

软件工程实训文档

北京交通大学

2017年7月

动态令牌认证系统

详细设计说明书

赵洲浩小组

成员：赵洲浩 刘晓宇 蒋小雨 孙林 王士昂

|  |  |
| --- | --- |
| 项目 | 动态令牌认证系统 |
| 文档 | 详细设计说明书 |
| 版本 | V 1.0 |
| 作者 | 赵洲浩组全体成员 |
| 最后更新时间 | 2017-07-08 |

版本更新概要

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 时间 | 更新人 | 更新摘要 |
| V1.0 | 2017-07-08 | 蒋小雨 | 初稿 |
| V1.1 |  |  |  |
| V1.2 |  |  |  |

目录

[1．引言 1](#_Toc506972944)

[1.1编写目的 1](#_Toc506972945)

[1.2项目背景 1](#_Toc506972946)

[1.3定义 1](#_Toc506972947)

[1.4参考资料 2](#_Toc506972948)

[2．总体设计 2](#_Toc506972949)

[2.1需求规定 2](#_Toc506972950)

[2.2软件结构 3](#_Toc506972951)

[3．程序描述 4](#_Toc506972954)

[3.1功能 4](#_Toc506972955)

[3.2输入项目 5](#_Toc506972956)

[3.3输出项目 5](#_Toc506972956)

[3.4算法 5](#_Toc506972956)

[3.5程序逻辑 5](#_Toc506972956)

[3.6接口 5](#_Toc506972956)

[3.7存储分配 5](#_Toc506972956)

[3.8限制条件 5](#_Toc506972956)

[3.9测试要点 5](#_Toc506972956)

# 1．引言

## 1.1编写目的

概要设计说明书根据动态令牌认证系统的特征、性能要求、可靠性要求、成本等方面的内容，针对产品使用的技术平台和软硬件架构，从总体上明确了系统的架构设计，以及系统各个功能模块设计、系统接口设计、数据库设计。

本概要设计说明书的目的就是进一步细化软件设计阶段得出的软件原貌，把它加工成在程序细节上非常接近与源程序开发的软件表示。

概要设计说明书预期读者：软件测试员、程序开发员、软件分析员

## 1.2项目背景

项目的委托单位：北京交通大学软件学院

项目开发单位： 北京交通大学软件学院赵洲浩组

项目主管部门： 北京交通大学软件学院赵洲浩组

动态令牌认证系统是根据专门的算法生成一个不可预测的随机数字组合，每个密码只能使用一次，成为最安全的[身份认证技术](http://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E8%AE%A4%E8%AF%81%E6%8A%80%E6%9C%AF)之一。动态令牌认证使用便捷，且与平台无关性，随着移动互联网的发展，[动态令牌认证技术](http://baike.baidu.com/item/%E5%8A%A8%E6%80%81%E5%8F%A3%E4%BB%A4%E6%8A%80%E6%9C%AF)已成为[身份认证技术](http://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E8%AE%A4%E8%AF%81%E6%8A%80%E6%9C%AF)的主流，被广泛应用于企业、网游、金融等领域。动态令牌认证系统是一种包含动态令牌和动态令牌认证综合系统，可以为应用系统提供动态令牌认证服务。

动态令牌认证系统由认证系统和密钥管理系统组成。动态令牌认证的设计思路是在登陆过程中加入不确定因素，使每次登陆过程中传递的信息都不相同, 从而提高信息系统的安全性。

