**百度车联网【福特项目】**

需求说明书

【地图安全隐私权限】

v1.0.1

**修订历史**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本号** | **修订日期** | **修订者** | **修订内容** |
| **V1.0.0** | **2021.8.26** | **原翼** | **创建** |
| V1.0.1 | 2021.8.30 | 原翼 | 修改了css=off的情况 |

分页符

目录

[**1.需求概述**3](bookmark://_Toc23623160)

[1.1背景价值3](bookmark://_Toc23623161)

[1.2名词解释3](bookmark://_Toc23623162)

[1.3阅读对象3](bookmark://_Toc23623163)

[1.4参考文档3](bookmark://_Toc23623164)

[**2.需求列表**3](bookmark://_Toc23623165)

[**3.需求描述**3](bookmark://_Toc23623166)

[*3.1第一个需求名字*3](bookmark://_Toc23623167)

[*3.2第二需求名字（同上）*4](bookmark://_Toc23623168)

[**4.合规意见**5](bookmark://_Toc23623169)

[**5.安全意见**5](bookmark://_Toc23623170)

[**6.项目实现目标期望**5](bookmark://_Toc23623171)

￼

分页符

1. **需求概述**
2. 背景价值

*客户针对路况开关默认开启方式进行确认。*

1. 名词解释

*CCS: Customer Connectivity Service 车机定位总开关*

1. 阅读对象

*参与功能设计/开发/测试的PM/UE/UI/RD/QA*

1. 参考文档

*列出本文档参考的文档名称，应有版本号或对应日期*

1. 需求使用版本范围

*福特phase5车型。*

1. **需求列表**

|  |  |  |
| --- | --- | --- |
| **模块** | **功能** | **概要描述** |
|  |  |  |
|  |  |  |
|  |  |  |

1. **需求描述**

1. **总体描述**

1.1背景：

随着国家个人信息保护相关法规的趋严，以及福特一致致力打造the most trusted company角度，福特需要为SYNC+系统打造一套全面完整的隐私权限管理方案。

相较于SYNC+ phase1/2，仅依靠《用户协议》和《隐私政策》的管控外，福特在SYNC+ phase3上引入了百度车机管家，对部分百度应用进行了隐私权限管理；phase4上结合福特CCS（Customer Connectivity Setting）和车机管家，进一步加强隐私权限的管理。

由于车机管家相较其他功能上线时间较晚，但是这一年来，团队非常努力，共同梳理了各个应用功能所需的隐私数据，更新MRD，并加速推进相关模块和应用的开发，已经取得一些成果。但是最近在Launcher相关的讨论中，鉴于Launcher的特殊性（不是一个真正意义上的客户应用功能，而更像各个应用信息的集成显示框架），其模块本身和内含卡片的隐私相关设计逻辑缺少充分的说明，在测试中产生了一系列的issue。

而针对百度地图，福特要求针对定位以及麦克风进行相应安全权限管控。而本MRD就是针对相应管控跳进进行需求策略描述。

1.2 法务隐私合规要求

* **权限最小必要性**

实现产品的功能与使用的隐私权限有直接关联关系（通过史宾格扫描）

* **权限可选择性**

使用敏感权限需要提供给用户选择同意和拒绝的界面，并说明每个权限的申请目的

* **禁止捆绑获取**

禁止APP不给权限不让用。产品功能申请的隐私权限拒绝后，应用退出，即为捆绑授权

* **禁止过度索取**

在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，或超出其业务功能或服务外，申请通讯录、定位、短信、录音、相机等权限。

* **权限可关闭性**

对于已经授权的权限，用户可以再次取消授权

* 1. 隐私定义
* **个人信息定义：**

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。



* **个人敏感信息定义**

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。



* **隐私权限定义**

安卓定义的敏感权限组，具体包括：定位、麦克风、摄像头、磁盘存储、电话、通讯录、日历、短信；其中摄像头、磁盘存储、电话、通讯录、日历、短信不在本项目管控范围内，APP默认具备相关权限。

