福特phase4、phase5项目百度地图签约管理产品方案v1.00.06

保密等级：机密

百度ASD工程交付中心

0 修订历史

版本号	修订日期	修订记录	修订人	审核人
1.00.00	2023/6/8	基于签约模块定稿v1.01.01编制地图签约模块方案 3.1.1增加百度地图侧接入签约合规方案的时机 3.2.2.2增加百度地对于敏感信息到期后处理逻辑 3.2.1.3 -》5.增加 百度地图不强制依赖百度账号登录	叶佳蕾	林长利
1.00.01	2023/6/9	3.1.1删除方案一，与福特确认，「行踪轨迹」采集方案使用方案二	叶佳蕾	林长利

3			3.1.2增加进入百度地图时的主要合规方案流程图 3.2.1.1更新架构图，增加地图apk		
4	1.00.02	2023/6/10	3.1.2修改进入百度地图时的主要合规方案流程图	叶佳蕾	林长利
5	1.00.03	2023/6/13	根据签约整体prd第2章节「默认勾选长期有效」修改为「默认不勾选」，同步纠正本文档，默认不勾选	叶佳蕾	林长利
6	1.00.04	2023/6/15	全文「行踪轨迹」修改为「位置」 3.2.2.2增加权限、隐私协议、敏感信息的解耦策略 3.2.2.2增加分开处理敏感信息关闭和授权到期的策略，保持和隐私协议的一致性	叶佳蕾	林长利
7	1.00.05	2023/6/15	3.1.2 增加phase4项目的流程图和描述 5.0 客户端页面触发机制增加地图触发签约弹框场景定义	全海波	苏静
8	1.00.06	2023/6/16	3.1.2 新增用户协议签署退出地图的流程图、敏感信息授权时效区分账号登陆模式和游客模式	全海波	苏静

1. 概述

1.1. 背景价值

随着个人信息保护政策的逐步完善，为规范汽车数据处理活动，保护个人、组织的合法权益，对用户签约流程及管理提出了更多的要求。根据个保法相关要求，对福特项目小度车载OS相关应用进行隐私协议和敏感信息授权合规设计。

1.2. 名词解释

Ø一般个人信息

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。

本项目中涉及的一般个人信息主要指：VIN、CUID、账号等可定位到具体个人的信息；

Ø个人敏感信息

是一旦泄露、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一般个人信息。

项目中涉及的敏感个人信息主要指：GPS位置、语音音频、通讯录、摄像头图像信息。

Ø宿主App

签约管理客户端不作为一个单独的APP，无应用中心（APPlist）的入口。对于福特phase4和phase5项目，帐号可作为签约宿主APP

1.3. 阅读对象

本文档的读者是百度和福特产品规划和评审人员、项目管理人员、技术开发人员、产品设计人员、测试相关人员、项目监管人员等。

1.4. 系统环境

1.4.1 硬件环境

芯片：高通8155、820A、安卓8.1版本

1.4.1 软件环境

操作系统：安卓11

1.5. 客户需求

暂无

1.6. 适用项目及车型

福特百度车机地图全部车型，后续如有其他新车型，则采用此方案横展。

phase5项目：CDX 707、U625、U611 CDX718

phase4项目：CD542H、U625ICA、CDX706H、CD764、483MCA、CX727、CDX706L、S650、U554、CD54L、P702、P702MCA、CD542ICAH、CD542ICAL、U625ICA TBL、CD764ICA、483PT ICA、CX727ICA、U725C

2. 需求列表

一级模块	一级模块	三级功能	功能说明	需求优先级
用户签约管理	文件及签约状态存储及管理	协议文件管理	协议文件及其参数的存储、更新、管理，包括待签署文件和已签署文件。	P0
		签约状态管理	用户的签约状态的存储、更新、管理，包括该帐号签署的协议类型、协议文件、签约时间等。	P0
		默认文件	考虑到弱网环境，提供本地默认文件。	P1
		签约状态广播/查询	提供接口告知客户端其它模块签约状态。	P0
	客户端签约HMI（用户可见）	用户签约页面	提供客户端签约页面，该页面可以被第三方应用调用或根据页面触发机制弹出。可在页面进行“同意协议、拒绝协议、同意全部协议按钮操作	P0
		协议查看页面	需提供页面给用户查看最新的已签署的协议（并非最新的协议！），用户可以查看协议标题、内容、签署时间、版本号、发布日期，除此之外，用户还可以在此页面撤销已经同意的协议。	P0

8			第三方模块调用能力	第三方应用可以调用用户签约页面和协议查看页面，需开放接口给其它应用调用。	P0
9			页面触发机制	根据帐号登录/切换登录、开机（用户未签署协议或已签署协议版本更新）、百度系应用业务逻辑触发等判断等自动调起用户签约页面。	P0
10			客户端页面其他需求	进入页面加载提示、webview加载提示； 进入协议查看页面，可能出现无任何已签署协议的情况，此时需要显示缺省页	P2
11		特殊场景	恢复出场设置	恢复出厂设置，视为全新车机需要重新签署	P2
12			更换车机	更换车机，视为全新车机，需重新签署	P2
13			车机皮肤适配	用户签约属于低频但必要功能，且html内容基本上是文字信息，建议从UI设计层面使用一套中性文字颜色+webview深色背景应对。	P2
14			语言切换	签约模块仅支持中文	P2
15	敏感信息授权	入口定义	访问入口	对用户车内敏感信息授权查看和管理的统一入口	P1
16		敏感信息授权设置弹框	敏感信息授权管理设置	查看并管理各应用的敏感信息开关，敏感信息列表及展示隐私权限相关应用列表、授权到期时间和开关按钮	P0
17				用户选择权限有效期后，根据当前的本地时间进行权限到期时间计算并进行权限到期时间展示，每次车机上电，“敏感信息SDK”在后台初始化完成后，获取系统时间并根据最新时间检测所有帐号的应用敏感信息授权有效期，关闭已过期的应用的敏感信息权限。同时更新在本地保存的授权信息	P0
18		敏感信息申请弹框	敏感信息申请弹框	车机应用通过调用敏感信息授权SDK，调起“应用权限申请弹窗”来申请应用所需要的敏感信息授权弹框。	P0
19			选择有效期	有效期”选项（3个月/6个月/12个月），每次最多可选择一个选项，默认不勾选。	P0

3. 需求描述

3.1. 总体产品设计

3.1.1. 需求概述

本文档内容包含内容如下：

- **《服务条款》和《隐私政策》授权（统称百度一般协议）**
  - 小度车载OS产品，使用一套协议进行签约；签约管理作为一个统一的模块，需对“用户协议及隐私声明”进行综合管理，用户签约状态存储和管理，用户签约HMI，协议签署情况同步小度车载OS相关应用等。
  - 百度一般协议签约要求：已登录百度帐号用户签约一次长期有效，支持用户撤回、取消协议签署；未登录百度帐号用户本次开机有效。
- **敏感个人信息授权**

