

北京市移动电子政务管理平台升级改造

**需求规格说明书**

|  |  |  |  |
| --- | --- | --- | --- |
| 编写 |  | 编写时间 | 2014年5月9日 |
| 审批 |  | 审批时间 |  |
| 版本 | V1.0 | | |

**北京成众志科技有限公司版权所有**

文档中的全部内容属北京成众志科技有限公司所有，

未经允许，不可全部或部分发表、复制、使用于任何目的。

目录

[第1章： 引言 1](#_Toc393988108)

[1.1目的 1](#_Toc393988109)

[1.2背景 1](#_Toc393988110)

[1.3术语和缩略语 1](#_Toc393988111)

[第2章： 系统概述 2](#_Toc393988112)

[2.1总体概述 2](#_Toc393988113)

[2.2总体需求 2](#_Toc393988114)

[2.3用户分类 3](#_Toc393988115)

[2.4角色划分 4](#_Toc393988116)

[2.5运行环境 4](#_Toc393988117)

[2.5.1 Web应用环境 4](#_Toc393988118)

[2.5.2政务通环境 5](#_Toc393988119)

[第3章： 功能需求 5](#_Toc393988120)

[3.1政务通升级改造 6](#_Toc393988121)

[3.1.1政务通单网版 6](#_Toc393988122)

[3.1.2政务通双网版 18](#_Toc393988123)

[3.1.3终端适配 28](#_Toc393988124)

[3.1.4政务通双网版SDK 29](#_Toc393988125)

[3.2后台管理系统升级改造 30](#_Toc393988126)

[3.2.1接入管理 30](#_Toc393988127)

[3.2.2移动用户注册管理 30](#_Toc393988128)

[3.2.3应用管理 31](#_Toc393988129)

[3.2.4查询统计 32](#_Toc393988130)

[3.2.5系统管理 33](#_Toc393988131)

[3.2.6安全管理 34](#_Toc393988132)

[第4章： 其他需求 35](#_Toc393988133)

[4.1性能需求 35](#_Toc393988134)

[4.2文档需求 36](#_Toc393988135)

[第5章： 界面设计 36](#_Toc393988136)

[5.1政务通 36](#_Toc393988137)

[5.2后台管理系统 37](#_Toc393988138)

# 引言

## 目的

本需求规格说明书用于合同附件，并作为系统设计、软件开发、制定测试计划、编写用户手册、项目验收的依据。

## 背景

根据《北京市信息化基础设施提升计划（2009-2012）》文件要求，2009年起，市经济信息化委组织建设全市统一的移动电子政务管理平台。该平台已于2010年投入运行，现已为市应急办、市科委、市经济信息化委、市国土局、市环保局、市交通委、市安全监管局、市文物局、市食品药品监管局、市城管执法局、西站地区管委会、天安门管委会、石景山区经信委、平谷区等20余家单位提供服务。随着管理平台服务单位和服务用户的增多，及移动互联网技术的日新月异，管理平台的功能不足、安全隐患突出、服务模式单一等问题日益凸显，需要进一步完善。

## 术语和缩略语

|  |  |
| --- | --- |
| **缩略语** | **说明** |
| 管理平台 | 北京市移动电子政务管理平台 |
| 政务通 | 北京市移动电子政务管理平台的移动终端程序/软件 |
| 后台管理系统 | 北京市移动电子政务管理平台的后台系统 |
| 政务网 | 政务外网 |
| APN | APN的英文全称是Access Point Name，中文全称叫接入点，是您在通过手机上网时必须配置的一个参数，它决定了您的手机通过哪种接入方式来访问网络。 |
| SDK | 软件开发工具包，提供一些可调用的[应用程序接口](http://baike.baidu.com/view/592964.htm)文件 |

# 系统概述

## 总体概述

管理平台由政务通软件和后台管理系统两部分组成。管理平台总体包括用户及设备授权、政务网络安全接入、可信政务应用发布、移动应用单点登录等功能和服务，实现了移动政务系统统一安全增强保障，提高了我市移动政务的整体安全性，规范了各单位移动政务应用建设，促进了移动政务应用的跨部门共享。

## 总体需求

管理平台由政务通软件和后台管理系统两部分组成，政务通是安装在移动终端上的客户端软件，只有安装政务通软件后移动终端才可访问政务外网。后台管理系统是web应用，主要负责客户端功能实现、客户端各版本管理、用户单位接入管理、应用分发管理以及综合统计分析。

管理平台提供不同的服务模式，包括网络模式和使用模式，由用户单位依据本单位需求选择使用。且所有服务模式共用一套后台管理系统。

从业务的安全需求上，政务通被分为单网版和双网版两种网络模式。

* 政务通单网版只能上政务网，禁止使用互联网等其他网络，并且所有移动政务APP必须要在安全政务工作区中运行；
* 政务通双网版既可以上政务网又可以上互联网，双网版除提供政务网的安全连接和唯一性访问的同时，也提供政务应用管理服务，用户单位可选择性使用。

根据用户单位对政务通使用方式的需求，政务通又被分为APP和SDK两种使用模式。

* 政务通单网版只提供APP的使用模式；
* 政务通双网版既提供APP的使用模式，也提供只有安全网络连接功能的SDK使用模式，各用户单位可将本单位的政务APP程序与政务通SDK进行集成。

## 用户分类

管理平台从使用用户的角度分为以下两类：

* 移动终端用户：使用政务通的用户，此类用户可通过政务通访问政务网。
* PC终端用户：使用后台管理系统的用户，基于管理平台角色划分机制，负责对用户单位相关业务的管理。

