1.1 案例六：智能网联汽车商用密码应用和解决方案——车联业务平台安全加固技术方案

1.1.1 方案概述

为了应对 XXX 车型搭载 V2X 功能后在跨企业的车车、车路等车路协同通信场景中由于网络信任体系缺失引发的信息安全问题，需要建立基于 V2X 车路协同通信场景的 V2X 安全证书管理系统，构建统一的车、路、云、端身份认证体系，保障与不同企业的车辆在通信过程中的安全互认。

V2X 安全证书认证管理系统（Security Certificate Management System，简称 SCMS）建设，实现 V2X 通信中的身份认证、安全传输、数据完整性、有效性等安全特性，解决当前车与车、车与路边单元、车与云、车与人通信的安全隐患，为智能网联汽车应用发展建立一个安全的网络运行环境。

1. 方案背景

在二十大报告中，“安全”一词也被多次提及，在经济领域包括要确保粮食、能源资源、重要产业链供应链安全。

车联网安全风险突出、安全威胁严重，安全形势亟待改善，安全防护水平急需提升。主要面临以下几个风险：

（1）通常车路端设备常年暴露在户外、野外等情况，车联网的安全更加容易受到安全威胁，轻则造成汽车失窃、个人隐私数据泄露，重则造成汽车失控，危害人员生命安全。

（2）目前我国 C-V2X 直连通信标准体系已初步形成，制定了一系列适用于 C-V2X 的技术标准，但是在车云、路云场景中仍使用的是传统的 X.509 公钥证书体系来实现 V2N 通信安全，这在已不适应在车

联网高速直连场景的应用需求。

（3）工业互联网信息系统比如车联网服务平台、车联网数据等服务平台大部分部署于云端，还面临着来自云上安全风险的威胁。

（4）方案基于密码技术解决了以上几个车联网应用的痛点，并且在车联网应用上率先通过了密评，是工业互联领域国产密码有效应用的、具有示范性的案例。同时方案还具备以下几个特点：

- 工业互联密码服务模式，快速覆盖全车系
- 工业互联多场景密码应用，车云网一体化安全
- 工业互联建立跨控制器间加密信道，实现车内通信安全
- 工业互联构建统一的多算法多协议的密码服务平台
- 工业互联实现 AUTOSAR 协议国密改造，推动自主可控
- 工业互联发挥密码特性，应用整车数据安全

2. 方案简介

上汽零束 OTA、TSP、数据工厂、SOA 开发者平台等车联业务平台的安全、可靠、稳定的 运行，需满足密码评定三级和等级保护三级的合规性需求。为了深入推进上海市重要领域密码应用，进一步提升重要网络和信息系统的安全防护能力，依据国家密码管理局《信息安全等级保护商用密码管理办法》，上海市密码管理局下 发了《信息安全等级保护商用密码技术应用指南》(以下简称《应用指南》)。《应用指南》提到了，重要网络和信息系统应当采用国产密码进行保护，密码应用系统方案属于安全方案的有机组成部分，选用的商用密码产品应当是国家密码管理局部分准予销售的产品。

为了落实和贯彻国家密码管理局和上海密码管理局等国家有关

部门信息安全工作要求，全面完善信息安全防护体系，提高整体信息安全防护水平。系统建设需要满足《信息系统安全等级保护基本要求》(以下简称《基本要求》)，在《基本要求》中，采用密码技术，多数安全功能(如身份鉴别、访问控制、数据完整性、数据保密性、抗抵赖等)为了获得更高的强度，均要基于密码技术，为了保证信息系统整体安全防护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、数据保密性、抗抵赖等安全功能的实现。对于涉及到身份的真实性、行为的抗抵赖、内容的机密性和完整性的要求项，密码技术都可以直接或间接地提供支持。

3. 方案目标

（1）总体目标

通过部署 V2X 安全证书管理系统，实现：以《基于 LTE 的车联网通信技术安全证书管理系统技术要求》为标准，建立车-路协同互认的 C-V2X 通信加密保护和安全认证体系，配合推动车联网 C-V2X 产业加速落地，构筑下一代安全、高效的智慧出行生活。

