# 车联网（智能网联汽车）密码支撑标准体系建设指南



2022 年 11 月

# 目录

# 前言

车联网（智能网联汽车）（以下简称车联网）是国家跨产业、跨行业融合的战略性新兴产业生态，我国高度重视车联网相关产业集群的发展。随着汽车的智能化、网联化程度越来越高，车联网也面临诸多安全风险。密码技术作为车联网安全保障的重要支撑，是解决车联网安全问题最有效、最可靠、最经济的手段。

为推动商用密码在车联网领域的应用，加快构建统一、科学、高效的车联网密码应用标准体系，发挥密码在维护车联网网络安全中的基础支撑作用，促进车联网产业健康发展，工业和信息化部组织制定《车联网（智能网联汽车）密码支撑标准体系建设指南》（以下简称《建设指南》）。

《建设指南》参考《国家车联网产业标准体系建设指南》，充分发挥标准在车联网密码支撑体系中的顶层设计和基础引领作用，从基础共性、智能网联汽车、信息通信、服务与平台、智能交通、密码应用管理与支撑等六个方面构建车联网密码应用标准体系，用于指导相关标准研制，为规范车联网产业密码应用、保障车联网安全、促进车联网产业发展提供支撑。

## 一、建设思路及目标

### （一）总体思路

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大、十九大和历次全会精神，贯彻党中央、国务院关于加快新型基础设施建设的决策部署，落实《中华人民共和国网络安全法》和《中华人民共和国密码法》，深入发挥密码在车联网安全中的核心保障和基础支撑作用，建立适应我国技术和产业发展需要的国家车联网密码支撑标准体系。

