身份验证方案

一、必要性与重要性：

①无接触式服务：数字经济时代，金融服务呈现出无接触式的特点，传统的线下办理手续业务向如今的线上开户和远程支付转变，移动支付大面积普及，数字金融应用场景不断丰富，身份验证应实现在保证安全性的情况下远程实时完成，建立一套高标准的金融身份验证系统成为了当下的大势所趋。

②维护账户安全与个人隐私：完善金融身份验证系统是防范金融犯罪的核心途径，传统密码易泄露易破解，而金融身份验证系统所采用的生物识别如指纹、人脸、虹膜等技术能够有效降低身份盗用风险，预防洗钱等金融犯罪行为。

③法律监管要求：各国的金融监管条例对金融身份验证做出了较高要求，各机构必须验证用户身份并保护好用户数据不被泄露，如香港虚拟银行的牌照明确指出申请者应证明其数字身份验证能力。

④提高品牌声誉与用户粘性：一套高标准的金融身份验证系统对机构方而言可以有效提高其品牌声誉与用户粘性，投资者在选择金融机构时往往看重其安全性与隐私性，能否有效保障其资金安全和个人数据，当机构得到用户信任时往往用户会长期选择。

⑤生成式 AI 威胁：AI 技术迅猛发展，生成式 AI 可以伪造声频与人脸，对金融身份验证系统提出了更高的要求，如何在未来在利用 AI 的同时对抗 AI 带来的风险挑战成为金融身份验证系统的一个核心议题。

・身份验证方案发展的**核心目标**：提高安全性、减少用户摩擦和增强隐私保护

二、目前市面已有的主流身份验证方案：

1、单因素身份验证（SFA）——最基本的身份验证方式

最常见的依赖**用户名与密码组合（静态密码）**。

发展历程：

早期阶段（1990 年代）：金融机构最早采用静态密码（或 PIN）作为基础验证手段，因技术门槛低、用户熟悉度高，成为网上银行的标配。

问题暴露（2000 年代后）：随着网络攻击频发（如钓鱼、撞库），静态密码的脆弱性凸显，逐步被更安全的方案补充或替代。

利弊：

优点：简单易用，用户无需额外知识

缺点：最不安全的身份验证类型，容易被盗取破解，在部分对安全性要求高的场景不适用，“不良做法”

用户便捷性：

操作简单：用户只需记住密码即可

痛点：需要频繁更换复杂密码，一旦遗忘密码体验较差

2、多重身份验证（MFA）

需要至少两种不同类型的因素，是 SFA 的扩展

双因素认证（2FA）：最常见的 MFA，使用两个身份验证因素

发展历程：

初期（2000 年代）：金融机构引入短信验证码（OTP）作为第二因素，提升安全性。

进阶（2010 年代后）：硬件令牌（如 RSA SecurID）、认证应用（Google Authenticator）普及，部分机构采用推送通知（如银行 APP 动态验证）。

利弊：

优点：降低单点失效风险，符合监管要求

缺点：短信验证码受 SIM 卡攻击影响较大，易遭劫持；硬件令牌成本较大，要求用户随身携带

用户便捷性：

流程复杂度增加：需多步操作（输入验证码、令牌等），延长交易时间

接受度：大多数用户逐渐习惯，部分用户群体（老年人等）感到不便

3、免密认证——生物识别技术

发展历程：

萌芽期（2010 年代初）：指纹识别随智能手机（如 iPhone 5s）进入金融领域，用于移动银行登录。

成熟期（2020 年代）：面部识别（FaceID、3D 结构光）、声纹识别普及，部分银行支持静脉识别或虹膜扫描。

利弊：

优点：具有强唯一性，难以伪造，用户体验接近无感

缺点：生物特征难以重置，一旦泄密后果较大；存在技术误判的难题（光线

导致面部识别出错等）

用户便捷性：

高效：无需记忆密码或携带特定设备即可完成验证

硬件要求：依赖设备性能（低端的设备可能无法完成高精度识别）

类型[1]（二者均可减少身份欺诈）：

Ⅰ主动生物特征身份验证：要求用户在摄像头前执行特定操作，实时性 e.g.转头眨眼

适用于高风险、高安全性金融情况，如：银行和支付提供商保证安全登录和高价值交易；新客户账户设置或入职；作为敏感交易的第二步验证

优势——准确性安全性极高

Ⅱ被动生物特征身份验证：使用面部特征或身体特征，不要求实时 e.g.面部识别，打字模式

优势——方便、可扩展、无摩擦，改善用户体验，后台运行，减少重复操作需要，快速

4、自适应身份验证（基于风险的身份验证，RBA）[2]

