科技创新工作室

本文档内容覆盖单点登录平台技术实现方案，包括需求分析、技术方案、实施方案，适用于上海农商银行所有与统一认证平台相关的设计人员开发人员、开发人员、测试人员。



技术方案

统一认证平台

**文档修改历史**

| 版本号 | 修改日期 | 编写 | 评审 | 批准 | 修改内容 |
| --- | --- | --- | --- | --- | --- |
| V1.0 |  | 钱成 |  |  | 初始第一版 |
| V1.1 |  | 钱成 |  |  | 修改OA登陆流程 |
| V1.1 |  | 钱成 |  |  | 更改统一认证流程 |
| V1.2 |  | 钱成 |  |  | 修改登录流程，增加登出流程 |
| V1.3 |  | 钱成 |  |  | 增加业务流程需求分析 |
| V1.4 |  | 钱成 |  |  | 增加CS架构单点登录流程 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**目录**

[第一章 总体概述 3](#_Toc457291146)

[§1.1 项目背景 3](#_Toc457291147)

[§1.2 项目目标 4](#_Toc457291148)

[§1.3 项目范围 4](#_Toc457291149)

[§1.4 术语表 4](#_Toc457291150)

[§1.5 参考文献 5](#_Toc457291151)

[第二章 需求分析 5](#_Toc457291152)

[§2.1 需求概述 5](#_Toc457291153)

[§2.2 功能性需求分析 6](#_Toc457291154)

[§2.2.1 业务功能点需求分析 6](#_Toc457291155)

[§2.2.2 统一认证接入准则 7](#_Toc457291156)

[§2.2.1 统一认证时序分析 7](#_Toc457291157)

[§2.2.2 B/S架构统一认证流程分析 10](#_Toc457291158)

[§2.2.3 C/S架构统一认证流程分析 12](#_Toc457291159)

[§2.2.4 硬件产品统一认证流程分析 12](#_Toc457291160)

[§2.3 非功能性需求分析 12](#_Toc457291161)

[§2.4 影响分析 13](#_Toc457291162)

[§2.4.1 会计核算影响分析 13](#_Toc457291163)

[§2.4.2 下游系统影响分析 13](#_Toc457291164)

[§2.4.3 其他影响分析 14](#_Toc457291165)

[§2.5 需求排期 14](#_Toc457291166)

[第三章 技术方案 14](#_Toc457291167)

[§3.1 技术方案概述 14](#_Toc457291168)

[§3.1.1 系统分类及等级保护 14](#_Toc457291169)

[§3.1.2 总体设计思路 14](#_Toc457291170)

[§3.1.3 总体设计原则 15](#_Toc457291171)

[§3.1.4 关键技术引用 15](#_Toc457291172)

[§3.1.5 技术方案关键点 16](#_Toc457291173)

[§3.2 系统上下文 17](#_Toc457291174)

[§3.3 总体架构总体架构 18](#_Toc457291175)

[§3.3.1 总体架构说明 19](#_Toc457291176)

[§3.3.2 总体架构决定 20](#_Toc457291177)

[§3.4 容量估算 24](#_Toc457291178)

[§3.4.1 数据库容量估算 24](#_Toc457291179)

[§3.4.2 文件容量估算 24](#_Toc457291180)

[§3.5 安全方案 25](#_Toc457291181)

[§3.5.1 身份鉴别&用户认证 25](#_Toc457291182)

[§3.5.2 操作审计功能 25](#_Toc457291183)

[§3.5.3 安全评估 25](#_Toc457291184)

[§3.6 系统方案 26](#_Toc457291185)

[§3.6.1 系统逻辑部署架构 26](#_Toc457291186)

[§3.6.2 灾备环境 27](#_Toc457291187)

[§3.7 网络方案 28](#_Toc457291188)

[§3.7.1 网络拓扑图 28](#_Toc457291189)

[§3.7.2 网络拓扑说明 28](#_Toc457291190)

[§3.8 运维方案 29](#_Toc457291191)

[§3.8.1 系统运行 29](#_Toc457291192)

[§3.8.2 系统监控 29](#_Toc457291193)

[§3.8.3 参数维护 29](#_Toc457291194)

[§3.8.4 备份清理 29](#_Toc457291195)

[§3.8.5 应急处理 29](#_Toc457291196)

[第四章 实施方案 30](#_Toc457291197)

[§4.1 工作量评估 30](#_Toc457291198)

[§4.2 项目实施计划 31](#_Toc457291199)

[§4.2.1 时间计划 31](#_Toc457291200)

[§4.2.2 资源计划 31](#_Toc457291201)

[§4.3 软硬件需求 31](#_Toc457291202)

[§4.3.1 软件需求 31](#_Toc457291203)

[§4.3.2 硬件需求 31](#_Toc457291204)

[§4.4 项目预算 32](#_Toc457291205)

[第五章 附录 32](#_Toc457291206)

# 总体概述

## 项目背景

在我行信息化建设过程中，由于业务的定位、用户范围不同，存在各类应用系统。随着系统的不断增加，由于用户信息、权限信息分别在各个系统中进行单独的维护。从而造成用户信息缺乏统一、用户权限管理困难，制约了我行信息化建设的进一步发展，从系统整体规划， 统一管理的角度出发，需要对我行系统的用户信息及权限进行统一管理。通过对内部数据和权限的梳理，实施统一认证平台，建立标准化管理规范。

## 项目目标

本项目建设目标为搭建我行行内系统统一的用户管理、安全认证、系统级权限分配，实现用户一站式登录后即可访问行内多个内部系统的统一认证平台。

统一认证平台作为上海农商银行统一用户系统管理的基础平台，主要完成用户统一的登录身份认证、用户和权限管理，实现用户一站式登录后即可访问多个行内内部系统，从而为用户提供灵活、便捷的办公体验，提高员工的工作效率。

## 项目范围

本项目包含行内统一认证平台搭建和接入应用系统改造，总体分三阶段实施：

第一阶段，办公类系统，行内统一认证平台搭建和行内员工内部管理系统接入，具体人员内部管理系统包括：OA系统、人力资源系统、行长驾驶舱，报表系统、合规管理系统、电子档案系统、邮件系统、实物资产管理系统，IMC认证，全行互联网访问认证，VPN认证等；

第二阶段，行内业务处理系统接入，比如CRM，CMIS、PLS等；

第三阶段，我行渠道系统接入，比如综合前端系统金融e云，网银等，逐步调研、审慎接入。

## 术语表

* SSO Single Sign On 单点登录，SSO是在多个应用系统中，用户只需要登录一次就可以访问所有相互信任的应用系统 。
* TGC：Ticket Granting Cookie，存放用户身份认证凭证的cookie，在浏览器和统一认证平台间通讯时使用，并且基于安全通道（https）传输，是统一认证平台用来明确用户身份的凭证。
* **TGT**：Ticket Granting Ticket，TGT是统一认证平台为用户签发的登陆票据，拥有了TGT，用户就可以证明自己在统一认证平台成功登陆过。TGT封装了cookie值以及此cookie值对应的用户信息。用户在统一认证平台认证成功后，统一认证平台生成cookie，写入浏览器，同时生成一个TGT对象，缓存在统一认证平台服务器中，其中TGT对象的ID值就是cookie的值。当HTTP再次请求到来时，如果传过来的是统一认证平台生成的cookie，则统一认证平台以此cookie值为key查询缓存中有无TGT ，如果有的话，则说明用户之前登录过，如果没有，则用户需要重新登录
* **ST**：Service Ticket，ST是统一认证平台为用户签发的访问某一service的票据。用户访问service时，service发现用户没有ST，则要求用户去统一认证平台获取ST。用户向统一认证平台发出获取ST的请求，如果用户的请求中包含cookie，则统一认证平台会以此cookie值为key查询缓存中有无TGT，如果存在TGT，则用此TGT签发一个ST，返回用户。用户凭借ST去访问service，service拿ST去统一认证平台验证，验证通过后，允许用户访问资源。
* **Session**:由各应用系统自己创建，用于记录是否已经成功登陆。