### （二）基本原则

**统筹规划，全面布局。**结合我国车联网产业和密码产业发展的现状及特点，发挥政府主管部门在顶层设计、组织协调和政策制定等方面的主导作用，制定政府引导和市场驱动相结合的标准体系建设方案，建立适合我国国情的车联网密码支撑标准体系。

**立足基础，急用先行。**依据产业急需程度，科学确定车联网密码支撑标准体系建设的重点方向，依托密码基础类标准，优先制定产业发展急需的相关标准，实现标准与车联网产业、密码产业发展的有机结合。

**多方参与，协同合作。**充分发挥标准化组织、科研机构、汽车企业、汽车技术服务企业、安全企业、密码企业等各方主体的力量，充分利用现有基础和成果，整合车联网产业和

密码产业现有资源，通力合作，共同构建车联网密码支撑标准体系。

（三）建设目标

到 2022 年，初步建立车联网密码标准体系，制修订相关标准 30 项，为开展车联网道路测试、车联网城市级验证示范等工作提供支撑。

到 2025 年，健全完善车联网密码标准体系，制修订覆盖人、车、路、云全维度的密码支撑标准 100 项，为车联网规模化应用提供安全保障。

## 二、建设内容

（一）车联网（智能网联汽车）密码支撑标准体系框架

车联网密码支撑标准体系包括基础共性、智能网联汽车、信息通信、服务与平台、智能交通、密码应用管理与支撑六大类标准。车联网密码支撑标准体系框架如图 1 所示。

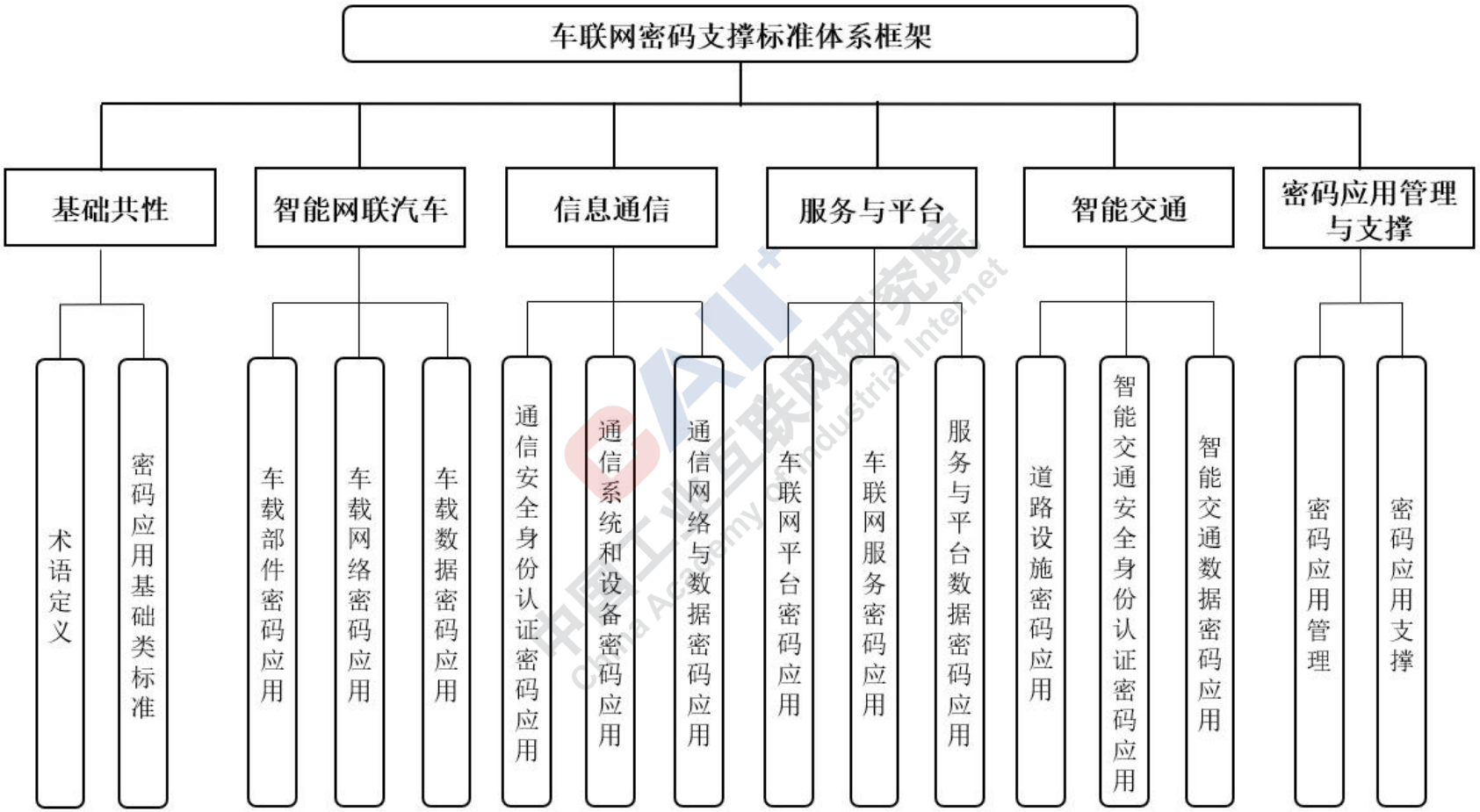


图 1 车联网（智能网联汽车）密码支撑标准体系框架

（二）重点标准化领域及方向

1. 基础共性标准

基础共性标准是车联网密码基础性、通用性、指导性标准，包括术语定义、密码基础类标准。如图 2 所示。

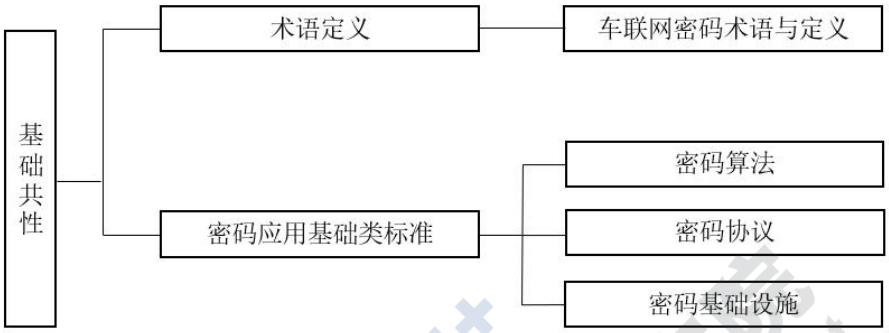


图 2 基础共性标准子体系

（1）术语定义标准

用于规范车联网密码相关概念，为其它各部分标准的制定提供支撑，包括车联网密码应用场景、技术、业务等主要概念定义、分类、相近概念之间关系等，避免不同行业间约定俗成不统一导致的理解歧义。