## 1.3定义

下列术语和定义适用于本概要设计说明书。

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 描述 |
| 1.1 | 令牌 Dynamic Code Token | 即动态令牌，是生成并显示动态口令的载体 |
| 1.2 | 动态口令 Dynamic Password | 由令牌种子与其他数据，通过特定算法，运算生成的一次性口令。 |
| 1.3 | 静态口令 Static Password | 用户设置的，除非用户主动修改，否则不会发生变化的密码。该口令通常存储在认证系统中，用于配合动态口令使用。该口令也可由认证双方临时协商确定。 |
| 1.4 | SM3 | 国家密码管理局批准的杂凑算法。 |
| 序号 | 名称 | 描述 |
| 1.5 | SM5 |  |
| 1.6 | UTC时间 Universal Time Coordinated | 协调世界时(Universal Time Coordinated)英文缩写，是由国际无线电咨询委员会规定和推荐,并由国际时间局(BIH)负责保持的以秒为基础的时间标度，是距1970年1月1日00:00时(格林尼治标准时间)的秒数。 |
| 1.7 | 令牌种子 Token Seed | 即令牌密钥，用于与其他数据组装，通过特定算法运算获得动态口令，同时存储于令牌和认证系统中. |
| 1.8 | 认证系统 Authentication System | 能够为应用系统提供动态口令身份认证服务的系统。 |
| 1.9 | 密钥管理 Key Management | 对种子密钥的生成、传输和存储的安全管理，种子密钥是否安全直接影响到整个认证系统是否安全。 |
| 2.0 | 密钥 Key | 一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的数据。 |
| 2.1 | 接口 Interface | 两个不同系统(或子程序)交接并通过它彼此作用的部分。 |

## 1.4参考资料

《软件配置管理计划说明书》

《软件质量保证计划指导书》

《北京交通大学开发流程和标准》

《北京交通大学编码规范》

《动态令牌认证系统需求规格说明书》

# 2．总体设计

## 2.1需求规定

1. 基于现在静态密码认证技术的的不安全性，例如：容易被他人所盗取密码、密码根据用户的水平不同而难易程度不一。
2. 基于现在最发达的生物特征识别技术（指纹、虹膜等的识别技术）的局限性，例如：指纹被破坏等不可抗力。
3. 动态令牌认证技术采用一次一密（One Time Password）的技术，使得动态令牌认证系统成为现在世界上最安全的身份认证方式之一。
4. 由于本系统将会应用在个人隐私或者一些机密领域，因此可靠性要强，安全性要高，要有定期备份数据的功能，还要在数据的通信过程中进行严格的加密措施。

