

中华人民共和国国家标准

GB/T 42930—2023

互联网金融 个人身份识别技术要求

Internet finance—Technical requirements for personal identification

2023-08-06 发布

2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 3

5 个人身份识别技术框架 3

 5.1 框架与各组成部分的作用 3

 5.2 个人身份识别实现的主要功能 4

6 个人身份识别凭据技术要求 4

 6.1 概述 4

 6.2 记忆凭据类 5

 6.3 OTP 令牌 6

 6.4 数字证书 7

 6.5 生物特征识别 8

 6.6 手机号认证 9

7 个人身份识别技术要求 9

 7.1 一般要求 9

 7.2 结合金融风险防控的个人身份识别 10

 7.3 个人身份识别因子 10

 7.4 持续个人身份鉴别 11

8 个人身份识别安全要求 11

附录 A（资料性） 典型场景个人身份识别技术应用建议 14

附录 B（资料性） 典型业务流程 16

 B.1 典型的通用流程 16

 B.2 个人身份核验 16

 B.3 凭据生成 17

 B.4 个人身份鉴别 18

参考文献 20

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：中国互联网金融协会、支付宝(中国)网络技术有限公司、中国建设银行股份有限公司、中国银联股份有限公司、北京旷视科技有限公司、北京同盾科技有限公司、中国农业银行股份有限公司、上海淇毓信息科技有限公司、证通股份有限公司、京东科技控股股份有限公司、人保金融服务有限公司、西安银行股份有限公司、拉卡拉支付股份有限公司、海通证券股份有限公司、安信证券股份有限公司、中互金数据科技有限公司。

本文件主要起草人：陆书春、朱勇、王新华、金磐石、刘燕青、彭晋、林冠辰、李武璐、王琪、梅敬青、郭振华、赵峰、马丹、国枫、刘涛、陈沛瑶、吴冉青、周超、许蓉、秘建宁、王健、高艳平、高飞荣、郭跃、段苏隆、李健。

引 言

随着互联网金融服务的快速发展,金融服务中对个人身份识别的需求也快速增长。在互联网环境下满足相关管理机构对于金融行业的严格实名认证要求,是互联网金融从业各方亟须解决的问题之一。

实施本文件,有助于在互联网金融服务中实现个人信息保护、信息安全、数据安全和交易便捷之间的良好平衡,助力有关机构实现个人身份识别可信度互认,促进以互联网为渠道的金融业服务的有效发展,推动互联网金融有序发展。

互联网金融 个人身份识别技术要求

1 范围

本文件规定了应用于互联网金融服务的个人身份识别技术要求,包括技术框架、凭据技术要求、身份识别技术要求以及安全要求。

本文件适用于互联网金融服务中与个人身份识别相关的服务与活动。

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 27912—2011 金融服务 生物特征识别 安全框架
- GB/T 35273—2020 信息安全技术 个人信息安全规范
- GB/T 37036.1—2018 信息技术 移动设备生物特征识别 第1部分:通用要求
- GB/T 40660 信息安全技术 生物特征识别信息保护基本要求
- GM/T 0028—2014 密码模块安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

互联网金融 internet finance

利用互联网技术和信息通信技术实现资金融通、支付、投资和信息中介服务的新型金融业务模式。

3.2

凭据 credential

凭证

用来鉴别个人身份的数据。

注1:本文件中,凭据在个人身份核验(3.4)阶段生成。

注2:在互联网金融领域,典型凭据如数字证书、静态口令、动态口令、生物特征识别信息等。

[来源:ISO 12812-1:2017,3.10,有修改]

3.3

个人身份识别 personal identification

在指定级别的可信度下确定个人声称的身份的过程。

注:个人身份识别通常包括个人身份核验(3.4)和个人身份鉴别(3.5)两个过程。

3.4

个人身份核验 personal identity proofing

个人初始身份鉴别

收集个人提交的身份信息,并验证与该个人真实身份是否相符的过程。

注:本文件的个人身份核验主要对应个人开通账户过程的身份识别,身份核验后生成相关凭据。

3.5

个人身份鉴别 personal identity authentication

根据凭据(3.2)确认个人身份的过程。

示例:通过校验一个口令确认个人身份或基于生物特征识别确认个人身份等。

注:本文件的身份鉴别对应个人开通账户之后,开展互联网金融业务过程中基于凭据的个人身份识别。

[来源:GB/T 5271.8—2001,08.04.12,有修改]

3.6

预设问题回答 preset question and answer

由个人预先设置问题及答案,或由认证服务方根据个人信息、历史行为等要素产生问题而由个人设置答案;在个人身份鉴别时,向个人展示问题,个人提交答案后由认证服务方验证答案是否匹配的个人身份鉴别(3.5)方式。

3.7

静态口令 static password

由个人设置,除非个人主动修改,否则不会发生变化的特定字符串。

注:静态口令通常由个人预先设定并存储在认证系统中。

3.8

动态口令 one-time password

基于时间、事件等因素动态生成的一次性口令。

示例:动态数字口令、动态二维码。

3.9

动态口令令牌 one-time password token

用来生成动态口令的软硬件。

注:动态口令令牌可能是一个专门的硬件设备,也可能是在某个通用设备(例如手机)上的一个模块或程序。

3.10

无硬介质证书 certificate without hardware carrier

存放在非专门硬件介质的数字证书。

注:一般说来,无硬介质证书不具备对存储区域的访问控制物理隔离能力。

3.11

有硬介质证书 certificate stored in hardware carrier

存储在硬件介质中的数字证书。

注:一般有硬介质证书具备对存储区域的访问控制物理隔离能力。硬件介质体不同,访问控制的方式和程度不同。

3.12

生物特征识别 biometrics

基于个体的生物学特性和行为特性对该个体的自动识别。

注:个体限指自然人。

[来源:GB/T 5271.37—2021,3.1.3,有修改]

3.13

可信环境 trusted environment

设备上的安全区域,可保证加载到其内部数据的安全性,包括保密性、完整性和可用性等,如可信执行环境(TEE)、安全元件(SE)、可信密码模块(TCM)或其他具备安全边界的保护区域。

[来源:GB/T 36651—2018,3.1,有修改]

3.14

生物特征样本 **biometric sample**

经过采集和处理得到的初始(原始)生物特征数据。

[来源:GB/T 27912—2011,4.10]

3.15

生物特征识别信息 **biometric information**

对自然人的物理、生物或行为特征进行技术处理得到的、能够单独或者与其他信息结合识别该自然人身份的个人信息。

注 1: 生物特征识别信息包括个人面部识别特征、虹膜、指纹、基因、声纹、步态、掌纹、耳廓、眼纹等。

注 2: 生物特征识别信息包括生物特征识别原始信息以及生物特征识别比对信息。

[来源:GB/T 40660—2021,3.3]

4 缩略语

下列缩略语适用于本文件。

DNS:域名系统(Domain Name System)

GSM:全球移动通信系统(Global System for Mobile Communications)

HTTP:超文本传输协议(Hypertext Transfer Protocol)

LEI:全球法人识别编码(Legal Entity Identifier)

OTP:动态口令(One Time Password)

PIN:个人识别码(Personal Identification Number)

SIM:用户身份模块(Subscriber Identity Module)

