

“电子公文传输系统”项目需求说明书

“电子公文传输系统”项目需求说明书

1 引言

1.1 编写目的

本小组依照课程要求开发项目“电子公文传输系统”，该系统利用了计算机网络和安全技术，实现政府部门与部门之间、单位与单位之间，对政府红头文件的起草、制作、分发、接收等功能，以达到政府机关内部电子公文替代纸质公文，实现安全、高效、无差错传输公文。

本说明适用对象：软件开发人员（Suppliers）。

1.2 背景

为响应环保政策、提高办公效率，政府机关正在大力推广“无纸化办公”，对实现电子公文传输的需求应运而生。电子公文传输系统需要满足的基本需求有：线上起草文件、制作电子公文、分发电子公文、接收电子公文等功能。同时，由于政府机关单位工作的特殊性，电子公文文件必须具有保密性、严肃性和不可抵赖性的特性，也要求系统保证电子公文的安全性。部分电子公文有很强的及时性，需要保证电子公文传输的高效性。针对不同年龄段、不同文化水平的政府办公人员，设计系统操作时需力求简洁、方便，满足操作的简便性。

1.3 定义

表1 术语、缩略语说明

术语、缩略语	解释
EDTS	电子公文传输系统 Electronic document transfer system

1.4 参考资料

列出用得着的参考资料，如：

- a. 本项目的经核准的计划任务书或合同、上级机关的批文；
- b. 属于本项目的其他已发表的文件；
- c. 本文件中各处引用的文件、资料、包括所要用到的软件开发标准。列出这些文件资料的标题、文件编号、发表日期和出版单位，说明能够得到这些文件资料的来源。

2 任务概述

2.1 目标

电子公文传输系统面向党政系统、各行政职能部门、企事业单位以及高校等对公文传输有较大需求的主体开发，可以提供安全保密的电子公文的发布、查询、传输、接收等功能。

系统开发分为前端、后端，分别对应用户Web端和服务端。系统基于B/S架构进行开发设计，用户通过网页浏览器进行访问。

2.1.1公文发布和上传

系统需要支持电子公文的发布、上传。在公文完成编辑后，需要上传到本系统随后进行公文的安全传输。上传和发布时可以指明公文的文号、单位、人员等相关信息。同时可以将公文按照不同类别进行分类。

2.1.2公文查询和管理

对于已经上传的公文，可以进行分类查询、公文的删除、设置接收公文对象等管理操作。对于已发布的文件，系统管理员统一管理所有已发布的文件，其他用户只能对自己发布的文件进行管理。

2.1.3公文的安全传输

公文在进行传输的过程中需要确保安全性，系统使用国密SM族算法确保传输过程中的保密性，身份的可验证性等。

2.1.4公文接受和签收

对于传输完成的公文，相应的接收单位需要进行验证和签收，完成整个传输过程，同时更新公文的传输状态，确保可以确认公文已经完成传输和签收。

2.2 用户类型

系统用户可以分为发文管理员、普通阅读者、系统管理员三类。

2.2.1发文管理员

管理员具有最高权限，在具有公文的上传发布、删除等权限。此类用户需要具有发布公文的权限和能力。用户需要具有基础的浏览器和文件操作能力。

2.2.2普通阅读者

普通阅读者用户可以进行公文的接收和阅读操作，但不能进行公文的发布。此类用户具有公文的阅读权限。用户需要具有基础的浏览器和文件操作能力。

2.2.3系统管理员

系统管理员可以进行系统的维护和管理，管理员需要确保系统能被各类用户正常使用。同时，系统管理员具有系统的高权限，可以增加，查看，删除，修改用户信息和列表，更改用户权限。此类用户需要具有信息安全基础知识，以及Web前、后端开发和问题排查的相关能力。

2.3 用户场景

用户

1. 公文草拟：根据自身需要进行公文的撰写，可与公文格式一同设计。
2. 公文格式：根据不同公文的密级、紧急程度不同制作不同的红头模板。
3. 公文上传：在安全登录的情况下，成功登陆的人员可将需要处理的公文上传至电子公文系统。
4. 公文下载：对用户的权限进行验证，验证成功则可对当前等级及以下的公文进行下载。
5. 公文发送：根据所要发送的对象、密级、紧急程度等对文件进行分类，再加密传送。
6. 公文接收：根据文件的密级，发送单位将文件分类，判断安全后进行解密。
7. 公文管理：登录者可根据自己的需求对公文进行分类归档。
8. 公文查询：根据签发部门，密级，紧急程度等查询公文。
9. 公文浏览：验证权限后可浏览相应密级的公文。

