浅谈 PCI DSS 涉及的认证技术

作者：atsec 杨秀玲

2025 年 10 月

关键词：身份认证因素、多因素认证、认证攻击、PCI DSS

atsec (Beijing) information technology Co., Ltd.

Floor 3, Block C, Building 1, Boya C-Center,

Beijing University Science Park, Life Science ParkChangping District, Beijing, Postcode: 102206
Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.com

目录

1 引言

在数字化技术不断提升的时代，账号盗用、数据泄露等安全威胁持续升级，简单的密码认证（Authentication）方式已难以抵御新的攻击方法。认证作为身份核验的重要技术，是提升访问控制安全性的基础。

本文档中的指导旨在为评估、实施或升级其认证方案的任何组织以及相关技术提供商提供参考，指导安全认证技术的实施，符合支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standard）标准要求，从而提升安全访问控制的技术手段，提高保护个人信息与企业资产的能力。

首先，我们介绍三个与认证相关的概念，包括认证流程、流程中包含的要素和生命周期。

认证流程中包含要素如下：

- 用户：请求进行身份认证的个人或系统。
- 凭证：用户 ID 与请求访问的用户提供的认证要素的组合。
- 认证系统/身份提供者：负责认证用户凭证并提供身份认证服务的系统、服务或应用程序。
- 被访问系统：经认证系统成功认证后向用户提供访问权限的系统。被访问系统与认证系统可能相同，也可能不同。
- 会话凭证：用于向认证系统以外的系统证明认证过程已发生。此类凭证通常被称为会话令牌、认证令牌、Cookie 或类似名称。

认证流程：用户在认证系统中输入已有的凭证，经认证系统认证通过后用户才能访问到被访问的系统。当被访问系统与认证系统不同时，则需要使用到会话凭证。会话凭证由认证系统提供，并在认证系统认证用户提供的凭证后分配给用户的会话。会话凭证免除了用户在每次访问新系统、应用程序或执行数据操作时重新向认证系统进行身份认证的需要。在某些情况下，用户访问的每个独立系统都可能提供新的访问令牌。多数（非全部）认证系统均采用会话凭证机制。

身份认证的生命周期包含三个阶段：

- 用户（重新）注册

用户身份认证凭证在系统中初始化，初始化可能在首次使用、重置或修改现有凭证时发生。重新注册可能因系统或流程错误（例如用户忘记密码）而发生，也可能因修改现有凭证（例如更新密码或从单因素类型切换至其他因素类型）而发生。

- 用户身份认证

指用户向认证系统提交凭证以验证其声明身份的过程。

- 会话认证

此阶段针对用户正在访问的系统和资源进行持续性身份认证。

本文将探讨基于认证技术的认证因素、认证类型、认证攻击，并深入介绍 PCI DSS 标准中涉及的要求。本文参考了 PCI SSC（PCI SSC： Payment Card Industry Security Standards Council） 在产业最新（2025 年 8 月）发布的相关指导，并结合 atsec 作者经验给出了最佳实践的总结。

2 认证因素

2.1 认证因素类型

身份认证因素用于证明或验证用户身份（例如计算机系统中的个人或进程）。这些因素可分为以下三类：

- 你所知晓的（知识型因素）：是以用户独知信息为形式的凭证，例如密码、口令或个人识别码 （PIN：Personal identification Number）。
  注：本指南中“PIN”指认证系统中使用的数字知识型因素，不涉及支付环节持卡人验证所用的卡片 PIN 码。
- 你拥有的东西（持有型因素）：与用户所持设备唯一关联的凭证，例如内置加密密钥的智能卡或显示动态 PIN 值的物理令牌。
- 生物特征因素（遗传/生物识别因素）：与用户生理特征独特属性关联的凭证，如指纹、面部识别或声音识别等。

这些因素的“独特性”对安全至关重要，由用户及其他认证对象共同知晓的认证因素，例如姓氏、父母或学校信息等，都不是安全的认证因素，其均不符合“独特性”的要求。

与密码类似，遗传或生物特征因素必须具有个体唯一性，且不易被复制或伪造。例如：用户是否拥有“面部”这一认证因素可视为遗传/生物特征因素的一种，但随着“深度伪造”及其他 AI 生成内容（视频、图片、语音等）制作门槛降低，曾被视为足够安全的继承性因素需重新评估，因此此类渠道应考虑采用额外认证方式。