## 参考文献

# 需求分析

## 需求概述

在信息化建设的过程中，由于业务定位、用户范围的不同，存在着各类应用系统。随着系统的逐步增多，由于用户信息和权限分别在每个系统各种独自维护，往往出现了如下问题：

* 用户信息缺乏统一

用户在所有应用系统中都存在用户和组织机构信息，而由于对用户信息的管理没有统一的规划设计，造成一个用户在多个应用系统中有不同的用户信息，信息重复且不准确，造成数据冗余且不统一。

* 密码繁多，不易维护

对与每一个应用系统，用户都需记录一套对应的密码，且应用系统密码设置规则不一致，造成用户密码繁多且不易记录，员工易忘记用户名和密码。

* 用户权限管理困难

在众多的应用系统中，哪些用户能够进入哪些应用系统需要管理员在每个应用系统中进行配置，既不方便、也容易出错。另外，在应用系统内部，每一个人的业务操作权限都是由相应系统管理员进行分配，每个人的职务、岗位分散在各个系统中，且叫法不一。这就造成了这些岗位、角色、部门信息的混乱、不一致，并且进行修改维护也需要在每一个系统中进行更改。造成管理员工作繁重，也带来了安全隐患。

* 管理混乱，成本浪费

各个业务系统都各自存在自己的用户管理、组织机构管理，账号开通、冻结都需要各自系统单独管理，并且各自建有独立的登录体系，意味着每个系统都需要维护一套安全规则，无法统一管理，给管理、维护造成不同程度的资源、成本的浪费。

上述问题的存在，制约了信息化建设的进一步发展，从系统整体规划，统一管理的角度出发，需要对系统的用户信息及权限进行统一管理。通过对企业内部数据和权限的梳理，实施统一用户及权限管理的认证系统，建立标准化管理规范。

## 功能性需求分析

### 业务功能点需求分析

|  |  |  |  |
| --- | --- | --- | --- |
| **业务功能编号** | **业务功能名称** | **业务功能描述** | **上级功能编号** |
| FR-0001 | 统一用户管理 | 人力资源系统发生用户增删改时，将最新用户信息同步至统一认证平台，后续统一认证平台将修改信息分发至各下游系统。 |  |
| FR-0002 | 统一身份认证 | 提供密码，指纹，人脸等多种身份认证服务。 |  |
| FR-0003 | 统一认证功能 | 提供票据生成，分发和验证功能。  提供C/S，B/S架构登录功能。 |  |
| FR-0004 | 用户密码身份信息管理 | 修改用户密码和生物信息。 |  |
| FR-0006 | 用户访问系统权限管理 | 对于不同角色，设置不同的访问系统权限。可手动修改人员访问系统权限。 |  |
| FR-0007 | 审计管理 | 审计功能能够提供全方位的用户管理、认证和授权的审计信息。通过审计系统，用户可以实时监控客户所定义的相关事件和日志。 |  |

### 业务流程需求分析

### 2.2.2.1 BS架构系统登陆

BS架构系统有OA系统、人力资源系统、实物资产管理系统、电子档案管理系统、邮件系统、行长驾驶舱PC版、报表系统和合规管理系统，对于上述系统，统一认证平台提供统一认证和单点登陆功能。上述系统登录前，需要首先登陆OA系统，再由OA界面提供的链接登陆相应的各系统，且在登陆相应系统时无需再次输入用户名/密码，登陆认证操作由统一认证平台完成。

### 2.2.2.2 CS架构系统登陆

CS架构系统有行长驾驶舱移动版和邮件系统（使用foxmail等客户端），对于上述系统，统一认证平台提供统一认证和单点登陆功能。上述系统登录前，需要首先登陆移动互联网平台，再由移动互联网平台登陆相应的各系统，且在登陆相应系统时无需再次输入用户名/密码，登陆认证操作由统一认证平台完成。

### 2.2.2.3 其他系统登录

其他系统包括IMC认证，外网上网认证和VPN认证，此类系统登录时，统一认证平台支持LDAP协议完成认证。

### 2.2.2.4 用户信息修改

统一认证平台用户数据以人力资源系统为准，保存人力资源系统用户姓名、拼音、工号、组织架构、手机和邮箱等信息。用户信息修改（增、改、删）由人力资源系统发起，并实时同步到统一认证平台。

### 2.2.2.5 用户密码修改

用户密码修改分为两种：主动修改密码和重置密码。

主动修改密码：统一认证平台密码有效期为三个月，密码到期后，在用户登录时提示用户主动修改密码，修改密码入口在OA页面，点击修改密码按钮，弹出统一认证平台内嵌修改密码页面；

重置密码：重置密码需提出重置申请，然后由统一认证平台管理员登陆管理页面完成重置。

密码修改后，根据各应用系统密码实时性要求不同，统一认证平台提供实时任务和定时任务修改对应应用系统密码，其中邮件系统需实时同步密码，其他系统采用定时任务方式。

### 2.2.2.6 访问权限控制

统一认证平台根据人力资源系统组织架构信息，生成员工的默认系统访问权限，统一认证平台管理员可以依据变更系统访问权限申请，手动修改员工的系统访问权限。

### 2.2.2.7 审计日志

记录用户访问应用系统的IP、时间和访问路径等信息。

### 2.2.2.8 登出

统一认证平台登出入口位于OA页面，其他系统页面无登出功能。

### 统一认证接入准则

统一认证平台采用我行员工工号作为各接入系统用户统一认证标识，如若接入系统无员工工号信息，需增加员工工号信息；若接入系统目前以其他信息作为登陆用户标识，需统一整改为以工号作为登陆标识。工号信息以目前人力资源系统为准，用户名拼音以外网邮件系统为准，如用户没有外有邮箱，则以目前OA系统为准。