|  |  |  |
| --- | --- | --- |
| 权限 | 中文对应 | 权限分类 |
| android.permission.BODY\_SENSORS | 访问身体传感器 | 传感器 |
| android.permission.READ\_EXTERNAL\_STORAGE | 读取外置存储卡 | 磁盘存储 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 写入外部存储卡 | 磁盘存储 |
| android.permission.CALL\_PHONE | 拨打电话 | 电话 |
| android.permission.PROCESS\_OUTGOING\_CALLS | 重新设置外拨电话的路径 | 电话 |
| android.permission.READ\_CALL\_LOG | 读取通话记录 | 电话 |
| android.permission.READ\_PHONE\_STATE | 读取手机状态和身份 | 电话 |
| android.permission.WRITE\_CALL\_LOG | 新建/修改/删除通话记录 | 电话 |
| android.permission.USE\_SIP |  | 电话 |
| com.android.voicemail.permission.ADD\_VOICEMAIL | 添加语音邮件 | 电话 |
| android.permission.ACCESS\_COARSE\_LOCATION | 获取粗略位置 | 定位 |
| android.permission.ACCESS\_FINE\_LOCATION | 获取精确位置 | 定位 |
| android.permission.READ\_SMS | 读取短信 | 短信 |
| android.permission.RECEIVE\_MMS | 接收彩信 | 短信 |
| android.permission.RECEIVE\_SMS | 接收短信 | 短信 |
| android.permission.RECEIVE\_WAP\_PUSH | 接收讯息 (WAP) | 短信 |
| android.permission.SEND\_SMS | 发送短信 | 短信 |
| android.permission.RECORD\_AUDIO | 录音 | 麦克风 |
| android.permission.READ\_CALENDAR | 读取日历活动和详情 | 日历 |
| android.permission.WRITE\_CALENDAR | 添加或修改日历活动 | 日历 |
| android.permission.CAMERA | 摄像头 | 摄像头 |
| android.permission.READ\_CONTACTS | 读取联系人 | 通讯录 |
| android.permission.GET\_ACCOUNTS | 查找设备上的帐号 | 通讯录 |
| android.permission.WRITE\_CONTACTS | 修改通讯录 | 通讯录 |

1. **业务规则描述**

 2.1 总体产品设计

2.1.2 UI部分

|  |  |  |  |
| --- | --- | --- | --- |
| 页面编号 | 页面划分 | 说明 | 备注 |
| 1 | 单个权限申请 | 地图对定位以及麦克风的权限申请授权 |  |

2.1.3 开发需求描述

1. 【开发阶段】各业务模块apk要通过史宾格检测，避免过度权限申请；具体操作及验证方法可参考以下链接：

<http://wiki.baidu.com/pages/viewpage.action?pageId=1042359684#id-%E8%BD%A6%E8%81%94%E7%BD%91%E9%A1%B9%E7%9B%AE%E5%8F%B2%E5%AE%BE%E6%A0%BC%E6%8E%A5%E5%85%A5-%E5%AE%89%E5%85%A8%E5%90%8C%E5%AD%A6todo%EF%BC%882%E9%A1%B9%EF%BC%89>

或联系百度安全模块团队。

1. 【开发阶段】针对定位以及麦克风隐私权限，需要通过【车机管家】进行权限申请和权限管理。

2.1.4 隐私管控

目前针对车机地图，隐私权限包括：定位，麦克风。

隐私权限管控策略：

地图的定位/麦克风权限原先为S1隐私管控权限，现更改为S2或S3隐私管控权限。

S1、车机激活前后都默认权限开启。在车机管家隐私页面不可以开启和关闭该应用隐私权限；

S2、车机激活前默认关闭，激活后默认开启。激活前可以通过应用隐私权限申请申请权限开启权限，可通过车机管家隐私设置页面开启或关闭隐私权限。

S3、车机激活前默认关闭，激活后默认开启。激活前不可开启权限，激活后可在车机管家隐私页面或权限申请弹窗中开启和关闭该应用隐私权限，权限被关闭后应用内弹窗申请让用户授权；

