第7卷第1期 空 军 工 程 大 学 学 报(自然科学版) Vol.7 No.1
2006年2月 JOURNAL OF AIR FORCE ENGINEERING UNIVERSITY(NATURAL SCIENCE EDITION) Feb.2006

基于 Web Services 架构的统一身份认证的设计与实现

张 旗, 张水平
(空军工程大学 电讯工程学院, 陕西 西安 710077)

摘 要:介绍了统一身份认证服务的概念、功能模块以及关键性问题,阐述了在 Web Services 架构中实现统一身份认证服务的设计思想与实现方法,并结合其在院校信息系统集成中的应用实例加以说明。

关键词:统一身份认证;Web Services;网络安全
中图分类号: TP391 **文献标识码**:A **文章编号**:1009-3516(2006)01-0075-05

身份认证是一种通过鉴别用户身份来确保应用系统安全的技术,在以往各种应用的认证模块中,一般固定的账号直接连接数据源,且同一账号供多用户共享,这造成应用系统的安全性和灵活性上均存在严重缺陷。而采取数据库表记录每个系统用户的账号信息、功能权限和数据权限信息,使用一个公共账号与数据源建立连接,并将此账号加密存储在客户端的配置文件中,这种做法不仅增加了用户管理和权限设置的灵活性,而且避免账号直接连接数据源。但随着网络应用的迅猛发展,尤其是 XML Web Services 技术的广泛引入,在进行平滑无缝集成各种应用系统的同时,又带来了新的问题:集成的各应用系统有其自身的用户管理和认证方式,对于用户,需面对不同的登录界面,记忆不同的账户信息;对于系统管理员,要维护多个系统中的用户信息;对于系统需求方,为认证模块重复开发付出了不必要的成本代价。显然,依靠传统的技术方法已很难支持网络信息系统建设对身份管理的需求。因此,为用户提供单一方便、安全可靠的认证服务,对于实现应用系统的整合具有重要的现实意义。在 Web Services 架构中实现统一身份认证服务就是合理解决此需求的专门技术。

1 统一身份认证服务(UIAS: Universal Identity Authentication Service)

UIAS 是实现系统间无缝集成时,在保证整体安全性和可用性的前提下进行身份认证的一种有效机制,其作用是为各种应用系统以统一接口插入信息平台提供有力的安全保障[1]。

1.1 功能需求与模块划分

UIAS 系统提供了一个公共的认证服务平台,将各应用系统的分散认证转变为集中认证,从而提高整体认证的可信度、可靠性及高效性。其功能特性主要应包括:①统一的身份信息存储:可对用户信息集中存储管理,以保证一致性;②统一的权限分配:允许管理员对用户权限进行合理的分配;③统一的身份认证方式:以一种标准的、统一的、规范的认证方式对用户身份识别和确认;④良好的扩展性和可集成性:既尽可能地避免对现有系统的身份认证模块设置进行大规模的修改,以降低修改费用,又能为新的应用提供用户认证服务,以节约开发成本。

根据的 UIAS 系统功能需求,可划分为以下 3 个功能模块[2]:

1)用户注册:用户在 UIAS 中心注册账号,该账号可用于所有使用 UIAS 的应用系统中;

2)账号关联:对于用户在相关应用中已建立的账号,可与 UIAS 的账号进行关联,以便在不改变原有账号的情况下仍能访问应用系统;

收稿日期:2005-06-14
作者简介:张 旗(1977-),男,湖南常德人,硕士生,主要从事计算机网络与数据库研究.

3)用户认证:对用户实施身份认证,为合法用户授予令牌,并在用户与应用间建立会话(Session)。

UIAS 机制涉及以下 4 个实体:①用户: 即 UIAS 的用户;②账号:应用系统的账号,与 UIAS 的用户相关联,一个用户可关联多个账号;③应用系统:使用 UIAS 的应用系统;④会话:当用户成功登录 UIAS 后,便创建一个会话,并获得会话认证令牌,用户凭该令牌可访问应用系统。

1.2 UIAS 关键性问题

在实施应用系统整合过程中,由 UIAS 服务器单独提供访问入口,保障整体的安全性,而系统的各分系统无需承担任何安全职责。这需要处理好以下关键性问题:

1)用户资料的集中存储和管理。用户资料是进行 UIAS 的基础条件,应建立统一的中央用户资料数据库,并保证数据库中用户数据的安全性、实时性和可靠性。用户资料包括:组织、工作单位、用户名、ID、登录密码等。

2)访问权限的集中控制和管理。对访问权限进行集中管控,便于从全局角度提高系统的安全性。通过建立应用访问策略机制,定义用户与访问资源之间的角色(映射)关系、访问条件和操作规则,系统将根据用户的角色,来授予访问权限。访问策略与用户资料均以标准格式(如:XML)的文档形式存放于中央用户资料数据库。

3)UIAS 与各应用系统间的信息交互。建立统一身份认证交互平台,用于在 UIAS 中心与各应用之间传递相关认证信息。用户应先访问统一身份认证交互平台,只有成功登录,才可访问相关应用。同时,UIAS 建立全局的会话机制,以确保访问集成环境中其它的应用系统时,无须再做重复的登录操作。

4)信息传输的安全保障。在用户信息交互过程中,应采取密文传输方式进行,以保证信息的有效性和安全性。

2 基于 Web Services 架构的 UIAS

基于 Web Services 架构的 UIAS 是对该架构下所有应用服务的用户身份信息进行统一管理和认证的解决方案。在 WEB 环境下,当用户访问各种应用系统或在其间做切换时,应通过对统一认证接口的调用,经安全认证通道(使用加密技术)来访问认证服务器,统一认证服务器从用户信息库提取数据与用户的登录信息进行判别,从而完成身份认证与授权访问过程。

2.1 设计思想

下面以某所综合性大学的资源信息网系统为例来说明 UIAS 系统的设计。某综合性大学为提高学校各种事务处理的信息化程度,采取 Web Services 技术集成了各院系、科研机构、机关部门的跨平台的多种应用系统,如:教学事务管理系统、财务管理系统、综合图书信息系统、人事档案管理系统、学籍管理系统等应用资源。然而,以上应用系统的用户身份认证各自为政,互不相同,其认证方式呈现多样化,这不仅使用户在应用系统间做切换访问时不得不重复多次登录,也给管理员的管理维护工作带来一定难度。针对以上情况,为解决信息"孤岛"问题并保证系统整体安全,可设计基于 Web Services 架构的 UIAS 平台以满足此需求。

2.1.1 整体架构模型

在应用集成架构中(如图 1 所示),中央用户资料数据库存储了用户相关的个人资料和对应用访问策略的定义。Web Services 集成引擎通过各类接口和功能模块将各应用子系统封装成 Web Services 部件后发布到 UDDI 注册中心,并通过接口调用相应的应用服务。集成引擎包括:SOAP 处理器、事务处理器和适配器 3 个模块[3]。SOAP 处理器实现 SOAP 消息的传递;事务处理器负责对用户各种事务请求的处理和响应;适配器作为集成引擎的核心,其中,适配器由以下几部分构成:①API 应用接口 为每个应用提供不同的接口以供调用;②安全认证 用于建立与后端服务器的通信连接和安全机制;③数据转换器 实现 SOAP 数据格式与应用子系统数据格式之间的转换;④消息路由器 实现在 SOAP 处理器与适配器之间的消息传递,经 SOAP 消息过滤后,路由到相应的目的地。UIAS 平台为集成所有的应用提供了一个公有的、高效的、安全的、可扩展的身份认证模块。利用中央用户资料数据库对各个应用子系统分散的用户信息集中管理,不仅给使用管理带来便利,而且增加了数据的安全性。采用统一的身份认证机制和应用接口,避免了各种应用子系统的重复开发,便于应用系统的集成。

