

软件工程实训文档

北京交通大学

2017年7月

动态口令

软件需求规格说明书

最可爱的小组

|  |  |
| --- | --- |
| 项目 | 动态口令 |
| 文档 | 软件需求规格说明书 |
| 版本 | V1.2 |
| 作者 | 赵洲浩 蒋小雨 刘晓宇 孙林 王士昂 |
| 最后更新时间 | 2017-07-07 |

版本更新概要

|  |  |  |  |
| --- | --- | --- | --- |
| 版本号 | 时间 | 更新人 | 更新摘要 |
| V1.0 | 2017-07-06 | 蒋小雨 | 初稿 |
| V1.1 | 2017-07-07 | 蒋小雨 | 文档格式规范化整理 |
| V1.2 | 2017-07-08 |  | 调整了专业术语的部分定义 |

目录

[1 引言 1](#_Toc487189315)

[1.1 编写目的 1](#_Toc487189316)

[1.2 项目背景 1](#_Toc487189316)

[1.3 定义 1](#_Toc487189316)

[1.4 参考资料 1](#_Toc487189316)

[2 任务概述 1](#_Toc487189315)

[2.1 编写目的 1](#_Toc487189316)

[2.2 运行环境 1](#_Toc487189316)

[2.3 条件与限制 1](#_Toc487189316)

[3 功能需求 1](#_Toc487189315)

[3.1 功能和权限分析 1](#_Toc487189316)

[1.1.1 1](#_Toc487189317)

[2.2 功能描述 1](#_Toc487189316)

[1.1.1 1](#_Toc487189317)

[4 性能需求 1](#_Toc487189315)

[4.1 数据精确度 1](#_Toc487189316)

[4.2 功能描述 1](#_Toc487189316)

[4.3 适应特性 1](#_Toc487189316)

[4.4 时间特性 1](#_Toc487189316)

[4.5 可使用性 1](#_Toc487189316)

[4.6 安全保密性 1](#_Toc487189316)

[4.7 可维护性 1](#_Toc487189316)

[5 其他需求 1](#_Toc487189315)

[附录 A 3](#_Toc487189318)

1 引言

1.1 编写目的

1. 编写本文档的目的是明确用户需求，在最终用户和开发者之间达成对软件产品要求的共用理解，作为项目开发的目标，为软件概要设计提供指导，并作为软件测试的依据。
2. 本规范规定了动态口令系统，动态口令生成方式，动态令牌特性，认证系统，密钥管理系统的相关内容。
3. 本文档的读者是最终用户代表、高级项目经理、项目经理、项目组成员、测试组成员、质量保证组成员。

1.2 项目背景

动态口令（Dynamic Password）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，目前已经被越来越多的行业所应用。由于它使用便捷，且与平台无关性，随着移动互联网的发展，[动态口令技术](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。动态口令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口令认证服务。

动态令牌认证系统由认证系统和密钥管理系统组成。动态口令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

|  |  |  |
| --- | --- | --- |
| 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

1. 软件配置管理计划指导书
2. 软件质量保证计划指导书
3. 北京交通大学开发流程和标准
4. 北京交通大学编码规范

2 任务概述

2.1 目标

本系统采用了时间同步的机制来实现动态口令技术，基于window与linux操作系统，编写一个动态口令认证系统。

2.2 运行环境

|  |  |
| --- | --- |
| 运行环境 | 描述 |
| 客户端运行环境 | 软件环境：  操作系统：Windows系列  浏览器程序： 浏览器IE 5.0以上  硬件环境：  网络接入设备（网卡,modem,adsl,isdn或其他网络接入设备）。 |
| 服务器端运行环境 | 软件环境：  操作系统：Linux(Redhat 7.0以上)系列,Unix系列或Windows 2000服务 器版  应用服务器程序：  Weblogic 6.0，Websphere 4.0及以上版本等。 |
| 数据库服务器运行环境 | 软件环境：  **操作系统：**Linux(Redhat 7.0以上)系列,Unix系列或Windows 2000服务器 版等操作系统。  数据库： Oracle8i,DB2,Sybase,SQLserver7.0等。 |

