方案描述

该方案仅实现用户对指定文件的授权访问机制，用户可以对某人或某一级（部门）的授权访问，即文件的定向分发。将某一行业、企业或部门系统数据化，可以看做一个闭环系统，将这个闭环系统中，给有数据需求的个人分配一个唯一的不可更改的身份标识（姓名、邮箱、工号等），利用这个标识生成与之对应的公私钥数据池，同时发布给每一个个体，这样每个个体在闭环系统中都可以通过对方的公开标识在公钥池中找到对方的公钥，对对方完成授权操作。

为了使用户私钥绝对安全，我们基于国家密码局发布的国密二级型号芯片设计了个人专用U盘承载用户私钥和公钥池并保证相关数据的安全性。具体数据处理流程：软件收到用户文件输入后，客户端软件随机生成文件保护密钥SM4Key,使用SM4Key将用户文件加密得到M1，依据被授权人标识寻找被授权人专有公钥，然后利用SM2算法加密SM4KEY得到M2，M1与M2按既定规则组合生产校验码C，M1、M2、C三部分按一定的规则进行组合后生成新的文件F,用户可将F使用任意途径外发，因为只有被授权人才可以打开F文件。

在日常使用中，存在用户将个人U盘丢失的情况，为了做到丢失可补发，所以发行系统需要安全的保存公钥文件、私钥文件、用户标识文件（发行系统放置在安全可信的环境中）。

发行软件功能

1. 生成公私钥矩阵

调用软件sm2或芯片的sm2生成密钥对接口生成N对（暂定N=1000）密钥对，本地分开存储（公钥文件、私钥文件）。

本功能为一次性功能，待公私钥文件生成后，本功能关闭，不允许再次使用，防止误操作重复生成。

1. 初始化设备
2. 为设备(U03)配置唯一编号（标识）；

标识可以写到KEY里（512字节私有区）。

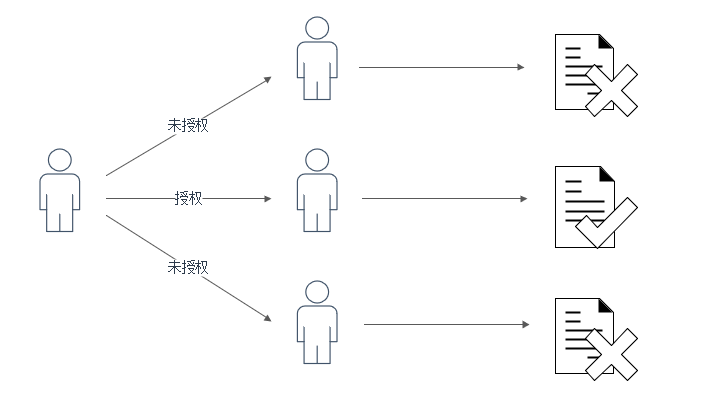
这里有个问题：要靠标识在公钥文件和私钥文件中找到唯一对应的密钥对。为了简单，可以在配置标识的同时为设备（U03）设置编号（1、 2 、 3……1000），在查找的时候，建立编号与标识的映射。（***做的时候再沟通***）

1. 将标识与编号的对应关系写入本地的一个文件（每初始化一个，写一个，累加）
2. 按照上一步分配的标号，从本地存储的公私钥文件中提取唯一的一对私钥下发给U03，同时调用对应接口，将1中生成公钥文件下发给U03；
3. 待所有的U03都发行完后，将B中生成的对应文件写入U03。

每次有新设备发行，都需要先将B生成的文件下发给所有设备，这个暂时靠人管理吧（在用户软件中，预留一个在线自动更新的接口，详见用户软件）。

用户软件

用户软件只有一个功能，加密文件。数据流程见方案设计。达到的效果图如下：



用户界面简框



1. 通过点击浏览选择需要的文件；
2. 通过下拉列表选择给谁发（也可以允许用户输入），下拉列表的数据可以从u03中读取（发行软件初始化时写入的标识与编号部分中的标识）；
3. 点击开始，开始按方案加密，生成加密后的文件，文件放在原文目录下，加密完成，“开始”变为“完成”。
4. 具体数据处理流程：软件收到用户文件输入后，客户端软件随机生成文件保护密钥SM4Key,使用SM4Key将用户文件加密得到M1，依据被授权人标识寻找被授权人专有公钥，然后利用SM2算法加密SM4KEY得到M2，M1与M2按既定规则组合生产校验码C，M1、M2、C三部分按一定的规则进行组合后生成新的文件F.

文件结构可以做的简单点：

