ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0299—2024

个人征信电子授权安全技术指南

Technical guidelines for security of electronic authorization for personal credit investigation

2024-01-15 发布　　2024-01-15 实施

中国人民银行　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国人民银行征信管理局提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国人民银行征信管理局，中国人民银行北京市分行、山东省分行，中金金融认证中心有限公司、中国银联股份有限公司、网联清算有限公司、中国邮政储蓄银行股份有限公司、重庆工商大学、山东财经大学、北京国家金融科技认证中心有限公司、中国光大银行股份有限公司、中国工商银行股份有限公司、武汉仲裁委员会、广西北部湾银行股份有限公司、中国科学院信息工程研究所、蚂蚁科技集团股份有限公司、北京百度网讯科技有限公司、深圳市腾讯计算机系统有限公司、京东科技控股股份有限公司、梅赛德斯-奔驰汽车金融有限公司。

本文件主要起草人：田地、杜静、常可、刘维特、曾志诚、林晓东、阚胜国、冯巍威、王秋香、马征、韩婷婷、朱钢、李达、李松涛、马春旺、谢宗晓、王自冲、隆峰、左小军、张诚、汤洋、郭林、廖渊、甄杰、董坤祥、李宽、史晨阳、夏雯君、武利娟、杨泽、母洪春、叶友、熊刚、李镇、夏葳、陆碧波、彭晋、王海棠、李克鹏、陈明、孙中伟、孙瑞。

引　言

在消费升级和金融科技共同推动下，金融机构线上个人信贷业务日益增长，线上渠道成为金融机构开展个人信贷业务的主要方式。金融机构办理个人信贷业务时，一般要在取得个人信息主体授权同意后，查询个人征信信息。线上信贷业务的发展凸显了电子方式取得个人信息主体有效征信授权的重要性。

为解决金融机构取得个人征信电子授权过程中普遍存在的鉴别手段简单、缺少安全可靠电子签章、缺乏存证意识等突出问题，保障个人征信电子授权的真实性和有效性，促进线上信贷业务健康规范发展，特制定本文件。

个人征信电子授权安全技术指南

1 范围

本文件提供了个人征信电子授权安全技术指南，包括个人征信电子授权机制、线上有效鉴别个人身份、签发数字证书、签署有效征信授权电子协议、存证有效征信授权电子数据、数据安全、个人信息保护等内容。

本文件适用于金融领域涉及个人征信电子授权的业务。

示例：征信信息采集、报送、查询等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

GB/T 27913—2022 用于金融服务的公钥基础设施 实施和策略框架

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范

GM/T 0015—2012 基于SM2密码算法的数字证书格式规范

JR/T 0118—2015 金融电子认证规范

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0223—2021 金融数据安全 数据生命周期安全规范

SF/T 0076—2020 电子数据存证技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子协议 electronic agreement

平等主体的自然人、法人、其他组织之间通过电子信息网络以电子的形式达成的设立、变更、终止民事权利义务关系的协议。

[来源：GB/T 36298—2018，3.1，有修改]

3.2

电子认证机构 certification authority；CA

对数字证书进行全生命周期管理的实体。

注：电子认证机构即证书认证机构。

[来源：JR/T 0118—2015，3.2]

3.3

注册机构 registration authority

受理数字证书的申请、更新、恢复和注销等业务的实体。

[来源：JR/T 0118—2015，3.3]

3.4

数字证书 digital certificate

由国家认可的，具有权威性、可信性和公正性的电子认证机构进行数字签名的一个可信的数字化文件。

[来源：GB/T 20518—2018，3.7，有修改]

3.5

电子签章 electronic seal

使用电子印章签署电子文件的过程。

[来源：GB/T 38540—2020，3.2]

3.6

时间戳 time stamp

对时间和其他待签名数据进行签名得到的数据。

注：时间戳用于表明数据的时间属性。

[来源：GM/Z 0001—2013，2.100，有修改]

3.7

电子数据存证 digital evidence preservation

通过互联网向用户提供电子数据证据保管和验证的服务。

[来源：SF/T 0076—2020，3.1]

3.8

电子数据存证服务提供者 digital evidence preservation provider

提供电子数据存证服务的机构或组织。

[来源：SF/T 0076—2020，3.2]