## 角色划分

管理平台从权限分配的角度，将后台管理系统划分为三种使用权限，分别如下：

* 用户单位：拥有申请本单位业务系统和用户接入；发布本单位应用；管理本单位组织机构和人员信息；完善本单位基本信息、修改本单位系统管理员密码；配置本单位应用黑名单；查询本单位接入申请、用户、应用、移动用户IP域、系统日志；查询本单位基本信息；系统通知；查询政务通版本及下载政务通安装包的权利。
* 资源中心：拥有审批用户单位接入申请；用户单位移动用户IP域、业务类型、系统通知、政务通版本；重置用户单位移动用户登录政务通的密码；查询统计包含用户统计分析，应用统计分析，应用查询，日志查询，政务通使用情况。
* 经信委：拥有查询统计权限，统计查询内容包括用户统计分析，应用统计分析，应用查询，日志查询，政务通使用情况。

## 运行环境

### Web应用环境

#### 硬件环境

服务器配置：管理平台当前的服务器配置。

#### 软件环境

服务器软件配置：根据需求进行技术选型后对服务器进行相关软件部署。

#### 网络环境

北京市政务外网（局域网）。

### 政务通环境

#### 硬件环境

本次升级改造需适配的两款主流PAD、两块智能手机。

#### 软件环境

本次升级改造需适配安卓操作系统主流版本。

#### 网络环境

北京市政务外网。支持基于中国移动、中国电信、中国联通三大运营商的政务外网接入点配置。

# 功能需求

基于管理平台原有功能进行功能升级改造和功能新增，满足管理本次平台升级改造的总体需求。

## 政务通升级改造

### 政务通单网版

#### 开关机处理

移动终端开机时，自动启动政务通的终端环境监听服务并显示政务通悬浮窗；每次正常断开政务网的同时要删除APN接入点的信息，同时清空缓存数据。

##### 功能概述

点击政务通启动图标后，自动进行政务通数据库文件、本地控制文件的存在状态检测及终端环境检测，根据检测情况进行相应处理。

##### 具体功能描述

1. 政务通数据库文件检测：首次启动时创建政务通数据库，之后每次启动自动检测数据库是否存在，不存在则创建。
2. 控制文件检测：启动政务通时检测本地控制文件是否存在，如果控制文件不存在则提供政务通注册功能；如果存在，则提供政务通登录功能。
3. 终端环境检测：检测内容及处理见本文档3.1.1.7章节。

#### 注册

##### 功能概述

首次安装政务通需进行用户信息注册，成功注册后方可进入政务通。

##### 具体功能描述

1. 注册信息输入：输入信息包括手机号（用户名）和密码。启动政务通后自动获取手机号并显示，无法获取时则由用户输入；密码默认为手机号后六位，由用户手动输入完成。本功能提供记住用户名的功能，方便获取不到手机号的用户进行登录
2. 注册认证：进行注册操作时，结合网络安全接入功能实现对移动终端上政务网APN的自动创建，完成用户身份基于AAA服务器的第一次认证。在连接的过程中，显示“正在连接AAA”服务器。认证通过，政务网连通；认证未通过进行信息提醒。
3. 注册超时：制定默认注册超时时间，如果到达该阀值仍未成功注册，则提示注册超时。目前测试的阀值为27S，如果超过27秒，则显示登陆注册超时
4. 取消注册：通过政务通启动图标启动政务通后，在未进行注册操作和注册过程中，可通过取消注册操作返回至移动终端应用桌面。
5. 终端信息采集：连通政务网后，终端自动采集SIM卡序列号和终端设备串号（IMEI）号并上报至后台管理系统，由后台管理系统进行用户注册绑定。在用户注册信息绑定前向政务通进行绑定确认，用户确认绑定则后台管理系统进行用户信息绑定，用户取消绑定则退出政务通。绑定信息包括单位代码、手机号、SIM卡序列号、终端设备串号（IMEI号）和用户密码。
6. 控制文件生成：后台管理系统绑定用户信息成功后，移动终端设备自动生成控制文件，存储控制信息。

#### 密码修改

1. 密码修改页面控制

注册成功后政务通自动跳转至密码修改页面，如果密码未修改则无法登陆。密码修改不可与与默认密码相同

1. 密码修改处理

用户通过密码修改界面取消密码修改则断开政务网（删除政务网APN），返回至移动终端应用桌面。确认修改操作时，后台管理系统自动完成用户密码变更并对用户进行密码修改成功与否的必要提醒。

##### 功能概述

实现对登陆信息自动获取、用户身份二次验证、登陆成功后相关功能的控制管理。

##### 具体功能描述

1. 登陆信息输入：输入信息包括手机号（用户名）和密码。启动政务通后自动获取手机号并显示，无法获取时则由用户输入。
2. 用户身份二次认证：成功注册后，每次登录时均会对用户身份进行二次认证。基于手机号和密码的第一次认证成功后，政务通采集终端信息（终端设备串号（IMEI号）、SIM卡序列号）并将单位代码（若获取不到，则系统自动下发一个流水号，规则定制）、手机号、用户密码、终端设备串号（IMEI号）、SIM卡序列号共同向后台管理系统发送，请求二次身份认证。认证通过则用户成功登录政务通，认证失败则提示认证失败的原因、并断开政务网（删除政务网APN）。如因设备变更、SIM卡变更导致用户二次身份认证失败，可以与单位管理员联系进行用户的设备变更激活操作。
3. 控制文件更新：每次成功登录后，后台管理系统会将最新的控制文件信息同步至移动终端设备上。控制文件包括了单位代码信息、APN动态密码、应用黑白名单等信息。
4. 强制安装应用检测：每次成功登录后，如果强制发布的应用已被安装，不做其他处理；如果未安装，则后台管理系统继续推送应用至移动终端并强制安装。
5. 应用注销检测：每次成功登录后，通过后台管理系统检测已安装应用的注销状态，如果被注销，则控制政务通上被注销的应用无法启动，系统自动提醒告知用户。
6. 应用列表更新：每次成功登录政务通后，检测是否有新发布的、可手动升级/下载的权限范围内应用，如果有则更新相应的应用列表。

