版本号：V1.0

**SecSpace License设计方案**

2018年4月

修订记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 修订日期 | 版本号 | 变更记录 | 修订描述 | 修订人 |
| 2018.04.11 | V1.0 |  | License设计方案草案 | 张俊 |
| 2018.04.16 | V2.0 | 增加License控制項，对License有效期控制设计进行修改 | License设计方案初定 | 张俊 |
| 2018.04.17 | V3.0 | 增加授权接口映射设计 | License设计方案完稿 | 刘大东 |
| 2018.04.17 | V3.0.1 | 控制项增加功能开关及格式说明；增加Licese信息查看项;文档格式修改； | License设计方案终稿 | 张俊 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

一、License简介 4

二、设计需求 4

2.1 需求背景 4

2.2 License设计需求 4

三、License控制项 5

3.1 企业名称 5

3.2 机构代码 5

3.3 有效期 5

3.4 最大用户数量 5

3.5 最大设备数量 5

3.6 最大子级机构数量 5

3.7 功能模块控制 5

3.8 服务器唯一标识码 6

3.9 最大在线用户数 6

3.10 移动终端权限控制 6

四、License 文件设计 6

4.1 授权文件 6

4.2 授权接口映射设计 9

五、License安全 9

5.1 密钥对 9

5.2 License文件加密 9

5.3 License签名 9

5.4 License 签名验证/解密操作 10

5.5 License签发服务 10

六、 License设计流程图 11

6.1 License过期通知及有效期设计 11

6.2 License 验证方案设计 12

# 一、License简介

License是版本许可证，相当于软件版权；是一种格式合同，由软件作者根据最终用户的需求制作的，用以规定和限制软件用户使用软件（或其源代码）的权利，以及作者应尽的义务。本质：防止盗版, 按功能收费，控制使用时间，控制用户数量，控制设备数量。

# 二、设计需求

## 2.1 需求背景

目前，商用软件都是采用License授权的方式来保证软件本身不被盗用，以保证自身的利益。对于软件特殊行业而言，通过License授权的方式是一种保护软件系统本身的一种有效的手段。

## 2.2 License设计需求

根据SecSpace的需求，此License设计需满足以下几点：

**2.2.1 机器绑定**

SecSpace服务器在启动后，需要验证License，这个License的某个信息字段要与

服务器的唯一识别码匹配，如果不匹配，则判License无效。可有效防止系统被克

隆使用。

**2.2.2 管理端模块权限**

根据与软件用户的协商，让用户在规定的权利内使用，License的信息字段要包含

模块权限的信息。

**2.2.3 系统权限**

根据与软件用户的协商，事先规定好企业名称，机构代码，用于控制安全空间登录

限制；达到分级管控的效果。

**2.2.4 有效期**

授予给软件用户的试用License，有效期一到，License失效。所有的模块均不能工

作；

**2.2.5 基本控制项**

SecSpace系统支持最大的用户数量／设备数量／子机构数量。

**2.2.6 管理端license信息查看**

管理端提供显示license信息的功能，主要是有效期、管理端提供license导入功

能

# 三、License控制项

## 3.1 企业名称

License授权信息中规定的授权企业的企业名称。

格式说明：允许使用中文或者英文企业名称

## 3.2 机构代码

License授权信息中规定的机构编码，此编码针对SecSpace系统级唯一，后期可用

于客户端登录SecSpace系统的标识，从而客户端与服务器做从属限定。

格式说明：待项目确定，“支持字母,数字,下划线组合”