4 个人征信电子授权机制

个人征信电子授权机制作用是由个人通过金融业务终端以电子签名的方式对本人电子征信进行授权，允许金融业务系统查询其个人征信信息。为确保个人征信电子授权的真实性、完整性、不可否认性，对线上有效鉴别个人身份、申请和签发数字证书、签署有效征信授权电子协议等过程进行存证。金融机构采用上述机制，在有效授权内开展活动，其中涉及的个人征信电子授权基本系统组件如下表所示。

表 个人征信电子授权基本系统组件

系统组件	说明
C_1（业务系统）	开展金融业务，调用其他组件实现个人征信电子授权机制的系统。
C_2（数字证书注册系统）	负责数字证书的申请、发放以及存储的系统。
C_3（CA系统）	负责受理证书申请，签发数字证书，并对数字证书全生命周期进行管理的系统。
C_4（业务终端系统）	承载金融业务，与C_1（业务系统）协同，金融客户使用C_4（业务终端系统）办理金融业务及执行个人征信电子授权的客户端软件。
C_5（存证系统）	负责电子证据数据存证，受理上述组件系统的电子数据，并履行存证流程的系统。

个人征信电子授权机制如下图所示。

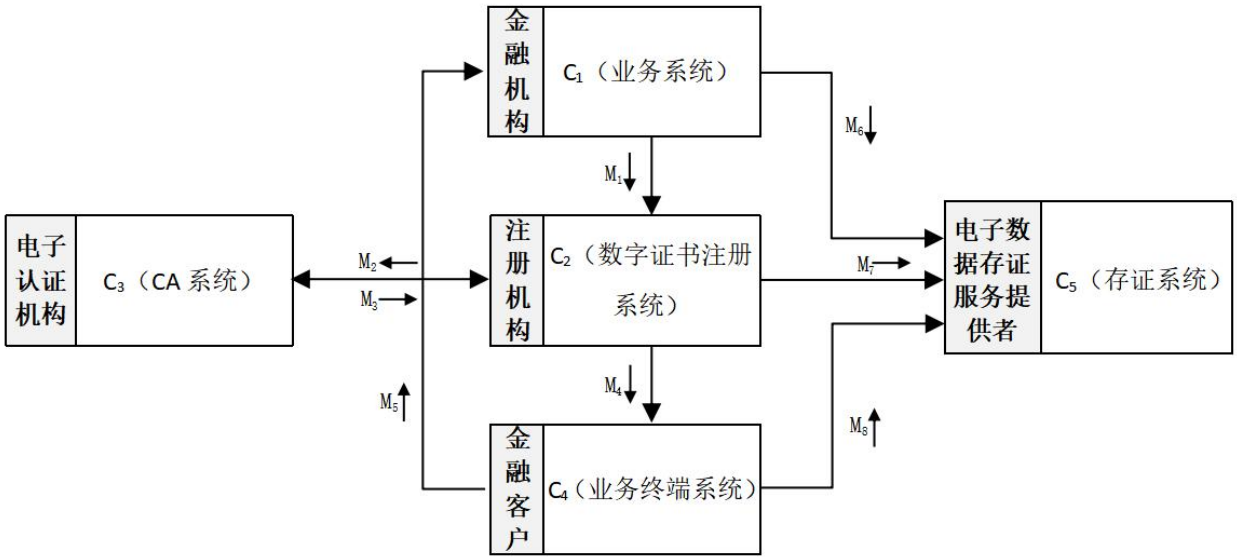

图　个人征信电子授权机制

个人征信电子授权机制的基本工作过程如下。

a）步骤M_1：金融机构C_1（业务系统）对金融客户开展身份鉴别，鉴别无误后，C_1（业务系统）向注册机构C_2（数字证书注册系统）提交金融客户数字证书申请信息。

b）步骤M_2：注册机构C_2（数字证书注册系统）受理来自C_1（业务系统）的数字证书申请信息，并提交给电子认证机构的C_3（CA系统）。

c）步骤M_3：电子认证机构C_3（CA系统）签发数字证书，并将该证书交付给注册机构的C_2（数字证书注册系统）。

d）步骤M_4：注册机构C_2（数字证书注册系统）接收数字证书并发放给金融客户，根据数字证书存储方案，选择存储在C_4（业务终端系统）、C_1（业务系统）或为C_1（业务系统）提供签名签章服务的关联系统中。

