附件 1

车联网身份认证和安全信任试点工作要求

一、试点方向

（一）车与云安全通信

面向车与云服务平台通信场景，建立车云通信安全信任体系。

1. 技术要求

通过基于商用密码的数字证书、数字签名、数据加密技术，实现车载信息交互系统、汽车网关、C-V2X 车载通信设备等与车联网服务平台间的安全通信。基于安全链路协议，建立车云通信安全隧道，保护车云通信数据机密性和完整性。基于密码应用中间件，在车端实现消息封装、证书管理，在平台侧实现证书验证、数据解析。车载设备按照有关标准实现与证书管理系统、相关车联网安全信任根的数据交互。

2. 应用场景

在车端与车企云平台、路侧边缘云平台、智能辅助驾驶服务平台、车载信息服务云平台、高精动态地图服务平台等车联网服务平台的车云通信场景下，实现车辆可信接入、车辆定位及感知数据的可信采集、车辆状态信息的可信上传、汽车远程升级可信验证、基于安全链路的可信车云交互等车云通信应用。

3. 试点目标

试点单位研发建立车云通信身份认证、数据加密等技术能力，实现各类车云通信场景下的身份认证、数据机密性和完整性保护，构建车云通信安全保障能力。

（二）车与车安全通信

面向车与车直连通信场景，建立车车通信安全信任体系。

1. 技术要求

在车端应用基于商用密码的安全芯片、软件模块等组件，实现密钥管理、证书管理、安全计算等车端安全凭证管理和数据处理功能。通过

车辆生产环节配置、运营商通道配置、服务器令牌授权等方式实现车载设备证书初始化。建立车载设备证书管理系统，为车载设备提供证书发布、更新、撤销等证书管理服务。车载设备按照有关标准实现与证书管理系统、相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台的数据交互。

2. 应用场景

在重点城市、高速公路、物流园区、港口、矿山、科技园区等场景下，实现基于安全通信的辅助驾驶和有条件自动驾驶应用，包括碰撞预警、盲区预警、变道辅助、异常车辆提醒、编队行驶等。

3. 试点目标

试点单位研发建立车车通信身份认证技术能力，对具备直连通信功能的 C-V2X 车型进行证书管理，通过接入相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台，在车辆驾驶应用场景中开展跨信任域的身份认证，保障多品牌车辆的安全通信，构建车车通信安全保障能力。

（三）车与路安全通信

面向车与路侧设施直连通信场景，建立车路通信安全信任体系。

1. 技术要求

路侧设备通过搭载基于商用密码的安全芯片、软件模块等组件，实现安全凭证管理和数据处理功能。建立路侧设备证书管理系统，为路侧设备提供证书发布、更新、撤销等证书管理服务。路侧设备按照有关标准实现与车载设备、证书管理系统、相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台的数据交互。

2. 应用场景

在重点城市、高速公路、封闭测试场、车路协同试点路段等场景下，实现基于安全通信的安全预警、效率提升等车路协同应用，包括红绿灯提醒及绿波通行、道路交通信息提示、弱势交通参与者提醒、公交优先通行、自动驾驶测试等。

3. 试点目标

试点单位研发建立车路通信身份认证技术能力，对试点区域具备直连通信能力的 C-V2X 通信设备进行证书管理，通过接入相关车联网安全信任根和工业和信息化部车联网安全信任根管理平台，开展跨信任域的身份认证，保障本区域多类路侧设备与车辆的车路安全通信，构建车路通信安全保障能力。

（四）车与设备安全通信

面向车与设备通信场景，建立车与设备通信安全信任体系。

1. 技术要求

通过基于商用密码的数字证书、数字签名、数据加密技术，实现车载信息交互系统与手持移动智能终端、新能源汽车与充电桩等车与外部设备交互场景的安全通信。基于商用密码技术，实现车载短距无线通信场景中的密钥可信交换和安全保护，采用安全协议对通信链路进行加密。