管理员

1.权限管理

- (1) 用户：可修改自己的登录密码、用户名等信息。（根据级别高低分配用户权限）
- (2) 管理员：可对系统用户信息进行增删查改的操作，可根据系统需求发布公告。

2.文件管理

- (1) 修改文件：管理员可对所有使用者用户发布的文件进行修改。
- (2) 查询文件：管理员可查询所有发布和接收的公文。
- (3) 文件列表：管理员可进入后台选择文件列表，查看用户发布及签收文件的情况。

3.配置管理

- (1) 字号管理：用于初始化、增加、删除和修改公文的字号。
- (2) 字号关联：用于设置使用者用户与公文字号的关联。每个机关单位只能使用特定范围的公文字号，通过设置用户和字号关联，减少操作错误，方便系统使用。

4.日志管理

日志管理包括系统的日志记录和查看模块，日志记录由系统在用户操作过程中自动生成，管理员可在系统中查看日志记录。

2.4 系统特点

- **标准化公文版式** 本系统采用国家公文的标准化格式，实现各单位之间以电子的方式进行公文流转。（参见《国家行政机关公文格式》，政府办公 13 种标准公文样式。）
- **不可更改的电子公文格式** 在点击科技公文传输管理系统中,进行转输的公文均转换成统一格式，从而保证公文传输过程中公文的完整性，并限制拷贝和打印。
- **强大的文档管理和监控功能** 公文传输管理系统具有强大的电子文档管理功能，包括公文扫描处理、全文检索（具有中文全文检索能力，包括任意字词检索和位置逻辑检索）、文档管理等。同时还对交换公文、信息发送、接收情况进行统计，对要求回复的公文的回复情况进行监控，起到监管和督促的作用。
- **良好使用性** 系统基于 B/S 构建，支持 IE 浏览器直接访问，由专业设计人员进行界面设计，具有较好使用性。
- **良好扩展性** 系统具有良好的扩展性，在充分考虑未来信息与业务增长需要的基础上，预留与上下级政府部门的公文与信息交换系统接口，为最终实现统一的电子政府打下基础。
- **多种安全手段** 数据在网络上加密传输或对关键数据加密存贮；数据的完整性，保证数据不被篡改和窃取；访问控制及身份认证，对用户访问应用和信息资源提供访问控制。
- **电子印章** 将待盖章的电子公文正文和其相应的红头及电子印章结合成一个正式的公文，然后使用透明的图像技术将电子印章加盖在公文上。
- **可视化公文浏览和打印** 所见即所得的公文浏览和打印，实现电子公文和纸质公文的同质转换。
- **良好的兼容性** 系统兼容各种 OA 系统，无需对现有 OA 系统工作流程做任何修改便可直接接入系统。
- **可靠性、高性能** 系统经过严格的质量测试审核。支持集群，响应速度快，能对访问进行负载均衡。目前系统支持同时在线用户达到 100 人时平均访问响应小于 20 秒

2.4 假定和约束

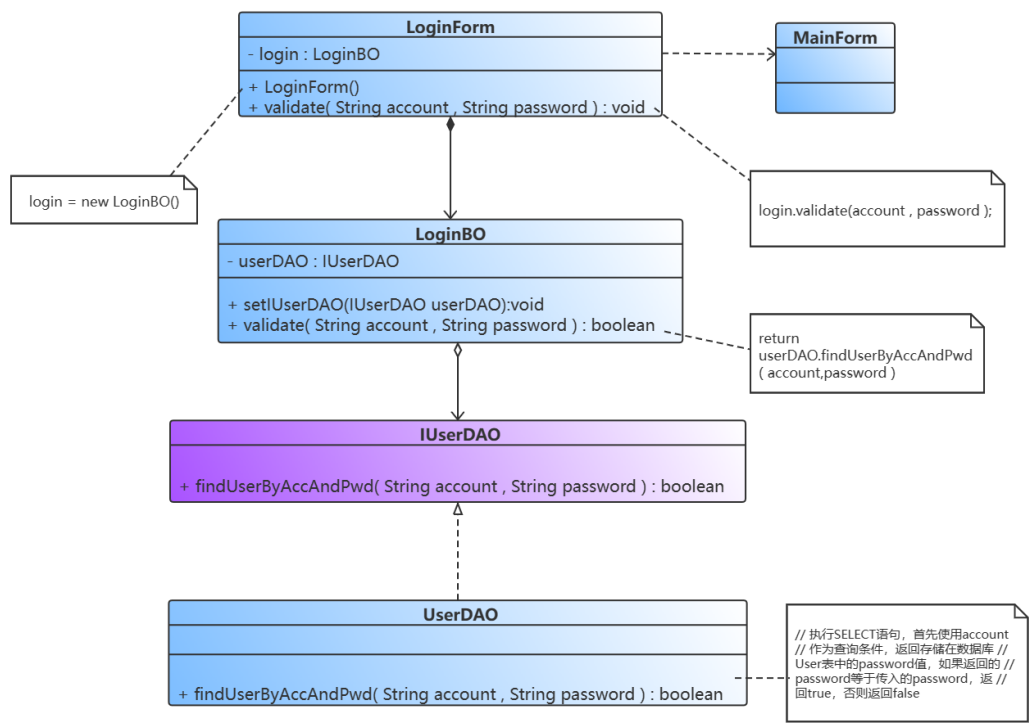
开发由小组所有成员完成，在信息安全系统课程和老师的指导下进行开发，开发期限本课程周等本系统为课程小组练习，无开发经费需求。

