

SAKAI Öğrenme Yönetim Sisteminde Tek Şifre Yönetimi

İrfan SÜRAL¹

¹ Eskişehir Osmangazi Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Eskişehir

isural@gmail.com

Özet: Bu çalışmada yükseköğrenime özelleşmiş, dünya üzerinde yaygın kullanıma sahip ve açık kaynak kodlu bir öğrenme yönetim sistemi olan Sakai’de tek şifre yönetiminin (single sign on) kullanımı hakkında bilgi verilecektir. Çalışmada alanyazın taraması yönteminden ve yazarın Sakai deneyimlerinden yararlanılacaktır. Bu bağlamda Sakai öğrenme yönetim sistemine tek şifre yönetiminin bütünleştirilmesi ve bu bütünleştirmenin detayları sunulacaktır. Ayrıca yazar Microsoft Active Directory üzerinde yer alan öğrenci hesaplarının LDAP hizmeti kullanılarak Sakai sistemine entegrasyonu ile ilgili deneyimlerini paylaşacaktır.

Anahtar Sözcükler: Sakai, LMS, LDAP, Tek Şifre Yönetimi, Microsoft Dizin Hizmetleri

Single Sign On in SAKAI Learning Management System

Abstract: In this paper, information about single sign on services in Sakai learning management system which is open source and widely used in higher education will be given. This study mainly based on authors’ Sakai experiences, and literature review method. In this context, single sign on integration of Sakai learning management system and details of this integration will be presented. In addition, author will share integration experiences about Microsoft Active Directory student account integration which are configured to support LDAP on Sakai.

Keywords: Sakai, LMS, LDAP, Single Sign On, Microsoft Active Directory.

1. Giriş

Artan eğitim ihtiyacını karşılamada kullanılan ve özellikle ülkemizde son yıllarda ivme kazanan uzaktan eğitim uygulamalarında içerik, öğrenen, eğitici arasında iletişim ve etkileşimi sağlamak için farklı birçok sistem kullanılmaktadır. Bu sistemlerin başında Öğrenme Yönetim Sistemleri (ÖYS) gelmektedir. Öğrenme yönetim sistemleri, eğitim içeriklerinin yönetimine, öğrenenler ve eğiticilerin izlenmesine, öğrenme öğretme süreçlerinin bireyselleştirilebilmesine olanak sağlayan bütünleşik sistemlerdir (Ozarslan, Süral, & Ozan, 2011). Dahası öğrenme yönetim sistemleri eş zamansız öğrenme malzemesi sunma, derslere kayıt olma, ödev ve projeler alma, sınavlara girme, ödev ve sınavlara ilişkin dönüt alma, öğrenen, eğitici ve sistem kayıtlarını tutma, raporlar alma gibi birçok

işlemi gerçekleştiren sistemlerdir. Günümüzde gerek ticari gerekse açık kaynak kodlu birçok öğrenme yönetim sistemi bulunmaktadır. Öğrenme yönetim sistemleri yüksek öğretimde ağırlıklı olarak uzaktan eğitim faaliyetlerini gerçekleştirmek için kullanılırken ilköğretim kademelerinde ise yüz-yüze eğitimi desteklemek için kullanılmaya başlanmıştır. Bu öğrenme yönetim sistemlerinden dünya üzerinde kayıtlı 350’den fazla eğitim kuruluşu tarafından kullanılan Sakai daha çok yüksek öğretime özelleştirilmiş açık kaynak kodlu bir öğrenme yönetim sistemidir (Ozarslan, 2012). Indiana Üniversitesi, Massachusetts Teknoloji Enstitüsü, Stanford Üniversitesi, Michigan Üniversitesi ve Valencia Polytechnic Üniversitesi önderliğinde oluşturulan “SakaiFoundation” organizasyon

yapısı altında akademik, ticari ve bireysel katılımlarla geliştirilen işbirliği ve öğrenme ortamıdır (Collaboration and Learning Environment (CLE)) (SakaiProject, 2012). Bilgi toplumu ile beraber insanlar farklı birçok sistem kullanmaya başlamıştır. Sistemlerin sayısı arttıkça kullanıcıların bu sistemlere erişmesi için kullandıkları kullanıcı adı ve şifrelerinin sayısı da artmış, bu durum bilgi güvenliği ve hesap karmaşasına neden olmuştur (Liang & Chen, 2012). Kullanıcılar farklı sistemler için genelde basit ve aynı kullanıcı adı, şifresini kullanmakta bu durum hesap bilgilerinin kolaylıkla ele geçirilmesine ve dolayısıyla sistem güvenliğinin tehlikeye girmesine neden olmaktadır. Sistem yöneticileri farklı sistemler için birçok veri tabanı kullanıcısı ve yetkilendirmesine ihtiyaç duymakta bu durum yönetim karmaşıklığını artırmaktadır. Tek şifre yönetimi bu problemi ortadan kaldırmak için sunulan bir çözüm önerisidir.