**\*说明：**

激活：是指车主在福特派手机端和sync+车机端完成车机激活操作。用户车机恢复出厂设置后需重新进行激活。

（具体详见百度车联网隐私管控MRD）

定位服务页面显示的APP，页面如下：



麦克风权限显示的APP，页面如下：



2.1.5 地图使用策略

地图应用App开启场景按照车辆状态分为激活和未激活状态，以下针对两种状态进行地图开启场景的策略描述。

<1>.车机未激活：

在车机未激活前，车机管家的定位服务页面为隐藏状态，麦克风页面为显示状态，所有应用的定位服务为关闭状态，用户定位权限用户不可开启，麦克风权限用户可开启；

用户使用地图app申请定位权限的弹窗中定位服务为默认不勾选，且不可勾选，麦克风为默认勾选状态，用户可以取消勾选。

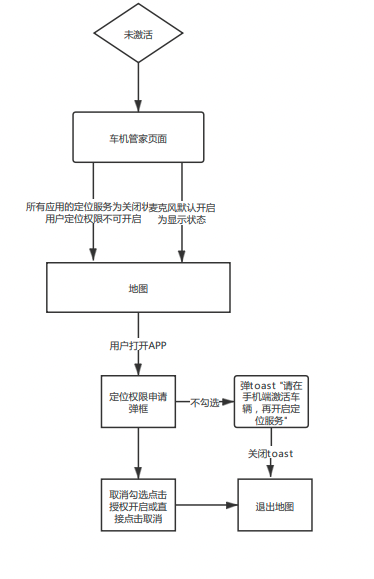


图1 未激活态定位获取

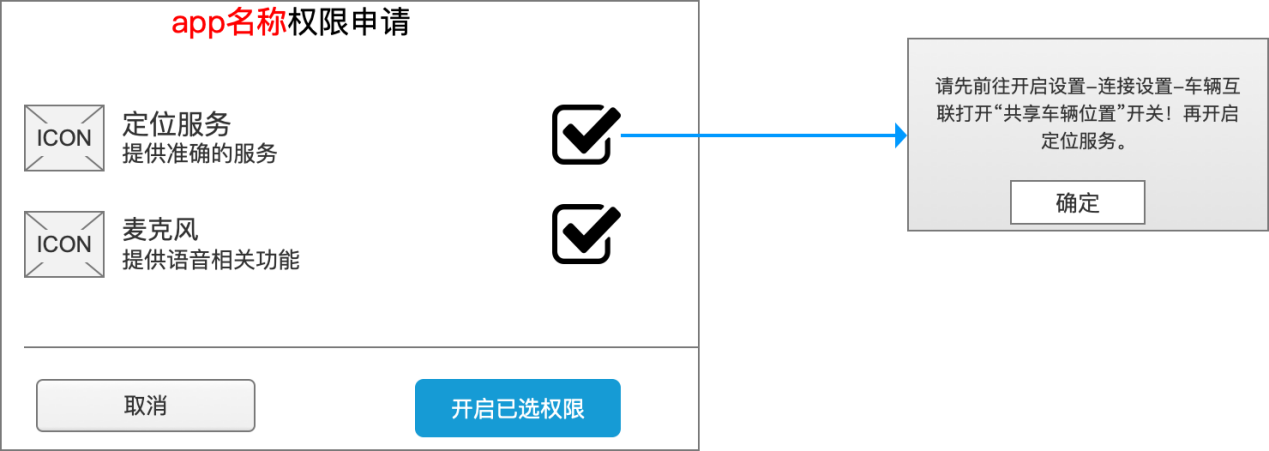


图2 权限消息弹窗

需要说明的是:

**【开启已选权限】**用户点击则开启以上勾选权限，不开启未勾选权限。如果车机未完成激活，在使用APP时，权限申请弹窗中【开启已选权限】/【确定】为~~致灰不可点击状态~~高亮状态（只要定位按钮不可选），用户点击后弹toast提示”请在手机端激活车辆，再开启定位服务” 当用户取消全部权限的勾选时，【开启已选权限】文案自动变更为【确认】。点击确认弹窗中权限拒绝，弹窗消失。且退出APP.

**【取消】**用户点取消按钮弹窗消失，直接退出app，不授予对应的权限.

<2>.车机已激活：

-车机激活后，车机管家的定位服务为显示状态，定位服务和麦克风为打开状态。恢复出厂设置后重新激活，隐私权限重置。

-CCS在车机激活后默认开启，并打开全部应用的定位开关。用户可以使用地图。

-若CCS被设置为off，用户打开地图后出现权限弹框，权限申请弹窗中【开启已选权限】/【确定】为~~致灰不可点击状态~~高亮状态，定位勾选默认置灰无法勾选，当用户点击定位勾选框，出现toast：『请先前往设置-系统设置-连接设置-车辆互联设置打开“共享车辆位置”开关！否则无法使用地图』。（所以此场景是即便麦克风权限开启，并授权，地图依然退出）

-若CCS=ON, 且用户主动在车机管家关闭定位按钮，用户打开地图后出现权限弹框，用户需要勾选授权，若用户拒绝授权，退出app.