（2）功能目标

通过 V2X PKI 信息安全体系的建设，实现对所有参与车-路协同业务实体对象的强身份表达；

保障车机设备与路侧设备信息传递的敏捷性、完整性，并实现车和路侧设备的隐私数据不被泄漏。

（3）技术目标

搭建 V2X-PKI 认证体系，并能根据需要及时颁发注册证书、假名证书、应用证书、身份证书；

能对证书状态进行定期维护和发布；

注册证书、假名证书、应用证书、身份证书生命周期管理；

路侧单元与车载单元通信前基于 V2X 证书执行强身份认证；

在保证路侧单元与车载单元通信数据实时传递的同时，实现传输数据的完整性、机密性和可靠性保护，避免中间人攻击；

在保证路侧单元与车载单元通信数据实时传递的同时，依托假名证书池技术实现传输数据的隐私性保护，避免被非授权设备定向跟踪。

1.1.2 方案实施概况

1. 方案总体架构

上汽集团基于传统 PKI 技术和 V2X PKI 技术建设了工业互联网可信体系，涵盖云管端上的可信标识、身份认证、加解密、安全存储和密钥管理等。

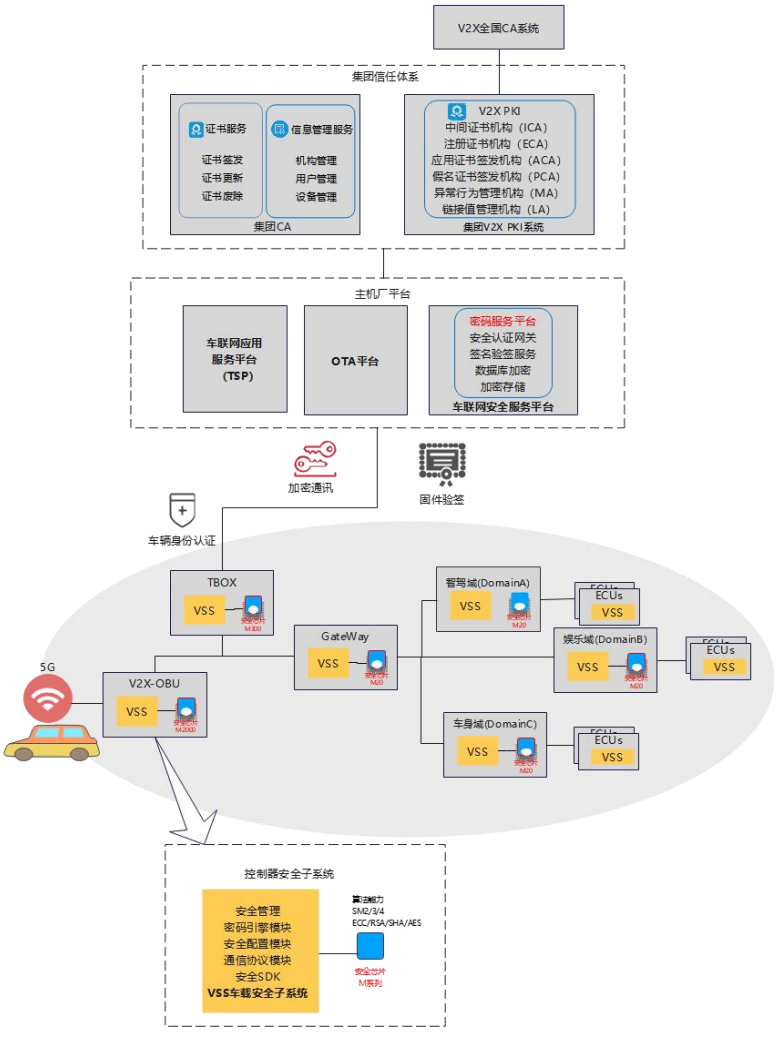


图 6-1 集团密码服务体系

该架构实现了车载端到车云端软硬件一体化的整体解决方案。红色部分为本次建设的密码服务平台和车端安全芯片提供了基础的密码支撑服务。

- 云安全服务平台：基于密码服务平台为车联网应用提供完整的云端系统安全解决方案,全面支撑车联网下的V2N车云认证、FOTA安全、数字钥匙、第三方内容认证等应用安全需求。
- 车载安全子系统（VSS)：基于安全芯片（Mizar M系列）的商用密码计算能力为各类车载控制器（ECU）提供完善的安全子系统功能，支撑车辆控制器的安全管理、软件保护、安全通信SecOC等应用安全需求。