2.5 类图

在这里将类图分为登录功能与传输接收功能两大部分

2.5.1 登录功能类图

登录模块功能描述如下：
用户通过登录界面(LoginForm)输入账号和密码，系统将输入的账号和密码与存储在数据库(User)表中的用户信息进行比较，验证用户输入是否正确。如果输入正确则进入主界面(MainForm)，否则提示“输入错误”。



类说明：

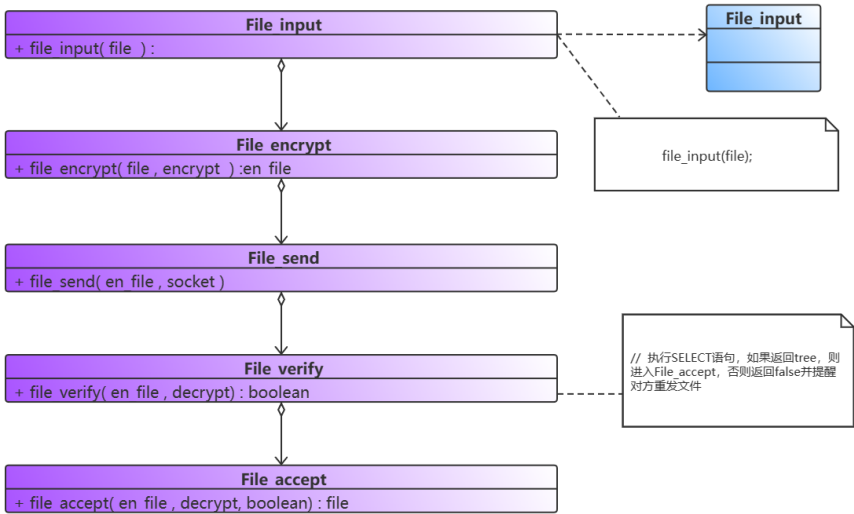
类 名	说 明
LoginForm	登录表单，省略界面组件和按钮事件处理方法（边界类）
LoginBO	登录业务逻辑类，封装实现登录功能的业务逻辑（控制类）
IUserDAO	抽象数据访问类接口，声明对User表的数据操作方法，省略除查询外的其他方法（实体类）
UserDAO	具体数据访问类，实现对User表的数据操作方法，省略除查询外的其他方法（实体类）
MainForm	主窗口（边界类）

方法说明

类 名	说 明
LoginForm类的LoginForm()方法	LoginForm构造函数，初始化实例成员
LoginForm类的validate()方法	界面类的验证方法，通过调用业务逻辑类LoginBO的validate()方法实现对用户输入信息的验证
LoginBO类的validate()方法	业务逻辑类的验证方法，通过调用数据访问类的findUserByAccAndPwd()方法验证用户输入信息的合法性
LoginBO类的setIUserDAO()方法	Setter方法，在业务逻辑对象中注入数据访问对象（注意：此处针对抽象数据访问类编程）
IUserDAO接口的findUserByAccAndPwd()方法	业务方法声明，通过用户账号和密码在数据库中查询用户信息，判断该用户身份的合法性
UserDAO类的findUserByAccAndPwd()方法	业务方法实现，实现在IUserDAO接口中声明的数据访问方法

