**基于属性加密的文件加密系统**

**概要设计说明书**

目录

**[一.项目背景](#_Toc27727_WPSOffice_Level1)** **[4](#_Toc27727_WPSOffice_Level1)**

[1.1 项目背景](#_Toc19286_WPSOffice_Level2) [4](#_Toc19286_WPSOffice_Level2)

[1.2 项目目标](#_Toc29538_WPSOffice_Level2) [4](#_Toc29538_WPSOffice_Level2)

**[二.总体设计](#_Toc19286_WPSOffice_Level1)** **[4](#_Toc19286_WPSOffice_Level1)**

[2.1系统简述](#_Toc1552_WPSOffice_Level2) [4](#_Toc1552_WPSOffice_Level2)

[2.2总体设计思路](#_Toc4674_WPSOffice_Level2) [4](#_Toc4674_WPSOffice_Level2)

[2.3系统总体结构](#_Toc13034_WPSOffice_Level2) [6](#_Toc13034_WPSOffice_Level2)

[2.4系统模块](#_Toc2924_WPSOffice_Level2) [7](#_Toc2924_WPSOffice_Level2)

[2.5业务流程](#_Toc29672_WPSOffice_Level2) [8](#_Toc29672_WPSOffice_Level2)

**[三.数据库设计](#_Toc29538_WPSOffice_Level1)** **[9](#_Toc29538_WPSOffice_Level1)**

[3.1 用户表（User）](#_Toc16411_WPSOffice_Level2) [9](#_Toc16411_WPSOffice_Level2)

[3.2 群组表（Club）](#_Toc30591_WPSOffice_Level2) [10](#_Toc30591_WPSOffice_Level2)

[3.3 关系表（Relationship）](#_Toc13965_WPSOffice_Level2) [10](#_Toc13965_WPSOffice_Level2)

**[四.数据源](#_Toc1552_WPSOffice_Level1)** **[10](#_Toc1552_WPSOffice_Level1)**

[4.1外部数据源](#_Toc24099_WPSOffice_Level2) [10](#_Toc24099_WPSOffice_Level2)

[4.2内部数据源](#_Toc15312_WPSOffice_Level2) [10](#_Toc15312_WPSOffice_Level2)

**[五.系统功能](#_Toc4674_WPSOffice_Level1)** **[10](#_Toc4674_WPSOffice_Level1)**

[5.1登录](#_Toc23921_WPSOffice_Level2) [10](#_Toc23921_WPSOffice_Level2)

[5.2 新建群组](#_Toc24773_WPSOffice_Level2) [11](#_Toc24773_WPSOffice_Level2)

[5.3 加入群组](#_Toc5524_WPSOffice_Level2) [11](#_Toc5524_WPSOffice_Level2)

[5.4 删除组内用户](#_Toc5239_WPSOffice_Level2) [11](#_Toc5239_WPSOffice_Level2)

[5.4 加密文件](#_Toc29388_WPSOffice_Level2) [11](#_Toc29388_WPSOffice_Level2)

[5.4 解密文件](#_Toc28158_WPSOffice_Level2) [11](#_Toc28158_WPSOffice_Level2)

**[六. 参考引用与术语](#_Toc13034_WPSOffice_Level1)** **[11](#_Toc13034_WPSOffice_Level1)**

# 一.项目背景

## 1.1 项目背景

自2008年，全市重点单位大部分三级（或以上）的信息系统已按《信息安全等级保护管理办法》等有关规定开展了等保测评工作，并取得了良好的成效。现如今已经进入信息化时代，对信息安全问题需求也日渐提高。由于对文件的保密需要，需设计一个对文件加解密的设计方案。

## 1.2 项目目标

本文对系统的功能进行了分解，描述了系统的模块、接口、数据库、文件等的框架设计。

系统应当满足以下几个需求：

1. 文件加密。对于测评过程中的重要文件，为了避免在数据传输过程中的窃取行为，应当在加密后进行传输。
2. 访问控制。由于用户属性和权限不同，用户并不必解密所有文件，仅需要解密与自己权限相符和与自己相关的文件。对于与自己无关和无权限文件，用户不能解密。

## 1.3 项目进度

（需要讨论）

# 二.总体设计

## 2.1系统简述



**图2-1-1. 网络拓扑图**

系统整体采用C/S结构，由用户通过PC端程序与公司服务器相连。公司服务器具有身份认证，（加密）属性生成，密钥分发，加密密钥等功能。PC端得到密钥和属性，可以对文件进行加密、解密。密文通过文件附件的形式上传用过263邮件服务器发送给邮件接收者。

## 2.2总体设计思路

为了满足以上要求，提供了一套基于ABE的属性加密方案。

用户的权限非分解成了各个属性，属性之间通过与、或运算，形成访问结构。在用户加密过程中，访问结构作为参数传入，参与用户加密。得到加密结果。解密过程中，用户从服务器请求密钥，服务器端根据用户属性生成对应密钥，用户得到密钥后进行解密。

## 2.3系统总体结构

## 用例图

**图2-3-1. 系统用例图**

## 2.4系统模块

在线申报系统主要功能模块如下：

功能列表：

**表2-4-1. 功能模块表**

|  |  |  |
| --- | --- | --- |
|  | **功能** | **备注** |
| Server | 属性群组管理 |  |
| 用户管理 |  |
| 密钥管理 |  |
|  |  |
| Client | 登录（获得最新的属性群组） |  |
| 新建属性群组 |  |
| 把某些人加入属性群组 |  |
| 删除群组 |  |
| 群发邮件 |  |
| 加密文件 |  |
| 解密文件 |  |
| 加密目录 |  |
|  |  |
| Browser | 解密文件 |  |
| 建属性群组个数权限更改 |  |
| 新建用户 |  |
| 删除用户 |  |
|  |  |

