让密码为零信任再添一把火

零信任非常火，零信技术的成立就是要让密码为零信任再添一把火，让零信任更火！

目前市场上的零信任安全参与者基本上都是各大安全厂商和互联网巨头，其解决方案也都是基于各自专业和专长的零信任安全解决方案，笔者总结这些解决方案是“福尔摩斯式”安全威胁分析甄别模式，这种模式仍然是基于传统安全防护的理念而设计，仍然无法逃出“道高一尺魔高一丈”的不断博弈的魔圈。

笔者从事 CA 运营和密码技术应用 17 年，一直从事的业务就是信任服务，欧洲称 CA 机构为信任服务提供商(TSP)。所以，我们坚信：要解决信任问题，当然离不开数字证书、离不开 PKI(公钥基础设施)和离不开密码技术！零信任理念的提出就是为了解决网络信任问题，当然也就不能缺席 PKI 和密码技术！因为 PKI 和密码技术就是为了解决网络信任问题而生，为了解决数据安全而生。所以，零信技术的诞生就是在百花齐放的零信任安全解决方案中再添一朵不一样的！零信技术，一个基于密码技术的创新零信任安全提供商。

美国国家标准研究院于 2020 年 8 月发布的 SP 800-207《Zero Trust Architecture (零信任构架)》中描述的零信任核心逻辑部件之一就是 PKI，只是并没有展开具体的 PKI 应用描述。而美国管理和预算办公室(OMB)于 2021 年 9 月 7 日发布的《美国联邦政府零信任战略》征求意见稿，详细地列出了美国联邦政府机构必须逐步转向基于零信任原则的安全架构的各项指标要求，包括对身份、设备、网络、应用、数据等五个方面的安全防护要求，其中有多项安全防护措施都是 PKI 和密码技术的核心应用，如 https 加密、邮件加密和 DNS 加密。

我国颁布的《密码法》则是明确要求关键信息基础设施必须采用商用密码进行保护，也就是说必须采用密码技术来实现安全认证和对信息进行加密保护。这实际上就是零信任！不信任没有采用密码技术保护的个体身份和各种信息。也就是说，零信任离不开密码技术，密码技术是零信任安全的底座和基石！

公司商号和商标

中文“**零信**”就是零信任的缩写，英文“**ZoTrus**”就是 Zero Trust 的缩写。核心标识就是“0”加“√”组合，意是基于零信任原则的网络信任与网络安全解决方案。

零信技术基于三大理念和五大原则为用户提供零信任安全产品和服务。

三大理念：永不信任、始终验签、始终加密。

五大原则：

原则一：不信任明文 http 网站，只信任 https 加密和已认证的网站。

原则二：不信任明文电子邮件，只信任已加密的电子邮件。

原则三：不信任无数字签名的软件代码，只信任有数字签名的软件代码。

原则四：不信任无数字签名的电子文档，只信任有数字签名的电子文档。

原则五：不信任未认证的身份和设备，只信任已认证的身份和设备。

零信任是一种生活智慧，保日常生活平安！零信技术是一种安全实践，保万物互联安全！零信技术，让密码为零信任再添一把火，让零信任旅程更轻松和更高效！

王高华

创始人、CEO&CTO

2021 年 12 月 20 日于深圳
2022 年 1 月 21 日更新

请关注公司公众号，实时推送公司 CEO 精彩博文。