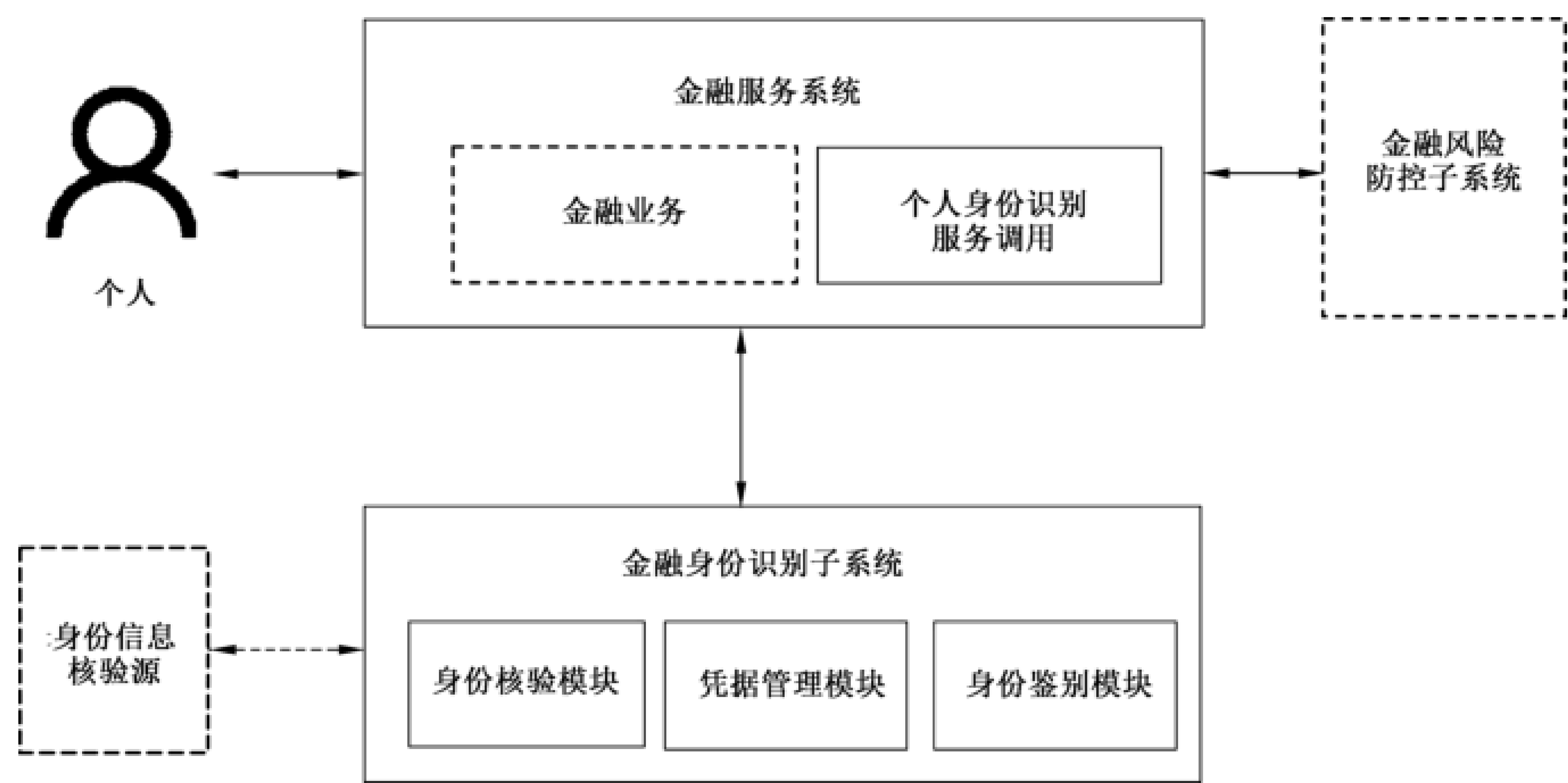
TLS:传输层安全协议(Transport Layer Security)

VPN:虚拟专用网(Virtual Private Network)

5 个人身份识别技术框架

5.1 框架与各组成部分的作用

互联网金融服务个人身份识别技术框架见图 1。互联网金融服务典型场景个人身份识别技术应用建议见附录 A。



注：本图为逻辑框架图，具体实现时可组合统一实现或者委托专业机构实现其中的部分功能，虚框表示相关模块的要求不属于本文件的范畴。

图 1 互联网金融服务个人身份识别技术框架

互联网金融服务个人身份识别技术框架中各组成部分的主要作用如下：

- a) 个人是发起互联网金融服务的主体，同时也是个人身份识别的对象；
- b) 金融服务系统为个人提供金融业务，并调用金融身份识别子系统的服务；
- c) 金融身份识别子系统向金融服务系统提供个人身份识别结果，包括身份核验模块、凭据管理模块、身份鉴别模块等；
- d) 金融风险防控子系统可在个人身份核验及个人身份鉴别过程中提供相关金融风险防控服务。

5.2 个人身份识别实现的主要功能

互联网金融服务领域中个人身份识别应实现的功能如下：

- a) 身份核验，即金融服务系统应收集并验证个人的身份信息资料，确认个人身份，必要时可借助于身份信息核验源实现；
- b) 凭据管理，即完成个人身份核验后，金融身份识别子系统应根据个人选择的认证方式生成凭据，凭据可由个人或金融身份识别子系统进行安全存储；
- c) 身份鉴别，即金融身份识别子系统根据个人凭据来确认个人身份，完成个人的身份鉴别，应结合金融风险防控实现。

互联网金融个人身份识别典型业务流程见附录 B。

6 个人身份识别凭据技术要求

6.1 概述

按照凭据不同，应用于互联网金融服务中的个人身份识别凭据技术类别如下：

- a) 记忆凭据类，包括静态口令、预设问题回答；
- b) OTP 令牌；
- c) 数字证书，包括无硬介质证书和有硬介质证书；
- d) 生物特征识别技术；

- e) 手机号认证。

6.2 记忆凭据类

6.2.1 静态口令

6.2.1.1 生成要求

静态口令的生成包括但不限于下列方面：

- a) 长度应不少于 6 个字符，宜 8 个字符以上；
- b) 对于非设备绑定个人标识的，静态口令除数字外还应至少包括大小写字母或特殊字符；
- c) 对于手势密码等其他静态口令，应满足一定复杂度要求（例如最少连接点数要求）；
- d) 认证系统应对个人输入口令的强度进行分析，给出口令强度的反馈；对于低强度的口令能警示个人更换为符合最低强度要求的口令；
- e) 如个人标识已经同设备绑定，或结合其他凭据，或受输入设备限制，可采用 6 个字符的纯数字口令。

6.2.1.2 使用要求

静态口令的使用要求如下：

- a) 通过受理终端或支付客户端应用程序输入静态口令时，应采取隐藏静态口令反馈信息等措施保护静态口令，且 POS 机等受理终端应具备口令输入防窥视功能；
- b) 应具备静态口令验证失败处理功能，可采取结束会话、限制错误密码输入次数、增强后续验证手段以及当网络登录连接超时自动退出等措施；

示例：增加图形验证码、滑块或点击人机交互验证都是增强后续验证手段。

- c) 应支持静态口令重置，在重置前应进行有效的个人身份识别；重置后的静态口令应符合 6.2.1.1 的要求；
- d) 静态口令应端到端加密传输和安全存储；
- e) 对于提供与个人信息相关的初始简单口令的，在互联网金融应用场景首次登录时应进行修改，且修改后的口令应符合 6.2.1.1 的要求。

6.2.1.3 设备要求及安全要求

静态口令设备及安全包括但不限于下列方面：

- a) 输入设备应具备适宜的物理、逻辑安全机制；

示例：安全机制如具备入侵检测机制、具备可信环境、具备完整的密钥体系等。

- b) 在口令输入设备和读卡机具间传输 PIN 时，应采取有效的措施保护所传输的数据；
- c) 输入控件应具备安全机制，如使用基于加密芯片实现的分体式安全键盘、基于软件实现的安全随机键盘等输入控件防止采用键盘监听等手段获取口令；
- d) 在输入控件和终端程序间传输静态口令时，应防止未经授权查看和变更传输的数据；
- e) 宜定期修改静态口令，口令修改后不应与当前口令一致；
- f) 宜采用设备风险检测技术对输入设备的环境安全状态变化进行有效感知。

