编号：CESI-SC-OD19

汽车数据处理安全服务认证规则

2025-8-31 发布　　2025-8-31 实施

北京赛西认证有限责任公司

前 言

本规则依据《中华人民共和国认证认可条例》制定。本规则明确了对汽车数据处理安全进行认证的基本原则和要求。

本规则首次发布日期：2024.6.13，实施日期：2024.6.13。

第一次修订（v1.1）日期及内容：2025.8.31，本次换版修订了服务特性测评过程、认证证书模板。

目　录

1 适用范围

本规则规定了对汽车数据处理安全进行认证的基本原则和要求。

认证领域或技术领域划分：SC12。

2 认证依据

GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》

3 认证模式

服务特性测评+服务管理审核+获证后监督

4 认证实施

4.1. 认证申请

4.1.1 申请范围界定

场所：认证申请方的汽车数据处理活动所在的物理场所。

活动：认证申请方的汽车数据处理活动。

类别：认证申请方的类别。

认证申请方的类别定义如下表所示：

类别名称	类别定义
第一类	汽车制造商和汽车供应链企业等参与汽车设计、生产和制造，及车联网平台和出行服务平台等向用户提供汽车出行应用服务产品。
第二类	地方自动驾驶示范区数据平台、新能源汽车数据平台等不参与汽车生产制造，但汇聚大量汽车数据。

注：组织只能申请第一类或第二类。

4.1.2 申请时需提交的文件资料

申请认证应提交认证申请书，并随附以下文件：

1) 有效法律地位证明复印件及适用时从事相关服务的资质和任何行政许可证明复印件；

2) 国家企业信用信息公示系统年度报告电子版；

3) 汽车数据处理安全能力自评价表；

4) 其他认证所需相关材料。

4.2. 申请评审

认证机构在 5 个工作日内对申请材料进行评审，确认资料的完整性、准确性和符合性。并将评审结果（包括受理、退回修改、不受理）告知认证申请方。

若决定受理，认证机构根据认证申请资料确定认证方案，并通知认证申请方。

4.3. 认证评价

认证机构对组织的数据安全能力实施服务特性检验、服务管理审核，并出具报告。

4.3.1. 服务特性测评

服务特性测评采用服务特性检验方式。

认证机构委托测评机构依据 GB/T 41871-2022 对汽车数据处理安全能力相关要求进行公开的服务特性检验，出具服务特性检验报告（即：汽车数据处理安全能力评估报告）。

服务特性检验流程包括：

针对申请方的类别，选取相应的标准条款（详见附录 A 汽车数据处理安全能力类别条款表）；评估申请方汽车数据处理安全能力的满足情况，并出具《服务特性检验报告》。

4.3.2. 文件审查

如《服务特性检验报告》的结论满足服务管理审核的现场评价条件，认证机构委派审查组对申请方的《汽车数据处理安全能力自评价表》和测评机构做出的《服务特性检验报告》以及相关佐证材料进行文件审查。

如文件资料存在不符合项，申请方应及时整改、补充提交必要的文件，文件整改实施期限原则上不超过 10 个工作日。

审查组出具文件审查报告，给出是否进行服务管理审核现场评价的建议及现场评价中需重点关注的事项。

4.3.3. 服务管理审核

由认证机构审查组进行服务管理审核的现场评价。

4.3.3.1. 评价内容

初次认证时，审查组到申请范围覆盖的汽车数据处理活动场所，进行服务管理审核。

现场评价重点是对申请方的服务管理条款进行审查，评价申请方服务能力的保证情

况。

4.3.3.2. 评价结论

审查组以评价报告的形式向认证机构报告评价结论。现场评价存在不符合项时，申请方应在认证机构规定的期限内完成整改，审查组采取适当方式对整改结果进行验证。逾期不能完成整改，或整改结果不合格，按现场评价结论不合格处理。

4.4. 复核、认证决定

认证机构应对认证相关的所有信息包括申请评审、评价过程和结论进行复核。

认证机构根据评价、复核以及其他相关的所有信息做出认证决定。

对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证申请方限期整改，整改后仍不符合的，以书面形式通知认证申请方终止认证。

4.5. 获证后监督

4.5.1. 监督的频次和方式

认证机构在认证证书有效期内，通过认证评价对获得认证的专业机构进行持续监督，年度监督审核至少每个日历年进行一次，初次认证后的第一次监督审查在认证决定日期起12个月内进行。若发生下述情况可适当增加监督频次：