Birçok üniversite ve eğitim kurumu öğrenme yönetim sistemleri ile beraber kütüphane bilgi sistemleri, öğrenci bilgi sistemleri gibi farklı birçok hizmet için piyasada bulunan farklı çözümler kullanılmaktadır. Bu çözümlerin çoğu birbiri ile haberleşememekte dolayısıyla her bir hizmet için farklı kullanıcı hesapları oluşturulmaktadır. Günümüzde farklı sistemlerin haberleştirilmesi için kurumlar ya ek yazılımlar ile servislerin haberleşmesini sağlamakta ya da tek şifre yönetimi gibi çözümler kullanılmaktadır.

Bu çalışmada Sakai öğrenme yönetim sisteminin LDAP servisini kullanarak tek şifre yönetimi yapılandırılması hakkında bilgi verilecektir. Microsoft Active Directory üzerinde bulunan öğrenci hesapları LDAP servisi aracılığı Sakai öğrenme yönetim sistemine tek şifre yönetimi ile bütünleştirilmiştir. Çalışmada yapılandırma deneyimleri ve Sakai öğrenme yönetim sisteminin desteklediği tek şifre yönetimleri incelenmiştir.

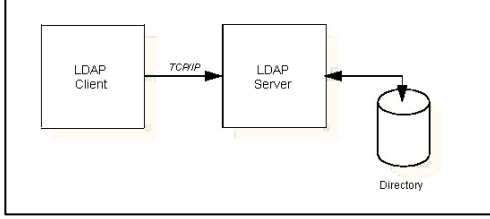
2. Tek Şifre Yönetimi (Single Sign On)

Tek Şifre Yönetimi (SSO) (ayrıca Enterprise Single Sign On veya "ESSO" olarak da bilinir), bir kuruluş içinde birden fazla uygulamaya oturum açmak için aynı kullanıcı adı ve şifreyi kullanabilme yeteneğidir. Tek şifre yönetimi ile kullanıcı oturumu bir kez açar ve buna bağlı tüm sistemlerde tekrar oturum açma zorunluluğu olmadan verilen yetkiler çerçevesinde başka uygulamalara erişir. Şifre ile erişim en düşük güvenlik mekanizmalarından biri olup tek şifre yönetimi düşük risk taşıyan portal uygulamaları, web sayfaları vb. üyelik sistemlerinde kullanılmaktadır (AuthenticationWorld, 2012). Bordro, otomasyon gibi sistemlerde tek şifre yönetimi ile beraber dijital kimlik, dijital sertifikalar ve güvenlik belirteçleri de kullanılabilir. Tek şifre yönetimi yazılımı internet üzerinden tarayıcı aracılığı ile gelen her isteğin kimlik doğrulama ilkesi taşıyıp taşımadığını kontrol etmek durumundadır. Kullanıcının farklı her bir URL adresine tıklama işlemi gerçekleştirdiğinde web uygulama sunucusu ile web tarayıcısı ve güvenlik sunucusu arasında bir trafik meydana gelmektedir. Bu trafik büyük ve performans açısından bakıldığında hantal olabilir. Bu nedenle birçok modern tek şifre yönetim sistemi kimlik doğrulama ve yetkilendirme ilkelerini saklamak için LDAP (Lightweight Directory Access Protocol – Basit Dizin Erişim Protokolü) dizinini kullanmaktadır. LDAP dizinleri yüksek performanslı aramalar dolayısıyla yüksek trafik yükü için kullanılır.

3. LDAP Kimlik Doğrulaması

LDAP ağ hizmetlerinin yerleştirilmesi için ortaya çıkmış , TCP/IP üzerinde çalışan izin servislerini sorgulama ve değiştirme amacıyla kullanılan uygulama katmanı protokolüdür. X.500 dizinlerinin gerektirdiği 7 katmanlı OSI katmanı yerine hafifleştirilmiş (lightweight) olan 4 katmanlı TCP/IP kullanılmıştır (Şen, 2001). LDAP

mesaj tabanlı bir protokol olup, istemci bir anda birden fazla istemde bulunabilir. Örneğin bir istemci aynı anda iki arama işlemini aynı anda yapabilir. Birden fazla işlemi aynı anda yapabilmeyi mümkün kılması LDAP protokolünü buna izin vermeyen HTTP ve benzeri protokollere göre daha esnek ve verimli bir protokol yapmaktadır.



Şekil 1: LDAP protokolü

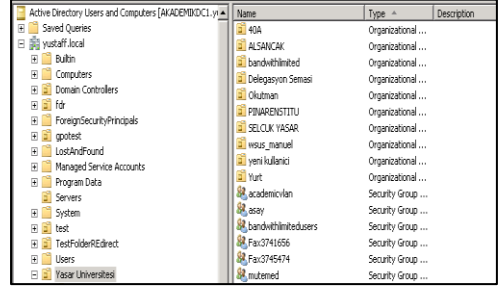
LDAP protokolünü hayata geçirmek için birtakım sunucu yazılımları mevcuttur. OpenLDAP, Sun Directory Server, Microsoft Active Directory, Novell eDirectory, Apple Open Directory bu yazılımlardan bazılarına örnek olarak verilebilir. LDAP protokolünün en yaygın kullanımı Microsoft Active Directory dizin yapısı üzerinde görülmektedir.

