

福特 phase4 车机管家 MRD

审核人	
重要性	高
紧迫性	高
拟制人	牛兵帅
提交日期	2019/12/27
需求变更控制时间点	

修改记录

更新时间	变更内容	变更撰写	变更理由
2019.12.27	新建需求 v1.0	牛兵帅	
<u>2020.1.14</u>	<u>新增 full feature R&R</u> <u>补充新增车型 764</u> <u>更新内存保护，应用沙盒权责描述</u> <u>Selinux 变更权责分配</u>	<u>牛兵帅</u>	<u>基于福特 review</u> <u>更新</u>

注：提交评审之前的修改也可以记录下来

目录

目录

目录	3
一、 产品背景	4
1. 需求概述	4
2. 项目目标	155
二、 需求概览	166
1. Feature List	166
2. 页面描述	187
3. 威胁分类	188
三、 Story 详述	198
1. Story: 车机管家-S1 入口	198
2. Story: 车机管家-S2 主页	199
3. Story: 车机管家-S4 一键优化	209
4. Story: 车机管家-S4 隐私	2343
5. Story: 车机管家-S5 安全功能模块/服务说明	3323

一、产品背景

1. 需求概述

1) 背景介绍：

随着汽车智能化、网联化和电动化程度的不断提高，智能网联汽车信息安全问题日益严峻，信息篡改、病毒入侵等手段已成功被黑客应用于汽车攻击中，特别是近年来不断频发的汽车信息安全召回事件更是引发行业的高度关注。智能网联汽车的信息安全危机不仅能够造成个人隐私、企业经济损失，还能造成车毁人亡的严重后果，甚至上升成为国家公共安全问题。2017 年 6 月 1 日正式实行的《中华人民共和国网络安全法》要求智能网联汽车制造厂商、车联网运营商“采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。”为有效保障车机系统的网络安全，百度研发了车机系统的安全应用——车机管家。

2) 产品功能介绍：

本产品定位为车机 IVI 安全产品，可以兼容主流硬件平台及安卓操作系统。通过提供 APP 加固，应用双向认证，数据加解密等基础功能，保障小度车载 OS 的安全性；同时提供了用户车内隐私的保护，支持用户关闭应用对定位服务、麦克风、摄像头、日历、通讯录、短信、电话、存储的访问权限；产品也提供了系统一键优化功能，通过用户触发，完成车机系统的扫描，系统垃圾的清理，提升系统的流畅体验。

3) 本文档的涵盖范围：

本文档覆盖福特 phase4 项目相关的安全需求。整体需求及需求分工如下表：

FORD SYNC+ ICA2/phase4 SECURITY R/R						
N O	Item	Category	Description	Phase4 R/R Split		
				B ai d	D es a	F o r

				u	y	d		
1	PKI	密钥	密钥的生成, 管理	—	•	—	<u>Desay Deliver:</u> <u>MCU secure boot Key (RSA)</u> <u>APK sign key</u> <u>SOC 与 MCU 通讯加密</u> <u>AES256 KEY</u> <u>SOC 与 MCU 认证 KEY</u> <u>(CMAC, 德赛提供详细方案)</u> <u>日志加密 AES256 Key</u>	—
2		证书	证书的生成, 管理	•	—	•	<u>Desay Deliver:</u> <u>SOC Secure boot (kernel) 签名的公私钥证书</u> <u>Baidu Deliver:</u> <u>OTA 双向认证公私钥证书</u> <u>(一机一密)</u> <u>车端验证云端服务的公私钥证书</u> <u>Ford Deliver:</u> <u>OTA, MCU, SOC Bootloader 签名的公私钥证书</u>	—
3	安全执行环境	TEE	密钥/证书安全存储	•	•	—	<u>Baidu : 负责开发 TEE 中的 TA 及 CA</u> <u>Desay : 提供稳定 TEE 环境</u> <u>(11/26 Ready 4 台机器)</u> <u>Desay : 负责生产线 KEY/</u>	—