1) 获证组织的服务活动出现严重质量问题，如：发生汽车数据安全事故或在汽车数据处理安全方面有重大投诉，并经查实为获证组织责任时；
2) 认证机构有足够理由对获证组织服务与认证要求的符合性提出质疑时；
3) 有足够信息表明获证组织因变更组织机构、服务场所、环境条件等，可能影响服务符合性或一致性时；
4) 违反法律法规、国家行业监督及媒体曝光等重大问题的情况；
5) 发生其他影响符合认证要求的能力变化的特殊情况时。

4.5.2. 监督的内容

监督时至少应评价以下内容：

（1）上次评价以来组织活动及运行的资源是否有变更；

（2）组织数据安全特性有关的活动是否有效运行；

（3）涉及法律法规规定的，相关法律法规或技术标准是发生变化，是否持续符合相

关规定；

（4）汽车数据处理安全能力是否持续保持；

（5）获证组织对认证证书和认证标志的使用或对认证资格的引用是否符合相关的规定；

（6）是否及时接受和处理投诉；

（7）针对投诉的问题，及时制定并实施了有效的持续改进。

监督至少应包括服务管理审核，且在一个认证周期内至少开展一次服务特性检验，监督采用条款抽样的方式开展，抽样条款的数量应不低于认证依据条款的 1/3。

4.5.3. 获证后监督结果的评价

认证机构对证后监督报告和其他相关资料信息进行综合评价，监督结果符合要求的，可保持认证资格，继续使用认证证书和认证标志；对监督复查时发现的不符合项应在认证机构规定期限内完成纠正措施。逾期按认证机构公开文件《服务认证程序规则》的要求执行，并对外公告。

4.6. 再认证

认证机构在认证证书到期前对获证机构进行再认证，再认证过程与初次认证保持一致，再认证可采用条款抽样的方式开展，抽样条款应不低于认证依据条款的 2/3。

4.7. 认证时限

认证时限是指自作出受理决定之日起至作出认证决定所实际发生的工作日，一般为 60 个工作日（不包含整改时间）。

5 认证证书

获证组织必须按认证机构公开文件《服务认证程序规则》的要求使用认证证书。

5.1. 证书的保持

认证证书有效期为 3 年。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。

证书到期需延续使用的，获证组织应当在有效期届满前 3 个月内提出认证申请。认证机构应当采用再认证的方式，对符合认证要求的申请换发新证书。

5.2. 证书的变更

认证证书有效期内，获证组织名称、地址，或认证评价内容等发生变化时，获证组织应当向认证机构提出变更申请。认证机构根据变更的内容，对变更申请资料进行评价，确定是否批准变更。如需进行认证评价，还应当在批准变更前进行认证评价。当认证要求（如标准）发生变化时，获证组织应按规定换证，未按规定换发的认证证书自行失效，同时认证机构应予以撤销证书，要求其停止使用认证标志。

认证的变更按照认证机构公开文件《服务认证程序规则》的要求执行。

5.3. 认证的暂停、撤销和注销

当获得认证组织不再符合认证要求时，认证机构对认证证书予以暂停直至撤销，要求其停止使用认证标志。认证申请方在认证证书有效期内可申请暂停或注销认证证书。认证机构采用适当方式对外公布被暂停、注销和撤销的认证证书。

暂停期限为 6 个月。暂停期限内，获证机构可提出恢复认证的申请，经认证机构评审、批准后，方可使用该证书。在暂停认证期间，获证机构不得继续使用证书和认证标志。暂停期满仍未恢复认证资格的，认证证书自动撤销。