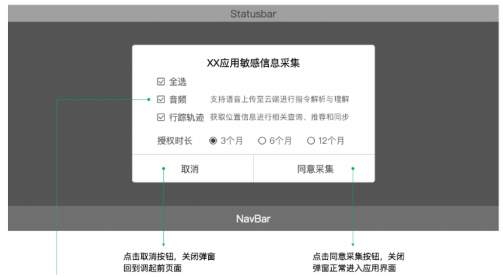
百度地图支持单独采集相关敏感信息，具体描述如下。

支持单独采集

仅勾选其中一项时，支持用户点击同意采集，再次进入应用触发敏感信息授权时，对应弹出未授权的敏感信息弹窗

音频未授权时

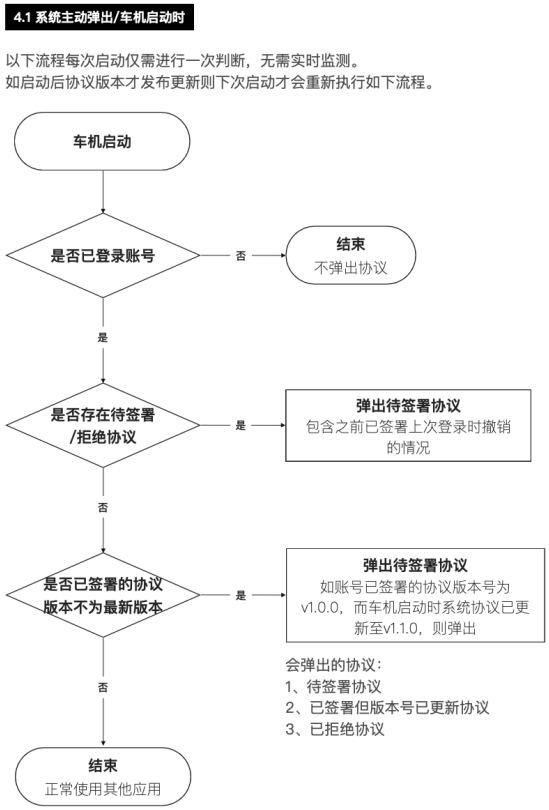
行踪轨迹未授权时

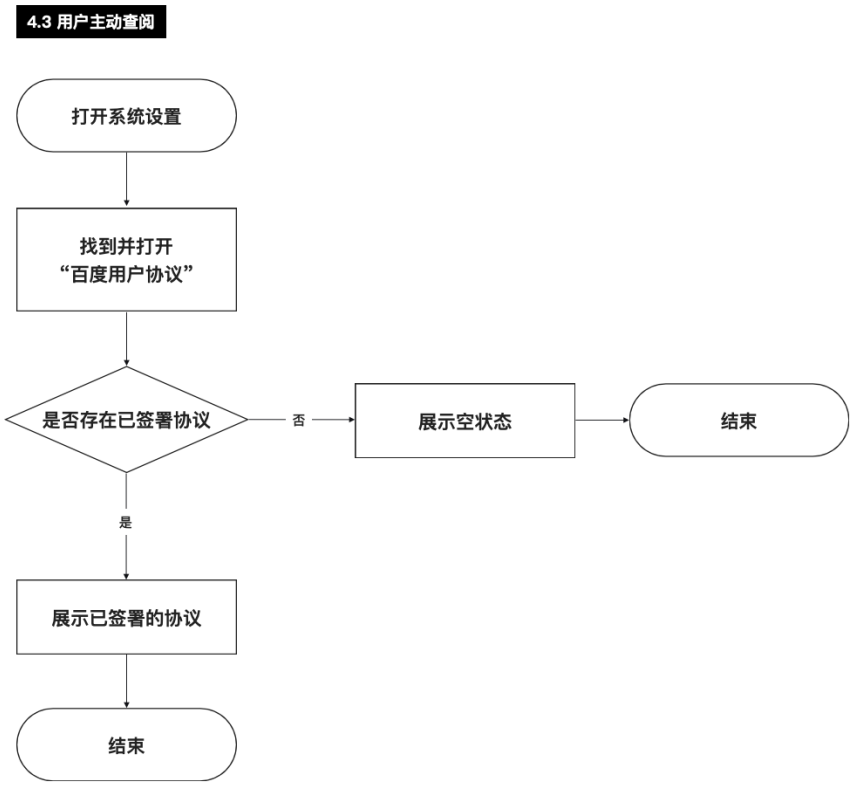
1	权限名称	应用位置	拒绝授权	图示
2	位置	打开地图首页	【时机】首次进入APP时提醒需要采集位置 拒绝后不可进入地图，并二次提示「未同意位置采集，不能使用百度地图」，显示5-8s，并退出地图。 （具体交互方式及内容以ue为主） @朱修齐	

3	位置	「位置」信息授权关闭	关闭敏感信息授权开关后，需要二次弹框确认，文案参考：「未同意位置采集，不能使用百度地图」，显示5-8s，并退出地图。关闭弹框后退出地图。具体交互方式及内容以ue为主 @朱修齐	
4	音频	事件上报-语音麦克风-开始	【时机】 a）首次进入地图时提示需要采集音频，若用户拒绝，则可正常进入地图。 b）点击使用「事件上报-语音麦克风-开始」功能时提示 拒绝后不可以正常使用地图的「麦克风」 1.拒绝后再使用「麦克风」功能，需要调起「签约接口」-音频采集权限，用户点击「同意采集」，即可正常退出授权页面，用户可以点击麦克风说话。 若用户点击「取消」，即退回到麦克风说话页面。再次点击麦克风又调起「音频采集页面」。 用户也可后退上一层页面，正常使用其他地图功能。 （具体交互方式及内容以ue为主） @朱修齐	 音频未授权时 
5	音频	「音频」信息授权关闭	关闭敏感信息授权开关后，需要二次弹框确认，提示【音频相关功能受限】，关闭弹框后留在地图页面。具体交互方式及内容以ue为主 @朱修齐	