2.技术路线

（1）密码服务平台

密码服务平台逻辑架构由密码资源池、密码机虚拟层、密码服务层、密码服务接口和平台管系统等构成。

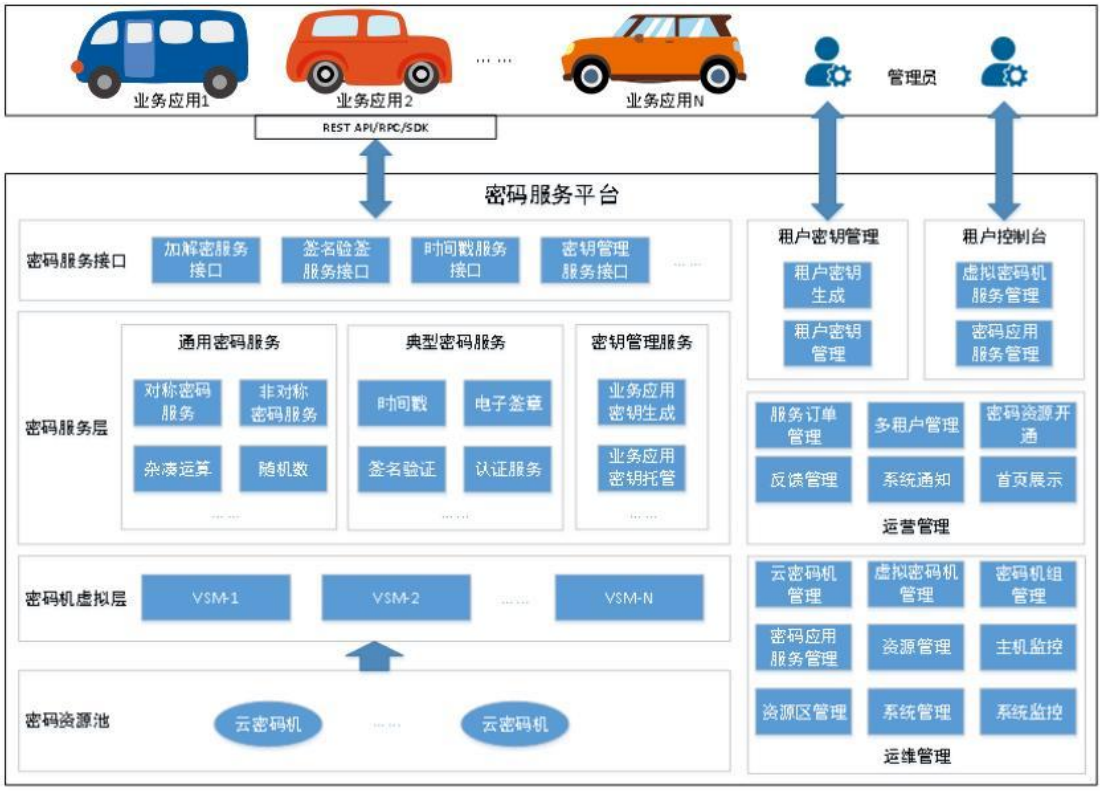


图 6-1　密码服务平台

（1）通用密码服务功能

通用密码服务基于虚拟密码机，通过标准 API 接口为业务应用加密/解密、签名/验签、杂凑运算、消息鉴别码产生和验证、密钥管理等通用密码服务。

（2）典型密码服务功能

- **安全认证网关服务：**安全认证网关服务在工业互联环境中，围绕通信

网络传输安全、安全区域边界及应用安全支撑等方面实现基于数字证书的身份认证与访问控制。

- **签名验签服务：**签名验签服务具有数据加解密、签名、验签、MAC、杂凑、数字信封、数字证书管理等功能，支持 SM2/SM3/SM4 国密算法。

- **存储加解密服务：**存储加密服务为应用提供本地设备一样访问远端或云端的存储路径，本地应用产生的数据通过安全加密存储网关以密文形式上传到对应存储设备。
- **数据库加解密服务：**数据库加解密服务提供数据库软件进行整库加密的能力。对于数据库软件提供存储时进行信息加密，读取时进行信息解密的机制。

（2）车载安全子系统

车载安全子系统包含安全管理模块、密码引擎模块、安全配置模块，在基础模块之上支撑了车载应用安全模块。基于车规级安全芯片的国密计算能力，可支持车云认证及车云通道的建立、Secure FOTA、OBD 接口的安全诊断、车内安全通信 SecOC、车控指令的加密传输、车辆防盗检测等安全场景下的商用密码的应用需求。

