(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101605030 B
(45)授权公告日 2012.09.05

(21)申请号 200810114899.4
(22)申请日 2008.06.13
(73)专利权人 新奥特(北京)视频技术有限公司
地址 100080 北京市海淀区西草场1号北京硅谷电脑城15层1501-1506室
(72)发明人 张云锋 孙伟 王弋珵
(74)专利代理机构 北京天悦专利代理事务所(普通合伙) 11311
代理人 田明 任晓航
(51)Int.Cl.
H04L 9/32(2006.01)
(56)对比文件
WO 2007/071191 A1,2007.06.28, 全文.
CN 101064695 A,2007.10.31, 全文.
CN 1731723 A,2006.02.08, 全文.
审查员 王伦杰

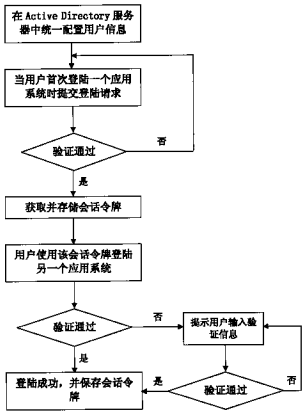
权利要求书 1 页 说明书 6 页 附图 2 页

(54)发明名称

一种面向电视台应用的基于Active Directory的统一认证实现方法

(57)摘要

本发明公开了一种统一认证实现方法,尤其是公开了一种应用于电视台主干网中的基于Active Directory的统一认证实现方法。在现有的统一认证方法中无法同时实现跨域和在多个浏览器之间实现统一认证。本发明所述的方法首先在Active Directory服务器中统一配置用户信息;当用户首次成功登陆一个应用系统后,获取并存储会话令牌;当用户使用该会话令牌登陆另一个应用系统时,该应用系统通过Active Directory服务器验证会话令牌的合法性,如果通过验证,则登陆成功。采用本发明所述的系统能够实现电视台内部处于不同域中的各个应用系统的单点登陆,应用系统可以为B/S或C/S结构。



CN 101605030 B

1. 一种面向电视台应用的基于 Active Directory 的统一认证实现方法，包括以下步骤：

(1) 在 Active Directory 服务器中统一配置用户信息以及各应用系统的信息；

(2) 用户第一次登陆一个应用系统成功后，获取一个针对该用户的会话令牌，并将该会话令牌存储到被登陆的应用系统中；

(3) 当该用户登陆其它应用系统时，首先将步骤 (2) 中存储的针对该用户的会话令牌传递至待登录的应用系统，然后待登陆应用系统通过Active Directory服务器验证该用户会话令牌的合法性，如果通过验证，则允许用户登陆，同时更新并返回该用户的会话令牌，并将更新后的会话令牌存入被登陆的应用系统中。

2. 如权利要求 1 所述的统一认证实现方法，其特征在于，步骤 (2) 中用户第一次登陆一个应用系统的过程为：将应用系统可区别姓名 DN、用户可区别姓名 DN 以及用户密码传送到 Active Directory 服务器，Active Directory 服务器先根据应用系统的可区别姓名 DN 验证该应用系统是否是统一认证的用户系统，再根据用户可区别姓名 DN 和用户密码验证用户的合法性，如果通过验证，则登陆成功。

3. 如权利要求 1 所述的统一认证实现方法，其特征在于，存储会话令牌的过程为：首先调用单点登陆客户端提供的 API，然后利用该 API 将会话令牌存储到被登陆应用系统的注册表中。

4. 如权利要求 1 所述的统一认证实现方法，其特征在于，步骤 (3) 中所述的验证会话令牌的合法性的过程为：将会话令牌连同待登陆应用系统的可区别姓名 DN 一起传送到 Active Directory 服务器，Active Directory 服务器先根据待登陆应用系统的可区别姓名 DN 验证该应用系统是否是统一认证的用户系统，然后再验证会话令牌的合法性。