## 3.3 有效期

根据与软件用户的协商，控制系统使用的有效期，当License过期后，管理端只提

供License导入功能，其他功能禁用。

格式说明：有效期采用：开始时间和结束时间，两项进行控制。

时间格式：2018-04-08 12:01:01

增加开关项，控制是否验证此字段

## 3.4 最大用户数量

控制整个SecSpace 系统添加的用户的最大数量，当用户数量达到授权数量后，不

允许再添加。

格式说明：数字。

增加开关项，控制是否验证此字段

## 3.5 最大设备数量

控制整个SecSpace 系统登录设备的最大数量，当设备数量达到授权数量后，不允

许新设备登录。

格式说明：数字。

增加开关项，控制是否验证此字段

## 3.6 最大子级机构数量

根据与软件用户的协商，控制系统最多可拥有的子级机构，当子级机构数量达到授

权数量后，不允许再添加。

格式说明：数字。

增加开关项，控制是否验证此字段

## 3.7 功能模块控制

根据License中的模块信息，控制管理端可以展示和使用的功能。同时模块信息也是

授权管理员功能依据

## 3.8 服务器唯一标识码

3.8.1 标识码设计

可有效防止SecSpace系统克隆被重复使用；经调研，服务器上没有任何一个单

独的信息可作为唯一标识码，需要硬件设备信息／系统uuid组合生成唯一标识；

在此设计方案，采用网卡mac地址 + 主板id + 系统uuid 组合验证(mac地址

获取设备第一块网卡的mac地址)，当这三种相同的情况下，可确认为同一台主

机，并将这三种信息最后做一次base64编码作为服务器的唯一标识码；

3.8.2 标识码获取

编写一个python（或者shell）脚本，在服务器设备上运行，运行的结果即为服务器标识码，在制作License时，将此标识码发给License制作者。

3.8.3 标识码验证控制

增加开关项，控制是否验证此字段

## 3.9 最大在线用户数

控制整个SecSpace 系统在线设备的最大数量，当在线设备数量达到授权数量后，不允许新设备登录。

格式说明：数字。

增加开关项，控制是否验证此字段

## 3.10 移动终端权限控制

3.10.1 移动终端模块控制用于控制secspace在到移动设备上时所需要的Android系

统权限信息。

3.10.2 在管理页面的设置中增加移动终端权限配置功能，页面中显示的信息项就是

