Computer Science and Application 计算机科学与应用, 2016, 6(5), 265-270
Published Online May 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.65032

Hans汉斯

Education Electronic Identity Based on the Related Certification

Yongjun Wen[1], Cheng Li[1], Jian Wang[2], Zhiliang Fan[2], Junlong Tang[1], Lijun Tang[1]

[1]School of Physical & Electronic Science, Changsha University of Science & Technology, Changsha Hunan
[2]The Education Department of Hunan Province, Changsha Hunan
Email: tanglj2000@263.net

Received: Apr. 29th, 2016; accepted: May 22nd, 2016; published: May 25th, 2016

Abstract

A multi-application systems integration platform has been achieved via associated certification of Education Electronic Identity. Therefore, the network resources are saved and the efficiency of access is improved through Single Sign-On and real-name to access multi-application systems. The Education Department of Hunan Province Xiang Teaching Cloud tests demonstrates that this method doesn't change the independent operating mode of original user system, realizing the resource integration among various independent applications and keeping the ability to respond quickly under high concurrency at the same time.

Keywords

Education Electronic Identity, Related Certification, Single Sign-On

基于教育电子身份号的关联认证

文勇军[1]，李　程[1]，王　键[2]，樊志良[2]，唐俊龙[1]，唐立军[1]

[1]长沙理工大学物理与电子科学学院，湖南　长沙
[2]湖南省教育厅，湖南　长沙
Email: tanglj2000@263.net

收稿日期：2016年4月29日；录用日期：2016年5月22日；发布日期：2016年5月25日

文章引用: 文勇军, 李程, 王键, 樊志良, 唐俊龙, 唐立军. 基于教育电子身份号的关联认证[J]. 计算机科学与应用, 2016, 6(5): 265-270. http://dx.doi.org/10.12677/csa.2016.65032

摘　要

针对多个应用系统组成的集成平台，用教育电子身份号(e^2ID)研究实现关联认证，通过单点登录、实名制访问多应用系统，节省了网络资源，提高了访问效率。经在湖南省教育厅湘教云平台应用测试，该方法在不改变原用户体系独立运行模式的基础上，能够实现各独立应用系统之间的资源整合，并具有高并发情况下的快速响应能力。

关键词

教育电子身份号，关联认证，单点登录

1. 引言

随着信息化水平不断提高，教育系统根据不同时期的业务需求逐步建成了相应功能的应用系统，各应用系统都有相对独立的用户信息库，而且身份认证机制也不尽相同。对用户而言，需要记住每一个应用系统的用户名和密码，登录的次数多，占用资源多，应用效率低。如湘教云平台集成了“湖南基础教育资源网”、“湖南教育资源汇聚与展示中心”、“湖南微课网”等 28 个应用系统，若保留各应用系统的原有用户体系，对湘教云各系统进行统一身份认证，实现单点登录[1]，对于节约资源、提高系统的响应能力和服务能力具有重要意义。本文主要探讨教育身份号实现关联认证的方法，解决湘教云一次登录访问和实名认证的问题。

2. 关联认证方案

湘教云平台独立应用系统多，有庞大的用户访问量，要实现单点登录，平台用户必须具有唯一的身份标识，并通过身份标识在平台应用系统中实现用户关联，且确保重定向凭证标识的安全和大并发情形下的高效响应。

教育电子身份号是与居民身份证号码一一对应的有效标识，已广泛应用于网络实名制管理。以教育电子身份号作为用户身份标识，研究教育电子身份号的关联方法、凭证传递的安全性与凭证注销等内容，设计实现基于教育电子身份号的关联认证方案。

2.1. 单点登录模型

针对应用系统服务，定制应用代理，实现两者之间的安全会话，并建立以用户为中心的单点登录模型[2] [3]。单点登录模型由统一身份认证平台、用户和应用服务三部分组成，如图 1 所示。

身份提供者和凭证提供者为统一身认证平台的基础组成部分，分别负责用户身份认证，生成、存储和校验凭证。应用服务由多个应用服务提供者构成，应用服务提供者包括应用代理与应用系统两个组成部分，应用系统提供服务资源的访问，应用代理负责向凭证提供者请求校验凭证是否有效，减少用户多重访问验证造成身份提供者负担过重问题。

身份提供者对通过身份认证的合法用户，生成用户凭证，并采用信息摘要算法进行加密；在用户利用 URL 重定向访问应用代理服务时，应用代理服务通过校验访问凭证是否有效，判别访问请求是否合法，应用代理服务对有效的访问请求定向至应用系统，应用系统响应用户访问请求，提供服务资源。用户只需要经过一次身份认证，就可以携带身份提供者生成的用户凭证，访问多个应用服务提供者，实现“一次认证，全局漫游”。