除上述主要认证因素外，还可添加来自补充因素的信息。补充因素单独使用时通常无法满足作为主要认证因素所需的“唯一性”要求，但它们能为认证系统提供有用的额外安全保障。补充因素可能包括：

- 基于位置的补充因素：与用户所在位置或所用访问设备相关的信息。例如物理位置、计算机 ID 或操作系统详情。
- 行为型补充因素：用户可执行的操作特征。例如访问时间、请求的访问类型或键盘输入习惯。

使用用户密码和用户位置作为身份认证因素的系统可以提供比单独使用用户密码更高的安全性。然而，这并不能满足多因素身份认证的要求，因为只使用了一个主要因素（密码）。

2.2 认证要素的存储与可用性

- 密码或加密密钥等机密值的安全存储

为降低泄露风险，这些机密值应被安全存储，绝不能以明文形式存储，而应采用“单向函数”处理。最佳实践是采用能同时增加比对时间和内存消耗的算法，而非仅通过标准哈希函数单次处理，后者

通常可被快速破解。使用密码唯一的“盐值”同样至关重要，可有效防止密码哈希字典（即“彩虹表”）的预计算。

- 密码和一次性密码（OTP：One-Time Password）的安全存储

认证流程还需要考虑到密码的易用性。用户可能难以生成、记忆和输入复杂密码、因此使用密码管理器等工具较为普遍。为保障此类工具的安全使用，密码和 OTP 输入框应支持用户直接粘贴内容。此举既能降低用户因操作便捷而使用安全性较低密码的概率，又能减少输入过程中的疏漏风险。一次性密码还应设置有效时限，防止攻击者预先生成密码以备后用。密码有效期应根据传输方式及系统风险分析结果确定。例如：通过认证应用获取的 OTP 有效期可设为 60 秒内使用，而通过消息系统（如电子邮件或短信）传递的 OTP 则需更长有效期以覆盖消息传输时间。所有场景下，OTP 有效期均应匹配当前认证流程所需时长，通常以分钟计而非小时或数十分钟。

- 加密密钥和会话令牌的安全存储与管理

用于派生其他密钥和会话令牌值的高级加密密钥应尽可能安全地存储——例如通过专用安全系统：硬件安全模块（HSM：Hardware Security Module），可信平台模块（TPM：Trusted Platform Module）、可信执行环境（TEE：Trusted execution environment）、安全元件（SE：Secure Element）或智能卡，可用于安全存储用户密钥或会话令牌。

2.3 个人识别码（PIN）的应用

在某些身份认证流程中，常会使用不符合严格复杂性要求的知识型因素——四位数 PIN 码便是一个典型例证。然而，只要对该因素的使用方式实施管控措施，既能防范在线暴力破解攻击，又能抵御离线暴力破解攻击。例如，若身份认证设备/应用程序将失败尝试次数限制在可防止暴力破解的水平，则用于解锁认证设备的 PIN 码即为可接受方案。对于四位数 PIN 码，常见限制为 3 次失败尝试。针对所有可能遭受此类攻击的凭证（包括密码），应实施暴力破解防护措施及在线暴力攻击检测机制（例如凭证填充攻击）。

2. 4 消息系统作为持有因素与设备无关性

某些认证方法通过消息系统向用户发送登陆专属凭证，例如一次性密码（OTP）或嵌入认证凭证的链接。此类实现中，用户对接收消息系统的访问权限被视为持有因素。此类情境中还需考虑因素的独立性问题：即攻击者若获取某一因素（例如设备 PIN 码），是否会自动获得另一因素（例如基于短信或邮件的 OTP）的访问权限。在此情况下，该方案是否真正实现了多重认证因素。PCI DSS 虽未强制要求多因素认证中不同因素独立性，但任何认证系统的风险分析都应将因素独立性纳入考量。

保障此类持有因素的安全至关重要，但往往较为复杂。例如，用户常通过多台设备访问同一消息账户，任何单一设备的安全漏洞，或消息账户在设备间的迁移过程，都可能形成可被利用的弱点。电子邮件账户劫持攻击或 SIM（Subscriber Identity Module）卡交换/迁移攻击，便是此类实现方案常见的攻击手段。

当使用消息系统传递认证因素时，接收消息的设备才是持有因素，而非消息本身。因此，所有可能接收消息的设备都应充分控制对消息账户的访问权限。使用消息系统时的最佳实践是为所有可能接收消息的设备配置各自独立的充分认证机制（例如设备锁屏），以验证消息访问者的身份。尤其在多用户计算系统中，必须实施个人用户认证，确保正确接收者获取认证消息。