5. 如权利要求 4 所述的统一认证实现方法，其特征在于：如果步骤 (3) 中会话令牌的合法性验证失败，则通知待登陆应用系统显示登陆界面，进行独立登陆。

6. 如权利要求 1 至 5 之一所述的统一认证实现方法，其特征在于：在用户注销后，应用系统删除该用户的会话令牌。

7. 如权利要求 1 至 5 之一所述的统一认证实现方法，其特征在于：所述的会话令牌具有生命期限，当用户登陆超过生命期限后，会话令牌被吊销。

一种面向电视台应用的基于 Active Directory 的统一认证实现方法

技术领域

[0001] 本发明涉及一种统一认证实现方法，尤其是涉及一种面向电视台应用的基于 Active Directory 的统一认证实现方法。

背景技术

[0002] 当前国内外广电行业网络化、信息化程度日益提高。电视台内部根据业务范围划分为多个不同的业务板块，不同的板块根据其业务需求，往往要使用不同的应用系统，例如总控收录系统、新闻制播系统、综合制作系统、演播室系统、媒资管理系统、播出系统等。各个应用系统都需要拥有一份统一的电视台内部人员组成信息，电视台需要为这些应用系统提供诸如部门人员结构、栏目组人员结构等信息，并且这些应用系统都需要提供一个登陆时验证用户名及密码的功能。工作时，用户经常需要在不同的板块之间来回切换。如果按照传统的开发模式，每个应用系统都必须开发各自独立的用户认证模块。这种模式主要存在以下弊端：

[0003] (1) 用户认证信息需要在多个应用系统的数据库中的重复存储，从而带来大量的数据冗余，也造成了各个应用系统的重复开发；

[0004] (2) 对系统的用户认证信息管理和用户的使用造成诸多不便：用户在注册或更改自己的认证信息时，必须在所有的应用系统中逐个注册或更改，在不同应用系统之间切换时，必须重复多次登录；

[0005] (3) 在安全性和系统管理方面，电视台需要大量的 IT 技术管理人员，分别管理和维护不同系统的用户信息；

[0006] (4) 传统的开发模式都是基于关系型数据库的用户认证信息管理模型，读取速度慢，可移植性差。

[0007] 电视台信息化建设需要建立可靠、安全、保密的业务系统网络环境，保证电视台的业务不受破坏和干扰。显然，这些传统的开发模式的诸多弊端已经严重影响了基于 WEB 的应用系统的性能和使用的方便性。

[0008] 所以，在电视台内部提供一个单点登陆方法，为各个业务板块提供集中 配置和统一认证功能是非常有必要的。

[0009] 单点登录 (Single Sign On)，简称为 SSO，是目前比较流行的企业业务整合的解决方案之一。SSO 的定义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。它包括可以将这次主要的登录映射到其他应用中用于同一个用户的登录的机制。

[0010] 目前业界已有很多产品支持 SSO，如 IBM 的 WebSphere 和 BEA 的 WebLogic，但各家 SSO 产品的实现方式也不尽相同。WebSphere 通过 Cookie 记录认证信息，WebLogic 则是通过 Session 共享认证信息。Cookie 是一种客户端机制，它存储的内容主要包括：名字、值、过期时间、路径和域，路径与域合在一起就构成了 Cookie 的作用范围，因此用 Cookie 方式

可实现 SSO，但域名必须相同。Session 是一种服务器端机制，当客户端访问服务器时，服务器为客户端创建一个惟一的 SessionID，以使在整个交互过程中始终保持状态，而交互的信息则可由应用自行指定，因此用 Session 方式实现 SSO，不能在多个浏览器之间实现单点登录，但却可以跨域。通常，在一个电视台内部网络中往往包含了多个子网，每个子网都是一个单独的域，并且各个子网中使用的软件也不全为 B/S 结构，也可能是不使用浏览器的 C/S 结构，所以上述两种方式在电视台的全台网环境下很难实现。

发明内容

[0011] 针对现有技术中存在的问题，本发明的目的是提供一种面向电视台应用的基于 Active Directory 的统一认证实现方法，该方法能够实现处于不同域中的各个应用系统的单点登陆，应用系统可以为 B/S 结构或 C/S 结构。