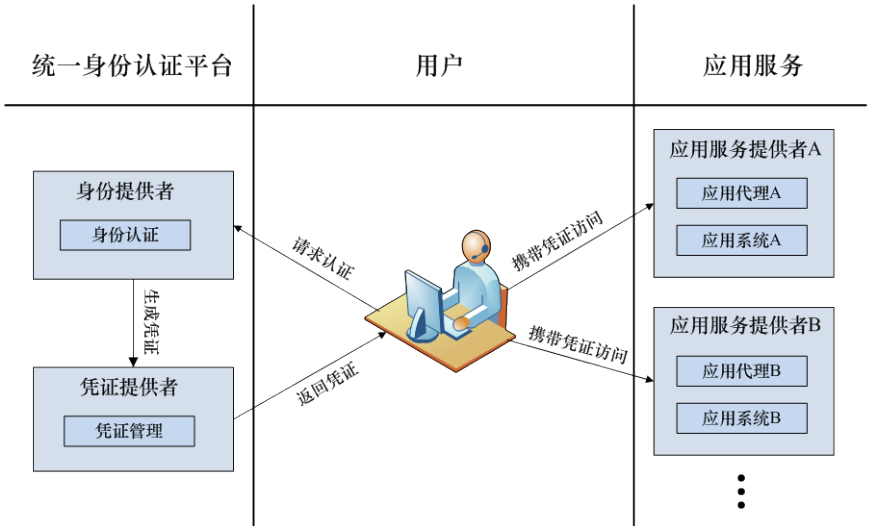

Figure 1. The model of single sign-on
图 1. 单点登录模型

2.2. 教育电子身份号的用户关联方法

单点登录普遍采用集中的用户信息库完成统一身份认证的机制。本文采用基于教育电子身份号的用户关联方法，利用教育电子身份号与应用系统原有用户体系的关联，实现统一的用户信息管理，管理人员无需进行数据同步，在统一认证平台就可以完成所有用户信息的维护，并保障多个应用系统中同一个用户信息数据的一致性。

用户在统一身份认证平台完成并通过身份认证后，通过定制的应用代理服务执行 URL 重定向，应用代理服务会首先查询 URL 中携带的教育电子身份号，是否已经完成与当前应用系统的原有用户信息关联，未完成关联则定向至关联页面。关联时需将教育电子身份号写入应用系统的用户信息库，实现教育电子身份号与应用系统的用户绑定。应用代理服务只对完成教育电子身份号与应用系统用户信息关联的用户，开放对访问服务资源请求的响应。

利用教育电子身份号的用户关联方法，在用户访问应用系统服务资源的同时，实现了教育电子身份号与应用系统原有用户体系的关联，并保留了应用系统原有的用户体系。

教育电子身份号的用户关联方法如图 2 所示。

2.3. 凭证传递的安全性

统一身份认证平台在实现单点登录的过程中，凭证是连接身份认证服务器与应用服务器之间的纽带，用户通过携带凭证进行URL重定向访问应用系统资源，为防止URL篡改而防范攻击，凭证传递的安全性至关重要。

凭证在传递过程中采用 MD5 算法进行加密，MD5 算法是一种提供消息完整性保护的散列函数，URL 重定向时携带 MD5 加密后的凭证和教育电子身份号，凭证校验时，凭证服务器会利用传递过来的教育电子身份号检索出原始的凭证，将原始凭证采用 MD5 算法进行加密，再判定加密后的数据和 URL 重定向携带的基础凭证是否一致，以此对传输过来的凭证是否有效性进行验证，只有通过以上校验过程，应用代理服务才会响应用户的访问请求并定向至相对应的页面。