## 2.5业务流程

## 2.5.1登录

用户使用时需要先登录系统，获取用户所在的邮箱信息、群组等信息等。

## 2.5.2 新建群组

已经登录的用户发起新建时，后台首先通过判断用户建组个数以及建组最大个数判断用户是否允许建组。若允许建组，后台讨论组中新建群组，并使得创建者携带此组属性。

****

**图2-5-1 建群过程序列图**

## 2.5.3 加入群组

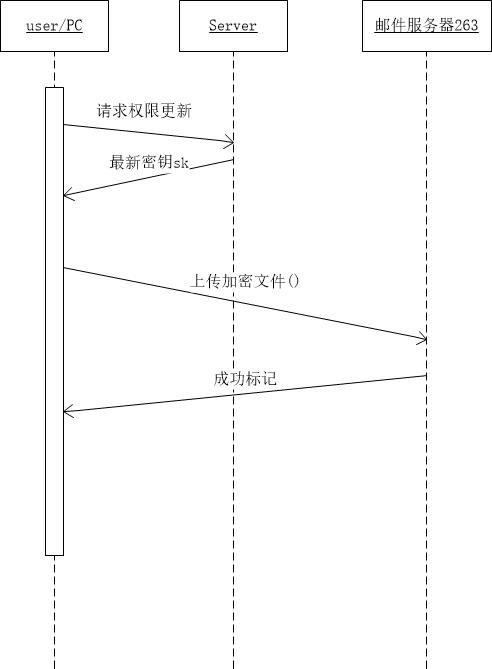
已经在群组内的用户可以通过勾选的方式选择其他未在组内的用户加入群组，使得未在群组内的用户携带此组属性。

## 2.5.4 删除组内用户

建组用户可以对已经在组内的用户进行删除。用户自身（除群组创建者例外）可以对自身删除。使其不携带此组属性。

## 2.5.4 加密文件

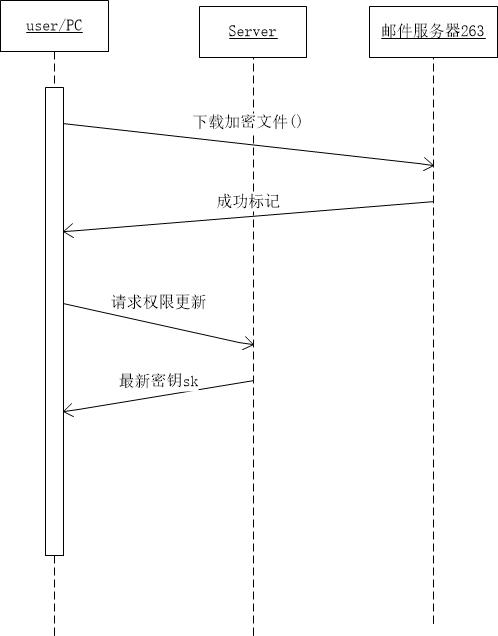
用户可以对文件加密。首先通过Server请求得到密钥PK。选择群组之后，可以对文件加密。得到加密后的文件。



**图2-5-1. 加密过程序列图**

## 2.5.4 解密文件

用户可以对文件加密。首先通过Server请求得到密钥SK以及群组。之后可以对文件进行解密。若非正常解密，意味着此人无访问权限。



**图2-5-2.** 解密过程序列图

# 三.数据库设计

## 3.1 用户表（User）

**表3-1-1用户表**

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 描述 | 备注 |
| Id | Int | 用户id | PK |
| Name | String | 用户名 |  |
| Department | String | 用户所在部门 |  |
| Position | String | 职位 |  |
| EMail | EMail | 邮件 | 自定义完整性判断（需有@） |
| Club\_limit | int | 可以创建的最大群组数 | Default=3 |
|  |  |  |  |

## 3.2 群组表（Club）

**表3-1-2群组表**

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 描述 | 备注 |
| Id | Int | 群组id | PK |
| Name | String | 用户名 |  |
| Create\_User | Int | 创建人 | 外键，关联用户表， |

## 3.3 关系表（Relationship）

**表3-1-1用户表**

|  |  |  |  |
| --- | --- | --- | --- |
| 字段 | 类型 | 描述 | 备注 |
| Id | Int | 关系id | PK |
| Club | Int | 群组Id | 外键，关联群组表 |
| User | Int | 用户Id | 外键，关联用户表 |

# 四.数据源

## 4.1外部数据源

本系统不涉及外部数据源

## 4.2内部数据源

系统的用户信息由公司统一收集。

密钥等关键信息由服务器器初始化后留存。

# 六. 参考引用与术语

基于属性加密（ABE）：基于属性加密，详见

https://baike.baidu.com/item/%E5%9F%BA%E4%BA%8E%E5%B1%9E%E6%80%A7%E5%8A%A0%E5%AF%86/13028914?fr=aladdin

PK：公钥，用于加密的比特串

SK：私钥，用于解密的比特串

访问结构：由属性之间通过AND/OR逻辑运算组成的与或树