

编号：CCIDCCICV-0101-2022

智能网联汽车网络安全管理体系 认证实施规则

北京赛迪认证中心有限公司

2022年3月

2022-3-30 发布

2022-3-30 实施

目录

1 适用范围	1
2 认证依据	1
3 认证程序	2
4 认证证书	16
5 认证记录管理	17
6 受理组织申诉	18

1 适用范围

1.1 本规则用于规范认证机构在中国境内开展智能网联汽车网络安全管理体系认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，对智能网联汽车网络安全管理体系认证实施过程做出具体规定，明确认证机构对认证过程的管理责任，保证智能网联汽车网络安全管理体系认证活动的规范有效。

1.3 本规则是认证机构在智能网联汽车网络安全管理体系认证活动中的基本要求，认证机构在该项认证活动中应当遵守本规则。

2 认证依据

2.1 智能网联汽车网络安全管理体系认证以 UNECE WP.29 Regulation No.155-《Cyber security and cyber security management system》及 ISO SAE 21434《Road vehicles-Cybersecurity engineering》为认证依据。

2.2 认证能力、内部管理和工作体系符合 GB/T 27021/ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求》。

2.3 建立内部制约、监督和责任机制，实现培训（包括相关增值服务）、审核和做出认证决定等工作环节相互分开，

符合认证公正性要求。

3 认证程序

3.1 认证申请与受理

3.1.1 认证机构应向申请认证的社会组织（以下简称申请组织）至少公开以下信息：

- （1）认证范围；
- （2）认证程序；
- （3）认证依据；
- （4）本规则的完整内容；
- （5）认证证书样式及内容；
- （6）对认证过程的申投诉规定。

3.1.2 认证机构应当要求申请组织至少提交以下资料：

- （1）认证申请书，申请书应包括申请认证的生产、经营或服务活动范围及活动情况的说明；
- （2）法人资格证明（工商营业执照、事业单位法人证书或社会团体法人登记证书）；
- （3）智能网联汽车网络安全管理体系覆盖的活动所涉及法律法规要求的行政许可文件、资质证书、强制性认证证书等的复印件（适用时）；
- （4）已按认证依据和相关要求建立和实施了文件化的智能网联汽车网络安全管理体系；

(5) 智能网联汽车网络安全管理体系有效运行 3 个月以上，并且已完成内部审核和管理评审。

(6) 智能网联汽车网络安全管理体系成文信息(适用时)。

3.1.3 认证机构应对申请组织提交的申请资料进行评审，根据申请认证的活动范围及场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，认证机构不应受理其认证申请。

3.1.4 对符合 3.1.2、3.1.3 要求的，认证机构可决定受理认证申请；对不符合上述要求的，认证机构应通知申请组织补充和完善，或者不受理认证申请。

3.1.5 在实施认证审核前，认证机构应与申请组织订立具有法律效力的书面认证合同，合同应至少包含以下内容：

(1) 申请组织获得认证后持续有效运行智能网联汽车网络安全管理体系的承诺；

(2) 申请组织对遵守认证认可相关法律法规，协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺；

(3) 申请组织承诺获得认证后发生以下情况时，应及时

向认证机构通报：

- ①客户及相关方有重大投诉；
- ②生产、销售的产品或提供的服务被质量或市场监管部门认定不合格；
- ③发生产品和服务的质量安全事故；
- ④相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格、强制性认证或其他资质证书变更；法定代表人、最高管理者变更；生产经营或服务的工作场所变更；智能网联汽车网络安全管理体系覆盖的活动范围变更；智能网联汽车网络安全管理体系和重要过程的重大变更等；
- ⑤出现影响智能网联汽车网络安全管理体系运行的其他重要情况。

(4) 申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息，不利用智能网联汽车网络安全管理体系认证证书和相关文字、符号误导公众认为其产品或服务通过认证；

