编号：CCID-Gz71103-2023

电动汽车远程服务与管理系统信息安全认证实施规则

V1.0

2023 年 12 月 29 日发布　　2023 年 12 月 29 日实施

北京赛迪认证中心有限公司

目 录

1. 适用范围

本规则适用于电动汽车远程服务与管理系统的信息安全认证。

本规则中的电动汽车远程服务与管理系统指纯电动汽车、插电式混合动力电动汽车和燃料电池电动汽车的车载终端、车辆企业平台和公共平台之间的数据通信。

2. 认证模式

产品型式试验+初始工厂检查+获证后监督

3. 认证依据的标准

GB/T 40855-2021 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

CSTCQBIVJB128:V1.0 电动汽车远程服务与管理系统信息安全测试规范及评价

4. 认证流程

认证流程通常包括如下环节:

（1）认证的申请、资料评审和受理

（2）划分认证产品单元、编制认证方案

（3）产品型式试验

（4）初始工厂检查

（5）认证结果的评价与批准

（6）颁发认证证书

（7）获证后的监督

（8）再认证

5. 认证申请

5.1 认证单元划分

（1）原则上，同一生产者（制造商）、同一生产企业（场所）生产的具有相同“规格型号和版本号”的产品为一个认证申请单元。

（2）当规格型号和版本号存在变更时，应当被认为是不同的认证单元，进行差异化认证或重新认证。

5.2 申请认证提交材料

5.2.1 申请材料

（1）产品认证申请书

（2）认证产品描述表

（3）工厂检查调查表

5.2.2 证明材料

（1）申请人、制造商、生产厂的注册证明，如营业执照（首次申请时）

（2）申请人为销售者、进口商时，还须提交销售者和生产者、进口商和生产者订立的相关合同副本

（3）如认证委托人通过代理人进行认证委托时，还应提供代理人的授权委托书（如有）

（4）有效的监督检查报告或工厂检查报告（如有）

（5）其他需要的文件

认证机构依据相关要求对申请资料进行评审，如申请资料需要补充或完善的，将与申请人进行沟通，要求补充提交相关资料，在资料评审完成后，及时向申请人发出受理或不予受理通知。

5.3 实施安排

申请评审完成后，认证机构依据评审结果指定认证方案，方案通常包括:

（1）所采用的认证模式和单元划分

（2）产品型式试验方案

（3）初始工厂检查方案

（4）其他需要说明的事项和要求

6. 产品型式试验

6.1 样品

6.1.1 样品选择

样品应是生产企业按照正常加工方式生产的产品，认证委托人应保证其所提供的样品与实际生产产品的一致性，不得借用、租用、购买样品等用于检测。检测机构对样品真实

性有疑问的应向北京赛迪认证中心有限公司说明情况，并作出相应处理。

6.1.2 样品数量

产品型式试验要求样品为电动汽车远程服务与管理系统 1 套。

6.1.3 样品及资料处置

试验结束并出具试验报告后，有关原始记录和相关资料由检测机构保存，样品由认证机构和企业协商处置。

6.2 试验项目和试验方法

试验项目和试验方法为产品适用标准规定的全部适用项目和有关试验方法。

表 1 产品型式试验要求

测试系统	测试项目/部件		依据标准
电动汽车远程服务与管理系统	车载终端信息安全	车载终端硬件信息安全	CSTCQBIVJB092: V1.0 汽车网关安全要求和检测规范
		车载终端固件信息安全	
		车载终端软件系统信息安全	
		车载终端数据存储信息安全	
		车载终端网络端口传输信息安全	
		车载终端远程升级功能信息安全	
		车载终端日志功能信息	

		安全	
		车载终端系统信息安全	
	平台间通信安全	认证机制核查	
		通信保密性传输	
		通信完整性传输	
		网络端口冗余及非授权访问	
		协议版本核查	
		协议功能核查	
		安全算法核查	
	车载终端与平台通信安全	车载终端与平台通信安全核查	
		车载终端与平台通信传输协议	
		车载终端与平台通信双向身份认证	
		车载终端与平台通信数据加密性	
		车载终端与平台通信数据完整性	

