中汽中心 | 检测

中汽研软件测评（天津）有限公司

商用密码上车应用政策标准与合规应对

中汽研软件测评中心（天津）有限公司

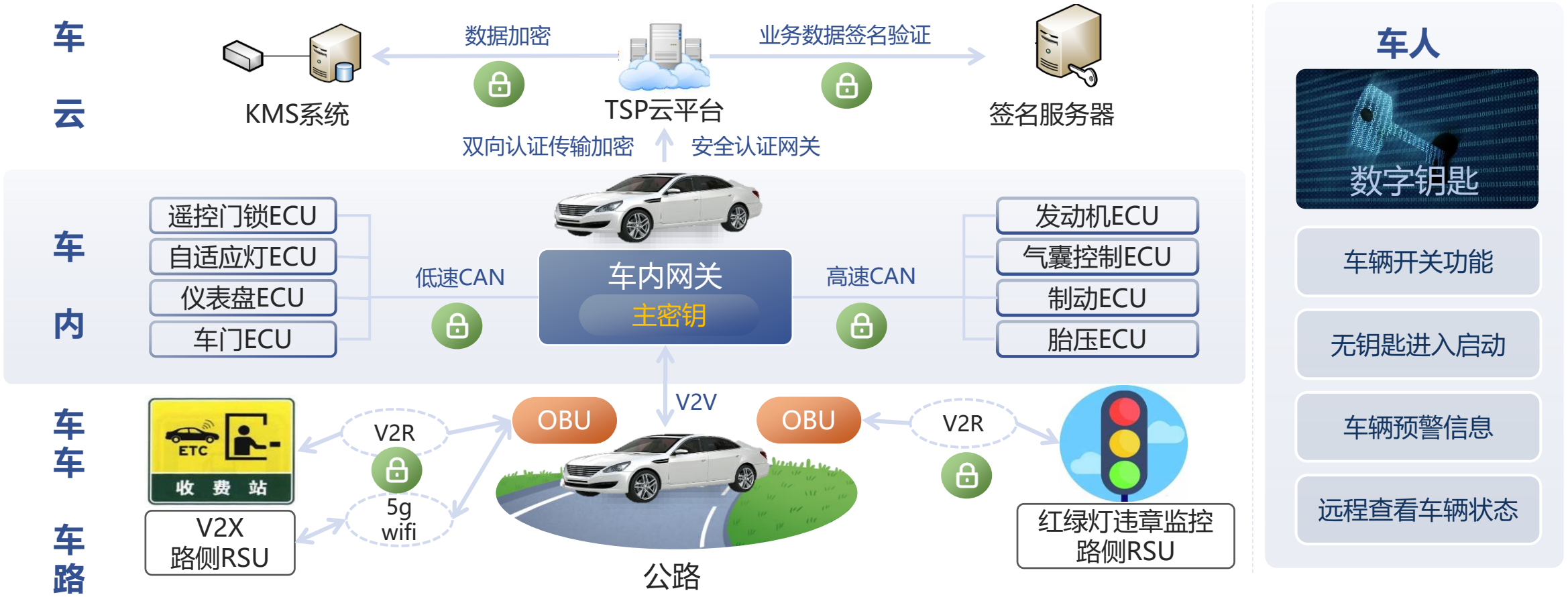
鲍越

目录

Contents

1.1 密码技术在车联网领域广泛应用

■ **密码是国之重器，是网络安全的核心保障与基础支撑，在智能网联汽车上应用广泛，包括车车/车路、车云、车内、车人等多种通信场景。**



1.2 国家政策法规

- 《网络安全法》《密码法》《数据安全法》相继发布，为汽车领域商密应用与安全提供上位法指导
- 《商用密码管理条例》**为商用密码具体的实施和执行提供了更为明确的政策指引**

《网络安全法》2017年正式实施

为科学治理和化解信息化发展中的网络安全问题与风险提供明确依据，使得智能网联汽车安全有法可依。

《密码法》2020年正式实施

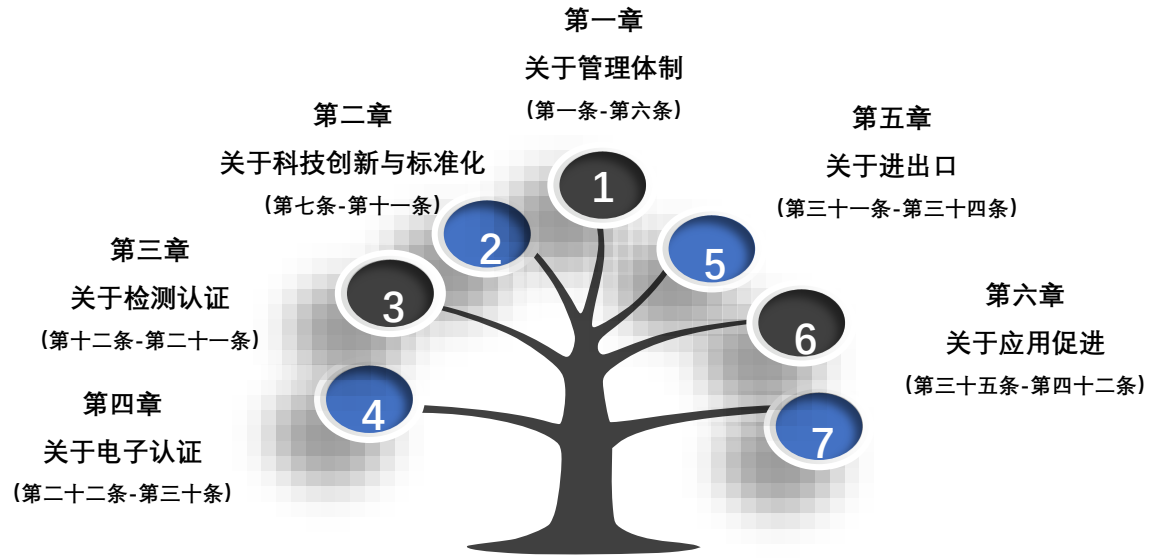
智能网联汽车网络安全事件多与密码应用密切相关，密码是保障智能网联汽车安全的最关键技术。

