设计大纲

设计目标

通过一套系统，能够实现文档自身的安全。能够对文件进行分类，实现文件对某人、某些人、某些层次的人进行不同颗粒度授权。具体功能包括但不限于以下场景：

限定条件：

指定设备打开，设备的MAC地址。

限定人员、群组、角色访问

限定时间打开

限定IP/地域打开

限定操作系统类型打开

允许实时控制打开授权，包括禁用文件打开

限定是否允许打印

限定是否允许另存

支持阅后即焚

支持文件生命周期管理，包括文件的生成、流转记录、轨迹、状态

所有功能均基于文件自身，支持所有可打印格式文件，能够支持互联网、内网部署应用。

具体技术原理：

全部实现的核心是在现有版式文件/PDF/OFD的外面外包一层壳，通过加密的方式对文件进行处理。在进行展示时，需要从服务端加载一部分密钥，经过计算得到最终的解密密钥。客户端与服务端的交互均走单向的SSL通道。

文件结构设计：

文件头+加密数据

文件头结构：

Typedef struct stEncHeader

{

Dword version; //高2个字节为大版本，低2个字节为小版本

Uchar filetype;//文件类型，0为pdf，1为ofd，后续可以累加

Dword fileLen; //加密前文件长度

Dword startPos; //文件加密起始地址

DWORD fileID; //被服务端加密后，采用雪花算法得到的文件标识

Uchar encType;//文件加密算法，0为sm4，后续可以累加，默认采用ecb分组模式

Char encKey[32];//加密密钥，需要和服务端半个密钥进行串联，SM3

Char padding[64];//随机数，后续备用

} EncHeader;

Sender 6020

Reciver 9999

Server file—》encKey🡪Reciver9999，Time：2020.02.25 1200-1300

前置条件

所有用户在使用前必须在网站上进行注册，注册须填写手机号、邮箱等信息，并通过短信认证码确认用户持有手机的有效性。

1. 文件被导出时

文件被导出时，需要弹出界面，让用户自行选择需要解密时的一些要求（参见场景）。用户可从内部选择配置好的人名（根据手机号码，从服务端查询，有备注，实际是手机号码）或者角色（适用于私有网络）进行请求加密处理，客户端会随机生成32字节的加密密钥。

服务端收到请求后，会判断当前用户是否为有效用户，若是，则会通过雪花算法生成一份fileID，作为本次加密文件的唯一标识（主键），并将此ID通过服务端自有加密方式进行加密，得到EID、服务端会随机生成新的32字节加密密钥以当前身份手机号+Salt的HASH值为密钥进行SM4 ECB加密，得到EPWD，并将加密后的数据反馈至客户端

客户端通过解密可以拿到可以拿到服务端生成的新32字节加密密钥，结合自身生成的共计64字节，通过本地HASH可得到最终的加密密钥。

客户端通过此加密密钥进行加密，并将文件头加盖到新的文件里面，形成最终文件。

1. 文件被导入时

加密的逆过程，所有的验证都需要在服务端来完成。

解析文件，获取本地电脑名称、MAC地址、操作系统，结合文件的FILEid传输至服务端。

服务端会根据文件类型查询验证内容：

指定设备打开，设备的MAC地址。--比对

限定人员、群组、角色访问—通过Session中的查询

限定时间打开—服务器时间比较

限定IP/地域打开—通过服务端获取客户端的地址比较

限定操作系统类型打开----通过回传的地址

允许实时控制打开授权，包括禁用文件打开—查询当前状态

限定是否允许打印—下发

限定是否允许另存—下发

支持阅后即焚—下发

服务端比较后，会下发具体要求。如果可以打开，则会把对应的服务端密钥发放至客户端（同样的加密和解密）。客户端拿到密钥，即可进行解密。解密后的文件全部存放在内存中（安全），通过阅读器进行浏览。

如果有阅后即焚的要求，解压到内存后，下次再打开时，就不再返回密钥了（只允许看一次）。

用户可通过自己的手机好吗和短信吗登录自己的空间。

在空间里面可以查看自己控制的文件状态，包括文件备注（譬如文件名），控制项等信息，可以修改。可以查阅当前文件记录信息。