[0012] 为了实现上述目的，本发明采用的技术方案是，面向电视台应用的基于 Active Directory 的统一认证实现方法，包括如下步骤：

[0013] (1) 在 Active Directory 服务器中统一配置用户信息以及各应用系统的信息；

[0014] (2) 用户第一次登陆一个应用系统成功后，获取一个针对该用户的会话令牌，并将该会话令牌存储到被登陆的应用系统中；

[0015] (3) 当该用户登陆其它应用系统时，首先将步骤 (2) 中存储的针对该用户的会话令牌传递至待登录的应用系统，然后待登陆应用系统通过 Active Directory 服务器验证该用户会话令牌的合法性，如果通过验证，则允许用户登陆，同时更新并返回该用户的会话令牌，并将更新后的会话令牌存入被登陆的应用系统中。

[0016] 如上所述的统一认证实现方法，步骤 (2) 中用户第一次登陆一个应用系统的过程为：将应用系统可区别姓名 DN、用户可区别姓名 DN 以及用户密码传送到 Active Directory 服务器，Active Directory 服务器先根据应用系统的可区别姓名 DN 验证该应用系统是否是统一认证的用户系统，再根据用户可区别姓名 DN 和用户密码验证用户的合法性，如果通过验证，则登陆成功。

[0017] 如上所述的统一认证实现方法，其中，存储会话令牌的过程为：首先调用单点登陆客户端提供的 API，然后利用该 API 将会话令牌存储到被登陆应用系统的注册表中。

[0018] 如上所述的统一认证实现方法，步骤 (3) 中所述的验证会话令牌的合法性的过程为：将会话令牌连同待登陆应用系统的可区别姓名 DN 一起传送到 Active Directory 服务器，Active Directory 服务器先根据待登陆应用系统的可区别姓名 DN 验证该应用系统是否是统一认证的用户系统，然后再验证会话令牌的合法性。

[0019] 如上所述的统一认证实现方法，如果步骤 (3) 中会话令牌的合法性验证失败，则通知待登陆应用系统显示登陆界面，进行独立登陆。

[0020] 如上所述的统一认证实现方法，在用户注销后，应用系统删除该用户的会话令牌。

[0021] 如上所述的统一认证实现方法，所述的会话令牌具有生命期限，当用户登陆超过生命期限后，会话令牌被吊销。

[0022] 本发明所述的方法通过在 Active Directory 服务器中为每个应用系统设置一个 DN 属性，作为会话令牌的唯一标识，应用系统不必像 Cookie 那样使用包含相同的域名的唯一标识，从而可以实现跨域单点登陆的功能。应用系统可以为 B/S 结构也可以为 C/S 结构。

附图说明

[0023] 图 1 是本发明具体实施方式中采用本发明所述方法的系统架构图；

[0024] 图 2 是本发明具体实施方式中所述的方法流程图。

具体实施方式

[0025] 下面结合实施例和附图对本发明的具体实施方式进行详细描述。

[0026] 本发明所述的方法主要应用于广电领域电视台的主干平台系统中，为电视台内各个业务板块提供相关部门结构、栏目结构等信息的集中配置以及用户的单点登陆方法。随着电视台内部业务系统的数字化改造，及台内各种系统网络的构建，往往一个电视台内部形成了采集收录、新闻制播、综合制作、演播网络、编排备播、媒资管理、播出分发等众多的应用系统。工作时，用户经常需要在不同的应用系统之间来回切换，重复验证用户信息，使用非常不便。如何在电视台内部提供一种跨域并且应用系统可以为 C/S 或 B/S 模式的单点登陆 (SSO :Single Sign-On) 方法，为各个应用系统提供集中配置和统一认证的功能便是本发明所要解决的问题。