							<u>证书的导入 (包含 Baidu 一机一密公私钥证书等多个密钥及证书)</u> <u>Desay: 20200401 B1 生产时, 进行产线 Key/证书的导入验证</u> <u>Desay : 提供一个独立的分区(16M) 用于 TEE</u> <u>Baidu : 提供需要导入 TEE 的清单 ----11/1</u>	
<u>4</u>	<u>安全启动</u>	<u>Secure boot</u>	<u>bootloader, spl,uuu</u>	—	⊙	—	<u>Desay 提供安全启动方案</u>	—
<u>5</u>	<u>加解密库</u>	<u>加解密 SDK</u>	<u>数据安全</u>	⊙	⊙	—	<u>Baidu Baidu 相关内容采用 Baidu SDK 进行加解密</u> <u>Desay : 日志采用 AES256 加密, 蓝牙通讯录 (EMMC 加密分区), Wifi 密码采用 AES256 加密</u>	—

6	<u>强制访问控制</u>	<u>SELinux</u>	<u>资源访问控制</u>	①	②	—	<u>Selinux 由 Desay 配置</u> <u>Desay 提供：宽容模式</u> <u>2020/02/E</u> <u>①百度回归所有业务，日志落盘（AVC，警告）</u> <u>②德赛提炼 Selinux 策略</u> <u>③德赛配置测试</u> <u>（根据实际情况进行 2-3 轮）</u> <u>Desay 提供开启强制模式</u> <u>（时间待确定）</u>	<u>Desasy 技术确认</u> <u>无法实现。根据</u> <u>一期，二期项目</u> <u>实施经验，</u> <u>现要求：</u> <u>百度负责实施其</u> <u>相关所有 APP 的</u> <u>SELinux 安全策</u> <u>略及配置。</u> <u>Desasy 负责实施</u> <u>其相关所有 APP</u> <u>的 SELinux 安全</u> <u>策略及配置。</u>
7	<u>Root 权限</u>	<u>Root 检测</u>	<u>判断是否</u> <u>为 Release</u> <u>版本，</u> <u>系统是否</u> <u>可以被调</u> <u>试。</u> <u>ADB 是否</u> <u>有 ROOT</u> <u>权限</u>	—	②	—	<u>Desay 实施</u>	<u>通过扫描是否有</u> <u>su,ADB，通用</u> <u>root 工具，系统是</u> <u>否由越狱工具实</u> <u>现</u>

8	应用安全	沙盒应用	APP Sandbox	+	+	-	Baidu & Desay 均可支持	限制应用之间的访问调用，最小化数据泄漏
9		非授权应用安全	禁止安装/运行非授权 APP 并周期扫描，禁止卸载授权 APP	-	+	-	Desay 实施 禁止安装/运行非授权 APP 周期扫描，禁止卸载授权 APP 再确认 ----11/1	检测到异常行为进行阻断，卸载
10		应用通讯安全	通讯加密 & 双向认证	+	-	-	Baidu 实施	-
11		应用混淆加固	对 APK 进行混淆及加固	+	+	-	Desay APK 全部做混淆，对关键 APK 做加固，Desay 提供 LIST Baidu APK 全部做混淆及加固，Baidu 提供 List (Baidu APK 加固后内存占用的增量为 110M-350M) 需要确认内存资源的消耗情况	谁的 apk，谁负责

12	<u>安全日志</u>	<u>车端安全日志</u>	<u>异常网络访问,非授权 APP 安装、运行、卸载,隐私数据非法访问,OTA 升级包异常等记录</u>	°	°	—	<u>Baidu: 隐私数据非法访问, OTA 升级包异常等记录</u> <u>Desay:提供安全日志加密及导出方案 ---11/中</u>	<u>福特无要求</u>
13		<u>云端安全日志</u>	<u>安全传输及存储</u>	°	—	—	<u>Baidu 实施</u>	—
14	<u>日志(非安全)</u>	<u>U 盘日志导出加密</u>	—	—	°	—	<u>Desay 负责,采用 AES256 加密</u> <u>车机端密钥保存方案,日志解密工具 Desay 提供</u> <u>开发阶段日志上传云端的需求(用于开发过程中问题点调查)</u> <u>Desay 业务明确需求并评估日志上传量大小 --10/31</u>	<u>离线 Log, logcat 包含 kernel panic 的加密</u>
15	<u>隐私管理</u>	<u>麦克风</u>	—	°	—	—	<u>Baidu 实施: 所有应用到麦克风的,增加是否授权</u>	—