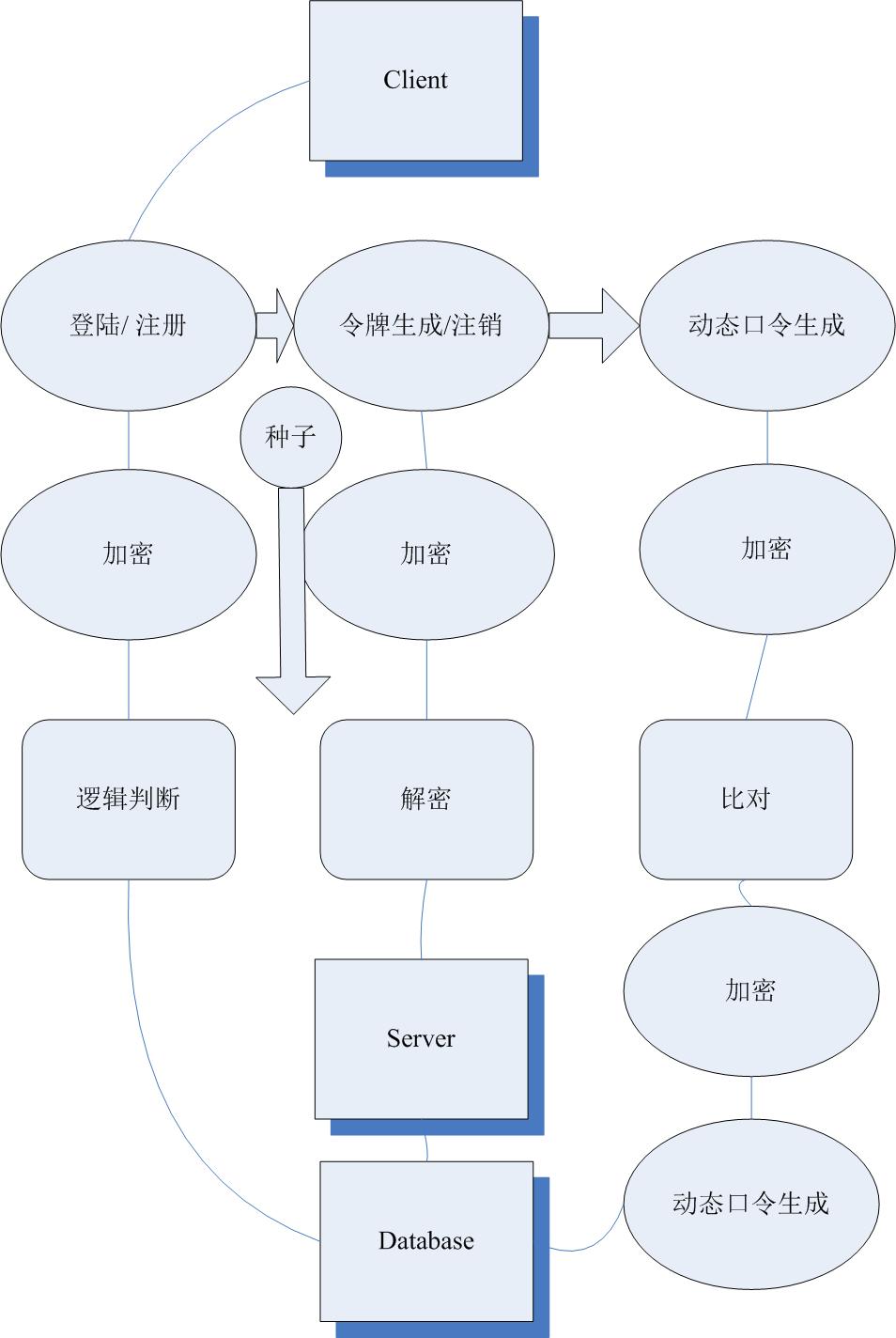
2.3 条件与限制

|  |  |
| --- | --- |
| 条件 | 限制 |
| 掌握基础知识 | 时间紧张 |
| 具有项目开发经验 |
| 具有良好的沟通技巧 |

3 功能需求

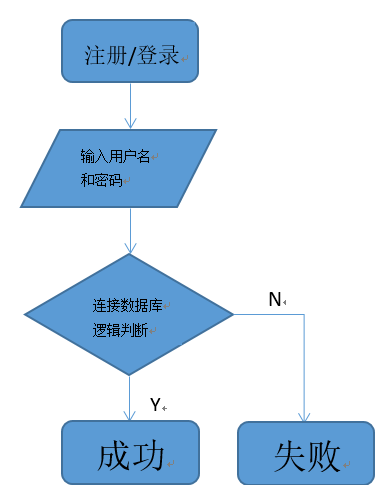
3.1 功能和权限划分

3.1.1 权限划分图

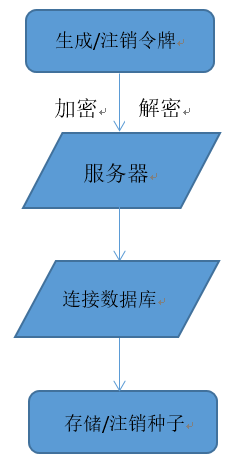


3.1.1.1 权限划分图

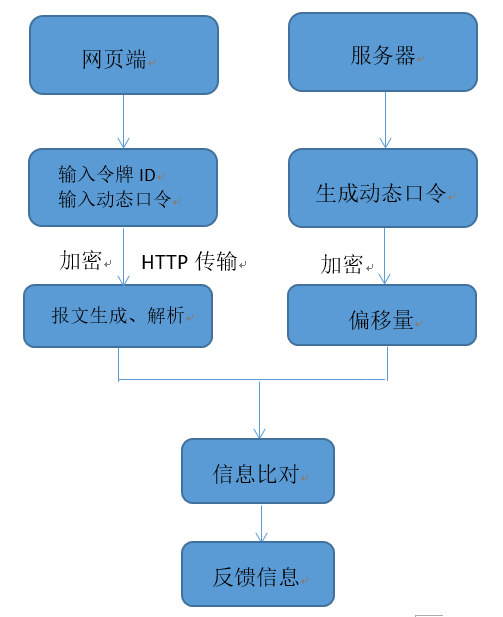
3.1.2 功能流程图



3.1.2.1 登陆注册流程图



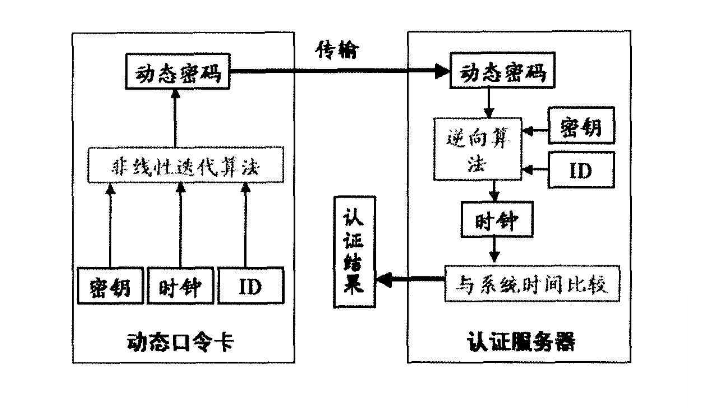
