编号：CCIDCCICV-0101-1-2022

智能网联汽车网络安全管理体系
认证申请书

申请方（甲方）：_____

认证方（乙方）：北京赛迪认证中心有限公司

郑 重 声 明

本公司自愿选择北京赛迪认证中心有限公司（以下简称：赛迪认证/CCIDCC）作为我组织管理体系认证机构。我公司郑重声明遵守如下要求：

1、 已从赛迪认证/-获取《公开文件》，并承诺始终遵守国家相关职能管理机构及赛迪认证/对认证的有关规定；

2、 为审核做出必要的安排，包括为进行授予、保持认证和/或解决投诉、非例行监督检查提供文件、开放所有区域、提供真实记录；

3、 仅就获准认证的范围做相应的宣传，宣传认证结果时绝不损害赛迪认证/CCIDCC 的声誉。不做使赛迪认证/CCIDCC 认为误导或未授权的声明；

4、 当接到暂停或撤销认证通知时,立即停止涉及认证内容的广告和宣传，并按赛迪认证/CCIDCC 的要求交回所有认证文件（证书和标志）；

5、 认证结果只能用来证明我公司管理体系符合了特定标准或其它规范性文件，不用认证结果来暗示本组织某一类产品或服务得到赛迪认证/CCIDCC 批准；用不产生误导的方式使用或部分使用认证文件、标志或报告；在传播媒体中（例如文件、小册子或广告）对认证内容的引用，符合赛迪认证/CCIDCC 的要求；

6、 承担双方协商的审核过程所发生的一切费用，按时缴纳认证费用；

7、 本公司认证体系相关的信息发生重大变化、发生质量事故时及时通知赛迪认证/CCIDCC；

8、 本表所填写内容及所提供的资料均真实有效，如有虚假，将承担由此带来的一切后果！

以上声明与认证合同同具法律效力！

申请方最高管理者/授权代表： 申请方公章 ：

日期： 年 月 日

一、申请方信息：

*申请组织名称: _____ *法人代表：_____

*注册地址：_____

*生产/经营地址：_____

*办公地址：_____

通讯地址:_____

*联系人：_____*电话：_____

*手 机：_____ *E-mail:_____

* 公司邮箱:_____*公司网址：_____

***为必填项，如果没有请填写无，E-mail很重要，请务必填写。**

二、申请方基本情况调查：

领域	认证标准
□智能网联汽车网络安全管理体系 （UNECE WP.29 Regulation No.155-《Cyber security and cyber security management system》及 ISO SAE 21434《Road vehicles-Cybersecurity engineering》）	
认证类型	□初次申请 □再认证第__次 □再认证超期，申请恢复 □ 认证证书转换 □其它：
申请组织基本概况	1）申请组织经济性质： □国有 □集体 □乡镇 □民营 □股份制 □外资 □合资 □其它：_____ 2）体系有效人数_____人 (1)是否存在相同多条生产线：○否 ○是 (2)生产线数量___条，涉及人数：___ 人 (3)公司是否采取轮班○否 ○是，实行_____班制； 每班人数约_____ 人；是否涉及夜班作业 ○否 ○是 3）是否已建立 GB/T 19001/ISO 9001 质量管理体系○否 ○是 是否已建立 GB/T 24405.1/ISO27001 信息技术服务管理体系○否 ○是 4）是否建立了文件化的管理体系： □尚未建立 □已建立，文件化管理体系自___年__月___日开始有效运行。 5）是否聘请咨询机构建立体系：□否 □是（咨询机构及人员：_____） 6）申请产品执行的标准：□有 □无 □ 国标，标准号：_____ □ 行标，标准号：_____ □ 企标，标准号：_____企标是否备案 ○是，备案号：_____○否 □ 其他（如：客户标准、内部服务规范等_____

	7）是否涉及同一组织多个企业名称、固定多场所、临时场所： □ 存在多场所，见《受审核组织多场所清单》。 固定多场所是否需要子证书 ○否 ○是 □存在同一组织多个企业名称、且需在认证范围中表述的情况,填写《受审核组织多场所清单》 是否需要子证书 ○否 ○是 8）近两年内是否发生重大质量/环境/安全事故/媒体曝光： □从未发生 □有发生，需简述事故发生及处置情况（另附页） 9）本次申请认证范围： （1）智能网联汽车网络安全管理体系覆盖的产品范围及主要过程（指设计/开发、生产/施工、安装、服务等活动）：_____
曾获其他认证机构认证证书组织概况	1）是否曾获其他机构体系认证： □否 □是，曾获：○QMS ○EMS ○OHS ○其他 2）曾获管理体系认证证书认证机构名称：_____， 现认证证书状态： □有效 □失效 □暂停 □撤消 3）申请认证转换的理由：_____ 4）一年内是否被其他机构暂停、撤消： □否 □是（请提供暂停、撤消通知书） 5）接受其它认证机构审核，但未通过：□否 □是，认证机构名称：_____，未通过原因：_____

