东数西算，安全是本

笔者在 2 月 17 日看到“东数西算”工程正式全面启动的新闻时，很是兴奋，这是一个提升国家算力和未来核心竞争力的大战略，大手笔，因为算力已经同水电气一样属于关键基础设施，有“南水北调“的异曲同工之妙。当时就想写点什么，但是一直没有下笔，是因为这个战略太重要了，还是先看看大家怎么说吧。刚刚看到搜狐号推出了一个投稿活动-《“东数西算“新赛道开辟》，明天截稿，这触动了笔者还是决定在搜狐号写一篇，当然还是老本行，说一说“东数西算”中的数据安全，希望能起到抛砖引玉的作用。

“东数西算”战略是指在京津冀、长三角、粤港澳大湾区、成渝、内蒙古、贵州、甘肃、宁夏等 8 地启动建设国家算力枢纽节点，并规划了 10 个国家数据中心集群。至此，全国一体化大数据中心体系完成总体布局设计，“东数西算”工程正式全面启动。“东数西算”中的“数”，指的是数据，“算”指的是算力，即对数据的处理能力。“东数西算”是通过构建数据中心、云计算、大数据一体化的新型算力网络体系，将东部算力需求有序引导到西部，优化数据中心建设布局，促进东西部协同联动。

笔者在查阅有关文件时注意到，国家发展改革委会同有关部门于去年 5 月 24 日就制定了《全国一体化大数据中心协同创新体系算力枢纽实施方案》，其中的 4 个基本原则之一是“安全可靠”：加强对基础网络、数据中心、云平台、数据和应用的一体化安全保障，提高

大数据安全可靠水平。加强对个人隐私等敏感信息的保护，确保基础设施和数据的安全。而其中的国家算力枢纽节点的 9 大重点任务之一是“确保网络数据安全”：完善海量数据汇聚融合的风险识别与防护技术、数据脱敏技术、数据安全合规性评估认证、数据加密保护机制及相关技术监测手段，同步规划、同步建设、同步使用安全技术措施，保障业务稳定和数据安全。加快推进全国互联网数据中心、云平台等数据安全技术监测手段建设，提升敏感数据泄露监测、数据异常流动分析等技术保障能力。

笔者认为这个实施方案中关于数据安全这一块还是讲得非常清楚的，要求也是非常明确的，也指明了一些关键的技术方向。笔者在本文结合本人的专业所长，就如何实现“确保网络数据安全”提出一些具体的技术解决方案，供有关部门和有关单位及业界同仁参考。

先说一件最近发生的与数据安全相关的大事，那就是美国联邦政府于 1 月 26 日发布了《联邦政府零信任战略》，要求各联邦政府机构调整其网络安全架构为基于零信任原则。这同我国 2 月 17 日发布的“东数西算”工程有什么关联吗？当然有，两个都是国家级战略，其中有些保护数据安全的技术措施值得我国的“东数西算”工程借鉴，具体来讲就是零信任原则加密码技术，这也是我国《密码法》对关键信息基础设施必须采用商用密码进行保护的强制要求，因为“东数西算”工程就是关键信息基础设施。

笔者认为：要保障“东数西算”工程的数据安全，必须采用零信任原则和密码技术来保障数据的全生命周期安全，遵循如下两个原则：

第一：坚持零信任原则。数据是“东”的，“西”就只能是完成“算”的工作，这就是零信任，只有这样，“东”的数据才愿意转移到“西”去算。同时，要对整个工程涉及到的各种身份零信任，包括服务器身份、数据生产者身份、数据使用者身份、相关设备身份和相关应用软件的身份等等。零信任是解决跨区域跨部门大型网络安全的最佳解决方案。

第二：必须采用密码来保护数据安全，包括数据的加密保护和安全认证，这也是《密码法》的合规要求。用密码技术、密码产品和密码服务来实现零信任，是最佳的零信任安全实践。

基于以上两个基本原则，笔者强烈推荐采用如下八个方面的基于密码技术的零信任安全保障措施，实现数据加密和安全认证。

1. 数据传输加密

各个数据中心的服务器之间的通信和数据交换必须采用加密链路实现加密传输，对明文传输零信任。如果是 http 协议实现数据交换，则必须是 https 加密方式实现。所有 Web 应用都必须是强制 https 加密访问，只有这样才能保障用户访问数据的安全。为了保障用户使用各