2.5.2传输接收功能类图

文件传输接收功能描述如下：
用户录入文件后进行加密传输，系统将加密后的文件发送给接收方，接收方验证文件是否正确，如果正确则接收，否则提示对方重发文件



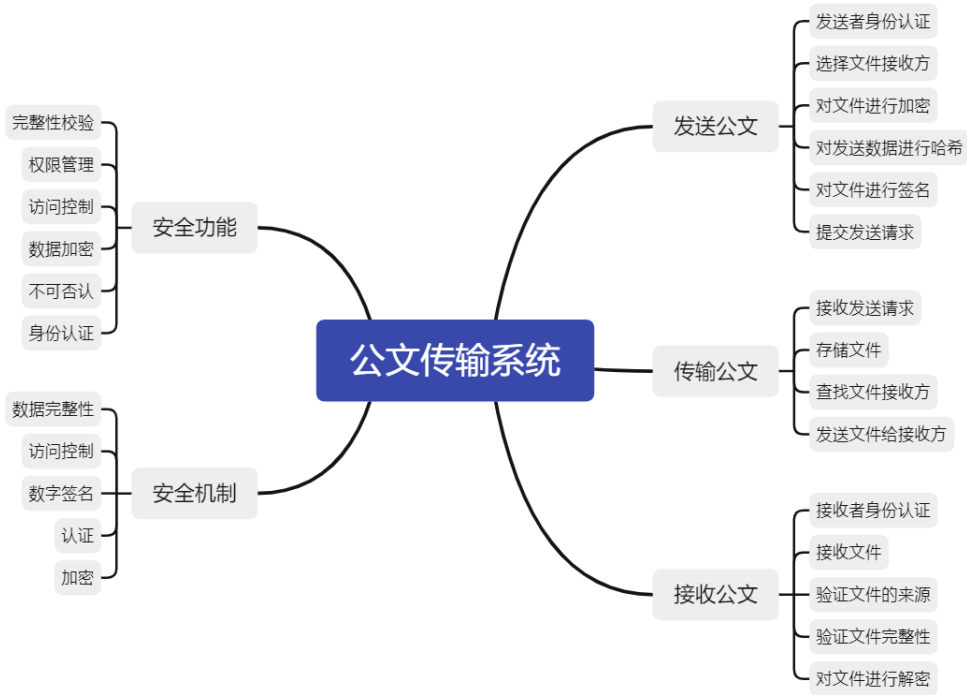
类说明：

类 名	说 明
File_input	文件录入
File_encrypt	实现文件加密，保障文件保密性与完整性
File_send	通过socket通信实现文件传输
File_verify	文件验证，对加密后的文件进行解密，并返回一个bool值
File_accept	接受文件并读取

