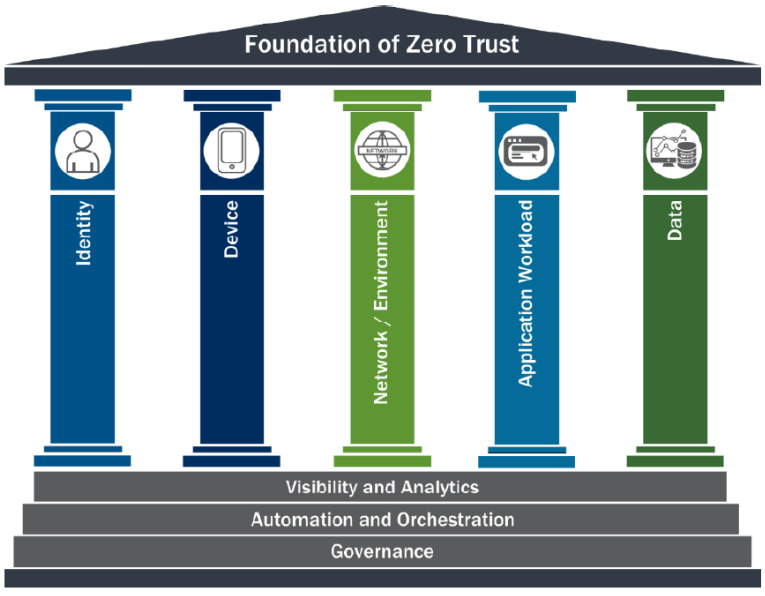
深度解读美国《联邦零信任战略》（一）

自从零信官网 6 月份正式上线零信浏览器和零信网站安全云服务就受到了有些用户和与零信任安全相关的友商的质疑，认为我司提供的服务与零信任安全无关。笔者认为：这几年零信任的确很火，但是都是传统的安全厂商在热炒，并且都是在基于自己的传统安全产品“炒剩饭”，不但没有任何新意，而且误导了市场和用户。笔者认为有必要再多写几篇文章多多宣传什么是真正的零信任，虽然笔者已经写了多篇，包括《零信任安全的四大误区》、《用户需要什么样的零信任》和《实施零信任安全，该从何入手》。

本文将深度解读美国管理和预算办公室 (OMB) 于 2022 年 1 月 26 发布的《联邦零信任战略》(Federal Zero Trust Strategy)，该战略提出了零信任安全五大目标和行动计划，解读这些行动计划就能帮助读者理解什么是真正的零信任。同时，笔者也希望能借本文为我国电子政务系统走向零信任安全原则和安全架构献计献策，古话说得好“他山之石，可以攻玉”，当然不是全盘照搬照抄，而是结合我国的实际情况提出适合我国国情的零信任安全之路。

美国管理和预算办公室(OMB)的职能是为美国总统服务、监督其愿景在整个政府行政部门的实施。其使命是协助总统实现政策、预算、管理和监管目标。之所以发布《联邦零信任战略》，是需要支持美国总统签署的第 14028 号行政命令“改善国家网络安全”，以推动并落实美国联邦政府机构的网络安全架构向零信任原则迈进。“Zero Trust”(零信任)这个词在这个总统令中被提到了 11 次，这是很少见的，只能说明美国政府很重视零信任。所以，管理和预算办公室出台了联邦零信任战略实施指导文件。



联邦零信任战略的目标是加速各个联邦机构尽快向零信任成熟度的安全基线迈进，并要求在 2024 财年末实现这些战略目标。零信任成熟度模型的安全基线是美国网络安全和基础设施安全局(**CISA**)开发的，以协助联邦机构实施零信任架构，旨在为联邦机构提供零信任路线图和资源，以实现最佳的零信任环境。美国网络安全和基础设施安全局的零信任模型描述了五个互补的工作领域(支柱)(身份、设备、网络、应用、数据)，其中三个主题跨越了这些领域（可见性和分析、自动化和编排、治理）。