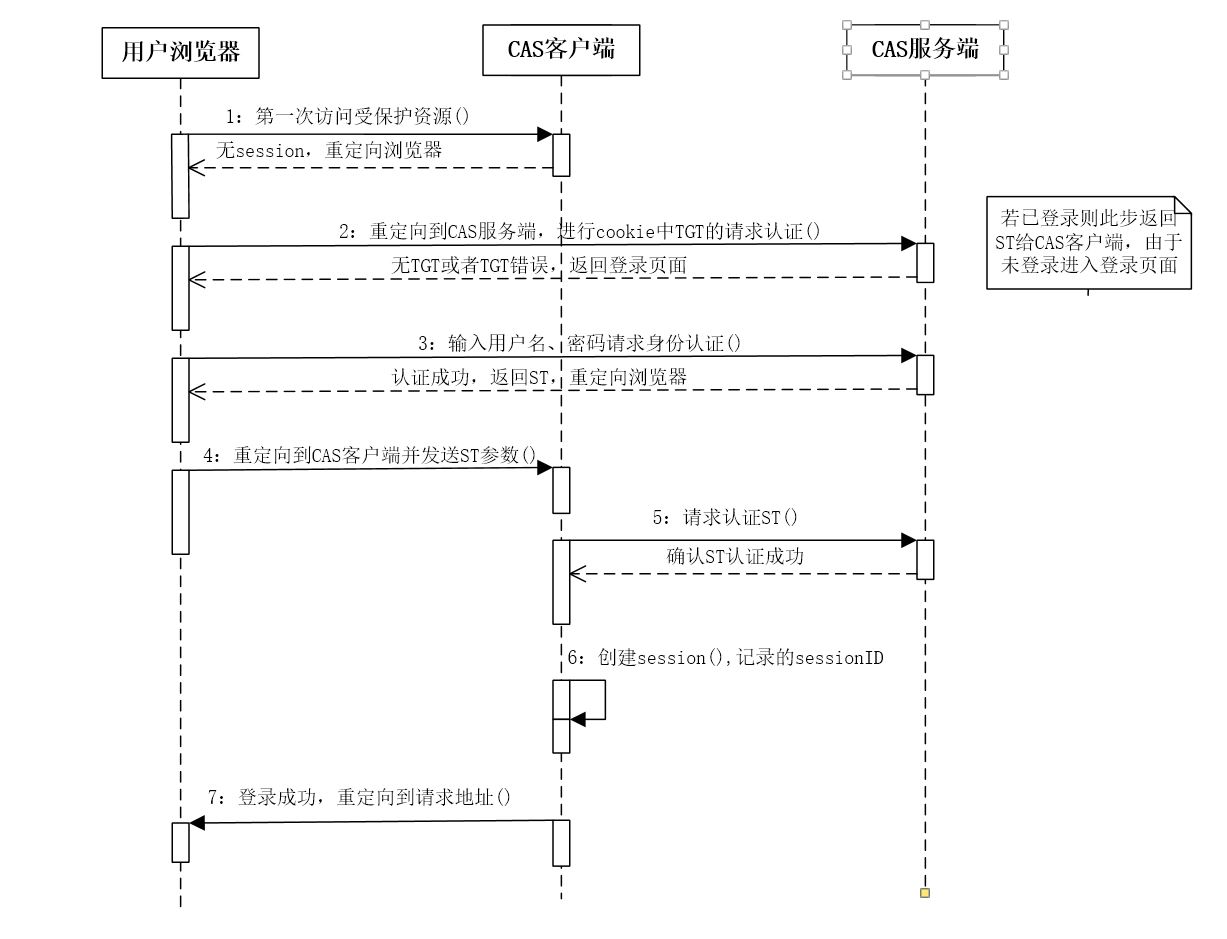
### B/S架构统一认证登陆流程

B/S架构接入应用系统主要有：OA、人力资源系统、行长驾驶舱，报表系统、合规管理系统、电子档案系统、内网邮件和实物资产管理系统。

* 登录认证流程图



**场景一：第一次访问OA流程：**



1. 浏览器向OA发送登陆请求（第一次）；
2. OA服务器检查SESSION，因为首次登陆，所以无session，组装URL，重定向到Server端：[http://casServer/?service=http://oa.srcb.com](http://casserver/?service=http://oa.srcb.com)；
3. 统一认证服务检查浏览器传来的TGC和缓存中的TGT，因为属于首次登录，所以TGC不存在，因此重定向到AO登录页面；
4. 客户输入认证信息，提交到统一认证服务端，统一认证服务端检查认证信息后，生成TGC写入浏览器，并生成TGT保存在服务端缓存中。同时使用上述TGT签发ST。将此ST以URL参数的形式返回OA系统，格式如下：Http://oa.srcb.com/?ST=xxx&Service= Http://oa.srcb.com
5. OA服务器获取ST后，以http请求的方式发起ST反向验证，统一认证服务器检查ST有效性，检查通过返回用户成功登录后的信息；
6. 跳转OA成功登陆页面，同时将登陆成功信息记入OA服务器session。

**场景二：OA登录成功,访问HR系统，TGT未失效（在TGT失效时间内访问HR系统）**

1. 浏览器向HR发送登陆请求；
2. 因为HR系统之前未登陆过，所以HR服务器session中无登陆信息。HR单点登录代理中filter拦截此请求，生成重定向请求 urt=http://sso.srcb.com/login?service=hr.srcb.com ，重定向到统一认证服务器
3. 统一认证服务器检查浏览器传来的TGC，因为OA已成功登陆，所以TGC存在，进一步以上述TGC为key值，从缓存中获取TGT且TGT未失效。
4. 统一认证服务器使用上述TGT签发ST，生成重定向url，url=http://hr.srcb.com/login?ST=xxx
5. HR服务器获取ST后，以http请求的方式发起ST反向验证，统一认证服务器检查ST有效性，检查通过返回用户成功登录后的信息；
6. 跳转HR成功登陆页面，同时将登陆成功信息记入HR服务器session。

**场景三：OA登录成功,访问HR系统，TGT已失效（在登陆OA后一直在OA内部操作，过了TGT失效时间才去登陆HR系统）**

1. 浏览器向HR发送登陆请求；
2. 因为HR系统之前未登陆过，所以HR服务器session中无登陆信息。HR单点登录代理中filter拦截此请求，生成重定向请求 urt=http://sso.srcb.com/login?service=hr.srcb.com ，重定向到统一认证服务器
3. 统一认证服务器检查浏览器传来的TGC，因为OA已成功登陆，所以TGC存在，进一步以上述TGC为key值，从缓存中获取TGT，此时发现TGT已失效。
4. 统一认证平台单点登出，通知其他应用系统删除该用户session
5. 跳转OA登陆主页面，要求重新登录OA
6. 以下步骤同场景一中4-6。

**场景四：OA未登录，访问HR系统**

1. 浏览器向HR发送登陆请求；
2. 因为HR系统之前未登陆过，所以HR服务器session中无登陆信息。HR单点登录代理中filter拦截此请求，生成重定向请求 urt=http://sso.srcb.com/login?service=hr.srcb.com ，重定向到统一认证服务器；
3. 统一认证服务检查浏览器传来的TGC和缓存中的TGT，因为属于首次登录，所以TGC不存在。
4. 跳转OA登陆主页面，要求先登录OA
5. 以下步骤同场景一中4-6。

### C/S架构统一认证流程分析



登陆步骤：

1. 移动互联网平台输入用户名密码，发送至VPN服务器，VPN服务器将用户名密码送至统一认证平台做校验，检验通过即完成VPN通道的创建。
2. 移动互联网平台将刚才用户所输用户名密码直接发送至统一认证平台，统一认证平台认证通过后，创建TGC和TGT，TGT存于统一认证平台服务端缓存中，TGC发送至移动互联网平台，存于移动互联网平台本地Cookie中。
3. 移动互联网平台中应用登陆时，从本地cookie中获取TGC，将登陆请求和TGC发至统一认证平台
4. 统一认证平台根据TGC获取缓存中的TGT，若TGT已失效，则调用移动互联网平台登出服务，要求用户重新登录移动互联网平台
5. 若TGT未失效，则用此TGT签发ST，将ST返回至应用系统
6. 应用系统通过http请求，至统一认证平台验证上述ST
7. 验证通过即应用系统登录成功，显示登录首页。

### 硬件产品统一认证流程分析

对于硬件设备产品集成LDAP认证的系统，如：IMC上网认证、外网上网认证和VPN认证等，统一认证平台提供基于LDAP协议用户认证服务接口，统一认证平台不记录审计日志信息。