当 SIM 卡作为此类系统的一部分使用时，除在设备锁屏界面拦截消息内容（涵盖所有适用消息类型）外，还应实施 SIM PIN 机制以防范丢失和被盗攻击。最后需针对使用 SIM 卡的场景考虑防范重放攻击和中继攻击的控制措施。

2.5 防钓鱼认证

许多认证因素的实现依赖于用户与所认证系统之间传输的机密数据。这类机密数据可能包括密码、PIN 码、OTP 等。此类实现方式容易遭受攻击者通过“网络钓鱼”截获机密数据，进而用于重放攻击或中继攻击。

采用“防钓鱼”认证机制可有效防范此类攻击。此类认证确保在未验证请求方身份前，绝不泄露认证密钥。美国国家标准与技术研究院 SP 800-63 规范将防钓鱼认证定义为：认证协议无需依赖声明方的警惕性，即可防止认证密钥及有效认证输出泄露给冒名验证者。

通常，防钓鱼认证会采用“零知识证明”技术，在不泄露任何密钥信息的前提下，确认用户持有特定密钥值。由于防钓鱼认证依赖于密码技术，它要求用户持有唯一的加密密钥并具备操作该密钥的能力。因此，防钓鱼认证属于持有因素类认证。此类认证还可能结合其他因素类型（如个人识别码或生物特征）来“解锁”加密密钥的使用权限。

尽管使用防钓鱼认证并非强制要求，但因其提供的钓鱼防护能力，该方案被视为最佳实践。然而，防钓鱼认证本身并非多因素认证，除非其要求使用其他因素（如生物特征或 PIN 码）。

2.6 高安全性区域与任务的身份认证

某些场景或环境需要更高的安全性和认证级别。例如将加密密钥加载到硬件安全模块（HSM）中，以及将账户数据配置到支付卡的环境。在这种情况下，通常要求某些任务采用“双重控制”机制。

双重控制要求由两名或更多人员共同授权任务执行。通常通过要求两人各自输入独立的身份认证凭证来实现。但并非所有系统都支持此类配置。在这种情况下，仍可通过“密码分割”实现双重控制——即由两人分别输入单一密码的两部分。密码分割不应与加密密钥的“分割知识”要求混淆。后者要求任何个人都不得知晓密钥的任何部分。密码分割的使用应仅限于无法采用更安全认证方法的情境，例如未使用智能卡或物理令牌等加密设备的情况。

在某些高安全环境中，计算系统常与企业广域网隔离（例如采用“物理隔离”）。此类环境需重点考虑身份认证管理策略，因为长期使用缓存会话凭证与定期重新认证提供的安全保障之间往往存在权衡关系。

2.7 通行密钥（Passkeys）

通行密钥是一种基于 FIDO2 标准的加密安全登录凭证。用户持有专属于其账户及所认证服务的私有加密密钥，而服务方则验证用户持有对应的公钥。登录时，服务方会验证公钥与私钥是否匹配。

密钥认证具备防钓鱼特性：既无可窃取的共享凭证，亦无可用于攻击的登录数据，且每个密钥均与特定认证系统绑定。此机制能有效抵御钓鱼攻击、凭证填充攻击及账户劫持等威胁。密钥可绑定于特定设备，也可实现跨设备同步（同步通行密钥）。

- 设备绑定型通行密钥

设备绑定密钥是指密钥的用户组件（私钥）被锁定在单一设备上，通常存储于设备内的专用安全区域，如 TPM、TEE 或 SE。设备绑定密钥可视为持有该绑定设备的凭证。

- 同步密钥

同步密钥不受限于单一设备，同一密钥可在多台设备间共享。PCI DSS 标准中并未禁止使用同步密钥、但需注意：使用同步密钥意味着所有可同步该密钥的系统均需满足相关标准的认证要求。这可能导致系统复杂度提高，因此应审慎评估同步密钥的使用，权衡其带来的便利性提升是否值得增加的复杂度与验证影响。

2.8 无密码（Passwordless）认证

“无密码认证”指无需用户输入基于知识的认证因素（如密码）的认证方式。该术语通常特指防钓鱼攻击的实现方案，但也可能涵盖其他类型方案。因此在规划无密码系统时，必须明确所采用和支持的底层认证机制。