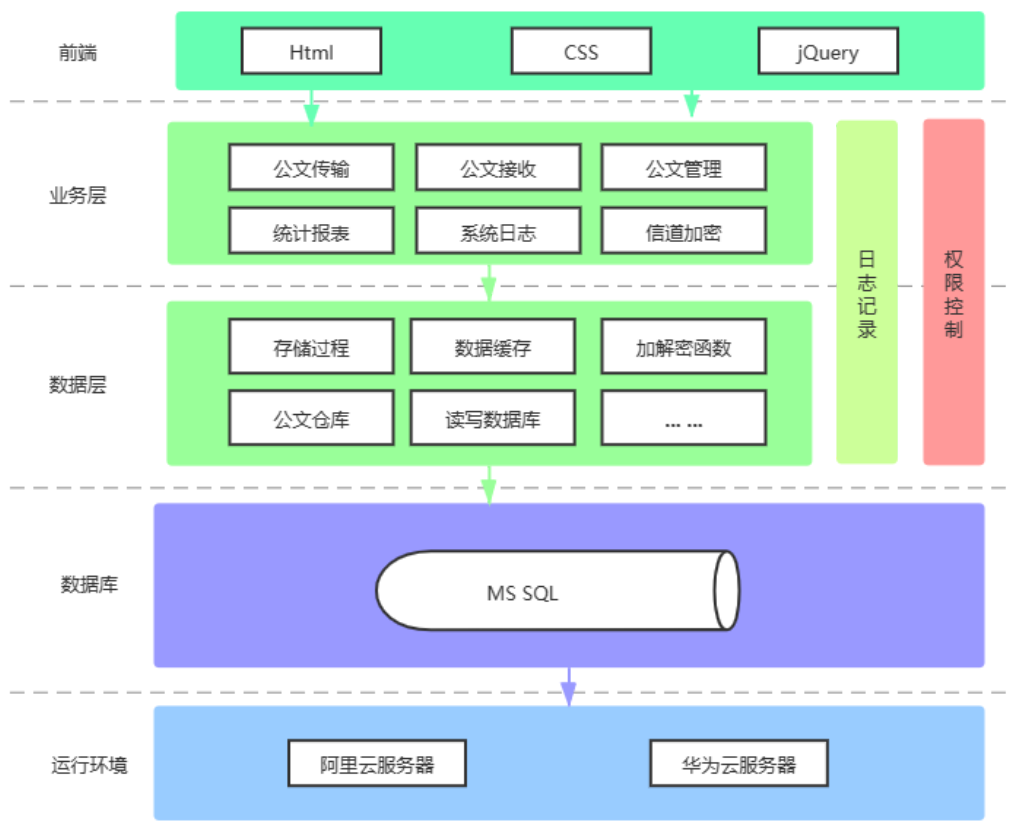
方法说明

方法 名	说 明
File_input类的file_input()方法	文件录入方法，对文件进行读取
File_encrypt类的file_encrypt()方法	加密方法，利用加密算法对文件进行加密
File_send类的file_send()方法	文件发送方法，通过socket实现文件传输
File_verify类的file_verify()方法	验证方法，用解密算法验证文件的保密性与完整性
File_accept类的file_accept()方法	文件接收方法，验证通过后对文件进行读取

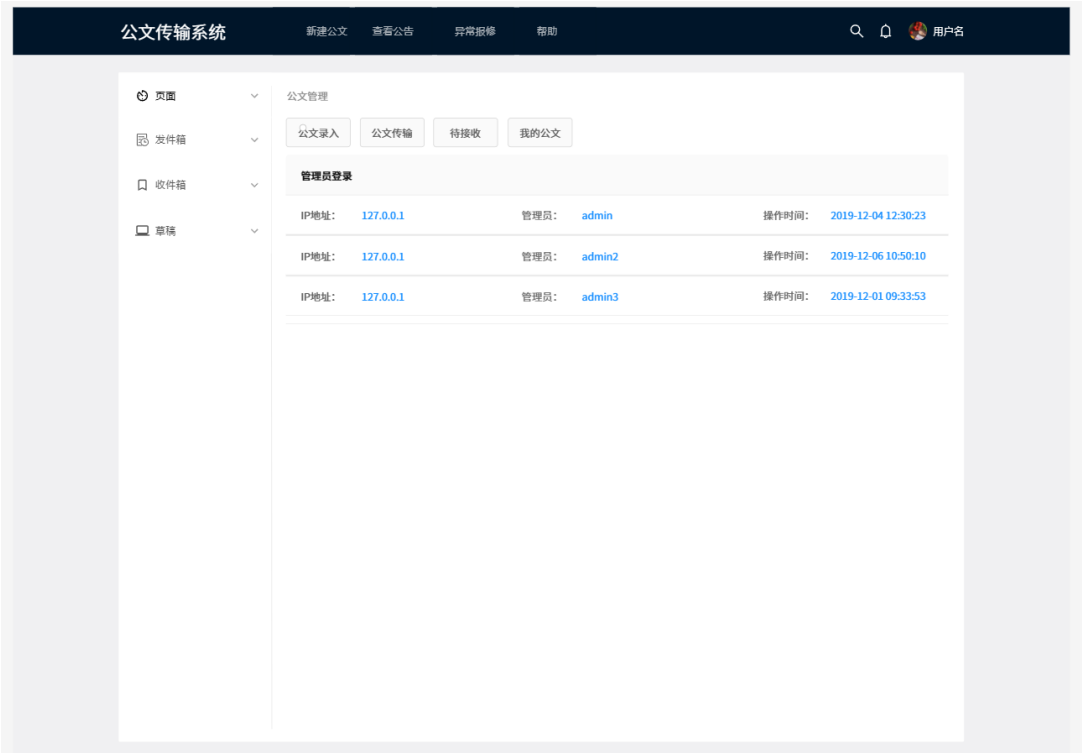
2.6 系统功能图示



2.7 系统架构图示



2.8 界面原型



- 发件箱

用于实现类似邮件发送的公文传输，可以查看已发送的文件

- 收件箱

类似邮件接收的收件箱，可以查看待接收的文件

- 草稿

可以实现公文的修改与保存

- 公文录入

实现将公文上传至服务器

- 待接收

查看对方已发送但未接收的文件

- 我的公文

对公文的管理，包括查询，删除等功能

3 需求规定

3.1 对功能的规定

用列表的方式（例如IPO表即输入、处理、输出表的形式），逐项定量和定性地叙述对软件所提出的功能要求，说明输入什么量、经怎样的处理、得到什么输出，说明软件应支持的终端数和应支持的并行操作的用户数。