3.1.2.2 生成注销令牌流程图



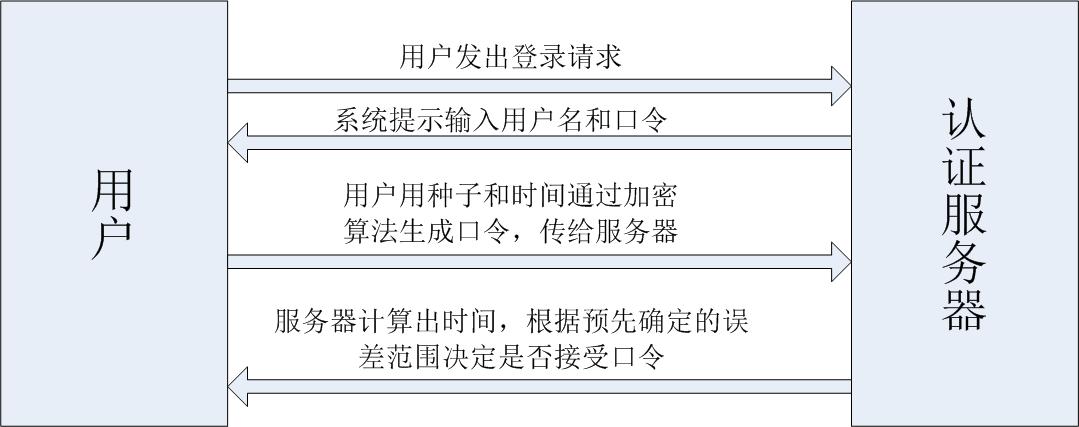
3.1.2.3网页与服务器通讯流程图

3.2 功能描述

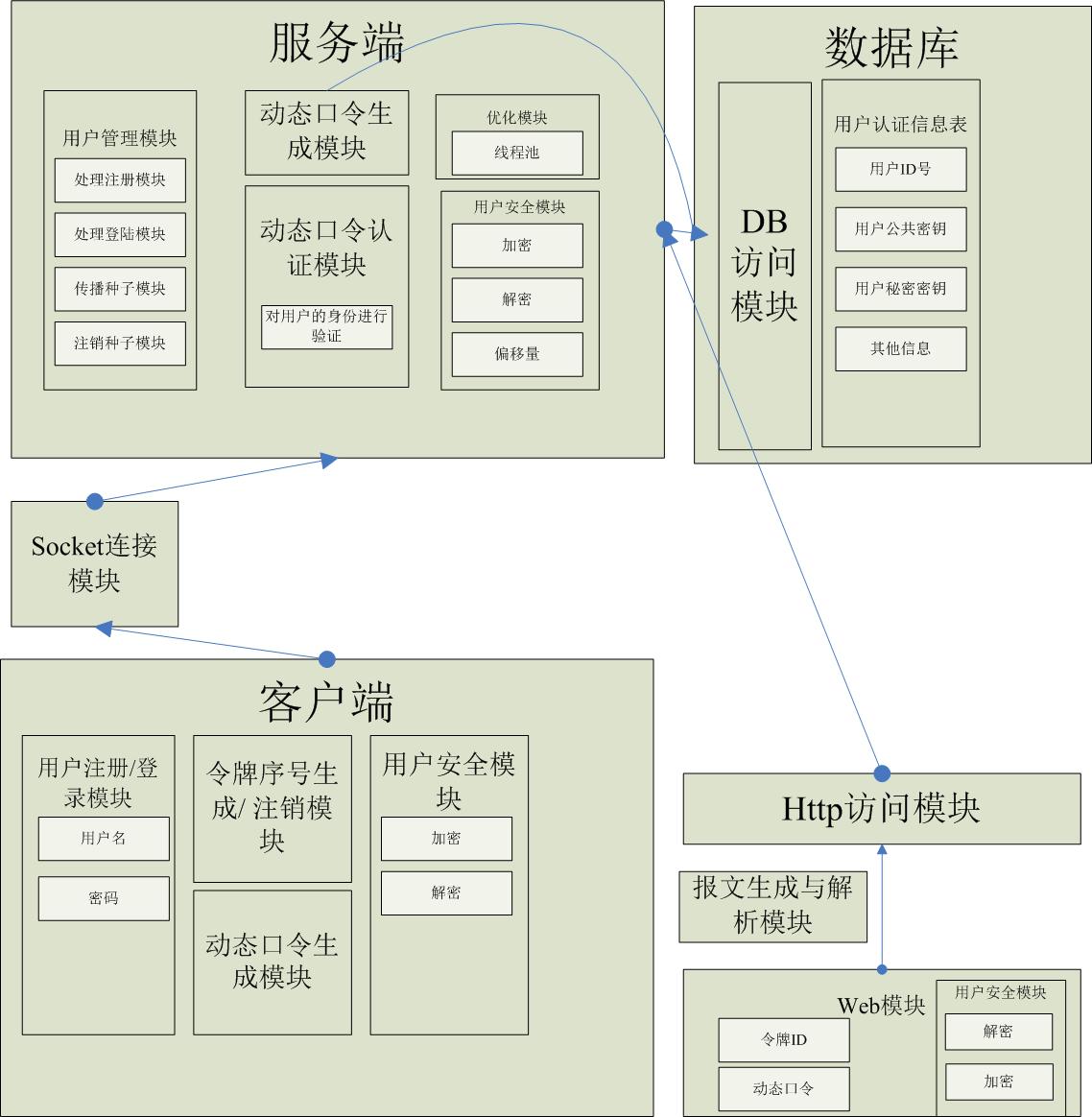
3.2.2 系统功能描述



3.2.1.1 动态口令认证图



3.2.1.2 客户端和服务器交互图



1. 用户登录/注册模块

该模块负责系统的用户登录/ 注册认证。

1. 用户管理模块

该模块负责处理注册、登陆、传播与注销种子

1. 动态口令生成模块

该模块主要用于生成动态口令。

1. 动态口令认证模块

该模块的功能是对比加密信息是否一致，并进行信息会回馈。

1. 令牌序号管理（生成/注销）模块