3 认证类型

3.1 多因素认证（MFA：Multi-Factor Authentication）

多因素认证，是一种用户身份认证方法，要求在授予访问权限前验证至少两种不同类型的主要认证因素。因此 MFA 必须包含至少两种不同类型的认证因素。

MFA 旨在为访问计算资源者的身份提供更高保障级别。这种增强保障机制类似于其他深度防御安全措施，迫使攻击者必须突破至少两种认证方式才能成功入侵。

若密码作为一种认证机制已被破解，使用两个（或更多）不同密码并不能提升安全性。这种仅使用单一因素的方式，并不属于 MFA 范畴。同理，同时采用用户密码和地理位置（补充因素）作为认证要素的系统，其安全性可能高于仅使用密码的系统。但此类方案仍不符合多因素认证要求，因为仅使用了单一的独特认证因素（密码）。

3.2 双步认证（Two-step Authentication）

双步认证与 MFA 存在差异：MFA 要求使用两种或更多不同类型的主要因素，而双步认证仅需提供两种认证因素，无论这些因素是否属于不同类型。

若双步认证需要三种主要因素中的至少两种，且在授予访问权限前两种因素都验证通过，则可作为 MFA 方案的组成部分。

3.3 升级认证（Step-up Authentication）

升级认证是一种额外的身份认证或识别方式，可根据特定访问请求相关的风险要求实施。单一因素认证成功后可获得基础访问权限，后续可能需要提供第二因素验证以获取更高权限。

升级认证不符合 PCI DSS 提及的多因素认证 MFA 的要求。

4 认证攻击

4.1 重放（Replay）攻击

重放攻击是指通过截获或获取有效认证数据，随后为恶意目的重新发送或重定向通信的攻击手段。在认证实现中，重放攻击通常利用合法凭证获取未经授权的访问权限，并可同时攻击多种认证因素。

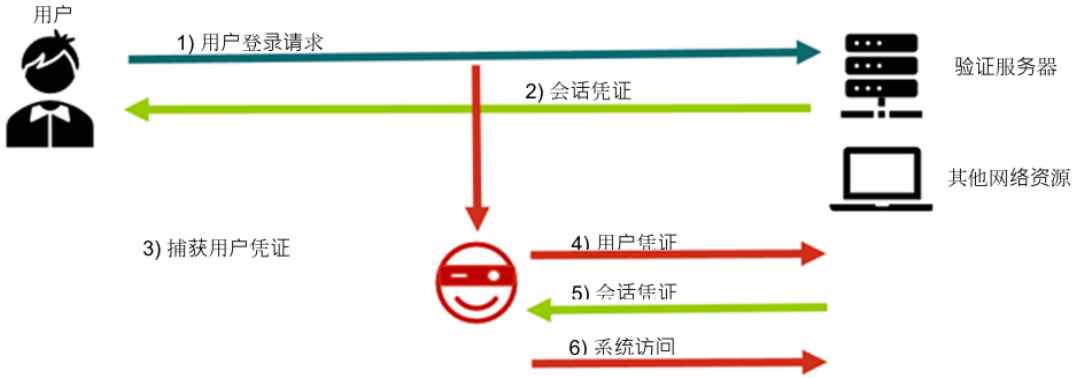


图 1： 重放攻击流程示意图 （图片源自 PCI SSC Authentication Guidance）

防范重放攻击的方法包括：检测并拒绝重复或延迟认证尝试的机制，具体措施包括但不限于：使用唯一会话标识符与会话密钥、时间戳、基于时间的一次性密码或验证码。

4.2 中继（Relay）攻击

中继攻击与重放攻击相似，攻击者会捕获合法用户的有效认证数据，并利用这些数据冒充该身份的所有者。但中继攻击的区别在于它是实时攻击，攻击者插入在用户与认证系统之间，如下图所示，对用户伪装成认证系统，对认证系统伪装成用户。中继攻击又称中间人攻击。

图 2： 中继攻击流程示意图 （图片源自 PCI SSC Authentication Guidance）

由于中继攻击发生在认证过程的实时阶段，它能绕过许多用于防范重放攻击的控制措施。此类攻击常针对使用一次性密码（OTP）的系统展开。尽管 OTP 因其一次性特性和使用时限限制难以被重放，但攻击者却能轻易实现其转发。

防范中继攻击通常需要实施方法确保用户能够验证其凭证接收方的身份。这可通过验证服务器端证书建立安全通道连接实现，例如采用传输层安全协议（TLS：Transport Layer Security）或虚拟专用网络（VPN：Virtual Private Network）。