《数据安全法》2021年正式实施

智能网联汽车行驶过程中采集了大量数据，合理、合规、安全的使用数据是底线要求。

《商用密码管理条例》2023年正式实施

规范商用密码应用和管理，鼓励和促进商用密码产业发展，保障网络与信息安全，对智能网联汽车同样重要



1.2.1《商用密码管理条例》

- **商用密码标准化是实现商用密码技术自主创新、促进商用密码产业发展、构建商用密码应用体系的重要支撑。**
- **从事商用密码产品检测的机构，须依法取得商用密码检测机构资质。**

01 标准制定与协调性

- 国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准，对商用密码团体标准的制定进行规范、引导和监督 。 国家密码管理部门依据职责 ， 建立商用密码标准实施信息反馈和评估机制，对商用密码标准实施进行监督检查。
- 其他领域的标准涉及商用密码的，应当与商用密码国家标准、行业标准保持协调。

——《条例》第十条

02 推动国际标准化活动

- 国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用，鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。

——《条例》第十条

03 强制性和推荐性标准遵循

- 从事商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准，以及自我声明公开标准的技术要求。
- 国家鼓励在商用密码活动中采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

——《条例》第十一条

依法检测

从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动，向社会出具具有证明作用的数据、结果的机构，应当经国家密码管理部门认定，依法取得商用密码检测机构资质。

——《条例》第十三条

1.2.2《自然资源领域数据安全管理办法》

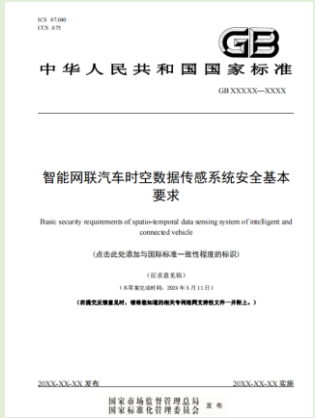
- **《自然资源领域数据安全管理办法》在数据全生命周期中强调使用密码技术对数据进行保护**
- **《智能网联汽车时空数据安全处理基本要求》《智能网联汽车时空数据传感系统安全基本要求》公开征求意见**

《自然资源领域数据安全管理办法》

- 第十二条（三）利用互联网等信息网络开展数据处理活动时，要落实网络安全等级保护、关键信息基础设施安全保护、**密码保护**和保密等制度要求。
- 第十二条（八）法律法规等规定的其他措施。重要数据和核心数据处理者，还应当：（四）在数据全生命周期的各环节，应当综合运用**加密**、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护,**并按照法律法规和国家有关规定要求使用商用密码进行保护。**
- 第十六条数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据和核心数据的，应当采取校验技术、**密码技术**、安全传输通道或者安全传输协议等措施。
- 第二十三条数据处理者应当在数据全生命周期处理过程中，记录数据处理、权限管理、人员操作等日志，并采用**商用密码技术**保护日志的完整性。

第五章保密处理要求

位置类数据和构图类数据应在存储和向车外传输前按照国家认定的地理信息**保密处理技术**完成处理。



第四章安全要求

4.1.2时空数据传感系统的存储模块和向车外传输模块在运行时,应具备地理信息保密处理功能，并应符合国家认定的地理信息**保密处理技术**要求。

4.3存储功能要求

时空数据传感系统外部接口应**具有访问控制和身份鉴别的机制**,确保存储的时空数据不被任意获取。

1.3 汽车安全标准情况

■ 汽标委已完成了四个批次共计多项信息安全领域的标准研究工作。

批次	序号/number	标准项目/standardproject		
第一批	1	《汽车信息安全通用技术要求》	GB	强制性国家标准
	2	《电动汽车远程服务与管理系统信息安全技术要求及试验方法》		
	3	《车载信息交互系统信息安全技术要求及试验方法》		
	4	《汽车网关信息安全技术要求及试验方法》		
	5	《电动汽车充电系统信息安全技术要求》		
第二批	6	**《汽车软件升级通用技术要求》**	GB/T	推荐性国家标准
第二批	7	《汽车诊断接口信息安全技术要求及实验方法》		
	8	《汽车信息安全应急响应管理指南》		
	9	《汽车信息安全风险评估规范》		
第三批	10	**《汽车整车信息安全技术要求》**		
	11	《道路车辆信息安全工程》		
第四批	12	**《汽车密码应用技术要求》**	预研	标准化需求研究
	13	《汽车数字证书技术规范》		
	14	《车载计算平台标准化需求研究》		
	15	《汽车电子控制单元（ECU）信息安全防护技术要求研究》		

1.3.1 《汽车整车信息安全技术要求》GB

- 本文件规定了汽车信息安全管理体系要求、信息安全一般要求、信息安全技术要求、检查与试验方法和同一型式判定。
- 本文件适用于M类、N类及至少装有1个电子控制单元的O类车辆。

《汽车整车信息安全技术要求》

标准正文：

6.8车辆制造商应使用公开的、已发布的、有效的密码算法，应根据不同密码算法和业务场景，选择适当的参数和选项。

《汽车整车信息安全技术要求-操作指南》（草案）

序号	要点	证明材料
1	车辆制造商应使用公开的、已发布的、有效的密码算法	车型所使用的全部密码技术列表，包括算法类型与依据标准
2	车辆是否根据不同密码算法和业务场景，选择适当的参数和选项	密码应用的核心业务场景（例如，外部连接、通信安全、软件升级、数据安全）所使用密码算法的技术文档

