因密而信

(2021 年 5 月 28 日)

“**因密而信**”是这次密信官网改版的主题口号，这是笔者从事 CA 证书业务和证书应用业务十七年的心得结晶。因为加密而信任，因为信任而安全，这也是网络安全的未来发展方向之一，大家也就不难理解为何零信任安全理念如此之火了。

网络安全产业界的一句流行语是“道高一尺，魔高一丈”，网络安全就是攻防双方不断在提高各自的能力而不断发展中，这似乎是一个永无止境的过程。但是，这个过程真的解决了安全问题了？答案是没有，各种网络安全事件时时刻刻都在不断的发生。

那么，这个怪圈是否有解呢？有!时任 Forrester 研究公司的首席分析师约翰·金德维格(John Kindervag)于 2010 年提出“零信任”这个概念的，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。笔者认为：这就是答案，零信任能解决目前的困局，无需再不断的斗法了，只需“零信任”就能解决安全问题。这也就不难理解 IDC 最近提出了“由安全市场转向信任市场成为趋势”的观点。

而如何解决信任问题，目前市场上就有各种各样的解决方案，最典型的方式是“福尔摩斯”方案，需要动态的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。而密信技术提出的零信任安全解决方案是采用 PKI 技术实现身份认证和数据加密，通过数字签名、加密和时间戳技术来实现信任，因为 PKI 技术就是为了解决信任问题而生，为了解决数据安全问题而生。

也就是说，为了安全，得先解决信任问题，而加密和数字签名就能解决信任问题，而解决了信任问题，也就解决了安全问题。这就是“因密而信”的内涵，这也就不难理解为何 4 月 20 日在北京举行的“**2021 密码大兴峰会**”提出的主题是“**因密而安**”，**因**为加**密**而信任，因为信任**而安**全。

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