### B/S架构统一认证登出流程

* 注销认证流程图

注销功能只有主站点OA系统具有此功能按钮，其它接入认证子系统该功能按钮需屏蔽。



* 1. 用户在OA页面发起单点注销请求
  2. 统一认证服务器获取浏览器上送TGC， 并销毁缓存中已此TGC为key的TGT。并根据TGT获取会话sessionId,销毁TGT和自身的session。
  3. 统一认证服务器找到所有通过上述TGC 登录的应用服务器URL提交请求注销请求，注销请求包含logoutRequest参数
  4. 所有收到请求的应用服务器解析logoutRequest参数，取得sessionId，并根据这个Id取得session后，把session删除
  5. 注销完成后，返回OA初始页面。

## 非功能性需求分析

|  |  |  |
| --- | --- | --- |
| **非功能需求编号** | **非功能需求描述** | **相关的业务功能编号列表** |
| NFR-001 | 系统响应时间小于2秒 | FR-0003 |
| NFR-002 | 服务峰值TPS不小于100TPS | FR-0003 |
| NFR-003 | 系统规模：系统总用户容量需满足1万客户  （目前行内用户6000人，按每年10%的增长率，5年后约为1万客户） |  |
| NFR-004 | 系统需支持7×24服务能力 |  |
| NFR-005 | 系统架构需支持横向扩展能力 |  |
| NFR-006 | 系统可用率不低于 99.95% |  |
| NFR-007 | 相关文档齐全、符合标准、逻辑清晰、描述准确，容易理解和定位 |  |
| NFR-008 | 千行代码缺陷数量小于10个，正负5% |  |
| NFR-009 | 系统故障响应时间小于20分钟，恢复时间小于8小时 |  |

## 影响分析

### 会计核算影响分析

无

### 下游系统影响分析

|  |  |
| --- | --- |
| **系统** | **影响范围** |
| 数据源系统 | 用户认证/登录/退出流程改造 |
| 统一认证平台主系统 | 用户同步实时接口，用户同步批量，用户认证/登录/退出流程改造 |
| 统一认证接入系统 | 用户同步实时接口，用户同步批量，用户认证/登录/退出流程改造 |

数据源系统：用户数据源系统为人力资源系统，需提供用户信息初始数据给统一认证平台作为用户信息铺底数据。需提供用户管理、权限管理等页面功能，通过ESB服务接口方式将用户信息传输给统一认证平台。

统一认证平台主门户系统：暂定OA系统，需集成统一认证平台用户认证功能，进行登陆流程修改。作为主站点需嵌入统一认证子系统列表连接等页面功能。

统一认证平台接入系统：包含OA系统、人力资源系统、行长驾驶舱，报表系统、合规管理系统、电子档案系统、内网邮件、实物资产管理系统等，需集成统一认证功能，并通过ESB实现实时用户信息更新或者定时任务实现批量用户数据更新，晚间根据统一认证平台下发的用户增量更新文件进行用户信息核对。

统一认证平台：满足BS/CS各类系统的单点集成组件，提供多种用户安全认证服务，将认证通过的访问重定向到接入系统；提供用户信息、用户权限等公共信息服务接口给接入系统，并将信息进行存储；存储用户安全认证、用户行为等审计日志数据的记录存储。

### 其他影响分析

如上述系统中用户机构信息存在不统一的情况，需对系统中存量用户数据进行刷新操作，统一用户机构信息。

对于IMC，外网上网认证和VPN认证，需将现在使用用户名拼音认证的方式改成以工号认证的方式。

## 需求排期

# 技术方案

## 技术方案概述

### 系统分类及等级保护

本系统为B类系统，等保级别为二级。

### 总体设计思路

1. 平台基于CAS框架实现客户端需要登录时,默认是跳转到统一登录页面；
2. 统一认证功能基于金融e云平台扩展；
3. 统一认证平台统一用户及密码规则，采用服务接口将数据下发到单点接入系统，确保用户数据信息的统一性。
4. 通过BS架构实现统一登录界面；
5. 通过LDAP记录用户结构信息，依托高效读取能力，增强系统的安全认证处理效率；
6. 通过缓存技术存储用户认证的TGT信息；
7. 通过DB2数据库实现用户访问权限、审计日志数据信息的记录；
8. 通过CFCA控件进行密码加密，保证用户访问安全；
9. 通过浏览器Cookie及Ticket实现用户双重安全认证；
10. 通过数据库服务器采用HA双机热备形式，提高系统的高可用性；
11. 通过WAS ND水平集群方式实现应用系统的扩展性、负载均衡、高可用性。

可扩展性：利用多台机器资源，服务更多客户，提高吞吐量；

负载均衡：平衡负载资源，使资源得以有效利用；

高可用性：

从部署架构上杜绝单点故障:

|  |  |
| --- | --- |
| 节点 | 策略 |
| F5 | 主/备 |
| 应用服务器 | 2台服务器，集群方式，每台3个节点 |
| LDAP服务器 | 2台服务器，主/备,文件数据同步 |
| DB2数据库 | 2台服务器，HA |
|  |  |

引用LDAP提高系统应用的处理效率；

通道访问的流量控制采用漏斗形策略(apache>app>DB)。

### 总体设计原则

实现本技术方案必须遵守的原则，具体举例如下：

1、本方案实现必须基于B/S架构。

2、本系统保留数据历史不得超过6个月；

3、本系统实现必须遵守我行《应用设计原则》；

4、本系统必须遵守我行《业务数据标准》；

1. 本系统必须遵守我行《ESB服务设计规范》；

6、本系统必须纳入集中备份、集中监控范围内；

### 关键技术引用

|  |  |  |
| --- | --- | --- |
| **技术要求** | **技术选型** | **简单描述** |
| 基本架构 | B/S | B/S结构（Browser/Server，浏览器/服务器模式） |
| 体系结构 | MVC | 是模型(model)－视图(view)－控制器(controller)的缩写，一种软件设计典范，用一种业务逻辑、数据、界面显示分离的方法组织代码，将业务逻辑聚集到一个部件里面，在改进和个性化定制界面及用户交互的同时，不需要重新编写业务逻辑。 |
| 框架选用 | SpringMVC&mybatis | 当前成熟的、高度可配置的框架。 |
| 开发语言 | Java | 一种可以撰写跨平台应用软件的面向对象的程序设计语言。 |
| 开发工具 | Eclipse | Eclipse 是一个开放源代码的、基于Java的可扩展开发平台。 |
| 依赖运行环境 | JDK 1.6以上版本 | JDK(Java Development Kit) 是 Java 语言的软件开发工具包(SDK)。 |
| 操作系统 | APP服务器：  RedHat Linux6.5  数据库服务器：  RedHat Linux6.5 |  |
| 数据库 | DB2 SERVER10.1.0.4 |  |