标准正文：

6.9车辆制造商应满足以下密码模块要求之一：

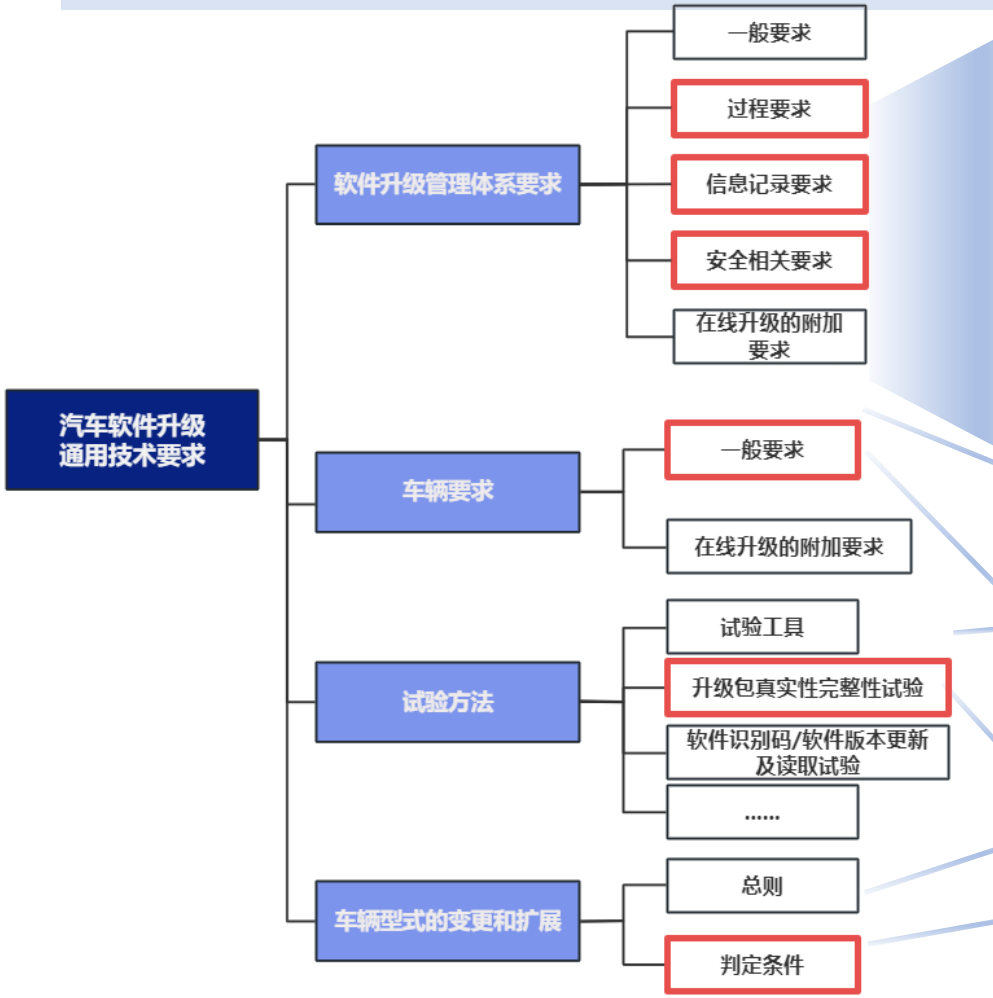
——采用符合国际、国家或行业标准要求的密码模块；

——未采用国际、国家或行业标准要求的密码模块，说明使用的合理性。

序号	要点	证明材料
1	车辆生产企业所使用的密码模块，是否满足国际、国家或行业标准要求，提供说明采用非标密码模块的合理性	车型所使用的密码模块情况总结报告
2		核心零部件的密码模块（例如，T-box、网关、车机、ADAS、DSSAD、数字钥匙等）须提供检测报告或检测认证证书（如商用密码产品认证证书或FIPS证书）
3		非标密码模块产品须提供检测报告（经过专家论证或审查的证明材料）

1.3.2《汽车软件升级通用技术要求》GB

■ 标准适用于具备软件升级功能的M类、N类汽车，主要包括管理体系要求、车辆要求、试验方法、车辆型式的变更和扩展等。



4.2.1 应具备唯一地标识准入或认证相关系统所有初始和更新版本的软件（**至少包括完整性验证数据**）以及相关硬件部件的过程。
4.2.2 对于具有软件识别码的车型，应具备:
b)在软件升级后，能更新软件识别码相关信息的过程，至少更新所有相关软件的版本及**完整性验证数据**；能验证相关系统中软件版本与相关软件识别码中软件版本保持一致的过程。

4.3.3 在软件升级前后，每个软件识别码应有一个可审核的记录用于描述所有相关的软件，至少应包括所有相关软件的版本及**完整性验证数据**。

4.4.1 应具备保护升级包的过程，合理地**防止其在执行前被篡改**。

5.1.1 应保护升级包的**真实性和完整性**，合理地防止其受到损害和防止无效软件升级。
5.1.4 应保护车辆上的软件识别码和/或软件版本**免受篡改**。

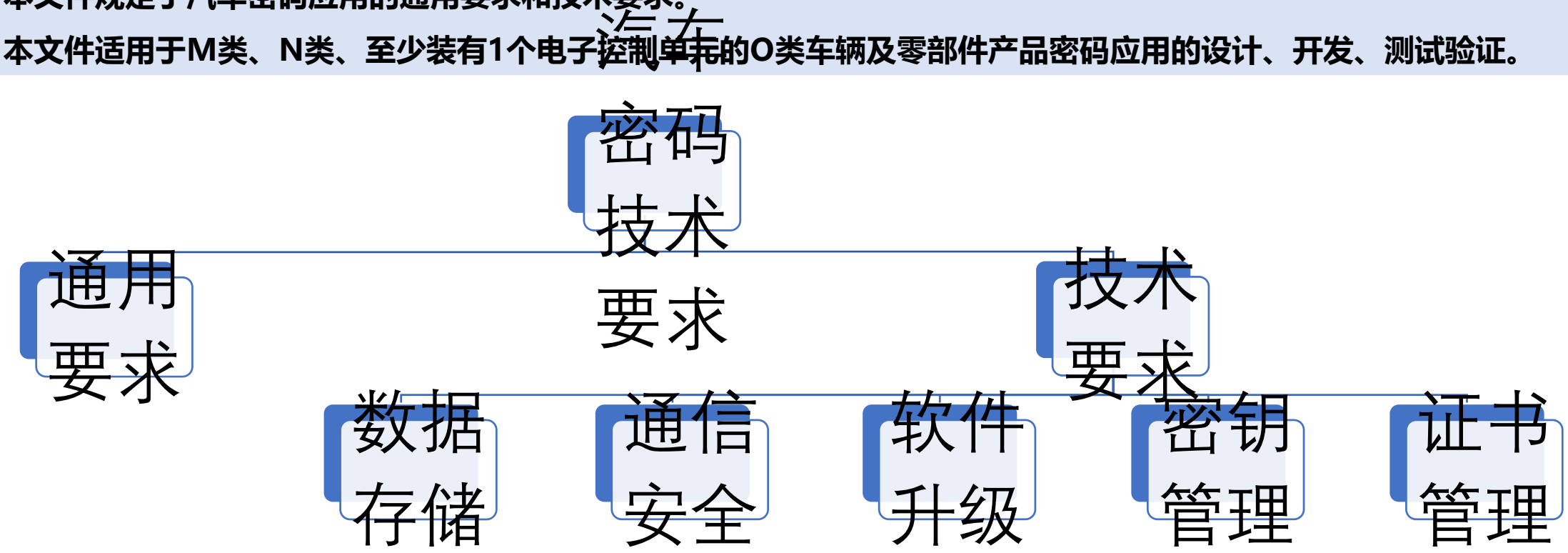
6.2 利用升级包篡改工具分别构造真实性被损害的升级包和完整性被损害的升级包，执行软件升级，检查并记录软件升级结果和日志中的校验结果，试验结果符合5.1.1的要求。