#### 网络安全接入

##### 功能概述

在管理平台原有APN接入政务网机制基础上，实现基于APN的动态密码管理，连接政务网。

#### 具体功能描述

1. APN新建：基于政务通本地控制信息中的APN动态密码，配置APN信息，完成政务网接入点的创建。
2. 编辑控制：政务通创建的APN不可手动编辑。

#### 终端环境检测

##### 功能概述

在点击政务通服务启用时，对移动终端环境进行检测，并与其他功能模块共同作业完成对检测情况的处理。

##### 具体功能描述

1. 检测终端状态：检测移动终端飞行模式和SIM卡状态。在移动终端处于飞行模式或无SIM卡的情况，做无法成功登录政务通的必要提示。若出现除上述两种情况而导致登录失败，则系统提示“网络不可用”
2. 检测终端功能状态：在政务通对终端蓝牙状态检测、wifi状态检测、网络共享状态检测（包含WLAN和USB）的基础上，新增对红外功能和USB数据拷贝功能的开启和关闭状态检测。如果蓝牙功能、wifi功能、网络共享功能、红外功能和USB数据拷贝功能处于开启状态，则结合终端功能管控模块，实现对开启功能的关闭。
3. 检测第三方应用：对移动终端上已安装应用进行检测，结合应用防火墙功能，实现对黑名单内应用的过滤与控制。

#### 终端环境监听

##### 功能概述

在移动终端开机后，对移动终端环境进行监听，并与其他功能模块共同作业完成对监听情况的处理。

##### 具体功能描述

1. 监听终端功能状态：在政务通对终端蓝牙状态监听、wifi状态检测、网络共享状态检测（包含WLAN和USB）的基础上，新增对红外功能和USB数据拷贝功能的开启和关闭状态检测。如果蓝牙功能、wifi功能、网络共享功能、红外功能和USB数据拷贝功能处于开启状态，则结合终端功能管控模块，实现对开启功能的关闭。
2. 监听网络状态：监听移动终端当前网络状态（联网、未联网），用于悬浮窗网络状态展示。
3. 监听网络流量：监听网络数据变化，用于悬浮窗流量展示。
4. 监听应用：监听移动终端上政务应用的下载完成状态和第三方应用的运行状态，并做如下处理：

* 监听政务应用的下载完成状态：通过管理平台发布的政务应用下载完成时，结合应用防火墙功能对应用进行可信认证。
* 监听第三方应用的运行状态：应用运行过程中，有试图接入政务网或使用政务网的情况，结合应用防火墙功能自动拦截未经授权使用政务网的APP。

#### 终端网络边界安全管理

##### 功能概述

对移动终端设备上存在安全隐患的终端功能进行管控、对移动终端设备上应用的过滤控制和访问拦截。

##### 具体功能描述

1. 终端功能管控：在政务通对终端wifi功能控制、网络共享功能控制（包含WLAN和USB）的基础上，新增对红外功能和USB数据拷贝功能的开启和关闭控制及APN的删除控制。
2. 应用防火墙：实现对应用黑名单的过滤与控制、应用拦截及应用安装可信认证管理。

* 应用黑名单过滤与控制：将移动终端设备上已安装的应用进行黑名单过滤，如果存在黑名单内的应用，则提供卸载应用和退出政务网功能供用户选择。选择卸载应用则系统自动卸载应用；选择退出政务网，则断开政务网连接（删除政务网APN），返回至移动终端应用桌面。
* 应用拦截 ：第三方应用运行时，如果发现应用既不在黑名单中，也不在白名单中，但却试图接入政务网或使用政务网，则提供关闭应用和退出政务网功能供用户选择。选择关闭应用则系统自动关闭应用服务；选择退出政务网，则断开政务网连接（删除政务网APN），返回至移动终端应用桌面。并将应用异常行为相关数据上报至后台管理系统用于日志统计。
* 应用安装可信认证：当终端环境监听功能监听到政务应用下载完成状态时，政务通通过应用防火墙配置信息中的应用白名单对应用进行可信认证，发现应用已被篡改，则把被篡改的应用做删除处理,同时给客户做删除提醒。

#### 悬浮窗

##### 功能概述

基于悬浮窗原有的网络状态展示、流量展示和主界面功能，新增悬浮窗的显示控制、横竖屏切换功能及界面优化。

##### 具体功能描述

1. 显示控制：移动终端开机显示。
2. 横竖屏切换：系统级控制悬浮窗的横竖屏切换显示。
3. 界面优化：对悬浮窗快捷功能界面和主界面进行优化，包括UI设计（如下图）、界面部署。



