

档案软件 - 数据传输加密功能【云丰档案软件功能介绍】

档案管理软件 · 功能介绍

档案在网络上传来传去，最担心的就是中途被偷看或被篡改。数据传输加密对系统与客户端之间、系统与系统之间的数据通道加密，让档案在传输过程中即使被截获也无法读懂、无法篡改。

一、为什么需要数据传输加密

档案从浏览器上传到服务器、从服务器调阅到屏幕、从一个系统交换到另一个系统，都要经过网络。明文传输在公共网络上等于明信片。

明文传输风险：档案内容与账号口令若明文在网络上传输，中途可能被截获窥探；

公共网络隐患：远程办公、跨网访问时，公共 Wi-Fi 下数据尤其暴露；

篡改难发现：传输途中数据被悄悄替换，接收方若无校验，可能存入错误档案；

合规有要求：等保与档案保密规定对传输保密性有明确要求，不加密难以过审。

传输加密给数据通道套上密封舱：内容即便被截获也不可读，完整性被破坏即可察觉，让档案在路上也安全。

二、怎么用：全程加密，无感使用

系统在底层启用加密通道，用户在浏览器或客户端正常操作即可，无须额外步骤，加密对业务透明。

表1 数据传输加密工作要点

环节	安全措施
通道加密	客户端与服务器之间全程加密传输，杜绝明文；
身份校验	通信双方先验证身份，拒绝陌生节点接入；
完整性校验	传输附带校验值，数据被篡改即识别丢弃；
接口加密	系统间数据交换同样走加密通道与鉴权；
运维透明	加密在底层自动完成，业务操作无需改变。

传输加密与存储加密前后呼应。数据在途中加密，落库后再加密存储，加上访问权限控制，构成一条完整的保密链条。密钥与权限分离管理，符合三员分离要求。

加密通道对业务透明，用户无需感知，但管理员可查看加密是否生效、证书是否到期。证书到期前系统会提醒更换，避免因证书过期导致连接中断。密钥与加密模块按三员分离要求管理，运维人员无法单独获取。

除传输层加密外，落库的电子档案按密级加密存储，密钥与数据分离保管，配合三员分离，任何单一管理员都无法单独调阅密件。审计日志完整记录加密策略的启用与变更，确保保密责任可追溯。

三、核心能力

表2 核心能力一览

能力	一句话价值	关键细节
全程通道加密	路上不泄密	浏览器、客户端、移动端与服务器之间全程加密，公共网络下也安全。
身份互验	只和可信方通信	通信双方先校验身份，陌生节点无法接入数据通道。
完整性校验	改了就知道	传输数据附带校验，中途被替换或损坏即可识别，防止错档入库。
接口同密	交换也安全	第三方对接与接口调用同样加密鉴权，不留明文后门。
业务无感	安全不加负担	加密在底层自动进行，用户正常上传调阅即可，无需额外操作。

四、典型使用场景

远程办公：档案员在家或外出通过加密通道访问库内档案，公共网络下内容不泄露。

跨网交换：与上级单位或协作系统交换档案目录，数据加密传输、防篡改。

移动端调阅：手机在外网借阅查看档案，通道加密，避免敏感内容被截获。

五、价值与产品定位

数据传输加密的价值在于补上档案离开库房后的那段路：内容在路上不可读、不可改，远程与跨网使用才真正放心。从端到端的加密再加上落库加密与权限隔离，档案在全程都处于受保护状态。

它与加密存储、权限分级、三员分离共同构成云丰档案的保密体系。系统已适配信创环境，满足机关与涉密单位对传输安全的合规要求。