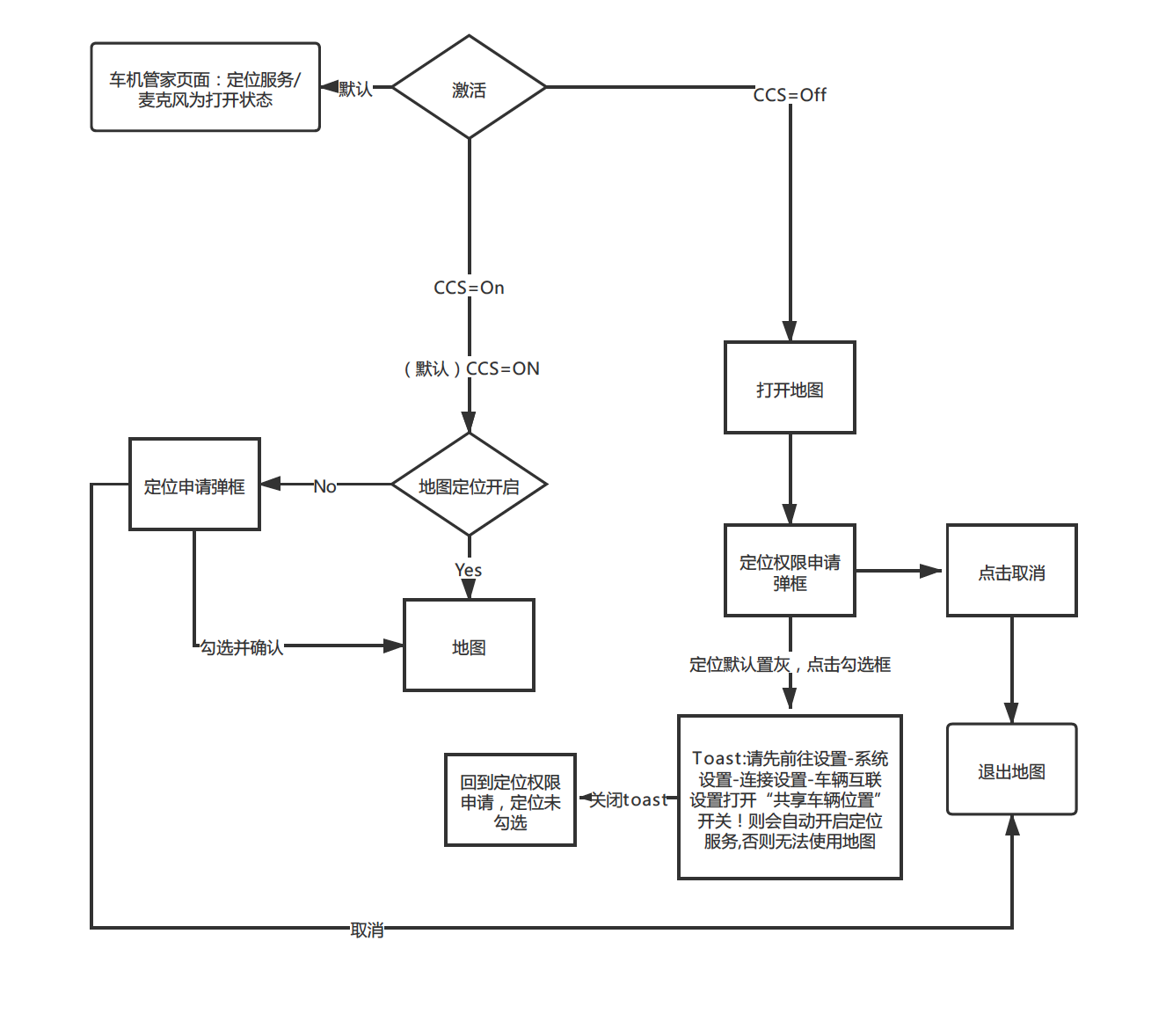


图3 激活态地图定位获取

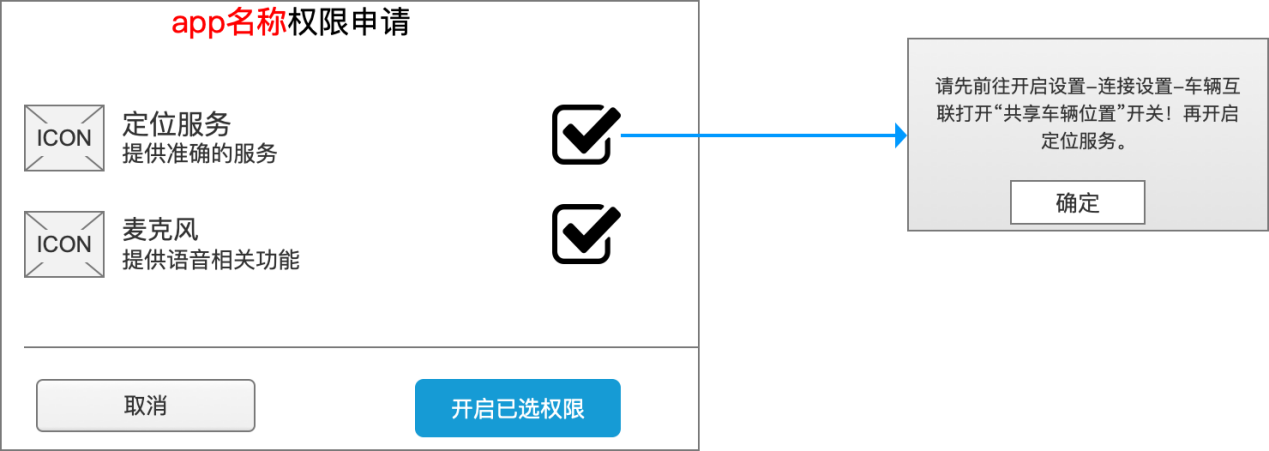


图4 CCS=Off的地图定位弹窗

若CCS=ON,且用户在首次进入地图没有授权麦克风，或是在车机管家主动关闭地图对麦克风的权限控制，当用户发起事件语音上报时，会出现麦克风权限弹窗，用户勾选确认进入事件上报，用户取消，报错无法上传事件。

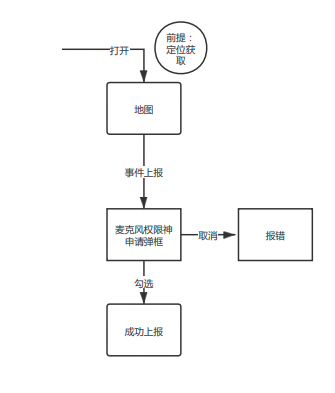


图5 麦克风权限获取

\*另车机管家内应用的开启打开以及集成应用弹框SDK等不在此MRD累述。

1. **埋点需求**

|  |  |  |  |
| --- | --- | --- | --- |
| 功能描述 | 事件编码 | 事件描述 | 属性字段 |
| 定位/定位+麦克风弹框取消按钮 |  | 以（天）为单位，记录次数，用户打开地图出现定位/麦克风权限弹框按钮，取消按钮点击次数/用户数，记录页面停留时间。 | TOUCH |
| 定位/定位+麦克风弹框『开启授权按钮』按钮 |  | 以（天）为单位，记录次数，用户打开地图出现定位/麦克风权限弹框按钮，开启已选权限按钮点击次数/用户数，记录页面停留时间。 | TOUCH |
| 激活toast确认按钮 |  | 以（天）为单位，记录次数，用户打开地图出现定位/麦克风权限弹框按钮，车辆未激活，用户点击开启授权按钮后出现toast,用户点击确定次数/用户数。 | TOUCH |