e）步骤M_5：金融客户使用C_4（业务终端系统）协同C_1（业务系统）签署有效征信授权电子协议，并将签署后的电子协议文件保存到C_1（业务系统）或保存到为C_1（业务系统）提供存储服务的关联系统中。

f）步骤M_6：金融机构C_1（业务系统）将身份鉴别过程和结果数据发送给电子数据存证服务提供者的C_5（存证系统）进行存证。

g）步骤M_7：注册机构C_2（数字证书注册系统）将证书申请、发放过程和结果数据发送给电子数据存证服务提供者的C_5（存证系统）进行存证。

h）步骤M_8：金融机构C_1（业务系统）统筹C_4（业务终端系统）授权协议签署过程和结果数据发送给电子数据存证服务提供者的C_5（存证系统）进行存证。

注：根据业务模型设计，步骤M_6、步骤M_7、步骤M_8能分阶段进行，也能在业务办结后统一进行。

5　线上有效鉴别个人身份

5.1　鉴别原则

金融机构宜以有效性为原则，充分鉴别个人身份，同时，宜仅采集身份鉴别所必需的最少信息，保护个人信息安全。

注：1. 金融领域有权判定鉴别手段效力的机构通常为金融管理机构和司法机构。金融机构履行客户尽职调查、身份鉴别义务时，必须按照法律、行政法规、部门规章的规定进行核查。

2. 有关法律、行政法规、部门规章规定了对于身份鉴别最少信息进行核查的内容，例如《常见类型移动互联网应用程序必要个人信息范围规定》（国信办秘字〔2021〕14 号文印发），以保证个人信息采集的合法、正当、必要。

5.2 线上鉴别个人身份

5.2.1 线上鉴别个人身份宜采取身份证鉴别和其他2种及以上成熟的身份鉴别措施对个人身份有效性进行鉴别。身份鉴别方式包括以下内容。

a）身份证鉴别：联网核查公民身份信息，宜同步鉴别身份证件真伪。

b）其他经过实践验证有效且被广为接受的身份鉴别措施。

示例：生物特征、银行卡、运营商实名验证等技术较为成熟、应用较为广泛的多种身份鉴别措施。

5.2.2 使用数字证书鉴别个人身份满足以下条款的，不必进行上述方式的身份鉴别。

a）使用网银智能密码钥匙中存储的电子认证机构数字证书，以及移动终端满足GB/T 37092—2018中密码模块安全二级及以上规定的数字证书开展身份鉴别。

b）验证数字证书有效性和该数字证书产生的电子签名有效性。

6 签发数字证书

6.1 电子认证机构

电子认证机构宜满足JR/T 0118—2015中5.1.1的内容。

6.2 数字证书格式及名称

数字证书格式及名称包括以下内容。

a）对采用国家密码管理部门认可的国产密码算法数字证书宜符合GM/T 0015—2012的相关内容。

b）标识个人身份的数字证书（以下简称个人证书）命名宜包括对应自然人名称信息。

c）电子认证机构不宜将同一数字证书主体名称的证书签发给不同的用户。

6.3 个人身份鉴别

电子认证机构签发数字证书时，可自行或授权金融机构作为注册机构执行个人身份鉴别工作、受理个人数字证书申请等。金融机构作为注册机构宜与电子认证机构约定向个人履行有关申请数字证书的提示告知义务，例如金融机构明确告知授权个人数字证书申请与金融业务开展过程中的身份鉴别同时进行。双方宜明确技术要求，金融机构采集和保存告知、开展有效身份鉴别的记录材料。