#### 数据加密服务

##### 功能概述

在不影响读取速度的情况下，提供客户端系统控制数据加密功能；并提供结构化数据加密存储接口。

##### 具体功能描述

1. 客户端系统控制数据加密。
2. 存储文件控制：root情况下，可见文件目录，但无法查阅文件内部信息，只有政务通具有存储文件的访问和其内部信息的读写权限。
3. 数据加密存储接口：提供用户单位APP可直接调用的数据加密存储接口，可定期存储和清除文本类型的数据。用户单位APP通过政务通去调用加密数据。该接口用户单位可自选使用。

#### 单点登录接口

提供政务通用户账号接口信息，与CA集成，支撑与用户单位APP的单点登录实现。该接口委办局可自选使用。

#### 政务工作区

##### 控制服务

1. 政务工作区创建：将个人应用与政务应用进行安全隔离。确保政务工作区內的控制数据加密存储，并且只能在工作区被读写；政务工作区外部的应用程序无法读取工作区内部的应用程序和数据。
2. 应用操作控制:通过后台管理系统发布的应用只能在政务工作区内下载、安装、升级、卸载、启动。
3. 政务网退出控制：政务通退出时，终端断开政务网，清除缓存数据，关闭政务工作区内打开的政务应用。
4. 政务通卸载控制：卸载政务通时，卸载所有通过政务通安装的政务应用，并清除政务通自身缓存数据。
5. 应用控制：政务通接收后台管理系统对安全工作区内政务应用的受控指令，实现对应用的强制安装（静默）、强制升级（静默）；政务通通过对应用注销情况的检测，实现对已安装应用的启动控制。

##### 应用管理

政务通提供对政务应用的下载、安装、升级、卸载、启动、使用反馈功能的管理。

1. 下载管理：对后台管理系统通过一般发布方式发布和共享方式发布应用的下载管理。包括应用的下载、下载过程、下载历史及多线程下载的管理。
   * + - 应用下载：用户可对未下载的应用进行下载操作。
       - 下载过程管理：包括对下载任务的查看、暂停、继续和取消功能；
       - 下载历史管理：包括对已下载完成但尚未安装的应用和已卸载但未删除安装包的应用的安装功能。
       - 提供多任务并行下载功能。
2. 安装管理：提供对已下载完成应用的安装功能。
3. 升级管理：每次成功登录政务通后，检测已安装的应用版本，并与服务器对比后提示用户升级，用户可升级高版本应用。
4. 使用反馈：用户可对已安装的应用进行文本信息编辑并提交至后台管理系统用于应用使用情况的统计分析。
5. 应用查询：支持按关键字对应用的模糊查询功能。
6. 应用列表更新：每次成功登录政务通后，检测是否有新发布的、可手动升级/下载的权限范围内应用，如果有则更新相应的应用列表。

##### 消息中心

1. 消息展示：政务通接收后台管理系统推送的系统消息，并展示。
2. 消息查阅状态管理：跟踪消息查阅状态，消息按时间节点划分，并且未读消息和已读消息有明显区分。
3. 消息删除：可删除在消息中心展示的消息。
4. 新消息提醒：对新发布但尚未阅读的消息进行新消息提醒。

### 政务通双网版

与单网版的区别：

* + - 1. 启动：点击政务通启动图标后，自动进行政务通数据库文件、本地控制文件的存在状态检测及终端环境检测，根据检测情况进行相应处理。
      2. 注册：双网版不用强制执行密码修改的功能，用户可设置无密码自动登陆。
      3. 应用管理：在双网版模式下，用户单位可选择通过政务通平台来进行应用的发布，也可将已授权的应用通过其他途径进行发布，但只要是通过管理平台发布的就按照政务工作区来管理。政务通退出时对非政务通下载的应用不做强制退出的操作。

#### 开关机处理

移动终端开机时，自动显示政务通悬浮窗。

#### 启动处理

##### 功能概述

点击政务通启动图标后，自动进行政务通数据库文件、本地控制文件的存在状态检测及终端环境检测，根据检测情况进行相应处理。

##### 具体功能描述

1. 政务通数据库文件检测：首次启动时创建政务通数据库，之后每次启动自动检测数据库是否存在，不存在则创建。
2. 控制文件检测：启动政务通时检测本地控制文件是否存在，如果控制文件不存在则提供政务通注册功能；如果存在，但则提供政务通登录功能。
3. 终端环境检测：检测内容及处理见本文档3.1.2.7章节。

#### 注册

##### 功能概述

首次安装政务通需进行用户信息注册，成功注册后方可进入政务通。

##### 具体功能描述

1. 注册信息输入：输入信息包括手机号（用户名）和密码。启动政务通后自动获取手机号并显示，无法获取时则由用户输入；密码默认为手机号后六位，由用户手动输入完成。
2. 注册认证：进行注册操作时，结合网络安全接入功能实现对完成移动终端上政务网APN的自动创建和编辑控制后，完成用户身份基于AAA服务器的第一次认证。认证通过，政务网连通；认证未通过进行信息提醒。
3. 注册超时：制定默认注册超时时间，如果到达该阀值仍未成功注册，则提示注册超时。
4. 取消注册：通过政务通启动图标启动政务通后，在未进行注册操作和注册过程中，可通过取消注册操作返回至移动终端应用桌面。
5. 终端信息采集：连通政务网后，终端自动采集SIM卡序列号和终端设备串号（IMEI号）并上报至后台管理系统，由后台管理系统进行用户注册绑定和设备管理。在用户注册信息绑定前向政务通进行绑定确认，用户确认绑定则后台管理系统进行用户信息绑定，用户取消绑定则推出政务通。绑定信息包括单位代码、手机号、SIM卡序列号、终端设备串号（IMEI号）。
6. 控制文件生成：后台管理系统绑定用户信息成功后，会向政务通返回用户身份认证信息（单位代码、手机号、SIM卡序列号、终端设备串号（IMEI号）和用户密码）、APN动态密钥和应用防火墙配置信息（应用黑名单、应用白名单），移动终端设备自动生成控制文件。