### 技术方案关键点

1、本系统存在高并发性访问, 需进行压力测试。

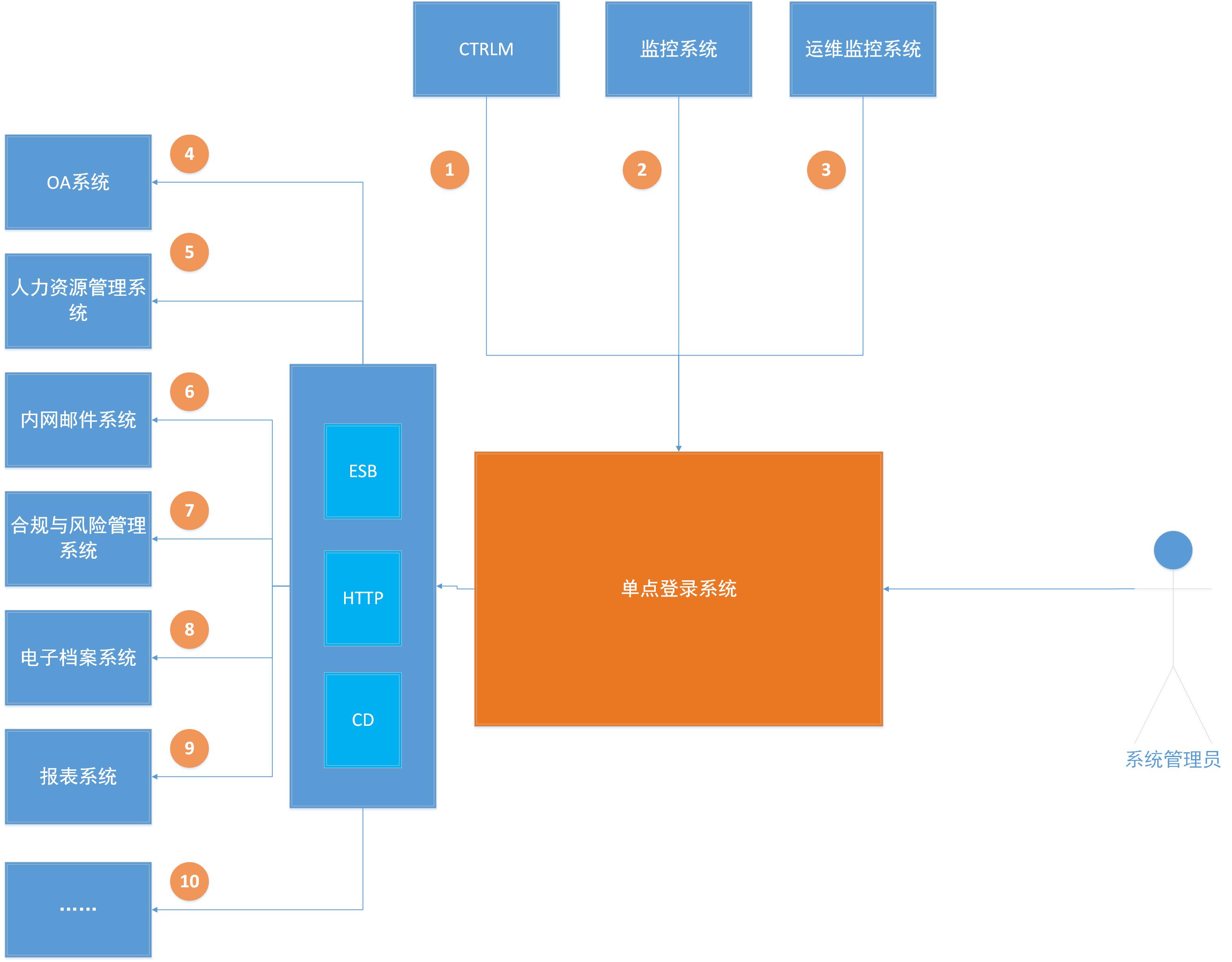
2、Ticket创建:用户信息MD5加密；

Ticket保存:保存在缓存中；

Ticket生命周期：缓存设置的有效时间过期自动销毁或者用户签退主动调用方法销毁缓存服务器Ticket数据。

## 系统上下文

（一）系统上下文图



（二）系统接口说明

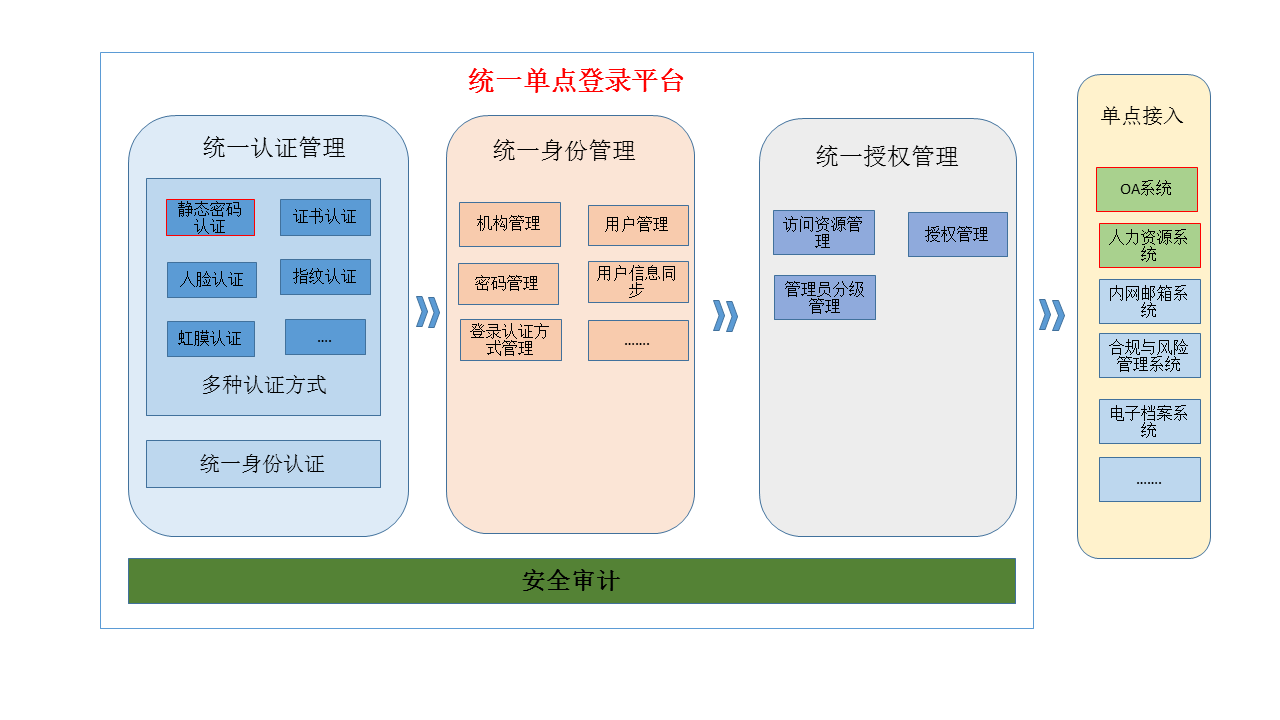
本章节对系统上下文图中所有和本系统交互的系统或者模块的接口进行说明，具体参见系统接口表：

|  |  |  |  |
| --- | --- | --- | --- |
| **交互对手名称** | **交互接口实现技术** | **交互接口目的说明** | **交互信息说明** |
| 数据源系统（人力资源系统） | ESB | 统一认证平台调用接口 |  |
| HTTP | 票据验证等 |  |
| 统一认证平台主门户（OA系统） | CD | 从统一认证平台同步用户数据 |  |
| ESB | 统一认证平台调用接口  用户更新接口 |  |
| HTTP | 登录, 票据验证等 |  |
| 统一认证接入系统  （内网邮件系统、合规与风险管理系统、电子档案系统、点鑫平台） | CD | 从统一认证系统同步用户数据 |  |
| ESB | 统一认证平台统调用接口  机构、用户更新接口 |  |
| HTTP | 票据验证等 |  |