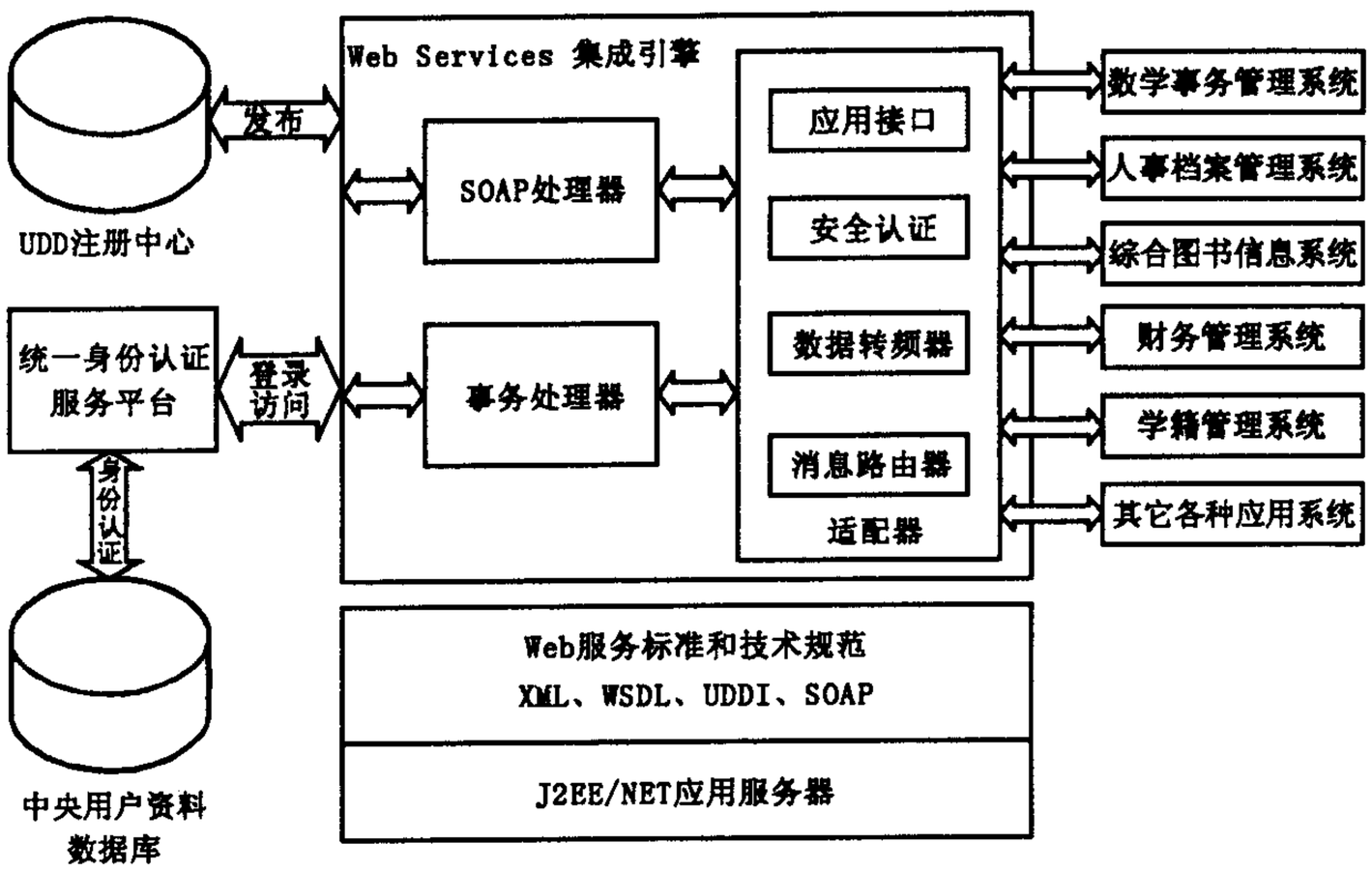

图 1　基于 UIAS 技术的 Web Services 架构图

实现原理:在 Web Services 架构下,任何支持 UIAS 的应用服务都需先以 UDDI(Universal Description,Discovery and Integration)数据实体 businessService 的形式注册到 UDDI 注册中心,并被分配一个 UUID(唯一标识符)。对于每个 businessService,均绑定了包括应用程序连接远程 Web 服务并与之通信的必要信息,如:Web 应用服务的入口地址、应用服务宿主、调用服务前必须调用的附加应用服务等。用户应将个人信息注册到中央用户资料数据库,生成账号并建立与各应用子系统的映射关系。若用户需访问应用系统必须先登录 UIAS 平台,UIAS 平台根据用户提交的登录信息(用户名、ID、密码、所需访问的应用服务等)进行身份认证,如果认证通过,便从中央用户数据库中查取被访问的应用系统所对应的 UUID。UIAS 再使用该 UUID 查询 UDDI 注册中心,以获取此应用系统的 businessService,由此得知访问入口后实施访问。若应用系统修改了访问入口或其它关键信息,它应在 UDDI 注册中心更新自己的信息,以便 UIAS 在下次实施关联查询时获取应用系统的新访问信息。