6.3 型式试验时限

除特殊项目外，一般为 60 个工作日（因检测项目不合格，企业进行整改和重新检验的时间不计算在内。）从收到认证所需的产品技术文件、样品和检测费用之日算起。

6.4 型式试验结果判定

型式试验应符合 3 中依据标准条款的要求。产品如有部分试验项目不符合标准的要求，允许委托人整改后重新提交样品进行试验。重新试验的样品数据和试验项目视不合格情况由检测机构决定。

任何一项不符合标准要求时，则判定该认证单元产品不符合认证要求。

6.5 型式试验报告

由认证机构指定的检测机构对样品进行试验，并按规定格式出具试验报告。

7. 初始工厂检查

7.1 检查内容

工厂检查的内容为工厂质量保证能力和产品一致性检查。

7.1.1 工厂质量保证能力检查

按附件 1 进行检查。

7.1.2 产品一致性检查

工厂检查时，应在生产现场检查申请认证产品的一致性，重点核查以下内容。

（1）认证产品的标识（如：名称、规格、型号和商标等）应与试验报告及委托认证提交的资料所标明的一致;

（2）认证产品的结构与参数，应与送样样品及委托认证提交的资料一致;

（3）认证产品的关键元器件与材料应与委托认证提交的资料一致。

7.2 初始工厂检查时间

一般情况下，产品型式试验合格后，再进行初始工厂检查。必要时，产品型式试验和工厂检查也可同时进行。

初始工厂检查原则上应在产品型式试验结束后一年内完成，否则应重新进行产品型式试验。初始工厂检查时，工厂应生产申请认证范围内的产品。

工厂检查人日数详见表 2。认证机构可根据企业实际情况额外增加人日数（按 3000 元每人日收费）。

表 2 工厂检查人·日数（初始检查/监督检查/复审检查）

工厂检查类型	初始检查	监督检查
人日数	4	2

7.3 初始工厂检查结论

检查组负责报告工厂检查结论。

（1）工厂检查未发现不合格项，则检查结果为通过。

（2）工厂检查存在不合格项，可允许整改，工厂应在 40 个工作日的期限内完成整改，认证机构采取适当方式对整改结果进行验证。

（3）未能按期完成整改的或整改不通过的，按工厂检查不通过处理。

7.4 工厂检查结论告知

检查组在工厂检查结束后，应将检查结果告知企业，如工厂检查中开具了不符合项，应对企业提出纠正措施的验证方式及整改时限做出明确要求，并将验证结果及时告知生产企业。

8. 认证结果评价与批准

8.1 认证结果评价与批准

认证机构组织对型式试验、工厂检查结论和有关资料/信息进行综合评价，评价合格后，向申请人按认证单元颁发产品认证证书；评价不合格的视为不通过，认证终止。

8.2 认证时限

认证时限是指自认证机构正式受理认证之日起至颁发认证证书时止的时间期限。在完成产品型式试验和工厂检查后，对符合认证要求的，一般情况下在 15 个工作日内出具认证证书。由于认证委托人及生产企业自身原因逾期未完成认证活动导致认证超时，不计入认证时间。

8.3 认证终止

当型式试验不合格或工厂检查不通过时，认证机构做出

不合格决定，终止认证。终止认证后如要继续申请认证，重新申请认证。

9. 获证后监督

获证后监督是指认证机构对获证产品及其生产企业实施的监督检查，以保证企业生产的产品持续符合认证标准及与型式试验样品的一致性。

9.1 监督检查时间

9.1.1 监督检查频次

一般情况下，获证后 12 个月内应安排年度监督，每次年度监督检查应在当年度内完成。若发生下述情况之一可增加监督频次:

（1）获证产品出现严重质量问题或用户提出严重投诉并经查实为证书持有人责任的;

（2）认证机构有足够理由对获证产品与认证依据标准的符合性提出质疑时;