（三）用户接口说明

|  |  |  |  |
| --- | --- | --- | --- |
| **最终用户角色** | **人机交互接口实现技术** | **人机交互接口实现技术目的说明** | **交互信息描述** |
| 系统管理员 | HTTP | 权限管理、修改密码、审计日志查询等 |  |

## 总体架构总体架构



### 总体架构说明

总体架构图的说明

系统整体功能架构主要由统一认证管理、统一身份管理、统一授权管理、安全审计四层组成，以上层次结构的设计主要功能如下

1. 统一认证管理

* 多种认证方式

统一认证在身份识别技术上提供静态密码，USB-KEY等传统识别技术和人脸、指纹、虹膜等生物识别技术。本项目第一阶段只涉及静态密码识别。

* 统一身份认证

平台建立统一用户信息数据库， 以树状的层次结构来存储数据，实现对服务、组织、人员、组、策略以及其他资源的集中、分层、分组管理。提供开发接口给新建系统，可为后续新的应用系统开发提供了统一的认证服务和接入标准。

1. 统一身份管理

* 用户管理

将用户的身份信息和密码同步到各个系统的数据库中，系统管理员在一个平台上统一管理用户在各个系统中的账号和密码。统一用户管理系统对用户身份信息进行统一的管理。 不仅管理方便，也防止过期的用户身份信息未及时删除给行内资产带来的安全风险。在人员离职、岗位变动时，只需在用户管理中心一处更改，即可限制其访问权限，消除对后台系统非法访问的威胁。

* 机构管理

将我行组织机构信息进行集中、分层管理（以人力资源系统组织机构为标准），提供添加、修改、删除操作。

* 登录认证方式管理

平台提供多种身份识别方式，根据用户身份信息与认证方式进行匹配管理，适应不同用户的使用习惯，提升系统使用便捷性。平台也可根据不同单点接入系统进行划分安全认证方式。

1. 统一授权管理

* 访问资源管理

平台上注册行内所有需要管理的应用系统，对其进行描述，管理。列出每一个应用系统下所具有的用户情况。在每个系统下查询用户情况，以直观的方式显示每一个资源下有权访问的用户信息。并对所有用户进行统一的授权。采用基于部门和人员的授权机制，按照人员权限申请和审批结果，自动分配不同的应用系统，以决定其是否可以访问还是不能访问某个系统。授权后，在统一认证平台门户OA上将只会显示其有权访问的系统。

* 授权管理

用户管理员在其管理范围内对用户组与应用系统的关联关系，部门和人员与应用系统的关联关系进行维护，以此来完成用户对应用系统访问的授权。

* 管理员分级管理

可对用户进行分级管理，设定不同级别的系统管理员，本级的管理员只能管理本级的用户，并为用户分配权限，不能管理其他组的用户。超级管理员可以管理所有的用户。解除了总部管理员的管理负担，明确管理职责，方便我行用户管理。

1. 安全审计

统一认证平台提供了安全审计功能，审计用户对应用系统访问的情况，为后续发生事故时提供了一个可追查的机制。审计内容：管理员对系统的管理行为；普通用户的身份认证、单点访问行为；同时，提供强大的查询功能，可以按组合查询。并对审计信息进行分析统计。

### 总体架构决定

分析一：

|  |  |  |  |
| --- | --- | --- | --- |
| **比较项** | **Ticket认证** | **令牌认证** | **用户密码认证** |
| 适用范围 | 所有可改造的系统，对不同登录名需在登录服务器的用户凭证库保存用户映射 | 同域，对不同登录名需增加对用户凭证库的访问 | 一般在CS架构中使用 |
| 用户信息 | 有 | 无 | 有 |
| 用户密码是否需要进行映射 | 不需要 | 否 | 需要 |
| 接入系统的改造工作量 | 中 | 高 | 低 |
| 统一认证平台工作量 | 低 | 低 | 高 |
| 登录模式支持 | 集中验证模式 | 集中验证模式/多点验证模式 | 集中验证模式 |
| 性能消耗 | 较小 | 非常小 | 较小 |
| 稳定性 | 高 | 高 | 中 |
| 扩展性 | 高 | 中 | 低 |
| 安全性 | 高 | 中 | 中 |

|  |  |
| --- | --- |
| **总体架构决定** | |
| **架构决定标题和ID** | 统一认证接入系统交互实现方式 |
| **技术域** | 应用（Application） |
| **架构决定背景描述** | 统一认证接入系统交互包括3种实现方式：Ticket认证；令牌认证；用户密码认证。 |
| **问题描述** | 对于统一认证接入系统交互的实现方式进行决策 |
| **前提假设** | 无 |
| **架构决定重要性** | 架构的选择决定了需求实现的复杂度 |
| **架构决定可选项及优缺点分析** | 分析一 |
| **架构决定结论** | 本次接入系统较多，时间周期紧，同时考虑到系统后续的扩展性，建议采用方案一：Ticket认证。针对CS架构系统提供用户密码认证 |
| **架构决定判断** |  |
| **衍生需求** |  |
| **相关的架构决定** |  |

分析二：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **比较项** | **CAS** | **OpenSSO** | **IBM Tivoli SSO** | **Oracle esso** |
| 成熟度 | 高  80%的市场占有率 | 中  SUN开源，目前已被Oracle收购，现已更名为OpenAM | 中 | 中 |
| 服务端语言 | JAVA | JAVA | SAML | Oracle |
| 技术实现原型 | Spring Framework | Sun Java System Access Manager | Tivoli Access Manager for Enterprise SSO | Oracle中间件 |
| 产品化 | 低 | 低 | 高  需进行产品化组件配置，较复杂，不易于扩展，国内使用较少 | 高  需进行产品化组件安装，较复杂，不易于扩展，国内使用较少 |
| 接入系统的改造工作量 | 低 | 低 | 低 | 低 |
| 统一认证平台工作量 | 低 | 中 | 中 | 中 |
| 扩展性 | 高 | 中 | 低 | 低 |
| 安全性 | 高 | 高 | 高 | 高 |

|  |  |
| --- | --- |
| **总体架构决定** | |
| **架构决定标题和ID** | 统一认证技术实现方式 |
| **技术域** | 应用（Application） |
| **架构决定背景描述** | 统一认证实现方式包括2种主流实现方式：CAS和OpenSSO ，2种产品实现：**IBM Tivoli SSO、Oracle esso** |
| **问题描述** | 对于统一认证的实现方式进行决策 |
| **前提假设** | 无 |
| **架构决定重要性** | 架构的选择决定了需求实现的复杂度 |
| **架构决定可选项及优缺点分析** | 见分析二 |
| **架构决定结论** | 基于框架的成熟度，为了保证项目的顺利实施，建议采用方案一：CAS。 |
| **架构决定判断** |  |
| **衍生需求** |  |
| **相关的架构决定** |  |