三、申请方智能网联汽车网络安全管理能力建设自查：

<table>
<tr><td colspan="5">一、车联网网络安全管理机构设置</td></tr>
<tr><td>1、车联网网络安全主管领导</td><td colspan="2"></td><td>职务</td><td></td></tr>
<tr><td rowspan="5">2、车联网网络安全管理机构</td><td>机构名称</td><td colspan="3"></td></tr>
<tr><td>机构性质</td><td colspan="3">☐专职机构 ☐兼职机构
(专职机构指专门为履行安全管理职能而设立的独立机构，兼职机构指除安全管理职能外还兼其他业务职能的机构)</td></tr>
<tr><td>机构负责人姓名</td><td></td><td>职务</td><td></td></tr>
<tr><td>机构职责</td><td colspan="3">（请分条说明机构主要职责）</td></tr>
<tr><td colspan="4">跨部门的网络安全机制建设情况：
☐有面向车联网网络安全的专门组织机构，开展跨部门的网络安全工作；
☐有面向车联网网络安全的专门组织机构，但没有跨部门的组织机构；
☐各部门分散处理车联网网络安全方面的工作，没有跨部门的工作机制。</td></tr>
<tr><td colspan="5">二、车联网网络安全管理人员配备情况</td></tr>
<tr><td rowspan="4">1、车联网网络安全人员情况</td><td>车联网网络安全机构人员数量</td><td colspan="3"></td></tr>
<tr><td>专/兼职情况</td><td colspan="3">专职安全人员_____人；
兼职安全人员_____人；</td></tr>
<tr><td>专业背景</td><td colspan="3">安全相关专业_____人，如计算机、信息安全、网络安全等；</td></tr>
<tr><td>技能背景</td><td colspan="3">持有安全相关资质共_____人，分别包括_____资质（分别列出，如cisp、cissp、等保测评等资质各多少人）；</td></tr>
</table>

<table>
<tr><td rowspan="3"></td><td rowspan="3">人员培训情况</td><td>培训频次</td></tr>
<tr><td>最近培训日期及范围</td></tr>
<tr><td>考核方式及内容</td></tr>
<tr><td colspan="3">三、车联网网络安全投入情况——网络安全占车联网相关投入规模及比例</td></tr>
<tr><td colspan="2">1、车联网相关信息化、智能化近三年平均年度投入规模</td><td>□0~100w □100~500w
□500~1000w □1000w~2000w
□2000w 以上</td></tr>
<tr><td colspan="2">2、车联网网络安全投入规模</td><td>□0~10w □10~20w □20~50w
□50w~100w □100w 以上</td></tr>
<tr><td colspan="2">3、车联网网络安全投入占车联网信息化投入比例</td><td>□0~1% □1%~3% □3%~5%
□5%~10% □10%以上</td></tr>
<tr><td colspan="4">四、企业车联网网络安全管理制度建设情况</td></tr>
<tr><td rowspan="11">现已制定实施的网络安全相关管理制度名称及主要内容</td><td>制度类别</td><td>制度名称</td><td>主要内容</td></tr>
<tr><td>总体网络安全方针</td><td></td><td></td></tr>
<tr><td>机构和人员管理类</td><td></td><td></td></tr>
<tr><td>供应链安全类</td><td></td><td></td></tr>
<tr><td>安全运维类</td><td></td><td></td></tr>
<tr><td>安全建设类</td><td></td><td></td></tr>
<tr><td>安全开发设计类</td><td></td><td></td></tr>
<tr><td>安全教育培训类</td><td></td><td></td></tr>
<tr><td>应急响应类</td><td></td><td></td></tr>
<tr><td>设备及系统安全管理类</td><td></td><td></td></tr>
<tr><td>其他安全管理类</td><td></td><td></td></tr>
<tr><td colspan="4">五、企业供应链安全管理建设情况</td></tr>
<tr><td colspan="2">供应链安全管理和责任划分情况</td><td colspan="2">是否对供应商进行网络安全要求和责任划分？
□是 □否
如有，说明如何对供应商进行网络安全要求和责任划分，描述涉及到的产品与功能，如 IVI、T-box、ECU 等关键零部件</td></tr>
<tr><td colspan="4">六、企业车联网网络安全应急管理机制建设情况</td></tr>
<tr><td rowspan="2">1、监测预警和信息通报</td><td>网络安全事件监测预警工作机制</td><td colspan="2">□已建立 □未建立 □未建立，但有建立计划
建设情况简述：</td></tr>
<tr><td>网络安全信息通报机制</td><td colspan="2">□已建立 □未建立 □未建立，但有建立计划</td></tr>
</table>