7.2.5 升级包**完整性和真实性的保护方式相同**.

■ **完整性验证数据：用以检测数据中的错误或变化的值。**
■ **示例：校验值、哈希值等。**

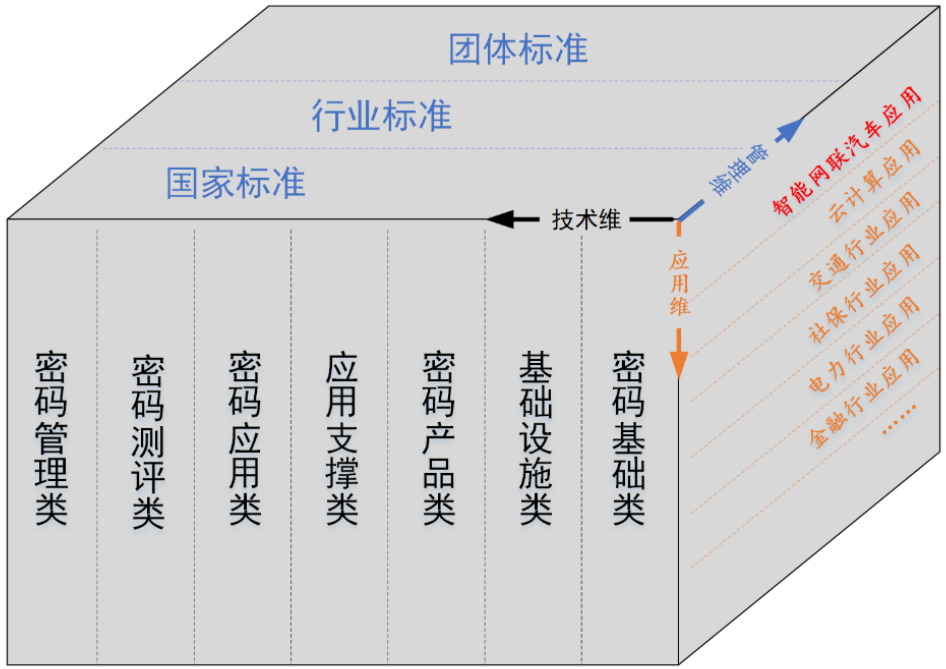
1.3.3《汽车密码应用技术要求》GB

- 本文件规定了汽车密码应用的通用要求和技术要求。
- 本文件适用于M类、N类、至少装有1个电子控制单元的O类车辆及零部件产品密码应用的设计、开发、测试验证。



1.3.4 密码行业配套标准

■ 为更好的支持商用密码在汽车行业的落地应用，密标委行业标准规划11项拟立项标准，涉及车载网关、自动驾驶数据记录系统、智能驾驶域控系统、地理信息处理模块等。

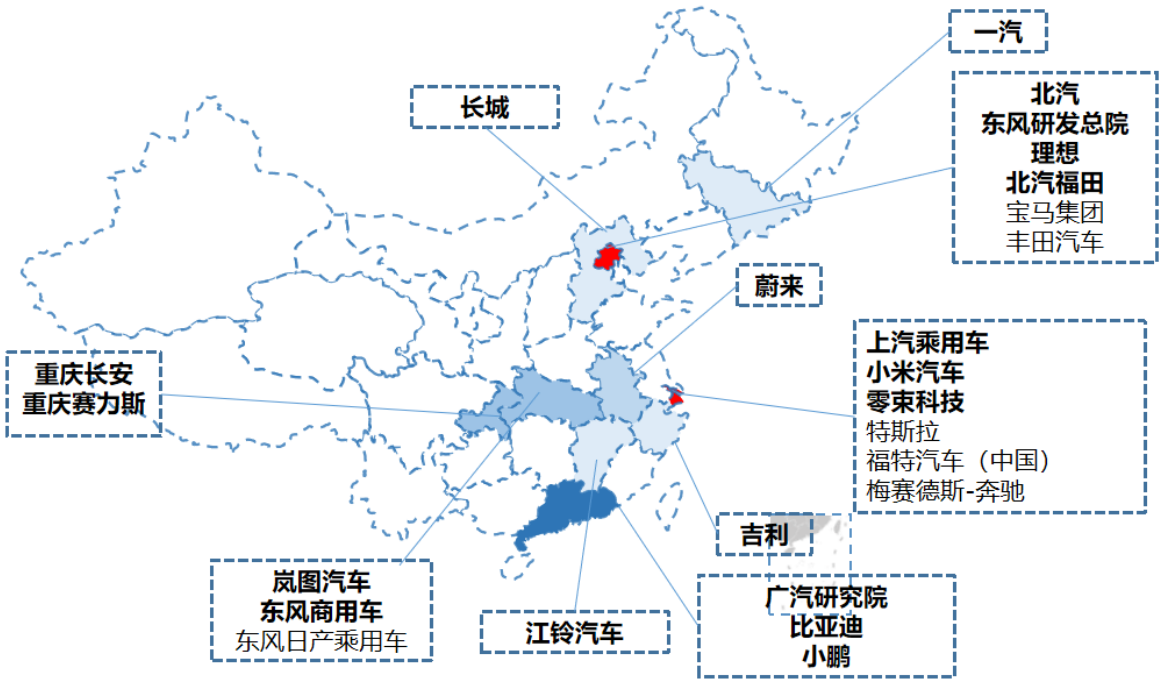


序号	标准名称
1	低空智联网密码标准体系
2	汽车数字证书格式
3	车联网信息系统密码应用测评要求
4	车载安全网关技术要求
5	车载安全网关检测规范
6	车载直连通信产品密码应用技术要求
7	车载直连通信产品密码应用检测规范
8	自动驾驶数据记录系统密码应用技术要求
9	自动驾驶数据记录系统密码应用检测规范
10	智能驾驶域控制器密码应用技术要求
11	智能汽车地理信息处理模块密码应用要求

