编号：NFCC-IR-000-03

金融机构人脸识别数据处理能力认 证实施规则 V1.0/0

2023-07-28 发布

2023-07-28 实施

重庆国家金融科技认证中心有限责任公司 发布

目 录

1 适用范围	1
2 认证依据	1
3 认证模式	1
4 认证基本环节	1
5 认证实施程序	2
5.1 认证委托	2
5.2 认证申请及受理	2
5.2.1 认证单元的划分	2
5.2.2 申请资料要求	2
5.3 技术验证（检测）及实施	3
5.3.1 技术验证（检测）	3
5.3.2 检测（技术）报告的提交	4
5.4 文件审查	4
5.5 现场检查	4
5.6 认证决定	5
5.7 认证时限	5
5.8 获证后监督	6
5.8.1 监督方式和频次	6
5.8.2 获证后监督结果的评价	6
6 认证证书	7
6.1 认证证书的保持	7
6.2 认证证书的使用	7
6.3 认证证书的管理	7
6.3.1 变更认证证书	7
6.3.2 暂停认证证书	8
6.3.3 撤销认证证书	9
6.3.4 注销认证证书	9
7 收费	9
附录 1：认证依据适用性说明	10

1 适用范围

本规则所指的人脸识别数据处理能力认证,是指对提供或使用人脸识别产品的机构在处理数据的收集、存储、使用、提供、公开、删除等方面进行的标准符合性认证。

适用机构包括但不限于:商业银行、金融科技企业以及相关产业机构开展人脸识别服务时受理终端、业务系统、客户端软件等的设计、生产、集成与应用。

2 认证依据

- GB/T 41819-2022《信息安全技术 人脸识别数据安全要求》;
- JR/T 0171-2020《个人金融信息保护技术规范》(适用时);

3 认证模式

人脸识别数据处理能力认证的认证模式为:

技术验证(检测)+文件审查+现场检查+获证后监督

获证后监督是指获证后的跟踪检查、生产现场抽取样品检测、市场抽样检测三种方式之一或组合。

4 认证基本环节

认证基本环节包括:

- (1) 认证申请及受理
- (2) 技术验证(检测)
- (3) 文件审查
- (4) 现场检查
- (5) 认证决定

(6) 获证后监督

5 认证实施程序

5.1 认证委托

认证委托方向指定的认证机构申请认证，认证机构对申请材料进行审核，确认合格后进行受理。检测机构（由认证委托方自主从指定检测机构名单中选取）应依据相关标准和技术规范进行检测，完成后向认证机构提交检测(技术)报告。认证机构针对检测（技术）报告及其他技术材料进行文件审查，组织进行现场检查。认证机构对检测、文件审查、现场检查的结果进行综合评价，向评价合格方颁发认证证书。认证机构组织对获证后的产品进行定期的监督。

5.2 认证申请及受理

5.2.1 认证单元的划分

原则上应按所申请人脸识别产品/系统的版本号申请。

5.2.2 申请资料要求

认证机构应当明确认证委托资料要求，应提交的材料包括但不限于：

- (1) 申请基本信息（纸质和电子各 1 份，须加盖公章）
 - 认证申请书。
 - 认证委托方营业执照复印件。
 - 无外包情况说明。
 - 近一年内是有无投诉的声明（适用时）。
- (2) 送检样品及其说明文档（适用时）
- (3) 相关管理制度文件
- (4) 技术文档（电子 1 份）

开发设计类文档，如安全设计文档、开发手册、接口文档、数据库设计/存储文档、操作手册、测试用例、相关测试报告等；

软件过程管理文件，如变更控制文档、发布管理、安全管理制度、运维管理制度等。

个人信息保护自查结果。

(5) 外包情况说明

认证机构认为有需要时，认证委托方需提供外包管理材料（适用于将产品研发、运维和安全管理等外包给第三方机构的认证委托方，提交纸质或电子版 1 份），至少包括：外包合同、外包安全保密协议等。

如果认证委托方在申请认证时，也提供了在认证申请范围内被认证对象的型式检测（技术）报告，则该检测（技术）报告应由认证机构公布的检测机构名录中的检测机构出具，且报告出具时间不能超过申请认证时限 6 个月。

5.3 技术验证（检测）及实施

5.3.1 技术验证（检测）

检测机构依据本文第 2 部分：认证依据、适用的法律法规及其他要求，对认证委托方样品的标准符合性进行检测。

(1) 送样原则（适用时）

依照认证委托方认证单元中确定的产品/系统名称/版本，送该产品/系统名称/版本的样品，若样品运行在专用移动终端硬件设备环境下时，需提供可运行该样品的所有不同型号的移动终端硬件设备（每型号 1 部）。