敏感信息授权要求：单独弹窗，且支持用户选择有效期、支持用户关闭授权。

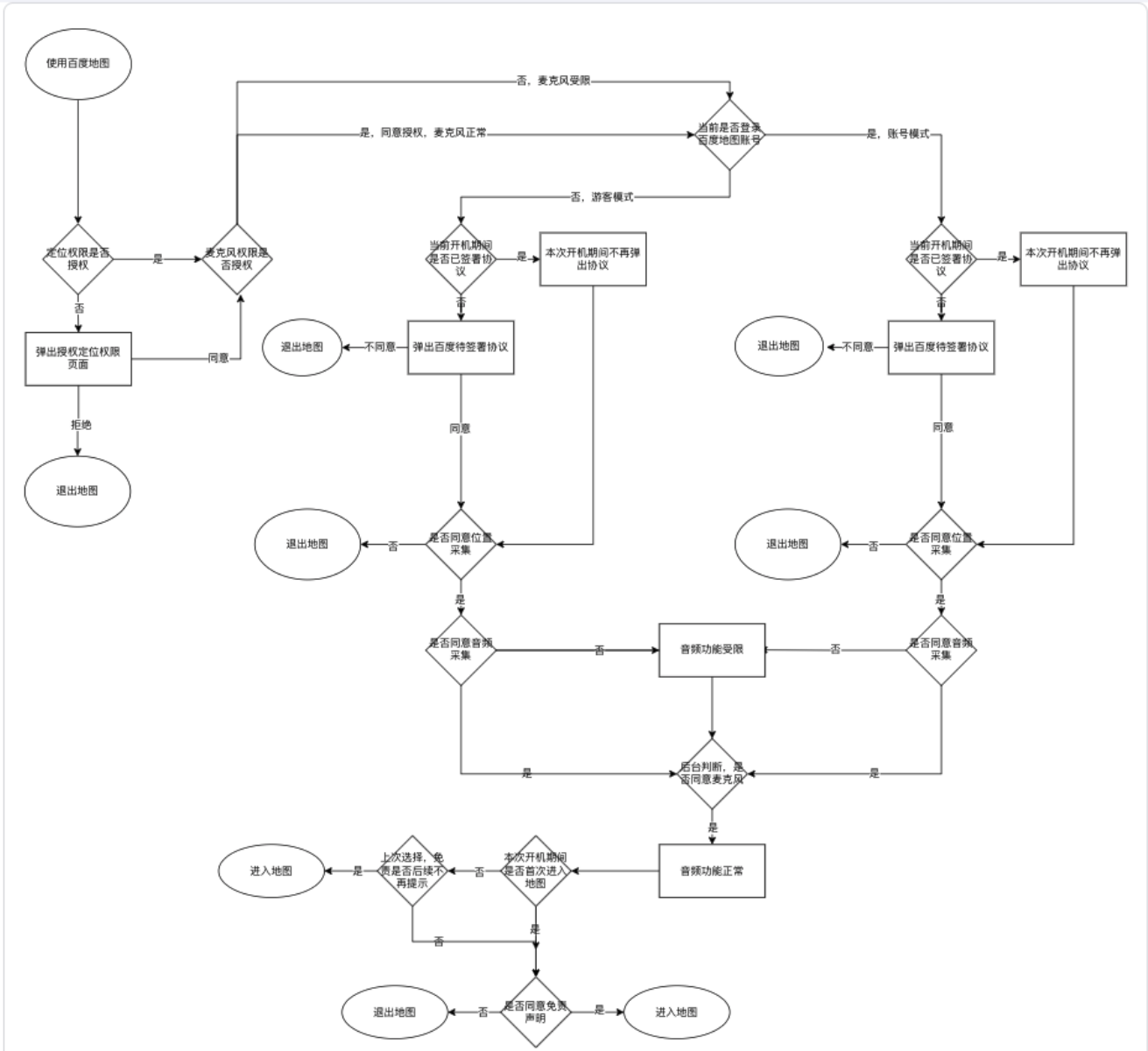
3.1.2.流程概述





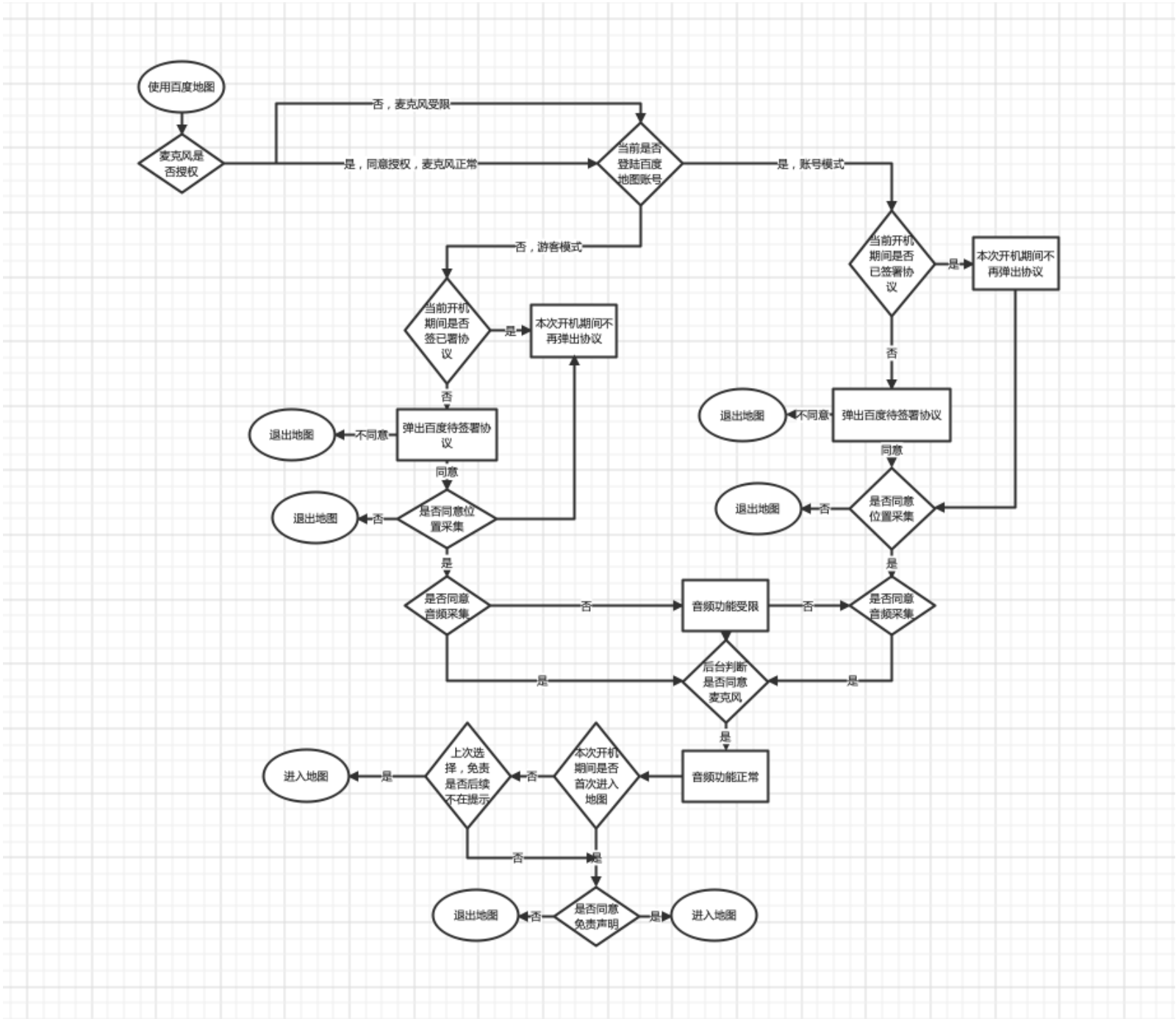
在百度地图侧需要打开如下授权：1定位权限，2麦克风权限，3签约界面（若需要签约则唤起签约界面，若不需要签约则无该界面），4位置采集，5音频采集，6免责声明。

主要流程如下：



注：关于敏感信息授权，在游客模式（未登陆账号）每次开机都会弹出敏感信息授权，登陆账号模式下根据用户上次选择的有效期（3月、6月、12月）进行敏感信息授权。

phase4项目的定位权限授权保持在白名单中，不会弹窗授权，首次启动APP先进入麦克风权限授权弹窗，具体流程图如下：


使用百度地图
麦克风是否授权
否，麦克风受限
是，同意授权，麦克风正常
当前是否登陆百度地图账号
是，账号模式
否，游客模式
当前开机期间是否已签署协议
是
本次开机期间不再弹出协议
否
退出地图
不同意
弹出百度待签署协议
同意
是否同意位置采集
否
是
是否同意音频采集
否
音频功能受限
否
是否同意音频采集
是
后台判断是否同意麦克风
是
音频功能正常
本次开机期间是否首次进入地图
否
上次选择，免责是否后续不在提示
是
进入地图
否
是
是否同意免责声明
否
是
进入地图

