编号：CCID-Gz70736-2023

**软件供应链安全能力认证实施规则**

**2023-11-30** 发布 **2023-11-30** 实施

北京赛迪认证中心有限公司

**目 录**

[1 适用范围 3](#_Toc165985097)

[2 认证依据 3](#_Toc165985098)

[3 认证模式 3](#_Toc165985099)

[4 机构职责及人员能力要求 3](#_Toc165985100)

[4.1 赛迪认证中心 3](#_Toc165985101)

[4.2 签约检测机构 3](#_Toc165985102)

[4.3 认证委托方 4](#_Toc165985103)

[5 认证流程 4](#_Toc165985104)

[6 认证实施 5](#_Toc165985105)

[6.1 认证申请及受理 5](#_Toc165985106)

[6.2 型式试验 6](#_Toc165985107)

[6.3 认证决定 6](#_Toc165985108)

[6.4 认证工作时限 7](#_Toc165985109)

[6.5 获证后监督 7](#_Toc165985110)

[6.5.1 获证后监督频次 7](#_Toc165985111)

[6.5.2 获证后监督方式 8](#_Toc165985112)

[6.5.3 获证后监督结果决定 8](#_Toc165985113)

[6.6 再认证 8](#_Toc165985114)

[7 认证证书 8](#_Toc165985115)

[7.1 认证证书有效期 8](#_Toc165985116)

[7.2 认证证书和认证标志的使用 8](#_Toc165985117)

[7.2.1 认证证书的使用 8](#_Toc165985118)

[7.2.2 认证标志的使用 9](#_Toc165985119)

[7.3 认证证书的管理 9](#_Toc165985120)

[7.3.1 变更认证证书 9](#_Toc165985121)

[7.3.2 暂停认证证书 9](#_Toc165985122)

[7.3.3 撤销认证证书 10](#_Toc165985123)

[7.3.4 注销认证证书 10](#_Toc165985124)

[8 收费 10](#_Toc165985125)

|  |  |
| --- | --- |
| 北京赛迪认证中心有限公司 | 认证实施规则 |
| 自愿性产品认证实施规则  软件供应链安全能力认证 | 文件编号：  CCID-Gz70736-2023 |
| 版次：01版第01次修订 | 实施日期：2023-11-30 |
| 修订日期：2024-04-30 |

**前言**

本认证实施规则由北京赛迪认证中心有限公司（以下简称赛迪认证中心）发布。本规则版权归赛迪认证中心，未经赛迪认证中心许可，任何组织及个人不得以任何形式全部或部分引用、使用本规则。当认证依据的标准、认证实施规则及有关要求发生变更时，本认证实施规则与赛迪认证中心发布的后续有关文件一并使用。

本版规则发布日期：2023年11月30日

参与起草单位：北京赛迪认证中心有限公司

本规则于2024年4月30日第1次修订，主要变化如下：

-依据标准增加GB/T 43698-2024《信息安全技术 软件供应链安全要求》

-机构职责及人员能力要求增加签约检测机构的相关要求

-修订完善了获证后监督的相关要求

-修订完善了认证证书管理的相关要求，包括变更、暂停、撤销、注销认证证书。

如需获取更多信息，请登录网站查询，或通过以下电话、邮件咨询，

联系方式如下：

地址：北京市海淀区赛迪大厦

网址： http://rz.cstc.org.cn/ 电话： 010-88559261 （业务咨询）

1. 适用范围

本规则用于赛迪认证中心开展软件供应链安全能力测评活动。包括以下软件类别：操作系统产品、数据库产品、中间件产品、云计算产品、办公软件、安全软件、应用系统产品的自愿性产品认证。

1. 认证依据

以CCID-JF-07020-2023《软件供应链安全能力测评规范》为认证依据，该测评规范将根据中央及国家相关规定、标准或技术要求的发布、产业发展、市场需求及其它因素，进行适时修订。

1. 认证模式

型式试验+获证后监督

1. 机构职责及人员能力要求

## 赛迪认证中心

赛迪认证中心主要职责如下：

1）负责编制认证规则、测评规范等认证工作的公开文件；

2）签约检测机构的认定和签约；

3）受理认证申请，负责审查申请材料的完整性和符合性；

4）做出认证决定，签发认证证书，实施认证后续监督；

5）受理认证申诉，处理认证投诉。

认证决定人员要求如下：

1. 具有相关专业教育和工作经历；
2. 熟悉GB/T 36637-2018《信息安全技术 ICT供应链安全风险管理指南》、GB/T 43698-2024《信息安全技术 软件供应链安全要求》等国家标准，具备相关的专业知识。