认证的暂停、恢复、撤销、注销及涉及的认证证书和标志使用的具体要求按照认证机构公开文件《服务认证程序规则》执行。

6 认证标志

在认证证书有效期内， 获证组织应当按照规定在广告等宣传中正确使用认证证书和认证标志，不得对公众产生误导。

获证组织必须按认证机构公开文件《服务认证程序规则》的要求使用认证标志。

7.1 准许使用的认证标志样式

1）认证标志样式：

2) 规格：标志图案的尺寸长宽比例 1:1，允许线性比例缩放。

3) 颜色：应使用基本颜色或单一黑色。

7.2 变形认证标志的使用

本规则覆盖的产品不允许使用任何形式的变形认证标志。

7.3 加施方式及位置

获证组织可在通过认证的系统、相关宣传材料上加施认证标志。

附录 A 汽车数据处理安全能力类别条款表

第一类认证申请方的评估包括 47 个条款。第二类认证申请方的评估包括 18 个条款。第一类包含第二类全部条款要求。

认证申请的评估类别的所有条款要求都满足时，才能授予相应证书。

第一类认证申请方的评估涉及的条款：

编号	条款号	条款内容
1	4.1 汽车数据处理者处理个人信息符合下列要求。	取得个人同意时，应通过至少一种显著方式向个人告知。显著方式包括用户手册单独章条提示、语音播放、车载显示面板单独弹窗提示、汽车使用相关应用程序交互、汽车销售协议单独章条提示、维修服务协议单独章条提示或出行服务应用程序交互等。
2		应使用清晰易懂的文字向个人信息主体说明收集个人信息的具体情境和必要性。
3		向个人信息主体告知各类型个人信息的保存期限时，应具体且明确，例如 30 天或 1 年等。
4		向个人信息主体告知其个人信息保存地点时，应将保存地点位置精确到地级市并告知所有保存地点。
5		应为个人信息主体提供便捷的查阅、复制和删除等个人信息管理功能;
6		提供的产品或服务支持交互操作时，例如提供网站、车载应用程序或移动通信终端应用程序等，个人信息管理功能应为交互式，其功能入口应处于个人信息主体容易察觉的显著位置。
7	4.2 汽车数据处理者处理敏感个人信息符合下列要求。	应对每项敏感个人信息取得个人信息主体单独同意，不应一次性针对多项敏感个人信息或多种处理活动取得同意。 注：汽车数据处理者为驾驶人提供语音识别功能需要处理语音数据，可针对该功能单独弹窗取得驾驶人同意，也可在告知同意中针对该功能设置可勾选的单独选项取得驾驶人同意。
8		取得个人信息主体单独同意时，处理敏感个人信息的同意期限不应设置为“始终允许”或“永久”。 注：汽车数据处理者为语音识别功能需要处理语音数据，取得个人信息主体单独同意时，可为个人信息主体提供单次、七天、三个月和一年等选项。

9		在收到删除个人信息请求后十个工作日内完成删除。
10		原则上应建立个人信息结构化目录，实现个人信息的可追溯管理。
11		原则上不应以改善服务质量、提升用户体验以及研发新产品等为目的处理敏感个人信息。
12	4.3 汽车数据处理者持续收集敏感个人信息符合下列告知要求。	应通过车载显示面板图标或信号装置指示灯的闪烁或长亮等方式提示收集状态。
13		持续提示收集敏感个人信息时，应根据信息类型的不同设置差异明显且清晰易懂的提示。 注：可通过摄像图标闪烁或长亮提示正在收集车内视频数据，通过录音图标闪烁或长亮提示正在收集车内语音数据，通过斜向上三角图标的闪烁或长亮提示正在收集位置数据。
14	4.4 汽车数据处理者处理人脸、声纹或指纹等生物识别特征信息符合下列要求。	应评估是否具有增强行车安全的目的和充分的必要性。 注：增强行车安全的目的包括身份验证以及驾驶人状态监测等。
15	4.5 汽车数据处理者在个人信息保护方面设置的用户权益事务联系人符合下列要求。	应具备个人信息保护和个人权益保护等方面的专业知识。
16		应及时受理并处置个人信息保护方面的投诉和举报。
17		应对外告知准确有效的姓名和联系方式，联系方式包括电话号码、邮箱地址、网址或即时通信平台账号等；不便对外告知真实姓名的，应告知长期且固定使用的别名。
18	4.6 涉及座舱数据、位置轨迹数据、车外视频和车外图像数据，以及涉及个人信息主体超过 10 万人的个人信息，汽车数据处理者应依法在中华人民共和国境内存储。	涉及座舱数据、位置轨迹数据、车外视频和车外图像数据，以及涉及个人信息主体超过 10 万人的个人信息，汽车数据处理者应依法在中华人民共和国境内存储。
19	4.7 汽车数据处理者处理重要数据，原则上应在完成脱敏处理后再进行其他处理；	处理重要数据，原则上应在完成脱敏处理后再进行其他处理