6.4 证书策略和认证业务说明

电子认证机构宜对数字证书制定证书策略，并在认证业务说明中对有关内容予以阐述。证书策略和认证业务说明包括以下内容。

a）证书策略宜满足GB/T 27913—2022中6.1的内容。

b）认证业务说明宜满足GB/T 27913—2022中6.2的内容。

6.5 证书生命周期操作

证书生命周期管理涵盖证书签发、证书更新、证书挂起、证书解挂和证书注销等管理操作，宜满足JR/T 0118—2015中5.2.3的内容。

6.6 数字证书存储安全

宜采取个人证书存储安全的有效措施，防止因私钥泄露导致个人征信电子授权业务风险。有效措施包括以下内容。

a）对于证书采用硬件介质存储的，宜满足 JR/T 0118—2015 中 6.2.1 的内容。

b）对于证书采用非硬件介质存储的，宜采用安全密码模块实现密码运算、密钥管理等功能，并满足 GB/T 37092—2018 中 5.3（密码模块安全二级）的内容。

c）对于实时性要求较高的场景个人证书，其密钥的生成、应用、销毁宜在内存操作，对于管理和使用场景个人证书的信息系统，宜符合 GB/T 22081—2016 中第 9 章的内容。

7 签署有效征信授权电子协议

7.1 电子签章生成流程

使用数字证书对电子授权协议进行电子签章，宜具备完整性、防篡改性和抗抵赖性。
电子签章生成流程宜满足 GB/T 38540—2020 中 7.2 的内容。

7.2 电子签章验证流程

电子签章验证流程宜满足 GB/T 38540—2020 中 7.3 的内容。

7.3 时间戳

电子授权协议宜加盖时间戳，宜满足JR/T 0118—2015中6.4.6的内容。

7.4 机密性

电子授权协议的机密性宜满足 JR/T 0118—2015 中 6.4.5 的内容。

8 存证有效征信授权电子数据

8.1 电子数据存证服务提供者

电子数据存证服务提供者宜满足SF/T 0076—2020中第4章的内容。

8.2 电子数据存证过程

电子数据存证过程宜满足SF/T 0076—2020中第6章的内容。

8.3 电子数据存证范围

个人征信电子授权各业务环节存证范围包括以下内容。
a）个人身份鉴别过程及结果。
b）签发数字证书过程及结果。
c）签署个人征信授权电子协议过程及结果。
d）其他相关业务环节的过程及结果。

8.4 出具有效征信授权佐证材料

验证个人征信电子授权有效性时，宜在线上或线下出具个人征信电子授权佐证材料。佐证材料包括以下内容。
a）个人征信电子授权业务报告，其模板见附录 A。
b）个人征信电子授权电子签章验证报告，其模板见附录 B。
c）个人征信电子授权电子数据验证报告，其模板见附录 C。
d）其他与个人征信电子授权相关的材料。
e）为充分证明个人征信电子授权的有效性，宜同时出具附录 A、附录 B、附录 C 所述佐证材料。

9 数据安全及个人信息保护

个人征信电子授权过程中的数据安全和个人信息保护，宜满足以下内容。
a）数据安全宜满足 JR/T 0223—2021 的内容。
b）个人信息保护宜满足 JR/T 0171—2020 的内容。

附 录 A
（资料性）
个人征信电子授权业务报告

业务发生机构全面说明业务基本情况、业务办理流程及征信业务相关情况、有关业务详细情况，并提供个人身份鉴别、数字证书签发、电子数据存证等合作方有关材料，以及佐证业务详细情况的图片、录音等材料。