						使用的 UI 选项	
16		定位服务	—	—	—	Baidu 实施	定位信息：酒店， 电影购票，外卖， 智慧停车场，保 养，在 UI 界面 里可设置
17	安 卓 原 生 内 容	禁用 OEM unlock	—	—	—	Desay 实施	对应 Pen Test 问 题点
18	的修改	去除系统 一些工具 及应用	—	—	—	Desay 实施	su, gdb 等
19	本 地 安 全 通 道	本地认证	SOC 与 MCU 之间 的认证	—	—	Desay 实施，基于 CMAC	—
20		本地加密 通讯	SOC 与 MCU 的通 讯加密	—	—	Desay 实施 加密范围德赛 再确认，通讯方式 SPI	基于一机一密的 AES 256 通讯加 密，
21	安 全 调 试	硬件调试 端口的禁 用	JTAGUAR T	—	—	Desay 实施	—
22	移 除 不 需 要 的	USB port	只识别 U 盘，其余去	—	—	Desay 实施	—

	驱动		除					
23	uboot	uboot	fastboot 的 禁用	—	⊙	—	Desay 实施	—
24	升级	SOC 升级 包制作	—	—	⊙	—	SOC 升级包 Desay 负责	—
25		SOC OTA 升 级 包 Ford 签名	—	—	—	⊙	Ford 实施	—
26		SOC OTA 升 级 包 Baidu 签 名+加密	—	⊙	—	—	Baidu 实施	—
27		SOC OTA 云端安全 及传输安 全	—	⊙	—	—	Baidu 实施	—
28		SOC USB 本地升级 安全	token 方 式，每个 SOC 包只 能在对应 的机器上 升级。	⊙	—	—	Baidu 实施	—
29		MCU 升级	bin , vbu	—	⊙	—	Desay 实施	—

		包制作						
30		MCU 升级包签名	bin , vbu	—	—	⊙	Ford 实施	—
31		MCU 本地 upgrade	安全升级	—	⊙	—	Desay 实施	FNOS class CCC (RSA) 实施 及 0x27 安全解锁服务
32		MCU OTA 云端及传输安全	—	—	⊙	—	MCU 与 SOC 做成一个大包，上传后 Baidu 进行签名加密，推到车机后 SOC 进行解密验签 差分更新与全量更新安全方案无差异	车机端由 Desasy 实施 OAT 云端需要业务确认，TBD。 SOC 和 MCU 之间的交互由 Desasy 负责。
33	Bluetooth 安全	—	—	—	⊙	—	Desay 实施	—
34	Wifi 安全	—	—	—	⊙	—	Desay 实施	—
35	RFQ/Privacy Questionnaire/Spec	—	—	—	—	⊙	Ford 主导 Baidu/Desay 配合	—
36	Threat modeling	—	—	—	—	⊙	—	—

37	<u>安全编码</u>	<u>静态代码检查</u>	<u>确保软件遵守安全编码规则</u>	☉	☉	—	<u>Desay Cover(tool: Coverity)</u>	<u>百度、Desay 各自负责自己部分的安全编码检查。</u>
38	<u>Fuzzing test</u>	<u>Bluetooth</u>	—	—	☉	—	<u>Desay 实施</u>	—
39		<u>Wifi</u>	—	—	☉	—	<u>Desay 实施</u>	—
40	<u>Penetration test</u>	—	—	☉	☉	☉	<u>Desay:提供 PEN TEST 报告 (Baidu APP 剔除, 第三方 Pen test 供应商告知 Ford)</u> <u>Baidu 提供 PEN TEST 报告 (范围内)</u>	—
41	<u>热修复</u>	<u>修复操作系统漏洞</u>	—	—	—	—	<u>针对谷歌发布的及已知的 CVE (Kernel,framework), 开发补丁, 在 OTA 版本前, 对 OS 及时进行修复。</u> <u>Desay 无法实施, Baidu 无法支持</u> <u>【非 FORD 强制要求】</u>	<u>非福特需求。</u>
42	<u>开源库 CVE</u>	<u>开源库 (APP 用到的第三方 SDK)</u>	—	☉	☉	—	<u>Baidu 部分 APK Baidu 可实施</u> <u>Desay 负责 APP,需要再确认 11/中回复评估结果</u>	<u>对开源漏洞库中 CVSS≥7 的 CVE 进行修复</u>