注：关于敏感信息授权，在游客模式（未登陆账号）每次开机都会弹出敏感信息授权，登陆账号模式下根据用户上次选择的有效期（3月、6月、12月）进行敏感信息授权。

3.2. 总体产品设计

3.2.1. 小度车载OS协议签署

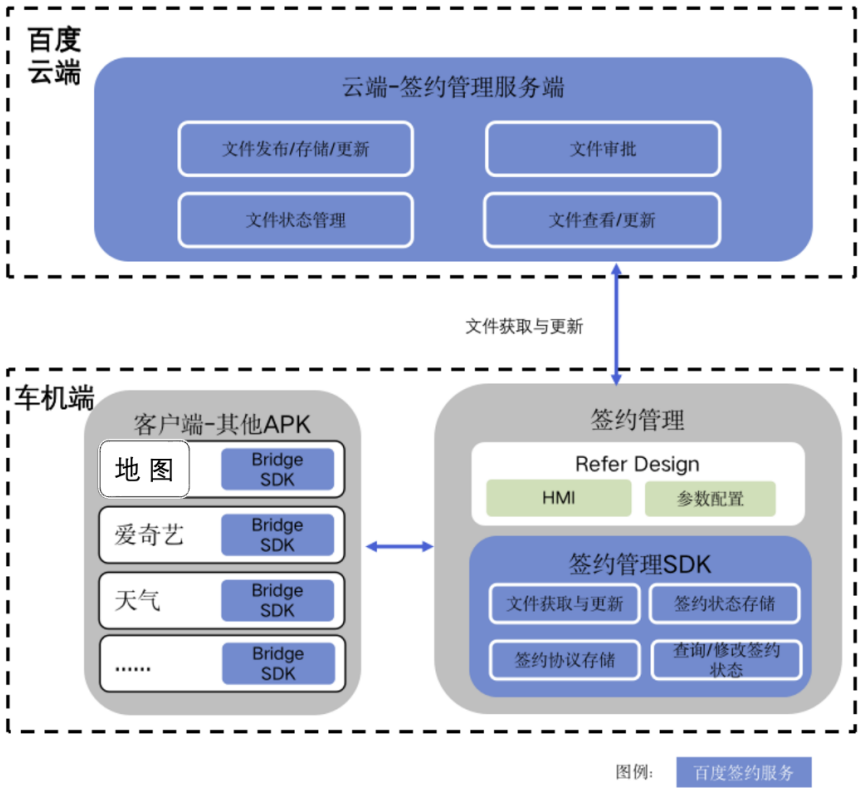
3.2.1.1. 产品架构

签约管理服务端：提供文件存储、发布、更新、文件状态管理、文件查看与更新等功能，并对运营人员提供web页面供其操作。

用户签约管理SDK：提供文件获取、文件更新等能力，并对外提供接口。

用户签约管理bridgeSDK：给其它业务模块集成，其它业务模块可以获取当前用户的签约状态。

签约模块（依赖宿主APP）提供查看已签署协议页面和用户签约页面。文件存储能力。并执行页面弹出逻辑。



3.2.1.2. 整体需求描述

用户签约管理客户端不作为一个单独的APP，无应用中心（APPlist）的入口。用户不能主动打开此模块，但是其页面可以根据逻辑弹出或被其他应用调出。对于福特phase4和phase5项目而言，帐号可作为（宿主APP）。客户端整体需求方案为：

- 协议及签约状态存储和管理；
- 车机端为用户提供签约页面，用户可以签署协议，也可以不签署协议，不得强制用户签约；
- 用户在车机端可以查看已签署的协议，并且撤销签署；
- 车机端将协议签署情况告知各个应用，各应用App根据未签署协议的用户定义产品管控逻辑；

3.2.1.3.客户端整体功能

用户签约管理客户端不作为一个单独的APP，无应用中心（APPlist）的入口。用户不能主动打开此模块，但是其页面可以根据逻辑弹出或被其他应用调出。对于福特Phase 6项目而言，帐号可作为（宿主APP）。

1.文件存储

文件（html文档）及参数需要存储在客户端（本地存储），按照以下要求维度存储：百度协议文件的存储需跟随帐号。

场景1：如果相同帐号在不同的车机上登录，则需要重新授权协议。

场景2：在同一个车机上切换帐号，则需要重新授权协议。

在系统中百度帐号和游客帐号都需要单独存储其已签署的文件及参数。如果百度帐号从车机系统里删除（如账号注销），则需删除已签署文件。游客视为一种特殊的帐号，游客帐号签署的文件仅在开机周期内保存，关机自动删除。

2.文件参数

在后台上传文件时，需要在服务端配置或自动生成参数，对于客户端，以下参数可以从服务端获取：

	参数	参数内容及要求	备注
1	文件类型	000：百度车机整体用户协议 001：百度车机整体隐私申明 002：OEM车机整体用户协议 003：OEM车机整体隐私申明 100-104：预留	在福特phase 4和phase5项目上，百度共2份协议，对应000及001。福特系统协议由车企自己管理，不在本次文件管理的范围内。 另外，为未来协议扩展预留，如果获取到编号100-104的文件时也视为本项目的有效文件，客户端显示协议时需根据后台数据动态显示，即显示可获取的协议文件（包括协议Tab、标题、协议内容等其他参数信息），如果无相应的文件则不显示该协议Tab和协议内容等参数信息。
2	版本号		默认版本号为V1.0.1，每次更新将自动更新版本号。
3	文件简称（文案）	汉字或数字、字母混排：不超过8个	将显示在客户端页面tab里，用户可以通过切换tab查看不同的协议。
4	文件正式标题（文案）		将显示在客户端页面的标题里
5	文件内容	HTML文档	将显示在客户端页面的正文里
6			

6	文件所属	百度文件	福特phase4和phase5项目文件所属为百度
7	发布日期及时间（生效节点）		正式发布的日期和时间，到达此节点后，客户端可获取新版协议。

3.签约状态存储和管理

客户端需根据所有系统中百度ID帐号记录用户的签署状态，记录的内容包括下表

序号	内容	说明
1	百度帐号ID	已登录帐号、游客帐号
2	已签署的文件参数（文件类型、版本号、发布时间、文件所属）	记录对应帐号签署过的文件类型、版本号、发布时间、文件所属。如果有多份文件，需全部记录。 存在用户签署后又撤销的情况，此时需删除记录。
3	签署文件时间	记录对应文件的签署，如果有多份，需全部记录。

备注：游客帐号为特殊处理，游客帐号签署记录仅跟随开机周期，重启后清空。

4.签约状态告知其他应用App

由帐号提供bridgeSDK给其它APP，告知当前帐号的签约情况：

序号	内容	说明
1	百度ID	当前登录的百度帐号ID，未登录为游客。
2	已签署的文件详情（文件类型、版本号）	记录对应帐号签署过的文件类型、版本号、发布时间、文件所属。如果有多份文件，需全部记录。