(5) 拟认证的智能网联汽车网络安全管理体系覆盖的生产或服务的活动范围；

(6) 在认证审核实施过程及认证证书有效期内，认证机构和申请组织各自应当承担的责任、权利和义务；

(7) 认证服务的费用、付费方式及违约条款。

3.2 审核前准备

3.2.1 认证机构应根据认证依据、程序等要求，及时对申请组织提交的申请文件和资料进行评审并保存评审记录，以确保：

- (1) 申请组织及其管理体系的信息充分，可以进行审核；
- (2) 认证要求已有明确说明并形成文件，且已提供给申请组织；
- (3) 解决了认证机构与申请组织之间任何已知的理解差异；
- (4) 认证机构有能力并能够实施认证活动；
- (5) 考虑了申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；

3.2.2 认证机构应制定详实的审核计划，包括以下方面：

(1) 审核时间：

为确保认证审核的完整有效，认证机构根据申请组织智能网联汽车网络安全管理体系覆盖的活动范围、特性、技术复杂程度、安全风险程度、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成审核工作需要的时间

(2) 审核组：

① 认证机构应当根据智能网联汽车网络安全管理体系覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，必要时可以选择技术专家参加审核组。

②审核组中的审核员承担审核任务和责任。技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

③审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

(3) 审核计划：

认证机构应为每次审核制定书面的审核计划。审核计划至少包括以下内容：审核目的，审核准则，审核范围，现场审核的日期和场所，现场审核持续时间，审核组成员。

在审核活动开始前，审核组应将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

3.3 审核实施

3.3.1 初次认证审核，分为第一、二阶段实施审核。

(1) 第一阶段审核

①确认申请组织实际情况与智能网联汽车网络安全管理体系成文信息描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、生产或服务过程等是否与申请组织的实际情况相一致。

②审核申请组织理解和实施相关标准及规则要求的情

况，评价智能网联汽车网络安全管理体系运行过程中是否实施了内部审核与管理评审，确认智能网联汽车网络安全管理体系是否已运行并且超过 3 个月。

③确认申请组织建立的智能网联汽车网络安全管理体系覆盖的活动内容、范围、过程和场所，遵守适用的法律法规及强制性标准的情况。

④评价申请组织的运作场所和现场的具体情况，并与申请组织的人员进行讨论，以确定第二阶段审核的准备情况。审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节。

⑤对智能网联汽车网络安全管理体系成文信息不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

(2) 第二阶段审核

第二阶段审核应在具备实施认证审核的条件下在申请组织的场所进行。如果第一阶段审核提出影响实施第二阶段审核的问题，这些问题应在第二阶段审核前得到解决。第二阶段审核的目的是通过在申请组织的现场进行系统、完整地审核，评价申请组织的智能网联汽车网络安全管理体系是否满足所有适用的认证依据的要求，并判断是否推荐认证注册。应重点关注申请组织是否充分识别了智能网联汽车网络安

全管理过程的重要性，并证实与申请组织的智能网联汽车网络安全活动是相适应的。具体包括：

①在相关职能、层次和过程上建立安全目标是否具体适用、可测量并得到沟通、监视。

②对智能网联汽车网络安全管理体系覆盖的过程和活动的管理及控制情况。

③申请组织实际工作记录是否真实。对于审核发现的真实性存疑的证据应予以记录并在做出审核结论及认证决定时予以考虑。

④申请组织的内部审核和管理评审是否有效。

(3) 智能网联汽车网络安全管理体系文件与其他管理体系文件的结合审核（适用时）

若智能网联汽车网络安全管理体系以及与其他管理体系的适当接口能够清楚地被识别，可以允许申请组织将智能网联汽车网络安全管理体系文件与其他管理体系文件（例如，GB/T 19001/ISO 9001 质量管理体系、GB/T 24405.1/ISO27001 信息技术服务管理体系等）相结合。

可以把智能网联汽车网络安全管理体系的审核和其他管理体系的审核相结合，但是这种结合必须以审核活动满足智能网联汽车网络安全管理体系认证所有要求为前提，并且审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与智能网联汽车网络安全管理体系有关

的重要要素的描述并易于识别。

3.3.2 发生以下情况时，审核组应向认证机构报告，经认证机构同意后终止审核。

- (1) 受审核方对审核活动不予配合，审核活动无法进行。
- (2) 受审核方实际情况与申请材料有重大不一致。
- (3) 其他导致审核程序无法完成的情况。

3.4 审核报告与结论

3.4.1 审核组应对第一阶段和第二阶段审核中收集的所有信息和证据进行汇总分析，形成书面审核报告并就审核结论达成一致，由审核组组长签字。其中，审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