表 1 列出了不同类型攻击或漏洞的参考信息。这些攻击与漏洞的具体细节如下：

- 网络钓鱼——恶意方试图欺骗或胁迫用户，使其向攻击者而非认证系统提供秘密凭证。网络钓鱼是一种中继或重放攻击，攻击者通过中继或重放用户凭证来冒充该用户。
- 认证器威胁——向用户提供认证凭证数据的应用程序或设备遭到威胁。包括物理认证器的丢失/被盗，以及认证器软件或密钥文件、用户密码和密码文件的威胁，以及针对生物特征系统呈现的攻击（如深度伪造）。
- 账户威胁——认证机制依赖于第二个用户账户，该账户一旦被攻破，将危及整个认证流程。典型案例包括：用于接收一次性密码的电子邮箱账户被攻破、密码管理器或认证应用账户被攻破、通讯设备账户被攻破。
- 中间人攻击——恶意方插入在用户与凭证验证器之间，从而使攻击者能够查看、修改或以其他方式破坏身份认证凭证。中间人攻击可能包含各类中继攻击。
- 加密漏洞——认证凭证或流程依赖于密码协议，一旦该协议被破解，认证过程便可能失效。典型案例包括针对密码系统的全新密码分析攻击，或密码学相关量子计算机的出现。
- 密钥泄露——认证方法依赖某些密钥值，一旦泄露将危及认证流程。包括用于生成一次性密码值的根级加密密钥丢失或被盗，或密码等基于知识的密钥遭泄露。密钥泄露涵盖各类重放攻击。
- 暴力破解——攻击者通过多次尝试猜测值或尝试大量可能的输入来寻找正确答案。例如凭证填充攻击、猜测低熵知识型密码（如结构不良的密码或短 PIN 码）。某些暴力破解攻击属于重放攻击，因为它们会复用先前泄露的值，例如凭证填充攻击。

表 1 列举了各类认证方式的示例、其相对强度以及增强各认证要素安全性的方法。认证要素下方的括号内标注了要素类型，格式为[要素类型]。

表 1：认证类型，强度与攻击类型 （表格源自 PCI SSC Authentication Guidance）

排名	认证因素和[类型]	示例	攻击类型	提升安全性
最佳实践	防钓鱼认证 [持有]	基于 FIDO2 的通行密钥	▪ 认证器威胁 、 ▪ 加密漏洞	使用设备绑定密钥
	加密挑战/响应 [持有]	基于令牌/智能卡的用户私钥，主机公钥	▪ 网络钓鱼 ▪ 认证器威胁 ▪ 中间人攻击 ▪ 加密漏洞 ▪ 秘密威胁	▪ 使用设备绑定密钥 ▪ 通知请求服务器更改/检测更改（这可以增加防网络钓鱼能力）
良好实践	长度较长的随机生成密码 [知识]	密码管理器生成的密码	▪ 网络钓鱼 ▪ 账户威胁 ▪ 中间人攻击 ▪ 暴力破解	▪ 使用安全的密码管理器 ▪ 确保密码生成规则足够复杂

			▪ 秘密威胁	
	本地生成的 OTP [持有]	由认证器应用或密钥卡生成的 OTP	▪ 网络钓鱼 ▪ 认证器威胁 ▪ 中间人攻击 ▪ 加密漏洞 ▪ 暴力破解 ▪ 秘密威胁	▪ 使用设备绑定密钥保护资产 ▪ 使用足够长的 OTP 值
	生物特征 [继承]	面部识别或指纹传感器	▪ 加密漏洞 ▪ 认证器威胁	▪ 使用本地验证的生物特征 ▪ 确保生物特征传感器和系统的质量 ▪ 实施深度伪造防护
可接受的做法	远程生成的 OTP [持有]	通过电子邮件或短信发送的 OTP	▪ 网络钓鱼 ▪ 账户威胁 ▪ 中间人攻击 ▪ 加密漏洞 ▪ 暴力破解 ▪ 秘密威胁	▪ 使用推送消息传递 ▪ 使用足够长的 OTP 值 ▪ 在 OTP 消息中实施用户可验证内容 ▪ 在第二因素前验证 OTP ▪ 安全消息设备
	带外会话令牌 [持有]	通过电子邮件或短信发送的链接	▪ 网络钓鱼 ▪ 账户威胁 ▪ 中间人攻击 ▪ 加密漏洞 ▪ 暴力破解	▪ 使用推送消息传递 ▪ 在链接消息中实施用户可验证内容 ▪ 在使用链接前验证二次因素 ▪ 安全消息设备
	用户生成的密码 用户 PIN [知识]	用户未通过密码管理器创建的密码或 PIN 码	▪ 网络钓鱼 ▪ 中间人攻击 ▪ 暴力破解 ▪ 秘密威胁	▪ 使用第二个非主要因素，例如位置 ▪ 提供暴力破解防护
	用户手势 [知识]	Android 滑动解锁		使用设备绑定密钥

