零信任，还可以更简单些！

（2021 年 5 月 7 日）

“零信任”(Zero Trust)是目前网络安全界很火的名词，各大安全厂商都纷纷推出了相应的产品和解决方案，笔者在粗略了解这些方案后认为：零信任，采用 PKI (公钥基础设施)技术，可以更简单！现在的方案太复杂，实施成本太高，也不一定能完全解决信任难题。

先说一说什么是零信任？这个概念是最早于 2010 年由时任 Forrester 研究公司的首席分析师约翰·金德维格(John Kindervag)提出来的，所有人和物都是不可信的，需要对其访问任何资源的任何请求进行信任管理和安全控制。现在，随着保护企业业务系统和数据的压力越来越大，并且攻击变得越来越复杂，企业 CIO，CISO 和其他高管正在越来越多地认同零信任的概念并实施零信任安全解决方案，支持零信任的安全技术已逐渐成为主流。

零信任是一个安全概念，并没有固定的某项技术，其核心思想是组织不应自动信任其边界之内或之外的任何人和物，必须在授予访问权限之前验证试图连接到各种系统的所有人和物。零信任模型从根本上遏制了城堡和护城河的旧思想，因为云计算和移动办公等新技术得到了广泛应用，城堡和护城河保护方法已经行不通了。应该始终假设网络充满威胁，外部和内部威胁每时每刻都充斥着网络，不能仅仅依靠网络位置来建立信任关系，所有设备、用户和网络流量都应该被认证和授权才能访问各种系统。

如何实施零信任？笔者并不评论某个厂家的解决方案的优缺点，只是提出了同传统安全厂商不同的解决思路供广大用户参考，传统安全厂商还是侧重于防护，而笔者的思路是直接保护被防护的最终目的地—数据。笔者认为：PKI 技术是解决信任问题和保护数据安全的最有效和最高效的可靠技术。依据《密码法》对密码的定义— “密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。” ，采用密码技术实现对用户的安全认证和对信息进行加密保护，就能解决零信任想要解决的问题，同时也能满足用户的《密码法》合规需求。

所谓“零信任”，通俗点讲就是不信任任何人和物，传统安全厂商提出的解决方案就是想办法证明人和物是可信任的才允许访问。其实，密码技术能高效地解决信任问题，很简单，所有人和物都需要通过实名认证，并签发一张可信身份证书用于证明其可信身份。当这个人或物连接系统资源时，不采用不安全的用户名和口令方式认证，而是要求这个人和物出示其身份证书(用签名证书数字签名)，只有符合安全规则的身份才能通过验证，才可以访问相应的资源，

简单高效。当然，对于一些重要应用可以采用双向认证，系统资源也需提供其身份证书(如网站 SSL 证书)，访问人或物也要验证系统的身份，人或物才会同系统交换数据。

这种基于 PKI 技术的零信任解决方案类似于现实世界的实名乘机，通过实名认证乘机人和航空公司资质认定来确保飞机旅行安全。而目前市场上的零信任解决方案，需要复杂的动态持续信任评估和对访问权限的动态调整，这是由于非实名认证不知道谁是坏人，只能靠福尔摩斯式的不断甄别，效率太低且容易判断失误。

另一方面，零信任防护的最终目的还是机密数据的保护，黑客攻击的目的是获取机密数据，如果我们用数字证书来加密待保护的机密数据，由于黑客没有用于解密的数字证书而使得窃取的机密数据失去了价值，从而真正从根本上有效地保护了机密数据资源。

还是拿我们擅长的邮件安全来说吧，传统安全厂商的方案当然是防护邮件服务器不会被攻击，而基于 PKI 技术的邮件安全零信任解决方案，则是除了在邮件服务器上部署 SSL 证书来保护邮件链路安全外，还可以使用签名证书来实现强身份认证，替代不安全的用户名和口令认证。密信 App 根据不同的用户身份自动配置不同身份认证级别的签名证书，可满足用户业务系统对不同的身份级别要求，包括仅验证邮箱的身份、验证个人的身份、验证单位的身份和验证单位员工的身份，这样，身份认证系统只需设置简单的访问策略就能让不同身份的人通过认证而访问能访问的资源。

而对于邮件数据本身，用户可以使用密信 App 作为邮件客户端软件来收发电子邮件，实现全自动加密每一封电子邮件。这样，存放在云邮件服务器上的邮件数据都是密文，即使被非法获得，由于无法解密而使得拿到的邮件数据是一堆废纸，使得这些攻击失去了攻击的价值。也就是说：含有机密信息的邮件数据，由于是以密文方式保存在邮件服务器上的，使得此数据失

去了被窃取的价值，也就保护了机密数据的安全。

而针对机密文档安全，特别是政务云中的各种含有机密信息的政务文件，除了同邮件安全保护一样采用数字证书认证技术实现强身份认证外，还必须保护含有机密信息的文件本身。密信技术提供的我签文档服务，不仅让用户可以全自动数字签名各种文档来证明文档可信身份，而且用户在数字签名文档时还可以选择用有权阅读者的加密证书来加密此文档，这样，这些含有机密信息的文档以密文方式存放在业务系统中，即使被非法泄露出去，由于无法获得用户的加密证书而无法解密此文件，使得拿到的文档是一堆废纸，使得这些攻击失去了攻击的价值。也就是说：含有机密信息的文档，由于是以密文方式保存在业务管理系统中的，使得此文档失去了被窃取的价值，也就保护了机密文档的安全。

当然，采用 PKI 技术的零信任解决方案的核心是必须有相关的 PKI 系统，需要这些系统给人和物签发签名证书和加密证书。密信技术也正是建设了云密码基础设施，才能赋能邮件客户端和文档签名工具软件，实现全自动电子邮件加密和数字签名，实现全自动文档数字签名和加密。密信技术同时提供云密码服务，为没有建设 PKI 系统的用户提供所需的密码服务，助力用户实现强身份认证和实现机密数据的数字签名、加密和时间戳服务，以实现零信任安全。

基于 PKI 技术的零信任安全解决方案还可以用于物联网安全，如车联网，每辆车都有一张数字证书来证明其可信身份，车与车，车与人，车与物通信时用数字签名来证明自己的可信身份，用加密证书来加密所有通信，确保车与车，车与人，车与物之间的通信内容不会非法窃取和非法篡改，从而保护车联网通信安全。这样的话，车联网的安全防护就非常简单，通信接收方必须验证发送方的数字签名，再根据安全规则决定是接收还是拒绝这次通信。也就是说车只接收可信的通信，从而有效地抵御了各种攻击，而无需额外的复杂的安全防护模块。

最后总结一下，由于云计算、移动办公和万物互联的广泛应用，使得企业边界瓦解，内网和外网都是不安全的，零信任概念就是为了解决这个难题而应运而生。但是，让我们回到问题的源头，我们是要保护企业数据，采用零信任的最终目的还是为了保护机密数据，所以，我们可以采用 PKI 技术，建设云密码基础设施或使用云密码服务，实现人和物身份可信和数据加密，从而达到简化身份管理和增强数据保护的目的。所以说，零信任，采用 PKI 技术，可以更简单，实施成本更低，而实施效果更好！

----------END----------

想联系我讨论此话题？请使用 密信 App (-) 扫码发加密邮件给我，我一定会回复您的加密邮件。