#### 登录

##### 功能概述

实现对登陆信息自动获取、用户身份二次验证、登陆成功后相关功能的控制管理。

##### 具体功能描述

1. 登录设置：提供自动登录设置功能，自动登录设置默认开启。

* 开启情况下，无登录页面，用户无需输入登录信息，点击政务通启动图标即可实现登录。
* 自动登录可手动设置关闭，关闭后，用户点击政务通启动图标后会出现登录页面，需输入登录信息方可实现登录。输入信息包括手机号（用户名）和密码。启动政务通后自动获取手机号并显示于登录页面，无法获取时则由用户输入；密码默认为手机号后六位，由用户手动输入完成。

1. 用户身份二次认证：每次登录时均会对用户身份进行二次认证。基于手机号和密码的第一次认证成功后，政务通采集终端信息（终端设备串号（IMEI号）、SIM卡序列号）并将单位代码、手机号、用户密码、终端设备号（IMEI号）、SIM卡序列号共同向后台管理系统发送，请求二次身份认证。认证通过则用户成功登录政务通，认证失败则提示认证失败的原因、断开政务网（删除政务网APN）。如因设备变更、SIM卡变更导致用户二次身份认证失败，则提示用户与管理员联系。
2. 控制文件更新：每次成功登录后，后台管理系统会将最新的控制文件信息同步至移动终端设备上。
3. 强制安装应用检测：每次成功登录后，如果强制发布的应用已被安装，不做其他处理；如果未安装，则后台管理系统继续推送应用至移动终端并强制安装。
4. 应用注销检测：每次成功登录后，通过后台管理系统检测已安装应用的注销状态，如果被注销，则控制政务通上被注销的应用无法启动，系统自动提醒告知用户。
5. 应用列表更新：每次成功登录政务通后，检测是否有新发布的、可手动升级/下载的权限范围内应用，如果有则更新相应的应用列表。

#### 网络安全接入

##### 功能概述

在管理平台原有APN接入政务网机制基础上，实现基于APN的动态密码管理，连接政务网。

##### 具体功能描述

1. APN新建：基于政务通本地控制信息中的APN动态密码，配置APN信息，完成政务网接入点的创建。
2. 编辑控制：政务通创建的APN不可手动编辑。

#### 终端环境检测

##### 功能概述

在点击政务通启动图标时，对移动终端环境进行检测，并与其他功能模块共同作业完成对检测情况的处理。

##### 具体功能描述

1. 检测终端状态：检测移动终端飞行模式和SIM卡状态。在移动终端处于飞行模式或无SIM卡的情况，做无法成功登录政务通的必要提示。
2. 检测终端功能状态：在政务通对终端蓝牙状态检测、wifi状态检测、网络共享状态检测（包含WLAN和USB）的基础上，新增对红外功能和USB数据拷贝功能的开启和关闭状态检测。如果蓝牙功能、wifi功能、网络共享功能、红外功能和USB数据拷贝功能处于开启状态，则结合终端功能管控模块，实现对开启功能的关闭。
3. 检测第三方应用：对移动终端上已安装应用进行检测，结合应用防火墙功能，实现对黑名单内应用的过滤与控制。

#### 终端环境监听

##### 功能概述

进入政务网后，对移动终端环境进行监听

具体功能描述

1. 监听终端功能状态：在政务通对终端蓝牙状态监听、wifi状态监听、网络共享状态监听（包含WLAN和USB）的基础上，新增对红外功能和USB数据拷贝功能的开启和关闭状态监听。如果蓝牙功能、wifi功能、网络共享功能、红外功能和USB数据拷贝功能处于开启状态，则结合终端功能管控模块，实现对功能的关闭。
2. 监听网络状态：监听移动终端当前网络状态（政务网、其他网络、未联网），用于悬浮窗网络状态展示。
3. 监听网络流量：监听网络数据变化，用于悬浮窗流量展示。
4. 监听应用：监听移动终端上政务应用的下载完成状态和第三方应用的运行状态并做如下处理：

* 监听政务应用的下载完成状态：通过管理平台发布的政务应用下载完成时，结合应用防火墙功能对应用安装进行可信认证。
* 监听第三方应用的运行状态：应用运行过程中，有试图接入政务网或使用政务网的情况，结合应用防火墙功能自动拦截未经授权使用政务网的APP。

#### 终端网络边界安全管理

##### 功能概述

对移动终端设备上存在安全隐患的终端功能进行管控、对移动终端设备上应用的过滤控制和访问拦截。

##### 具体功能描述

1. 终端功能管控：在登陆政务网时实现对终端wifi功能控制、网络共享功能控制（包含WLAN和USB）的基础上，新增对红外功能和USB数据拷贝功能的开启和关闭控制。
2. 应用防火墙：实现对应用黑白名单的过滤与控制、应用拦截及应用可信认证管理。