（3）有足够信息表明生产者、生产企业由于变更组织机构、生产条件、质量管理体系等而可能影响产品符合性或一致性时。

9.1.2 监督检查人日数

见表 2。

9.2 监督检查的内容

认证机构根据附件 1 对工厂进行监督检查。并同时对认证标志、认证证书的使用情况及前次工厂检查和型式试验不符合项的整改情况进行监督检查。

获证产品一致性检查的内容与工厂初始检查时的产品一致性检查内容基本相同。必要时，进行获证产品的监督抽样检测或监督抽样核查。

9.3 监督检查结论

检查组负责报告监督检查结论。

（1）监督检查结论为不通过的，检查组直接向认证机构报告。

（2）监督检查存在不符合项时，工厂应在 40 个工作日的期限内完成整改，认证机构采取适当方式对整改结果进行验证。

（3）未能按期完成整改的或整改不通过，按监督检查不通过处理。

9.4 结果评价

认证机构组织对监督检查结论和有关资料/信息进行综合评价，评价合格的，认证证书持续有效。当监督检查不通过时，按照 11.3 规定执行。

10. 认证证书

10.1 认证证书的有效性

本规则覆盖产品的认证证书有效期为 2 年。证书的有效性依赖认证机构的获证后监督获得保持。

10.2 认证证书的变更

10.2.1 变更的申请

出现下列情况时，应进行认证证书的变更:

（1）证书上的内容发生变化的。

（2）或已获证产品发生技术变更（设计、技术规格参数、软件版本、关键元器件及供应商等）影响相关标准的符合性时。

（3）认证标准有更新时，或认证机构规定的其他事项发生变更时。

证书持有人应向认证机构提出变更申请，经认证机构评估确认后提供书面文件或资料证明，必要时应送样进行试验，经认证机构批准后方可实施认证变更。

10.2.2 变更的评价和批准

认证机构根据变更的内容和提供的资料进行评价，确定是否可以变更。如需安排试验和/或工厂检查，则试验合格和/或工厂检查通过后方能进行变更。原则上，应以最初进行产品型式试验的认证产品为变更评价的基础。试验和工厂检查

按认证机构相关规定执行。

对于换发新的认证证书的情况，新证书的编号、批准有效日期保持不变，并注明换证日期。

10.3 认证证书的暂停、恢复、注销和撤销

10.3.1 证书的暂停

出现下列情况之一时，暂停认证证书的使用:

（1）监督结果表明认证产品不符合认证要求，但不需要立即撤销认证证书的;

（2）获证机构不恰当地使用了认证证书和标志，而没有将其收回或采取适当补救措施的;

（3)任何其他违反认证方案的规定或认证机构程序行为的;

（4）企业申请暂停证书。

10.3.2 证书的撤销及停止

出现下列情况之一时，由认证机构撤销认证证书，并责令停止使用产品认证标志:

（1)监督结果表明认证产品不能持续符合本规则要求的;

（2)暂停认证证书的使用，整改期满仍不能达到要求的;

（3）通过认证的产品质量严重下降，或出现重大质量问题，且造成严重后果的;

（4）转让认证证书、产品认证标志或违反有关规定、损害产品认证标志信誉的;

（5）获证后不履行认证付款义务的;

（6）没有正当理由而拒绝监督检查的;

（7）对未作变更申请,而继续使用认证证书和产品认证标志的。

被撤消认证证书的企业，自接到通知之日起一年后，认证机构方可重新受理其产品认证申请。

10.3.3 证书的注销及停止

出现下列情况之一时，由认证中心注销认证证书，并责令停止使用产品认证标志。

（1）由于认证规则要求的内容发生较大变化，认证证书持有者认为达不到变化后的要求，不再申请产品认证的;

（2）获证机构不再生产认证证书中包含的所有型号的产品。

11. 再认证

证书持有人应在距证书有效期满之日的 6 个月前提交再认证申请，流程和要求同初次认证。型式试验可进行部分项目检测,必要时进行全部项目检测。再认证评价合格后发新证书。

12. 产品认证标志的使用

认证标志由获证单位向认证机构提出使用申请，获得书面授权后按照认证机构标志使用管理办法使用。获证组织应在获准认证范围内使用，不得以任何方式转让、出售、借用、冒用。在使用标志图案时，应按照认证机构规定的图样以相应的比例放大或缩小。