1.4 行业情况

■ **本次问卷共收集39份问卷，其中有效问卷为37份，整车企业共收集问卷26份，零部件企业收集8份，密码企业收集2份，其他企业收集3份。**

参与问卷调研车企地域分布情况



汽车企业

- 一汽
- 东风
- 长安
- 北汽
- 上汽
- 广汽
- 比亚迪
- 长城汽车
- 吉利汽车
- 岚图汽车
- 蔚来汽车
- 小鹏汽车
- 北京车和家
- 赛力斯
- 小米汽车
- 东风商用车
- 零束科技
- 北汽福田
- 江铃汽车
- 特斯拉
- 东风日产
- 丰田汽车
- 福特汽车
- 奔驰梅赛德斯
- 宝马集团

零部件企业

- 博世
- 宁德时代
- 国芯科技
- 地平线
- 高通
- 德赛西威
- 知行科技
- 株式会社爱信

密码企业

- 华大电子
- 信大捷安

其他企业

- 斑马智行
- 北京航迹
- 中国汽车工程研究院

1.4.1 调研内容

■ **为开展汽车行业密码应用情况调研，设计关于开展《汽车密码应用技术要求》标准工作的调查问卷，了解汽车行业在密码技术应用的现状，收集汽车行业对密码技术应用的意见与建议。**

应用现状

车载系统/零部件

研究对象（10个）
- T-box
- 车载网关
- V2X OBU
- 车机
- 自动驾驶系统
- 电池管理系统
- 无钥匙进入
- 动力总成控制
- 车身控制系统
- 底盘控制系统

商用密码类型（18种）
- 对称算法
- 非对称算法
- 杂凑算法

密码应用需求（6种）
- 机密性
- 抗重放攻击
- 真实性
- 安全通道
- 完整性
- 不可否认

密码部件（3种以上）
- 硬件密码模块
- 软件密码模块
- 安全芯片
- 其他

应用场景（3种）
- 数据存储
- 通信安全
- 软件升级

数据类型（7种以上）
- 车辆基本数据
- 感知数据
- 决策数据
- 运行数据
- 个人信息
- 其他数据

行业声音

《汽车密码应用技术要求》研制建议

标准内容
- 通用要求
- 软件升级
- 总体架构
- 数据存储
- 密钥管理
- 适用范围约束
- 通信安全
- 证书管理

标准协调性
- 编制思路
- 编制内容
- 管理实施

标准体系建设
- 配套标准

汽车行业密码应用难点
- 政 策
- 技 术
- 成 本

其他

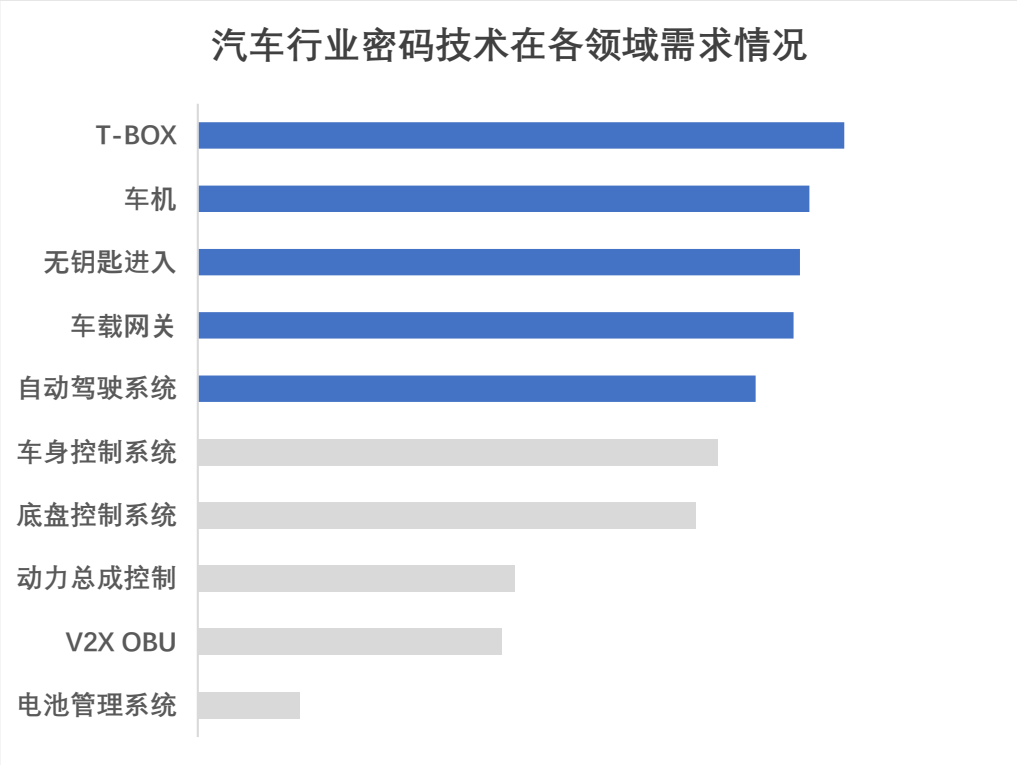
人员结构
- 密码专业人员
- 学历

1.4.2 调研结果

■ **密码算法在智能网联汽车的T-BOX、车机、无钥匙进入、车载网关、自动驾驶系统的应用最为典型。**

密码需求强度

T-BOX、车机、无钥匙进入、车载网关、自动驾驶系统密码算法应用需求强烈且明确。



算法应用情况

- 智能网联汽车关键零部件使用的常见算法，如AES、RSA2048等；
- 应用情况最理想的零部件：**T-BOX**、**V2X OBU**、**车机**；
- 应用情况最理想的车载系统：**自动驾驶系统**；
- 车载网关与无钥匙进入系统算法应用情况落后；
- 部分零部件或系统双技术路线并行。