		漏洞修复						
43	安全监控及防护	联网防护, 防火墙	—	—	②	—	Desay 实施, 百度提供白名单的详细列表	对不在网络访问策略规则里的网络连接, 进行阻断并记录
44	流量统计	—	TBD, 业务端需求占不明确	—	—	—	Baidu 实施	统计每个应用所消耗的流量 (用户付费)
45	系统优化	对系统进行监控, 优化	—	—	②	—	BAIDU 实施, 与隐私服务同 1 个 APP, 可监控每个 APP 和整个系统。	监控 CPU、内存、磁盘空间的占用情况, 如果超过比例, 根据算法建模, 进行一些策略的处理
46	MCU CAN 通讯白名单	—	—	—	②	—	Desay 提供白名单的详细列表	—
47	SOC CVE 修复	Kernel	—	—	②	—	Desay 对应	—
48	非 root 操作	—	—	—	②	—	Desay 对应, 提供 LIST	检测应用是否不需 root 权限, 越权

								使用 root 权限
49	内存保护	—	—	—	②	—	Desay 对应, Baidu 负责的 APK 在编译时,需要配置内存保护相关配置项	内存 protection 开启,内存地址随机化,防溢出

4) 说明

Phase4 的安全需求是在 phase1、phase2 基础上做了裁剪,更轻量化,同时融合了产品的最新能力——一键优化。相关差异部分的具体内容在文档中使用**黑色粗体**进行标识。以下内容为用户可感知的差异部分整体的概览:

- a) 产品名称:车机助手——> 车机管家
- b) 功能名称:隐身模式——>无痕模式
- c) 隐私模块:隐私管控权限
 - i. 由 2 项变为 8 项
 - ii. 由默认授权改为默认不授权
 - iii. 由管控若干百度 APP 改为管控所有百度 APP
- d) 去掉防火墙模块
- e) 新增【一键优化】功能模块

2. 项目目标

- 1) 作为安全模块,整体融合到小度车载 OS 里,搭载到福特 phase4 项目中。交付内容包括 APK ,sdk , bin 文件等,并提供友好的用户交互界面。
- 2) 软硬件环境:
 - a) 硬件平台:高通 S820A

- b) U-boot 版本：没有用，用的是 lk
- c) Linux Kernel 版本：4.4.138
- d) 安卓操作系统版本：8.1
- e) 车型及车机屏幕：

Program	Vehicle	Screen
CD542Ambient/Trend	Ford New Mondeo 改款高配	27" Extra Landscape (756*4032, 10:53)
CD542Titanium/ST Line	Ford New Mondeo 改款低配	13.2" Landscape (1080*2348, 10:21.7)
CX727	Ford Mustang	15.5" Portrait (1920*1200, 16:10)
U725	Ford Bronco SUV	12" Landscape (1200*1920, 10:16)
P702	Ford Raptor F-150(Pick up truck)	12" Landscape (1200*1920, 10:16)
U554	Lincoln Navigator Large SUV(3 row seats)	13.2" Landscape (1080*2348, 10:21.7)
U625ICA	Ford Explorer	27" Extra Landscape (756*4032, 10:53)
764		

- 3) 记录车机管家模块内各页面跳入跳出路径、时间数据，用于分析、改进产品。
- 4) 安全日志采集并上传到百度的服务器，用于分析、改进产品。

二、需求概览

1. Feature List

C 端用户可见部分

功能划分	功能描述	备注
车机监控防护显示 (launcher 卡片页)	纯色的防护图标，文案： “已安全守护 X 天” 以及 “>” 可点击引导箭头。点击图标或文案区域，跳转到车机管家主页	更多规则请参考 launcher 页 MRD