（2）密码应用基础类标准

用于规范车联网业务中应用的密码应用基础标准，包括密码算法、密码协议、密码基础设施等标准。

2. 智能网联汽车密码应用标准

用于规范车端密码应用与测评要求，主要包括车载部件密码应用、车载网络密码应用、车载数据密码应用标准等。如图 3 所示。

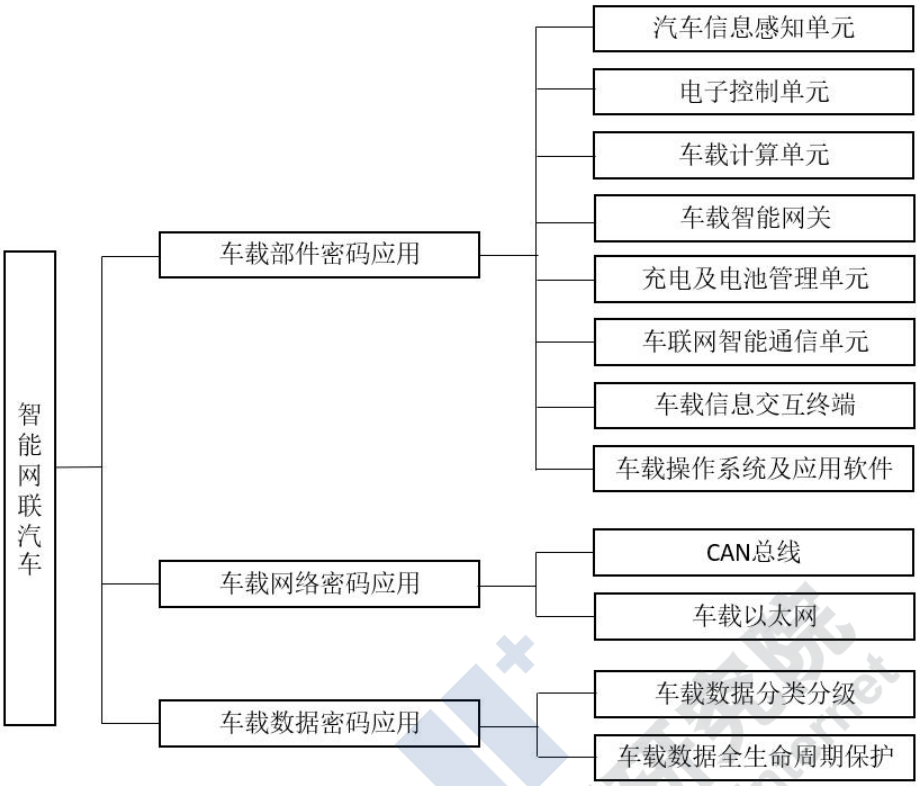


图 3 智能网联汽车标准子体系

（1）车载部件密码应用标准

用于规范关键车载部件中的密码应用要求与测评方法，主要包括汽车信息感知单元、电子控制单元、车载计算单元、车载智能网关、充电及电池管理单元、车联网智能通信单元、车载信息交互终端、车载操作系统及应用软件等密码应用与测评标准。

（2）车载网络密码应用标准

用于规范常见的车载网络中的密码应用要求与测评方法，主要包括控制器局域网络(Controller Area Network, CAN)、车载以太网等密码应用与测评标准。

（3）车载数据密码应用标准

用于规范车载数据保护中的密码应用要求与测评方法，主要包括车载数据分类分级、车载数据全生命周期保护等密码应用与测评标准。

3.信息通信密码应用标准

信息通信密码应用标准用于规范车联网主体之间通信相关的密码应用与测评要求，主要包括通信安全身份认证密码应用、通信系统和设备密码应用、通信网络与数据密码应用标准等。如图 4 所示。