车载系统/零部件	SM2	SM3	SM4	AES	ECC	DSA	RSA2048	RSA3072	MD5	SHA-1	SHA-256	SHA-512	SHA-3
T-BOX	65%	45%	40%	90%	45%	0%	70%	35%	20%	5%	90%	20%	5%
V2X OBU	55%	50%	45%	45%	15%	0%	30%	10%	15%	0%	35%	5%	0%
车机	45%	40%	45%	95%	40%	0%	85%	25%	15%	5%	90%	15%	0%
自动驾驶系统	25%	25%	25%	95%	55%	0%	85%	25%	20%	0%	90%	20%	0%
车载网关	20%	20%	20%	90%	35%	0%	80%	10%	5%	0%	80%	20%	0%
无钥匙进入	10%	10%	15%	90%	30%	0%	50%	15%	0%	0%	65%	10%	0%
底盘控制系统	10%	10%	10%	60%	25%	5%	55%	15%	0%	0%	60%	10%	0%
电池管理系统	10%	10%	10%	70%	20%	0%	40%	15%	0%	0%	60%	10%	0%
动力总成控制	10%	10%	10%	75%	20%	0%	55%	10%	0%	0%	70%	10%	0%
车身控制系统	10%	10%	10%	70%	25%	0%	60%	10%	5%	0%	70%	10%	0%

目录

Contents

2.1 汽车商用密码应用改造合规应对总体方案

- 为保证满足《汽车密码应用技术要求》标准的合规性要求，建议关注典型场景和典型功能的密码应用
- 核心零部件的密码应用可作为后续合规工作关注的重点对象

T-box

车机

车载网关

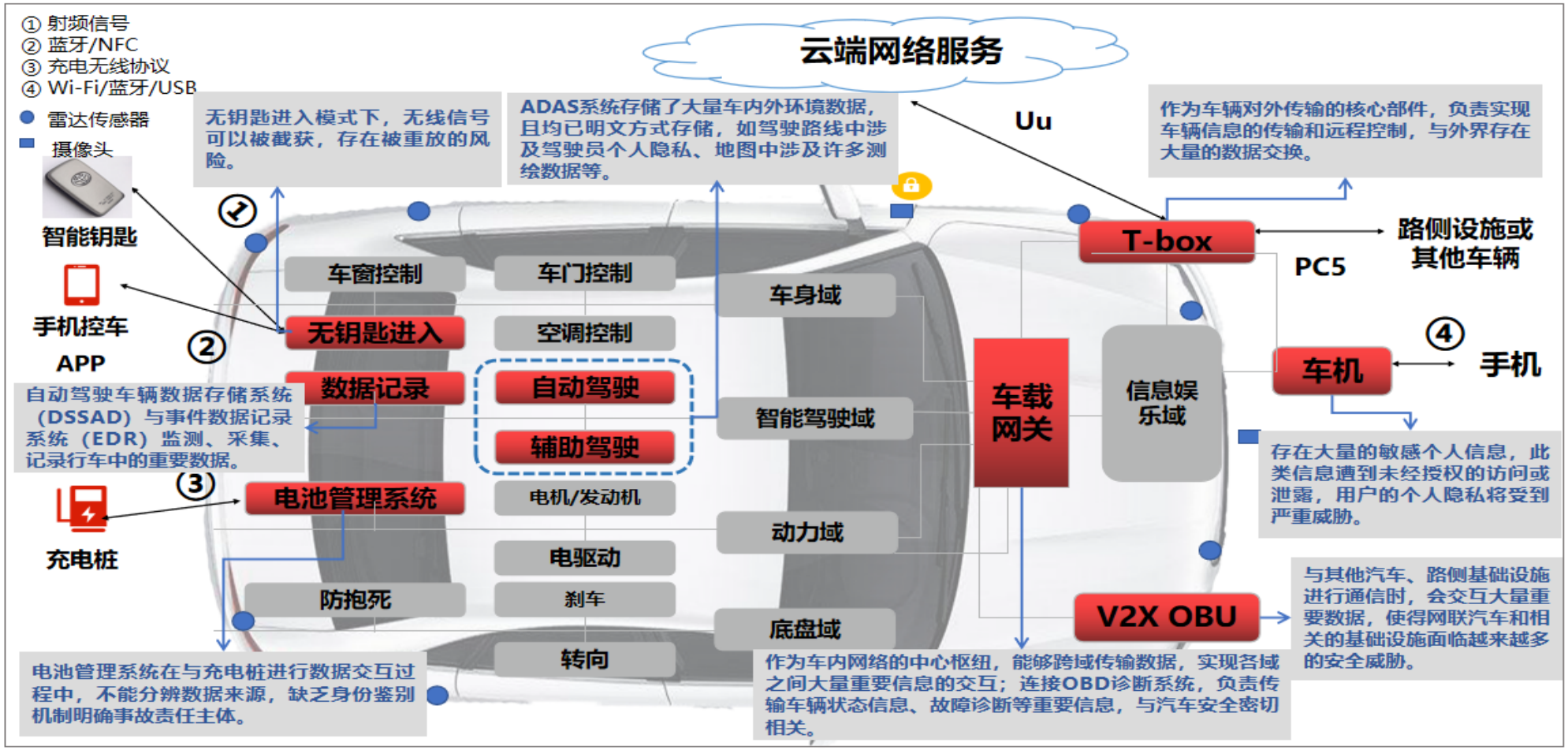
V2XOBU

自动驾驶
辅助驾驶

无钥匙进入

数据记录

BMS



2.2 解决方案一：端|遵照标准研发设计密码模块

- 密码模块国内外遵循两套标准，国内37092与国外FIPS
- 自 2022 年 4 月 1 日起，对于新提交的加密模块，FIPS PUB 140-3 加密模块安全要求取代 FIPS 140-2