* 应用黑名单过滤与卸载控制：将移动终端设备上已安装的应用进行黑名单过滤，如果存在黑名单内的应用，则提供卸载应用和退出政务网功能供用户选择。选择卸载应用则系统自动卸载应用；选择退出政务网，则断开政务网连接（删除政务网APN），返回至移动终端应用桌面。
* 第三方应用拦截与入侵行为反馈 ：第三方应用运行时，如果发现应用既不在黑名单中，也不在白名单中，但却试图接入政务网或使用政务网，则提供关闭应用和退出政务网功能供用户选择。选择关闭应用则系统自动关闭应用服务；选择退出政务网，则断开政务网连接（删除政务网APN），返回至移动终端应用桌面。并将应用异常行为相关数据上报至后台管理系统用于日志统计。
* 应用防篡改安装：当终端环境监听功能监听到政务应用下载完成状态时，政务通通过应用防火墙配置信息中的应用白名单对应用进行可信认证，发现应用已被篡改，则断开政务网（删除政务网APN），。

#### 悬浮窗

##### 功能概述

基于悬浮窗原有的网络状态展示、流量展示和主界面功能，新增悬浮窗的显示控制、横竖屏切换功能及界面优化。

##### 具体功能描述

1. 显示控制：移动终端开机显示。
2. 横竖屏切换：系统级控制悬浮窗的横竖屏切换显示。
3. 界面优化：对悬浮窗快捷功能界面和主界面进行优化，包括UI设计（同单网版一致）、界面部署。

#### 数据加密服务

##### 功能概述

在不影响读取速度的情况下，提供客户端系统控制数据加密功能；提供结构化数据加密存储接口。

##### 具体功能描述

1. 客户端系统控制数据加密。
2. 存储文件控制：root情况下，可见文件目录，但无法查阅文件内部信息，只有政务通具有存储文件的访问和其内部信息的读写权限。
3. 数据加密存储接口：提供用户单位APP可直接调用的结构化数据加密存储接口，可定期存储和清除文本类型的数据。用户单位APP通过政务通去调用加密数据。该接口用户单位可自选使用。

#### 单点登录接口

提供政务通用户账号接口信息，与CA集成，支撑与用户单位APP的单点登录实现。该接口委办局可自选使用。

#### 政务应用管理（可选使用）

##### 控制服务

1. 政务网退出控制：政务网退出时，同时退出应用管理内所有当前处于开启状态的应用，并自动清除所有缓存数据。
2. 政务通卸载控制：卸载政务通时，清除政务通自身缓存数据。
3. 应用控制：政务通接收后台管理系统对政务应用市场内政务应用的受控指令，实现对应用的强制安装（静默）、强制升级（静默）；政务通通过对应用注销情况的检测，实现对已安装应用的启动控制。

##### 应用管理

政务通提供对政务应用的下载、安装、升级、卸载、启动、使用反馈功能的管理。

1. 下载管理：对后台管理系统通过一般发布方式发布和共享方式发布应用的下载管理。包括应用的下载、下载过程、下载历史及多线程下载的管理。
   * + - 应用下载：用户可对未下载的应用进行下载操作。
       - 下载过程管理：包括对下载任务的查看、暂停、继续和取消功能；
       - 下载历史管理：包括对已下载完成但尚未安装的应用和已卸载但未删除安装包的应用的安装功能。
       - 提供多任务并行下载功能。
2. 安装管理：提供对已下载完成应用的安装功能。
3. 升级管理：每次成功登录政务通后，检测已安装的应用版本，并与服务器对比后提示用户升级，用户可升级高版本应用。
4. 启动管理：用户可启动已安装完成的应用。
5. 使用反馈：用户可对已安装的应用进行文本信息编辑并提交至后台管理系统用于应用使用情况的统计分析。
6. 应用查询：支持按关键字对应用的模糊查询功能。
7. 应用列表更新：每次成功登录政务通后，检测是否有新发布的、可手动升级/下载的权限范围内应用，如果有则更新相应的应用列表。

##### 消息中心

1. 消息展示：政务通接收后台管理系统推送的系统消息，并展示。
2. 消息查阅状态管理：跟踪消息查阅状态，并且未读消息和已读消息有明显区分。
3. 消息删除：可删除在消息中心展示的消息。
4. 新消息提醒：对新发布但尚未阅读的消息进行新消息提醒。

### 终端适配

政务通需适配两款机型（三星、E人E本），包括操作系统适配、界面适配、功能使用适配。其中，SDK版政务通不需要进行界面适配。

### 政务通SDK

基于本文档内政务通双网版功能，开发政务通安全网络链接的SDK供第三方APP调用，SDK主要提供进入政务网接口、政务网退出接口和网络状态检测接口。实现用户使用注册、用户登录、终端环境检测、终端环境监听、终端功能管控、应用防火墙、悬浮窗功能，不提供政务应用市场的功能。

提供政务通悬浮窗登陆界面程序包给第三方应用，由第三方应用进行调用。

#### 政务网退出接口

提供政务网退出接口，用户单位APP调用该接口后，可实现政务网退出功能，退出政务网后终端环境监听功能、悬浮窗功能全部退出。

#### 网络状态检测接口

提供网络状态检测接口，用户单位APP调用该接口后，可知当前移动终端上的网络状态。

## 后台管理系统升级改造

### 接入管理

实现移动用户、业务系统的接入管理，并支持对接入申请的打印和查询功能。主要包括对移动用户和业务系统服务器的接入管理。

* 移动用户管理：新增移动用户、删除移动用户。移动用户新增成功，即完成了该用户的IP分配，该用户注册绑定了设备、SIM卡、单位代码后方可访问政务网；移动用户删除成功后，用户被注销，其绑定的设备被停用、SIM卡被停用、移动IP被收回。
* 业务系统服务器管理：新增业务系统服务器、删除业务系统服务器、新增业务系统服务器访问策略。业务系统服务器新增成功，即完成了该服务器的IP分配；业务服务器删除成功，即完成了该服务器的IP收回；业务系统服务器访问策略新增成功，即完成了服务器访问策略的配置。