## 2.2软件结构

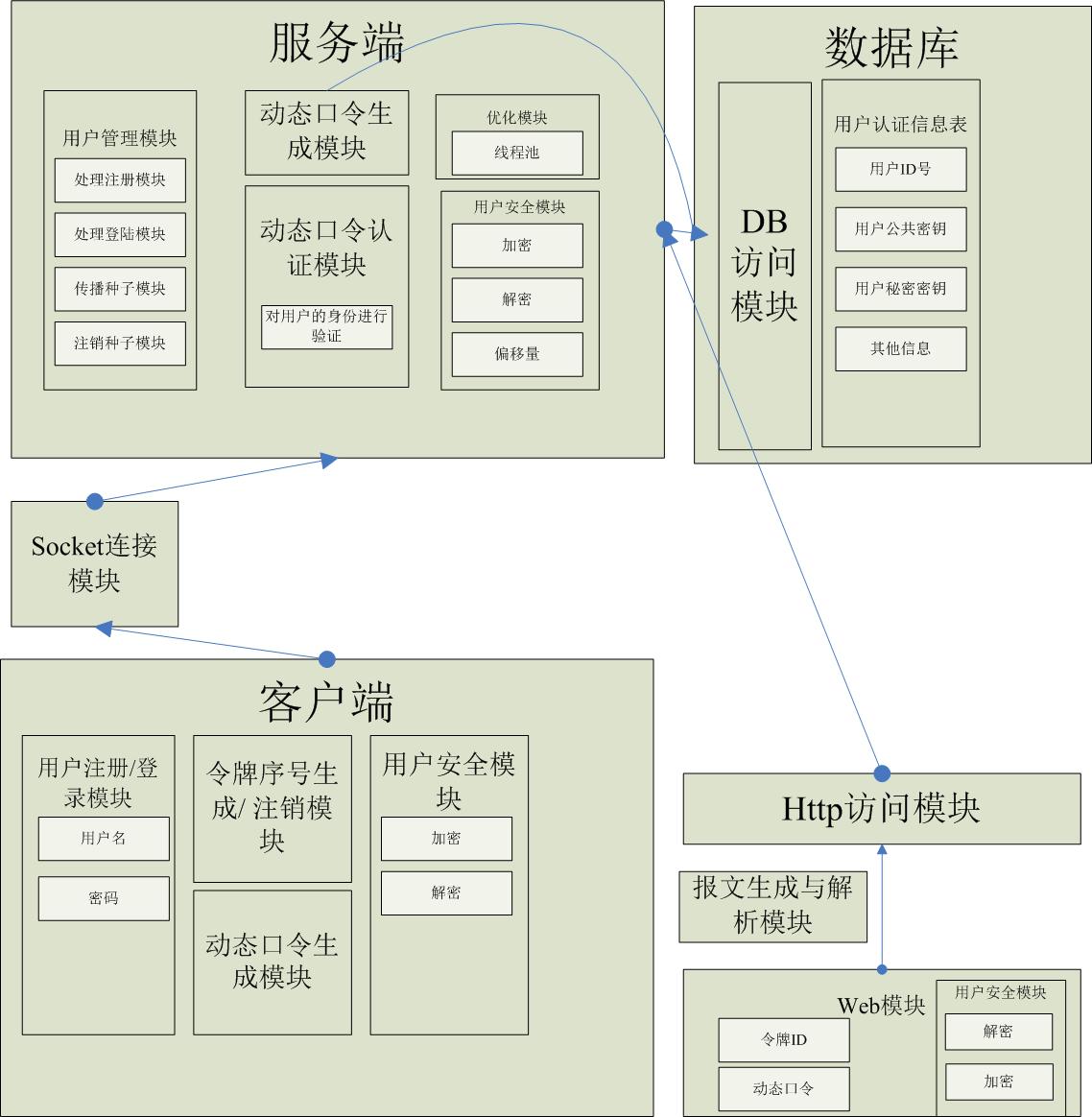


图2-2-1

动态令牌认证系统涉及到用户、服务器、浏览器验证，以及涉及到服务器与客户端之间的通信，因此在系统的总体设计上采取多层的架构设计。

**表2-2-2 层次结构与模块设计**

|  |  |  |
| --- | --- | --- |
| 客  户  端 | View层 | 登录/注册、令牌生成/注销、动态口令显示、返回信息 |
| Logical层 | 用户信息判断、动态口令生成、用户功能/动态令牌/注销 |
| Transport层 | Socket连接、信息处理、加密 |
| Storage层 | 日志管理、种子存储 |
| Web端 | View层 | 令牌/动态验证码、返回信息 |
| Transport层 | HTTP连接、加密 |
| 服  务  器 | Logical层 | 动态口令生成/加密、Client处理、Web处理 |
| Transport层 | Socket连接、加密、线程池 |
| Storage层 | 日志管理 |

# 3．程序描述

## 3.1 注册

3.1.1功能

实现登录/注册界面，用户在此界面中输入用户名和静态密码，判断输入是否为空。

3.1.2输入项目

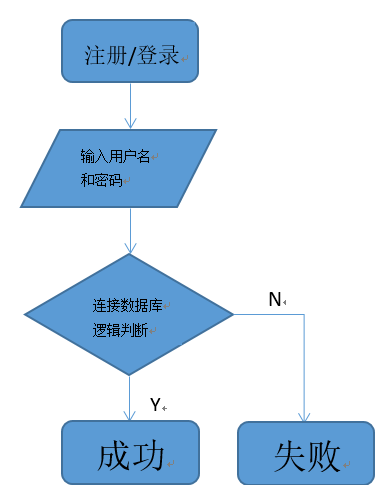
在注册页面填写注册信息，要求填写用户名，密码，确认密码，进行注册。

3.1.3输出项目

提交注册信息时，有必填项未填写或格式不正确时，提示用户正确填写相应项，当注册失败时在注册页面显示“注册失败！”。当所有信息填写正确，提交表单，注册成功跳转到登录页面，如果程序出现异常则跳转到异常页面。