## 签约检测机构

签约检测机构受赛迪认证中心的委托，由检验员依据CCID-JF-07020-2023《软件供应链安全能力测评规范》开展软件供应链安全能力测评工作，并出具软件供应链安全能力测评报告。

检验员要求如下：

1. 熟悉适用的法律、法规和测评程序；
2. 熟悉GB/T 36637-2018《信息安全技术 ICT供应链安全风险管理指南》、GB/T 43698-2024《信息安全技术 软件供应链安全要求》等国家标准，理解相应的测评方法；
3. 了解信息安全、软件供应链安全等相关技术；
4. 具有计算机、信息技术、网络安全等相关专业背景或从业经历；
5. 检验员需经过软件供应链安全相关培训，通过考核及上岗审批。

## 认证委托方

认证委托方按照赛迪认证中心《申请人需向CCID和检测机构提交的资料》提供关于软件供应链安全能力认证所需的材料和证明文件，认证委托方应确保文件内容的真实性、有效性。认证委托方应配合签约检测机构开展软件供应链安全能力测评活动。

1. 认证流程



图 1软件供应链安全能力认证流程图

1. 认证实施

## 认证申请及受理

认证委托方向赛迪认证中心提出认证申请，按照赛迪认证中心提供的《自愿性产品认证申请书》填写相应内容（申请书模板详见赛迪认证中心官方网站）。申请认证材料包括但不限于：

1. 《自愿性产品认证申请书》（加盖单位公章，纸版和电子版各一份），明确认证委托方基本信息、申请认证产品的软件名称及版本号、申请软件供应链安全能力等级等信息；
2. 认证委托方的工商营业执照（或事业单位法人证）复印件（加盖单位公章）；
3. 软件产品的说明或用户手册；
4. 软件产品的计算机软件著作权登记证书。

原则上，同一认证委托方、同一软件产品研发单位、同一类别、同一版本为同一个自愿性产品认证单元。相同软件产品研发单位、不同软件版本，或同一软件类别及版本、不同认证委托方，作为不同的认证单元。

赛迪认证中心收到申请书后，对认证申请材料进行文档审查，包括产品/系统名称及版本号/型号、产品类别、产品认证标准等相关内容，确定文件内容完整性、一致性、合规性等内容，并在5个工作日内确认是否受理认证申请。若文档审查不通过，则要求委托方按照审查意见补充申请材料。

## 型式试验

型式试验由赛迪认证中心签约检测机构的检验员在规定的时间内依据CCID-JF-07020-2023《软件供应链安全能力测评规范》的相关要求实施，测评的样品包括需认证的软件产品，以及与产品对应的功能说明书、用户手册或相关技术文档。检验员通过文档审核、系统验证、工具检测等方式对申请认证的软件产品开展测评工作，详细记录测评内容，判定测评结果，实验室应确保测评结论真实、准确，对测评全过程做出完整的记录并归档留存，以保证测评过程和结果的记录具有可追溯性。型式试验后，出具软件供应链安全能力测评报告。

若存在不符合的测评项，实验室将通知认证委托方进行整改。若认证委托方在一年内3次整改仍未合格，则认为此次测评不合格。认证委托方如还希望获得赛迪认证中心认证，需重新提出认证申请。测评通过后，实验室向赛迪认证中心提交测评报告。

## 认证决定

赛迪认证中心检查员按照《初次认证文件审核报告》的审核内容对相关材料进行审核并形成审核结果。

赛迪认证中心认证决定人员按照《认证评价和决定记录表》的要求对相关资料进行综合审查和评价，形成认证评价意见，做出“通过认证”或“不通过认证”的决定。

对于授予认证资格的认证委托方，对其颁发认证证书，明确申请单位名称、申请单位地址、软件产品名称/版本号、软件供应链安全能力等级等信息，并通过赛迪认证中心官方网站发布赛迪认证中心公告。对于不授予认证资格的认证委托方，以书面形式通知其不能获得认证资格的原因。

## 认证工作时限

认证工作时限是指自认证申请正式受理之日起至颁发认证证书时止所实际发生的工作日，包括型式试验、认证决定评定和批准时间、证书制作时间。

型式试验时间一般不超过60个工作日（因测评项不符合，进行整改的时间不计算在内，整改时间一般不超过2个月），在测评项通过的情况下于15个工作日内提交测评报告。

认证决定评定和批准时间、证书制作时间共计不超过10个工作日。

认证委托人应配合赛迪认证中心的相关工作。由于认证委托人自身原因逾期未完成认证活动导致认证超时的，不计入认证时限内。

## 获证后监督

### 获证后监督频次

一般情况下，获证产品从证书批准之日起，即可安排证后监督。证后监督每12个月不少于一次。

如发生下述情况之一时，可增加证后监督频次：

（1）获证产品出现严重安全问题或用户对软件产品供应链安全保障有投诉并经查实为持证人责任的；

（2）赛迪认证中心有足够理由对获证产品与认证要求的符合性提出质疑时；

（3）有足够信息表明因软件产品成分、供应活动、组织机构等变更，从而可能影响软件产品供应链安全时。

赛迪认证中心可根据申请认证单位的软件产品特性等原因适当延长监督周期，一般不超过6个月。由于不可抗拒因素需要延长监督周期的，经赛迪认证中心研究同意并做出延长监督周期的决定。

