

FTS 档案文件传输技术

FTS 是文件传输服务的简称。该技术由服务器与客户端插件两部分组成。该技术是为了解决档案原文在网络环境中申请、调阅的安全保密要求。

1. 档案原文件组织方式

常见的档案原文件利用现有环境、系统安全来达到这一目的。如将档案原文件直接存放至数据库中或建立 FTP。

常见的大型关系型数据库都具有很好安全性,将要案原文直接存放这些数据库是一个可行的方案,可以利用数据库的用户、角色与档案系统的功能访问设计达到安全目的。这样也会带来一些弊端,比较突出现象有: 1. 数据库会快速膨胀。由于浙江移动已经积累了大量的档案,在系统规划的 3-5 年时间内会逐年递增,从而达到 TB 级容量,甚至更多。维护这样一个庞大的数据库将存在很大的风险,如备份、数据库损坏。备份会占用较多的资源,一旦损坏损失将不可估计。2. 性能降低。性能降低的最大原因在于将混合的数据库与大容量二进制数据共同存放在数据库,系统 I/O 将受到影响。

建立 FTP 可以很好地避免上述两种现象,但 FTP 的访问权限控制要与档案管理系统用户绑定在一起就非常困难了。浙江移动的档案用户要与 OA 系统等其他业务系统整合,这样会加大工作难度,当用户变更时,其对应的权限与用户信息无法得到同步更新。

因此,只有建立专门的文件传输服务,从底层提供访问接口,可以很好与关系型数据库、档案管理系统结合起来。

2. FTS 原文件组织方式

FTS 建立了一个用于网络内文件互传互访的专有加密机制。FTS 注册于档案专门的文件服务器,随操作系统的启动自动运行。

FTS 服务注册方式。FTS 内部建立了动态缓冲池,数据包格式大小、网络超时时间片、文件存放路径等。

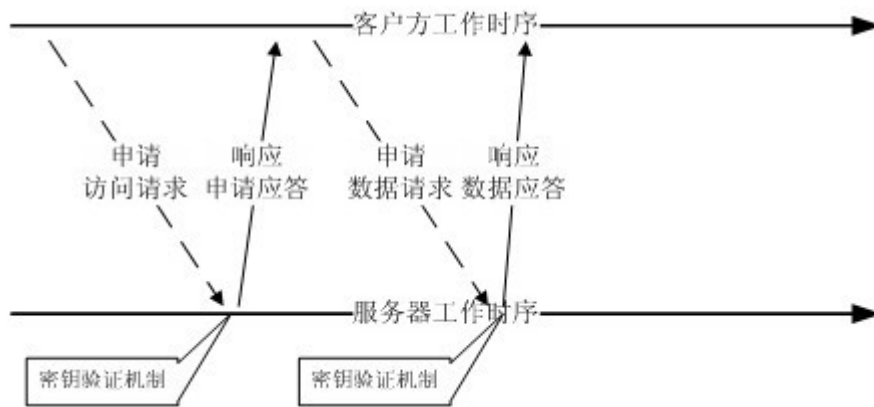
FTS 工作模式。FTS 的文件路径指定了档案资源管理系统原件的存放位置。当档案管理员上传、下载、调阅原文时按照系统设计的存放原则分类存放于该路径下。

FTS 综合了将档案原文件直接存放至数据库中与建立 Ftp 两项常见技术的优点。文件直接存放至服务器指定路径便于系统维护,系统管理员可以有预见性地备份单个或批量备份部分文件,当某个文件损坏时不会殃及全部;具有较高的性能,一般 FTS 都建立在高性能服务器上,FTS 在上传、下载、调阅原件时直接按路径地址存取;通过该服务能方便使用编程技

术将访问控制于档案的业务紧密结合起来；具有较高的安全性，当用户提交上传、下载或调阅命令时，网络上传输的指令均被加密处理，防止被截取利用；当通过该服务传输数据内容时，可以有选择地将数据库压缩，以减小网络传输的负载。

3. 客户端插件

客户端插件是配合 FTS 在客户端使用的上传、下载、调阅的专门控件。该控件与原文服务器配合组成一个安全体系。该安全技术提供了一项档案的保密措施，保密体现在档案信息在网络传输过程中不泄露，不可窃取，还体现在档案信息在知识产权上的保护。它们之间采用了“客户-服务”模式，系统提交的“请求-应答”采用了专门的“密钥报废机制”，传输的档案信息内容采用了“随机”加/解密，在客户区呈现、打印时加入水印与版权。如图表述其工作时序：



信息加密技术是为档案管理系统的安全管理专门设计的。档案管理系统系统除了操作系统、数据库等提供的安全特性以外，还专门设计了档案内容访问的安全控制，基于档案内容的加密手段。

从客户提交“请求”时，系统先申请一段加密码，将该加密码发送至服务器，服务器接收到该“请求”后参照密钥原则，验证其合法性，并做出“应答”，发送给客户方。确认后客户方再次发送“请求”数据的密码串。

当服务器验证非法时，则拒绝客户请求。由于用户操作存在网络延迟情况，系统在服务器上设置时间戳来验证是否存在超时。

系统在网络上做出的“请求”与“应答”均采用加密机制，以防止通过传输线电磁感应截获相应的数据信息。客户网页端 PC 接收到的数据存放到内存特定区域，不缓存到本地存储介质。

为了数据在客户申请的 PC 上正常显示，我们内嵌专门的图像浏览器，用来解释接收到

的数据。该图像浏览器提供打印、下载等功能。只有具有特定权限的档案管理人员才能使用打印与下载功能。打印的档案纸或下载到本地的档案页被系统随机加载“水印”，而不能被去除。“水印”一般为“复印品”、“打印件”、“版权信息”等字样内容组成。