GB/T 37092-2018
信息安全技术 密码模块安全要求

安全域	安全一级	安全二级	安全三级	安全四级
1 密码模块规格	密码模块、密码边界、核准的密码功能以及正常的工作模式的说明； 密码模块的描述，包括所有硬件、软件和固件部件； 所有服务提供状态信息以指示服务何时按照核准的方式使用核准的密码算法、安全功能或过程			
2 密码模块接口	要求的和可选的接口； 所有接口和所有输入输出数据路径的说明		可信信道	
3 角色、服务和鉴别	要求的角色、服务与可选的角色、服务逻辑上相隔离	基于角色或基于身份的操作员鉴别	基于身份的鉴别	多因素鉴别
4 软件/固件安全	核准的完整性技术，以及定义的软件或固件密码模块接口、混合固件密码模块接口	基于核准的数字签名或带密钥信息消息鉴别码的完整性测试	基于核准的数字签名的完整性测试	
	以及混合软件固件密码模块接口；可执行代码			
5 运行环境	不可修改的、受限的，对敏感安全参数的控制			
	可修改的，对敏感安全参数的控制	可修改的，基于角色或自主访问控制，审计机制		
6 物理安全	产品级部件	拆卸证据，不透明的遮盖物或外壳	封盖和门上的侵入检测与响应电路，牢固的外壳或涂层，防止直接探测的保护，EFP 或 EFT	拆卸检测和响应封壳，EFP，故障注入的缓解
7 非入侵安全	能够缓解附录 F 中规定的非入侵式攻击			
	文档说明附录 F 中规定的缓解技术和有效性		提供缓解检测方法	缓解检测
8 敏感安全参数管理	随机数生成器、敏感安全参数生成、建立、输入和输出、存储以及置零			
	自动的敏感安全参数传输或敏感安全参数协商使用核准方法			
	手动建立的敏感安全参数可以以明文的形式输入或输出		手动建立的敏感安全参数，可以以加密的形式、通过可信信道或使用知识拆分过程输入或输出	
9 自测试	运行前，软件/固件完整性测试、旁路测试以及关键功能测试			
	条件，密码算法、配对一致性、软件/固件加载、手动输入、条件旁路以及关键功能测试			
10 生命周期保障 1) 配置管理	密码模块、部件和文档的配置管理系统，每一项在整个生命周期中都有唯一标识并可追踪		自动配置管理系统	
2) 设计	密码模块设计成允许对所有提供的安全相关服务进行测试			
3) FSM	有限状态模型			
4) 开发	有注释的源代码、原理或 HDL	软件高级语言；硬件高级描述语言		文档注明密码模块部件执行的前置条件，以及当部件执行完毕时预期为真的后置条件
5) 测试	功能测试		底层测试	
6) 配送与操作	初始化流程	配送流程		使用厂商提供的鉴别信息的操作员鉴别
7) 生命终止	安全清理密码模块的流程		安全销毁密码模块的流程	
8) 指南文档	管理员和非管理员指南			
11 其他攻击的缓解	缓解其他攻击的说明，目前对这些攻击还没有可检测要求			验证缓解技术的有效性

Federal Information Processing Standards Publications 140-3

Requirement Area	FIPS 140-3 Security Level 1	2	3	4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel	
Roles, Services, and Authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security	Approved integrity technique. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature based integrity test	
Operational Environment	Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security	Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation
Non-Invasive Security	Module is designed to mitigate against non-invasive attacks specified in Annex "F".			
	Documentation and effectiveness of mitigation techniques specified in Annex "F"		Mitigation testing	Mitigation testing
Security Parameter Management	Random bit generators, SSP generation, establishment, entry & output, storage & zeroization			
	Automated SSP transport or SSP agreement using approved methods			
	Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures	
Self-Tests	Pre-operational: software/firmware integrity, bypass, and critical functions test			
	Conditional: cryptographic algorithm, pair-wise consistency, SW/FW loading, manual entry, conditional bypass & critical functions test			
Life-Cycle Assurance				
Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system	
Design	Module designed to allow testing of all provided security related services			
FSM	Finite State Model			
Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language		Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed
Testing	Functional testing		Low-level testing	
Delivery & Operation	Initialisation procedures	Delivery procedures		Operator authentication using vendor provided authentication information
Guidance	Administrator and non-administrator guidance			
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available			Specification of mitigation of attacks with testable requirements

FIPS 140-3的改进内容

- 批准的操作模式指示器适用于所有级别，模块提供的每项服务都必须报告。
- 对关键安全参数 (CSP) 的归零要求更为严格。
- 身份验证数据的复杂性不再允许通过程序手段来实施，必须由模块强制执行。
- 第 3 级物理安全要求模块检测超出范围的电压或温度并做出反应（环境故障保护 (EFP)），或者进行环境故障测试 (EFT)。对于第 4 级，现在需要 EFP 和故障注入保护。
- 第 4 级多重身份验证 (MFA) 要求。
- 模块开发生命周期的新保证要求，引入关键安全实践，如开发人员测试模块和使用自动安全诊断工具（例如静态分析）
- 非侵入式安全性是作为一项可选要求引入的，将涵盖针对侧信道攻击的测试指南。

2.3 解决方案二：管|车云数据传输

■ 参考《汽车密码应用技术要求》各项标准远程通信的要求，对于车云通信的密码应用有着较为清晰和统一的要求，满足本部分的合规性是较为容易的。

安全芯片

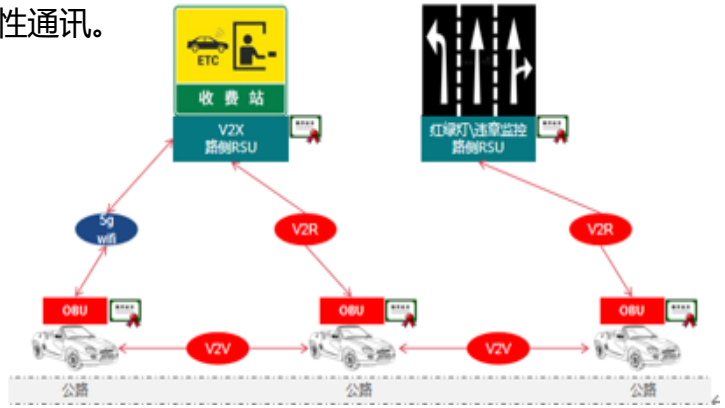
在车内中央网关预置安全芯片，初始化商用密码算法。

证书申请

车辆销售后，车主启动车辆，车载终端生成公私钥对及车辆基本信息发送云端，云端签名后，为车辆生成公钥证书。

证书应用：证书和假名证书

为保障车辆通信安全，车辆拥有车辆证书与短期假名证书。一般证书证书用于车云通信。假名证书用于保障车车、车路等临时性通讯。



2.4 解决方案三：云|车联网商用密码应用安全性评估

■ 依托信息系统等保定级进行密码测评：除密码算法、密码技术、密码产品和密码服务等通用要求外，从技术和管理两个层面对信息系统密码应用进行要求。以等保三级为例，共41项指标要求（1项“可”，14项“宜”，26项“应”），15个高风险项（用“★”表示）。