2.1.2　UIAS 平台的设计

UIAS 平台是实现身份认证的基础,它提供所有在 UDDI 中心注册过的应用服务选择,并接收用户对应用子系统服务的请求,根据中央用户资料数据库来分析其是否有权访问所申请的资源,如果具备访问权限则提供应用服务,否则拒绝请求。UIAS 平台包括以下几个功能模块:

1)主界面模块:为用户提供公共的身份认证界面,用户通过它进一步访问应用系统。

2)身份认证模块:对用户身份进行认证,以确定是否授予访问 Token,并在持有 Token 的用户与被访问应用子系统之间创建 Session。

3)用户信息管理模块:实现用户个人资料的添加、编辑、删除等操作。

4)账号管理模块:提供用户账号注册、注销和关联功能。

5)访问控制管理模块:由管理员集中设置控制各个应用系统的访问权限。

6)资源查询模块:可查询集成环境下所能提供的应用服务。

2.2　UIAS 工作过程

2.2.1 用户注册与账号关联

通过 UIAS 平台将用户的信息注册到中央用户资料数据库,生成用户账号并与 UDDI 注册中心的 Web Services 建立关联,同时根据需要生成访问策略。由于 XML 具有自描述性、结构性、可扩展性、可校验性等诸多优点,因此使用 XML Schema 定义用户信息,有利于按照统一格式进行数据交换和处理,内容及格式如下:

基本信息(用户 id,姓名,单位)
可访问资源 1
访问信息(访问协议、端口号)
扮演角色及其作用域
[
　角色名 1
　数据库连接信息(DBMS,ServerName,DBName,LoginName,Password);
　作用域
　[
　　访问域 1(策略 1:约束名约束条件约束值;

策略 2:约束名约束条件约束值;
……)
权限(只读、写、审计……)
访问域 2(策略 1:约束名约束条件约束值;
策略 2:约束名约束条件约束值;
……)
权限(只读、写、审计……)
……
]
角色名 2
数据库连接信息(DBMS,ServerName,DBName,LoginName,Password);
作用域[……]
……
]
可访问资源 2
……