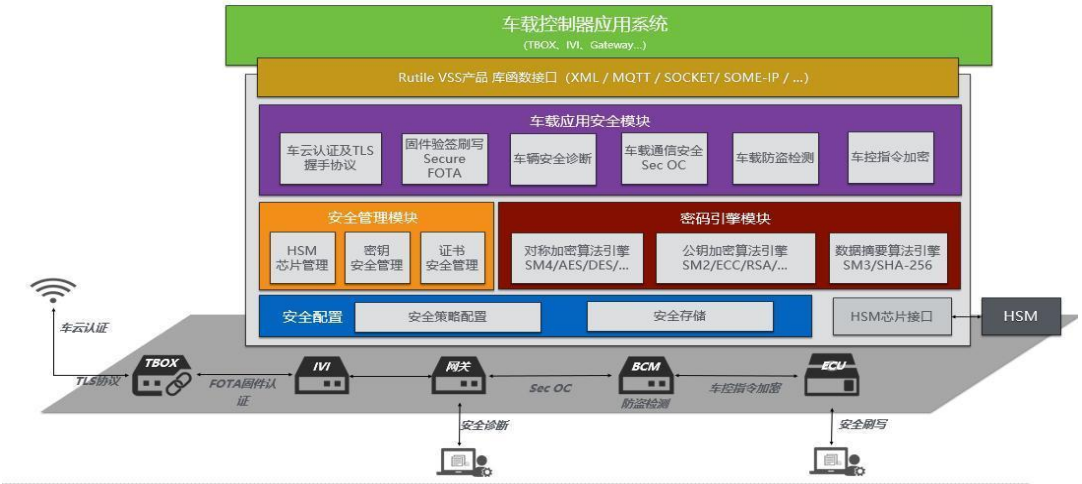


图 6-2　车载安全子系统

安全模块

- **芯片管理：**SS 通过安全芯片的密码计算能力对外提供基础的安全存储、密钥管理、密码算法等功能。芯片支持 SM2/SM3/SM4 算法。

- **密钥管理：**统一管理 SeoOC 通信，车控指令加解密，应用数据传输，车辆防盗等业务所需的对称密钥，包括密钥的生成、导出、变更、销毁。
- **安全存储：**使用 VSS 内部的加密算法，对系统业务密钥和敏感数据做安全存储。
- **安全 SDK：**车载安全子系统提供的安全接口如下图所示：

类型	接口名称
密钥管理	ECC密钥对生成并导出接口
	SM2密钥对生成并导出接口
	RSA密钥对生成并导出接口
	ECC密钥对生成并存储接口
	SM2密钥对生成并存储接口
	RSA密钥对生成并存储接口
	导入会话密钥
	读取会话密钥
	生成对称密钥
	导出对称密钥
	根据码单产生密钥
证书管理	证书导入
	证书删除
固件安全	固件文件签名验证
	固件文件加解密
SecOC	Csm_MacGenerate
	Csm_MacVerify
	Csm_KeyElementSet
	Csm_KeySetValid

类型	接口名称
安全通道	产生证书请求
	安全通道-对称加密运算
	产生会话密钥
	数据签名
	计算握手结束校验值
	读取证书信息
	证书合法性验证
	证书公钥加密接口
	重置会话密钥接口
	更新KMC
	验证证书信息
TLS安全通讯协议	上下文初始化接口
	安全通讯握手接口
	安全数据发送接口
	安全数据接收接口
管理接口	修改密钥激活属性
	更改密钥属性
	算法库初始化接口
	获取版本信息接口

类型	接口名称
基础算法	ECC数据运算接口（外部密钥）
	ECC数据运算接口（内部密钥）
	SM2数据运算接口（外部密钥）
	SM2数据运算接口（内部密钥）
	RSA数据运算接口（外部密钥）
	RSA数据运算接口（内部密钥）
	RSA公钥数据运算接口
	AES对称运算
	SM4对称运算
	AES计算MAC
	SM4计算MAC
	产生随机数
	HASH计算
	HMAC计算
	ECC数据签名
	ECC验证签名
	SM2数据签名
	SM2验证签名
	ZUC对称运算

图 6-3　车载安全子系统接口

3.工业互联典型应用场景

（1）FOTA 车云安全

在 FOTA 流程中面临的风险主要包括传输风险和升级包篡改风险，车载安全支撑系统配合云端 OTA 服务器完成安全 FOTA，为 FOTA 升级的安全提供保障。

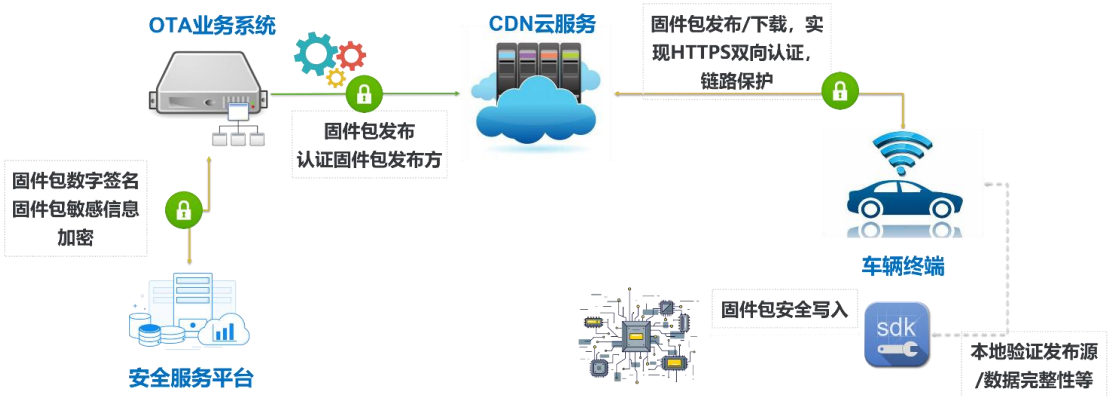


图 6-4　FOTA 安全

（2）OBD 诊断安全

由于通常 CAN 总线不加密不认证，攻击者可以轻易伪造 CAN 总线报文或者获取车辆敏感数据，OBD 诊断接口安全也是当前主机厂关注的要点。车载安全支撑系统支持 OBD 诊断接口接入设备的身份认证，为 OBD 诊断接口的安全提供保障。认证流程如下图所示：