联邦零信任战略指出：零信任架构的一个关键原则是没有网络被隐含地认为是可信的，这一原则可能与一些联邦政府机构当前保护网络和相关系统的方法不一致。所有流量必须尽可能都加密和认证，包括内部流量，所有数据在传输过程中都必须加密。该战略要求联邦政府机构重点放在被广泛使用的两个关键协议上，即 DNS 和 HTTP 流量的加密，同时还将评估电子邮件加密解决方案。

联邦零信任战略目标分别从身份、设备、网络、应用、数据等五个方面提出了具体行动计划和要求，本文重点解读对网络部分的要求，其他几个方面的要求将在后续博文继续深度解读。

网络部分的愿景是：各联邦机构对其网络环境中的所有 DNS 请求和 HTTP 流量进行加密，并开始执行实施计划，将其边界分解为孤立的环境。

网络部分的行动计划有 4 个：

只要技术条件允许，联邦政府机构都必须使用加密 DNS 解析 DNS 查询。网络安全和基础设施安全局的保护 DNS 计划支持加密 DNS 请求。

联邦政府机构都必须对其网络环境中的所有 Web 网站和 API 调用流量强制实施 HTTPS 加密。必须与网络安全和基础设施安全局合作，将其.gov 域名“预加载”到浏览器中实现浏览器只能通过 HTTPS 访问联邦政府网站。

网络安全和基础设施安全局将与联邦风险和授权管理计划项目管理办公室合作，评估联邦政府范围内可行的电子邮件加密解决方案，并向管理和预算办公室提出建议。

联邦机构必须与网络安全和基础设施安全局协商，制定一个零信任架构计划，说明如何实施网络环境的隔离，并将其作为零信任实施计划的一部分提交给管理和预算办公室。

以上内容根据原文翻译整理，原汁原味，相信这是其他零信任安全提供商不会提的最重要的内容。不知道读者注意到没有，这个战略的摘要部分把流量加密放在的非常重要的位置，所用词语是“关键原则(key tenet)”、“重点(focus)”、“关键(critical)”。请注意：在零信任战略的摘要部分把身份认证和访问控制与流量传输加密放在数一数二的位置，因为用户的身份流量如果不加密的话就失去了“始终验证”的意义！不能谈起零信任就只剩下身份认证了！这一点请读者朋友参阅《零信任安全的四大误区》，笔者就不在本文重复此类内容了。

下面，笔者就结合自己的密码专业知识特长，重点解读并总结如下四点。

第一：所有联邦政府网站必须强制实施 https 加密，这是零信任的重点和关键原则。

要求所有联邦政府网站都必须强制实施 https 加密，这是对 http 网站明文传输的零信任，这是零信任架构的首要原则，必须加密所有 Web 流量。而且要求必须采用 HSTS 技术实现浏览器只能用 https 加密访问，这是不信任 http 网站会自动跳转到 https 加密，由浏览器来强制执行 https 加密连接，这也是对政府机构是否能严格执行强制 https 加密的零信任。这两点都非常值得我国政府网站学习和借鉴。

据 CNNIC 统计数据，截至 2021 年 12 月，我国共有政府网站 14566 个，而从谷歌证书透明系统查到的.gov.cn 域名只申请了 4251 张 SSL 证书，不排除重复域名申请的情况下的证书申请率也仅为 29%，说明大部分政府网站还没有部署 SSL 证书实现 https 加密，其中 31 个省级政府网站中只有 19 个省实现了 https 加密，但有些网站即使部署了 SSL 证书并没有强制自动跳转到 https 加密。

第二：我国政府网站必须强制实施国密 https 加密，这是我国的零信任战略的重点和关键原则，也是《密码法》的合规要求。

对于我国的政府网站来讲，即使部署了 RSA 算法 SSL 证书实现了 https 加密还是不够的。不知道读者是否了解俄乌冲突发生后国际 CA 机构纷纷吊销已经签发给俄罗斯政府网站和银行网站的 SSL 证书，短短几天就吊销了三千多张，导致大量的政府网站和银行网站无法正常访问。在当前非常不确定的国际环境下，我国应该如何避免此类网站安全事件发生呢？答案只有一个，那就是：我国政府网站和银行网站必须尽快全部强制部署国密 SSL 证书，这是对 RSA 算法 SSL 证书的零信任，也是《密码法》的合规要求，因为《密码法》明确要求关键信息基础设施必须采用商用密码来实现加密保护。