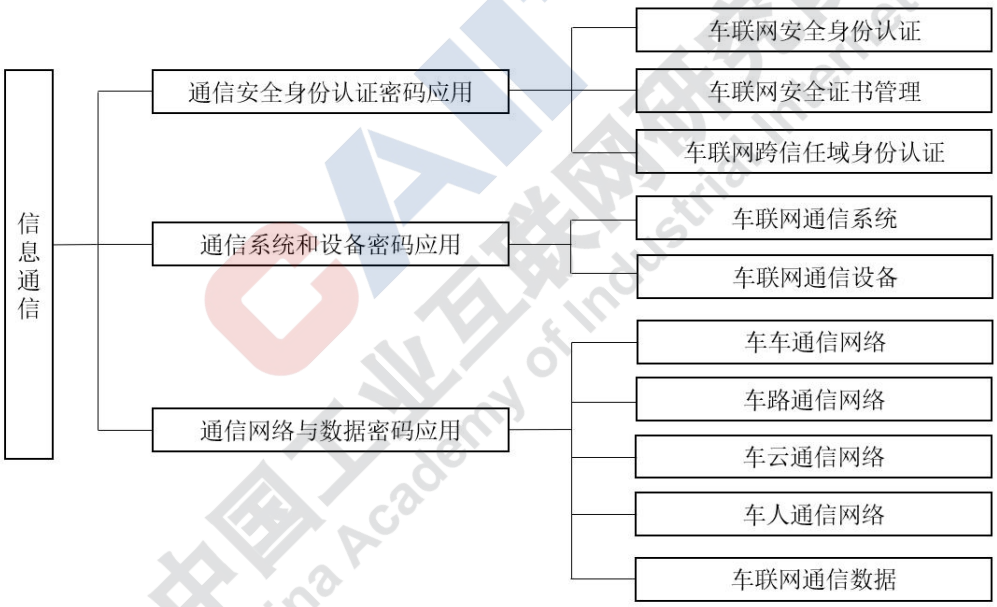


图 4 信息通信标准子体系

（1）通信安全身份认证密码应用标准

用于规范车联网通信安全身份认证系统的密码应用要求和测评方法，主要包括车联网安全身份认证、车联网安全证书管理、车联网跨信任域身份认证等密码应用与测评标准。

（2）通信系统和设备密码应用标准

用于规范车联网通信系统、车联网通信设备等产品和系统的密码应用要求和测评方法，主要包括车联网通信系统、车联网通信设备等密码应用与测评标准。

（3）通信网络与数据密码应用标准

用于规范车联网通信网络与数据密码应用要求和测评方法，主要包括车车（车与其他车辆）、车路（车与道路基础设施）、车云（车与云平台）、车人（车与行人）、车联网通信数据等通信网络与数据密码应用与测评标准。

4. 服务与平台密码应用标准

服务与平台密码应用标准用于规范实现车联网各个参与方协同工作的信息平台及平台提供的服务中的密码应用和测评要求，主要包括车联网平台密码应用、车联网服务密码应用、服务与平台数据密码应用标准等。如图 5 所示。