车机防护 (车机管家主页)	车机防护动图	防护动效
	车机防护项	显示各防护项, 包括:- 防火墙 APP 对外通信加密及双认证 数据防护
防火墙	流量统计	统计各应用的数据流量, WLAN 流量使用情况。维度:-本月, 上月, 按照使用量排序
	联网防护记录	逐条显示联网防护的内容及处理结果 将防护记录加入白名单功能
隐私	隐私内容列表	包括定位服务、麦克风 日历, 相机, 通讯录, 电话, 存储, 短信 (此 6 项为在 phase1&2 基础上新增)
	无痕模式	一键关闭所有应用对上述隐私内容的访问权限
	逐项隐私权限设置	逐个管理每个应用对上述隐私内容的访问权限
一键优化 (车机管家主页)	系统扫描&清理	点击后执行系统扫描&清理, 并显示相应动画

C 端用户不可见部分

功能/服务模块	描述
系统补丁	采用百度业界首创的热修复方案
操作系统配置安全	当前系统是否为 release 版 ADB 是否具有 Root 权限 系统是否可以被调试 符合福特提供的安全标准, 具体实现方案参考相关设计文档。
非 root 操作	防止应用程序拥有 root 权限 检测系统是否有 root 工具
内存保护	开启内存保护机制
内存保护	德赛对应, Baidu 负责的 APK 在编译时, 需要配置内存保护相关配置项
修复 CVE	根据确认的邮件分工, 对百度用到的 open source software 中的已知 CVE 进行修复
代码混淆	采用百度加固方案
非授权应用安全	防止安装、运行非授权、被篡改的应用软件 保护授权应用不被非法卸载, 篡改
应用沙盒	开启应用沙盒
应用沙盒	默认开启 sandbox. 百度做百度的。Desasy 做 Desasy 的。
SELinux	开启 SELinux, 百度负责实施其相关所有 APP 的 SELinux 安全策略及配置 德赛负责德赛相关的; 百度负责百度相关的
隐私	对麦克风、GPS、 日历, 相机, 通讯录, 电话, 联系人, 短信 数据的非法访问进行监控
PKI	百度提供 PKI OTA 双向认证公私钥证书 (一机一密) 车端验证云端服务的公私钥证书

带格式的: 非删除线

带格式的: 非删除线

带格式的: 删除线

TEE 数据安全	数据安全防护 SDK 密钥、证书安全存储 SDK 负责开发 TEE 中的 TA 及 CA
安全 OTA	云端安全包制作及车端安全包校验 SOC OTA 升级包 Baidu 签名+加密 SOC OTA 云端安全及传输安全 SOC USB 本地升级安全(token 方式，每个 SOC 包只能在对应的机器上升级)
通信安全	关键业务实现通信双向认证，并使用 TLS1.2 通信协议
车端安全日志	包括异常网络链接、非授权 App 事件、root 检测，隐私数据非法访问及 OTA 升级异常
云端安全日志	车端安全日志上传到云端，并进行安全存储 云端安全日志传输到车厂

2. 页面描述

页面编号	页面划分	说明	备注
0	APP 入口	Launcher 车辆卡片页下方文案	
		更多 APP→车机管家	
1	APP 主页	一键优化；隐私模块功能入口	
2	防火墙	包括流量统计及联网防护记录	
3	隐私	无痕模式 各应用对定位服务、麦克风，日历，相机，通讯 录，电话，存储，短信的访问控制	

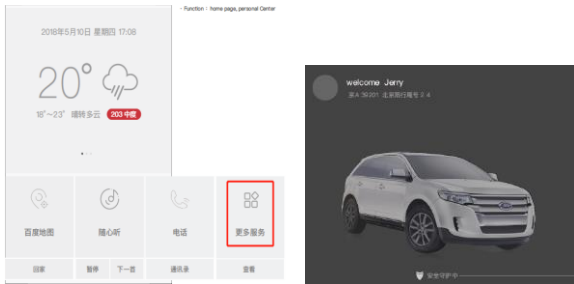
3. 威胁分类

SN	威胁类型	描述	威胁等级	处理结果
1	APP 应用安全	非授权应用安装、执行 授权 APP 的卸载	中	需要记录相关日志。
2	OTA 升级安全	车机端篡改包的安装	中	阻止篡改包的安装，并记录相关日志

