政务数据资源集中管理的零信任

现在，各省市政府都建立了大数据局，要求各个局委办的数据都集中到政务大数据中心来统一集中管理，这是为了能更好地实现政务数据的资源共享，让老百姓办事更通畅和更方便，不再需要为了一件事跑遍所有局委办，政务服务“一网通办“收到了其用户(市民和企业)的欢迎。但是，如何让各个局委办放心地把自己的数据集中到政务大数据中心统一管理？或者说，政务大数据中心应该如何管理这些数据才能让各局委办放心？笔者作为一个曾任深圳市信息网络中心总工程师的过来人，结合多年来在密码领域的潜心钻研和探索，在本文给出了对上述两个问题的思考。

让我们先思考一下为何美国联邦政府高度重视零信任安全，为何在“改善国家网络安全“美国总统令中 11 次提到“零信任”，为何美国制定了“联邦零信任战略”、发布了“零信任成熟度模型”和“零信任架构”等一系列关于零信任的标准和指导文件。这是因为政务数据上云后的网络环境和数据的使用场景发生了巨大的变化，我国的政务数据统一上政务云实现统一管理也是一样的应用场景，也必须采用零信任架构来保障政务数据安全。

也就是说，各个局委办把数据统一交到政务大数据中心也是要基于零信任的安全理念，我不放心很正常，但是你得拿出办法出来让我放心，让我放心地把数据交出来共享。笔者参考美国“联邦零信任战略”的实施目标要求，结合我国《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要求，给出了五个实施建议，供各地政务大数据中心参考。

第一：身份认证和身份管理

谁能使用某个数据需要依据零信任原则实现实时身份认证，没有隐式信任。如何可靠地实现身份认证，当然是采用数字证书实现强身份认证(推荐 USB Key 证书)，每个数据的访问者必须出具其可信数字身份，通过数字签名来验证可信身份。而不能是不安全的用户名和口令方式认证，因为这种方式无法切实保证是正确的人来访问数据资源。

第二：设备管理

不仅要求每个局委办的办公电脑都有可信数字身份(身份证书)，而且政务大数据中心的所有服务器都必须有 SSL 证书来证明其可信身份，服务器与服务器之间的连接都必须出具其 SSL 证书来证明其身份，只有这样，才能使得各局委办用户无需考虑服务器的物理位置在哪，可信地实现对数据资源服务器的逻辑可控。通过设备证书来实现设备的可信管理，是零信任安全的必配基础要求。

第三：网络流量安全

如果各种政务业务管理系统不部署 SSL 证书，则整个政务业务系统的流量都是明文流量，由于政务数据中心一般不会同各局委办在同一栋大楼内，从局委办办公室到政务数据中心之间的数据传输就是不安全的(即使是内网)，因为明文传输数据非常容易被抓包软件非法窃取和非常容易被非法篡改。按照零信任原则，不相信内网或内部专线是安全的，必须加密所有 http 流量，只有这样才能保障数据的安全传输。同时，政务邮件流量也是必须实现端到端加密，DNS 流量也必须实现每一层级都加密。

第四：应用安全

不仅需要持续不断的对各种应用进行安全评估，最重要的是所有应用软件都必须有数字签名，所有政务服务设备的远程升级软件都必须有可信数字签名，政务办公电脑只安装有可信数字签名的软件，只有这样才能保证是可信的应用软件访问政务系统。

第五：数据安全

这是重中之重，数据放到了政务大数据中心，按照零信任原则，为了防止数据被滥用，必须把重要数据加密存放，用有权使用此数据的单位或个人的证书来加密此数据，则只有该单位或个人才能解密此数据，这与数据放在哪里就没有关系了，真正实现零信任数据安全。

各种政务数据不仅仅要加密，而且还需要数字签名加时间戳签名，数字签名证明数据属于

谁，时间戳签名证明数据是何时提交到政务数据中心的。而对于数据使用，数据使用者不仅要通过身份认证证明有权使用此数据，同时还应该用使用者的身份证书数字签名来证明其使用数据的行为不可否认，用时间戳签名来证明数据使用时间是可信的、不可篡改和不可否认的。

至此，读者应该可以看出，以上这五大零信任措施实际上就是密码的全面应用，既实现了政务数据的零信任管理，同时也满足了《密码法》对数据安全保护的合规要求，这就是零信任加上密码技术的魅力之处，零信任加密码技术能让各局委办放心地把数据集中到政务大数据中心统一管理，各局委办只需专心做好自己的业务即可。

王高华

2022 年 1 月 5 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。