完整版)统一身份认证设计方案(最终版)

统一身份认证设计方案

日期：2016 年 2 月

目录

1.1系统总体设计

1.1.1总体设计思想

本系统的总体设计思想是实现用户统一身份认证和授权管理，提供安全可靠的身份认证服务。同时，该系统还要考虑到用户的便捷性和易用性。

1.1.2平台总体介绍

该平台是一个基于 Web 的身份认证和授权管理系统，采用 B/S 架构。系统主要包括用户管理、证书管理、授权管理和认证管理四个模块。

1.1.3平台总体逻辑结构

该平台的总体逻辑结构分为客户端和服务器端两部分。客户端包括浏览器和客户端应用程序，服务器端包括 Web 服务器、应用服务器和数据库服务器。

1.1.4平台总体部署

该平台可以在局域网内或互联网上进行部署。部署时需要考虑服务器的性能和安全性。

1.2平台功能说明

该平台的主要功能包括用户管理、证书管理、授权管理和认证管理。用户管理模块实现用户信息的录入、修改和删除等功能；证书管理模块实现数字证书的管理；授权管理模块实现

对用户权限的管理和控制；认证管理模块实现用户身份认证功能。

1.3集中用户管理

1.3.1管理服务对象

该模块主要管理系统中的用户信息，包括用户的基本信息、身份信息和权限信息等。

1.3.2用户身份信息设计

1.3.2.1用户类型

系统中的用户分为内部用户和外部用户两种类型。内部用户是指公司内部员工，外部用户是指公司的客户、供应商等。

1.3.2.2身份信息模型

身份信息模型包括用户的身份属性和身份认证方式。用户的身份属性包括用户名、密码、证书等；身份认证方式包括口令认证、数字证书认证、Windows 域认证和通行码认证等。