| CCS关闭Toast 确认按钮 |  | 以（天）为单位，记录次数，CCS=OFF,用户打开地图出现定位/麦克风权限弹框按钮，用户点击开启授权按钮后出现toast,用户点击确定次数/用户数。 | TOUCH |
| CCS开启定位/定位+麦克风弹框确认按钮 |  | 以（天）为单位，记录次数，CCS=on,用户打开地图出现定位/麦克风权限弹框按钮，用户勾选，开启已选权限转为确认，用户点击确定次数/用户数。 | TOUCH |
| 麦克风弹框取消按钮 |  | 以（天）为单位，用户使用事件语音上报，出现麦克风授权弹框，用户点击取消次数/用户数 | TOUCH |
| 麦克风弹框确认按钮 |  | 以（天）为单位，用户使用事件语音上报，出现麦克风授权弹框，用户勾选，开启已选权限转为确认，用户点击确定次数/用户数。 | TOUCH |

1. **异常情况**

*针对上述规则，是否存在异常情况，如有描述异常情况，以及对应的兜底措施（如有）*

1. **可行性**

*分析技术上是否可行，是否存在技术壁垒*

1. **验收标准**

验证环境：*可以是所处地理环境，也可以是验收时使用的硬件设备环境*

前置条件： *需在什么样的前提条件下进行验收，例如网络良好，GPS信号正常等*

验收标准： *在以上验证环境和前置条件下，进行什么样的操作及得到对应什么结果，可视为通过验收*

。

1. *第二需求名字（同上）*
2. **总体描述**
3. **业务规则描述**
4. **异常情况**
5. **可行性**
6. **验收标准**

验证环境：

前置条件：

验收标准：

1. **合规意见**

*该需求是否存在潜在违规风险*

1. **安全意见**

*给出安全团队的意见*

1. **项目实现目标期望**

*阐述该需求在本项目需实现的目标*