数字化转型，密码，零信任

本文标题的三个名词都是目前最热门的词汇，笔者今天就讲讲它们之间的关系。可能有些读者看到题目会理解为“数字化转型的密码(秘诀)是零信任”，这个理解只对了一半，零信任的确是保障数字化转型成功的秘诀之一。但是，本文所指的“密码”是《密码法》定义的“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，是指密码技术、密码产品和密码服务，不是银行卡“密码”，也不是“秘诀”。标题的是意思是数字化转型需要密码技术和零信任的双重保障，才能确保转型成功，才能保障转型后的正常运转，没有安全保障的数字化转型随时会崩塌。

大家都知道，我国乃至全球无论是国家层面还是企业层面都在推动数字化转型，数字化转型改变了业务的完成方式，甚至创造了全新的业务类型，采用云计算和大数据等数字技术以实现提高效率、价值的总体目标，以为客户创造价值为目的。这个转型，不仅仅是数据上云，业务上云，员工和设备都不再局限于办公室和办公局域网，与用户的沟通方式也不再是电话和当面拜访，而是充分利用社交媒体、电子邮件和视频会议等实现数字化沟通，为客户提供更好的体验和创造新的价值。

由此可见，传统的基于护城河和堡垒的安全防护方案在数字化转型中已经不管用了，因为云服务不是你的，你的数据也不在你自己的服务器上，你的员工也不一定在你的办公室办公，这些改变如果网络安全保障措施没有跟上，则随时有可能从数字化转型时代瞬间打回到纸质办公时代，甚至打回原始时代而无法正常办公，因为纸质文件都没有了。怎么办？

零信技术给出的答案是零信任加密码技术，数字化转型需要零信任和密码技术的双重保障。零信技术基于密码技术和零信任原则为保障数字化转型提供五大云服务，第一个云服务是网站安全云服务，因为 Web 应用是数字化转型的基础和底座，必须首先夯实基础和筑牢底座。零信网站安全云服务是一个集 https 加密、云 WAF 防护和网站可信认证于一体的全方位 Web 应用安全解决方案，能有力保障各种 Web 应用的机密信息加密传输安全、防攻击安全和防身份假冒安全。用户无需向 CA 申请 SSL 证书，只需做两次 CNAME 域名解析，10 分钟开启网站 https 加密和云 WAF 防护，高效保障 Web 业务系统安全。

电子邮件是互联网的第二大流量，也是数字化转型的重要通信工具之一，但是由于电子邮件服务都已经迁移到云上，电子邮件已经不在你自己的邮件服务器中。保护含有大量个人机密信息和商业秘密的电子邮件的安全，必须采用零信任原则，不信任电子邮件明文存放在云里是安全的，必须加密每一封电子邮件，确保每一封电子邮件是密文存放在云里。第二个云服务就是邮件安全云服务，这是一个实现端到端加密的电子邮件全生命周期安全解决方案，一个集邮件加密、数字签名和数字邮戳于一体的电子邮件安全解决方案，能有效杜绝邮件欺诈、邮件泄密和邮件身份假冒等各种邮件安全问题，从而保障数字业务通信安全。

现在，大量的业务文档也已经上云管理，如何保障大量机密文档的安全，也必须采用零信任原则，不信任电子文档明文存放在云里是安全的，必须加密每一个文档，确保每一份文档是密文存放在云里。第三个云服务是文档安全云服务，这是一个采用数字签名和加密来保障文档安全的解决方案，也是一个依据零信任原则的云签名解决方案，不上传用户的待签名文档，仅需提交待签名文档的摘要到零信云签名服务系统，能有效保护文档机密信息安全。而文档加密则采用数字证书在用户电脑加密，能有效保证机密文档不会被泄密，实现仅有权阅读者才可以无缝解密已加密文档。电子文档的数字签名、加密和时间戳能有效保障各种电子文档的安全可信。

第四个云服务是应用安全云服务，这也是一个采用数字签名来证明应用软件可信的唯一可靠技术手段，实现各种应用软件的始终验证签名来确保应用软件来源可信，从而保障软件运行的安全。同时，对于需要下载更新软件的物联网设备，必须采用可信的 https 加密通道下载更新包，并验证更新包的数字签名和时间戳签名，只安装有可信数字签名和时间戳签名的软件更新包，有效并且高效保障物联网设备的远程升级安全，杜绝各种通过软件升级实现的攻击和勒索事件发生。

第五个云服务是身份可信云服务，这是一个基于零信任原则的身份认证和身份验证服务，每个个体都有一个可信的数字身份证书，个体访问任何资源都必须通过数字签名验签来实现始终验证身份。而个体通过认证后访问的数字资源所在的网站的身份，则由 SSL 证书来证明并

由浏览器或 APP 来验证其可信身份。今天上线的网站可信认证服务就是身份可信云服务的主要产品之一，实现互联网第一大流量的网站的身份可信。

最后值得一提是零信浏览器，作为零信技术的首发产品，它不仅仅是一个浏览器，不仅仅是一个免费的国密浏览器，也不仅仅能显著展示网站可信身份、WAF 防护和国密 https 加密，更重要的，它是一个对“仅云”零信任的客户端软件，用户需要一个能本地存储和管理机密信息包括加密密钥等重要数据的客户端软件，不能把全部数据都交给云，必须是“端云一体”，这样才能既充分发挥“云”的算力优势而实现全自动加密和数字签名，又能让重要数据“端”在用户自己手中，彻底解决“仅云”无法实现的数据安全和保护隐私难题，端云一体共同保障数字化转型安全。

总之，数字化转型是必须的，但没有安全保障的数字化转型是灾难的根源，具有随时可能打回远古时代的风险。所以，必须高度重视数字化转型的安全保障措施建设。而最有效的安全保障是对个体身份的零信任、网站身份的零信任、对 Web 流量的零信任、对 Web 连接的零信任、对明文电子邮件的零信任、对无身份文档的零信任和对无身份应用软件的零信任，这些零信任安全解决方案都必须采用密码技术来实现，采用数字证书实现数字签名、加密和时间戳服务，只有这样才能有效和高效地保障各种业务系统的安全，从而保障数字化转型成功并持续可靠运行。

王高华

2022 年 6 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。