(2) 送样要求（适用时）

提供载有可安装运行送检软件的光盘或其它介质。介质和其外包装上应有产品/系统名称、版本号、生产单位和联系方式等标识。

若采用专用移动终端硬件设备时，应提供专用移动终端硬件设备清单，清单内容包括：硬件设备型号、硬件配置、不同型号的设备数量、操作系统环境和基本软件配置等。

软件产品的用户文档一份，用户文档包括电子文档，文档内容也包括封面、

目录、页码等，封面内容包含软件名称、版本号、软件生产单位和联系方式等标识，纸质文档应装订成册。文档至少应包括以下内容：

环境要求：软件运行要求的软件、硬件、网络等最低配置说明等；

软件应用范围和对象的说明

软件安装过程指南；

软件操作使用说明；

使用软件的具体操作和步骤，用例图加以说明等。

检测的样品由认证委托方负责选送，并对选送样品负责。

（3）样品处置

检测机构应对技术验证（检测）过程中的样品至少保存三年，认证失效后，认证委托方可向检测机构申请取回样品。

5.3.2 检测（技术）报告的提交

检测机构应于检测工作完成后 10 个工作日内向认证机构提交检测（技术）报告（电子一份）。

其他相关资料由认证委托方和检测机构妥善处置。

5.4 文件审查

认证机构在收到检测机构出具的检测（技术）报告及相关材料后，安排检查员进行文件审查。文件审查的范围包括所有申请材料及检测报告。

文件审查依据“2. 认证依据”章节的标准及相关法规要求对认证申请范围内的被认证对象的标准符合性进行审查，获取认证委托方所提供的被认证对象是否符合认证规范的证据。如有与申请认证业务范围相关的投诉记录，应分析对认证要求符合性的影响。

原则上，每款产品/系统文件审查一般为 2 至 4 个人日。

5.5 现场检查

证机构依据“2. 认证依据”章节的标准及相关法规要求，对认证委托方申请

范围内的客户端软件的数据的收集、存储、使用、提供、公开、删除等方面进行抽查，获取认证委托方持续满足认证要求的证据。

原则上，每款产品/系统现场检查一般为 2 至 4 个人日。

5.6 认证决定

认证机构根据认证委托资料、检测（技术）报告、现场检查结果和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。如发现认证委托人、网络运营者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。如认证决定过程中发现不符合认证要求项，允许限期（通常情况下不超过 3 个月）整改，如期完成整改后，认证机构采取适当方式对整改结果进行确认，重新执行认证决定过程。对于不授予认证资格的认证委托方，认证机构应向其以书面形式明示不能获得认证资格的原因。

5.7 认证时限

认证时限是指自申请被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。其中，认证机构在收到认证委托方的认证申请后，于 5 个工作日内完成申请资料审核，审核通过后受理认证申请。补充材料时间不计算在内。检测机构收到样品（适用时）后，于 20 个工作日内完成检测，整改时间及补充材料时间不计算在内。认证机构收到检测（技术）报告后，于 5 个工作日内完成认证检查安排。认证检查完成后，认证机构于 15 个工作日内完成发证流程。认证时限一般在 80 个工作日内，最长不应超过 120 个工作日。各认证环节整改时间及补充材料时间不计算在内。

5.8 获证后监督

5.8.1 监督方式和频次

证后监督的常规方式为技术验证（检测）+文件审查+现场检查。检测在证后监督环节应至少每 3 年覆盖所有检测项。

初次认证后的第一次监督应在认证证书签发日期 12 个月内进行。以后，监督应当至少每个日历年进行一次，且两次监督的时间间隔一般情况下不超过 15 个月。每次证后监督原则上由认证机构提前 3 个月通知获证机构（必要情况下，认证机构可采取事先不通知的方式对获证机构实施监督）。