3.1.4算法

3.1.5程序逻辑



3.1.6接口

3.1.7存储分配

3.1.8限制条件

用户名（必填，4~20个汉字、字母、数字或下划线组成的字符串，且不能有重名注册）

密码（必填，6~12个字符）

确认密码（和密码保持一致）

3.1.9测试要点

数据库连接情况：正常情况，数据库文件缺少，外部系统异常。 系统设置获取：正常情况，外部系统异常。

对用户输入的响应： 合法输入，能够正常调用子模块； 非法输入，系统能否辨别，并作出响应(提出警告)；

## 3.2 登陆

3.2.1功能

实现登录/注册界面，用户在此界面中输入用户名和静态密码，判断输入是否为空。

3.2.2输入项目

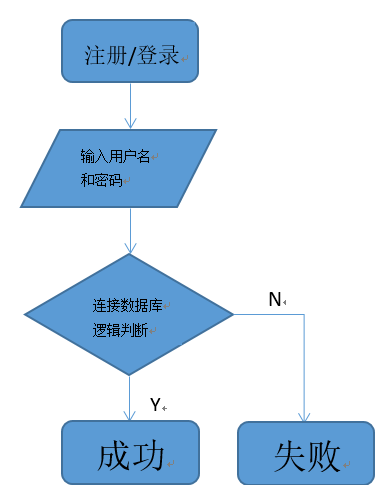
在登陆页面填写用户信息，要求填写用户名，点击“登录”按钮进行登录。

3.2.3输出项目

用户名或密码为空则在登录页面给出错误提示。登录失败时在登录页面提示“用户名或密码错误！”登录成功跳转到主界面，并显示当前登录用户名。

3.2.4算法

3.2.5程序逻辑



3.2.6接口

3.2.7存储分配

3.2.8限制条件

用户名（必填，按照注册时的正确信息填写，4~20个汉字、字母、数字或下划线组成的字符串，且不能有重名注册）

密码（必填，按照注册时的正确信息填写，6~12个字符）

3.2.9测试要点

数据库连接情况：正常情况，数据库文件缺少，外部系统异常。 系统设置获取：正常情况，外部系统异常。

对用户输入的响应： 合法输入，能够正常调用子模块； 非法输入，系统能否辨别，并作出响应(提出警告)；

## 3.3 生成令牌

3.3.1功能

实现令牌生成界面，用户在此界面中点击生成用户自己的令牌。

3.3.2输入项目

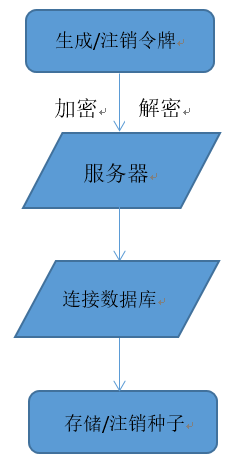
点击生成用户自己的令牌，生成令牌

3.3.3输出项目

生成令牌

3.3.4算法

3.3.5程序逻辑



3.3.6接口

3.3.7存储分配

3.3.8限制条件

客户端令牌采用md5进行加密，将加密后的密文提交给服务器校验，服务器采用同样加密算法。

3.3.9测试要点

数据库连接情况：正常情况，数据库文件缺少，外部系统异常。 系统设置获取：正常情况，外部系统异常。

对用户输入的响应： 合法输入，能够正常调用子模块； 非法输入，系统能否辨别，并作出响应(提出警告)；

## 3.4 注销令牌

3.4.1功能

实现令牌注销界面，用户在此界面中点击注销已经存在的令牌。

3.4.2输入项目