该模块的功能是根据序号生成规则生成动态令牌的唯一序列号。

1. 用户安全模块

该模块主要对动态口令进行加密、解密等操作。

1. Socket连接模块

该模块的功能完成客户端与服务器之间的通讯。

1. http访问模块

该模块的功能是完成web端与服务器之间的通讯。

1. DB访问模块

该模块的功能是完成数据库与服务器之间的通讯。

1. 报文生成与解析模块

3.2.2 系统功能分级

|  |  |  |  |
| --- | --- | --- | --- |
| 身份 | 模块 | 功能点 | 需求分级 |
| 服务端 | 用户管理模块 | 传播种子 | A |
| 注销种子 | A |
| 用户账号和角色的分配、修改和删除 | A |
| 动态口令生成模块 | 生成动态口令 | A |
| 动态口令认证模块 | 认证动态口令 | A |
| 用户安全模块 | 加密 | A |
| 解密 | A |
| 偏移量 | A |
| 优化模块 | 线程池 | B |
| 客户端 | 用户登录/注册模块 | 注册用户 | A |
| 登录用户 | A |
| 令牌序号管理（生成/注销）模块 | 生成令牌 | A |
| 注销令牌 | A |
| 动态口令生成模块 | 生成动态口令 | A |
| 用户安全模块 | 加密 | A |
| 解密 | A |
| 偏移量 | A |
| Web端 | 用户安全模块 | 加密 | A |
| 解密 | A |
| 偏移量 | A |
| 通讯 | Socket模块 | | A |
| http访问模块 | | A |
| 报文生成与解析模块 | | A |