### 移动用户注册管理

1. 注册绑定：后台管理系统接收政务通提交的用户注册信息，根据手机号匹配用户，向政务通确认绑定后，自动完成用户注册信息的绑定。
2. 变更绑定：

* SIM卡序列号、终端设备号（IMEI号）变更：政务通进行用户二次身份认证时检测到SIM卡序列号、终端设备号（IMEI号）变更，需用户单位管理员通过后台管理系统进行变更确认,单位管理员会通过设备变更模块来完成用户注册信息的变更绑定，变更后用户权限不变。
* 登录密码变更：通过政务通进行密码修改或通过后台管理系统进行密码重置。

1. 密码重置：提供对移动用户登录政务通的密码重置功能，重置后的移动用户密码为默认密码。

### 应用管理

1. 应用注册：应用本身信息输入（应用名称、大小、截图、功能说明、APK文件上传）、应用发布方式选择、应用权限用户选择。
2. 应用授权：提供对用户单位APK文件的授权打包处理。应用授权，即为每一个应用自动生成一个唯一的软件授权码后将应用重新打包（不同版本的应用软件授权码不同）。被授权的应用会自动添加至应用白名单，用于应用可信认证。支持对授权打包后应用的下载。
3. 应用发布给本单位的人员使用，也可共享给外单位或者外单位的某位人员。
4. 应用基本信息维护：包括对应用的创建、查询、修改、删除。
5. 应用控制服务：提供应用强制发布和共享发布两种发布方式。强制发布的应用会强制安装到政务通上，用户可直接使用；共享发布的应用，用户可通过政务通自选下载安装使用；非共享的应用其他单位的人员可以在政务通中看到此应用的基本信息，无法下载。
6. 应用发布：应用审核通过即执行发布操作。系统基于应用选择的发布方式，完成应用的一般发布、强制发布、共享发布。
7. 应用升级管理：支持对低版本应用的升级发布管理。应用升级时会校验APK包内签名的一致性。
8. 应用注销：可对某个/某些用户进行应用注销，可对单个应用进行应用注销。应用注销后，会自动在应用白名单中删除该应用，客户端不再提供改应用的下载；政务通上已安装且被注销后的应用无法启动，系统自动提醒告知用户。
9. 应用黑名单管理：包括对黑名单应用的创建（无需上传APK文件、但必须输入包名）、修改、查询、删除。
10. 应用白名单管理：白名单为自动生成，无需增删改的操作
11. 应用历史版本管理：可查阅应用所有不同版本的相关信息，并支持对应用程序包的下载。

### 查询统计

1. 移动用户查询统计：按时间维度，对各用户单位接入用户情况、用户使用政务网情况、活跃用户（登录次数）进行统计分析。并支持多种统计图表展示功能。
2. 用户单位应用查询统计：按时间维度，对各用户单位应用的发布情况、应用的下载情况进行统计分析；按业务类别维度，对各单位不同时间段的应用的发布情况、下载情况进行统计分析。并支持多种统计图表展示功能。
3. 政务通查询统计：按时间维度，对各单位使用政务通（不同类别、不同版本）的移动用户量进行统计分析。并支持多种统计图表展示功能。
4. 查询统计的表头部分支持升序或者降序的排列功能。

### 系统管理

1. 权限管理：为经信委、资源中心、用户单位分配不同的权限。
2. 组织机构管理

* 单位管理：包括对组织机构的创建（包含单位及单位下属的一级部门）、修改、查询、启用和禁用管理。单位禁用后，单位内所有移动用户被注销、单位管理员被停用。
* 人员管理：包括对单位内人员信息的创建、修改、查询、删除管理，同时支持excel形式的人员导入管理。

1. 业务类别管理：包括对业务类别的创建、修改、查询、删除管理，业务类别不提供多级管理。
2. 移动用户IP域管理：包括对移动用户IP域的创建、修改、查询、删除管理。
3. 系统消息管理：提供基于模板形式的系统消息内容发布管理
4. 政务通管理

* 政务通版本管理：提供不同类别政务通的发布及版本升级管理。
* 政务通安装包下载：通过后台管理系统可对不同类别政务通的不同版本进行下载操作。

1. APN动态策略配置：设置系统级APN密钥的动态策略（如一个月变化一次、一个星期变化一次、每次登陆变化一次等。（注：每次登陆均发生变化为默认项），由用户单位自行设置。APN秘钥数据会基于管理平台的控制文件管理机制，实现在移动终端的数据更新。
2. 日志管理：对系统管理员操作行为、移动终端应用访问行为、移动用户操作行为进行记录，供查询分析。
3. 消息提醒

* 任务提醒：每次登陆后台管理系统后，对各管理员当日待办任务、已办任务进行提醒。
* 过期提醒：单位管理员选择设置不活跃用户时间周期，分为一个月，三个月，六个月，十二个月，也可自定义过期提醒时间，单位（月）