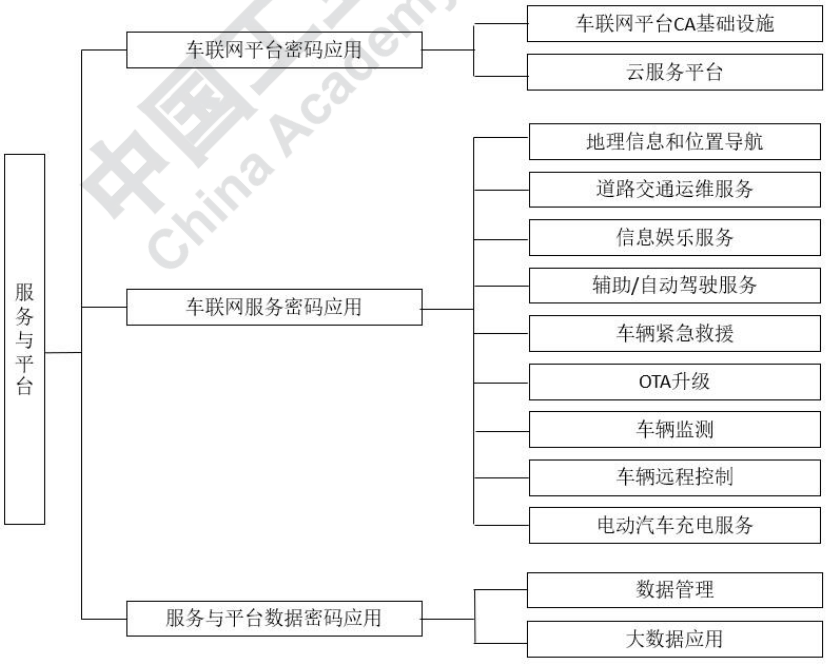


图 5 服务与平台标准子体系

（1）车联网平台密码应用标准

用于规范车联网相关平台的密码应用要求与测评方法，主要包括车联网平台CA基础设施、云服务平台等密码应用与测评标准。

（2）车联网服务密码应用标准

用于规范车联网提供的各类服务的密码应用要求与测评方法，主要包括地理信息和位置导航、道路交通运维服务、信息娱乐服务、辅助/自动驾驶服务、车辆紧急救援、OTA升级、车辆监测、车辆远程控制、电动汽车充电服务等密码应用与测评标准。