输入	处理	输出
Usname:Passwd	Login()、Compare(Database)	False/True
Document	Encrypt(D)、Sign(D)	{Encrypto(D),Sign(D)}
OptionParam	Add()、Del()、Edit()、Search()	False/True
ExitSignal	Logout()	NULL
Download	Verify()、Decrypt()	Document

3.2 对性能的规定

3.2.1 精度

无精度要求。

3.2.2 时间特性要求

该项描述在网条件正常的情况下各模块的时间特性：

- a. 响应时间
 - 常规页面响应时间应当在3s内对请求做出响应
- b. 更新处理时间
 - 页面显示数据应当以30s为周期进行更新
- c. 数据处理时间
 - 考虑到涉及加解密及签名运算，该项时间应当尽量控制在30s以内
- d. 数据传输时间
 - 数据传输时间应当控制在5s内

3.2.3 灵活性

a. 操作方式的变化

公文传输系统操作方式相对固定，该项需求发生变更概率低。考虑到存在增添功能模块的可能，在设计系统时应当事先预留接口以供后续添加新的功能模块。

b. 运行环境的变化

国内正在进行国产化替代工作，本系统在当前主流软硬件环境下运行的同时，应当考虑国产软硬件环境的适配。

c. 同其他软件的接口的变化

考虑到公文传输系统常用于局域网环境下，在局域网环境发生变化时，系统同网络的接口可能发生变化，故系统应当具有对网络环境的自适应能力。

d. 有效时限的变化

公文传输系统存储公文的时间可能收到硬件设施、管理条例等因素的影响而发生变化，故系统应当具有对有效实现的即时修改功能。

e. 计划的变化或改进

在计划执行过程中计划可能发生变化或改进，产生对于需求或功能的变更，故系统应当进行模块化、细粒度设计，在保证功能完善的同时做到“高内聚，低耦合”。

对于为了提供这些灵活性而进行的专门设计的部分应该加以标明。

3.3 输入输出要求

公文以XML文档形式存储和传输，在系统中的输入输出形式应为XML格式。

系统涉及密钥均以二进制文件形式进行密态存储，其在系统中输入输出均为比特流。

3.4 数据管理能力要求

数据项	管理能力要求
文卷和记录的个数	5 00 000 000个
表和文卷的大小规模	10T
增长率	10%/年

3.5 故障处理要求

- 前端页面显示故障
导致系统功能无法正常使用。启用备用前端页面，查找故障原因。
- 传输通道故障
导致系统功能无法正常使用。启用备用传输通道，立即查找故障原因。
- 后端数据处理故障
系统功能异常，系统无法正常使用。立即启用备份服务器，转移用户数据，挂起服务进程查找故障原因。
- 数据库故障
用户数据无法使用，系统功能异常。启用容灾备份数据，紧急恢复数据库。

3.6 其他专门要求

- 保密安全要求
系统应当具有分级权限，具有严格的保密等级制度。
- 使用方便性
系统应当用户友好，操作界面简洁易懂，具有易操作、易上手等特点。
- 可维护性
系统应当留置维护入口，具有热维护能力。
- 可补充性
系统应当具有拓展能力，能够在已有功能的基础上新增功能。
- 易读性
系统的操作标识和指引应当具有易读性，文字说明应当简洁明了，直观达意。
- 可靠性
系统应当具有较高的可靠性，运行稳定，具有较强的鲁棒性。
- 运行环境可转换性
系统应当能够在多平台环境下运行，能够适应不同运行环境的运行要求，并支持平台转换。

4 运行环境规定

4.1 硬件环境

- 服务器
 - (1) 处理器（CPU）：Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz及以上
 - (2) 内存容量（RAM）：4.0GB及以上
- 客户端

(1) 处理器 (CPU) : Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz及以上

(2) 内存容量 (RAM) : 4.0GB及以上

- 外部设备: 打印机、传真机

4.2 软件环境

- 数据库服务器端
- Web 服务器端
- 客户端

4.3 接口

- 硬件接口

考虑到大量数据的备份等要求, 需要USB接口来兼容存储设备的使用。

- 软件接口
- 用户接口

4.4 控制

由于本系统采用目前的主流技术, 对程序的运行和控制都没有特殊要求。