		建设情况简述：	
	网络安全监测预警技术平台	□已建设 □未建设 □未建设，但有建设计划 建设情况简述（含监测内容）：	
	网络安全事件监测方式	□人工监测 □系统监测 □第三方监测 建设情况简述：	
	网络安全事件监测情况	近三年至今安全事件共监测发现_____起。其中： 特别重大事件_____起； 重大事件_____起； 较大事件_____起； 一般事件_____起。 (事件定级可参照《国家网络安全事件应急预案》)	
	网络安全事件处置流程		
2、安全管理基本策略	网络安全规划	□已制定（制定时间： 年 月） □未制定 □未制定，但有制定计划 建设情况简述：	
	网络安全应急预案	□已制定（制定时间： 年 月） □未制定 □未制定，但有制定计划 建设情况简述：	
		应急预案培训周期及次数	
		应急预案框架构成（如启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。）	

		应急评估、修订周期及次数	
3、网络安全应急演练	上年度演练情况	是否制定演练计划	□是 □否
		演练次数	□企业级，次数：_____ □部门级，次数：_____
	本年度演练情况	是否制定演练计划	□是 □否
		计划演练次数	□企业级，次数：_____ □部门级，次数：_____
	应急演练过程中发现问题的整改情况		
七、车联网网络安全风险评估情况			
1、风险评估对象	□整车 □T-BOX/IVI □OTA □APP □关键 ECU___ □平台 □其它 □无		
2、风险评估方法	□EVITA □HEAVENS □其它____		
3、风险评估参考标准			
4、风险评估流程涵盖环节	□资产识别 □威胁场景识别 □影响评级 □脆弱性分析 □攻击路径分析 □攻击可行性评估 □风险判定与风险处置 □其它____		
5、风险评估实施方	□自评估，实施团队及职责分工： □第三方风险评估，实施团队及职责分工：		
6、风险评估数据库	□资产库 □威胁场景库（来源_____） □漏洞库（来源_____） □其它_____		

7、风险接受与处置	风险接受准则	
	风险处置原则及流程	
8、说明残余风险评估处理方式		

五、车型网络安全开发流程		
是否考虑网络安全因素	输入	输出
□概念设计阶段		
□研发阶段		
□生产阶段		
□运营阶段		
□维护阶段		
□报废阶段		

八、车型网络安全测试验证情况及结果	
1、硬件网络安全测试	□自身开展测试 □产品供应商测试 □委托第三方测试 □供应商测试，并自身进行测试验证 □未开展测试 测试对象_____
2、软件网络安全测试	□自身开展测试 □产品供应商测试 □委托第三方测试 □供应商测试，并自身进行测试验证 □未开展测试 测试对象_____
3、系统集成网络安全测试	□自身开展测试 □产品供应商测试 □委托第三方测试 □供应商测试，并自身进行测试验证 □未开展测试 测试对象_____
4、整车网络安全测试验	□自身开展测试 □产品供应商测试 □委托第三方测试 □供应商测试，并自身进行测试验证 □未开展测试 测试对象_____
5、网络安全测试验证结果及处理原则	

九、车联网安全漏洞跟踪与处置	
1、漏洞跟踪机制	是否建立漏洞跟踪机制：☐是 ☐否 漏洞来源：☐CVE ☐CNVD ☐CNNVD ☐其他 漏洞跟踪流程概述 （包括跟踪流程、跟踪机构等）
2、漏洞处置机制	是否建立相应的漏洞处置流程：☐是 ☐否 漏洞验证主体：☐主机厂 ☐供应商 ☐无 漏洞处置主体：☐主机厂 ☐供应商 ☐无 是否对跟踪漏洞进行处置：☐是 ☐否 已处置漏洞列举 漏洞处置机制概述（包括处置流程、处置机构、处置记录等）

附表：申请方提供的文件清单（三-能力建设自查的证明材料）

序号	文件名称	覆盖的标准条款