6.2.2 预设问题回答

6.2.2.1 生成要求

预设问题与对应的答案作为凭据，其生成包括但不限于下列方面：

- a) 预设问题与答案均应明确最低复杂度,以防范猜测攻击;
- b) 预设问题不宜与个人身份信息、个人隐私信息相关;
- c) 预设问题宜能防范被猜测破解;
- d) 预设问题可设置一定的提示信息,辅助用户记忆。

6.2.2.2 使用要求

预设问题回答的使用包括但不限于下列方面:

- a) 应能在通过个人身份识别后重置预设问题或答案;
- b) 问答应设置在既定概率下能防范猜测攻击的错误尝试次数;
- c) 连续两次预设问题与答案不应使用完全相同的问题或问题组合;
- d) 预设问题回答会话应设置超时时间,超时后应重新开始预设问题回答过程,并且计为一次尝试失败;
- e) 从终端向服务器传输预设问题与答案的相关数据,应进行加密传输;
- f) 可在一次身份鉴别应用中使用多个预设问题回答。

6.3 OTP 令牌

6.3.1 生成要求

OTP 令牌作为凭据,其生成包括但不限于下列方面:

- a) 应使用安全可信的 OTP 生成模块,如安全可信的终端生成模块或服务器端生成模块等;
- b) OTP 应随机生成;
- c) OTP 应设置有效时长,一般不宜超过 5 min。

6.3.2 使用要求

OTP 令牌的使用包括但不限于下列方面:

- a) 应采取有效措施防范 OTP 被中间人攻击;

示例 1: 基于密码学的安全传输等为常见措施。

- b) 每次业务处理中的 OTP 应各不相同,且使用后立即失效;
- c) 应具有激活尝试次数限制功能,当激活操作连续错误一定次数之后,在既定概率下能防范穷举攻击的时间段内锁定后才可重新执行激活操作;
- d) 应设定一定的认证有效期;

示例 2: 30 s 至 60 s 均是常见的认证有效期。

- e) 应限制验证出错次数,超过则采取账户锁定等安全措施;
- f) 重新获取 OTP 后,原 OTP 应失效;
- g) 凭据宜与同一机构的个人身份标识一对一绑定。

6.3.3 安全要求

OTP 令牌安全要求如下:

- a) 应采取有效措施保证种子密钥数据在整个生命周期的安全;

注: 种子密钥是 OTP 鉴别双方的共享密钥。

- b) 应防范通过物理攻击的手段获取设备内的敏感信息;

示例: 开盖、搭线、复制都是典型的物理攻击的手段。

- c) 应采取相关措施确保只有授权客户才可使用,如采取静态口令等措施;
- d) 加密芯片应具备抵抗旁路攻击的能力;
- e) 在外部环境(例如电磁环境等)发生变化时,OTP 令牌不应泄露敏感信息或影响安全功能;
- f) 应具备一定的防止意外(例如跌落等)造成种子密钥丢失的功能。

6.4 数字证书

6.4.1 无硬介质证书

6.4.1.1 生成要求

无硬介质证书生成包括但不限于下列方面:

- a) 用于签名的公私钥宜在终端的可信环境中生成和存储;如果由服务器端生成,应保障生成环境的可信以及下发通道不可被窥探;
- b) 应保证私钥的唯一性;
- c) 应使用安全措施防止私钥受到未授权的访问;
- d) 应通过安全机制防止无硬介质证书对应私钥被非法复制到其他设备上使用,例如证书绑定、可信环境存储等;
- e) 应设置无硬介质证书的有效期,保障该证书过期后不可用;
- f) 应定期检查无硬介质证书注销列表。

6.4.1.2 使用要求

无硬介质证书使用包括但不限于下列方面:

- a) 无硬介质证书的发放宜使用离线或 VPN 专线方式,确需通过公共网络发放的,应提供安全通道下载,且应加密传输;
- b) 无硬介质证书使用时应检查其合法性。

6.4.1.3 安全要求

无硬介质证书安全包括但不限于下列方面:

- a) 签名密钥由软件密码模块内部生成,签名密钥等密钥信息均不应明文存储在非易失性存储器上;
- b) 对于高安全需求业务,相应的密码模块宜至少符合 GM/T 0028—2014 规定的安全二级要求;
- c) 使用基于密码学的安全机制等控制软件密码模块的访问权限;
- d) 采用限制错误操作次数等安全机制对关键操作(例如签名等)进行保护,防范穷举攻击;
- e) 软件密码模块具备软件完整性检测与关键功能自测试功能;
- f) 个人可主动发起无硬介质证书注销,特殊情况下服务器侧也可发起无硬介质证书注销,无硬介质证书注销后不应再次使用。

6.4.2 有硬介质证书

6.4.2.1 生成要求

有硬介质证书生成要求如下:

- a) 应能支持一个或多个应用;
- b) 应能提供和保持不同应用之间的安全性;

- c) 应设置有效期。

6.4.2.2 使用要求

有硬介质证书使用包括但不限于下列方面：

- a) 应保证一个应用不会影响另一个应用的安全操作；
- b) 应保证一个独立应用的信息不能被其他应用访问和修改；
- c) 证书存储介质在连接到终端设备一段时间内无任何操作时宜自动关闭；应重新连接后才能继续使用；
- d) 证书存储介质应能够自动识别其是否与终端连接；宜具备在规定的时间与终端连接而未进行任何操作时提醒等功能。

示例：语言提示、屏幕显示均为可能的提醒功能。

6.4.2.3 设备要求及安全要求

有硬介质证书设备及安全包括但不限于下列方面：

- a) 应使用通过认可的第三方测评机构安全检测的证书存储介质；
- b) 对于高安全需求业务，相应的密码模块宜至少符合 GM/T 0028—2014 规定的安全二级要求；
- c) 应采取有效措施防范证书存储介质被远程恶意调用，如基于密码学等的授权机制等；
- d) 证书存储介质应具备支持密钥生成和数字签名运算能力的安全芯片，敏感操作应在安全芯片内进行；
- e) 证书存储介质的主文件应受到安全机制保护，个人无法进行删除和重建；
- f) 应保证私钥在生成、存储、使用、更新、销毁等全生命周期的安全，比如基于可信环境进行私钥全生命周期管理等；
- g) 参与密钥、PIN 码运算的随机数应在证书存储介质内生成，其随机性指标宜符合国际或者国内通用标准的要求；
- h) 密钥文件在启用期应封闭；
- i) 签名交易完成后，状态机应立即复位；
- j) 应保证 PIN 码的安全；
- k) 对证书存储介质固件进行的任何改动，都应实施以保证证书存储介质中不含隐藏的非法功能和后门指令为目的归档和审计；
- l) 证书存储介质应具备抵抗旁路攻击的能力；
- m) 在外部环境发生变化时，证书存储介质不应泄露敏感信息，影响安全功能；
- n) 应采取有效措施防止数据被篡改；
- o) 未经个人确认，证书存储介质不应输出数据；经过设定时间段后依旧未接到个人确认的情况下，证书存储介质可自动清除数据并复位状态。