1.3.2.3身份信息的存储

用户的身份信息存储在数据库中，采用加密方式进行存储，保证用户信息的安全性。

1.3.3用户生命周期管理

用户生命周期管理主要包括用户注册、审核、激活和注销等过程。在用户注销后，该用户的身份信息将被删除。

1.3.4用户身份信息的维护

用户身份信息的维护包括用户信息的修改、删除和查询等操作。同时，还需要考虑到用户信息的安全性和可靠性。

1.4集中证书管理

1.4.1集中证书管理功能特点

该模块主要实现数字证书的管理，包括证书的颁发、撤销和更新等功能。同时，还需要考虑到证书的安全性和可靠性。

1.5集中授权管理

1.5.1集中授权应用背景

该模块主要实现对用户权限的管理和控制，确保用户只能访问其具备权限的资源。

1.5.2集中授权管理对象

该模块管理的对象包括用户、角色和资源等。用户可以被分配到不同的角色，不同的角色可以访问不同的资源。

1.5.3集中授权的工作原理

集中授权的工作原理是通过角色的分配和资源的授权来实现对用户的权限管理和控制。

1.5.4集中授权模式

集中授权模式包括基于角色的授权和基于资源的授权两种方式。

1.5.5细粒度授权

细粒度授权是指对资源的访问进行更加精细的控制，可以实现更加精细的权限管理。

1.5.6角色的继承

角色的继承可以实现角色的复用，提高系统的可维护性和可扩展性。

1.6集中认证管理

1.6.1集中认证管理特点

该模块主要实现用户身份认证功能，确保用户的身份信息是真实有效的。

1.6.2身份认证方式

身份认证方式包括用户名/口令认证、数字证书认证、Windows 域认证和通行码认证等。

1.6.2.1用户名/口令认证

用户名/口令认证是指用户通过输入用户名和口令来进行身份认证。

1.6.2.2数字证书认证

数字证书认证是指用户通过数字证书来进行身份认证。

1.6.2.3 Windows 域认证

Windows 域认证是指用户通过 Windows 域来进行身份认证。

1.6.2.4 通行码认证

通行码认证是指用户通过输入通行码来进行身份认证。

1.6.2.5 认证方式与安全等级

不同的身份认证方式对应着不同的安全等级，需要根据实际情况进行选择。

1.6.3 身份认证相关协议

身份认证相关协议包括 SSL 协议、Windows 域和 SAML 协议等。

1.6.3.1 SSL 协议

SSL 协议是一种安全的传输协议，可以保证数据的安全性和完整性。

1.6.3.2 Windows 域

Windows 域是一种常用的身份认证方式，可以实现用户的单点登录。

1.6.3.3 SAML 协议

SAML 协议是一种基于 XML 的身份认证协议，可以实现跨域身份认证。

1.6.4集中认证系统主要功能

集中认证系统主要功能包括用户身份认证、用户身份信息管理和单点登录等。

1.6.5单点登录

份认证就可以访问多个系统。

1.1系统总体设计

为了加强对业务系统和办公系统的安全管控，提高信息化安全管理水平，我们设计了基于 PKI/CA 技术为基础架构的统一身份认证服务平台。

1.1.1总体设计思想

为实现构建针对人员帐户管理层面和应用层面的、全面完善的安全管控需要，我们将按照以下设计思想设计并实施统一身份认证服务平台解决方案：

在内部建设基于 PKI/CA 技术为基础架构的统一身份认证服务平台，通过集中证书管理、集中账户管理、集中授权管理、集中认证管理和集中审计管理等应用模块实现员工帐户统一、系统资源整合、应用数据共享和全面集中管控的核心目标。

提供现有统一门户系统，通过集成单点登录模块和调用统一身份认证平台服务，实现针对不同的用户登录，可以展示不

的功能。

建立统一身份认证服务平台，通过使用唯一身份标识的数字证书即可登录所有应用系统，具有良好的扩展性和可集成性。

提供基于 LDAP 目录服务的统一账户管理平台，通过 LDAP 中主、从账户的映射关系，进行应用系统级的访问控制和用户生命周期维护管理功能。

用户证书保存在 USBKEY 中，保证证书和私钥的安全，并满足移动办公的安全需求。

1.1.2平台总体介绍

以 PKI/CA 技术为核心，结合国内外先进的产品架构设计，实现集中的用户管理、证书管理、认证管理、授权管理和审计等功能，为多业务系统提供用户身份、系统资源、权限策略、审计日志等统一、安全、有效的配置和服务。

如图所示，统一信任管理平台各组件之间是松耦合关系，相互支撑又相互独立，具体功能如下：

户生命周期的集中统一管理，并建立与各应用系统的同步机制，简化用户及其账号的管理复杂度，降低系统管理的安全风险。

集中证书管理系统：完成证书管理、证书颁发、证书吊销和证书更新等功能，保证证书的安全性和可靠性。

集中认证管理系统：完成用户身份认证、认证策略管理、认证日志记录等功能，保证用户身份的安全性和可靠性。

集中授权管理系统：完成用户权限管理、权限策略管理、权限审批流程等功能，保证系统资源的安全性和可靠性。

集中审计管理系统：完成审计日志记录、审计数据分析、审计报告生成等功能，保证系统的安全性和合规性。

系统

集中用户管理系统旨在实现企业内部用户账户的统一管理，包括用户信息的导入、导出、映射和同步等功能。该系统支持LDAP 身份源系统数据，提供统一用户接口，方便企业内部各个系统之间的用户信息共享。

为了提高管理效率，该系统采用了过程管理的方式，使得用户账户的管理变得更加规范化和自动化。同时，该系统还支

任的应用系统，提高了用户的使用体验。

随着企业信息化的不断发展，我们已经经历了网络基础建设和应用系统建设两个阶段。现在，我们正处于实现人员统一管理和安全控制的阶段。随着企业网络基础设施的不断完善和应用系统的不断扩展，企业信息化规模也在迅速扩大，更多的人员被融入信息化环境。无论是网络系统、业务系统还是办公系统，它们最终的主体都是企业内外的人员。因此，对于人员的可信身份管理显得尤为重要，只有加强人员的可信身份管理，才能做到大门的安全防护，才能为企业的管理、业务发展构建可信的信息化环境。数字证书认证和应用可以做到全过程可信身份的管理，确保每个操作都是可信得、可信赖的。