（3）服务与平台数据密码应用标准

用于规范车联网相关平台及服务数据密码应用要求与测评方法，主要包括数据管理、大数据应用等密码应用与测评标准。

5.智能交通密码应用标准

智能交通密码应用标准用于规范智能交通道路侧密码应用及测评要求，主要包括道路基础设施、智能交通安全身份认证、智能交通数据等密码应用及测评标准等。如图6所示。

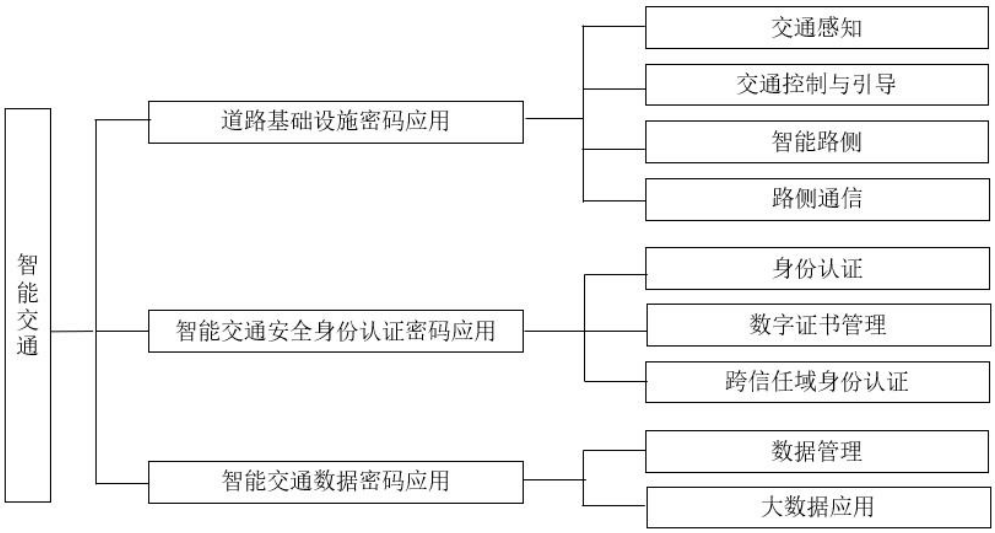


图 6 智能交通标准子体系

（1）道路基础设施密码应用标准

用于规范道路基础设施中的密码应用与测评要求，主要包括交通感知、交通控制与引导、智能路侧、路侧通信等密码应用与测评标准。

（2）智能交通安全身份认证标准

用于规范道路侧通信安全身份认证系统的密码应用要求与测评方法，主要包括交通设施身份认证、数字证书管理、跨信任域身份认证等密码应用与测评标准。

（3）智能交通数据密码应用标准

用于规范智能交通道路侧数据保护相关密码应用要求与测评方法，主要包括数据管理、大数据应用等密码应用与测评标准。

6. 密码应用管理与支撑标准

用于规范车联网密码应用管理与支撑相关的要求，包括密码应用管理、密码应用支撑等标准。

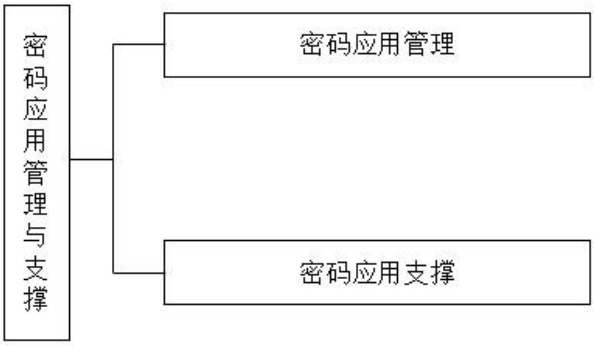


图 7 密码应用管理与支撑标准子体系

（1）密码应用管理

用于规范车联网密码应用相关管理要求，包括密码人员管理、密钥管理、建设运行、应急管理等标准。

（2）密码应用支撑

用于车联网密码应用相关支撑要求，包括风险评估、密码监测等标准。

## 三、组织实施

**一是实施动态更新。**实施动态更新完善机制，随着经济社会数字化转型持续推进、车联网密码应用认知与实践水平的提高，结合车联网密码应用相关法律法规的最新要求，适时滚动修订《建设指南》。

**二是推进标准研制。**组织行业协会及车联网企业、车企、电信运营商、密码应用企业、科研院所、高校等单位，按照

《建设指南》明确的标准研制路径，有序推进行业标准研制工作，注重车联网密码应用标准化工作与车联网密码应用最新研究成果、行业最佳实践的有机结合。

**三是加强宣贯实施。**充分发挥标准化组织、行业协会作用，组织相关专家开展标准研讨活动，通过培训、咨询、论坛等手段推进标准的宣贯。积极组织开展标准试点示范，形成最佳实践，促进标准在业界的应用推广。

**四是加强国际交流合作。**加强与国际标准化组织的交流与合作，积极参与国际标准化组织（ISO）、国际电工技术委员会（IEC）等国际标准化组织活动及国际标准研制。积极促进国内标准与国际接轨，推动国内先进标准向国际标准转化。

附件

# 车联网（智能网联汽车）密码相关标准项目明细表

| 序号 | 标准编号 | 标准名称 | 标准化组织 | 进展 | 项目性质 |
|---|---|---|---|---|---|
| **100 基础共性** | | | | | |
| **101 术语定义** | | | | | |
| 车联网密码术语与定义 | | | | | |
| 1. | / | 车联网密码术语与定义 | / | 待制定 | 推荐 |
| **102 密码应用基础类标准** | | | | | |
| 密码算法 | | | | | |
| 2. | / | 车联网隐式证书机制 | / | 待制定 | 推荐 |
| 3. | / | 车联网轻量级对称密码算法 | / | 待制定 | 推荐 |
| 4. | / | 车联网轻量级非对称密码算法 | / | 待制定 | 推荐 |
| 5. | / | 车联网轻量级密码杂凑算法 | / | 待制定 | 推荐 |
| 密码协议 | | | | | |
| 6. | / | 车联网证书注册协议 | / | 待制定 | 推荐 |
| 7. | / | 车联网数据传输安全协议 | / | 待制定 | 推荐 |
| 密码基础设施 | | | | | |
| 8. | / | 车联网证书认证系统技术要求 | / | 待制定 | 推荐 |
| 9. | / | 车联网网络信任体系构建指南 | / | 待制定 | 推荐 |
| **200 智能网联汽车** | | | | | |
| **201 车载部件密码应用** | | | | | |
| 汽车信息感知单元 | | | | | |
| 10. | / | 智能网联汽车 车载摄像头密码应用技术要求 | / | 待制定 | / |