利用账号关联功能使用户在 UIAS 生成的账号与相关应用系统中已存在的账号建立关联,以便在不改变原有账号的情况下仍能访问应用系统。具体工作流程如图 2 所示。

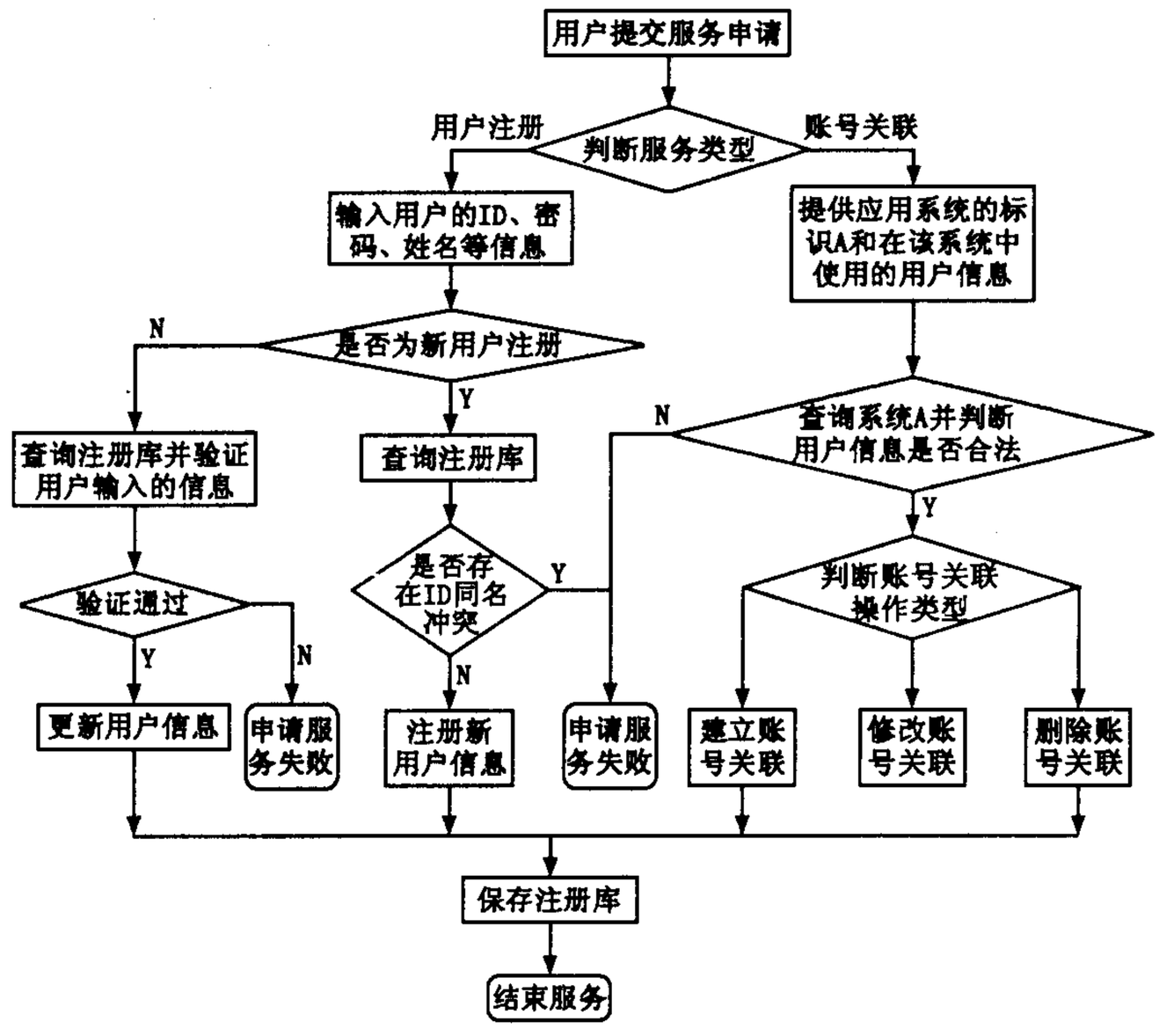

图 2 用户注册与账号关联工作流程图

2.2.2 身份认证

在 Web Services 架构下,UIAS 平台利用 SOAP 和 HTTP 协议进行数据通信与交互,提供 sign_in、check - authToken、discard_authToken 等 API 函数完成认证服务,最终实现对应用系统的调用。其中:

sign_in:用于登录 UIAS,若 sign_in 调用成功,将返回 authToken 响应消息,它包含单个 认证消息 authInfo(即认证令牌);

check_authToken:用于验证认证令牌的合法性;

ldiscard_authToken:当用户完成各种操作,为避免认证令牌被非法滥用,可调用该函数完成 UIAS 的注销工作,以结束当前会话,此后任何对该认证令牌的调用将遭拒绝。UIAS 平台的认证信息交互可采用以下三种模式:

1)身份认证组件模式 :以应用系统的身份认证组件形式工作,涉及的账号必须是经 UDDI 注册过的账号,其工作流程:用户使用经 UIAS 注册后的用户名和密码登录应用系统 A;应用系统 A 将用户名、密码和自身标识一起转发给 UIAS,要求完成登录操作;UIAS 检查应用系统注册库,核查系统 A 是否为 UIAS 的用户系统,并验证用户名和密码的正确性;如果检查通过,UIAS 响应应用系统 A,登录成功;应用系统 A 生成权限令牌给用户,二者间建立会话,用户凭权限令牌服务访问应用系统,直至退出或会话超时。