- (1) 申请组织的名称和地址。
- (2) 申请组织活动范围和场所。
- (3) 审核的类型、准则和目的。
- (4) 审核组组长、审核组成员等。
- (5) 审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。
- (6) 识别出的不符合项。
- (7) 审核组对是否通过认证的意见建议。

3.4.2 认证机构应保留用于证实审核报告中相关信息的证据。

3.4.3 认证机构应在做出认证决定后 30 个工作日内将审核报告提交申请组织，并保留签收或提交的证据。

3.4.4 对终止审核的项目，审核组应将已开展的工作情况形成报告，认证机构应将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

3.5 不符合项的纠正和纠正措施及其结果的验证

3.5.1 对审核中发现的不符合项，认证机构应要求申请组织分析原因，并提出纠正和纠正措施。对于严重不符合，应要求申请组织在最多不超过 6 个月期限内采取纠正和纠正措施。认证机构应对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。如果未能在第二阶段结束后 6 个月内验证对严重不符合实施的纠正和纠正措施，则应按 3.6.5 条处理，或者重新实施 3.3.1 第二阶段审核。

3.6 认证决定

3.6.1 认证机构应该在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，做出认证决定。

3.6.2 认证决定人员应为认证机构管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

3.6.3 应该以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实申请组织建立智能网联汽车网络安全管理体系的管理评审和内部审核的方案已经得到有效实施并且将得到保持，才可决定申请组织通过认证。

3.6.4 对于通过认证的申请组织，向其颁发智能网联汽车网络安全管理体系认证证书。

3.6.5 对于未通过认证的申请组织，应以书面形式明确说明其不能通过认证的原因。

3.6.6 认证机构在颁发认证证书后，应当按照规定的要求将认证结果相关信息进行公示并报送国家认监委。

3.7 监督审核

3.7.1 认证机构应对持有其颁发的智能网联汽车网络安全管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行智能网联汽车网络安全管理体系并符合认证要求。

3.7.2 为确保达到 3.7.1 条要求，认证机构应在满足认可要求的基础上，根据获证组织智能网联汽车网络安全管理体系覆盖的业务活动的特点以及所承担的风险，合理设计和确定监督审核的时间间隔和频次。当获证组织智能网联汽车网络安全管理体系发生重大变更，或发生重大问题、服务质量事故、客户投诉等情况时，认证机构视情况可增加监督的频次。

3.7.3 监督审核的最长时间间隔不超过 12 个月。由于获证组织业务运作的时间(季节)特点及其内部审核安排等原因，可以合理选取和安排监督周期及时机，在认证证书有效期内的监督审核必须覆盖智能网联汽车网络安全管理体系

系认证范围内的所有业务活动。获证企业的产品被主管机构查出不合格时，自官方发出通报起 30 日内，认证机构应对该企业实施监督审核。

3.7.4 监督审核时至少应审核以下内容：

(1) 智能网联汽车网络安全管理体系保持和变化情况；如有变化，涉及变化的范围。

(2) 对上次审核中确定的不符合项采取的纠正和纠正措施是否继续有效。

(3) 智能网联汽车网络安全管理体系覆盖的活动涉及法律法规规定的，是否持续符合相关规定。

(4) 内部审核和管理评审是否规范和有效。

(5) 获证组织对认证标志的使用或对认证资格的引用是否符合《认证认可条例》及其他相关规定。

(6) 是否及时接受和处理投诉。

(7) 针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

3.7.5 对于监督审核合格的获证组织，认证机构应做出保持其智能网联汽车网络安全管理体系认证资格的决定；否则，应暂停、撤销或注销相应的认证资格。

3.8 再认证

3.8.1 认证证书期满前，若获证组织申请继续持有认证证书，认证机构应当实施再认证审核，并决定是否延续认证

证书。

3.8.2 认证机构应结合历次监督审核情况，考虑智能网联汽车网络安全管理体系在认证周期内的绩效，制定再认证审核计划交审核组实施。

3.8.3 在智能网联汽车网络安全管理体系及获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段审核。当存在重大变更时，认证机构应有程序确保对再认证审核活动可能需要进行的第一阶段审核实施管理。