6.5 生物特征识别

6.5.1 概述

用于个人身份识别的生物特征识别模态一般包括：

- a) 人脸识别；
- b) 指纹识别；
- c) 声纹识别；

- d) 虹膜识别；
- e) 静脉识别；
- f) 多模态识别；
- g) 根据技术发展新出现的其他模态识别。

6.5.2 技术要求

基于生物特征识别技术的个人身份识别,生物特征识别技术应符合 GB/T 27912—2011 的规定。此外,还包括下列方面。

- a) 应充分评估所使用的生物特征识别技术的特点及存在的风险,按照 GB/T 37036.1—2018 的要求合理地选择远程模式或本地模式。
- b) 处理高安全需求业务时(例如网络支付等)应采取适当的措施防范呈现攻击并具备相应的处理机制,防止恶意伪造攻击,检测和处理的呈现攻击手段要求如下:
 - 1) 形状包括但不限于二维(2D)、三维(3D);
 - 2) 载体包括但不限于图像、视频、头模、指纹膜、合成或翻录语音;
 - 3) 材质包括但不限于纸质、电子显示屏、硅胶。
- c) 处理高安全需求业务时(例如网络支付等),对于不具备某种生物特征识别呈现攻击检测的应用场景[例如下一代超文本标记语言(H5)、网页页面应用等],生物特征识别不应作为唯一身份识别手段,应增加其他的随机交互验证手段,比如验证码等;当个人未同意授权生物特征识别时,应提供其他方式完成个人身份识别。
- d) 对于生物特征识别信息的保护要求应符合 GB/T 40660 的规定,并确保生物特征样本采集、质量判断、呈现攻击检测、生物特征项提取和传输等过程中,个人生物特征数据的保密性和完整性。
- e) 应对生物特征识别验证次数进行限制,达到设置的验证限制次数后,可采取一定时间之后才能再次进行生物特征识别验证、额外增加验证因素等措施。
- f) 应确保生物特征识别的错误接受率、错误拒绝率、防呈现攻击失败率等指标在可接受的范围内。
- g) 宜结合可信环境实现生物特征识别。

6.6 手机号认证

手机号认证是由移动运营商提供,采用“通信网关取号”及 SIM 卡识别等技术实现的一种移动互联网身份识别方法,包括但不限于下列方面:

- a) 应对个人实名手机号进行相关注册或登记;
- b) 验证时应有通信数据网络信号覆盖;
- c) 一键授权应用场景下,应具备授权页面,应用(APP)开发者经个人授权后可获得号码,适用于注册、登录等场景;
- d) “本机号码校验”应用场景下,本机号码校验不返回完整号码,仅返回验证是否一致的结果;
- e) 宜具备相关机制保障手机号认证的手机终端为手机号实名人所有并使用。

7 个人身份识别技术要求

7.1 一般要求

在金融服务系统中进行个人身份识别时,应根据金融行业管理要求及实际业务需求,提供特定的身

身份证件,或提供通过有效法定身份证件办理的有效身份证明材料,或提供个人生物特征识别信息。

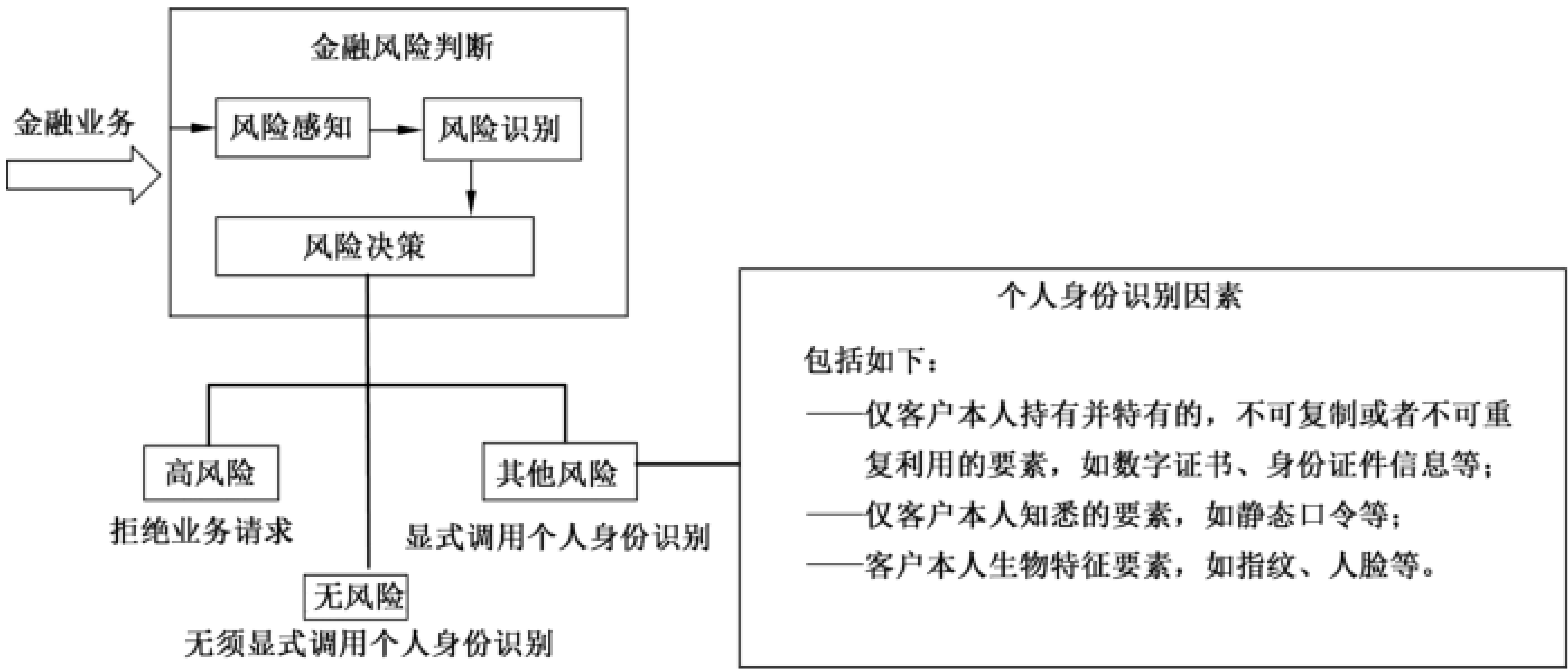
根据个人信息分级分类管理的要求,对个人身份识别涉及的个人信息及个人金融信息的收集、传输、存储、使用、委托处理、共享、转让、公开披露应符合 GB/T 35273—2020 的规定。

个人身份识别材料真实性、有效性和可追溯性的保障,包括但不限于下列方面:

- a) 身份核验时个人应提供法定身份证件,金融服务系统应采取有效措施核验个人提供的实名身份证件信息,可采取与第三方权威核验源比对的方式确保信息的真实性和有效性;
- b) 宜对身份核验过程中个人本人提交的法定身份证件的图像质量进行判断,确保个人本人提交的身份证件关键信息清晰可辨,如姓名及证件号码等;
- c) 属于个人通过法定身份证件办理的身份材料(如银行卡信息等),应在有效期内,且状态正常;
- d) 个人法定身份证件或通过法定身份证件办理的身份材料,如其可信程度难以满足金融行业中个人身份识别要求,应使用额外的个人身份识别材料来进行身份识别(如生物特征识别信息等);
- e) 若采用生物特征识别信息进行个人身份识别,应确保生物特征采集自个人本人并且获得本人单独同意,且保障留存的生物特征样本的质量;
- f) 对于弱势群体,宜采取相关措施保障无障碍身份识别。

7.2 结合金融风险防控的个人身份识别

互联网金融个人身份识别一般结合金融风险防控实现。金融风险防控子系统对服务请求进行风险防控处理并进行风险防控决策,可采取直接拒绝服务请求、无需显式调用个人身份识别或显式调用不同强度的个人身份识别因子进行身份识别。结合金融风险防控的个人身份识别示意图见图 2。