| | | | | | |
|---|---|---|---|---|---|
| 11. | / | 智能网联汽车 车载雷达密码应用技术要求 | / | 待制定 | / |
| 电子控制单元 | | | | | |
| 12. | / | 智能网联汽车 电子控制单元密码应用技术要求 | / | 待制定 | / |
| 车载计算单元 | | | | | |
| 13. | / | 智能网联汽车 车载计算单元密码应用技术要求 | / | 待制定 | / |
| 车载智能网关 | | | | | |
| 14. | / | 智能网联汽车 车载智能网关密码应用技术要求 | / | 待制定 | / |
| 充电及电池管理单元 | | | | | |
| 15. | / | 智能网联汽车 充电单元密码应用技术要求 | / | 待制定 | / |
| 16. | / | 智能网联汽车 电池管理单元密码应用技术要求 | / | 待制定 | / |
| 车联网智能通信单元 | | | | | |
| 17. | / | 智能网联汽车 车载智能通信单元密码应用技术要求 | / | 待制定 | / |
| 车载信息交互终端 | | | | | |
| 18. | / | 智能网联汽车 信息娱乐终端密码应用技术要求 | / | 待制定 | / |
| 19. | / | 智能网联汽车 地图导航终端密码应用技术要求 | / | 待制定 | / |
| **202 车载网络密码应用** | | | | | |
| CAN 总线 | | | | | |
| 20. | / | 智能网联汽车 CAN 总线密码应用技术要求 | / | 待制定 | / |
| 车载以太网 | | | | | |
| 21. | / | 智能网联汽车 车载以太网密码应用技术要求 | / | 待制定 | / |
| **203 车载数据密码应用** | | | | | |
| 车载数据分类分级 | | | | | |
| 22. | / | 智能网联汽车 数据分类分级保护密码应用技术要求 | / | 待制定 | / |
| 车载数据全生命周期保护 | | | | | |
| 23. | / | 智能网联汽车 数据全生命周期保护密码应用技术要求 | / | 待制定 | / |

| 300 信息通信 | | | | | |
|---|---|---|---|---|---|
| **301 通信安全身份认证密码应用** | | | | | |
| 车联网安全身份认证 | | | | | |
| 24. | YD/T 0022-2019 | 基于 LTE 的车联网无线通信技术 安全认证测试方法 | 中国通信标准化协会 | 制定中 | 推荐 |
| 25. | / | 基于 5G 的车联网安全身份认证技术要求 | / | 待制定 | / |
| 车联网安全证书管理 | | | | | |
| 26. | YD/T 3957-2021 | 基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求 | 中国通信标准化协会 | 已发布 | 推荐 |
| 27. | / | 基于 5G 的车联网无线通信技术 安全证书管理系统技术要求 | / | 待制定 | / |
| 28. | / | 基于 5G 的车联网无线通信技术 安全认证技术要求 | / | 待制定 | / |
| 29. | / | 车联网 V2X 安全证书应用接口规范 | 工业和信息化部商用密码应用推进标准工作组 | 制定中 | 推荐 |
| 车联网跨信任域身份认证 | | | | | |
| 30. | / | C-V2X 安全认证系统跨域互认技术要求 | 中国通信标准化协会 | 制定中 | 推荐 |
| **302 通信系统和设备密码应用** | | | | | |
| 车联网通信系统 | | | | | |
| 31. | YD/T 3594-2019 | 基于 LTE 的车联网通信安全技术要求 | 中国通信标准化协会 | 已发布 | 推荐 |
| 32. | / | 车联网通信系统密码应用技术要求 | / | 待制定 | / |
| 车联网通信设备 | | | | | |
| 33. | / | 车联网通信设备密码应用技术要求 | / | 待制定 | / |
| **303 通信网络密码应用** | | | | | |
| 车车通信网络 | | | | | |
| 34. | / | 车车通信网络密码应用技术要求 | / | 待制定 | / |
| 车路通信网络 | | | | | |
| 35. | / | 车路通信网络密码应用技术要求 | / | 待制定 | / |
| 车云通信网络 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 36. | / | 车云通信密码应用基本要求 | 工业和信息化部商用密码应用推进标准工作组 | 编制中 | / |
| 37. | / | 车云通信网络密码应用技术要求 | / | 待制定 | / |
| 车人通信网络 | | | | | |
| 38. | / | 车人通信网络密码应用技术要求 | / | 待制定 | / |
| 车联网通信数据 | | | | | |
| 39. | YD/T 3751-2020 | 车联网信息服务 数据安全技术要求 | 中国通信标准化协会 | 已发布 | 推荐 |
| 40. | / | 车联网通信数据保护密码应用技术要求 | / | 待制定 | / |
| **400 服务与平台** | | | | | |
| **401 车联网平台密码应用** | | | | | |
| 车联网平台 CA 基础设施 | | | | | |
| 41. | / | 车联网证书认证系统部署实施指南 | / | 待制定 | 推荐 |
| 42. | / | 车联网证书互操作指南 | / | 待制定 | 推荐 |
| 云服务平台 | | | | | |
| 43. | / | 车联网云服务平台密码应用技术要求 | / | 待制定 | 推荐 |
| 44. | / | 车联网云控平台密码应用技术要求 | / | 待制定 | 推荐 |
| **402 车联网服务密码应用** | | | | | |
| 地理信息和位置导航 | | | | | |
| 45. | / | 地理信息和位置导航密码应用指南 | / | 待制定 | / |
| 道路交通运维服务 | | | | | |
| 46. | / | 道路交通信息服务密码应用指南 | / | 待制定 | / |
| 信息娱乐服务 | | | | | |
| 47. | GB/T 40856-2021 | 车载信息交互系统信息安全技术要求 | 全国汽车标准化技术委员会 | 已发布 | 推荐 |
| 48. | / | 信息娱乐服务密码应用指南 | / | 待制定 | 推荐 |