### 安全管理

1. 控制文件管理：负责控制文件的信息更新与同步管理，政务通处于政务网状态时，一旦控制文件有更新便立即同步至政务通，由政务通完成本地控制文件的更新。控制文件主要包括用户身份认证信息（单位代码、手机号、SIM卡序列号、终端设备号（IMEI号）和用户密码）、应用防火墙配置信息（应用黑名单和应用白名单）和APN动态密钥。
2. APN动态密钥管理：后台管理系统基于用户信息制定政务网APN连接的秘钥组成和认证机制，支持秘钥的动态策略。
3. 用户身份二次认证：根据政务通的二次身份认证请求，后台管理系统通过手机号匹配用户当前存在于数据库中的有效用户信息，与通过政务通提交的单位代码、SIM卡序列号、终端设备号IMEI号进行二次安全认证，AAA服务器认证通过但二次认证未通过，则告知政务通认证未通过原因。

# 其他需求

## 性能需求

（1）客户端登陆时终端环境及终端功能管控的时间<=2秒;主要包含以下内容：

* 获取sim卡序列号响应时间：<=0.01秒
* 获取电话号码响应时间：<=0.01秒
* 获取IMEI编号响应时间：<=0.01秒
* 飞行模式检测响应时间：<= 0.02秒
* Sim卡检测响应时间：<=0.02秒
* USB网络分享检测与关闭响应时间：<=0.1秒
* Wlan网络分享检测与关闭响应时间：<=0.1秒
* 蓝牙检测与关闭响应时间：<=0.1秒
* 新建APN响应时间：<=0.2秒
* 打开网络开关响应时间：<=0.02秒

（2）客户端启动打开时间<=2秒;

（3）客户端本地功能打开响应时间;

（4）平台能支撑持1万个用户的正常使用；

（5）政务通退出时<=2秒

## 文档需求

1. 用户文档

* 安装手册：用于指导管理平台安装的文件，Word格式。
* 用户使用手册：用于指导用户使用管理平台的文件，Word格式。

1. 技术文档

* 需求文档：本需求规格说明书。
* 设计文档：用于指导管理平台软件开发和测试的概要设计、详细设计及数据库设计文件，Word格式。
* 测试文档：用于指导测试的测试用例文件和基于测试用例文档的内部测试报告，Word格式。

# 界面设计

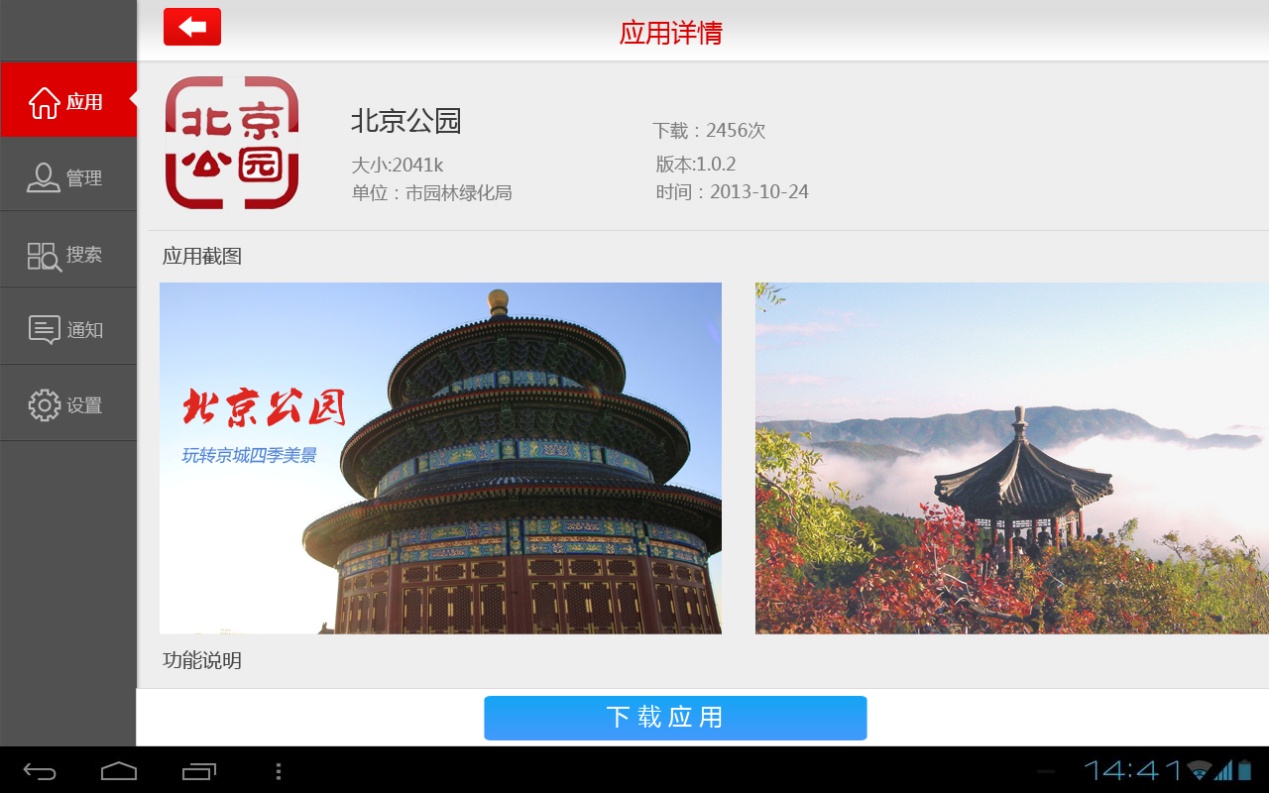
## 政务通

* 个人应用工作区



* 应用搜索







* 应用管理









* 设置



* 通知



## 后台管理系统

参见原型设计。