注：个人身份识别因素即不同类别的身份识别手段,本文件按照仅客户持有并且特有、仅客户本人知悉以及客户本人生物特征三个类别进行划分。

图 2 结合金融风险防控的个人身份识别示意图

7.3 个人身份识别因子

7.3.1 概述

个人发起互联网金融业务请求时,金融服务系统需根据个人当前登录认证方式、业务场景等要求,采用单因子、双因子或多因子的方式进行个人身份识别。

7.3.2 单因子个人身份识别

单因子个人身份识别根据本文件中个人身份识别凭据技术中的某个因子进行身份识别,例如记忆凭据或者生物特征识别信息等。

7.3.3 双因子个人身份识别

双因子个人身份识别根据本文件中个人身份识别凭据技术中的两个不同因子组合进行身份识别。双因子个人身份识别凭据示例见表 1。

表 1 双因子个人身份识别凭据示例

个人身份识别凭据	说明
记忆凭据	静态口令或预设问题回答
生物特征识别信息	个人的指纹、虹膜、人脸、声纹等生物特征识别信息

7.3.4 多因子个人身份识别

多因子个人身份识别是在双因子个人身份识别基础上,增加额外的个人身份识别因子来进行个人身份识别,提升个人身份识别的真实性和有效性。

多因子个人身份识别凭据示例见表 2。

表 2 多因子个人身份识别凭据示例

个人身份识别凭据	说明
数字证书	软件证书或硬介质证书
记忆凭据	静态口令或预设问题回答
生物特征识别信息	个人的指纹、虹膜、人脸、声纹等生物特征识别信息

7.4 持续个人身份鉴别

对于复杂环境,不应仅依赖于网络范围进行个人身份鉴别,环境发生变化时应进行持续个人身份鉴别,具体要求如下:

- a) 应具备相关机制以保障应用、硬件(服务器)、个人身份等标识的安全可信,相关标识全生命周期内唯一且不可篡改;
- b) 应具备相关机制保障在环境[服务器、网际互连协议(IP)地址、设备等]发生变化时,启动个人身份鉴别。

注:网络范围指某个确定的网络域,如某个专用网络或者公网等。

8 个人身份识别安全要求

在个人身份识别过程中,应采取相关防范措施保障个人身份识别的安全,防止攻击者通过虚假身份注册或非法获取合法个人所持有的能够用以证明其身份的凭据,假冒成合法个人造成危害。个人身份

识别安全威胁以及防范措施示例见表 3。

表 3 个人身份识别安全威胁和防范措施示例

威胁	描述	攻击示例	防范措施示例
暴力破解/在线猜测/字典攻击	也称为“蛮力破解”或“穷举攻击”，是一种特殊的字典攻击。在暴力破解中所使用的字典是字符串的全集，对可能存在的所有组合进行猜测，直到得到正确的信息为止	攻击者通过尝试猜测或穷举的方式来试图获取到正确的口令	防范目标是让攻击者在没有更多先验知识的情况下，仅通过重复尝试猜测来攻击变得不可行。 具体防范措施可为：限制失败尝试次数、在每次尝试失败后都要求等待一段时间后才能继续尝试、要求验证对象通过公开的图灵测试机制来防范机器人猜测等
键盘监听	通过对个人的实体或虚拟键盘进行监听，获取个人的输入信息	按键记录软件以木马方式植入到个人设备后，能记录下个人的每次按键动作，从而窃取个人输入的口令，并按预定的计划把收集到的信息通过电子邮件等方式发送出去	具体防范措施可为：终端安装必要的杀毒软件并定期查杀；使用 APP 定制的加密动态键盘，打乱键位
钓鱼攻击（假冒网页）	注册个人被引诱与一个假冒的验证方进行交互，并被其欺骗，泄露了所持有的验证信息、敏感个人信息或者凭据密钥等，攻击者在获得这些数据后可假冒成注册个人与真正的验证方进行交互并通过其验证	某注册个人收到了一封邮件并被引导到了一个假冒的网站，在该假冒网站上登录时泄露了其个人信息	防范目标是让攻击者无法成功获取凭据密钥或者认证有效验证值，用以后续假冒注册个人进行攻击。 具体防范措施可为：使用个性化的设置来提示个人是否遇到了假冒服务器，比如个人自行设定的登录前提示语、登录后欢迎词等；使用基于密码学原理的安全鉴别机制等
网域欺骗	注册个人在尝试连接一个合法的验证方时，被攻击者通过修改 DNS 或路由表的方式引导到攻击者的网站	通过对 DNS 服务进行劫持，将用户希望访问的网站解析为假冒网站的 IP 地址，注册个人在登录一个合法网站时被引到了一个假冒网站，在该假冒网站上登录时泄露了其个人信息	
窃听攻击	攻击者通过监听认证协议报文来获取可用于后续假冒注册个人的信息	攻击者通过监听获取了在传输过程中的个人口令或者口令哈希值	防范目标是让攻击者即使录制了注册个人与身份识别服务之间的通信报文，也无法从中分析出能够让攻击者假冒成注册个人的有效信息。 具体防范措施可为：使用受保护的安全通信协议如 TLS 等
重放攻击	攻击者通过重复使用此前获取的报文信息来假冒注册个人到验证方进行验证	攻击者在此前的一个实际验证会话中获取了注册个人的口令或者口令哈希值，并在后续使用该信息再到验证方进行验证	防范目标是防止攻击者通过记录并重放此前的成功验证协议报文，来通过后续的个人身份识别过程。 具体防范措施可为：在通信协议中增加使用随机数或者挑战值

表 3 个人身份识别安全威胁和防范措施示例（续）

威胁	描述	攻击示例	防范措施示例
会话劫持	攻击者将其自身嵌入到注册个人与验证方的通信会话中,面对注册个人能伪装成验证方,反之面对验证方可假冒成注册个人	攻击者通过窃听或者预测等手段获取用于标识 HTTP 请求的验证值,并非法使用该验证值假冒成注册个人,达到攻击目的	防范目标是将认证与数据传输绑定起来,防止攻击者参与了数据传输会话而没有被检测到。 具体防范措施可为:为每次验证会话生成单独的会话密钥用于会话数据传输
中间人攻击	攻击者将其自身放置在注册个人与验证方之间,能够获取并修改通信报文中的内容。一般而言,攻击者会同时面向注册个人伪装成验证方和面向验证方假冒成注册个人	攻击者通过侵入路由表转发注册个人与验证方之间的报文。转发报文时,攻击者使用自己的公钥代替验证方的公钥,注册个人被其欺骗后,攻击者就可解密获得注册个人的信息	弱级别中间人攻击的防范目标是提供措施供注册个人判断其是否在与真实的验证方之间进行通信,但仍存在一定的机会,让攻击者获得注册个人的验证值,用于假冒注册个人并能通过验证方的验证; 强级别中间人攻击的防范目标是能够完全避免注册个人向攻击者泄露任何能供攻击者用于假冒注册个人的信息,防止让攻击者能够利用该信息假冒注册个人通过验证方验证。 具体防范措施可为:使用安全的通信协议如 TLS;使用高强度的凭据等
伪基站技术	攻击者使用伪基站方法,利用 GSM 网络(即 2G 网络)的既有漏洞,采用“GSM 劫持+短信嗅探”技术,可实时监听基站发送给个人手机的短信内容	攻击者采用“GSM 劫持+短信嗅探”技术,实时监听基站发送给个人手机的短信内容,进而利用各银行机构网站、互联网金融应用等存在的技术漏洞和缺陷,实现信息窃取、资金盗刷和网络诈骗等犯罪行为	具体防范措施可为:特殊时段比如夜间减少短信验证码的使用;增加其他个人身份识别因子等
虚拟摄像头攻击	通过劫持终端操作系统的摄像头底层接口,绕过真实摄像头,传入攻击视频文件作为摄像头录入内容以达到攻击目的	攻击者采用多种方式对抗呈现攻击检测,比如提前准备人像点头、摇头等动作视频,使用工具操作人像动作,通过虚拟摄像头代替系统摄像头传入影像,达到绕过呈现攻击检测的目的	具体防范措施可为:严控在模拟器环境下打开应用;针对特定设备型号、操作系统版本加强风险管控等
旁路/侧信道攻击	通过程序执行时间、功耗、电磁辐射等物理信息,结合统计理论快速破解口令,获取敏感信息	通过侧信道分析,破解出芯片中的根密钥,从而解密数据或者复制设备身份标识,假冒设备身份	具体防范措施可为:硬件层面使用安全芯片或者 TEE 存储密钥等敏感信息,软件层面使用随机加扰等方法对抗侧信道攻击