[0027] 图 1 出示了采用本发明所述方法的系统架构图，主要包括 ActiveDirectory 服务器、单点登陆服务器和单点登陆客户端。Active Directory 服务器用于存储应用系统的组织结构信息以及用户信息，并对用户信息或会话令牌进行认证；单点登陆服务器用于解析客户端传来的认证信息或操作请求，对 Active Directory 服务器进行操作，并获取从 Active Directory 服务器返回的认证或操作结果；单点登陆客户端用于存储并在应用系统之间传递会话令牌。

[0028] 图 2 出示了一种面向电视台应用的基于 Active Directory 的统一认证实现方法，包括以下步骤。

[0029] (1) 在 Active Directory 服务器中统一配置用户信息以及各应用系统的信息。

[0030] Active Directory 是指 Windows 2000/2003 网络中的目录服务。它有两个作用，一是目录服务功能。Active Directory 提供了一系列集中组织管理和访问网络资源的目录服务功能。Active Directory 使网络拓扑和协议对用户变得透明，从而使网络上的用户可以访问任何资源 (例如打印机)，而无需知道该资源的位置以及它是如何连接到网络的。Active Directory 被划分成区域进行管理，这使其可以存储大量的对象。基于这种结构，ActiveDirectory 可以随着企业的成长而进行扩展。二是集中式管理。ActiveDirectory 还可以集中管理对网络资源的访问，并允许用户只登陆一次就能访问在 Active Directory 上的所有资源。

[0031] 本实施例中，采用微软公司的 LDAP 服务器产品 Active Directory 服务器作为电视台内部用户信息的存储体并对用户信息进行验证。首先需要对 Active Directory 服务器进行必要的配置。本实施例中，在 Active Directory 中添加三个根节点，分别为部门结构、栏目结构和应用系统。这三个组织单位节点需要用户手工添加，分别代表电视台内部的部门人员结构、栏目及其栏目成员、电视台全台网中需要实现单点登陆的应用系统。用户可以在这三个根节点下分别添加相应的隶属节点。如在部门结构节点下添加电视台、频道、部门、人员等，其中电视台、频道、部门为组织单位类型的节点，人员为用户类型的节点。在栏

目结构节点下添加具体的栏目名（安全组类型的节点）以及在应用系统节点下添加具体的应用系统。

[0032] 然后设置 Active Directory 服务器的名称项（可以填域控制器的 IP 地址或者“域控制器名．域名．扩展名”）、访问 Active Directory 服务器的用户 DN(Distinguished Name,可区别名称）、访问 Active Directory 服务器的密码、部门人员的根 DN（以节点 DN 格式表示的字符串，对应于部门结构节点）、栏目设置的根 DN（以节点 DN 格式表示的字符串，对应于栏目结构节点）、应用系统的根 DN（以节点 DN 格式表示的字符串，对应于应用系统节点）、会话令牌的最长生命期限（分钟）以及会话日志的保留天数等。会话令牌具有生命期限，当需要保持会话令牌的有效状态时，需要根据会话令牌的失效时间定期激活该会话令牌，否则将过期的会话令牌吊销。会话令牌过期后会被移入会话日志表，为防止会话日志表无限增大，根据设置的会话日志保留天数，决定会话日志的删除策略。

[0033] (2) 用户第一次登陆一个应用系统成功后，获取一个针对该用户的会话令牌，并将该会话令牌存储到被登陆的应用系统中。

[0034] 本实施例中，假设有一个应用系统 App1，首先需要配置 App1 的 DN。DN 是 App1 在 Active Directory 服务器中的唯一标识，由 Active Directory 服务器提供，并存储在 Active Directory 服务器中。

[0035] 用户首次登陆 App1 时，将 App1 的 DN、用户 DN 以及用户密码传送到 ActiveDirectory 服务器，Active Directory 服务器先根据 App1 的 DN 验证 App1 是否是统一认证的用户系统，再根据用户 DN 和用户密码验证用户的合法性，如果通过验证，则登陆成功，否则返回错误消息。