			如果未签约则为空。
4	3	签署文件时间	记录对应文件的签署时间，如果有多份，需全部记录。
5	4	最新的文件详情（文件类型、版本号）	如果最新的文件版本号与已签署的文件版本号不同，说明该ID未同意最新的协议。 如果有最新的文件，但无已签署的文件，说明该ID未签署过该文件。

可以采用接口回调或广播方式（由RD决定），但务必保证接入SDK的其他模块能够在客户签约状态改变时实时获得最新的签约状态。

5.客户端页面触发机制

客户端签约页面其触发机制包括以下4种：

- **车机启动后触发**

1）场景1描述：车机启动，宿主App 应用自启动后，若帐号已登录需判断该用户未签约或签约协议更新时由帐号调起签约弹框；

2）场景2描述：车机启动，宿主App 应用自启动后，若百度帐号未登录则为游客，游客模式不弹出签约弹框；

- **进入百度系应用时触发**

签约页面还可以被百度其它应用拉起，需开放接口给其它应用调用。百度各应用接入签约的产品管控策略属于各业务APP的逻辑，具体参照各业务APP产品定义。从整体上方案上建议进入百度系应用时，细分强依赖百度帐号登录和不强依赖帐号登录进行产品定义：

1）若该应用app强依赖百度帐号登录，应用app未登录时，先调起百度帐号登录，登录后由帐号APK查询该帐号是否签约或协议版本更新，调起签约弹框（未签约或签约协议更新时）；若该应app已登录百度帐号，则由各应用APP查询签约状态，未签约或协议版本更新时，由应用APP由调起签约弹框。

2）若该应用app不强依赖百度帐号登录，各应用APP内触发调起签约弹框。百度地图不强依赖百度账号登录。

用户进入APP，需要判断是否签约，用户签约了才能进入地图

1. APP 获得已签约的状态，可以正常进入APP

2. 签约过，百度账号登陆变更，APP判断签约状态，客户端获取状态再次拉起签约页面；用户重新签约后，正常使用
3. 签约过，用户取消或变更签约状态，用户再次进入APP后重新拉起签约
4. 点击【撤销协议】，弹窗二次提醒用户进行确认，若二次确认撤销，地图服务不可用，提示用户并退出应用

- **客户端百度帐号状态更新后触发；**

由于百度协议文件需要关联百度帐号，在非开机引导页面需要监听百度客户端帐号变化，如果有帐号变化，需要按以下表格所罗列的情况拉起协议签署页面（该页面不含福特的协议文件）。

情况列举	百度帐号登录情况	判断条件	协议签署页
1	百度帐号登录	对比存储的待签署文件和该帐号的已签署文件，任意待签署文件版本号比已签署文件版本号更新	弹出
2	百度帐号登录	对比存储的待签署文件和该帐号的已签署文件，所有待签署文件版本号与已签署文件版本号一致或更旧	不弹出
3	百度帐号登出	NA	不弹出

- **用户主动查看已签署协议**

在系统设置页面预留“查看百度协议页面”入口，用户点击此入口触发进入“查看已签署协议”页面。

6.默认待签署文件

为了防止弱网极端环境下，第一次启动时客户端无待签署文件展示，在项目适配过程中需要存储默认签约文件（预制在项目APP里）。

文件版本：固定为V1.0.1

文件类型、文件名、发布时间、简称、文件内容（html文件）、文件所属可以根据项目适配要求而配置，在SOP前提供。

默认文件及默认参数由PM在发版前提供。

7.通用规则

- 恢复出厂设置后，视为全新车机；
- 更换车机后，视为全新车机；
- 音频策略：按键声音大小、音量、类型、是否静音跟随系统，使用系统统一的音频策略。
- 语音切换：签约模块从产品功能上支持中文。
- 走形规则：跟随系统的走行规则（福特项目不涉及）。

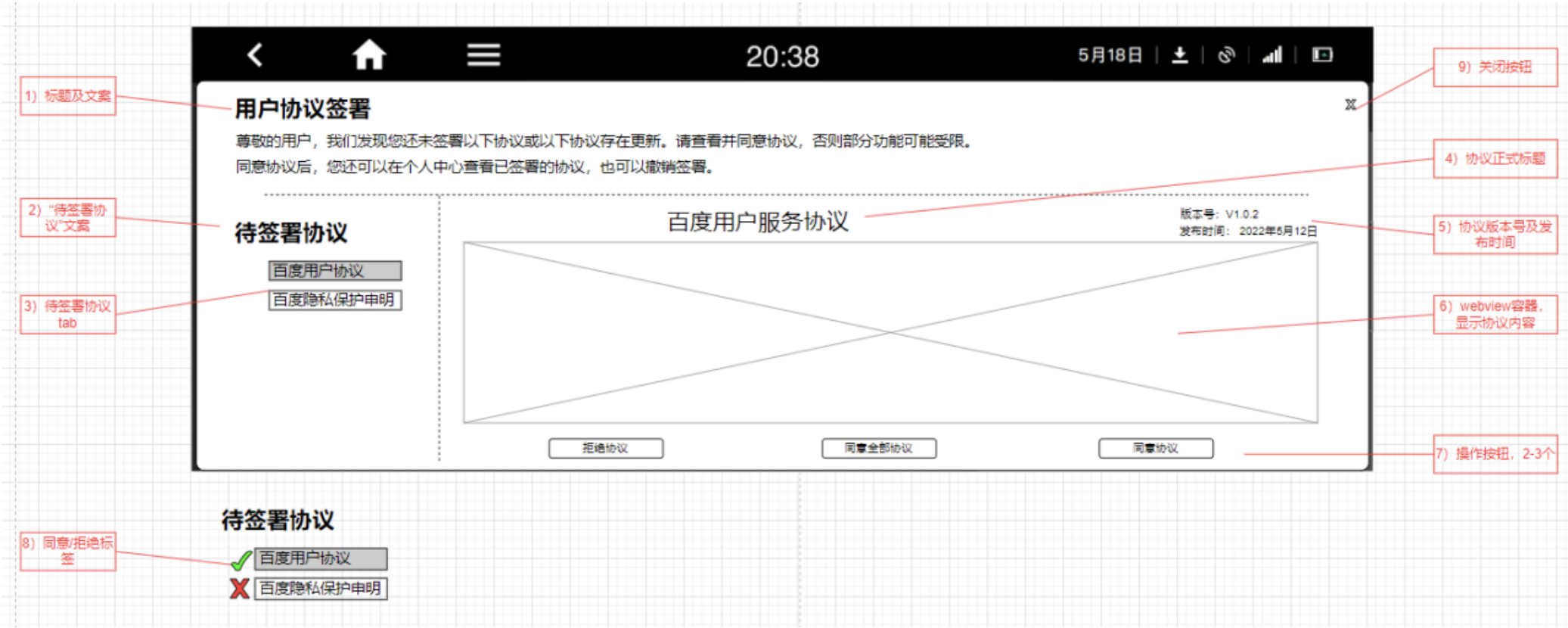
8.客户端用户界面

签约管理客户端用户界面由签约管理宿主APP（帐号APK）实现。

- **用户签约页面**

提供客户端签约页面，该页面可以被第三方应用调用或根据页面触发机制弹出。

参考界面如下，以下界面仅做示意，以UE设计文档为准。：



界面显示元素如下：

序号	元素	说明及要求
1	页面标题及文案	固定文案
2	待签署协议文案	固定文案
3	待签署协议tab	Tab文案来自于参数：文件简称（文案）。 本页面仅显示需要签署协议的Tab，用户已经签署且没有更新的协议不需要显示。 **例1：**新用户显示所有的待签署协议，可引导签署全部协议，如果有2份则显示2份，如果有3份则显示3份。 **例2：**2份文件中有且仅有1份存在更新，且该更新文件未签署，其余文件已经签署，此时仅显示需要更新的文件。