3.8.4 对再认证审核中发现的严重不符合项，认证机构应规定时限要求获证组织实施纠正与纠正措施，并在原认证证书到期前完成对纠正与纠正措施的验证。

3.8.5 认证机构做出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

3.9 暂停或撤销认证证书

3.9.1 认证机构应制定暂停、撤销认证证书或缩小认证范围的规定和文件化的管理制度，规定和管理制度应满足本规则相关要求。认证机构对认证证书的暂停和撤销处理应符合其管理制度，不得随意暂停或撤销认证证书。

3.9.2 暂停证书

(1) 获证组织有以下情形之一的，认证机构应在调查核实后的5个工作日内暂停其认证证书：

①智能网联汽车网络安全管理体系持续或严重不满足

认证要求，包括对智能网联汽车网络安全管理体系运行有效性要求的。

②不承担、履行认证合同约定的责任和义务的。

③被有关执法监管部门责令停业整顿的。

④持有的与智能网联汽车网络安全管理体系范围有关的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的。

⑤主动请求暂停的。

⑥其他应当暂停认证证书的。

(2) 认证证书暂停期不得超过 6 个月。但属于第④项情形的暂停期可至相关单位做出许可决定之日。

(3) 认证机构应以适当方式公开暂停认证证书的信息，明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

3.9.3 撤销证书

(1) 获证组织有以下情形之一的，认证机构应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书：

①被注销或撤销法律地位证明文件的。

②被监管部门列入质量信用严重失信企业名单。

③拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的。

④拒绝接受国家产品质量监督抽查的。

⑤出现重大的产品和服务等质量安全事故，经执法监管部门确认是获证组织违规造成的。

⑥有其他严重违反法律法规行为的。

⑦暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的与智能网联汽车网络安全管理体系范围有关的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）。

⑧没有运行智能网联汽车网络安全管理体系或者已不具备运行条件的。

⑨不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过2个月仍未纠正的。

⑩其他应当撤销认证证书的。

(2) 撤销认证证书后，认证机构应及时收回撤销的认证证书。若无法收回，认证机构应及时在相关媒体和网站上公布或声明撤销决定。

3.9.4 认证机构暂停或撤销认证证书应当在其网站上公布相关信息，同时按规定程序和要求报国家认监委。

3.9.5 认证机构应采取有效措施避免各类无效的认证证书和认证标志被继续使用。

4 认证证书

4.1 认证证书内容应至少包含以下信息：

(1) 认证证书名称，即智能网联汽车网络安全管理体系认证证书。

(2) 获证组织名称、地址和统一社会信用代码（或组织机构代码）。该信息应与其法律地位证明文件的信息一致。

(3) 智能网联汽车网络安全管理体系覆盖的生产经营或服务的地址和业务范围。若认证的智能网联汽车网络安全管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息。

(4) 智能网联汽车网络安全管理体系符合 UNECE WP. 29 Regulation No.155-《Cyber security and cyber security management system》及 ISO SAE 21434《Road vehicles-Cybersecurity engineering》的表述。

(5) 证书编号。

(6) 认证机构名称、印章、法定代表人或其授权人的签字。

(7) 有效期的起止年月日。（证书应注明：获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息。）

(8) 相关的认可标识及认可注册号（适用时）。

(9) 证书查询方式。认证机构除公布认证证书在本机构

网站上的查询方式外，还应当在证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站上查询”，以便于社会监督。

4.2 初次认证认证证书有效期最长为3年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加3年。

4.3 认证机构应当建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

5 认证记录管理

5.1 认证机构应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

5.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间至少应当与认证证书有效期一致。

5.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式。

5.4 所有具有相关人员签字的书面记录，可以制作成电子文档保存使用，但是原件必须妥善保存，保存时间至少应当与认证证书有效期一致。

6 受理组织申诉

申请组织或获证组织对认证决定有异议时，认证机构应接受申诉并且及时进行处理，在 60 日内将处理结果形成书面通知送交申诉人。

书面通知应当告知申诉人，若认为认证机构未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。