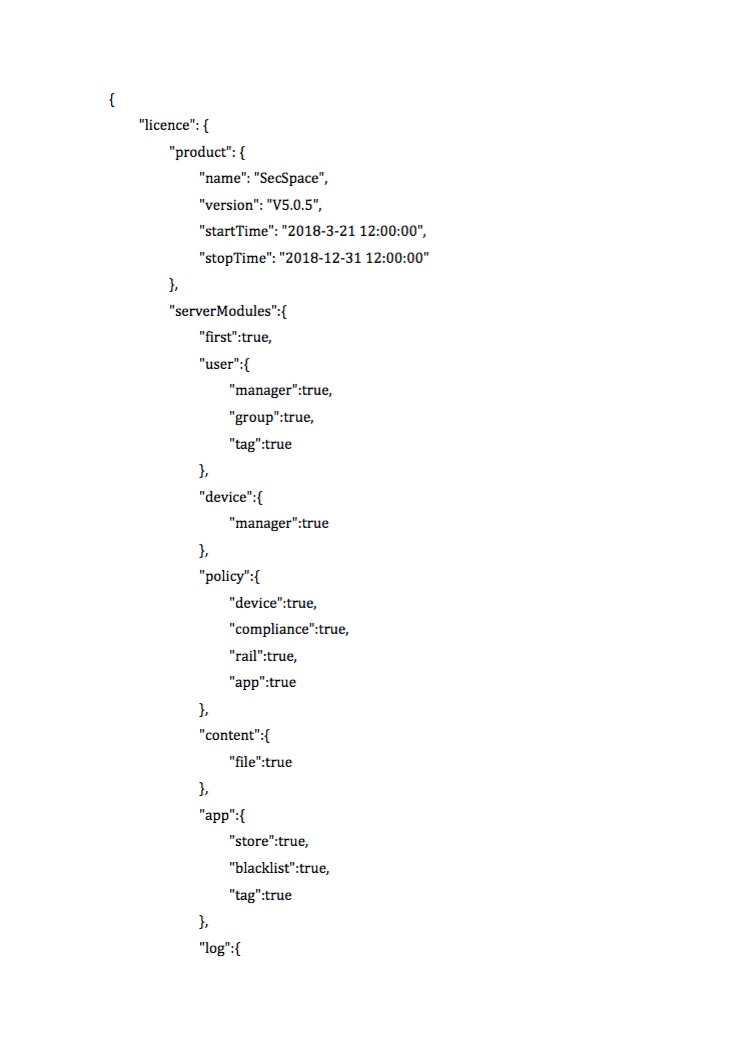
License中设置的移动终端设置信息。

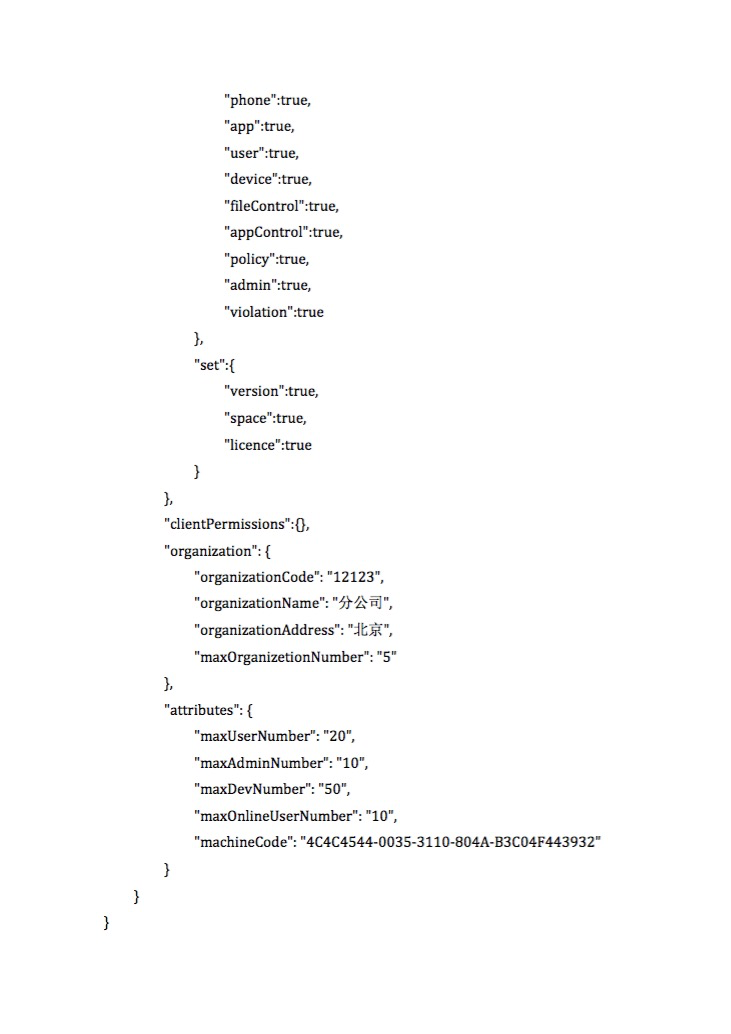
# 四、License 文件设计

## 4.1 授权文件

根据此次License设计需求的控制项，对License授权文件的内容进行了格式设计，采用json格式阐述各控制项，其内容主要包括五个部分：

|  |  |
| --- | --- |
| **License字段** | **描述** |
| **product** | **产品信息** |
| **serverModules** | **服务端授权模块** |
| **clientPermissionss** | **客户端端授权模块** |
| **organization** | **机构信息** |
| **attributes** | **其它控制项** |





## 4.2 授权接口映射设计

4.2.1基本思想

根据授权文件层次结构，拼接授权正则表达式，过滤请求。

4.2.2具体步骤

1）声明授权数组aRegLicUrl，遍历授权文件的授权模块，获取关键字，判断末

端布尔值，拼接正则格式的授权接口，存入aRegLicUrl授权数组；

授权文件serverModules片段：

serverModules ：{

“first”：true，

“users”:{

“manager”: true,

“group”: false,

“tag”: true

}，

……

}

映射aRegLicUrl授权数组：

[

‘/man/first(/[a-zA-Z]\*)\*’、

‘/man/users/manager(/[a-zA-Z]\*)\*’、

‘/man/users/tag (/[a-zA-Z]\*)\*’

]

2）将aRegLicUrl带入置于其它接口之前的node路由中间件，当有请求进入时，

先匹配授权数组中的正则格式接口，过滤请求。

# 五、License安全

## 5.1 密钥对

生成密钥对的方法很多，在此使用RSA的方式生成一对密钥对。

## 5.2 License文件加密

采用生成的RSA 私钥对License文件进行加密。(可参考SecSpace系统中消息推送的加密方式)