4 性能需求

4.1 数据精确度

(1)确保用户输入的数据不乱码；兼容度高；重要数据需要高精确度。

(2)在精度需求上，根据实际需要，数据在输入、输出及传输的过程中要满足各种精度的需求根据关键字精度的不同。

(3)时间同步方式的难点在于对双方的时间精准度要求较高，需要解决用户和服务器之间时钟偏移的问题。

4.2 时间特性

网页刷新时间短；响应时间短；登录/注册时间短；尽量避免用户长时间等待。

4.3 适应性

(1)系统算法兼容性：能够支持多种分组密码算法来对密钥的管理。

(2)浏览器的兼容性：在操作方式、运行环境、软件接口或开发计划等发生变化时，应具有适应能力。

4.4 可使用性

(1) 操作界面简单明了，易于操作

(2) 对格式和数据类型限制的数据，进行验证，包括客户端验证和服务器验证

(3) 采用错误提醒机制，提示用户输入正确数据和正确的操作系统。

(4) 采用时间同步的方式，减少了用户和系统交互的次数，不需要专用的读入设备，免去了耗时复杂的认证过程。

4.5 安全保密性

只有合法用户才能登录使用系统，对每个用户都有权限设置。对登录名、密码、以及用户重要信息进行加密，保证账号信息安全。

|  |  |  |
| --- | --- | --- |
| 序号 | 安全性 | 描述 |
| 1 | 接入端控制 | 认证服务器应具有控制应用服务器安全接入的方法和措施。  认证服务器应具有时间校准的处理方法和措施。 |
| 2 | 信息存储加密 | 认证系统中的种子密钥是加密存储的，当认证服务器接收到认证请求时，认证服务器会首先读取种子密钥加密密钥密文，调用加密机或加密卡的接口使用主密钥解密种子密钥加密密钥密文，然后读取种子密钥密文，再使用种子密钥加密密钥解密种子密钥，通过种子密钥和时间因子等信息生成对应的动态密码，并与接收到的动态密码进行比较，从而完成动态密码身份验证。 |
| 3 令牌安全性控制 | | |
| 3.1 | 锁定及解锁 | 可以按照用户要求提供锁定机制，当一个令牌连续尝试认证失败次数累计达到上限，则对令牌进行锁定，同时提供人工解锁和自动解锁机制。 |
| 3.2 | 防重复认证 | 重复认证检测，对于已经通过认证的动态密码，认证服务器将予以作废，只要已经通过认证的动态密码，均不能再次通过认证。  对于特定的使用场景，可允许正确的动态口令一定次数范围内的重复使用，但认证系统必须具备保护此环境下身份认证安全性和有效性的机制。 |
| 3.3 | 日志安全 | 日志信息应具有校验码，只要用户对日志信息进行修改，就可通过校验码检查出来。  敏感数据应具有备份恢复机制。  认证系统针对日志访问应具备相应的访问控制策略，对日志的操作应有对应记录，以保证日志的完整性和安全性。 |
| 4 | 认证系统安全 | 认证系统安全必须符合目标应用服务或系统的安全需求，具体可参照目标应用服务或系统的相应规范或标准。 |

4.6 可维护性

(1) 系统采用了记录日志，用于记录用户的操作及故障信息

(2) 本系统采用的C /S模式，结构清晰

5 其他需求

5.1 界面设计

5.1.1 风格的一致性

界面的一致性既包括使用标准的控件，也指相同的信息表现方法，如在字体、标签风格、 颜色、术语、显示错误信息等方面确保一致。

|  |  |  |
| --- | --- | --- |
| 序号 | 分类 | 描述 |
| 1. | 在不同分辨率下的美观程度 | 软件界面要有一个默认的分辨率，而在其他分辨率下也可以运行，分别在 800×600， 1024×768，1280×768，1280×1024，1200×1600 分辨率下的大字体、小字体下的界面表现。 |
| 2. | 界面布局要一致 | 如所有窗口按钮的位置和对齐方式要保持一致。 |
| 3. | 界面的外观要一致 | 如控件的大小、颜色、背景和显示信息等属性要一致，一些需要特殊处理或有特殊要求 的地方除外。 |
| 4. | 界面所用颜色要一致 | 颜色的前后一致会使整个应用软件有同样的观感，反之会让用户觉得所操作的软件杂乱 无章，没有规则或言。 |
| 5. | 操作方法要一致 | 如双击其中的项，触发某事件，那么双击任何其他列表框中的项，都应该有同样的事件 发生。 |
| 6. | 控件风格、控件功能要专一 | a.不错误的使用控件  例如使用 Button 样式做 Table 的功能，拿主菜单条显示版权信息等  b.一个控件只做单一功能，不复用  如果在特殊情况下出现复用的时候，可采用以下两种方法解决：  \* 分组，使用双份控件  \* 使用 Table 页，给用户很明显的视觉变化 |
| 7. | 标签和讯息的措词要一致 | 如在提示、菜单和帮助中产生相同的术语。 |
| 8. | 标签中文字信息的对齐方式要一致 | 如某类描述信息的标题行定为居中，那么其他类似的功能也应该与此一致。 9.快捷键在各个配置项上语义保持一致 |

附录 A

无