2.4. 凭证注销

凭证作为统一身份认证平台与应用代理服务之间进行通信的受信任关系，只有在其生命周期内才可

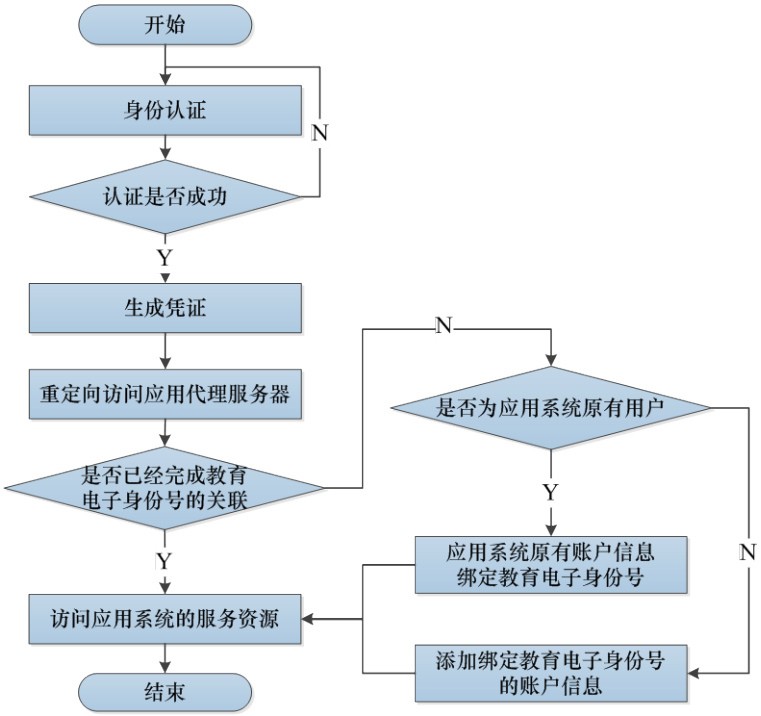

Figure 2. The method of user associated with e2ID
图 2. 教育电子身份号的用户关联方法

以被使用，应该在凭证的生命周期结束时完成对凭证的注销任务，凭证注销[4]有以下三种情况。

1) 统一身份认证平台的注销：当用户发出注销的请求后，首先向凭证服务器发送注销当前凭证的请求，凭证服务器响应请求，删除当前存储在凭证库中的凭证信息，然后再注销当前用户在统一认证平台的会话状态。

2) 浏览器关闭：在统一认证平台的主页的页面脚本的<body>中添加 onbeforeunload 事件，实现对浏览器关闭的监听，在响应 onbeforeunload 事件的 Javascript 脚本中，编写注销当前用户会话的请求，服务器响应用户请求，注销当前会话信息，向凭证服务器发送注销当前凭证的请求。

3) Session 失效：利用 Servlet 规范中定义的事件监听器(Listener)实现对 Session 失效的监听，当 Session 失效时触发 HttpSession 的销毁事件，执行 SessionDestroyed 方法，向凭证服务器发送注销当前凭证的请求。

3. 系统实现

3.1. 系统总体架构

基于教育电子身份号的关联认证系统的总体架构，如图 3 所示。

身份认证服务器：保存用户身份信息，并提供身份认证服务。利用教育电子身份号建立集中的用户管理体系，采取统一身份认证的机制，组建湘教云各个应用系统的公共的统一身份认证平台，达到简化用户操作、优化用户体验，保持各个应用系统之间用户数据的一致性的目的。

凭证服务器：记录用户身份认证生成的凭证，并提供凭证生成与存储、凭证验证、凭证注销等服务。凭证的组成包含了用户的教育电子身份号、认证时间、客户端 IP、统一身份认证平台的 Session ID 等基础信息。

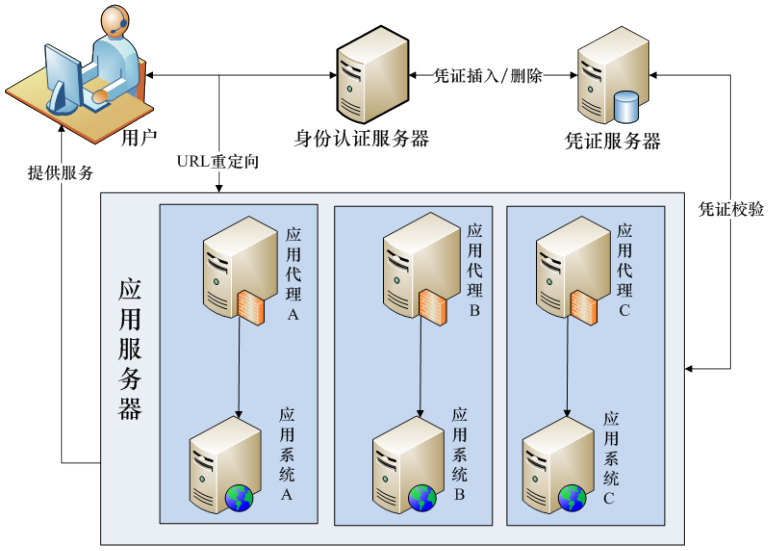

Figure 3. The overall architecture of the related certification system
图 3. 关联认证系统总体架构图

应用服务器：由应用系统与应用代理两部分组成，应用代理针对不同的应用系统而定制开发，并和与其对应的应用系统部署在相同的服务器上，主要负责鉴权用户从统一认证平台发出的访问请求，根据鉴权结果再对用户的访问请求进行重定向，不仅保障了用户在各个应用系统之间的有序切换，而且不需要对进行整合的各个应用系统做出改动。

3.2. 统一身份认证工作流程

统一身份认证的工作流程，如图 4 所示。

1) 用户对应用代理服务发出访问请求，应用代理服务向凭证服务器发送验证请求，在凭证有效的情况下，则执行步骤(4)；凭证无效的情况下，应用代理服务将用户定向至身份认证服务器进行身份认证；