5 PCI DSS 提及的认证要求

5.1 要求概述

PCI DSS v4.0.1 的认证要求包含在要求 8.3、8.4 和 8.5 中，总结如下：

要求 8.3.1：所有用户对系统组件的访问都至少通过一个认证因素进行认证。

要求 8.4.1：对于所有管理人员进入持卡人数据环境（CDE：Cardholder Data Environment）的非控制台访问，均需实施 MFA。

要求 8.4.2：对于所有管理人员进入 CDE 的非控制台访问，均需实施 MFA，但需要注意的是，该要求不适用于仅使用防网络钓鱼认证因素进行认证的用户账户。

要求 8.4.3： 对于所有来自实体网络外部、可能访问或影响 CDE 的远程访问，均需实施 MFA。

要求 8.5.1：MFA 系统配置了若干特性以防止滥用。

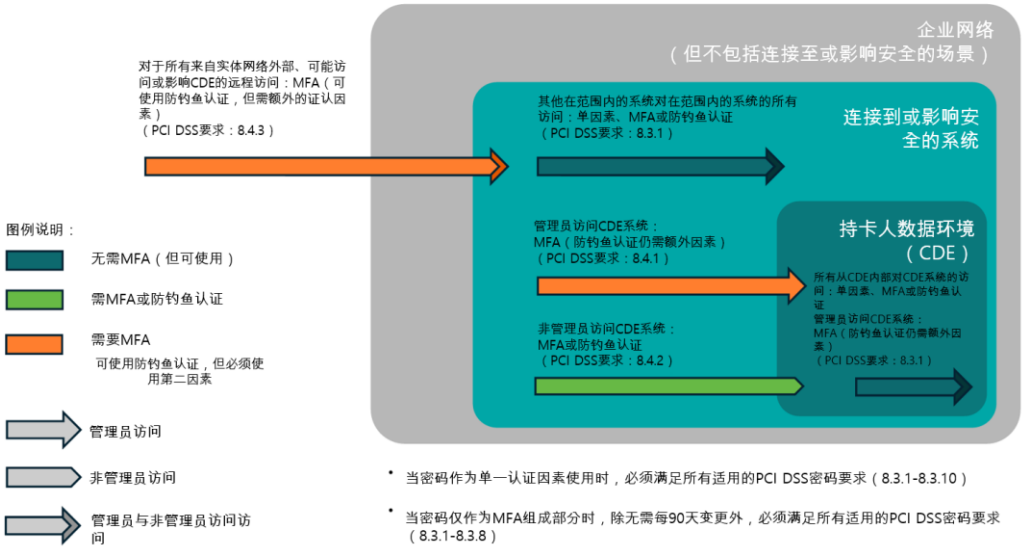
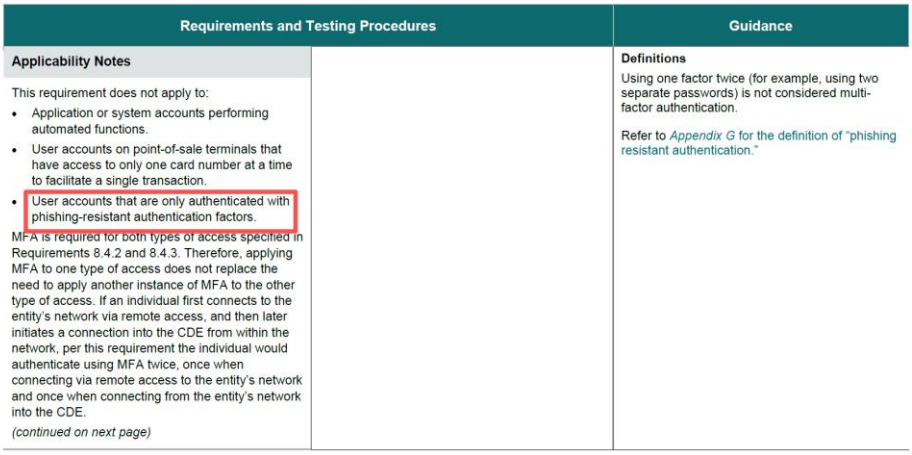