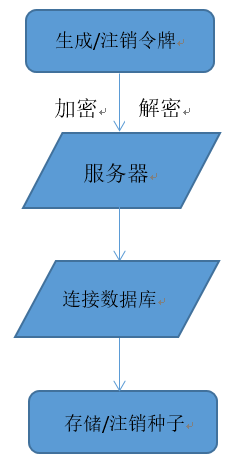
点击注销用户自己的令牌，注销令牌

3.4.3输出项目

注销令牌

3.4.4算法

3.4.5程序逻辑



3.4.6接口

3.4.7存储分配

3.4.8限制条件

客户端令牌采用md5进行加密，将加密后的密文提交给服务器校验，服务器采用同样加密算法。

3.4.9测试要点

数据库连接情况：正常情况，数据库文件缺少，外部系统异常。 系统设置获取：正常情况，外部系统异常。

对用户输入的响应： 合法输入，能够正常调用子模块； 非法输入，系统能否辨别，并作出响应(提出警告)；

## 3.5 获取动态口令

3.5.1功能

实现动态口令显示界面，用户在此界面中可以看到动态口令。

3.5.2输入项目

点击生成用户自己的令牌后，等待。

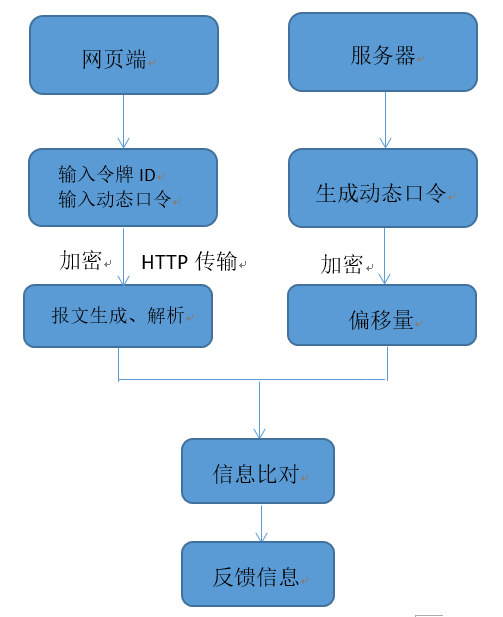
3.5.3输出项目

显示动态口令，动态口令每60s更新一次。

3.5.4算法

基于时间的同步口令

3.5.5程序逻辑



3.5.6接口

3.5.7存储分配

3.5.8限制条件

3.5.9测试要点

数据库连接情况：正常情况，数据库文件缺少，外部系统异常。 系统设置获取：正常情况，外部系统异常。

对用户输入的响应： 合法输入，能够正常调用子模块； 非法输入，系统能否辨别，并作出响应(提出警告)；

## 3.6 认证动态口令

3.6.1功能

对比加密信息是否一致，并进行信息会回馈。

3.6.2输入项目

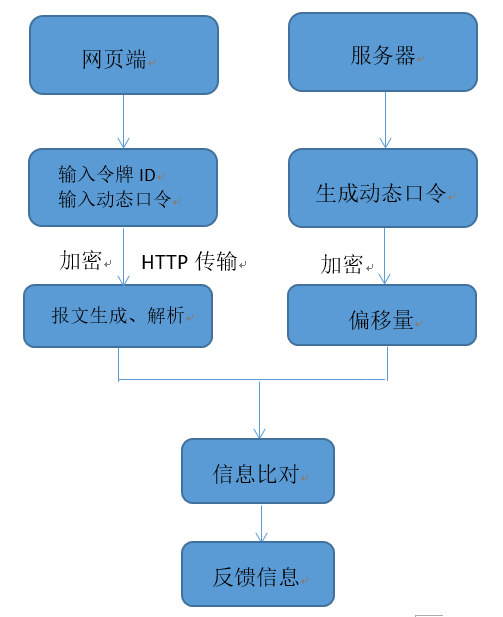
在Web端输入令牌ID与动态口令，点击验证。

3.6.3输出项目

令牌ID与动态口令输入正确，验证成功；令牌ID与动态口令输入正确，超时，提示验证超时；令牌ID或动态口令输入错误，提示令牌ID或动态口令输入错误.

3.6.4算法

3.6.5程序逻辑



3.6.6接口

3.6.7存储分配

3.6.8限制条件

通过增大偏移量的技术（前后10分钟）来进行同步，确保其能够继续使用，降低对应用的影响，但对于超出默认（共20分钟）的时间同步令牌，将无法继续使用或进行远程同步，必须另行处理。同样，对于基于时间同步的服务器，应较好地保护其系统时钟，不要随意更改，以免发生同步问题，从而影响全部基于此服务器进行认证的令牌

3.6.9测试要点

数据库连接情况：正常情况，数据库文件缺少，外部系统异常。 系统设置获取：正常情况，外部系统异常。

对用户输入的响应： 合法输入，能够正常调用子模块； 非法输入，系统能否辨别，并作出响应(提出警告)；