而为了用户体验，网站不能强制要求用户使用何种浏览器，所以暂时必须部署双算法(SM2/RSA)双 SSL 证书实现自适应 https 加密，以保证不支持国密算法的浏览器和移动 App 也能正常访问网站。但我国必须大力推广和普及使用支持国密算法和国密 SSL 证书的国密浏览器，大力推广和强制要求常用的移动 App 支持国密 https 加密。只有这样，才能避免遭遇俄罗斯一样的网站 SSL 证书被吊销和被断供的严重安全事件，一旦用户已经习惯使用国密浏览器上网和常用移动 App 支持国密算法，即使 RSA 算法 SSL 证书被吊销，由于实际上 RSA SSL

证书并没有起作用，所以证书被吊销并不会影响用户正常上网！

笔者很高兴地看到已经有多个政府网站部署了国密 SSL 证书实现了国密 https 加密，中国银行个人网银系统也部署了国密 SSL 证书实现了国密 https 加密网银交易数据，并且这些网站部署的都是双 SSL 证书，实现了自适应加密算法的 https 加密。而一旦 RSA SSL 证书被吊销，则未使用国密浏览器的用户只需改用国密浏览器即可，丝毫不影响网站的正常加密运行。前车之鉴，未雨绸缪，希望我国政府网站和银行网站能加快国密 SSL 证书部署步伐，以切实保障我国电子政务系统和网银系统安全。

第三：必须高度重视 DNS 加密，这是对明文 DNS 的零信任。

联邦零信任战略要求联邦政府机构都必须使用加密 DNS 解析 DNS 查询，这一点也非常值得我国学习。从相关搜索结果来看，DNS 加密并没有得到重视，首先是提供上网服务的运营商并没有实现默认采用加密 DNS 上网，政府机构也没有这方面的强制要求，这一点值得我国相关部门高度重视。

要求采用加密 DNS 是对明文 DNS 的零信任，以保护上网关键数据的安全，有效防止 DNS 欺骗攻击。而实现 DNS 加密的两个主流技术 DNS over TLS 和 DNS over HTTPS 也都离不开 SSL 证书，期待我国的 DNS 加密能早日采用国密 SSL 证书来实现并普及应用。