		例3：页面打开前（如上次开机时），用户同意了2份协议中的1份，则只显示未签署的1份协议。 默认排序按照文件类型顺序排序，Tab需要有选中态，默认选中第一个协议，选中时在右侧展示选中协议信息。默认遵循接口返回顺序
4	协议正式标题	来自云端配置参数：文件正式标题（文案）
5	协议版本号及发布时间	来自参数
6	Webview容器及协议内容	使用webview容器显示协议html内容。如果文案过长，还需要显示滑动条。
7	操作按钮	“拒绝协议”按钮：必须显示。点击按钮后，更新待签署协议tab。 “同意协议“按钮：必须显示。点击后该协议变为已签署协议，更新待签署协议tab，如果所有协议都已经签署，则直接关闭页面。 “同意全部协议”按钮：仅在tab大于等于2个时显示。点击后所有协议变为已签署协议并关闭页面。
8	同意/拒绝标签	该标签共3种形态： 同意：表示用户在页面中已经操作同意了协议。 拒绝：表示用户在页面中已经操作拒绝了协议。 无标签：表示用户未进行任何操作。

待签署协议tab的显示和更新逻辑：

待签署协议的tab显示：此页面打开时，对比存储的待签署文件和已签署文件，如果有待签署文件版本号比已签署文件版本号更新时，需将所有符合要求的待签署文件显示。

示例1：如果待签署文件版本号是V1.0.2，已签署文件版本号是V1.0.1，V1.0.2版本需要显示。

示例2：如果待签署文件版本号是V1.0.1，已签署文件版本号是空值（无已签署文件），V1.0.1版本需要显示。

待签署协议的tab：页面打开后，待签署协议的tab不再增加或减少，仅tab的“同意/拒绝”标签变化。

操作逻辑及标签显示：

手动切换tab：用户可以在tab上点击切换不同的tab来查看不同的协议，切换tab后，被切换的tab有选中态，且右侧显示为tab对应的协议内容。

自动切换tab：在未进行任何操作的tab中，用户进行了同意或拒绝操作，则自动切换到下个未操作tab。如果在已经操作过（同意或拒绝）的tab中，用户再次操作，则不自动切换。

同意/拒绝操作：用户可以在页面中选择同意协议或拒绝协议，tab标签将对应的显示签署状态。注意在页面退出前，用户可以反复进行同意或拒绝操作。

页面退出机制：

1、页面自动退出：

1）用户点击“同意全部协议”后，自动退出；

2）用户对所有tab都进行了操作，且所有在tab的协议都已经操作“同意协议”按钮了，则页面自动退出。如果页面内有拒绝的协议，即使进行了全部的操作也不自动退出。

2、页面手动退出：当用户点击“返回”按钮，需弹出二次确认对话框，用户点击继续后再退出，关闭页面且回到该页面打开前的界面

页面层级及覆盖关系

1、签约页面被其它应用拉起时，覆盖在其它应用之上。

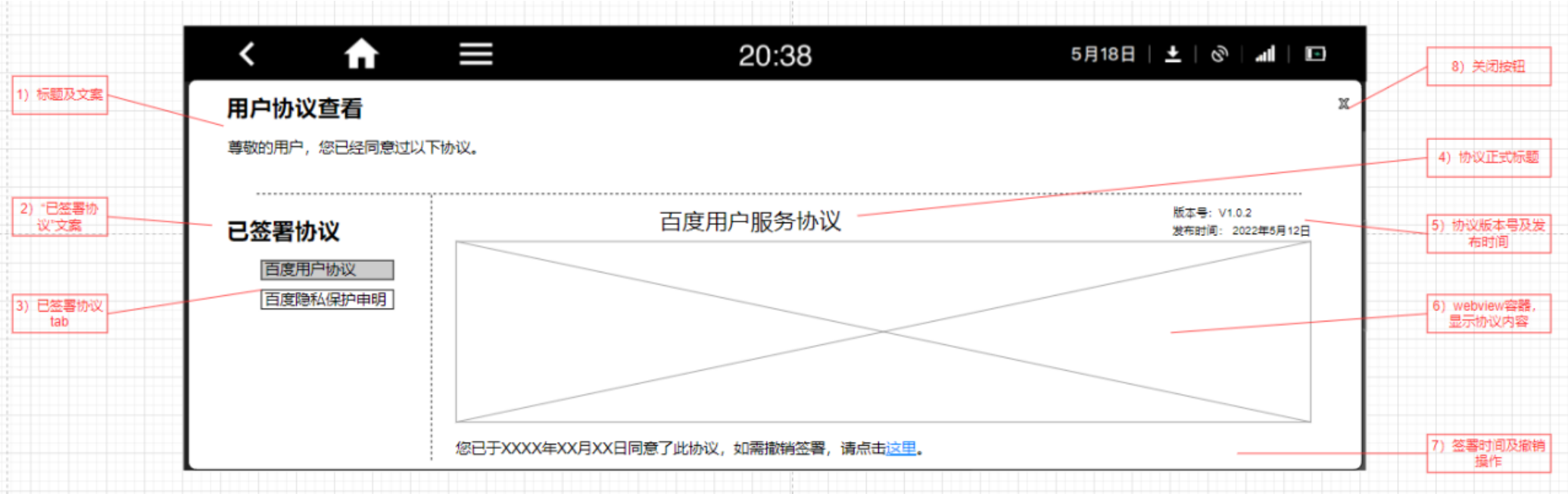
如果出现1）物理按键跳出签约页面（侧边栏/home键等）；2）被系统级应用打断（遵循系统设计）；以上两种情况用户签约会被其他应用打断，等同前台关闭签约页面。

2、当系统级应用运行时，如果用户触发签约弹窗，签约界面将在后台挂起，直到系统级应用关闭再展示给用户，继续签约行为。

- **用户已查看页面**

需提供页面给用户查看最新的已签署的协议（并非最新的协议！），用户可以查看协议标题、内容、签署时间、版本号、发布日期，除此之外，用户还可以在此页面撤销已经同意的协议。以下界面仅做示意，以UE设计文档为准。

- **参考界面如下：**



- 界面显示元素如下：

序号	元素	说明及要求
1	页面标题及文案	固定文案
2	已签署协议文案	固定文案
3	已签署协议tab	Tab文案来自于参数：文件简称（文案）。 仅显示已签署的Tab，未签署的不显示。 Tab需要有选中态，默认排序按照下图
4	协议正式标题	来自参数：文件正式标题（文案）
5	协议版本号及发布时间	来自参数
6	Webview容器及协议内容	使用webview容器显示协议html内容。如果文案过长，还需要显示滑动条。

8	7	签署时间及撤销操作	签署时间根据实际情况显示，格式为：YYYY年XX月XX日。 参考文案：您已于xxxx年xx月xx日同意了此协议，如需撤销签署，请点击“撤销”实际文案参考UE文档定义。

- **已签署协议页面入口定义：**

系统设置模块提供查看已签署协议统一入口；具体参考UE 文档

- **撤销协议定义：**

在查看已签署协议页面，用户可点击”撤销“按钮撤销协议，用户点击撤销后，需弹出二次确认框，

文案参考：如果不同意协议，对应百度系应用的部分或全部功能将受限，是否确定要撤销?

