息保护方面的管理强度，完善对合作方的管理。

“能力开放平台”登录过程明文传输，建议浙江移动对登录过程中的账户、密码等信息加密传输。



# 整改建议

1. 管理体系方面

* 建议梳理业务相关管理规范，完善“能力开放平台”的信息安全管理；
* 建议建立好业务应急处置机制；
* 建议加强对业务人员、运维人员的网络与信息安全要求，完善对相关人员的保密要求，如签订信息安全责任书、保密协议等；
* 建议加强对业务相关人员的在信息安全方面的培训；
* 建议加强对合作单位的管理，明晰信息安全责任；
* 建议加强新技术新业务信息安全自评估工作。

2. 业务安全方面

* 建议对“能力开放平台”账户登录过程中的账户名、密码等敏感信息进行加密传输；
* 建议设置错误登录次数限制。