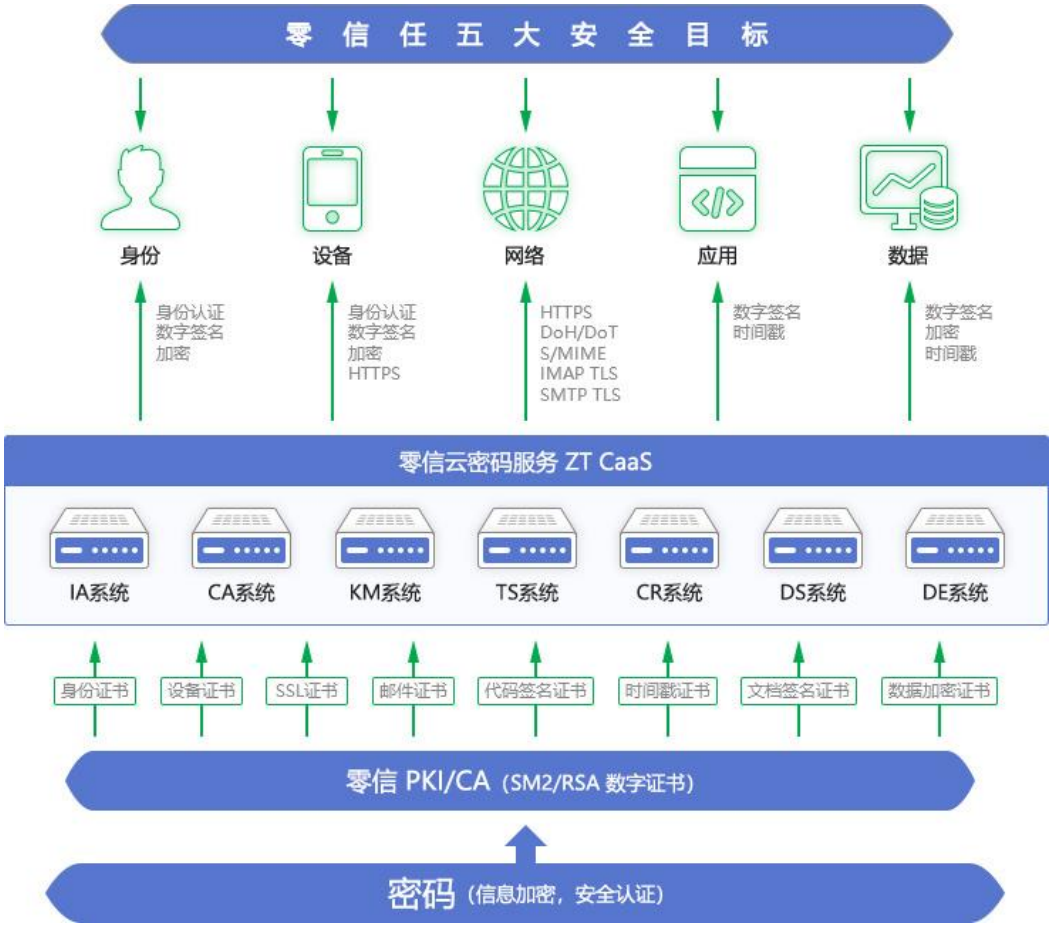
第四：必须重视电子邮件加密，这是对明文电子邮件的零信任。

对于电子邮件加密，虽然目前联邦零信任战略并没有给出解决方案，但是已经开始评估各种邮件加密方案。相比国外的普及电子邮件办公的情况，我国并没有普及使用电子政务邮件。但值得注意的是，有些省市的电子政务邮件系统并未部署 SSL 证书，这也是非常不安全的，必须尽快部署以保障 Web 登录账号安全和邮件传输安全。当然，推荐部署国密 SSL 证书。笔者将会单独写一篇博文来详细讲一讲邮件加密的话题，我公司正在研发邮件安全云服务，一个创新解决邮件加密难题的云服务。

以上就是笔者对美国联邦零信任战略中的身份、设备、网络、应用、数据等五个方面的网络部分的重点解读，为何先解读这一部分，因为这部分的内容已经在我国被严重忽视，大多数零信任安全厂商可能由于不熟悉这个领域而没有重点关注和没有重点宣传这一部分内容。笔者理解为何美国联邦零信任战略把 Web 流量的加密放在如此重要的位置的原因是：只有 Web 数

据安全了，用户的身份认证才有意义，否则 Web 数据和用户数据都不会安全，也就失去了用户身份“始终验证”的意义。理解到这一点对于正确理解零信任至关重要！

最后总结一下，零信任的五大安全目标是：网络中的个体身份可信、网络中的设备可信、网络中的流量加密、网络中的应用可信和网络中的数据加密，这五大目标都可以通过数字证书的数字签名和加密来实现，其核心基础技术是密码和 PKI/CA 技术。



零信技术的使命是“为保护身份、设备、网络、应用、数据的安全提供各种创新的密码产品和服务”，这是一个 100%的符合零信任战略的零信任安全产品路线，零信技术采用密码技术和零信任原则为用户提供身份可信云服务、网站安全云服务、邮件安全云服务、应用安全云服务和文档安全云服务。零信技术是一个不折不扣的基于密码技术的零信任安全提供商。

王高华

2022 年 9 月 9 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。