[0036] 当用户登陆 App1 成功后，从单点登陆服务器返回给 App1 一个针对该用户的会话令牌，然后 App1 的客户端程序调用单点登陆客户端提供的 API，利用该 API 将会话令牌存储到 App1 的注册表中。

[0037] 会话令牌是一个 XML 字符串，其结构如下：

[0038] <xs:complexType name ＝″ Token_Type″ >

[0039] <xs:sequence>

[0040] <xs:element name ＝″ TokenID″ type ＝″ xs:string″ >

[0041] <xs:annotation>

[0042] <xs:documentation> 令牌的 ID</xs:documentation>

[0043] </xs:annotation>

[0044] </xs:element>

[0045] <xs:element name ＝″ UserName″ type ＝″ xs:string″ >

[0046] <xs:annotation>

[0047] <xs:documentation> 用户名称 </xs:documentation>

[0048] </xs:annotation>

[0049] </xs:element>

[0050] <xs:element name ＝″ UserDN″ type ＝″ xs:string″ >

[0051] <xs:annotation>

[0052] <xs:documentation> 用户的 DN,DN——

[0053] DistinguishedName</xs:documentation>

[0054] </xs:annotation>

[0055] </xs:element>

[0056] <xs:element name =" CreateTime" type =" xs:string" >

[0057] <xs:annotation>

[0058] <xs:documentation>令牌的创建时间,格式为 :2000-01-01

[0059] 12:12:12</xs:documentaion>

[0060] </xs:annotation>

[0061] </xs:element>

[0062] <xs:element name =" ExpireTime" type =" xs:string" >

[0063] <xs:annotation>

[0064] <xs:documentation>令牌的失效时间,格式为 :2000-01-01

[0065] 12:12:12</xs:documentation>

[0066] </xs:annotation>

[0067] </xs:element>

[0068] <xs:element name =" SystemDN" type =" xs:string" >

[0069] <xs:annotation>

[0070] <xs:documentation>第一次从哪个应用系统登录,此为该应用系统的

[0071] DN,该 DN 在 LDAP 中配置,并告知各个应用系统 </xs:documentation>

[0072] </xs:annotation>

[0073] </xs:element>

[0074] </xs:sequence>

[0075] </xs:complexType>

[0076] (3) 当该用户登陆其它应用系统时,首先将步骤 (2) 中存储的针对该用户的会话令牌传递至待登录的应用系统,然后待登陆应用系统通过 ActiveDirectory 服务器验证该用户会话令牌的合法性,如果通过验证,则允许用户登陆,同时更新并返回该用户的会话令牌,并将更新后的会话令牌存入被登陆的应用系统中。

[0077] 在本实施例中,当用户登陆另一个应用系统 App2 时,App2 的客户端程序 (C/S 模式) 或者浏览器 (B/S 模式,此时需要使用 javascript) 调用单点登陆客户端提供的获得会话令牌函数,获取该用户登陆 App1 后的会话令牌,然后将获得的会话令牌传送到 Active Directory 服务器,ActiveDirectory 服务器先根据 App2 的 DN 验证该应用系统是否是单点登陆的用户系统,再验证会话令牌的合法性。如果通过验证,则允许用户登陆,同时更新并返回该用户的会话令牌,App2 调用单点登陆客户端提供的存储会话令牌函数将更新后的会话令牌保存到 App2 的注册表中,如果失败则通知 App2 的客户端程序或浏览器显示登录界面,独立登录,登录成功后同样需要保存会话令牌。无论是 App1 还是 App2,在用户注销后都需要执行单点登陆客户端提供的删除会话令牌函数,以便单点登陆客户端确定是否有必要保存当前的会话令牌。

[0078] 用户可以用与登陆 App2 同样的方式登陆其他应用系统。

[0079] 此外，实现本发明所述的方法还需要满足以下条件。

[0080] (1) 单点登陆服务器必须隶属于一个 Active Directory 域中，并且单点 登陆服务器能够被要求实现单点登陆功能的应用系统访问。如果不能满足该条件，将无法对 Active Directory 进行相关节点的查询、添加、删除、修改功能，进而导致统一认证功能无法实现。