3	异常网络访问	不在 IP,APP 网络访问策略规则里的网络连接	中	阻止、断开连接，并记录相关日志
4	隐私访问	对用户 GPS 及麦克风的访问记录	低	记录相关的异常访问日志

三、 Story 详述

1. Story: 车机管家-S1 入口



通过点击车机首页的更多服务，或 launcher 车辆状态卡片页中防护图标或文案，或通过语音的交互”查看/打开/进入**车机管家**页面”或“查看/了解**车机管家**”，进入车机管家主页面；

通过点击“系统设置”中“隐私设置”，或通过语音“查看/进行隐私设置”进入隐私主页；“查看流量情况”进入防火墙主页；

在 launcher 页，通过语音“进行一键优化”直接在后台执行系统扫描&清理动作，不进入对应的页面；完成后由 launcher 显示清理结果。

2. Story: 车机管家-S2 主页

车机管家主页包括一键优化和隐私模块功能入口两部分，界面示意图如下：



3. Story: 车机管家-S4 一键优化

3.1 功能描述

该功能包括系统监控及系统清理。

3.1.1 系统监控

实时监控（“实时”定义：进程启动后 30s 开始执行，每隔 15S 进行一次系统资源数据的采集）以下

内容，并且监控项支持 OTA 更新：

- CPU 占用百分比
- 内存占用百分比
- 磁盘空间占用百分比，包含 data 分区，map 分区，update 分区
- 页面帧率

当监控到以下事件时，将监控信息及对应事件进行落盘：

- 【资源消耗峰值预警】以下任一项达到，即满足预警条件：
 - a) CPU 占用百分比: 全核超过 80%
 - b) 内存占用百分比：超过 80%
 - c) 磁盘空间占用百分比：超过 90%
- 【页面卡顿】连续检测 3 次，即 45S，若最后一次仍卡顿，则判断为卡顿。卡顿定义：
 - ◆ 大卡顿：绘制一帧的数据大于 70ms

◆ 小卡顿，在 1s 时间，绘制 ≤ 40 帧

- 【手动清理】清理前，清理后

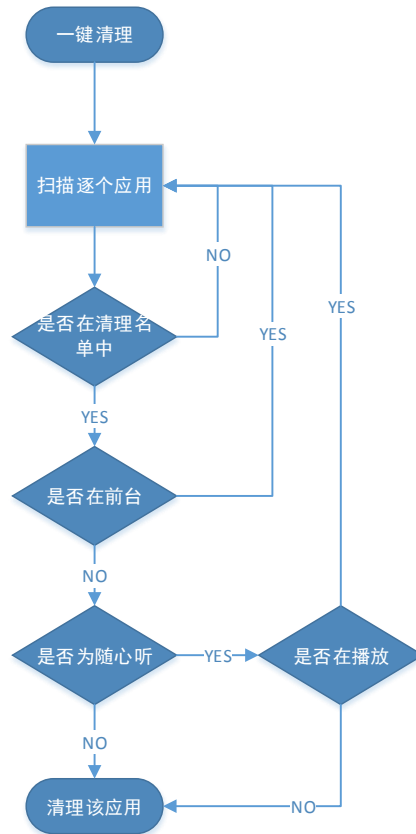
落盘内容如下：

内容	分类	子项	描述/备注
监控项	CPU 占用百分比		小数点后 1 位，格式举例：80.0%
	内存占用百分比		小数点后 1 位，格式举例：80.0%
	磁盘空间占用百分比		小数点后 1 位，格式举例：80.0%
	页面帧率		Frame Per Second
日期时间			格式举例 2019 年 6 月 28 日 11:42:22
驱动事件	资源消耗峰值预警	CPU 占用预警	
		内存占用预警	
		磁盘占用预警	
	页面卡顿	大卡顿	
		小卡顿	
	手动清理	清理前	
		清理后	