12.1 准许使用的标志样式

准许证书持有人使用的认证标志:

12.2 认证标志的加施

证书持有者应向认证机构购买标准规格的标志，或申请按实施规则中规定的合适方式来施加认证标志。应在产品本体明显位置、铭牌或说明书、包装上施加认证标志。

13. 收费

认证及检测的收费以赛迪认证中心和签约实验室正式发布的收费文件为准。

14. 认证责任

（1）认证机构对认证结论负责。

（2）检测机构对试验结果和试验报告负责。

（3）认证申请人对其所提交的申请资料及样品的真实性、合法性负责。

附件 1

工厂质量保证能力要求

本文件作为产品认证的工厂产品质量保证能力的检查依据文件之一,规定了申请产品认证的工厂的产品质量保证能力要求。

为保证生产的认证产品与已获型式试验合格的样品的一致性，工厂应满足本文件规定的产品质量保证能力要求。如有特殊要求的，按具体产品认证规则中有关规定执行。

1. 职责和资源

1.1 职责

工厂应规定与质量活动有关的各类人员职责及相互关系，且工厂应在组织内指定一名质量负责人,无论该成员在其它方面的职责如何，应具有以下方面的职责和权限:

a）确保本文件的要求在工厂得到有效地建立、实施和保持;

b）确保加贴认证标志的产品符合认证标准的要求;

c）建立文件化的程序，确保认证标志的妥善保管和使用;

d）建立文件化的程序，确保不合格品和获证产品变更后未经认证机构认可，不加贴认证标志。

1.2 资源

工厂应配备必须的生产设备和检验设备以满足稳定生产符合认证标准要求的产品；应配备相应的人力资源，确保从事对产品质量有影响工作的人员具备必要的能力；建立并保持适宜产品生产、检验试验、储存等必备的环境。

对于需以租赁方式使用的外部资源，工厂应确保外部资源的持续可获得性和正确使用；工厂应保存与外部资源相关的记录，如合同协议、使用记录等。

2. 文件和记录

（1）工厂应建立、保持文件化的认证产品的质量计划或类似文件，以及为确保产品质量的相关过程有效运作和控制需要的文件。质量计划应包括产品设计、实现过程、检测及有关资源的规定，以及产品获证后对获证产品的变更（标准、参数、设计等）、标志的使用受理等的规定。

（2）工厂应建立并保持文件化的程序以对本文要求的文件和资料进行有效的控制。这些控制应确保：

a）文件发布前和更改应由授权人批准，以确保其适宜性；

b）确保文件的更改和修订状态得到识别，防止作废文件的非预期使用；

c）确保在使用处可获得相应文件的有效版本。

（3）工厂应建立并保持文件化的质量记录的标识、储存、

保管和处理的文件化程序。质量记录应清晰、完整以作为产品符合规定要求的证据。质量记录应有适当的期限。

（4）工厂应建立并保持获证产品的档案。档案内容至少应包含证书、实验报告、工厂检验报告、获证产品变更的申请和批准资料等。

3. 生产过程控制

（1）工厂应对影响认证产品质量的工序（简称关键工序）进行识别，所识别的关键工序应符合规定要求。关键工序操作人员应具备相应的能力；关键工序的控制应确保认证产品与标准的符合性、产品一致性；如果关键工序没有文件规定就不能保证认证产品质量时，则应制定相应的作业指导书，使生产过程受控。

（2）产品生产过程如对环境条件有要求,工厂应保证工作环境满足规定要求。

（3）必要时，工厂应对适宜的过程参数进行监视、测量。

（4）工厂应建立并保持对生产设备的维护保养制度，以确保设备的能力持续满足生产要求。

（5）必要时，工厂应按规定要求在生产的适当阶段对产品及其特性进行检查、监视、测量，以确保产品与标准的符合性及产品一致性。

4. 例行检验和确认检验

工厂应制定并保持文件化的例行检验和确认检验程序，以验证产品满足规定的要求。检验程序中应包括检验项目、内容、方法、判定等。并应保存检验记录。具体的例行检验和确认检验要求应满足相应产品的认证实施规则的要求执行。

