 DOI: https://doi.org/10.12349/iser.v6i4.5315

Identification and avoidance of information system key management risk

Wenxia Yin

Dengbao (Shanghai) Enterprise Development Co., Ltd., Shanghai, 201601, China

Abstract

Key is the cornerstone of information system security, key management risk identification and avoidance is the focus of information system development, use, evaluation. This paper systematically analyzes the security risk control points of information system key management from the aspects of cryptographic algorithm compliance, key management standardization and security protection effectiveness. The typical problems in the whole life cycle of the key, such as lack of randomness, lack of transmission security, insecure storage, non-compliant use, incomplete update and destruction, are deeply discussed. In order to solve these problems, an improvement strategy is proposed to meet the requirements of security assessment for commercial cryptography applications.

Keywords

commercial cryptographic application security assessment, key management, information system security, cryptographic technology

信息系统密钥管理风险识别与规避

殷文霞

等保（上海）企业发展有限公司，中国 · 上海 201601

摘　要

密钥是信息系统安全的基石，密钥管理风险识别与规避是信息系统研发、使用、评估的重点。本文从密码算法合规性、密钥管理规范性、安全防护有效性等维度，系统分析信息系统密钥管理的安全风险控制点。深入探讨密钥全生命周期中的典型问题，如随机性不足、传输安全性缺失、存储方式不安全、使用不合规、更新与销毁不彻底等。针对这些问题，提出符合商用密码应用安全性评估（密评）要求的改进策略。

关键词

商用密码应用安全评估、密钥管理、信息系统安全、密码技术

1 引言

密码技术作为信息安全的基石，通过对数据的加密和解密，保障信息的保密性、完整性与可用性。而密钥，作为密码技术的核心，如同开启信息安全之门的钥匙，其管理质量直接决定密码系统乃至整个信息系统的安全效能。信息系统密钥管理实践中的问题进行剖析，并探索有效的突破路径，具有重要的现实意义与实践价值。

2 密钥管理实践中的风险识别

2.1 密钥生成环节问题

随机性与不可预测性不足：密钥生成应具备足够的随机性和不可预测性。然而在实践中，部分信息系统为简化开发流程，采用伪随机数生成器来生成密钥。伪随机数生成器（PRNG）基于特定算法和初始种子值产生序列，若种子值选取不当或算法存在缺陷，生成的密钥易被预测。密钥协商前活协商过程中没有验证对方身份真实性。即使采用硬件随机数生成器（HRNG），但未采用通过认证的随机数发生器生成密钥，且无公开文献和证据证明随机数发生器的合理性和正确性。

密钥长度与强度不符：一些信息系统为节省资源或因开发人员对标准理解不足，选择较短的密钥长度。如在对数据保密性要求较高的金融交易场景中，应使用高强度的 256 位 AES 密钥，部分系统却仍采用 128 位甚至更低强度的密钥，大大增加了密钥被暴力破解的风险。

2.2 密钥分发环节问题

传输安全性缺失：密钥分发过程需确保密钥在传输过程中的保密性和完整性。然而，部分信息系统在密钥分发时，未对传输的密钥进行加密处理，直接以明文形式在网络中传输。例如，一些内部信息系统认为网络环境安全，忽略了内部网络也存在被攻击的可能性，攻击者可通过网络嗅探技术截获明文密钥。即使对密钥进行了加密传输，若采用的加密

【作者简介】殷文霞（1979–），女，中国江苏人，硕士，工程师，从事信息安全研究。

算法强度低或加密密钥管理不善，也无法保证传输安全。此外，在密钥传输过程中，若未采用消息认证码（MAC）等技术保证数据完整性，攻击者可能篡改密钥，导致接收方使用错误密钥进行加密或解密操作。

身份认证机制不完善：准确验证接收方身份是密钥分发的关键。实践中，部分信息系统的身份认证机制过于简单，容易被绕过。比如仅依靠用户名和弱口令进行身份验证，攻击者可通过暴力破解或社会工程学手段获取合法用户的认证信息，冒充接收方获取密钥。还有些系统在密钥分发过程中，缺乏对发送方和接收方的双向身份认证，导致中间人攻击风险增加，攻击者可在通信双方不知情的情况下截取并篡改密钥分发信息。

2.3 密钥存储环节问题

存储方式不安全：密钥应采用加密等安全方式存储。但许多信息系统为方便访问和使用，将密钥以明文形式存储在数据库或文件系统中。一旦系统遭受攻击，数据库或文件被窃取，密钥将直接暴露给攻击者。即使采用了加密存储，若加密密钥同样存储在不安全位置或保护措施不当，攻击者获取加密密钥后，仍可轻易解密存储的密钥。而且，用于加密密钥的口令以明文的形式存储或复杂度小于 10^{12} 另外。