20	处理个人信息，原则上应在匿名化处理或去标识化处理后再进行其他处理。	处理个人信息，原则上应在匿名化处理或去标识化处理后再进行其他处理。
21	5 车外数据安全要求 汽车数据处理者对车外数据进行匿名化处理符合以下要求。	车外数据未完成匿名化处理前，不应向车外提供。
22		经过匿名化处理的视频以及图像应无法复原且无法关联个人信息主体，包括以下实现方式： 1）完整删除：处理图像时，将包含人脸以及车牌等个人信息的图像直接删除；处理视频时，删除视频中所有包含人脸以及车牌等个人信息的视频帧； 2）局部轮廓化处理：将视频以及图像中包含人脸以及车牌等个人信息的区域彻底擦除，或者将这些区域替代为无法关联个人信息主体且不可复原的其他图像。
23		匿名化处理过程中，除分析确定包含人脸以及车牌等个人信息的区域，以及对这些区域进行删除或局部轮廓化处理外，不应进行人脸比对、步态分析以及语音识别等其他处理。
24		匿名化处理完成后，过程数据应立即删除，不应向车外提供。
25	6.1 除非驾驶人自主设定，汽车应默认设定为不收集座舱数据的状态，包括不打开车内的摄像头、传声器、红外传感器和指纹传感器等部件，当驾驶人通过实体按键或触摸按键等方式主动选择后才能开始收集，汽车可根据驾驶人设定，保持驾驶人选择的状态或恢复默认状态。	除非驾驶人自主设定，汽车应默认设定为不收集座舱数据的状态，包括不打开车内的摄像头、传声器、红外传感器和指纹传感器等部件。
26		当驾驶人通过实体按键或触摸按键等方式主动选择后才能开始收集。
27		汽车可根据驾驶人设定，保持驾驶人选择的状态或恢复默认状态。
28	6.2 汽车不应向车外提供座舱数据，下列情形除外。	除例外情形，汽车不应向车外提供座舱数据。

29		汽车向车外提供座舱数据例外情形： a）为实现语音识别功能以实时判断汽车控制指令，将语音指令数据在车外处理，取得个人信息主体同意，功能实现后即时删除原始数据及处理结果。 b）为实现远程查看车内情况或云存储功能，向使用者提供数据，取得个人信息主体同意，并采取安全措施，除使用者外的其他组织和个人不能访问。 c）道路运输车辆依据相关规定向所属运输企业监控平台、公共管理平台和监管机构传输数据。 d）出租汽车和公共汽车等营运车辆向监管机构传输数据。 e）道路交通事故发生后按执法部门要求传输数据。
30	6.3 汽车数据处理者应提供便利的终止收集座舱数据的方式。	汽车数据处理者应提供便利的终止收集座舱数据的方式，包括实体按键、语音控制、触摸按键以及汽车使用相关应用程序等。
31		在保证行车安全以及人身安全的情况下，驾驶人选择终止收集后，应关闭车内传声器和摄像头等收集座舱数据的部件。
32		为保证行车安全以及人身安全，下列情况可不关闭相关部件： a）正在提供公路营运服务的道路运输车辆持续收集座舱数据。 b）正在提供出行服务的公共汽车持续收集座舱数据。
33	7.1 汽车数据处理者开展汽车数据风险评估，评估内容一般包括汽车数据识别、数据处理活动识别、汽车数据安全风险识别和风险分析及评价等，可采取自评估或第三方评估的形式进行。	汽车数据处理者开展汽车数据风险评估。
34		评估内容一般包括汽车数据识别、数据处理活动识别、汽车数据安全风险识别和风险分析及评价等。
35		可采取自评估或第三方评估的形式进行。
36	7.2 汽车数据安全管理负责人应由汽车数据处理者主要负责人或分管数据安全负责人担任，并应熟悉我国数据安全和个人信息保护政策法规，具备安全管理工作经历。	汽车数据安全管理负责人应由汽车数据处理者主要负责人或分管数据安全负责人担任。
37		应熟悉我国数据安全和个人信息保护政策法规。
38		应具备安全管理工作经历。

39	7.3 汽车数据处理者应建立健全安全事件应急处置机制，每年至少开展一次应急演练，宜通过汽车数据存证、汽车数据溯源等机制支撑安全事件发生后的取证分析。	汽车数据处理者应建立健全安全事件应急处置机制。
40		每年至少开展一次应急演练。
41		宜通过汽车数据存证、汽车数据溯源等机制支撑安全事件发生后的取证分析。
42	7.4 汽车数据处理者应通过电话或即时通信平台等方式受理汽车数据安全投诉，在接到投诉后一般在 10 个工作日内处理完成，并对处理过程以及处理结果进行完整记录。	汽车数据处理者应通过电话或即时通信平台等方式受理汽车数据安全投诉。
43		在接到投诉后一般在 10 个工作日内处理完成。
44		对处理过程以及处理结果进行完整记录。
45	7.5 汽车制造商应全面掌握其生产的整车所含各零部件收集、传输数据情况，对零部件供应商处理汽车数据的行为进行约束和监督，汽车数据向外传输的完整情况应每年或在出现重大变更时向用户披露。	汽车制造商应全面掌握其生产的整车所含各零部件收集、传输数据情况。
46		对零部件供应商处理汽车数据的行为进行约束和监督。
47		汽车数据向外传输的完整情况应每年或在出现重大变更时向用户披露。