附录 A
(资料性)
典型场景个人身份识别技术应用建议

互联网金融服务典型场景个人身份识别技术的应用建议见表 A.1。

表 A.1 典型场景个人身份识别技术应用建议

应用场景	个人身份识别技术应用建议
消费金融申请	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等，并且检验人证合一有效性
互联网金融业务签约（包括电子银行签约、快捷支付签约、理财基金签约、代收代付签约、保函审批等）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等，并且检验人证合一有效性
远程银行卡业务（包括银行卡开户、银行卡解挂、补换卡、口令重置等）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等，并且检验人证合一有效性
在线信用卡申领	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等； 申请时检验人证合一有效性；领取时可直接进行个人身份识别
网上银行/APP 登录	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等
金融账户远程开户（不含 I 类银行账户）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等，检验人证合一有效性
账户解锁	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等
柜台办理互联网金融业务	建议可选的凭据技术：记忆凭据类，OTP 令牌，OTP 设备，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等，检验人证合一有效性
网络支付	建议可选的凭据技术：记忆凭据类，OTP 令牌，OTP 设备，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等
在线投保	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等，并且检验人证合一有效性
在线理赔	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等
保单服务（包括保单贷款、红利账户领取、生存金领取、保单贷款清偿、万能账户追加等）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等

表 A.1 典型场景个人身份识别技术应用建议（续）

应用场景	个人身份识别技术应用建议
变更服务（续期交费信息变更、客户联系信息变更、红利派发方式变更、生存给付续领账户变更等）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等
股票买卖、理财产品买卖、股票 APP 登录	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等
非金融产品售后服务（产品包含但不限于：投顾投研产品、资讯类产品、行情工具策略相关类产品、积分产品、视频音频直播类产品等）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、声纹等），手机号认证等
远程证券业务开户	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、活体、声纹等），手机号认证等，并且检验人证合一有效性
证券业务办理（密码重置、手机号码修改、销户等）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、活体、声纹等），手机号认证，并且校验人证合一有效性
证券业务办理（账户涉税调查、委托方式新增、密码修改等）	建议可选的凭据技术：记忆凭据类，OTP 令牌，数字证书，生物特征识别（指纹、人脸、活体、声纹等），手机号认证等

附录 B
(资料性)
典型业务流程

B.1 典型的通用流程

互联网金融个人身份识别典型的通用流程见图 B.1。

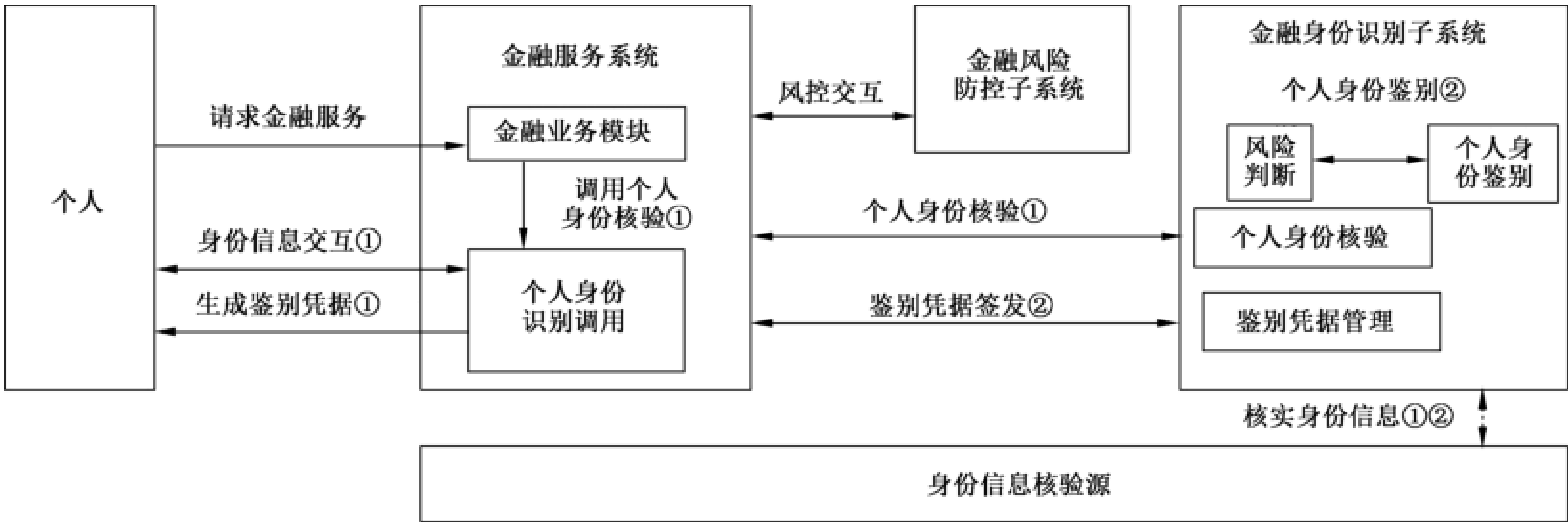


图 B.1 个人身份识别通用流程

个人身份识别包括个人身份核验(图 B.1 中的①进行标注)以及个人身份鉴别(图 B.1 中的②进行标注)两个典型通用流程。典型的个人身份识别通用流程示例如下所述。

- a) 个人身份核验流程：
- 1) 个人发起开通金融业务请求，金融服务系统判断该个人未注册，调用并启动个人身份核验流程；
 - 2) 金融服务系统根据业务规则确定所需核验的个人身份信息，采集个人身份信息，调用金融风险防控处理服务，并通过身份信息核验源核实身份信息；
 - 3) 个人身份核验成功后，生成凭据；
 - 4) 完成个人身份核验并进行注册。
- b) 个人身份鉴别流程：
- 1) 个人发起金融业务请求；
 - 2) 金融服务系统判断为已注册个人，根据业务规则启动相应的个人身份鉴别流程；
 - 3) 金融服务系统调用金融风险防控子系统对请求进行风险判断并处理；
 - 4) 根据风险防控处理结果选择不同的个人身份鉴别模式或其组合，进行个人身份鉴别，必要时通过权威身份信息核验源核实个人身份信息；
 - 5) 完成个人身份鉴别。

