统一身份认证机制研究与分析

李 婕

（四川美术学院网络工作部 重庆 401331）

[摘 要]随着信息技术的高速发展，统一身份认证应用越来越广泛，智慧校园建设中也需要采用易于管理安全度高的认证系统。本文阐述了统一身份认证机制的必要性，分析了身份认证的方式及常见的认证技术，总结了作为智慧校园的重要的基础平台应当建设，为统一身份认证平台的建设做出理论指导。

[关键词]统一身份认证；智慧校园

【DOI】10.12252/j.issn.2096-6261.2020.06.1105

1.为什么要实现统一身份认证

智慧校园具有统一性和一致性，这与应用系统的独立性和多样性特点存在矛盾。各应用系统因安全策略和授权方法不同，各具有不同的帐号和口令，这种独立认证的方式不管对于用户还是对于应用系统的整合都是一件麻烦的事情。

弊端如下：

1.1用户身份不一致：同一用户在不同的应用系统中可能存在不同的属性，拥有不同的权限及优先级定义，相互矛盾，最终造成一个用户在数字校园中有多个不同身份。

1.2用户信息无法统一：当一个用户的属性发生变化时，只是有限的应用系统进行更改，其他系统无法同步更新，造成用户信息无法统一。

1.3信息重复：对整个系统来说，同一个用户信息在不同应用系统中重复存放，数据冗余量过大，造成信息管理成本上升，性能下降。

1.4增加用户操作的复杂性：用户在使用不同应用系统时，需要记忆不同的用户名及口令，需要反复登录系统，操作相对复杂、烦琐。

1.5增加用户信息维护难度：当用户信息变更时，需要同时修改不同应用系统的大量信息，增加管理难度。

2.统一身份认证方式

目前，计算机及网络系统中常用的身份认证方式主要有以下几种：

2.1用户名/密码方式

用户名/密码是最简单也是最常用的身份认证方法，每个用户的密码是由用户自己设定的，只有用户自己才知道。只要能够正确输入密码，计算机就认为操作者就是合法用户。实际上，由于许多用户为了防止忘记密码，经常采用诸如生日、电话号码等容易被猜测的字符串作为密码，这样很容易造成密码泄漏。即使能保证用户密码不被泄漏，由于密码是静态的数据，在验证过程中需要在计算机内存中和网络中传输，而每次验证使用的验证信息都是相同的，很容易被驻留在计算机内存中的木马程序或网络中的监听设备截获。因此，从安全性上讲，用户名/密码方式一种是极不安全的身份认证方式。

2.2智能卡认证

智能卡是一种内置集成电路的芯片，芯片中存有与用户身份相关的数据，智能卡由专门的厂商通过专门的设备生产，是不可复制的硬件。智能卡由合法用户随身携带，登录时必须将智能卡插入专用的读卡器读取其中的信息，以验证用户的身份。智能卡认证通过智能卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从智能卡中读取的数据是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息，因此还是存在安全隐患。

2.3动态口令

动态口令技术是一种让用户密码按照时间或使用次数不断变化、每个密码只能使用一次的技术。它采用动态令牌的专用硬件，内置电源、密码生成芯片和显示屏，密码生成芯片运行专门的密码算法，根据当前时间或使用次数生成当前密码并显示在显示屏上。认证服务器采用相同的算法计算当前的有效密码。用户使用时只需要将动态令牌上显示的当前密码输入客户端计算机，即可实现身份认证。由于每次使用的密码必须由动态令牌来产生，只有合法用户才持有该硬件，所以只要通过密码验证就可以认为该用户的身份是可靠的。而用户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

2.4 USB Key认证

基于USB Key的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key是一种USB接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用USB Key内置的密码算法实现对用户身份的认证。基于USB Key身份认证系统主要有两种应用模式：一是基于冲击/响应的认证模式，二是基于PKI体系的认证模式。

3.认证技术

3.1消息摘要

消息摘要算法的主要特征是加密过程不需要密钥，并且经过加密的数据无法被解密，只有输入相同的明文数据经过相同的消息摘要算法才能得到相同的密文。消息摘要主要用于保证数据的完整性，校验和就是消息摘要的一个特例。它有两个基本属性：不同的报文无法产生相同的消息摘要；消息摘要是单向函数，只能进行正向的信息摘要，无法从摘要中恢复出任何消息。