2)统一认证模式:以 UIAS 为核心,若用户登录成功,便可访问所有支持 UIAS 的应用系统。其工作流程:用户使用经 UIAS 注册后的用户名和密码来登录 UIAS;若登录成功,UIAS 便创建一个会话,并生成权限令牌给用户;用户通过权限令牌根据需要来访问支持 UIAS 的应用系统;被访问的应用系统将访问者的权限令牌传递给 UIAS,要求验证其有效性;权限令牌只有经 UIAS 验证视为合法后,才允许应用系统接收访问,并返回访问结果。

3)信任代理模式:建立 UIAS 代理机制,使所有应用系统仅接收来自 UIAS 的访问请求,以便于将安全保障集中部署在 UIAS 端,其工作流程:用户使用经 UIAS 注册后的用户名和密码来登录 UIAS;若登录成功,UIAS 便创建一个会话,并生成权限令牌给用给用户;用户使用权限令牌,传递包含应用系统 ID 的请求消息给 UIAS,要求访问某个支持 UIAS 的应用系统;UIAS 访问应用系统注册库,核查该应用系统是否支持 UIAS,并获取应用系统的访问入口;UIAS 再将请求消息转发给应用系统;应用系统将请求结果返回给 UIAS,最终 UIAS 将响应消息返回给用户,从而完成调用。采取信任代理模式实施认证服务过程描述为:①用户使用在 UIAS 注册的用户名和密码登录,假设用户名是"UATest",密码使用 Base64 编码表示的 HASH 值;②UIAS 创建一个会话,并将与该会话关联的访问认证令牌返回给用户,在 SOAP 消息中,访问认证令牌使用 Base64 编码;③用户使用该认证令牌访问教学事务管理系统(TBMS),用户请求中标识了 TBMS 的 ID,将之传给 UIAS;④UIAS 访问应用系统注册库,获取 TBMS 的访问入口;⑤UIAS 将请求消息转发给指定的 TBMS,如果 TBMS 使用自己的用户系统,则该消息应当包含了预先定义好的相关联的用户名和密码等信息;⑥TBMS 将请求结果返回给 UIAS,再由 UIAS 将响应消息返回给用户,完成调用。

2.3　系统性能

通过建立 UIAS 机制,使所有参与集成的应用系统均共享同一 UIAS 系统进行身份认证。与原有分散的认证方式相比,性能上具有较大进步,主要体现在:

1)增强了系统安全性 采用 UIAS 管理机制减少了原有分散认证的数据不一致性,对应用系统访问权限进行统一控制。

2)提高了运行效率 为用户提供了单点登录全网访问的运行模式,也给管理员对所有用户访问控制管理带来极大便利,极大提供了认证和授权效率。

3)提升了系统的资源利用率 由于集中式管理用户信息,不仅节省了原有应用系统的用户信息数据库资源,提高了信息共享度,而且兼容原有应用系统的身份认证模块、用户设置和权限设置,系统整合时可避免对其大规模的修改,同时也为新应用系统的开发节约了成本。

3　结束语

作为信息资源整合的重要环节,基于 Web Services 架构的 UIAS 具有便于用户访问,易于管理维护的特点,避免了重复建设、重复管理和重复维护等工作。但由于 Web 系统集成的多变性、复杂性,在具体实施过程中,还应充分做到统一资源访问授权机制、统一日志审计机制统一身份认证机制的三者间有机结合,只有这样才可能为上层应用提供安全可靠的低层基础平台。

参考文献:

[1]　Justin Menga. CCSA NG:Check Point 认证安全管理员全息教程[M]. 北京:电子工业出版社, 2003

[2]　柴晓路,梁宇奇. Web Services 技术、架构和应用[M]. 北京:电子工业出版社, 2003.

[3]　李爱华,徐立臻. 基于 ICE 技术的身份认证交互模型[J]. 计算机应用, 2005,25(3):567 - 569.

(编辑:门向生)

Design and Realization of Universal Identity Authentication Service Based on Web Services Framework

ZHANG Qi, ZHANG Shui - ping

(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

Abstract: This paper introduces the concept of Universal Identity Authentication Service, the function module and some key problems about it. The designed idea and implementation approach of UIAS based on Web Services framework are expatiated. Meanwhile, an UIAS case applied to the integrated college information system is given to illustrate the operation principle of the system.

Key words: universal Identity; Web Services; network security