集中用户管理系统主要是完成各系统的用户信息整合，实现用户生命周期的集中统一管理，并建立与各应用系统的同步机制，简化用户及其账号的管理复杂度，降低系统用户管理的安全风险。该系统主要面向企业内外部的人、资源等进行管理和提供服务，具体对象可以分为最终用户、主账号、从账号、应用系统及其下具体资源和功能等。用户身份信息设计需要考虑用户类型和身份信息模型。用户类型主要分为员工和外部用

和从账号的对应关系等。

为了实现用户身份信息的有效维护，需要建立完善的用户身份信息维护流程。该流程包括用户信息的录入、修改、审核和删除等步骤，以及相应的审批流程和权限控制机制。同时，需要建立定期更新用户信息的机制，确保用户信息的准确性和完整性。

针对不同类型的用户，需要建立相应的身份信息维护规范和流程。例如，对于离职员工，需要及时注销其账户并进行身份信息的归档；对于临时工或外包人员，则需要建立相应的期限控制机制，确保其身份信息及时失效。

在用户身份信息的维护过程中，需要注意信息的安全性和保密性。对于敏感信息，需要进行加密和权限控制，以防止信息泄露和滥用。

维护用户身份信息不仅是企业信息化建设的基础，也是保障信息安全的重要措施。只有建立完善的身份信息管理体系，才能有效地保护企业的核心信息资产。

域和

LDAP 作为基础数据源，而集中用户管理系统则是主要的用户信息维护入口。人力资源部门的工作人员可以通过该系统执行用户账户的创建、修改、删除、编辑、查询以及数字证书的发放等操作。当 AD 域中的用户信息发生变动时，适配器会将这些变动同步到平台用户身份信息存储（目录服务器）中，并可由平台的用户管理员直接修改平台中集中存储的用户身份信息，然后再同步到各个应用系统中。

集中证书管理功能主要面向用户的 CA 系统，包括证书申请、制作、生命周期管理（有效期、审核、颁发、吊销、更新、查询、归档）以及证书有效性检查等。该功能集支持多种 CA 建设模式（自建和第三方服务）、多 RA 集中管理、扩展性强等特性，从技术和管理上以灵活的实现模式满足用户对证书集中管理的迫切需求，解决管理员对多平台进行操作及维护困难的问题。

集中证书管理功能的实现是通过集成证书注册服务（RA）和电子密钥（USB-Key）管理功能实现的。其中，集中制证主要是为用户进行集中制证，包括集中申请和自动审批。管理员

通过 CA 的配置路径访问指定的 CA 系统，然后该系统签发数字证书并返回给管理员，管理员将证书装入 USB Key 中，最终将数字证书发送给用户。

通过集中证书管理功能，可以实现对所制证书的生命周期管理，包括证书的查询、吊销等，并可以实现对证书有效性的检查。证书有效性检查可支持与 CA 系统的 CRL（证书掉销列表）服务联动及手动导入 CRL 列表。用户可以通过证书认证方式登录“登录门户”，将证书信息提交到“证书管理模块”，服务检查证书信息，若有效，将有效值返回“证书管理模块”，然后“证书管理模块”将有效值返回“登录门户”，用户通过认证后正常进入应用系统。

该功能还支持多种 CA 建设模式和多 RA 集中管理。通过平台与 RA 的集成，可以支持与企业内的多 RA 进行集成，实现单平台多 RA 的集中管理。此外，该功能还具有灵活的扩展性。

集中证书管理功能不仅可以实现证书的集中制证和证书生命周期管理，还具备多 RA 管理、支持用户 CA 系统的自建和服务模式、灵活扩展等特点。它可以与 RA 完全集成，通过平

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/238077011067006074