[0081] (2) 以单点登陆方式访问应用系统时，要以一个对注册表具有操作权限的用户登陆。由于单点登陆客户端在用户登陆的时候将涉及到令牌信息在注册表中的存取和修改操作，如果当前用户不具备对注册表操作的权限，将无法在某个应用系统关闭后，持久化地保存用户会话令牌信息。

[0082] 本发明所述的方法并不限于具体实施方式中所述的实施例，本领域技术人员根据本发明的技术方案得出其他的实施方式，同样属于本发明的技术创新范围。

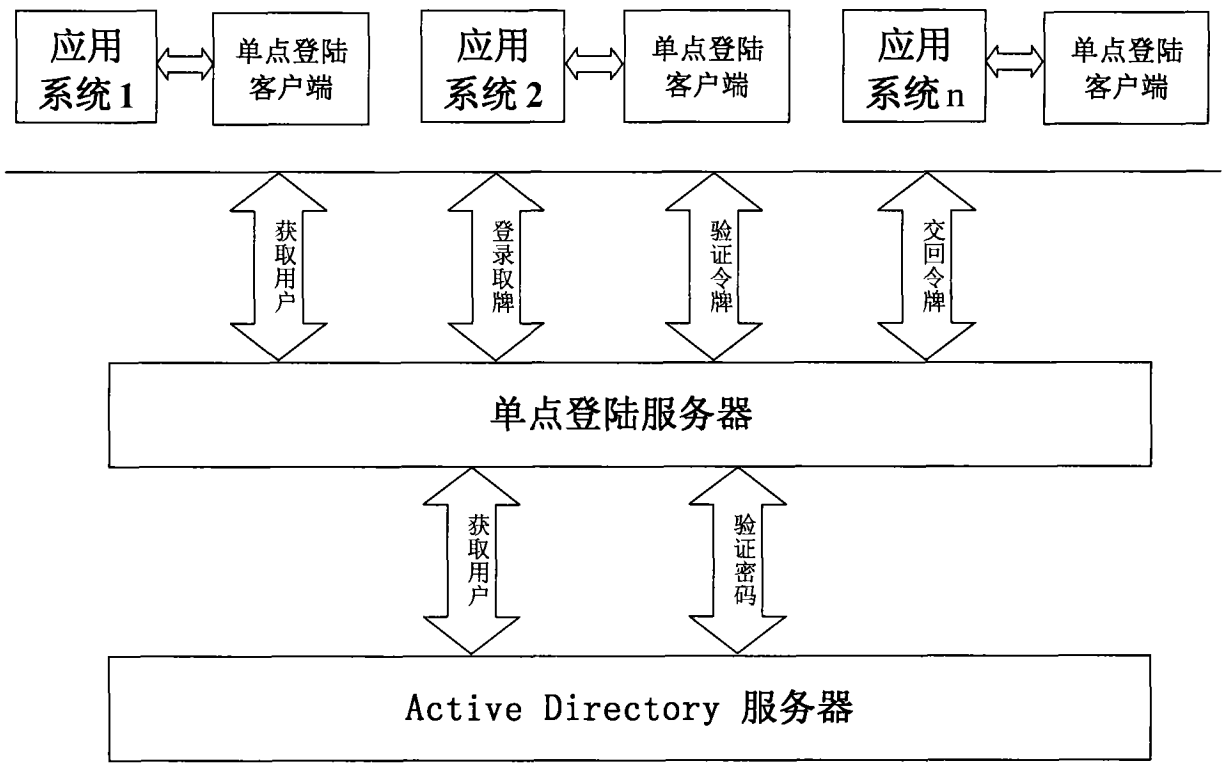

应用系统1
单点登陆客户端
应用系统2
单点登陆客户端
应用系统n
单点登陆客户端
获取用户
登录取牌
验证令牌
交回令牌
单点登陆服务器
获取用户
验证密码
Active Directory 服务器