如果用户点击确认后，该协议被撤销签署，并从已签署协议的tab里删除。

其他需求

- **空白页面**

用户撤销协议后，可能出现无任何已签署协议的情况，此时需要显示缺省页面。

- **Webview Loading画面（Webview加载协议内容）**

在用户签约页面和协议查看页面中，第一次打开此页面时，需要加载Html内容，因此在webview容器显示区域需要提供loading画面，提示用户正在加载。

- **全局 Loading画面**

在用户打开页面是，可能需要加载内容，需提供全页面的loading过渡。

3.2.2 敏感信息授权方案

敏感信息授权，要求在对向车外传输连续地理打点、音频等敏感信息时，需要获取用户的单独授权。授权要设置有效期范围，且支持用户选择关闭。由于本项目中涉及多个应用需要进行敏感信息授权，故引入敏感信息授权SDK对敏感信息授权统一管理，各个应用向敏感信息SDK查询和更新敏感信息授权状态。本方案前提是基于百度系应用不依赖车机系统权限统一管理。

3.2.2.1 整体描述

1、敏感信息授权SDK提供的标准服务包含：

（1）授权状态的存储：授权敏感信息内容（包括位置、音频等）、授权的应用（app 包名）、授权有效期、vin、账号

（2）授权状态查询：查询当前vin/账号在某个应用使用中的位置/音频等敏感信息是否在授权有效期内；

（3）敏感信息授权：提供接口，为让用户选择有效期、进行敏感信息授权；

（4）授权信息变更：用户更新有效期、关闭授权时，调整授权期限；

（5）授权信息变更通知：授权信息变更时，发送广播，给各个应用；

2、敏感信息授权整体说明：

（1）敏感信息授权SDK客户端不作为一个单独的APP，无应用中心（APPlist）的入口。对于福特phase4和phase5项目而言，百度帐号可作为（宿主APP）提供授权状态存储、授权状态查、敏感信息授权弹框、授权信息变更通知等后台功能。

（2）在系统设置界面，增加【敏感信息状态查询】的入口，通过此入口可进入【敏感信息状态】设置弹框。此弹框为各应用调用敏感信息授权SDK的公共弹框。

3.2.2.2 敏感信息授权SDK统一管理（百度帐号APK实现）：

1、具体根据3.1.1需求概述中收集福特phase 4 和phase5项目各应用实际业务过程中涉及采集用户个人敏感信息的实际情况梳理福特phase 4和phase5项目敏感信息管控的APP 包括：语音、地图、小程序、场景引擎；

1	项目	语音	地图	小程序	场景引擎
2	福特phase 4、phase5	涉及麦克风硬件授权（系统隐私权限）	涉及系统定位授权	--	先获取地图，地图获取不到再获取系统定位
3		用户音频 用户定位	涉及位置授权 涉及音频授权	涉及用户定位授权	涉及用户定位授权（开机上传定位）

2、用户主动完成授权前，各应用管控敏感信息默认授权状态为“关闭”。具体应用的敏感信息管理方式示例如下：

权限名称	管理方式	可见类型
位置	默认“不允许”或“关闭权限”	展示“权限/权限组”
音频	默认“不允许”或“关闭权限”	展示“权限/权限组”

3、敏感信息授权状态跟随百度账号本地存储

（1）敏感信息授权状态跟随百度账号进行本地保存；切换百度账号后，未授权应用需重新授权；

（2）游客模式下（未登录百度帐号情况下），各应用需授权敏感信息。同意授权后一次点火周期有效。

（3）帐号信息以百度帐号为准，如果用户没有绑定百度帐号，以游客模式进行展示。

4、授权状态跟随百度账号进行绑定，用户场景说明：

（1）帐号1授权了“百度地图”的位置权限，帐号2未进行授权，在账号1切换至账号2的过程中，如果“百度地图”在前台使用时，可能会导致应用退出，重新打开后需重新申请权限；

（2）开机后，后台侧未收到帐号模块发来的帐号通知时，以游客模式进行权限展示。用户打开“百度地图”授权位置权限后，后台侧收到帐号模块发来的帐号信息通知时，可能导致“百度地图”退出，重新打开应用，需重新申请位置权限；

（3）在本次开机过程中，以游客账号登录后，切换至账号1，则游客账号中所有授权的应用权限保存，本次开机期间，重新以游客账号登录时，已经授权的应用无需重新申请权限。

（4）授权有效期

当后台“获取系统时间为系统默认时间（默认出厂时间。如：1990.01.01 00:00），则默认所有应用的权限均在有效期范围内。

在选择应用权限有效期后，用户手动调整系统时间：以后台中记录的到期时间为准。即手动调整时间后，可能会导致隐私权限的有效期缩短或延长。

3.2.2.2 敏感信息授权设置弹框

敏感信息设置弹框为各应用调用的公共弹框，用于展示并管理相关APP的各敏感信息授权状态。系统设置-->常规设置-->百度用户协议-->敏感信息状态查询入口。点击“敏感信息状态查询”入口 ，点击进入敏感信息设置弹框。实际交互可参考UE设计文档。示意图如下：

- **“敏感信息授权”设置弹框**

1、敏感信息授权设置弹框包含【敏感信息】选项 和对应敏感信息所使用的应用选项、及授权到期时间及开关按钮

（1）展示策略：一级列表为应用选项；二级列表为敏感信息选项，展示开关默认为关闭状态。

（2）敏感信息选项排序：选项列表为固定排序。详见UE 文档定义。

（3）敏感信息选项无法多选，每次最多可选中一个选项。应用列表选项无法多选，每次最多可选中一个选项。

2、敏感信息授权设置开关按钮（除游客模式），具体规则如下：

（1）当开关按钮为开启状态时，再次点击则切换为关闭状态。关闭敏感信息授权开关后，需要二次弹框确认提示部分功能受限（具体弹框提示follow A PP的业务逻辑定义），关闭后该应用立即退出系统后台，还是继续使用，帐号APK管控不到各应用，具体由各应用定义。需遵循原则：若应用不授权敏感信息，则该应用不应采集该敏感信息。

在关闭敏感信息授权后，该应用的敏感信息授权有效期记为结束，**下次使用时（具体详见各APP定义触发时机）**，重新弹出“应用敏感信息申请弹窗”，有效期重新计算；

敏感信息授权结束有几种场景，考虑到用户自主选择和非自主选择，从法规和导航安全角度综合考虑，分为几类：

场景	地图表现
用户自主关闭授权	需要告知用户，授权影响地图使用。 a）若是位置授权关闭，则再次打开地图需重新弹窗，确认位置采集。

		b）若是音频授权关闭，则事件上报的语音上传功能受限，使用到该功能时再弹窗采集音频信息。 （具体交互方式及内容见ue）
2 3	用户切换账号，当前账号主体有变化	需要重新弹窗，确认敏感信息采集 （具体交互方式及内容见ue）
4	用户未切换账号，授权信息自动过期	本次使用地图不受影响，下次再重新打开地图应用（杀死地图进程后再次打开地图）时，需要重新弹出“应用敏感信息申请弹窗”，有效期重新计算；