第二类认证申请方的评估涉及的条款：

编号	条款号	条款内容
1	4.5 汽车数据处理者在个人信息保护方面设置的用户权益事务联系人符合下列要求。	应具备个人信息保护和个人权益保护等方面的专业知识。
2		应及时受理并处置个人信息保护方面的投诉和举报。
3		应对外告知准确有效的姓名和联系方式，联系方式包括电话号码、邮箱地址、网址或即时通信平台账号等；不便对外告知真实姓名的，应告知长期且固定使用的别名。

4	4.6 涉及座舱数据、位置轨迹数据、车外视频和车外图像数据，以及涉及个人信息主体超过 10 万人的个人信息，汽车数据处理者应依法在中华人民共和国境内存储。	涉及座舱数据、位置轨迹数据、车外视频和车外图像数据，以及涉及个人信息主体超过 10 万人的个人信息，汽车数据处理者应依法在中华人民共和国境内存储。
5	4.7 汽车数据处理者处理重要数据，原则上应在完成脱敏处理后再进行其他处理；处理个人信息，原则上应在匿名化处理或去标识化处理后再进行其他处理。	处理重要数据，原则上应在完成脱敏处理后再进行其他处理
6		处理个人信息，原则上应在匿名化处理或去标识化处理后再进行其他处理。
7	7.1 汽车数据处理者开展汽车数据风险评估，评估内容一般包括汽车数据识别、数据处理活动识别、汽车数据安全风险识别和风险分析及评价等，可采取自评估或第三方评估的形式进行。	汽车数据处理者开展汽车数据风险评估。
8		评估内容一般包括汽车数据识别、数据处理活动识别、汽车数据安全风险识别和风险分析及评价等。
9		可采取自评估或第三方评估的形式进行。
10	7.2 汽车数据安全管理负责人应由汽车数据处理者主要负责人或分管数据安全负责人担任，并应熟悉我国数据安全和个人信息保护政策法规，具备安全管理工作经历。	汽车数据安全管理负责人应由汽车数据处理者主要负责人或分管数据安全负责人担任。
11		应熟悉我国数据安全和个人信息保护政策法规。
12		应具备安全管理工作经历。
13	7.3 汽车数据处理者应建立健全安全事件应急处置机制，每年至少开展一次应急演练，宜通过汽车数据存证、汽车数据溯源等机制支撑安全事件发生后的取证分析。	汽车数据处理者应建立健全安全事件应急处置机制。
14		每年至少开展一次应急演练。
15		宜通过汽车数据存证、汽车数据溯源等机制支撑安全事件发生后的取证分析。
16	7.4 汽车数据处理者应通过电话或即时通信平台等方式受理汽车数据安全投诉，在接到投诉后一般在 10 个工作日内处理完成，并对处理过程以及处理结果进行完整记录。	汽车数据处理者应通过电话或即时通信平台等方式受理汽车数据安全投诉。
17		在接到投诉后一般在 10 个工作日内处理完成。
18		对处理过程以及处理结果进行完整记录。

附录 B 认证证书样式

汽车数据处理安全服务认证证书

证书编号：CESI20xxVDSC1xxxxx

OID 编号：1.2.156.1.2. CESI20xxVDSC1xxxxx

兹证明

XXXXXXXXXXX 公司

（统一社会信用代码：xxxxxxxxxxxxxx）

（xxxxxxxxxxxxxxxxxxxxxx）

汽车数据处理安全达到

GB/T 41871-2022《信息安全技术 汽车数据处理安全要求》

第一类

认证模式

服务特性测评+服务管理审核+获证后监督

认证规则

CESI-SC-OD19《汽车数据处理安全服务认证规则》

涉及的场所及相关活动：

地址：xxxxxxxxxxxxxx

活动：xxxxxxxxxxxxxxxxxxx

（本证书有效性依据发证机构的定期监督获得保持，证书有效性信息请登录 www.cc.cesi.cn 进行查询）

（本证书信息可在国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 上查询）

颁证日期：20xx 年 xx 月 xx 日　　有效期至：20xx 年 xx 月 xx 日

签发人：

发证机构：北京赛西认证有限责任公司

地　　址：北京市东城区安定门东大街一号院 1 号楼 2 层

客服电话：4000719000　　网址：www.cc.cesi.cn