存储介质管理不善：密钥存储介质的管理至关重要。在实际情况中，一些企业对存储密钥的介质，如 USB 密钥、智能卡等，缺乏严格的登记、保管和使用记录。存储介质可能随意放置，易丢失或被盗取。部分系统密钥（除公钥外）未设置访问控制机制，可以被非授权访问、使用、泄露、修改和替换。此外，当存储介质达到使用寿命或不再使用时，未按照标准要求进行安全销毁，残留的密钥信息可能被恢复利用。

2.4 密钥使用环节问题

使用不合规：密钥应按照特定用途和权限使用。但在实际应用中，存在密钥滥用现象。例如，本应用于数据加密的密钥被用于数字签名，或者低权限用户获取高权限密钥进行操作。这不仅违反了密钥使用的合规性原则，还可能导致安全漏洞。

审计与监控缺失：对密钥使用进行审计和监控能够及时发现异常操作。然而，许多信息系统未建立完善的密钥使用审计机制，无法记录密钥使用的时间、用户、操作等详细信息。当出现密钥泄露或滥用事件时，难以追溯原因和责任。同时，缺乏实时监控机制，不能及时发现异常的密钥使用行为，如短时间内频繁使用密钥进行大规模数据解密，可能预示着系统遭受攻击，但因无监控机制无法及时察觉并采取措施。

2.5 密钥更新、销毁环节问题

密钥更新不及时：随着时间推移和技术发展，密钥可能面临更高的破解风险，因此需定期更新。但实践中，部分信息系统未按照规定的周期或条件进行密钥更新。一方面，可能由于系统维护人员对密钥更新重要性认识不足，忽视了密钥更新工作；另一方面，密钥更新涉及系统多个模块的调整和数据迁移，操作复杂，部分企业因担心影响业务正常运行而拖延更新。长期使用同一密钥，大大增加了密钥被破解的可能性，一旦密钥泄露，将对整个信息系统安全造成严重威胁。

密钥销毁不彻底：当密钥不再使用时，需进行安全销毁，防止密钥残留带来安全隐患。然而，在实际操作中，许多系统未能做到彻底销毁密钥。例如，在删除存储密钥的文件时，只是简单删除文件索引，而存储设备上的数据并未真正擦除，攻击者可通过数据恢复技术获取残留的密钥信息。此外，对于一些采用硬件加密模块存储的密钥，在硬件设备报废时，未对其中的密钥进行彻底清除，导致报废设备可能成为密钥泄露的源头。

3 基于密评要求的密钥管理优化策略

3.1 密钥生成环节

强化随机数生成机制：为确保密钥生成的随机性与不可预测性，信息系统应采用经过国家密码管理部门认证的高质量随机数生成器。硬件随机数生成器（HRNG）基于物理噪声源产生随机数，如热噪声、量子现象等，能提供更高的随机性。对于采用伪随机数生成器（PRNG）的系统，需严格选取不可预测的种子值，并定期更新种子。

合理确定密钥长度与强度：对于金融、医疗等对数据保密性要求极高的领域，应优先采用高强度的加密算法和足够长度的密钥，如 256 位的 AES 密钥用于数据加密。同时，密切关注密码学技术的发展动态，及时更新加密算法和密钥长度标准。

3.2 密钥分发环节

保障传输安全：在密钥分发过程中，必须采用高强度的加密算法对密钥进行加密传输。例如，使用 SSL/TLS 协议对传输通道进行加密，确保密钥在网络传输过程中的保密性。同时，结合消息认证码（MAC）技术，为传输的密钥数据附加认证信息，接收方通过验证 MAC 来确保密钥的完整性。此外，引入密钥封装机制（KEM），将对称密钥用接收方的公钥进行加密封装后传输，进一步提高传输的安全性。在选择加密算法和密钥封装方式时，要遵循国家标准和行业最佳实践，并根据实际情况定期更新算法和参数。

完善身份认证机制：构建多层次、强身份认证体系，提升密钥分发的安全性。除传统的用户名 / 口令认证外，引入多因素认证方式，如基于硬件令牌的动态口令认证、生物特征识别（指纹、面部识别等）。在密钥分发过程中，实施严格的双向身份认证，发送方和接收方相互验证对方的身份。例如，采用数字证书进行身份验证，双方通过交换数字证书并验证证书的有效性和真实性，确保通信双方身份可靠。同时，建立身份认证审计机制，详细记录每次身份认证

过程，以便在出现问题时进行追溯和分析。

3.3 密钥存储环节

优化存储方式：采用加密存储是保障密钥安全存储的关键。使用专门的密钥管理系统（KMS），对密钥进行加密存储，并采用分层密钥架构，主密钥用于加密保护其他密钥。对于存储在数据库或文件系统中的密钥，采用对称加密算法进行加密，并将加密密钥妥善保管。同时，对存储密钥的设备和系统进行严格的访问控制，仅授权人员能够访问密钥存储位置。设置细粒度的访问权限，根据用户角色和业务需求分配不同的访问级别，防止密钥被越权访问。