3.1.2 系统清理

该功能包括内存清理及磁盘清理。

- 内存清理
 - 清理名单：只清理百度负责的、有界面的应用，其中去除地图，launcher，语音。
 - 清理流程如下：



- 磁盘清理

- 清理原则：只清理百度负责的应用的缓存

3.2 功能触发

用户可以通过语音或点击触发此功能。

- 在 launcher 页触发此功能后,在后台完成系统的扫描及垃圾清理工作,完成后,清理结果由 launcher 显示。

- 在当前页面触发此功能后，前端即播放清理优化的动画及整体进度，同时后台进行系统的扫描及垃圾清理工作，完成后，提示文案“已清理内存：XXM，垃圾：XXM”。单位为 GB 时，XX 取整数；单位为 MB 或 KB 时，XX 保留小数点后两位。清理结束后的线框图如下：



- 特殊场景考虑：
 - 若清理过程中用户退出当前页面，仍在后台完成清理，结束后不在前端进行提示
 - 当清理结果为 0 时，显示文案为：状态已达最佳
 - 当从当前页面退出再次进入一键优化页面时，如果上次清理结果没有结束，显示上次清理百分比进度；如果上次清理已完成，不显示清理结果，显示一键优化初始状态

4. Story: 车机管家-S4 隐私

隐私模块是查看和管理各应用对用户车内隐私的使用权限的统一入口。基于安卓系统权限定义，并结合车载场景，对定位服务，车内麦克风，**日历，相机，磁盘存储，电话，联系人，短信进行整体动态管理。即，如果没有应用使用上述权限，此权限不在管控范围。**所有隐私项，在 launcher 页或车机管家主页均可通过语音进行开关控制，如“开启/关闭 GPS（定位服务）”，“开启/关闭麦克风”，“**开启/关闭车内相机**”，“**允许/禁止使用磁盘存储**”，“**允许/禁止使用电话**”，“**允许/禁止访问联系人**”，“**允许/禁止访问短信**”，“**允许/禁止访问日历**”等；完成相关控制后，进行对应的语音播报，如“已开启/关闭 GPS 访问权限”，“已开启/关闭麦克风访问权限”，“**已开启/关闭相机访问权限**”，“**已开启/关闭磁盘存储访问权限**”，“**已开启/关闭电话访问权限**”，“**已开启/关闭联系人访问权限**”，“**已开启/关闭短信访问权限**”，“**已开启/关闭日历访问权限**”。隐私页面示例如下



页面元素说明

元素	说明	备注
返回	点击跳转到车机管家模块主页	
隐私	当前页面名称	
无痕模式	默认关闭。用户一键开启后，则关闭所有隐私设备和信息的应用访问权限；用户一键关闭，则恢复原来的权限访问设置。	
文案描述	开关开启的时候，文案：已禁用以下隐私设备和信息的应用访问权限 开关关闭的时候，文案：已开启以下隐私设备和信息的应用访问权限	
隐私列表	隐私内容名称，开关状态，可点击引导图标“>”	点击后进入各隐私项的单独设置页面。见 4.1~4.8

4.1 定位服务

查看和管理各应用对定位服务的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对定位服务的访问。一键打开时，恢复原来的权限访问设置。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
定位服务	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对定位服务的访问权限 开关关闭的时候，文案：已关闭以下应用对定位服务的访问权限	
“定位服务”， “  ”图标	定位服务一键开关。状态为“关闭”时，列表内所有应用无法使用定位服务。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关闭”状态
应用列表	应用图标，应用名称，“  ”图标， 所有申请了“定位服务”访问权限的应用	

4.2 麦克风

查看和管理各应用对麦克风设备的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对麦克风设备的访问。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
麦克风	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对麦克风的访问权限 开关关闭的时候，文案：已关闭以下应用对麦克风的访问权限	
“ 麦 克 风 ” ，  图标	麦克风一键开关。状态为“关闭”时，列表内所有应用无法使用麦克风。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关闭”状态
应用列表	应用图标，应用名称，  图标， 所有申请了“麦克风”访问权限的应用	

4.3 磁盘存储

查看和管理各应用对磁盘存储的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对磁盘存储的访问。一键打开时，恢复原来的权限访问设置。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
磁盘存储	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对磁盘存储的访问权限 开关关闭的时候，文案：已关闭以下应用对磁盘存储的访问权限	
“磁盘存储”， “  ”图标	磁盘存储一键开关。状态为“关闭”时，列表内所有应用无法使用磁盘存储。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关闭”状态
应用列表	应用图标，应用名称，“  ”图标， 所有申请了“磁盘存储”访问权限的应用	