图 3： 中继攻击流程示意图 （图片源自 PCI SSC Authentication Guidance）

要求 8.4.2 包含一项适用性说明，即该要求不适用于“仅通过防网络钓鱼认证因素进行认证的用户账户”。对于此要求，根据 FIDO2 要求实施的凭证（包括设备绑定和同步通行密钥）可作为单因素认证使用以替代 MFA。

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
8.4.2 MFA is implemented for all non-console access into the CDE.	**8.4.2.a** Examine network and/or system configurations to verify MFA is implemented for all non-console access into the CDE.	Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase.
	8.4.2.b Observe personnel logging in to the CDE and examine evidence to verify that MFA is required.	
Customized Approach Objective		
Access into the CDE cannot be obtained by the use of a single authentication factor.		*(continued on next page)*

图 4：PCI DSS 要求 8.4.2 （图片源自 PCI DSS V4.0.1 标准）



Requirements and Testing Procedures	Guidance
Applicability Notes This requirement does not apply to: • Application or system accounts performing automated functions. • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction. • User accounts that are only authenticated with phishing-resistant authentication factors. MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting from the entity's network into the CDE. *(continued on next page)*	**Definitions** Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. Refer to *Appendix G* for the definition of "phishing resistant authentication."

图 5：PCI DSS 要求 8.4.2-续 （图片源自 PCI DSS V4.0.1 标准）

对于要求 8.4.1 和 8.4.3（不包括上述要求 8.4.2 的适用性注释），仍可使用防钓鱼认证，但必须辅以额外的认证因素（例如密码、PIN 或生物特征）才能满足这些 MFA 要求。该第二种因素可用于解锁防钓鱼凭证的使用，或在认证过程中作为单独凭证提供。

PCI DSS v4.x 要求所有认证因素均成功通过后才能授予访问权限。对于多因素认证（MFA）的部署，若在展示后续任一认证因素前，先提示前一因素已验证成功，这符合 PCI DSS 的 MFA 要求。但是，在验证所有因素均成功之前，不得提供访问权限。

最佳实践建议采取以下两种方式之一：

1）在所有因素都提供之前，不提供任何因素成功的反馈；

2）在认证不同会话中相同的因素（例如密码）之前，使用会话唯一因素（例如 OTP 或防钓鱼因素）进行认证。

PCI DSS 要求 8.5.1 规定，MFA 系统应配置为防止滥用。这意味着 MFA 系统应配置为：

1）不受重放攻击的影响。

2）除非有明确记录、获得授权且仅限于有限时间，否则任何用户（包括管理用户）都无法绕过。

3）要求使用至少两种不同的认证因素类型。

4）要求所有认证因素均成功后才授予访问权限。

5.2 远程访问

PCI DSS 8.4.3 涉及远程访问的 MFA。在此要求中，“远程”一词适用于通过公共或不可信网络进行的任何访问。这包括建立任何虚拟专用网络（VPN）连接所涉及的认证流程。

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows, such as a password or passphrase. **Definitions** Multi-factor authentication (MFA) requires an individual to present a minimum of two of the three authentication factors specified in Requirement 8.3.1 before access is granted. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication. *(continued on next page)*
8.4.3 MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE.	**8.4.3.a** Examine network and/or system configurations for remote access servers and systems to verify MFA is required in accordance with all elements specified in this requirement.	
	8.4.3.b Observe personnel (for example, users and administrators) and third parties connecting remotely to the network and verify that multi-factor authentication is required.	
Customized Approach Objective		
Remote access to the entity's network cannot be obtained by using a single authentication factor.		

图 6：PCI DSS 要求 8.4.3 （图片源自 PCI DSS V4.0.1 标准）

Requirements and Testing Procedures	Guidance
Applicability Notes	
The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. This includes all remote access by personnel (users and administrators), and third parties (including, but not limited to, vendors, suppliers, service providers, and customers). If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.	