| | | | | | |
|---|---|---|---|---|---|
| 辅助/自动驾驶服务 | | | | | |
| 49. | / | 辅助/自动驾驶服务密码应用指南 | / | 待制定 | 推荐 |
| 车辆紧急救援 | | | | | |
| 50. | / | 车辆紧急救援系统密码应用指南 | / | 待制定 | 推荐 |
| OTA 升级 | | | | | |
| 51. | / | OTA 升级密码应用技术要求 | / | 待制定 | 推荐 |
| 车辆监测 | | | | | |
| 52. | / | 电动汽车远程服务与管理系统密码应用要求 | / | 待制定 | 推荐 |
| 车辆远程控制 | | | | | |
| 53. | / | 汽车远程监控系统密码应用要求 | / | 待制定 | 推荐 |
| 电动汽车充电服务 | | | | | |
| 54. | / | 电动汽车充电系统密码应用技术要求 | / | 待制定 | / |
| **403 服务与平台数据密码应用** | | | | | |
| 数据管理 | | | | | |
| 55. | / | 车联网服务与平台 数据分类分级保护密码应用技术要求 | / | 待制定 | 推荐 |
| 56. | / | 车联网服务与平台 数据全生命周期保护密码应用技术要求 | / | 待制定 | 推荐 |
| 大数据应用 | | | | | |
| 57. | / | 车联网平台大数据应用安全密码应用技术要求 | / | 待制定 | 推荐 |
| **500 智能交通** | | | | | |
| **501 道路基础设施密码应用** | | | | | |
| 交通感知 | | | | | |
| 58. | / | 交通信息采集密码应用技术要求 | / | 待制定 | 推荐 |
| 交通控制与引导 | | | | | |
| 59. | / | 车路协同 交通控制系统密码应用技术要求 | / | 待制定 | 推荐 |
| **502 智能交通安全身份认证密码应用** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 身份认证 | | | | | |
| 60. | / | 智能交通身份互认技术要求 | / | 待制定 | 推荐 |
| 数字证书管理 | | | | | |
| 61. | / | C-V2X 车联网证书策略与认证业务声明框架 | / | 待制定 | 推荐 |
| 跨信任域身份认证 | | | | | |
| 62. | / | 跨信任域身份认证证书验证要求 | / | 待制定 | 推荐 |
| **503 智能交通数据密码应用** | | | | | |
| 数据管理 | | | | | |
| 63. | / | 智能交通 数据分类分级保护密码应用技术要求 | / | 待制定 | 推荐 |
| 64. | / | 智能交通 数据全生命周期保护密码应用技术要求 | / | 待制定 | 推荐 |
| 大数据应用 | | | | | |
| 65. | / | 智能交通多方计算数据安全要求 | / | 待制定 | 推荐 |
| **600 密码应用管理与支撑** | | | | | |
| **601 密码应用管理** | | | | | |
| 66. | / | 车联网密码应用人员管理要求 | / | 待制定 | 推荐 |
| 67. | / | 车联网密码应用密钥管理要求 | / | 待制定 | 推荐 |
| 68. | / | 车联网 V2X 密钥管理系统技术规范 | 工业和信息化部商用密码应用推进标准工作组 | 制定中 | 推荐 |
| 69. | / | 车联网密码应用应急管理要求 | / | 待制定 | 推荐 |
| **601 密码应用支撑** | | | | | |
| 70. | / | 车联网密码应用安全评估要求 | / | 待制定 | 推荐 |
| 71. | / | 车联网密码应用安全监测平台通用技术要求 | / | 待制定 | 推荐 |