2. 应用场景

实现基于身份认证和加密技术的车与设备通信应用，包括用户手持移动智能终端的车辆远程控制、车辆信息查询、安全预警等应用，无钥匙进入、车载设备互联等车载短距无线通信应用，以及新能源汽车充电应用等。

3. 试点目标

试点单位研发建立身份认证、安全加固等技术能力，支持各类车与设备通信场景下的身份认证、数据机密性和完整性保护，构建车与设备通信安全保障能力。

二、试点申报要求

（一）申报主体。基础电信企业、互联网企业、汽车生产企业、电子零部件企业、网络安全企业、商用密码企业、交通运输企业、科研院所，以及网络安全创新应用先进示范区、国家级车联网先导区、国家智能网联汽车测试示范区（基地）、智慧城市基础设施与智能网联汽车协同发展试点城市等的建设运营单位等。

（二）申报资格。由具备车联网身份认证管理和运营能力的单位作为牵头单位，联合相关产业链主体（牵头单位 1 家，联合单位不超过 10 家）联合进行申报。申报主体应在中华人民共和国境内注册、具备独立法人资格，具有较好的技术研发和融合创新能力。单一申报主体牵头的试点项目总数原则上不超过 2 个。

（三）技术要求。试点项目符合《基于 LTE 的车联网通信技术 安全总体技术要求》《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》《信息安全技术 信息系统密码应用基本要求》《信息安全技术 公钥基础设施 数字证书格式》《信息安全技术 证书认证系统密码及相关安全技术》《车联网无线通信安全技术指南》《车联网信息服务平台安全防护技术要求》《车联网信息服务 数据安全技术要求》《车联网信息服务 用户个人信息保护要求》等要求。试点项目不涉及需要第三方认证的电子认证服务。

（四）安全保障。试点单位要落实网络安全主体责任，健全完善企业网络安全管理制度，针对参与试点相关整车及关键部件、车联网平台、车联网 APP、数据和用户个人信息，在防攻击、防病毒、防入侵、防控制、防窃取等方面落实网络安全防护要求。涉及商用密码应用的，按照《中华人民共和国密码法》有关要求，加强商用密码应用安全性评估。

（五）各省、自治区、直辖市工业和信息化主管部门、通信管理局和中央企业集团公司可进行推荐。

三、工作流程

（一）申报方式。申报主体于 2021 年 7 月 1 日前将车联网身份认证和安全信任试点申报书一式三份及电子版报联盟秘书处。由各地工业和信息化主管部门、通信管理局和中央企业集团公司推荐的申报主体，申报书需加盖推荐单位印章。

（二）组织实施。工业和信息化部遴选符合要求的项目开展试点工作。试点牵头单位制定试点实施方案和计划，开展技术验证和联调测试，于 2022 年 6 月底前完成试点项目任务。试点牵头单位建立工作机制，

加强组织协调，有序推进试点工作。工业和信息化部和试点推荐单位加强对试点工作的指导，并组织对试点项目进行评价。

（三）支撑保障。成立车联网身份认证和安全信任工作专家委员会，为试点工作提供技术支持和咨询。中国信息通信研究院、中国工业互联网研究院、国家工业信息安全发展研究中心、中国电子信息产业发展研究院、工业和信息化部装备工业发展中心、中国汽车技术研究中心有限公司、国汽（北京）智能网联汽车研究院有限公司、中国通信学会、中国通信标准化协会、中国汽车工业协会、车载信息服务产业应用联盟等第三方专业机构负责试点支撑工作。

（四）退出程序。试点单位因自身原因决定终止试点工作的，提出退出申请，经工业和信息化部（网络安全管理局）批准后启动试点退出。试点单位存在责任落实不到位、经营服务出现重大问题、造成重大网络安全事件、严重违法违规等行为，取消其试点资格。退出试点的单位，需妥善处理善后事宜。

（五）试点总结。试点牵头单位会同参与单位对试点情况、主要做法、经验成效、存在的问题、车联网身份认证管理规范和流程建议等进行总结，形成书面材料，于 2022 年 6 月底前报工业和信息化部（网络安全管理局）及试点推荐单位。