B.2 个人身份核验

个人身份核验基于真实身份信息对个人进行确认，个人身份信息可包括个人的法定身份证件、个人自身所拥有的生物特征识别信息或者是个人通过法定身份证件办理的身份材料。

个人身份核验由个人的互联网金融服务请求触发，以创建了个人对应的身份识别标识为结束标志。注册阶段典型的个人身份核验流程见图 B.2。

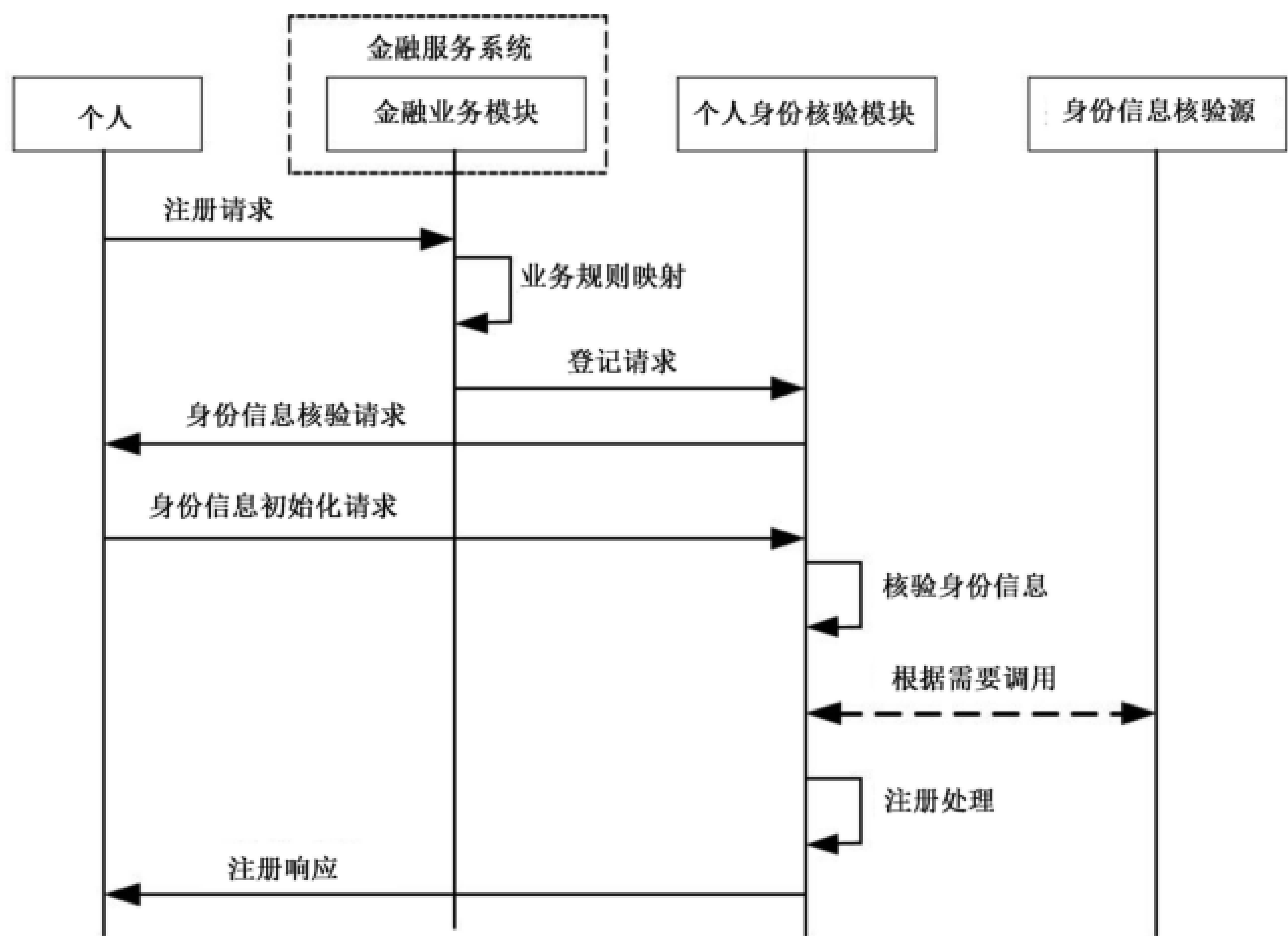


图 B.2 典型的个人身份核验流程

注册中个人身份信息核验过程包括但不限于如下步骤：

- a) 个人发起金融业务注册请求；
- b) 金融服务系统根据服务规则,判断需要核验的身份信息；
- c) 个人根据需要核验的身份信息,发起身份信息初始化请求；
- d) 个人身份核验模块完成身份信息的核验,必要时调用第三方权威核验源；
- e) 通过身份信息核验后,个人发起注册请求；
- f) 个人身份核验模块提供必要的注册处理,包括但不限于:创建个人身份标识等；
- g) 反馈注册响应；
- h) 结束个人身份核验过程。

B.3 凭据生成

金融服务系统通过个人提供的身份核验材料对个人身份确认后,金融身份识别子系统生成凭据,并在后台将与该凭据关联的凭据信息和个人身份进行绑定。凭据的生成过程中,根据具体所使用的凭据类型,可新建凭据并提供给个人使用,也可将个人已经拥有的凭据与此次注册过程关联起来。凭据的种类和要求见第 6 章。

凭据的生成在个人身份核验成功后进行,典型的以个人获取并存储凭据为结束标志。典型的凭据的生成流程见图 B.3。

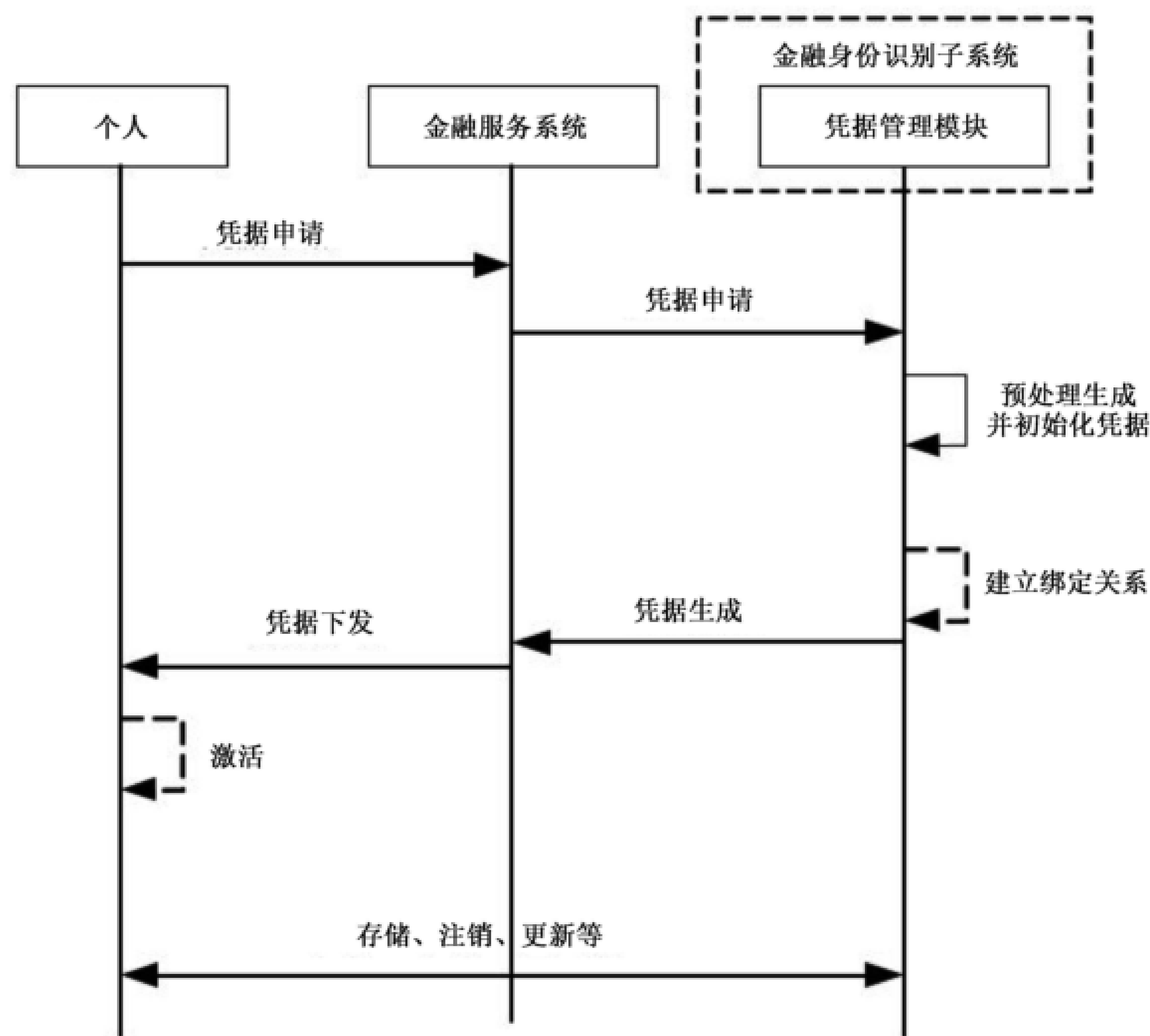


图 B.3 典型的凭据的生成流程

典型的凭据的生成过程如下：

- a) 个人发起凭据申请；
- b) 凭据管理模块生成凭据；
- c) 将凭据与个人绑定；
- d) 必要时,将凭据下发给个人；
- e) 根据凭据的不同,必要时由个人激活凭据；
- f) 个人或系统安全地存储凭据,必要时进行凭据的注销或更新等操作；
- g) 结束流程。

