

企业需求

企业希望能够通过文档安全产品来协助提高企业整体信息安全水平。在保证安全性的同时，通常希望产品能够具有如下特点：

- 信息加解密必须是强制的，以防止内部员工主动泄密；
- 不改变使用者的使用习惯；
- 在特殊情况下需要将文件外发的，可由使用者提出申请，由管理员审批；
- 计算机能够脱离网络环境使用，同时保证信息安全；
- 用户对文档的操作都能够被审计下来，并根据条件定期出具泄密风险报告；
- 能够与现有的业务系统（如 OA、PDM）结合，提高业务系统的安全性；

项目目标

简单归结，项目目标应该包括：

1. 文档的真正所有者是公司；
2. 员工无法通过简单的手段直接带走大量信息（例如某个项目的完整资料），即使想要越权，只能采用成本较高的办法（例如拍照、手抄等）；

使用铁卷

在正常使用的过程中，最终用户一般感受不到铁卷的存在，除非用户需要：

将文件解密；

带电脑离开公司的网络环境；

希望产生的文档不加密；

需要把机密文档中的文字复制到特定的网站。

解密文档

在某些情况下，用户需要将文件进行解密，铁卷的客户端能够使得用户提出解密申请，该消息转发到指定的管理员处，由指定的管理员进行审批。如下图所示：



经过管理员的审批后，用户端的加密文档立即被解密。

计算机离线使用

和解密申请一样，计算机的离线使用也能够通过由客户端发起、由管理员进行审批的方式进行。



离线用户需解密文档，可将文档发回给公司人员，交由其代为解密或由管理员赋予离线用户以自行解密文档的权限。自行解密文档的日志记录将在计算机再次联入公司网络时传入公司的日志服务器中以供审核。

授权文档的控制

铁卷能够通过将文档转换成 EXE 可执行文件的形式来授权文档，使得该文档能够在任意地方使用，同时保证该文档安全性，实现如下功能：

阅读次数限制；
阅读时间限制；
阅读密码限制；
在特定的计算机上查看；
包含水印。

当这封文档超出了使用限制后，文档可以自行销毁。

计算机的离线

铁卷提供了多种可供用户离线使用的方案，以便用户在各种条件下都能够正常工作，尽可能的减小加密软件给用户带来的使用难度。

非正常离线的处理

客户端在非正常状态下离线，有如下可能性：

客户端计算机被人为的脱离了内部网络环境；

客户端计算机网线被无意中碰松或拔出；

网络设备损坏或宕机；

铁卷的服务器损坏或宕机；

网络延迟较高被计算机认为是离线。

依照此问题我们允许用户自行设置一个时间参数，此参数用于客户端在离线后的多长时间内，依然能够正常的加解密文档。

比如可以设定 20 分钟，即：在客户端连接不上服务器的 20 分钟内，客户端依然能够正常工作。并通知管理员及时处理问题。解决了因后四种原因导致的客户端非正常离线而影响工作的问题。

日志审计

铁卷提供了详细的文档操作日志审计，便于管理员做好有效的事前监督工作。日志记录的内容包括：



灾难恢复

为了保证 XXXXXX 的业务在任何时候都能够正常运行，铁卷的灾难恢复控制能够使得 XXXXXX 的管理员在任何情况下都有解决方案，以保证业务的高可用性、高可靠性和高安全性。

- 服务器发生故障
 - 一旦主服务器发生故障，客户端会自动连接到备用服务器，切换完全无缝。保证在服务器出现问题时候的业务连续性。
- 网络暂时中断
 - 在网络出现暂时中断（例如机房断电、网络设备宕机等突发事件）时，客户端计算机能够在设定的时间内继续正常工作。
 - 管理员能够通过分发离线授权文件使得客户端能够正常工作。

-
- 管理员能够通过分发 USB KEY 使得客户端能够正常工作。