使用 AI 和机器学习（ML）来分析用户行为并计算风险级别，根据用户当前行为的风险程度动态改变身份验证要求。e.g. 常用设备和位置——只需输入密码；新设备 or 常识访问敏感数据——高风险，要求提供更多身份因素

发展背景：人工智能和机器学习技术的发展

利弊：

优点：①从根本上防止帐户接管欺诈、移动和在线欺诈攻击；②根据风险级别为每笔交易应用精确的安全级别，减少不必要身份验证步骤，减少摩擦，增强客户体验，有利于银行数字化转型，维持客户忠诚度，释放增长机会；③限制黑客注入恶意软件的能力

缺点：①AI、ML 需大量数据训练，用户个人隐私泄露风险；②需较高技术投入和数据保护措施，对中小型金融机构而言成本压力大

用户便捷性：

用户行为较为稳定时——减少验证步骤，提升用户体验

高风险情境——繁琐的验证步骤，增加用户的操作负担

・MFA、生物识别技术、RBA 通常结合使用来动态评估风险。

5、DID（去中心化身份）

---

[1] 确保金融科技安全：主动身份验证 | ComplyCube

[2] https://www.fortunebusinessinsights.com/zh/risk-based-authentication-market-106503

发展历程：

探索期（2018 年后）：部分银行和金融科技公司（如瑞士瑞银、蚂蚁链）尝试基于区块链的 DID 系统，实现跨机构身份互认。

实践期（2020 年代）：结合零知识证明（ZKP）和可验证凭证（VC），用于跨境 KYC、供应链金融等场景。

利弊：

优点：用户自行管理身份数据，避免重复提交信息；系统基于区块链，链上存证，可审计性强

缺点：技术复杂度高，法律认可度低（DID 法律效力在许多国家如中国、俄罗斯未得到承认，仅有欧盟等少数国家承认其法律地位）

用户便捷性：

长期便捷：一次注册，多机构通用，跨境开户无需额外 KYC

短期门槛较大：用户需适应密钥管理（如助记词备份），学习曲线陡峭。

6、目前身份验证方案通常不是独立运作，而是彼此**交叉融合**（多层次多维度组合）

① **Session-Cookie 会话认证**

原理——用户登录成功后，服务器生成一个会话 ID（Session ID）存储在 Cookie 中，用于识别用户的身份。

优点——简单易用，适合 Web 网站。

缺点——不支持跨域应用，且需要服务器保存会话状态，移动端不方便使用。

② **JWT（JSON Web Token）**

原理——将用户信息、令牌和签名放在一个 JSON 对象中，每次请求时发送给服务器，服务器验证签名判断用户身份。

优点——无状态验证，减少服务器压力，适合分布式系统。

缺点——一旦签发，无法撤销，安全性依赖于密钥。

③ **SSO（单点登录）**

原理——通过一个中心认证服务（CAS），实现不同系统之间的用户身份共享，用户只需一次登录便可访问多个系统。

优点——用户体验好，适合多系统统一认证。

缺点——依赖于中心认证服务器，一旦服务出问题，所有系统都会受到影响。

④ **OAuth 2.0**

原理——基于授权码的三方认证协议，通过授权服务器实现第三方应用访问用户资源。

应用场景——移动应用、第三方网站的授权登录。

优点——适合多设备、分布式的场景，支持第三方授权访问。
缺点——实现较为复杂，需要更高的安全要求。

	Session-Cookie	JWT	SSO	OAuth 2.0
SFA/MFA	作为身份验证后的会话保持	JWT 可结合 MFA 使用	SSO 可以结合 MFA 保证安全性	OAuth 2.0 可以使用 MFA 增强授权流程
生物识别技术	可用于登录时生成 session	通过生物识别生成的 token 可用	可作为 SSO 登录时的一部分	可通过 OAuth 2.0 进行认证
DID（去中心化身份）	支持传统 Session，但通常与 DID 配合使用	可以将 DID 作为身份验证的部分	可通过 DID 提供去中心化认证	DID 可以结合 OAuth 2.0 提供身份认证
自适应身份验证	基于会话信息调整验证强度	使用 JWT 的信息进行风险评估	在 SSO 登录中结合动态验证	OAuth 2.0 可能会触发自适应验证
免密认证	Session 可能用于免密认证的会话保持	免密认证后的 JWT 作为身份凭证	免密认证可以与 SSO 结合	OAuth 2.0 与免密认证结合时不需输入密码

https://www.authing.co/solutions/finance
https://www.ibm.com/cn-zh/think/topics/authentication