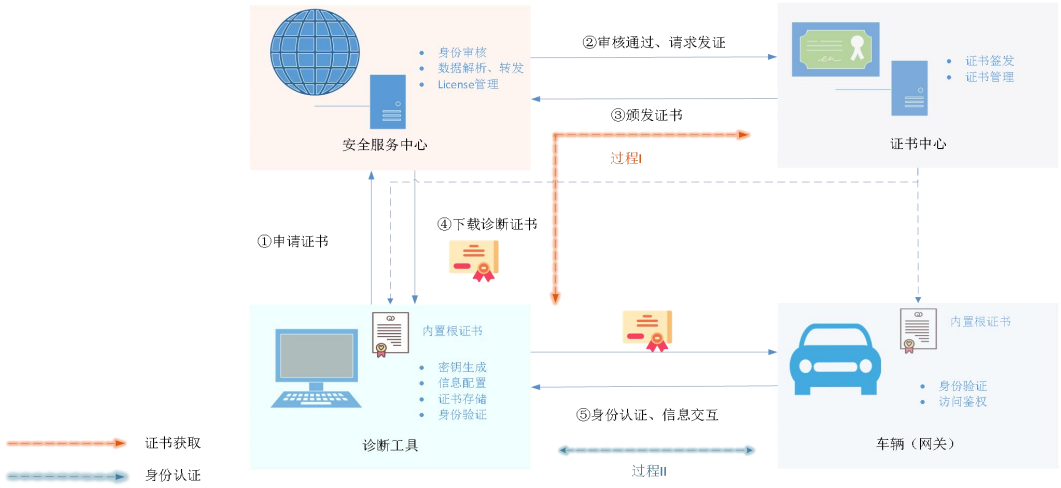


图 6-5　OBD 诊断安全

（3）C-V2X 应用安全

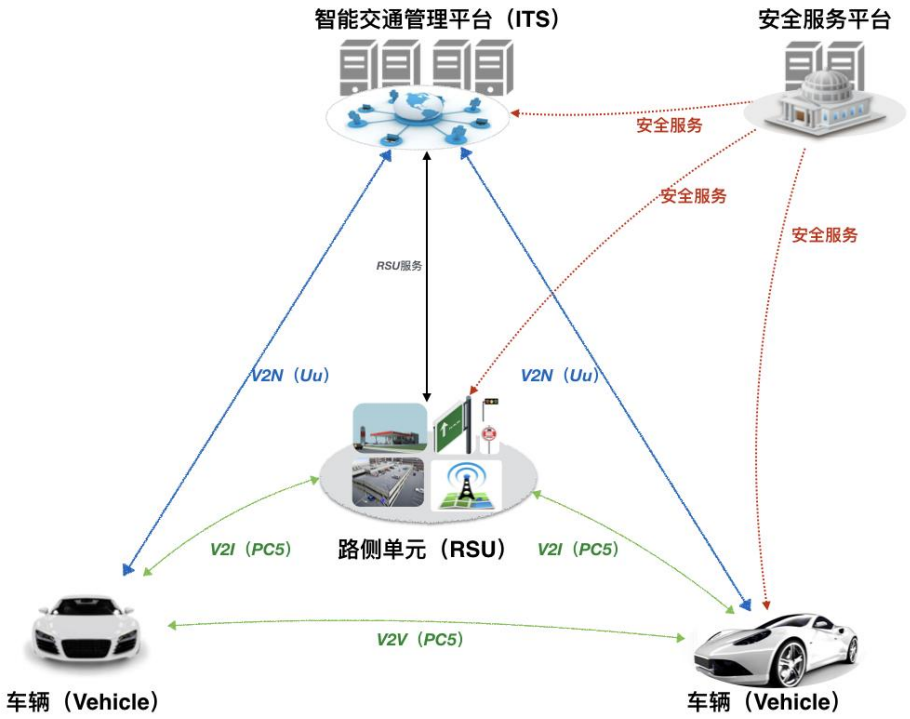


图 6-6　C-V2X

如上图所示，为保障 V2X 场景下设备间的安全认证和安全通信，基于国密 SM2 算法的 PKI 机制，并采用数字签名等技术手段实施 V2V（车-车）/V2I（车-基础设施）/V2P（车-行人）直连通信安全。将数字身份认证技术应用于车联网通信中，实现车载设备、路侧设备、应用服务商等各个角色的相互认证，保证通信消息来源的真实性，有效做到防重放、防止中间人攻击、防止身份假冒等。为依托车联网通信技术实现的安全预警和效率提升等车联网应用提供关键的基础安全保障。