加强存储介质管理：建立完善的存储介质管理制度，对存储密钥的 USB 密钥、智能卡等介质进行详细登记，包括介质编号、使用人、存储密钥类型等信息。设置专门的存储区域，对存储介质进行集中保管，采用保险柜、加密存储柜等物理防护措施，防止介质丢失或被盗。定期对存储介质进行检查和维护，监测其存储状态和使用寿命，及时更换老化或损坏的介质。当存储介质不再使用或达到使用寿命时，采用符合国家标准的销毁方法，如多次数据擦除、物理粉碎等，确保密钥信息无法恢复。

3.4 密钥使用环节

规范密钥使用：制定严格的密钥使用策略，明确规定每个密钥的使用范围、用途和权限。在系统设计阶段，将密钥使用权限与用户角色和业务功能紧密绑定，通过访问控制列表（ACL）等技术实现对密钥使用的精确控制。例如，只有具备特定权限的用户才能使用用于数据解密的密钥，且只能在授权的业务流程中使用。同时，定期对密钥使用策略进行审查和更新，确保其与业务需求和安全要求相匹配。加强对员工的培训，提高其对密钥使用合规性的认识，避免因误操作或违规行为导致密钥滥用。

建立审计与监控机制：搭建全面的密钥使用审计与监控系统，记录密钥使用的详细日志，包括使用时间、使用用户、操作类型、涉及数据等信息。通过审计日志，能够对密钥使用行为进行追溯和分析，及时发现异常操作。利用大数据分析和机器学习技术，对密钥使用模式进行建模和分析，实时监测密钥使用行为是否符合正常模式。例如，当出现异常的高频密钥使用或不符合权限的密钥操作时，系统立即发出警报，并采取相应的阻断措施。同时，定期对审计数据进行深度分析，总结潜在的安全风险和漏洞，为优化密钥管理策略提供依据。

3.5 密钥更新、销毁环节

及时进行密钥更新：建立密钥更新计划，根据标准以及业务系统的安全需求，设定合理的密钥更新周期。例如，对于高度敏感的数据加密密钥，每季度或半年进行一次更新。在密钥更新过程中，采用安全的密钥过渡机制，确保新旧密钥的平稳切换，不影响业务的正常运行。先使用新密钥对部分数据进行加密，并逐步扩大使用范围，同时保留旧密钥一段时间以处理历史加密数据。另外，将密钥更新纳入系统维护计划，定期检查密钥更新执行情况，对未按时更新的密钥进行预警和督促更新。

确保密钥彻底销毁：当密钥不再使用时，遵循严格的密钥销毁流程。对于存储在电子设备中的密钥，采用多次覆写的方式进行擦除，确保原有密钥数据无法恢复。例如，使用专门的擦除工具，按照国家标准规定的擦除次数和模式对存储密钥的区域进行多次覆写。对于存储在物理介质上的密钥，如智能卡、USB 密钥等，采用物理粉碎、消磁等方法进行销毁。在销毁过程中，进行详细记录，包括销毁时间、销毁方式、参与人员等信息，并由专人负责监督销毁过程，确保密钥被彻底销毁。

4 结论与展望

随着量子计算和人工智能（AI）技术的快速发展，密钥管理领域仍面临重大挑战。未来，信息系统密钥管理的优化不应仅局限于全生命周期的风险识别与规避，还需结合新兴技术趋势，探索更具前瞻性的安全增强方案。如制定面向 PQC 算法的密钥生命周期管理规范，确保后量子时代的密钥安全性，加快国产化量子随机数生成器（QRNG）的研发与应用，提升密钥生成的随机性与不可预测性；建立密钥操作行为的动态可信评估机制，结合 AI 技术实现异常行为的实时检测与响应；研究隐私计算环境下的多方密钥协商协议，确保分布式计算场景中的密钥安全交换等。我们在探索新技术的同时，仍需严格遵循密码应用基本要求，确保密钥全生命周期的安全管理。通过标准化、自动化手段，将合规要求融入量子安全、AI 增强密钥管理等前沿领域，构建更健壮的信息安全体系。

参考文献

[1] 裴斐.国密算法赋能的分布式加密存储系统及应用研究[J].网络安全和信息化,2025,(03):109-111.

[2] 任飞.基于国家数据共享交换平台的数据存储密码改造应用实践[J].信息安全与通信保密,2025,(02):56-64.

[3] 尹开贤.单位信息系统的安全防范与对策研究[J].网络安全和信息化,2025,(03):23-25.

[4] 任飞.基于国家数据共享交换平台的数据存储密码改造应用实践[J].信息安全与通信保密,2025,(02):56-64.