3.2数字签名

数字签名使用了消息摘要算法和公开密钥技术。首先对消息进行哈希运算，产生消息摘要，发送者用自己的私钥加密消息摘要后产生一段字串，然后把此字串附加到要发送的消息之后传给接受者接收者收到报文后，就可以用发送者的公钥对数字签名进行验证，确定消息来源于谁，同时也是对发送者发送信息完整性的一个证明。由于发送者的私钥是私有保密的，发送者对所发信息不能抵赖。

3.3数字证书

数字证书是目前国际上最成熟并得到广泛应用的信息安全技术。数字证书是一个经过证书授权中心数字签名的包含公开密钥拥有者信息和公开密钥的文件。数字证书将身份和一对可以用来加密和签名的电子密钥相绑定。数字证书以密码学为基础，采用数字签名、数字信封、时间戳服务等技术，在互联网上建立有效的信任机制。数字证书能够验证一个人使用给定密钥的权利，有助于防止他人利用假密钥冒充其他用户。

3.4生物识别技术

生物识别技术是利用人体生物特性进行身份认证的一种技术。生物特征是唯一的，可以被测量或可自动识别和验证的生理上的，如虹膜识别技术、面部识别、声音识别、指纹识别等。其原理是对生物特征进行取样，提取其唯一的特征，转化成数字代码，并进一步将这些代码组成特征模板加以存储。当人们同识别系统交互进行身份认证时，识别系统获取其特征并与数据库中的特征模板进行对比，以确定是否匹配，从而决定接受或拒绝该人。

4.总结

统一身份认证机制是一项易于管理、安全性高的认证方式，应当在智慧校园中加以应用，作为智慧校园的基础平台是必要的，可以有规划、有步骤、有协调的建设完成认证平台系统。

参考文献

[1]郝辉，钱华林.网络服务系统统一身份认证模型的研究与设计[J].计算机科学，2005，32（009）：72-75.

校企共建混合所有制实训基地的研究与探索

孙承智

（辽宁石化职业技术学院 辽宁 锦州 121000）

[摘 要]辽宁石化职业技术学院与中石油锦州石化分公司在校区共建混合所有制实训基地研究过程中，就如何实现校企双赢、如何建立长效机制等方面进行了探索，实践表明校企合作共建混合所有制实训基地对教学改革、“双师型”教师培养、学生就业、服务地方等方面起到了积极的作用。

[关键词]校企共建；混合所有制

【DOI】10.12252/j.issn.2096-6261.2020.06.1106

职业教育虽然发展了很多年，但是大部分的学校仍然处于教学和管理学生为主的思想中，并没有实现市场化，没有融入行业和企业的变革中，所以使企业共同参与到职业院校人才培养模式和教学课程的设计中，探索培养更符合社会和企业需求的高质量的技术技能型人才已迫在眉睫。

一、探索公办高职院校混合所有制的意义

混合所有制职业院校是指由国有资本、集体资本、非公有资本等不同所有制中的两个或者两个以上的共同主体举办，产权结构与治理主体的多元化是其本质。在公办高职院校中进行混合所有制的改革和探索有着以下的意义。

（一）引进社会资本到学校办学，增加办学实力。有效缓解实训资源单一的局面，通过学校与企业优势互补，强强联合，有利于实现学生技能“岗位零对接”。

（二）可以进一步激发办学的活力。将企业的资本、知识、技术、管理优势融入办学，调动校企双方的优势资源投入到人才培养、招生就业、产业发展等方面，摆脱一些原有的制度缺陷，增强活力。

（三）促进公办院校人才培养质量的提升。企业能准确掌握需要什么样的人才，根据需求设计培养人才方案，并深入教学课程设计，有的放矢，有针对性的提升学生技术技能。

二、学院具体做法和取得的成效

1.解放思想、转变观念，认识先行

（1）深化校企合作办学思想的大讨论，统一思想、提高认识、推进改革。（2）确定了“合作办学，利益考量、特色发展、成果共享”的合作理念。（3）打破资产所有制的陈旧观念，倡导 “不为我所有，而为我所用”的资产观。（4）建立你中有我、我中有你的楔入式合作。

2.校企共建西区实训基地

西区实训基地建设是实践教学的根本保障，是特色办学的重要体现，是校企合作的楔合点和融合点，已经成为知识整合、技能训练、信息交流与资源共享的开放式多元化平台，其教育功能拓展得到企业资源的有效支撑。实训基地既保证了工学