4.4 摄像头

查看和管理各应用对摄像头的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对摄像头的访问。一键打开时，恢复原来的权限访问设置。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
摄像头	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对摄像头的访问权限 开关关闭的时候，文案：已关闭以下应用对摄像头的访问权限	
“摄像头”，“  ”图标	摄像头一键开关。状态为“关闭”时，列表内所有应用无法使用摄像头。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关闭”状态
应用列表	应用图标，应用名称，“  ”图标，	

	所有申请了“摄像头”访问权限的应用	
--	-------------------	--


4.5 电话

查看和管理各应用对电话的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对电话的访问。一键打开时，恢复原来的权限访问设置。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
电话	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对电话的访问权限 开关关闭的时候，文案：已关闭以下应用对电话的访问权限	
“电话”，“  ”图标	电话一键开关。状态为“关闭”时，列表内所有应用无法使用电话。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关闭”状态


应用列表	应用图标，应用名称，“  ”图标， 所有申请了“电话”访问权限的应用	
------	--	--


4.6 日历

查看和管理各应用对日历的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对日历的访问。一键打开时，恢复原来的权限访问设置。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
日历	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对日历的访问权限 开关关闭的时候，文案：已关闭以下应用对日历的访问权限	
“ 日 历 ” ， “  ”图标	电话一键开关。状态为“关闭”时，列表内所有应用无法使用日历。	当有至少一个应用的开关为“打开”状态时，一键开关为“打开”状态；当所有应用的开关为“关闭”状态时，一键开关为“关


		闭”状态
应用列表	应用图标，应用名称，“  ”图标， 所有申请了“日历”访问权限的应用	


4.7 通讯录

查看和管理各应用对通讯录的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对通讯录的访问。一键打开时，恢复原来的权限访问设置。页面如下



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
通讯录	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对 通讯录的访问权限 开关关闭的时候，文案：已关闭以下应用对 通讯录的访问权限	
“ 通 讯 录 ” ， “  ”图标	电话一键开关。状态为“关闭”时，列表内所 有应用无法使用通讯录。	当有至少一个应用的开关为 “打开”状态时，一键开关为“打 开”状态；当所有应用的开关为

		“关闭”状态时，一键开关为“关闭”状态
应用列表	应用图标，应用名称，“  ”图标，所有申请了“通讯录”访问权限的应用	

4.8 短信

查看和管理各应用对短信的访问权限。可以对每个应用单独进行设置，也支持一键关闭所有应用对短信的访问。一键打开时，恢复原来的权限访问设置。页面如下

短信

已开启以下应用对短信的访问权限

 百度地图

 爱奇艺



短信

已关闭以下应用对短信的访问权限


 百度地图

 爱奇艺



页面元素说明

元素	说明	备注
返回	点击跳转到隐私主页	
短信	当前页面名称	
文案描述	开关开启的时候，文案：已开启以下应用对短信的访问权限 开关关闭的时候，文案：已关闭以下应用对短信的访问权限	
“ 短 信 ” ，  图标	电话一键开关。状态为“关闭”时，列表内所有应用无法使用短信。	当有至少一个应用的开关为“打开”状态时，一键开关为“打

		开”状态 ;当所有应用的开关为 “关闭”状态时，一键开关为“关 闭”状态
应用列表	应用图标，应用名称，“  ”图标， 所有申请了“短信”访问权限的应用	

5. Story: 车机管家-S5 安全功能模块/服务说明

4.1 密钥及证书

支持 ford 密钥标准和密钥注入交换流程，支持 ford 证书。

4.2 安全 OTA

云端安全包制作及车端安全包校验，主要包括如下内容。具体实现方案参考相关设计文档。

云端安全包制作	升级包加密
	升级包签名（支持福特签名）
	身份认证
	升级包防拷贝签名
	身份 Token 生成
	安全升级包制作
车端安全包验证	升级包防重放
	升级包解密
	升级包验证签名
	升级包鉴定来源可信
	升级包防拷贝验证签

	升级包双向身份认证（在线升级）
通讯通道	支持 HTTPS/TLS 协议