服务器端服务调用说明

辽宁CA

地址：

TEL：

FAX：

Http://

**变更记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 日期 | 作者 | 变更说明 | 状态 | 页数 |
| 1.0 | 2014-11-3 | 段晓君 | Initiated | Draft | 11 |
| 1.1 | 2014-12-25 | 段晓君 | 修改3.2登录流程 |  | 13 |
| 1.2 | 2015-1-9 | 段晓君 | 修改5.2、5.6接口参数描述 |  | 14 |
| 1.3 | 2015-4-9 | 丰 洋 | 增加5.10 接口描述 |  |  |

目录

[1 概述 3](#_Toc408562450)

[2 服务器部署 3](#_Toc408562451)

[3 系统功能及登录流程 3](#_Toc408562452)

[3.1系统功能 3](#_Toc408562453)

[3.2登录流程 3](#_Toc408562454)

[3.3 登录说明 6](#_Toc408562455)

[3.3.1 随机数 6](#_Toc408562456)

[3.3.2 Token 6](#_Toc408562457)

[4其它服务器部署方式 6](#_Toc408562458)

[5 系统API 7](#_Toc408562459)

[5.1取随机数 7](#_Toc408562460)

[5.2登录 7](#_Toc408562461)

[5.3更新token 8](#_Toc408562462)

[5.4登出 9](#_Toc408562463)

[5.5取token详情 9](#_Toc408562464)

[5.6签名存储 10](#_Toc408562465)

[5.7取用户证书详情 10](#_Toc408562466)

[5.8数据验签 11](#_Toc408562467)

[5.9数据签名 11](#_Toc408562468)

5.10 sm2 rsa 证书登录

[6功能测试 12](#_Toc408562469)

[6.1 设置认证服务器 12](#_Toc408562470)

[6.2 获取随机数 12](#_Toc408562471)

[6.3 签名登录 13](#_Toc408562472)

[6.4 更新令牌 13](#_Toc408562473)

[6.5 获取令牌信息 13](#_Toc408562474)

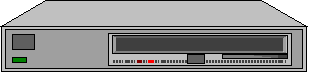
[6.6 获取证书信息 14](#_Toc408562475)

[6.7 退出登录 14](#_Toc408562476)

# 1 概述

网关服务器为业务服务器提供对客户端身份验证的服务，主要负责：用户登录、签名存储、证书存储、数据加密、数据验签。

# 2 服务器部署

验证结果

网关服务器

访问请求

业务服务器

客户端

图1 服务器部署一

# 3 系统功能及登录流程

## 3.1系统功能

网关系统的登录功能主要负责：用户登录（验证用户信息、生成token、更新token）、签名存储、证书存储、数据加密、数据验签。所有服务都是使用web post方式执行，返回的格式是JSON。

网关系统实现了服务器的反向代理功能，主从备份功能，可配置时间戳服务器，性能可拓展。

## 3.2登录流程

当客户端访问业务服务器时，业务服务器把客户端的信息（随机数、对随机数的签名结果、客户端证书）通过http发送给网关服务器；网关服务器对客户信息进行验证，验证成功后，生成token，把验证结果及token通过http返回给业务服务器；业务服务器把token返回给客户端。详细流程如下：

1. 用户访问客户端的登录界面，向业务系统发出登录请求
2. 业务系统收到请求后，向网关服务器发送随机数生成请求
3. 网关系统生成一个随机数
4. 网关系统把随机数返回给业务系统
5. 业务系统把随机数发送给客户端
6. 客户端获得该随机数，并对其签名，将签名结果、随机数和客户端证书发送给业务系统
7. 业务系统向网关系统发出验证请求
8. 网关系统验证签名及证书
9. 验证成功后，生成token
10. 网关系统把token返回给业务系统
11. 业务系统把token返回给客户端
12. 在token过期时间内，业务系统向网关系统发送更新token请求
13. 网关系统更新token
14. 客户端向业务系统发出登出请求
15. 业务系统向网关系统请求登出
16. 网关系统销毁token

登录流程图如下图所示：

网关系统

业务系统

客户端

1. 访问请求

2. 随机数生成请求

3. 生成随机数

4.随机数

5.随机数

6. 随机数、客户端证书、随机数签名结果

7. 验证请求(随机数、客户端证书、随机数签名结果)

8. 验证签名及证书

9. 生成token

10. token信息

11.token信息

12. 请求更新token

13 更新Token

14. 登出请求

15. 请求登出

16 销毁Token

图2 登录流程

## 3.3 登录说明

### 3.3.1 随机数

用户登录时，随机数是网关服务器生成，发给业务服务器，业务服务器把随机数及需要签名的内容发给客户端，用户在客户端用随机数给待签名内容签名，交给业务服务器，再由网关服务器验证签名。这样，用户在登录之前无法知道需要签名的内容，就无法事先就用UKey生成签名混入业务系统，保障用户访问的安全性。