注：车机管家的「定位，麦克风」权限，签约管理的「一般协议，隐私协议」，及敏感信息的「位置，音频」三者的状态是解藕的，开关状态互不影响

（2）当开关按钮为关闭状态时，再次点击弹出“敏感信息采集”对话框。**有效期选项为3个月、6个月、12月，**每次最多可选择一个选项，无默认选项。示意如下，示意图中关于有效期选项仅为示意，实际以UE文档为准：

（3）点击【确定/同意】按钮

点击后，保存当前“有效期”并关闭“敏感信息采集”对话框；该应用的【敏感信息采集】到期时间联动切换并按本次的操作时间计算截止时间，同时将应用的有效期进行本地保存；

点击【取消】按钮，点击后，关闭“敏感信息采集”对话框。

（4）对话框展示规则（此部分仅说明页面展示元素信息，实际以UE设计文档为准）

1）“有效期”选项，展示【3天】【6个月】【12个月】。

2）选项排序：按“3个月->6个月->12个月”由上至下排列。

（5）文案说明：

对话框文案：“xxx应用敏感信息采集” 。其中“xxx”应用名称，示例：语音应用敏感信息采集；

3、点击【返回】按钮，返回上一级页面。

4、授权有效期说明

（1）用户选择权限有效期后，后台根据当前的本地时间进行权限到期时间计算并展示（如果用户手动调整时间后，进行应用权限的有效期选择，以调整后的时间为准）；

（2）权限到期时间为权限授权后的整数天。如：用户在2022.05.30 15:24授权“百度地图”的位置权限，有效期选择“7天”。即车机上电后，检测时间超过2022.06.06 15:24后收回“百度地图”的位置权限；

（3）对应用授权的有效期进行本地保存，保存内容包括但不限于：帐号信息、应用信息、应用授权状态、授权有效期。如：帐号1，百度地图，已授权，2022.05.31 15:24；

（4）每次车机上电，后台在xx启动完成后，获取系统时间并根据最新时间检测所有帐号的应用权限有效期，关闭已过期的应用权限。同时更新在本地保存的授权信息，内容包括但不限于：帐号信息、应用信息、应用授权状态、授权有效期。如：帐号1，百度地图，未授权，2022.05.31 15:25。

（5）用户选择权限授权有效期后，默认不可修改，在授权关闭（包括在【隐私权限】页面内手动关闭和授权到期时自动关闭）后，可重新选择有效期时长；

5、关于【游客帐号】的特殊说明

【游客帐号】各APP采集使用个人信息的情况说明：

地图：在不登录帐号时，会连续上报位置信息，“VIN +位置 ”，其他服务依赖帐号登录；

- **授权状态**

1、音频和地理位置授权状态跟随账号+VIN进行存储，切换新账号后需重新授权；

2、游客模式下的敏感信息授权，仅在本次开机期间授权有效，断电重启后，所有应用的所有相关敏感信息权限需重新授权。

3、当开关按钮为开启状态时，再次点击则切换为关闭状态：关闭敏感信息授权开关后，需要二次弹框确认提示部分功能受限（具体弹框提示follow APP的业务逻辑定义），关闭后该应用立即退出系统后台，还是继续使用，帐号APK管控不到各应用，具体由各应用定义。需遵循原则：该应用不授权敏感信息，则该应用不应采集该敏感信息。

敏感信息授权结束有几种场景，考虑到用户自主选择和非自主选择，从法规和导航安全角度综合考虑，分为几类：

	场景	地图表现
2	用户自主关闭授权	需要告知用户，授权影响地图使用。 a）若是位置授权关闭，则再次打开地图需重新弹窗，确认位置采集。 b）若是音频授权关闭，则事件上报的语音上传功能受限，使用到该功能时再弹窗采集音频信息。 （具体交互方式及内容见ue）
3	用户切换账号，当前账号主体有变化	需要重新弹窗，确认敏感信息采集 （具体交互方式及内容见ue）
4	用户未切换账号，授权信息自动过期	本次使用地图不受影响，下次再重新打开地图应用（杀死地图进程后再次打开地图）时，需要重新弹出“应用敏感信息申请弹窗”，有效期重新计算；

注：车机管家的「定位，麦克风」权限，签约管理的「一般协议，隐私协议」，及敏感信息的「位置，音频」三者的状态是解藕的，开关状态互不影响。

4、游客模式下，当开关按钮为关闭状态时，再次点击则打开”敏感信息采集”弹框。弹框内不显示有效期选项，默认为一次点火周期内有效。关机或断电重启时需重新授权；

5、游客模式下，【敏感信息授权】设置弹框页面内不展示有效期到期时间。

3.2.2.3 敏感信息授权申请弹框

各应用APP 在实际使用过程中，将根据业务触发时机触发调起“敏感信息授权申请”对话框，示意如下，实际以UE设计文档为准。

- **敏感信息授权申请弹框**

1、敏感信息授权申请列表

（1）展示策略：该应用需要使用的敏感信息选项、处理文案、及授权有效期选项。

（2）列表字段：

敏感信息名称：名称包括“音频/位置”，相关应用在同时申请多个敏感信息时，“敏感信息授权”弹框始终按“音频-位置”的顺序由上至下排列；

辅助文案：展示该敏感信息的用途说明；

敏感信息开关勾选框默认不勾选，不允许默认选中；可以展示全选框，默认不勾选。

2、“有效期”选项

（1）基于 法务意见：不能设置“长期有效”选项，最多有效期1年；

定义如下：“有效期”选项（3个月/ 6个月/ 12个月），每次最多可选择一个选项，无默认选项。

3、点击【确定】按钮

（1）点击后，允许应用本次申请的所有敏感信息按“有效期”选项的规则访问相关敏感信息授权，并关闭“该应用敏感信息授权申请弹窗”；

（2）【敏感信息授权弹框】页面相应应用的有效期到期时间联动根据本次的操作结果计算，同时将应用的有效期进行本地保存；

4、点击“取消”按钮，系统不记录本次操作，关闭“敏感信息授权申请弹窗”。

- **文案说明：**

（1）对话框主文案：xxx 应用敏感信息采集，示例：地图应用敏感信息采集。

（2）对话框辅助文案：根据应用使用敏感信息的实际用途进行相关展示。

3.4. 语音指令需求

无

3.5. 车控需求

无

3.6. 激活需求

无

3.7. 账号&支付需求

3.8. 国际化需求

无

3.9. 隐私权限需求

参考3.2章节定义

3.10. 走行规制需求

无

3.11. 主题换肤需求

用户签约属于低频但必要功能，且隐私协议html内容基本上是文字信息，建议从UI设计层面使用中性文字颜色+webview背景应对。

协议正文的文字是可以通过编辑html文档设定，但只能一个颜色。但该颜色可以适配不同的webview容器背景。详细换肤设计以UI文档为准。

3.12. 非功能需求

无

4. 数据埋点需求

无

5. 外部依赖及关联需求

无

6. 合规意见

无

7. 安全意见

无

8. 附件

无