例行检验是在生产的最终阶段对生产线上的产品进行的100%检验，通常检验后，系统功能、参数不再进一步改变。

确认检验是为验证产品持续符合标准要求进行的抽样检验。

5. 不合格品的控制

（1） 对于采购、生产制造、检验等环节中发现的不合格品，工厂应采取标识、隔离、处置等措施，避免不合格品的非预期使用或交付。返工或返修后的产品应重新检验。

（2）对于国家级和省级监督抽查、产品召回、顾客投诉及抱怨等来自外部的认证产品不合格信息，工厂应分析不合格产生的原因，并采取适当的纠正措施。工厂应保存认证产品的不合格信息、原因分析、处置及纠正措施等记录。

（3）工厂获知其认证产品存在重大质量问题时（如国家级和省级监督抽查不合格等），应及时通知认证机构。

6. 内部质量审核

工厂应建立文件化的内部质量审核程序，确保质量体系的有效性和认证产品的一致性，并记录内部审核结果。

对工厂的投诉尤其是对产品不符合标准要求的投诉，应保存记录，并应作为内部质量审核的信息输入。

对审核中发现的问题，应采取纠正和预防措施，并进行记录。

7. 认证产品的一致性

工厂应对生产产品与型式试验合格的产品的一致性进行控制，以使认证产品持续符合规定的要求。

工厂应建立产品关键标识、参数等影响产品符合规定要求因素的变更控制程序，认证产品的变更（可能影响与相关标准的符合性或型式试验样机的一致性）在实施前向认证机构申报获得批准后方可执行。

8. 产品风险评估分析

信息安全风险评估从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护政策和整改措施，将风险控制在可接受的水平，最大限度保障车辆信息安全。为保证企业能有效的降低信息安全风险，本规则针对企业风险评估过程进行评价，评价主要围绕一下内容展开:

a）风险评估目标的制定应明确且清晰;

b）风险评估的范围应清晰;

c）风险评估实施人员职责应分明;

d）针对风险评估中的资产识别、威胁场景、影响评估、脆弱性识别展开审计，查看操作是否充分且合理;

e）风险评估文件中应包括目前所采取的安全措施分析;

f）针对风险评估中的攻击路径分析，攻击可行性分析、风险分析、风险处置、残余风险识别相关内容展开审查，查看分析过程是否合理。

9. 产品安全升级评价

远程升级指通过云端升级技术,为具有连网功能的设备以按需，以扩展的方式获取系统升级包，并通过远程升级进行云端升级，完成系统修改和优化的功能，协助整车厂商快速修复安全漏洞和软件故障。同时，通过远程升级可以实现对相关服务的功能性升级，不断丰富功能模块。升级和安全往往是一个密不可分的整体，本规则针对升级过程进行评价。

10. 产品防护项评价

电动汽车远程服务与管理系统提供了远程控制、车辆监测和数据交互等功能,使车主能够通过手机应用或互联网与车辆进行交互。在提供便捷的同时所面临的风险也日益增多，为了尽可能的规避安全风险,应在产品开发周期内添加相应的安全防护措施。主要围绕以下内容展开:

a）系统应具备预防远程攻击的防护，如果系统存在漏洞或不安全配置，黑客可能通过远程攻击手段入侵系统，获取车

辆的敏感数据、篡改车辆的功能或控制车辆行为。

b）预防软件漏洞和恶意软件，若系统的软件存在漏洞，黑客可以利用这些漏洞进行攻击。同时，恶意软件或病毒可能通过下载应用、更新系统等途径被植入到远程服务与管理系统中，从而危及车辆和车主的安全。

c）数据隐私保护措施，远程服务与管理系统涉及到车辆和车主的各种数据，如车辆位置、驾驶行为、个人账户信息等。如果这些数据未经适当保护，黑客可能获取到这些敏感数据，侵犯车主的隐私。

d）身份验证和授权问题，远程服务与管理系统需要建立有效的身份验证和授权机制，以确保只有授权用户才能访问和操作车辆。如果身份验证和授权机制存在漏洞或不安全，未经授权的人员可能滥用系统或进行非法操作。