图 7：PCI DSS 要求 8.4.3 -续（图片源自 PCI DSS V4.0.1 标准）

5.3 非控制台访问

PCI DSS 要求 8.4.1 和 8.4.2 都要求对进入 CDE 的所有非控制台访问实施 MFA。

Requirements and Testing Procedures		Guidance
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Requiring more than one type of authentication factor reduces the probability that an attacker can gain access to a system by masquerading as a legitimate user, because the attacker would need to compromise multiple authentication factors. This is especially true in environments where traditionally the single authentication factor employed was something a user knows such as a password or passphrase. **Good Practice** Implementing MFA for non-console administrative access to in-scope system components that are not part of the CDE will help prevent unauthorized users from using a single factor to gain access and compromise in-scope system components. **Definitions** Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.	**8.4.1.a** Examine network and/or system configurations to verify MFA is required for all non-console into the CDE for personnel with administrative access.	
	8.4.1.b Observe administrator personnel logging into the CDE and verify that MFA is required.	
Customized Approach Objective		
Administrative access to the CDE cannot be obtained by the use of a single authentication factor.		
Applicability Notes		
The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection.		

图 8：PCI DSS 要求 8.4.1 （图片源自 PCI DSS V4.0.1 标准）

控制台访问与非控制台访问的区别如下：

- 控制台访问通常指用户通过直接物理连接与系统交互，该连接不依赖于网络、无线或交换式连接。这意味着访问是从控制台通过物理电缆到系统组件的。控制台访问是系统管理员通常使用的机制，通过物理电缆连接位于 CDE 或敏感区域的系统，以管理该系统。控制台访问是一种更安全的访问形式，因为未经授权的用户难以对其进行截获。某些系统可能采用非直接连接方式，但只要所有连接均清晰可见，且可以验证未包含恶意设备（例如服务器故障紧急维护系统），这类系统的部署仍属于控制台访问。
- 非控制台用户通常指用户通过联网硬件设备切换器、连接到共享 USB（Universal Serial Bus）集线器（并非仅用于提供控制台访问）的 USB 键盘或无线键盘进行的访问。

5.4 身份认证与密码学

认证通常与密码学紧密关联：无论是认证过程本身（如使用密钥认证）、保障密钥存储安全，还是为用户与认证系统间通信提供安全通道。因此，在讨论密码学使用及适用性的任何要求范围内，都应将认证机制中使用的密码学纳入考量。

一个典型示例是 PCI DSS 要求 12.3.3，该条款规定加密技术的使用需至少每 12 个月进行一次文档记录与审查。这属于更广泛的加密敏捷性概念范畴——即快速响应加密实现安全变化的能力。例如，某认证方法采用 RSA 加密技术，则必须理解该技术特性，并追踪可能影响该算法安全的密码分析或计算方法的任何变化。

6 结语

本文围绕“认证技术”详细介绍了当下常见的认证因素类别、认证类型以及基于认证的常见攻击手段，并结合了 PCI DSS 要求中的相关认证要求点，可以从中获得对应的安全合规的方案参考，从而提升安全合规建设能力。本文档中的指导旨在为评估、实施或升级其认证解决方案的任何组织以及认证解决方案的提供商提供参考。

以下列举了实施认证系统时应考虑的最佳实践示例（非强制要求）：

- 教育用户如何生成安全密码。
- 实施控制措施以减轻深度伪造攻击的影响。
- 为一次性密码（OTP）使用设置合理时限，允许用户将数据粘贴至密码和 OTP 输入框。
- 采用安全存储认证密钥的方法，例如使用内存密集型比对函数并为每个密码设置唯一盐值，或采用抗攻击存储方案如硬件安全模块（HSM）或硬件管理设备（HMD）。
- 为凭证实施在线和离线暴力破解防护。
- 通过实施 SIM 卡 PIN 码、锁屏控制、通知拦截、账户迁移管控等措施，保障可用于获取认证要素的系统安全。
- 考虑使用更安全的身份认证因素，而非基于消息传递的因素。
- 将凭证存在或可能遭泄露的所有位置纳入适用安全控制的范围。
- 尽可能实施防钓鱼认证机制。
- 针对敏感访问操作（如管理员访问或高安全区域/任务访问），应采用设备绑定型因素（如设备绑定密钥、智能卡、令牌等）。
- 限制同步密钥的业务使用场景，以最小化适用安全要求的范围。
- 尽可能实施多因素认证。
- 确保（重新）注册流程的安全性，以防止账户接管攻击。
- 尽可能将会话凭证绑定至特定设备或用户。
- 在判定验证成功/失败前，必须验证所有多因素认证（MFA）要素或非静态要素。
- 在评估可接受的加密最低标准和加密灵活性时（例如 PCI DSS 要求 12.3.3），需纳入认证方法。

atsec 也将持续跟进产业技术研讨和标准发展，协助不同机构实现合规（如 PCI DSS 标准）体系建设。

A 参考资料

i. https://www.pcisecuritystandards.org/

ii. https://www.atsec.com/