## 5.3 License签名

采用自签名的CA证书，将私钥保留在公司，并使用私钥对包含授权信息（如使用截止日期，模块授权信息等）的加密后的license文件进行数字签名。

## 5.4 License 签名验证/解密操作

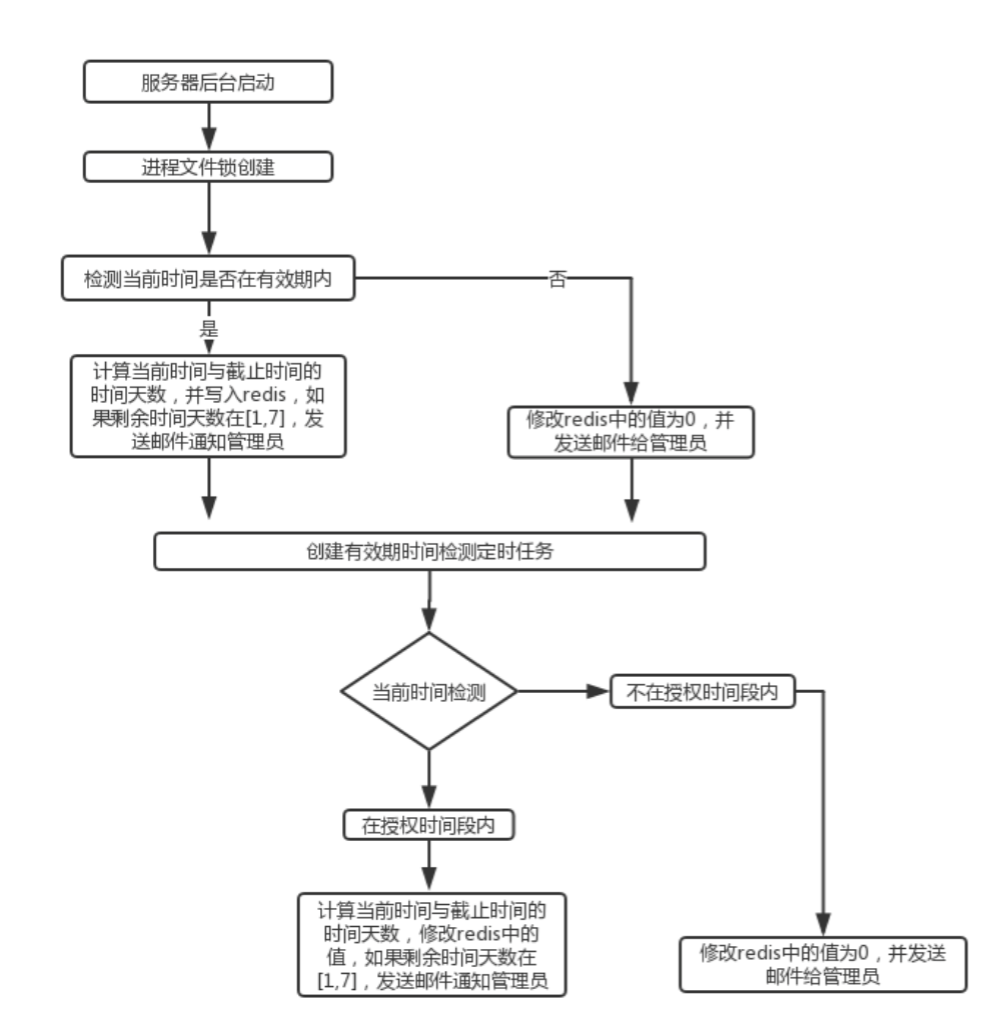
将自签名的CA公钥放在验证的代码中使用，用于验证license是否符合使用条件。验证通过后，利用RSA的公钥(放在解密的代码中)解密License文件，并提取License文件里面的信息，进行系统权限验证。

## 5.5 License签发服务

可在内网环境下，设计一个License制作制作。将原始的License文件(Json格式)上传至内网服务器，在服务器接口中实现RSA私钥加密／CA私钥签名，并将最终生成的.lic文件(文件名格式： 客户名\_签发时间\_授权天数.lic)的下载地址返回

# 六、 License设计流程图

## 6.1 License过期通知及有效期设计



## 6.2 License 验证方案设计