1.1.3 下一步实施计划

后续将在现有认证的服务模式下，深化服务内容，结合跨域交易的业务情况，提供跨域签章、跨域签名等更深层次的安全保障服务，实现进一步的安全服务。通过商用密码技术与 V2X 技术深度结合的典型应用，通过部署满足商用密码技术和管理要求的 V2X 安全证书管理系统 SCMS，以国家通信行业标准《基于 LTE 的车联网通信技术安全证书管理系统技术要求》为指导，建立了车联网联汽车试验场地车-路协同互认的 LTE-V2X 通信加密保护和安全认证体系，推动了车网联汽车试验场地智能网联 V2X 产业加速落地，构筑了下一代安全、高效的智慧出行生活示范应用。在各通信实体身份认证、数据校验及保护等方面本案例都充分利用了商用密码高安全、高效率、高可用等特性，实现了 V2X 通信安全防护的业务要求，为国内车网联建设提供了可参考、可复制的先行经验，其未来前景可期。

1.1.4 方案创新点和实施效果

1.先进性

（1）工业互联密码服务模式，快速覆盖全车系

与传统面向单车单厂建立一套独立的密码服务体系模式不同，我

们采用云密码多租户的服务模式，系统架构上具备的弹性部署能力和应用对接的标准化能力的特色，可以适应各种企业规模。既可以适用单个车机厂，也可以适应整个集团下所有车机厂。

可以为集团建立了一套整体的密码服务架构，其中不同的车厂可以看做不同的租户，不同的车型看做不同的应用，通过系统的弹性部署能力，快速创建多租户多应用的方式，将密码支撑能力快速复制到多车厂，或者多车型，最终达到覆盖全车系的效果。

（2）工业互联多场景密码应用，车云网一体化安全

方案面向车、云、网三个维度提供了一个完整的解决方案。在云端，通过密管平台可以快速建立了一个密码支撑体系，基于云应用的模式，可以实现对应用快速部署密码服务支撑的能力，应用通过低代码的标准化的接口，可以快速批量对接密码服务能力。

在车端，车载安全方案通过 M 系列安全芯片将安全能力进行了全链路的覆盖，涵盖了包括车载中央网关、T-Box 网联部件、车内娱乐系统、智能座舱、智驾域控制、电控单元、电机控制单元、车身控制模块以及空调控制等控制设备，并且通过统一的开发接口，可以快速复制对接新车型，可以快速为车身安全赋能，属于早期具备了在行业中进行全链路国产密码应用推广能力的方案。目前，已经定点应用于上海的两家大型汽车厂（OEM）。

（3）工业互联建立跨控制器间加密信道，实现车内通信安全

车端侧，基于安全芯片建立的车载安全子系统的密码支撑能力相对更广泛的覆盖了整车部件。在场景上，从安全启动，到车内模块之间的通讯，包括模块之间的车云认证；在 OTA 远程升级安全、远程诊断防火墙、安全虚拟车钥匙等业务中证书的签名、验证都使用国密 SM2、SM3 算法代替国际算法 ECC 和 SHA；在车内通信、车控指令、应

用数据、安全数据传输等使用对称密钥的业务场景，全面使用国密算法 SM4 代替 AES 等国际算法，实现了自主可控。

2.创新点

（1）工业互联构建统一的多算法多协议密码服务平台

方案构建了统一的多算法多协议的服务平台，可以基于统一的管理界面对人、车、终端进行证书管理；在整个密码服务生态里面，兼容了不同体系，包括传统的 X509，V2X PKI 体系。密码支撑能力覆盖了多个协议，包含了面向车云的协议，面向端到端的 C-V2X 直连协议，面向车内的 AUTOSAR 协议。