2) 用户身份认证通过的同时，身份认证服务器请求凭证服务器生成用户凭证，然后将认证结果和凭证返回给客户端；

3) 用户携带凭证，执行步骤(1)；

4) 应用系统为用户提供相应的网络资源。

3.3. 服务与部署

采用轻量级的 Rest (Representational State Transfer) 协议的 Web Service 架构[5]，将身份激活、登录认证、凭证校验等服务封装成独立的接口。Rest 模式一种针对网络应用的设计和开发方式，可以降低开发的复杂度，提高系统的可伸缩性，并且在响应速度，性能、效率和易用性上都优于 SOAP 协议，解决了 SOAP 协议的 Web Service 架构下的大并发的性能问题；通过统一的接口标准将服务接入系统平台，保证各个应用服务与系统平台之间的松耦合性和易扩展性；利用 apache 的 proxy_ajp 实现认证服务器的集群，提高大用户下的系统吞吐量及并发响应能力。

3.4. 数据库安全性

采用应用服务器与数据库服务器独立部署的方式，只允许局域网内部指定的服务器访问数据库，隔离数据库服务器与外部网络，加强数据的安全防护等级。

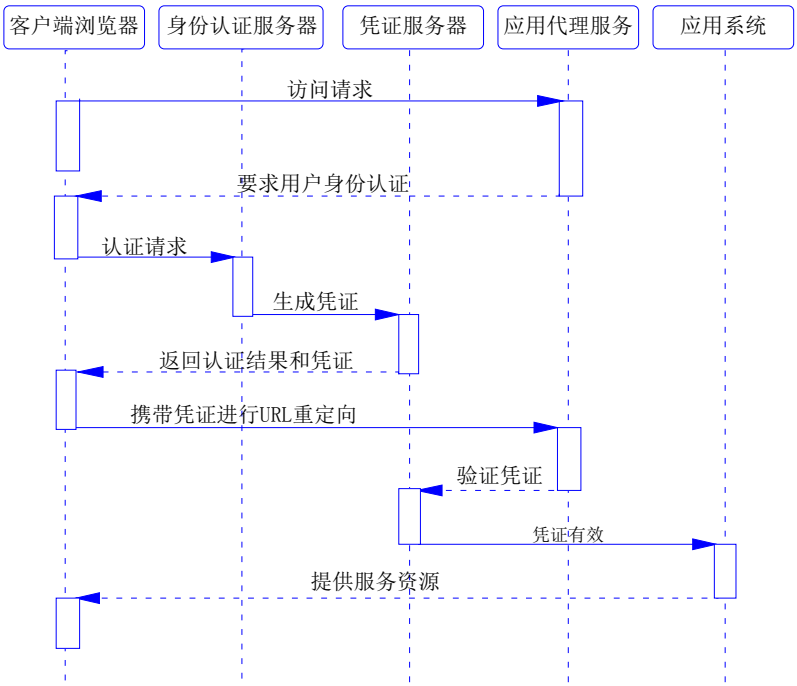

Figure 4. Unified authentication workflow
图 4. 统一身份认证的工作流程

3.5. 应用效果

湘教云平台已有“湖南基础教育资源网”、“湖南教育资源汇聚与展示中心”等七个应用系统接入统一身份认证平台，目前拥有 100 余万教育电子身份号注册用户，从应用效果来看，单点登录为用户解决了多个系统重复登录的麻烦，也没有出现高并发时的网络拥堵问题。

4. 结束语

基于教育电子身份号的关联认证方法，实现多应用系统的单点登录，有利于各独立应用系统资源整合，且不改变原用户体系独立运行的模式，适用于实现网络实名制访问的多应用系统资源整合，在湖南省湘教云应用过程中表现出了良好的并发响应能力，可以进一步推广应用。

基金项目

国家科技支撑计划课题(2014BAH28F04)。

参考文献 (References)

[1] Radha, V. and Hitha Reddy, D. (2012) A Survey on Single Sign-On Techniques. *Procedia Technology*, **4**, 134-139. http://dx.doi.org/10.1016/j.protcy.2012.05.019

[2] Suriadi, S., Foo, E. and Jøsang, A. (2009) A User-Centric Federated Single Sign-On System. *Journal of Network and Computer Applications*, **32**, 388-401. http://dx.doi.org/10.1016/j.jnca.2008.02.016

[3] 王曦, 张斌. 基于代理签名的 SAML 单点登录协议[J]. 计算机工程, 2012, 38(16): 130-133.

[4] Suoranta, S., Manzoor, K., Tontti, A., *et al.* (2014) Logout in Single Sign-On Systems: Problems and Solutions. *Journal of Information Security and Applications*, **19**, 61-77. http://dx.doi.org/10.1016/j.jisa.2014.03.005

[5] 周文哲, 王如龙, 张锦. 基于 REST 软件体系结构研究及应用[J]. 硅谷, 2012(2): 102, 74.