### 3.3.2 Token

Token（令牌）是网关系统赋予登入用户的一个临时、独有的访问ID，用户用这个ID来证明自己已经通过网管的登录验证，业务系统可以据这个ID来判断用户是否已通过网关系统的登录验证。

为保障已登入用户访问的安全性，Token（令牌）令牌是有寿命的，寿命终结后持有该令牌的已登入用户的访问被禁止，因此需要在寿命终结之前更新令牌以延长令牌寿命，保持访问的有效性。已登入的活动用户在使用系统时需要由业务系统周期性地向网关系统发出申请以及时更新令牌，使令牌处于有效状态。

业务系统可以使用令牌向网关服务器请求登录用户的详细信息，如证书实体、登录时将、IP、证书SN、证书主题。

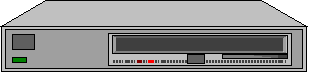
业务系统可以向网关服务器请求删除令牌，终止用户的登录状态。

# 4其它服务器部署方式

网关服务器采用服务器部署一的部署方式时，客户端直接与业务系统交互，符合访问服务器的使用习惯，业务系统需要频繁与网关系统交互实现用户的登录验证等功能。

如果已经部署好业务服务器需要增加网关服务器时，业务服务器需要增加与网关服务器交互的功能，提供第二种网关服务器的部署方式，减少业务系统与网关的交互。

服务器的部署方式二如下图所示，网关服务器提供登录首页，以及验证用户登录的页面，用户请求需要通过网关转发给业务服务器，未经认证的用户是不能通过网关将请求发给业务服务器的。转发的请求会在头部增加令牌信息，业务服务器可以通过该令牌信息对网关查询用户的登录信息。与部署方式一相比，采用部署方式二时，现有的业务服务器不需实现与网关服务器的频繁登录验证交互，网关服务器需要转发客户端请求。

访问请求

访问请求

客户端

网关服务器

业务服务器

图3 服务器部署二

# 5 系统API

网关服务器的http服务可访问固定端口。

## 5.1取随机数

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | getrand | | |
| 功能描述 | 获取随机数 | | |
| 参数 |  |  | |
| 返回值 | rand | | 产生的随机数 |
| ret | | 1：产生随机数成功 |
| 0：产生随机数失败 |
| errinfo | | 产生随机数失败原因 |

## 5.2登录

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | sm2certlogin | | |
| 功能描述 | 使用证书登录 | | |
| 参数 | rand | 由getrand产生的随机数，该随机数只能使用一次 | |
| cert | 用户证书实体，base64编码 | |
|  | signed | 已签名的信息 | |
| 返回值 | ret | | 1：登录成功 |
| 0：登录失败 |
| errinfo | | 失败原因：  parameter invalid：挑战字不存在  cert format invalid：证书格式错误；  the cert is not of sm2 type：证书类型错误；  cert was blacklisted：证书入黑名单；  cert usage wrong：证书用法错误；  the cert has expired：证书过期；  the cert was not issued by ca：该证书非注册的根证书签发；  issuer not found：根证书未在系统注册；  wrong sign：挑战字签名结果错误； |
|  | token | | 产生的sso登录令牌 |

## 5.3更新token

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | updatetoken | | |
| 功能描述 | 更新token过期时间 | | |
| 参数 | token | 登录令牌 | |
| 返回值 | ret | | 1：更新token成功 |
| 0：更新token失败 |
| errinfo | | 更新token失败原因 |

## 5.4登出

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | logout | | |
| 功能描述 | 用户登出 | | |
| 参数 | token | 登录令牌 | |
| 返回值 | ret | | 1：登出成功 |
| 0：登出失败 |
| errinfo | | 登出失败原因 |

## 5.5取token详情

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | gettokeninfo | | |
| 功能描述 | 取token详情 | | |
| 参数 | token | 登录令牌 | |
| 返回值 | ret | | 1：获取成功 |
| 0：获取失败 |
| errinfo | | 获取失败原因：  缺少token  token无效 |
| certsn | | 证书序列号 |
| logindate | | 登录日期 |
| subject | | 证书主题 |
| ip | | 登录ip |
| cert | | 证书实体 |

## 5.6签名存储

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | insert\_sign\_record | | |
| 功能描述 | 存储签名信息 | | |
| 参数 | appid | 业务系统模块编号 | |
| docid | 在用户的业务系统中的文档号 | |
| docname | 文档名称 | |
| textinfo | 签名内容（二进制内容需要进行base64编码） | |
| signdata | 签名结果（如果所签内容是二进制数据，需要在签名之前进行base64编码） | |
| signcert | 签名证书 | |
| signdate | 用户机器签名日期 | |
| 返回值 | ret | | 1：存储成功 |
| 0：存储失败 |
| errinfo | | 存储失败原因 |
| id | | 网关存储流水号，可据此在认证网关管理器中查找该签名内容 |
| svrtime | | 服务器签名时间 |
| svrsig | | 服务器签名结果 |
| svrcert | | 服务器证书 |
| clicert | | 客户端签名证书 |
| clisig | | 客户端签名结果 |
| timestamp | | 时间戳签名 |