获证机构如出现以下情况之一，认证机构可视情况增加证后监督审查的频次：

（1）获证产品出现严重质量问题时，或者用户提出投诉并经查实为证书持有者责任时。

（2）认证机构有足够理由对获证产品与本规则中规定的标准要求符合性提出质疑时。

（3）有足够信息表明获证机构因组织机构、生产条件、质量管理体系等发生变更，从而可能影响产品质量时。

证后监督现场检查时间根据获证产品的单元数量确定，并适当考虑获证机构的生产规模及变更情况。一般不超过初次认证的人日数。证后监督现场检查的方式和内容参照 5.5。

5.8.2 获证后监督结果的评价

认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形作出暂停直至撤销认证证书的处理。

6 认证证书

6.1 认证证书的保持

认证证书有效期为 3 年。在有效期内，通过每年对获证产品进行监督，确保认证证书的有效性。

证书到期需延续使用的，认证委托人应当在有效期届满前 6 个月内提出认证委托。认证机构应当采用获证后监督的方式，对符合认证要求的委托换发新证书。

6.2 认证证书的使用

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、广告和宣传资料或广告宣传等商业活动中，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产品、服务、管理体系获得认证，宣传认证结果时不应损害认证机构的声誉。

认证证书不准伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印。获证机构应妥善保管好证书，以免丢失、损坏。如发生证书丢失、损坏的，获证机构可申请补发。

获证机构应建立认证证书、审核报告使用和管理制度，对认证证书的使用情况如实记录存档。

6.3 认证证书的管理

6.3.1 变更认证证书

认证证书有效期内，若发生下列情况之一，获证机构应向认证机构提出变更申请。认证机构策划并实施适宜的审查活动，并按照要求做出认证决定。审查活动可与证后监督同时进行。

- (1) 产品/系统名称/版本变更。
- (2) 证书持有者变更。

(3) 委托人名称及地址、制造商名称及地址、生产企业名称及地址变更。

(4) 认证所依据标准的改变。

如果产品发生功能/版本变化，获证机构应提交变更后产品与已获证产品之间的差异性说明，由认证机构评估是否进行检测和/或现场检查。

如果获证机构需要扩大/缩小认证范围时，应向认证机构同时提交扩大/缩小范围的理由、事实的说明，以及扩大的产品与已获证产品之间的差异性说明。认证机构应按照核查扩大/缩小认证范围与原认证范围的一致性和差异，确认原认证结果对扩展产品的有效性，需要时应针对扩大/缩小认证范围和其对原认证范围的影响进行检测和现场检查，并根据获证机构的要求单独颁发认证证书或换发认证证书。

如果认证变更只涉及到注册名称、注册地址的变更，获证机构须递交变更申请，经书面审查批准后，认证机构仅对证书更新并收回原证书。

认证所依据标准发生变更时，认证机构应通知相关获证机构，并要求其在规定的时间内重新申请认证。

6.3.2 暂停认证证书

获证机构有下列情形之一的，认证机构应当暂停认证证书。

(1) 未按照规定及时接受证后监督审查。

(2) 获证机构未按规定使用认证证书和认证标志。

(3) 监督结果证明获证机构不符合认证要求，但不需要立即撤销认证证书。

(4) 获证机构未履行与认证机构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) 获证机构主动请求暂停。

(6) 在特定时期国家或行业管理部门有要求予以暂停的。

(7) 获证机构出现严重问题或获证机构发生重大安全事故。

暂停期限一般为3个月。在3个月内，获证机构可提出恢复证书的申请，认证机构经审查、批准后，方可使用该证书。在认证证书暂停期间，获证机构不得使用证书。

6.3.3 撤销认证证书

获证机构有下列情形之一，认证机构应当撤销其认证证书。

(1) 获证机构出现严重问题，在短期内无法恢复符合性的或获证机构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) 获证机构发生重大安全事故，造成客户资金安全受到威胁或损失，造成社会不良影响，或潜在风险短期内无法消除的。

(3) 获证机构不接受认证机构对其实施的证后监督审查。

(4) 认证证书暂停使用期间，获证机构未采取有效纠正措施。

(5) 认证证书暂停使用期满，获证机构未申请恢复证书。

认证证书撤销后，认证机构应收回认证证书，并在认证机构官方媒体上予以公告。自证书撤销之日起，获证机构不得继续使用认证证书，或宣称获得该认证。

6.3.4 注销认证证书

获证机构因为自身原因申请注销认证证书，认证机构应当给予注销。

认证证书注销后，认证机构应收回认证证书，并在认证机构官方网站上予以公告。

7 收费

收费由认证机构、检测机构按国家有关规定统一收取。

附录 1：认证依据适用性说明

根据对本实施细则适用范围的分析，原则上，JR/0171-2020《个人金融信息保护技术规范》标准 6.1.1 条款、6.1.2 条款、6.1.3 条款、6.1.5 条款、6.1.6 条款、7.2 条款、7.5 条款适用于本实施细则，且认证机构可根据实际实施情况适当调整。