简译版

2021 年六大加密趋势

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	Six cryptographic trends we' ll see next year		
原文作者	瑞安·史密斯（Ryan Smith）	**原文发布日期**	2020 年 12 月 7 日
作者简介	瑞安·史密斯是 Futurex 全球业务发展副总裁。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/12/07/cryptographic-trends-2021/		
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	• 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有方式，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。		

2021 年六大加密趋势

瑞安·史密斯

2020 年 12 月 7 日

2020 年是企业转型的一年，是企业适应和应对新挑战的一年。当我们与企业合作部署关键数据安全解决方案时，加密是一个常见的话题。那么在 2021 年，加密领域会有哪些趋势呢？

1. 云将发挥更重要的作用，尤其是在金融服务领域。

越来越多的企业将会进行云加密和密钥管理，而且这种趋势将会加速。企业会将更多的业务迁移到云端，特别是金融服务机构——他们正在将支付处理迁移到云端。

云提供商不断提供更强大、更灵活的安全解决方案，以满足企业“保留对密钥的控制并避免局限于一家供应商”的需求。云提供商一直在听取企业对数据安全实践的需求，并在数据访问、密钥管理和数据保留策略方面取得了长足的进步。

2. 同态加密将更加普遍

同态加密是指在处理和操作数据时保持数据的加密状态。同态加密可用于保护存储在云中或传输中的数据。这使企业能够在不损害数据完整性的情况下使用数据（例如对客户群进行分析）。

3. “自带加密”（BYOE）的使用将增加

如果企业在管理数据安全策略时能够确定所需的控制水平，那么 BYOE 就是其下一个发展方向。

举例来说，如果企业受到传唤，且其云提供商将相关文件上交给主管部门，会怎样呢？如果企业能够控制其密钥并可以在本地进行客户端加密，则主管部门即使拿到这些数据也毫无用处。这将是重大的里程碑事件——第三方将企业的信息上交给主管部门也无妨。

4. 加密+密钥管理，对管理更短的证书生命周期至关重要。

企业需要比以往更严格的加密和密钥管理策略。随着安全行业向一年期证书过渡，企业

需要管理更短的数字证书周期。因此，跟踪失效日期就非常重要了。在这方面，自动化将发挥重要的作用。

为了改善安全状况，企业可将密钥管理提高到与加密相同的级别。如果企业部署了良好的加密策略，但其密钥管理策略不佳，也无法实现良好的安全性。

5. 加密对 DevSecOps（尤其是代码签名）非常重要

DevOps 团队需要获取用于保护其基础架构（而不降低速度）的工具，这一点至关重要。企业应为 DevOps 团队提供密钥管理、硬件安全模块（HSM）、加密和第三方监控工具，帮助其集成安全功能，快速确定故障区域并进行故障排除。

这样做的目标是消除痛点，同时扩大企业内部加密的使用。在代码签名方面，HSM 扮演着至关重要的角色。代码签名证书、安全密钥生成和证书存储应实现集中化和自动化，并与“持续集成/持续交付”（CI/CD）系统本地集成。

6. 长期设备的制造商寻求加密敏捷性

2020 年，关于量子计算机会打破当前加密技术的讨论有很多。在 2021 年，那些使用寿命为 10 至 20 年的设备（卫星、汽车、武器、医疗设备等），其制造商将会寻求量子安全加密。敏捷加密解决方案可以采用混合证书：目前使用常规的非对称加密证书进行签名；但是要具有足够的灵活性，以便在需要时平稳过渡到量子安全加密，以应对量子计算威胁。

无论是迁移到云端并保留对密钥的控制、BYOE、同态加密，DevSecOps 采用加密技术，还是采用混合证书实现加密敏捷性，下述两点最为重要。

- 加密和密钥管理：两者缺一不可
- 更短的证书周期需要更严格的密钥管理策略

2021 年将是激动人心的一年！

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，目前，安天的威胁检测引擎为全球超过八十万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