## 5.7取用户证书详情

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | getcertinfo | | |
| 功能描述 | 取得用户证书详情 | | |
| 参数 | cert | 证书实体base64编码 | |
| 返回值 | ret | | 1：获取成功 |
| 0：获取失败 |
| errinfo | | 获取失败原因 |
| SN | | 证书序列号 |
| CN | | 国家 |
| OU | | 组织单位 |
| Subject | | 证书主题 |
| Notbefore | | 日期之前不生效 |
| Notafter | | 日期之后不生效 |
| is\_sm2cert | | 是否是SM2证书 |

## 5.8数据验签

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | verifysm2 | | |
| 功能描述 | 数据验签 | | |
| 参数 | text | 原文 | |
| cert | 签名证书，base64编码 | |
| signed | 签名结果 | |
| 返回值 | ret | | 1：验签成功 |
| 0：验签失败 |
| errinfo | | 存储失败原因 |

## 5.9数据签名

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | signsm2 | | |
| 功能描述 | 使用服务器签名证书对数据签名 | | |
| 参数 | text | 原文 | |
| 返回值 | ret | | 1：签名成功 |
| 0：签名失败 |
| errinfo | | 签名失败原因 |
| cert | | 签名证书 |
| signed | | 签名结果 |

## 5.10登录（支持RSA证书 和 SM2证书）

访问服务器<http://ip:port/ssoworker>

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | certlogin | | |
| 功能描述 | 使用证书登录 | | |
| 参数 | rand | 由getrand产生的随机数，该随机数只能使用一次 | |
| cert | 用户证书实体，base64编码 | |
|  | signed | 已签名的信息 | |
| 返回值 | ret | | 1：登录成功 |
| 0：登录失败 |
| errinfo | | 失败原因：  parameter invalid：挑战字不存在  cert format invalid：证书格式错误；  the cert is not of sm2 type：证书类型错误；  cert was blacklisted：证书入黑名单；  cert usage wrong：证书用法错误；  the cert has expired：证书过期；  the cert was not issued by ca：该证书非注册的根证书签发；  issuer not found：根证书未在系统注册；  wrong sign：挑战字签名结果错误； |
|  | token | | 产生的sso登录令牌 |

# 6功能测试

测试功能页面如下：



## 6.1 设置认证服务器

输入认证服务器地址，格式为：<http://ip:port/ssoworker>，输入完成后，点击“设为测试的认证网关”完成认证服务器设置；

## 6.2 获取随机数

用户登录时，服务器产生随机数，用户取得对随机数并对其签名，服务器验证签名。

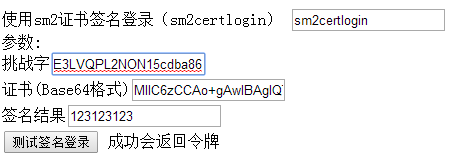


点击“获取随机数”按钮，得到获得随机数的结果：”ret”:”1”表示获得随机数成功；”errinfo”:’’”表示没有错误信息；rand:”QFM4NE3LVQPL2NON15cdba86”是获得的随机数。



## 6.3 签名登录

使用证书签名登录，在参数挑战字中输入获得的随机数，点击“测试签名登录”



显示登录结果，”ret”:”1”表示登录成功；”errinfo”:’’”表示没有错误信息；

”token”:” E0Y1V1MQ7RS9VWXWSUVJS67I2RSQQ6K415cdba88”是登录产生的登录令牌。



测试该功能时不验证证书是否有效，不检查签名结果。

## 6.4 更新令牌

令牌的有效时间是300s，从令牌产生的时刻起，经过300s后该令牌失效，如果需要重复使用该token，则需要在令牌失效前更新令牌，使令牌的有效起始时间更新。在令牌输入框中输入登录获得的令牌，点击“更新令牌”



显示更新结果，”ret”: ”1”表示更新成功；”errinfo”:”“表示没有错误信息；



## 6.5 获取令牌信息

在令牌输入框中输入登录获得的令牌，点击“返回登录信息”



显示获取结果，

{"ret":1, "errinfo":"","certsn":"4ff3b35b85327573761fb7b6998ce958","logindate":"20141125135841","ip":"20141125135841","sub":"C=CN,ST=辽宁,L=沈阳,O=沈阳,OU=@012345678955444,OU=市局,CN=服务器

","cert":""}

## 6.6 获取证书信息

在证书输入框中输入证书信息，点击“证书信息”



显示证书信息

{"ret":1, "errinfo":"","SN":"4ff3b35b85327573761fb7b6998ce958","CN":"服务器","OU":"市局","sub":"C=CN,ST=辽宁,L=沈阳,O=沈阳,OU=@012345678955444,OU=市局,CN=服务器","notbefore":"20140925165303","notafter":"20150925165303","is\_sm2cert":true}﻿

## 6.7 退出登录

在令牌输入框中输入令牌，点击“退出登录”



显示表示退出登录成功。退出后再用该令牌进行操作会提示登录失败{"ret":"0", "errinfo":"fail"}