分析三：

|  |  |  |
| --- | --- | --- |
| **优缺点** | **LDAP** | **数据库+缓存** |
| 读 | 高 | 高 |
| 写 | 低 | 高 |
| 认证效率 | 高 | 高 |
| 统一认证平台工作量 | 中 | 低 |
| 目前使用系统范围 | OA、邮箱系统、电子档案系统、实物资产管理系统、IMC、VPN | 行长驾驶舱、报表、人力资源系统 |
| 复杂度 | 中 | 低 |
| 扩展性 | 低 | 高 |
| 便捷性 | 中  结构单一，设计后不易于更改变动，具有一定局限性 | 高  结构较复杂，有力于设计的扩展，便于单点系统的用户数据下发 |

|  |  |
| --- | --- |
| **总体架构决定** | |
| **架构决定标题和ID** | 统一认证用户认证实现方式 |
| **技术域** | 应用（Application） |
| **架构决定背景描述** | 统一认证用户认证实现方式包括2种实现方式：LDAP和DB2 |
| **问题描述** | 对于统一认证的用户认证实现方式进行决策 |
| **前提假设** | 无 |
| **架构决定重要性** | 架构的选择决定了需求实现的复杂度 |
| **架构决定可选项及优缺点分析** | 见分析三 |
| **架构决定结论** | 基于多数系统使用LDAP，部分硬件设备无法修改兼容除LDAP外的其它方式。LDAP主要用于用户信息存储，介于用户数据变动较少，LDAP具有高效的读取效率。数据库+缓存无法兼容我行目前所有系统的登录认证服务以及统一认证平台统一认证模式考虑，顾建议采用方案一：LDAP |
| **架构决定判断** |  |
| **衍生需求** |  |
| **相关的架构决定** |  |

分析四：

|  |  |  |  |
| --- | --- | --- | --- |
| **优缺点** | **Session** | **Cookie** | **Session+Cookie** |
| 验证范围 | 服务端 | 客户端 | 服务端+客户端 |
| 实施复杂度 | 低 | 低 | 低 |
| 安全性 | 中 | 中 | 高 |

|  |  |
| --- | --- |
| **总体架构决定** | |
| **架构决定标题和ID** | 统一认证会话实现方式 |
| **技术域** | 应用（Application） |
| **架构决定背景描述** | 统一认证会话实现方式包括3种实现方式：Session、Cookie和Session+Cookie。 |
| **问题描述** | 对于统一认证的会话实现方式进行决策 |
| **前提假设** | 无 |
| **架构决定重要性** | 架构的选择决定了需求实现的复杂度 |
| **架构决定可选项及优缺点分析** | 见分析三 |
| **架构决定结论** | 基于安全性考虑，建议采用方案三：Session+Cookie。 |
| **架构决定判断** |  |
| **衍生需求** |  |
| **相关的架构决定** |  |

## 容量估算

### 数据库容量估算

在系统运行过程中，统一认证平台数据库中记录数增长较快的主要是审计日志，其中包括：认证日志，访问日志。对上述表容量的估算详见下表。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **数据表** | **单条记录占用的空间（K）** | **单条索引占用的空间（K）** | **保留**  **时间** | **保留时间内的预估记录数** | **占用空间（G）** |
| 认证日志表 | 3 | - | 6月 | 10000（人）\*10（次／天）\*6（月）\*20（天/月）  =24000000（条） | 69 |
| 访问日志表 | 2 | - | 6月 | 10000（人）\*50（次／天）\*6（月）\*20（天/月）  =60000000（条） | 115 |
| 合计 | - | - | - | - | 184 |

### 文件容量估算

在系统运行过程中，统一认证平台产生的文件主要包括：日志、用户信息同步文件，数据库本地备份。对上述文件容量的估算详见下表。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **文件类型** | **单个文件大小** | **保留时间** | **保留时间内的文件数量** | **占用空间（G）** |
| 日志 | - | - | - | 可忽略 |
| 用户信息同步文件 | - | - | - | 可忽略 |
| 数据库集中备份 | 200G | 30天 | 30 | 6000 |
| 合计 | - | - | - | 30 |

## 安全方案

### 身份鉴别&用户认证

用户身份识别使用用户名/密码，业务人员账号禁止并发登录，管理员账号可以并发登录。密码保存使用国密算法加密，要求密码中必须包含英文小写字母，大写字母和数字，密码长度为不少于8位，并设有密码有效期（90天），需定期更改 (密码的复杂度策略需要明确) 。平台采取结束会话、限制非法登录次数（5次），连续失败5次后锁定，第二天自动解锁和自动退出等措施，并在日志中记录登录失败信息（时间，IP，错误次数）。

### 密码存储

统一认证平台储存原密码经国密加密算法加密后的密文，其他应用系统的密码为原密码+系统前缀后经国密加密算法加密后的密文。

### 操作审计功能

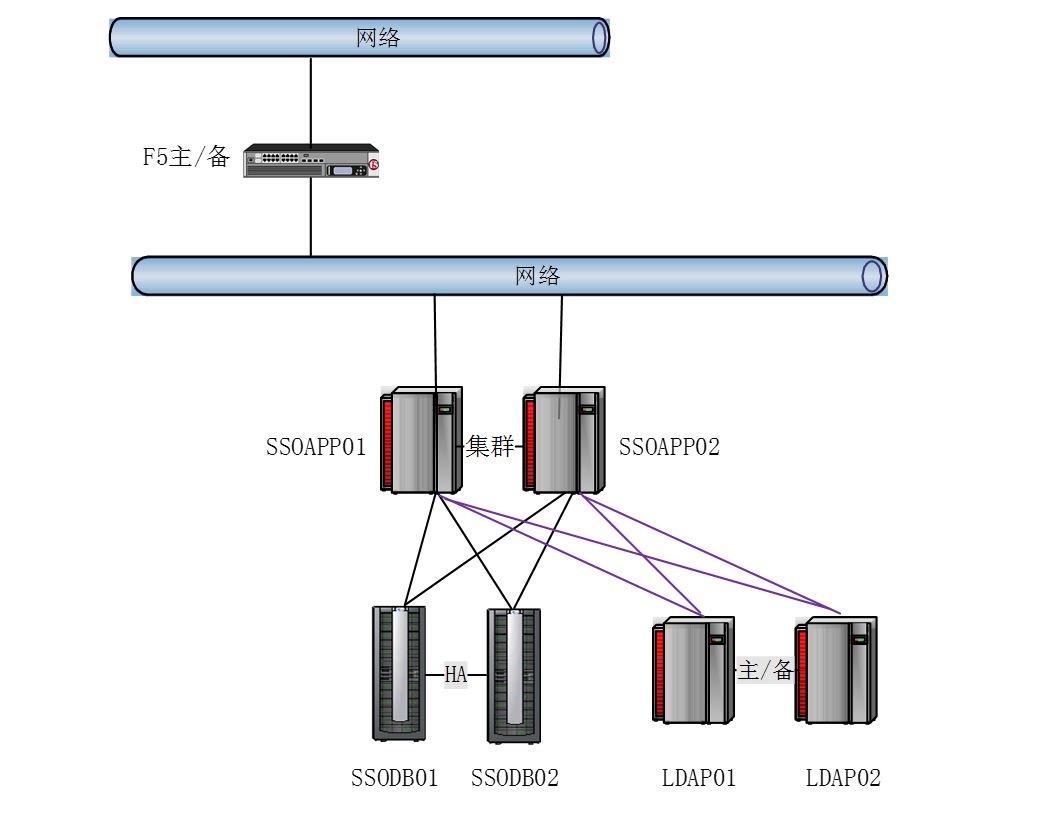
本系统不包含业务功能，对于用户的安全认证进行数据库记录和日志信息记录，对于统一认证访问轨迹进行数据库记录和日志信息记录，并提供页面查询统计功能。

### 安全评估

本系统暂不开放互联网访问，后续如若提供互联网访问需进行防范SQL注入、跨站脚本、文件和目录攻击、逻辑错误等漏洞的措施

## 系统方案

### 系统逻辑部署架构



金融e云目前有2台应用服务器和2台数据库服务器，服务器操作系统，was，db2版本均为老版本，与行内目前版本基线不一致。因此建议统一认证平台通过新搭建服务器的方式部署，具体如下：