本附录以示例的形式提供个人征信电子授权业务报告模板。

示例：

个人征信电子授权

业务报告

出具单位：XXX

日　　期：X 年 X 月 X 日

一、业务基本情况

说明业务名称、类型、办理渠道、覆盖范围等业务基本情况。

二、业务办理流程及征信业务相关情况

（一）总体业务流程。

说明获客、鉴别个人身份、签发数字证书、签署征信授权电子协议、查询个人信用报告、查询结果使用、存证征信授权电子数据等情况。

（二）征信业务有关环节。

1.鉴别个人身份。

说明鉴别个人身份的业务环节、鉴别措施、各类鉴别措施的合作方及其合法有效性、鉴别结果处理及存储、签发数字证书等具体情况。

2.签署征信授权电子协议。

说明签署征信授权电子协议的业务环节、供个人查看方式、防篡改措施、抗抵赖措施、加盖时间戳、网络传输可信性等具体情况。

3.存证征信授权电子数据。

说明存证征信授权电子数据的合作机构、系统对接情况、采用的存证技术、存证覆盖范围、存证内容等具体情况。

三、有关业务详细情况

按照时间顺序和业务流程，详细说明各业务环节的个人操作、办理结果等情况。

附件：个人身份鉴别、数字证书签发、电子数据存证等合作方有关材料，佐证业务详细情况的图片、录音等材料

附 录 B
（资料性）
个人征信电子授权电子签章验证报告

业务发生机构对电子签章提出验证申请，由电子认证机构说明验证结论，并出具验证报告。本附录以示例的形式提供个人征信电子授权电子签章验证报告模板。

示例：

个人征信电子授权

电子签章验证报告

出具单位：XXX

日　　期：X 年 X 月 X 日

一、出具机构说明

说明出具机构是由国务院信息产业主管部门许可的电子认证机构，具备有关业务许可资质。

二、验证申请说明

（一）申请单位名称。

说明申请验证机构名称。

（二）申请日期。

说明提出申请验证的时间。

（三）申请验证材料说明。

说明提交的待验证材料名称、文件格式等有关内容。

三、验证结论

（一）身份鉴别信息。

鉴别类型：电子认证机构自行身份鉴别或授权金融机构身份鉴别。

鉴别方式及实施：说明身份鉴别的具体方式及实施情况。

鉴别措施：说明采用的身份鉴别措施（例如身份证鉴别、生物特征鉴别、银行卡鉴别）。

（二）证书持有人注册身份信息。

证书持有人详细身份信息（例如持有人姓名、身份证号）。

（三）数字证书信息。

说明证书中的主题信息（对应用户名称，例如通用名称信息）。

证书序列号。

证书有效期。

证书签发机构名称。

（四）电子签章信息。

经验证的电子签章时间，电子签章是否有效，时间戳验证情况。

对经电子签章的有关材料在签章后是否发生过改变（篡改）的验证结果，例如“交验资料自电子签章时间起至今未发生任何改动”。

附件：1.电子认证服务许可资质证明材料

2.待验证电子签章有关文件（包括有关征信授权电子原件或打印件）

3.验证过程说明（说明验证计算及得出待验证资料没有经过篡改的过程信息）

4.其他有关材料（可选）

附 录 C
（资料性）
个人征信电子授权电子数据验证报告

业务发生机构对电子数据提出验证申请，由电子数据存证服务提供者说明验证结论，并出具验证报告。

本附录以示例的形式提供个人征信电子授权电子数据验证报告模板。

示例：

个人征信电子授权

电子数据验证报告

出具单位：XXX

日　　期：X 年 X 月 X 日

一、出具单位说明

说明存证机构信息、采用的存证技术，按照制度文件及行业标准开展存证的工作情况，如何防篡改，如何保证存证数据的完整性。

二、验证申请说明

（一）申请单位名称。

说明申请验证机构名称。

（二）申请日期。

说明提出申请验证的时间。

（三）申请验证内容。

说明申请验证的业务名称及具体内容。

三、验证结论

（一）身份鉴别数据。

说明身份鉴别环节，数据提交方存证的信息（包括身份鉴别手段、时间、结果及鉴别服务提供商等信息）、存证服务机构对待验证数据进行比对的一致性说明。

（二）签署行为记录数据。

说明签署环节，数据提交方存证的信息（包括用户签署征信授权电子协议的行为、方式、时间等信息）、存证服务机构对待验证数据进行比对的一致性说明。

（三）签署后电子文件数据。

说明签署后的电子文件数据，数据提交方存证的信息（签署后的合同文件）、存证服务机构对待验证数据进行比对的一致性说明。

（四）其他数据。

说明其他环节，数据提交方签署过程中涉及的其他相关环节数据（例如用户登录、浏览等环节）、存证服务机构对待验证数据进行比对的一致性说明。

附件：1.电子数据存证有关资质证明材料

2.签署方身份验证记录

3.签署行为记录数据

4.征信授权书

5.其他有关材料（可选）

参 考 文 献

[1] GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式

[2] GB/T 36298—2018 电子合同订立流程规范

[3] GM/Z 0001—2013 密码术语

[4] 《常见类型移动互联网应用程序必要个人信息范围规定》（国信办秘字〔2021〕14号文印发）.2021-03-12

[5] 《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》（中国人民银行 中国银行保险监督管理委员会 中国证券监督管理委员会令〔2022〕第1号发布）.2022-01-26