种浏览器都能无缝实现 https 加密，服务器必须部署双算法 SSL 证书(RSA/ECC 算法和 SM2 算法)，条件成熟后最终将统一到国密 SM2 算法实现 https 加密。

2. 数据存档安全

考虑到从“东”到“西”的网络延时，有些对实时要求比较高的计算，当然还是要就地完成，这也就是为何 8 个算力枢纽节点中有 3 个是在“东”的。而对于一些存档的数据，如日志数据、每日办事结果数据、历史交易数据等等，当然应该送到“西”存储，但这个存储也一定要采用零信任原则，存档数据必须有数字签名证明数据拥有者的身份，用时间戳签名来证明数据存档时间，保密数据还需要用有权使用者的数字证书加密。这是保障存档数据安全的唯一可靠技术措施。

3. 邮件数据安全

电子邮件是互联网上第二大数据源，海量的电子政务邮件、企业邮件和个人邮件都是含有机密信息的数据，必须实现电子邮件数据的全加密，从电子邮件发出就加密，实现电子邮件在途和在云的全程全生命周期的安全。当然，对于电子政务邮件依据《密码法》要求也必须采用国密算法加密。

4. 文档数据安全

电子文档也是一个重要的数据源，无论是政务文档、企业文档或个人文档，只要是云上存储都必须有可信数字签名来证明文档的可信身份，重要文档都必须用证书加密，用有权使用此文档的用户证书加密。当然也是要求用国密证书实现文档数字签名和加密，在现阶段也可以采用双证书双算法实现双数字签名，以兼容常用文档阅读器和所有操作系统。

5. 服务器身份可信

各地数据中心中的所有服务器都必须采用可信的 SSL 证书来证明其可信身份，服务器之间的通信必须先验证身份才能通信，对无法提供可信身份的服务器零信任。只有这样才能保证数据中心中的千万台服务器的安全，这个服务器身份验证方式也是微软云采用的方式，值得借鉴。当然，关键服务器的身份必须用国密 SSL 证书来证明其可信身份，这个应用由于不涉及到浏览器支持和信任问题，完全可以全部和全面采用国密算法和国密 SSL 证书实现。

6. 设备身份可信

整个工程中所有连接的其他设备，除了服务器可以用 SSL 证书来证明其可信身份外，其他所有设备都应该有可信数字身份证书，每次访问数据资源必须实时验证其可信数字身份才能访问，没有默认始终信任的身份，必须坚持始终验证。这个应用也完全可以全部和全面采用国密算法和国密身份证书实现。

7. 应用软件可信

所有在整个项目中运行的软件都必须有可信的数字签名和时间戳签名，所有算力节点和各数据中心都必须验证每次启动运行的软件的数字签名，只有具有可信数字签名的软件才允许运行，这是对应用软件来源的零信任，只有这样才能防止和杜绝恶意软件攻击，确保算力节点和数据中心的可靠运行。而依据《密码法》的要求，这个可信的数字签名必须是采用国密 SM2 算法实现代码签名。个别需要全球信任的应用场景可以采用双算法双证书实现数字签名，以满足全球信任和国密合规的应用需求。

8. 数据时间可信

每个数据在生成时就必须同时生成时间戳签名数据，用以证明数据时间可信和将来的数字生成时间溯源，否则无法证明数据的生成时间可信，不能仅仅只是数据库的时间字段，必须是时间戳字段。而数据的使用时间也必须有时间戳签名数据，用以证明使用数据的时间可信和可追溯。当然，这个时间戳签名也必须是采用国密算法实现，以满足国密合规要求。

总之，“东数西算”工程是一个利国利民的大工程，必须在启动建设和运行维护中始终依据《网络安全法》、《密码法》、《电子签名法》、《数据安全法》和《个人信息保护法》等相关法律法规，采用零信任原则和密码技术来保障数据的全生命周期安全，只有这样采用真正保障“东数西算”工程的顺利实施和可靠运行，保障政府和企业的数字化转型成功，让“东数西算”工程更安全地造福老百姓。

王高华

2022 年 3 月 7 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。