B.4 个人身份鉴别

个人身份鉴别过程中,个人按照约定的鉴别协议,通过向金融服务系统证明其拥有并控制有效注册凭据来证明其身份。个人身份鉴别由个人发起的互联网金融服务请求触发,以反馈个人身份鉴别结果为结束标志。

典型的个人身份鉴别流程见图 B.4。

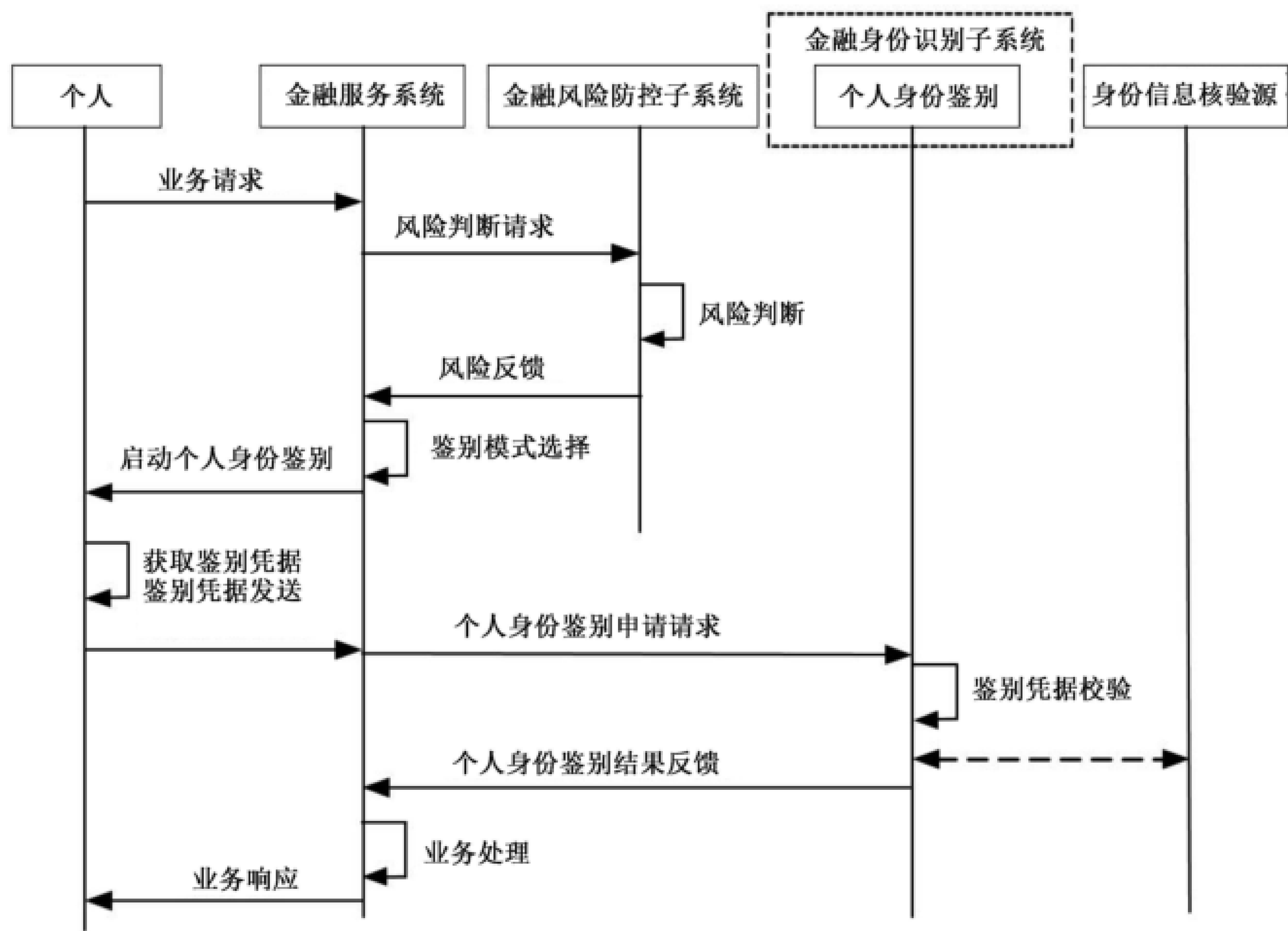


图 B.4 个人身份鉴别流程

典型的个人身份鉴别过程如下：

- a) 个人发起金融业务请求；
- b) 金融风险防控子系统对业务请求进行风险判断；
- c) 金融服务系统选择个人身份鉴别的模式，启动个人身份鉴别，要求个人提供相应的凭据；
- d) 个人提供所要求的凭据；
- e) 个人身份鉴别完成凭据的校验；
- f) 金融服务系统根据个人身份鉴别结果进行业务处理；
- g) 金融服务系统向个人返回业务响应；
- h) 结束个人身份鉴别流程。

注：根据需要，个人可能需提供多个凭据并成功通过校验后进行业务处理。

参 考 文 献

[1] GB/T 5271.8—2001 信息技术 词汇 第 8 部分:安全

[2] GB/T 5271.37—2021 信息技术 词汇 第 37 部分:生物特征识别

[3] GB/T 36651—2018 信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架

[4] GB/T 37036.2—2019 信息技术 移动设备生物特征识别 第 2 部分:指纹

[5] GB/T 37036.3—2019 信息技术 移动设备生物特征识别 第 3 部分:人脸

[6] GB/T 37036.4—2021 信息技术 移动设备生物特征识别 第 4 部分:虹膜

[7] GB/T 38542—2020 信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架

[8] GB/T 38671—2020 信息安全技术 远程人脸识别系统技术要求

[9] JR/T 0068—2020 网上银行系统信息安全通用规范

[10] JR/T 0164—2018 移动金融基于声纹识别的安全应用技术规范

[11] JR/T 0171—2020 个人金融信息保护技术规范

[12] ISO 12812-1:2017 Core banking—Mobile financial services—Part 1: General framework

[13] ISO/IEC 7816-11:2022 Identification cards—Integrated circuit cards—Part 11: Personal verification through biometric methods

[14] ISO/IEC 19790:2012 Information technology—Security techniques—Security requirements for cryptographic modules

[15] 中国人民银行.非银行支付机构网络支付业务管理办法(中国人民银行公告〔2015〕第 43 号)

[16] 中国人民银行、工业和信息化部、公安部、财政部、国家工商总局、国务院法制办、中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会、国家互联网信息办公室.关于促进互联网金融健康发展的指导意见(银发〔2015〕221 号)

[17] 中国人民银行.人民币银行结算账户管理办法(中国人民银行令〔2003〕第 5 号)

[18] 中国人民银行.人民币银行结算账户管理办法实施细则(银发〔2005〕16 号)

[19] 中华人民共和国反洗钱法,2006 年 10 月 31 日

[20] 中国人民银行.移动金融客户端应用软件无障碍服务建设方案(银发〔2021〕69 号)

[21] 中国人民银行.征信业务管理办法(中国人民银行令〔2021〕第 4 号)