新建2台应用服务器，用于统一认证平台应用部署，每台服务器配置3个节点，总共6个节点，采用was集群部署。后续，随着业务量的增加，可横向扩展。2台应用服务器采用F5实现负载均衡。在服务端部署memcached用于用户认证TGT共享缓存存储。

新建2台LDAP服务器，用于用户信息树形结构数据文件存储，采用LDAP群组主从配置实现数据文件的同步。

新建2台数据库服务器，用户统一认证平台数据库部署，采用HA方式实现热备。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **分区编号** | **服务器名称** | **资源说明** | | **备注** |
| 1 | 统一认证平台应用服务器 | 硬件 | 4C 16G | PC服务器\*2 |
| 软件 | Redhat 6.5  WAS 8.5.5.2  memcached |
| 2 | 统一认证平台数据库服务器 | 硬件 | 4C 16G | PC服务器\*2 |
| 软件 | Redhat 6.5  DB2 10.1.0.4 |
| 3 | 统一认证平台LDAP服务器 | 硬件 | 4C 16G | PC服务器\*2 |
| 软件 | Redhat 6.5  openldap 2.4.30 |

### 灾备环境

完善的灾备体系是现代商业银行的重要特征。统一认证平台为全行统一登录安全认证系统，应具备完善的灾备体系，满足系统不间断性、业务连续性和数据完整性要求，从而提高应对因不可抗力导致生产系统无法访问的应急处置能力。考虑到灾备环境为生产环境的临时替代，可无需按照生产环境硬件配置进行部署，以避免资源浪费。统一认证平台灾备环境硬件需求如下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **分区编号** | **服务器名称** | **资源说明** | | **备注** |
| 1 | 统一认证平台应用服务器 | 硬件 | 2C 8G | PC服务器\*1 |
| 软件 | Redhat 6.5  WAS 8.5.5.2  memcached |
| 2 | 统一认证平台数据库服务器 | 硬件 | 2C 8G | PC服务器\*1 |
| 软件 | Redhat 6.5  DB2 10.1.0.4 |
| 3 | 统一认证平台LDAP服务器 | 硬件 | 2C 8G | PC服务器\*1 |
| 软件 | Redhat 6.5  openldap 2.4.30 |

## 网络方案

### 网络拓扑图



统一认证平台硬件设备SSO应用服务器、SSO缓存服务器、数据库服务器均部署在业务三区。统一认证平台与使用用户网络区域具有两道防火墙隔离，防火墙是单统一认证平台各个网络区域的路由选择，同时具有对网络区域之间的数据流进行过滤的功能，对系统服务及内部资源起到安全保障作用。

### 网络拓扑说明

|  |  |  |
| --- | --- | --- |
| **网络设备/服务** | **是否需要** | **需求说明** |
| 负载均衡（F5） | 是 |  |
| VPN | 否 |  |
| NAS | 否 |  |
| 外联网络 | 否 |  |
| 办公网络 | 是 |  |

## 运维方案

### 系统运行

1、系统会定时执行每日的数据跑批，完全纳入CTRL-M调度系统

2、支持7x24小时运行，正常运行期间无需人工操作。

### 系统监控

1、通讯中间件WAS运行状态

2、应用系统通讯状态

### 参数维护

无

### 备份清理

于每日批处理后进行数据备份。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **备份内容** | **备份方式** | **备份介质** | **备份周期** | **备份数量** | **数据保存周期** |
|
| 数据库 | 用户数据备份 |  | 天 | 1 | 每天集中备份，保留1个月 |
| 应用（应用 、交易日志） | 全备 | 本地 | 天 | 1 | 每天集中备份，本地保留7天 |

### 应急处理

系统应用故障：

1. 重启服务：判断统一认证平台应用程序是否正常，重启统一认证平台应用；判断统一认证平台WAS服务是否正常，重启WAS服务；连接数据库异常，重启数据库监听。
2. 启动灾备。
3. 为了保证我行人员的工作有序进行，在统一认证平台试运行期间需保留接入系统原有登录方式。在正式上线后，统一认证接入系统需有开关控制，在统一认证平台正常时，该开关控制为关闭状态，用户只能从统一认证平台进入；在统一认证平台故障时，能紧急启用保留的登录界面，用户可从系统的原有登录界面进行登录。

系统压力过大故障：

1. 数据库服务器压力过大：使用DB2数据库命令强制释放所有连接。

# 实施方案

## 工作量评估

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **条线团队** | **任务项** | **工作量** | **评估说明** |
| 1 | OA系统 | 需求分析、集成开发、配合测试、上线投产 |  |  |
| 2 | 人力资源管理系统 | 需求分析、集成开发、配合测试、上线投产 |  |  |
| 3 | 邮件系统 | 需求分析、集成开发、配合测试、上线投产 |  |  |
| 4 | 合规与风险管理系统 | 需求分析、集成开发、配合测试、上线投产 |  |  |
| 5 | 行长驾驶舱 | 需求分析、集成开发、配合测试、上线投产 |  |  |
| 6 | 报表 | 求分析、集成开发、配合测试、上线投产 |  |  |
| 7 | 实物资产管理系统 | 需求分析、集成开发、配合测试、上线投产 |  |  |
| 8 | 电子档案系统 | 需求分析、集成开发、配合测试、上线投产 |  |  |
| 9 | 移动业务应用平台 | 配合测试 |  |  |
| 12 | 统一认证平台 | 需求分析 |  |  |
| 概要设计 |  |  |
| 详细设计 |  |  |
| 系统开发 |  |  |
| 单元测试 |  |  |
| 数据迁移 |  |  |
| 集成测试（SIT） |  |  |
| 验收测试（UAT） |  |  |
| 上线环境准备 |  |  |

## 项目实施计划

### 时间计划

### 资源计划

## 软硬件需求

### 软件需求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 软件名称 | 版本号 | 提供厂商 | 是否新采购 | 说明 |
| 1 | DB2 | 10.1.0.4 | IBM | 否 |  |
| 2 | WebSphere Application Server（WAS） | 8.5.5.2 | IBM | 否 |  |
| 3、 | openldap | 2.4.30 |  | 否 |  |
| 4、 | memcached |  |  |  |  |

### 硬件需求

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备型号 | 操作系统 | 提供厂商 | 数量 | 是否新采购 | 说明 |
| 1 | 统一认证平台应用服务器 | RedHat Linux6.5 | NA | 2 | 是 |  |
| 2 | 统一认证平台数据库服务器 | RedHat Linux6.5 | NA | 2 | 是 |  |
| 3 | 统一认证平台LDAP服务器 | RedHat Linux6.5 | NA | 2 | 是 |  |
| 4 | F5 |  | NA | 2 | 否 |  |

## 项目预算

【按照任务项及参与团队分项列举项目预算。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **预算项** | **团队** | **金额** | **说明** |
| 1 | 软件预算 |  | ￥\*\*\*\* |  |
| 2 | 硬件预算 |  | ￥\*\*\*\* |  |
| 3 | 开发及单元测试预算 | 会计业务条线团队 | ￥\*\*\*\* |  |
| 4 | 网金业务条线团队 | ￥\*\*\*\* |  |
| 5 |  |  |  |
| 6 | 集成测试 | 测试管理团队 | ￥\*\*\*\* |  |
| 7 | 数据迁移 |  |  |  |
| 8 | 验收测试 |  |  |  |
| **总计** | | | ￥\*\*\*\* |  |

】

# 附录