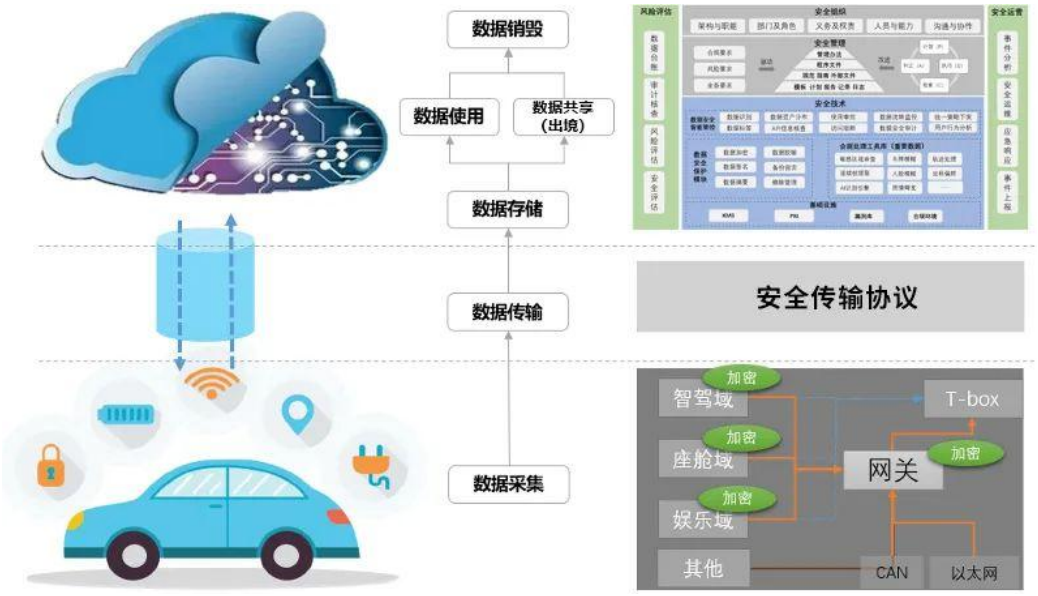
（2）工业互联实现 AUTOSAR 协议国密改造，推动自主可控

汽车开放系统架构（AUTomotive Open System Architecture）是一家致力于制定汽车电子软件标准的联盟。各伙伴公司携手合作，致力于为汽车工业开发一个开放的、标准化的软件架构。AUTOSAR 这个架构有利于车辆电子系统软件的交换与更新，因此应用的非常广泛，很多全世界行业大厂都是 AUTOSAR 成员。

我们在工业互联场景里实现了 AUTOSAR 对国密协议的底层支持。在 AUTOSAR 架构的 SecOC 通信组件中，将加解密运算和验证接口替换为 VSS 车载安全子系统中的国密 SM4 算法接口，完成国密与 AUTOSAR 的底层支持。

（3）工业互联发挥密码特性，应用整车数据安全

把握汽车数据的法规需求，制定汽车数据安全分类分级制度规范，按照数据全生命周期，从汽车数据采集、传输、存储、利用、共享、出境、销毁、备份恢复等环节分别明确汽车数据安全需求。通过商用密码技术构建零束的汽车数据安全技术防护体系，防范数据泄露、篡改、滥用等风险，全面保障汽车数据安全合规。



3.标准符合性

根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，本方案的密码支撑目标是终端、用户与云上系统之间的“设备和计算安全”、“应用和数据安全”以及“网络和通信安全”。

4. 实施效果

（1）工业互联场景下车载密码应用合规要求

本方案于 2022.5.20 日过密评。属于工业互联网行业中通过密评比较早的企业。对于同类的规划具有相当的示范作用。在集团里，既有传统的 PKI，又有新兴的 V2X PKI 系统，既有软件的密码模块，又有车规级的安全芯片，既有移动端的安全风险，又有云的安全风险。这样一个复杂的场景中，我们探索出了一个满足合规的解决方案，在集团这里得到了较好验证和应用，对处于同样类型的企业具备相当的示范效应。

（2）工业互联全面全域提升整车安全性

VSS 车载安全子系统在车辆各类控制器（ECU）上的安全部署以构建一个完整的防护体系，支撑车辆控制器的各类安全需求，包括有

车辆身份认证、远程安全通信、安全固件升级、安全诊断防火墙、车内安全通信以及车控指令加密等。该产品无需车企或者零部件供应商改动原先的硬件单元，而只需要在相关控制芯片中加入算法包实现通信安全。因此相较于其他硬件安全方案的部署，VSS 软件产品在诸如底盘、动力、车身控制等成熟度较高的车辆电子电气域中有着较为明显的优势与竞争力。

（3）推动工业互联各领域车厂密码应用落地

密码服务平台基于云原生理念，面向车企各部门的应用系统，提供“即申请，即调用，即服务”的密码基础服务，从实际效果反馈，简化上云的复杂度，降低上云成本，降低上云对接时间，基于该模式的密码应用已经在上海电子政务 XC 云上得到了广泛应用，在实际应用中，因为接口的标准性，同一家开发商的多个应用均可以批量复制，实现短时间快速对接了大量的应用。另外弹性按需申请的模式，也大量节约了密码服务建设费用和使用费用。同时因使用费用降低，得到了更广泛的应用，带来安全性也产生了巨大的社会效益。

（4）建设工业互联上海 V2X 根体系

建立了上海的 V2X 根体系，实现上海范围内不同主机厂车辆，不同 V2X PKI 体系的互通互信。其中 V2X 业务体系已对接工信部全国 V2X PKI 根体系的能力，可支持各类车联应用对全国范围的覆盖，可助力国家统一大市场的宏观规划。

（5）加快推动软件定义汽车，助力汽车新零售模式

汽车硬件将成为模块化、通用化的平台和资源池，支撑整车软件多样化开发与部署。软件定义汽车功能的增加与升级可通过软件的远程部署与更新来实现，随着这种场景的应用深入，催生出汽车新零售的全新业务模式也在不断的成熟。在这种场景下各种车载的配置数据