### 获证后监督方式

获证后监督由赛迪认证中心检查员实施，可采用现场检查，也可视情况利用远程信息化手段开展。对已获证的软件产品，依据初次测评结果选取重点指标项进行再次确认。

### 获证后监督结果决定

赛迪认证中心经评价做出监督结论，并将监督结论通知认证委托人。监督结论分为“通过”或“不通过”。凡存在下列情况之一的，监督结论为“不通过”：

（1）获证后监督检查存在不符合项；

（2）不符合项整改时间超过3个月。

若获证后监督结论为“通过”，赛迪认证中心保持其证书；若获证后结论为“不通过”或不能按要求接受获证后监督的，赛迪认证中心按规定暂停或撤销其证书。

## 再认证

认证证书有效期满的前三个月内，获证方可申请再认证，即重新申请认证。

1. 认证证书

## 认证证书有效期

本规则覆盖的软件供应链安全能力认证证书有效期为3年。有效期满后可重新提出认证申请。

## 认证证书和认证标志的使用

### 认证证书的使用

认证证书是赛迪认证中心颁发给认证委托方证明其符合认证要求的证明文件。认证证书可以展示在文件、网站、通过认证的工作场所、销售场所、广告和宣传资料中或广告宣传等商业活动，但不得利用认证证书和相关文字、符号，误导公众认为认证证书覆盖范围外的技术特性获得认证。

认证证书不得伪造、变造、冒用、买卖和转让，获证组织应妥善保管好证书，以免丢失、损坏。

### 认证标志的使用

认证标志由获证单位向赛迪认证中心提出使用申请，获得书面授权后按照赛迪认证中心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。

认证标志使用时，应与获证组织单位名称和软件名称/版本放在一起。在使用标志图案时，应按照赛迪认证中心规定的图样以相应的比例放大或缩小。

认证标志样式如下：



## 认证证书的管理

### 变更认证证书

（1）获证方基本信息的变更

当获证方软件产品名称或申请单位名称等发生变更时，应向赛迪认证中心提出变更申请，并提交相关变更申请材料。赛迪认证中心组织进行相关审查活动，并按照要求做出认证决定。

（2）获证软件版本或相关供应活动的变更

获证后的软件产品版本或相关供应活动发生变更时，应向赛迪认证中心提出变更申请，并附上软件相关变更声明（需加盖公章）。赛迪认证中心根据获证方提供的变更声明和相关资料进行综合评价，以确定是否可以变更。对于影响软件产品供应链安全能力的变更，应对变更后的软件产品进行重新测评，测评合格后方能进行变更，并换发新证书；对于不影响软件产品供应链安全能力的变更，原则上不需要进行重新测评。

### 暂停认证证书

获证方有下列情形之一的，赛迪认证中心将暂停认证证书。

（1）未按照规定申请获证后监督；

（2）未按照规定申请再认证；

（3）获证方未按规定使用认证证书；

（4）获证方未履行与赛迪认证中心签署的认证合同中规定的责任和义务，如未按时支付认证费用等；

（5）获证方主动请求暂停；

（6）在特定时期国家或行业管理部门有要求予以暂停的。

暂停期限一般为3个月。在3个月内，获证方可提出恢复证书的申请，赛迪认证中心经再次测评、批准后，方可使用该证书。在认证证书暂停期间，获证组织不得继续使用证书。

### 撤销认证证书

获证方有下列情形之一，赛迪认证中心将撤销其认证证书。

（1）获证方出现严重问题，在短期内无法恢复符合性的或在认证范围内无法满足适用的最新法律法规、认证标准规范的要求，并在短期内无法采取措施或采取措施无效的；

（2）获证方不接受赛迪认证中心对其实施的或未申请再认证的；

（3）认证证书暂停使用期间，获证方未采取有效纠正措施。

### 注销认证证书

获证方因为自身原因申请注销认证证书，赛迪认证中心将给予注销。认证证书注销和撤销后，赛迪认证中心将收回认证证书，并在赛迪认证中心网站上予以公告。

1. 收费

认证及测评的收费以赛迪认证中心和签约检测机构正式发布的收费文件为准。