图 1

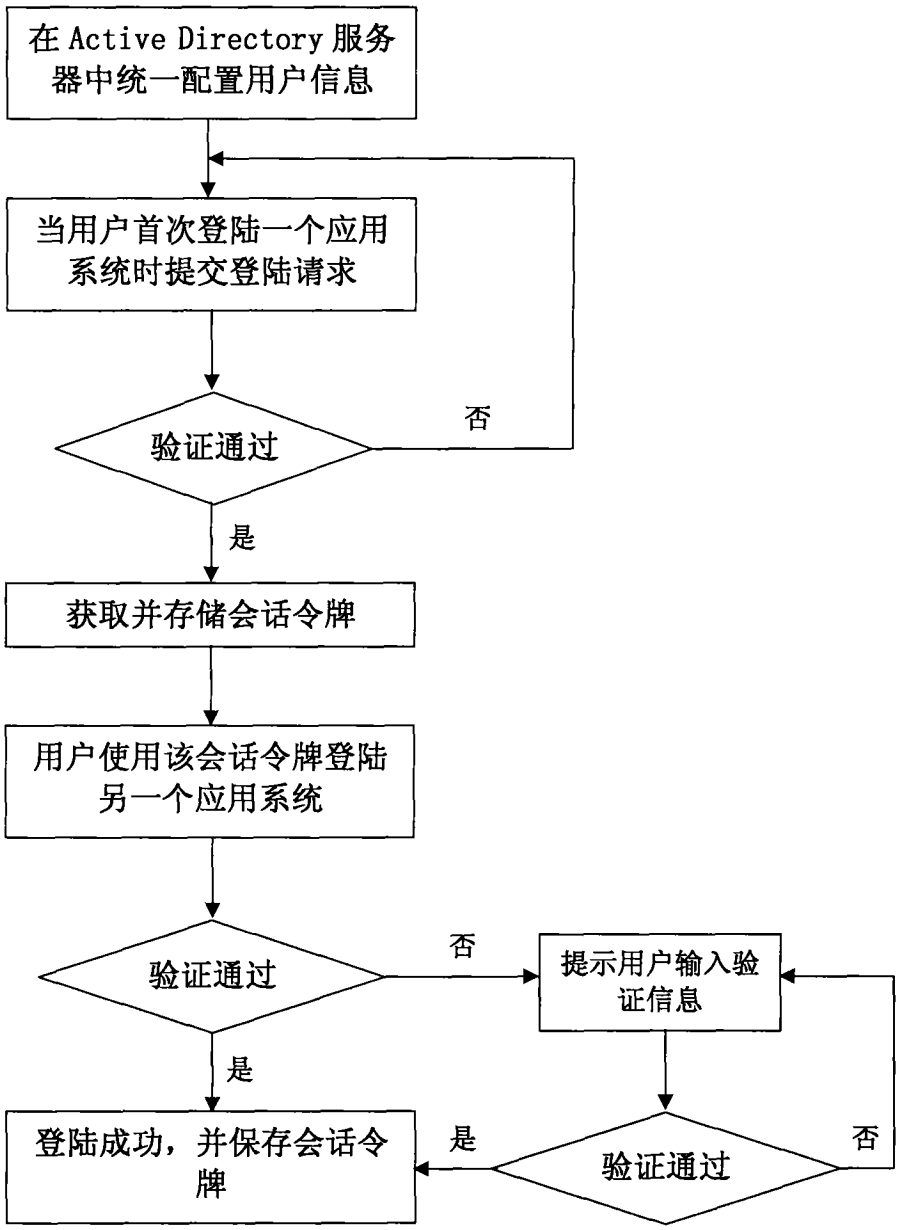

在 Active Directory 服务器中统一配置用户信息
当用户首次登陆一个应用系统时提交登陆请求
验证通过
否
是
获取并存储会话令牌
用户使用该会话令牌登陆另一个应用系统
验证通过
否
提示用户输入验证信息
是
登陆成功，并保存会话令牌
是
验证通过
否

图 2