都将高度依赖车载安全系统的数据保护的能力。在硬件安全芯片加持下的VSS车载安全子系统对配置系统提供签名验签、加解密的保护，将有效支撑新场景、新业务的应用。

1.1.5 单位基本信息

1.中移（苏州）软件技术有限公司

中移（苏州）软件技术有限公司是中国移动通信集团有限公司2014年注资31.72亿元成立的全资子公司，公司定位为中国移动云设施构建者、云服务提供者、云生态汇聚者，目前正处在快速发展阶段，先后取得了国家高新技术企业、国家重点软件企业、江苏省高新技术企业、苏州市云计算工程技术研究中心等资质。

公司主营业务移动云是中国移动面向政企、事业单位、开发者等客户推出的基于云计算技术、采用互联网模式、提供基础资源、平台能力、软件应用等服务的业务系统，自主开发建设、拥有完全的自主知识产权，能够提供保密性强的 IT 设施环境。通过建设N个集中节点、31个省级属地化节点、X个边缘节点，打造“一朵云”的全域资源布局，移动云业务遍布全国，2021年移动云收入超180亿元。

2. 中国移动通信集团公司有限公司信息安全管理与运行中心

2011年11月，中国移动通信集团有限公司信息安全管理与运行中心成立（以下简称“信安中心”），具备“管理+生产”双重职能，负责归口信息安全管理与不良信息治理，开展不良信息集中治理与信息安全集中运营。2018年8月，集团成立中国移动网络安全领导小组，领导小组办公室设在我中心，负责集团网络安全相关工作统筹和协调。信安中心深入学习贯彻习近平总书记关于网信工作的重要指示精神，以建设网络强国为己任，工作范围覆盖终端安全、网络安全、应用安全、业务安全、内容安全等多领域，形成了全国“一盘棋”的

工作格局，相关工作整体能力与水平始终保持行业领先。近年来，信安中心在开展网络安全重保、防范打击电信诈骗、组织网络安全攻防竞赛、开展网络安全研发等方面卓有成效。在工业互联网方面，特别成立了专门的研发中心，开展工业互联网业务及工业互联网安全防护解决方案的研制和推广。

3. 格尔软件股份有限公司

格尔软件股份有限公司（简称“格尔软件”）是中国信息安全数字信任领域的先行者和领导者，成立于 1998 年 3 月，2017 年 4 月在上交所上市，被誉为“国内最早登陆 A 股的信息安全软件企业”（股票代码：603232.SH）。

始于密码，臻于匠心。格尔软件是中国首批研制和推出 PKI 公钥基础设施产品的厂商，也是国内首批通过国家密码管理局审查、支持 SM2 算法、省级电子认证服务机构的建设单位。20 多年来，格尔软件秉持“关键技术自主可控、密码产品安全易用”的研发理念，相继开发出密码基础、身份管理、访问控制、数据安全、PKI/CA、电子签名、安全网关、终端接入、视频安全、工控安全等 11 类近 100 款产品，建立了上海、北京、西安、成都、南京 5 大研发中心，先后承担了 20 余项国家级、省部级的重点信息安全科研方案的研究与开发工作，参与承建了我国多个第三方数字认证中心系统。公司拥有发明专利近 80 项、计算机软件著作权近 200 项，牵头或参与制定国家标准 20 余项、行业标准 40 余项，先后 2 次荣获国家科学技术进步奖二等奖，多次荣获国家党政密码科技进步奖和上海市科学技术进步奖。

深耕细作，笃行致远。格尔软件聚焦“让互联更可信、让数据更安全”的企业愿景，坚持以密码技术为核心，以业务应用为导向，以可信身份为基础，逐渐成长为我国网络空间和数字资产安全的领导者，

员工近1000人。公司实行“上海+北京”的双总部战略，打造“行业+区域”的全流程生态模式，旗下拥有格尔安全、格尔安信、格尔科安、北京格尔国信、上海信元通5家全资子公司，建立了北京、上海、郑州、西安、成都、南京、杭州、广州、乌鲁木齐、拉萨、武汉、沈阳、昆明等13个区域营销中心和交付中心，铺设了覆盖全国34个省级行政区和24个省会城市的营销服务网点，为32个国家部委、100多家国企央企、200多家银行提供全域全栈的专业级信息安全服务。

以梦为马，不负韶华。格尔软件始终坚持党建与业务融合发展，聚力将党建工作的政治优势和组织优势转化为推动企业发展的市场优势，为我国网络安全信任体系建设和党政机关、军工军队、公检司法、国企央企、金融机构等重要用户信息系统提供数字资产安全整体解决方案。近年来，格尔软件不断基于国产密码技术和可信身份管理进行密码应用创新，构建了具有格尔特色的云密码服务体系和零信任安全架构，实现了多场景下密码服务的无缝集成、无感调用、无处不密、处处用密，基本具备“密码即服务，安全可内生”的综合服务能力。2020年，被评为“中国信创产业60强”。2021年，被评为“中国网络安全企业100强中‘身份与访问安全’与‘商用密码’领域十强”，2022年被评为“中国网安产业竞争力50强”。