

选择加密密钥管理系统：需要考虑五个因素

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	5 factors to consider when choosing an encryption key management system		
原文作者	Shachar Roth	原文发布日期	2019 年 11 月 7 日
作者简介	Shachar Roth 是 Kindite 公司研发副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/11/07/encryption-key-management-system/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

选择加密密钥管理系统：需要考虑的五个因素

Shachar Roth

2019 年 11 月 7 日

2019 年是数据丢失最严重的年份之一，数据泄露规模创下历史新高。在数据安全战争中，加密被视为在整个数据生命周期内提供保护的黄金标准。但是，在选择和实施正确的加密解决方案上，企业面临着诸多挑战。实施强大加密的最大障碍之一是加密密钥管理。

如其保护的数据一样，加密密钥也具有生命周期，包括以下四个阶段：

- 创建
- 存储和保护（现有和过期密钥）
- 分配
- 替换和销毁

密钥是加密系统不可或缺的一部分，因此密钥管理对于确保加密系统的整体安全性至关重要。正是由于这一原因，美国国家标准技术研究院（NIST）在 2018 年末发布了一份报告，给出了有关加密密钥管理的建议。该报告根据多个领域的专家的意见编写。在下文中，我将参考该报告的一些观点，给出密钥管理的一些建议。

我认为，在选择密钥管理解决方案时应考虑以下五个因素。

1. 密钥存储

机密不可共享，而加密密钥是企业最宝贵的机密。因此，企业需要充分了解加密密钥的存储位置，以及可能访问它们的人员。例如，如果所讨论的解决方案要求加密密钥可用于云基础架构（处理加密数据时的常见要求），那么该方案就不安全。

2. 密钥轮换和销毁

诸如“支付卡行业数据安全标准”（PCI DSS）之类的标准要求定期进行密钥轮换。密钥轮换是指定期生成新密钥，并将其设置为主密钥。然后，使用该主密钥和新的加密逻辑来加密数据。

由于新的主密钥无法解密由旧密钥加密的数据，因此旧密钥也可用。这样就能够确保：使用新密钥对数据进行加密，同时又能够读取旧数据。但是，旧密钥不再用于加密。问题在于：当密钥轮换时，是否以及如何保留这些记录？

3. 密钥生成粒度

“零信任”密钥管理方法可确保将密钥保存在安全的环境中——该环境被认为是最安全的。理想情况下，密钥管理系统应实施细粒度的访问控制，这意味着在部门/角色/用户/设备范围内的最低级别上管理对该系统的访问。

另一个重要问题是，密钥管理系统是否允许在数据、用户或应用程序级别进行访问控制？用户或应用程序会引入需要解决的潜在漏洞，因此数据和设备级别将是首选。

4. 自动化

在密钥的生命周期中，很多事件可以自动执行，以防止发生错误。此外，手动密钥管理会占用大量时间。想象一下，为快节奏的企业级公司中的任何新招聘人员手动创建密钥会有多麻烦——因此，这基本上是不可能的。密钥管理系统应该采用自动化方法处理一些重复性的任务。但是，这些自动化方法应该足够灵活，以便在条件发生变化时易于修改。

5. 易于使用的界面

设计不佳的用户界面（UI）可能会对安全性产生严重的影响。配置事故或功能误用（例如密钥轮换设置）会加剧安全问题。即使密钥管理系统具有所有必需的功能，但如果表达不佳，可能也无法正确使用。

评估密钥管理系统的 SEC 规则

密钥管理是加密系统的重要部分，能够确保在整个数据生命周期中安全地实施加密。在企业寻找正确的密钥管理系统时，应遵循三个评估规则——SEC。

- S（安全性）。确保加密密钥不会泄露到企业外部。
- E（易于使用）。密钥管理系统应该具有直观的界面并提供高度的自动化，以减少管理成本。
- C（控制）。在数据级别，应针对每一台设备实现细粒度的访问管理。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>