指标体系			高风险项	第一级	第二级	第三级	第四级
技术要求（70分）	物理和环境安全（10分）	身份鉴别	★	可	宜	宜	应
		电子门禁记录数据存储完整性		可	可	宜	应
		视频监控记录数据存储完整性		—	—	宜	应
	网络和通信安全（20分）	身份鉴别	★	可	宜	应	应
		通信数据完整性		可	可	宜	应
		通信过程中重要数据的机密性	★	可	宜	应	应
		网络边界访问控制信息的完整性		可	可	宜	应
		安全接入认证	★	—	—	可	宜
	设备和计算安全（10分）	身份鉴别	★	可	宜	应	应
		远程管理通道安全	★	—	—	应	应
		系统资源访问控制信息完整性		可	可	宜	应
		重要信息资源安全标记完整性		—	—	宜	应
		日志记录完整性		可	应	宜	应
		重要可执行程序完整性,重要可执行程序来源真实性		—	—	宜	应
	应用和数据安全（30分）	身份鉴别	★	可	宜	应	应
		访问控制信息完整性		可	可	宜	应
		重要信息资源安全标记完整性		—	—	宜	应
		重要数据传输机密性	★	可	宜	应	应
		重要数据存储机密性	★	可	宜	应	应
		重要数据传输完整性		可	宜	宜	应
		重要数据存储完整性	★	可	宜	宜	应
		不可否认性	★	—	—	宜	应

指标体系			高风险项	第一级	第二级	第三级	第四级
管理要求（30分）	管理制度（8分）	具备密码应用安全管理制度	★	应	应	应	应
		密钥管理规则		应	应	应	应
		建立操作规程		—	应	应	应
		定期修订安全管理制度		—	—	应	应
		明确管理制度发布流程		—	—	应	应
		制度执行过程记录留存		—	—	应	应
	人员管理（8分）	了解并遵守密码相关法律法规和密码管理制度		应	应	应	应
		建立密码应用岗位责任制度		—	应	应	应
		建立上岗人员培训制度		—	应	应	应
		定期进行安全岗位人员考核		—	—	应	应
		建立关键岗位人员保密制度和调离制度		应	应	应	应
	建设运行（8分）	制定密码应用方案	★	应	应	应	应
		制定密钥安全管理策略		应	应	应	应
		制定实施方案		应	应	应	应
		投入运行前进行密码应用安全性评估		可	宜	应	应
		定期开展密码应用安全性评估及攻防对抗演习		—	—	应	应
	应急处置（6分）	应急策略		可	应	应	应
		事件处置		—	—	应	应
		向有关主管部门上报处置情况		—	—	应	应

注释：应(应该)宜(建议)可(可以)

2.5 解决方案四：图|地理信息数据保护

■ **OBU、RSU 广播的地理信息相关数据（经度、纬度、高程）采用先偏转后加密。**

- 地图偏转：OBU采用中国测绘科学研究院插件对数据进行偏转，实现坐标系转换。
- 数据加密：所有位置相关消息（BSM、RSI、RSM、MAP）采用先偏转后加密，由路侧、车载终端对外广播。

- 31比特的纬度[-900000000,900000001]
- 32比特的经度[-1799999999,1800000001]
- 16比特的高程[-4096,61439]
- 采用基于SM4的FPE算法，对BSM、RSI、RSM、MAP中的位置信息加密，不增加编码后数据长度和取值空间

国密SM4算法和FPE模式

平台	经度（10万次）		纬度（10万次）	
	加密	解密	加密	解密
IMX6Q(cortex-a9，1.2G)	1.53秒	1.53秒	1.53秒	1.53秒

国内唯一具有密码测试能力的汽车检测机构

■ **软件测评中心是国家密码管理局批复的汽车商用密码检测机构，可合法合规的开展密码检测业务，牵头《汽车密码应用技术要求》等标准和配套实施标准，引领行业技术合规发展。**

具备商用密码检测机构资质

获得国家密码管理局颁发的**商用密码检测机构资质证书**，具备商用密码产品检测能力。

序号	机构名称	资质认定业务范围	有效截止日期
1	中汽研软件测评（天津）有限公司	商用密码产品检测：a智能密码钥匙，a智能IC卡。注：带有“a”的商用密码产品种类，具备GM/T 0028《密码模块安全技术要求》安全等级第二级及以下检测能力。安全芯片类商用密码产品具备GM/T 0008《安全芯片密码检测准则》安全等级第二级及以下检测能力。	2029-04-29

参与多项国行标准

序号	标准名称	标准属性	参与情况	归口单位	立项日期	发布日期
1	汽车密码应用技术要求/GB	国家标准	牵头	汽标委	24.12.31	26.10
2	车载信息交互系统密码检测规范	行业标准	参与	密标委	2021.9	25.8
3	V2X证书认证系统密码应用检测规范	行业标准	参与	密标委	2021.9	已发布

合作共赢

深度参与政策制定

支持国家密码管理局制定《车联网密码应用与安全性评估实施指南》，出台国内首家车载软件密码模块测试认证项目。

密码应用调研

支持编制指南


ICV密码保护演示


国密局来访调研

全面布局测试能力

密码应用合规性检测能力　商用密码算法检测能力　通信密码应用分析检测能力　车载板卡类产品检测能力
密码应用异常监测管理能力　密码运行监测可视化能力　源代码缺陷分析检测能力　整车密码应用仿真验证能力

中汽中心 | 检测

中汽研软件测评（天津）有限公司