4. Microsoft Active Directory

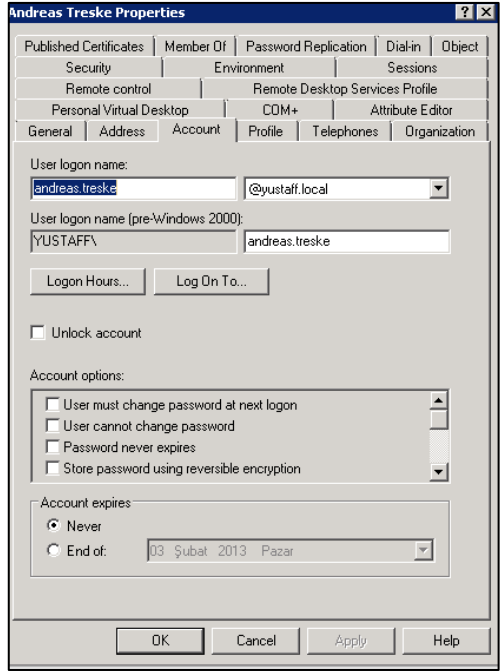
Active Directory, Microsoft ağlarında kullanılan dizin hizmetidir. Bu veritabanı, kullanıcılar, bilgisayarlar, mekanlar, yazıcılar gibi organizasyonun tüm bilgilerini saklar. Bu dizin vasıtasıyla çeşitli yönetimsel kısıtlamalar oluşturulabilir ya da kullanıcıların çalışma ortamları ihtiyaçlar ve standartlar doğrultusunda şekillendirilebilir (Vikipedi, 2013). Microsoft Active Directory dizin hizmeti üzerinde oluşturulacak hesaplar her kurumun organizasyon yapısına uygun bir şekilde kurulan servis aracılığı ile rahatlıkla oluşturulabilir.

Şekil 2’de Microsoft Active Directory’de organizasyon üniteleri ve oluşturulan hesaplar paylaşılmıştır. Şekil 3’te ise oluşturulan bir hesabın özelliklerini

değiştirmek için kullanılan uygulama penceresi yer almaktadır.



Şekil 2: Microsoft Active Directory Ekranı



Şekil 3: Active Directory Hesap Yönetimi

Active Directory içindeki her bir nesnenin adı vardır. Bu adı Distinguished Name denir. Bu adlar nesnenin bulunduğu domain’i tanımlar. Tipik bir Distinguished adı şu şekilde tanımlanır:

DC=com, DC=ogu, CN=Kullanıcılar, CN=Tansu Mutlu

Burada ogu.com domaini içinde Tansu Mutlu için bir Distinguished ad tanımlanmıştır.

5. Sakai LDAP Entegrasyonu

Sakai ile entegrasyon öncesinde Sakai öğrenme yönetim sistemine erişim yetkisi verilecek hesapların Microsoft Active Directory dizininde hangi organizasyon ünitesi (OU) içinde yer alacakları belirlenmeli ve erişecek tüm hesaplar burada yer almalıdır. Bu işlem ardından LDAP sorgusu ile Microsoft Active Directory'deki hesaplar üzerinde sorgulama yapılıp yapılamadığı kontrol edilmelidir. Aksi durumda yapılandırma sonrasında sorunun nedenini anlamak bir hayli araştırma gerektirmektedir. Active Directory servisine LDAP ile bağlantı testi için Sakai kurulan makineden ldapsrch ile aşağıdaki komut verilebilir.

```
ldapsrch -LLL -h ogu.com -p 389 -b
'dc=ogu,dc=com' -D 'testhesap' -w 'testsifre'
'(sAMAccountName=ogrenci_no)'
```

Bağlantı testi başarılı ise Sakai öğrenme yönetim sistemine bütünleştirme için gerekli yapılandırmaya başlanabilir. Sakai LDAP entegrasyonu için JLDAP bileşenini kullanmaktadır. JLDAP, OpenLDAP projesi ile geliştirilen ve Java tabanlı sınıf kütüphaneleridir. OpenLDAP, LDAP'ın OpenLDAP Project tarafından geliştirilmiş açık kaynak kodlu bir uygulamasıdır.

Sakai 2.5 ve üst sürümlerinde entegrasyon adımları aşağıda verilmiştir:

1. Sakai kaynak kodunda bulunan aşağıdaki adreste JLDAP desteği etkinleştirilmelidir.

Dosya adı: pom.xml

sakai-kaynak/providers/component/pom.xml

```
<dependency>
<groupId>org.sakaiproject</groupId>
<artifactId>sakai-jldap-provider</artifactId>
<version>${sakai.version}</version>
```

```
</dependency>
<dependency>
<groupId>openldap</groupId>
<artifactId>ldap</artifactId>
<version>2005.03.29</version>
</dependency>
```

2. Jldap-beans.xml etkinleştirilmelidir.

Dosya adı: jldap-beans.xml

sakai-
kaynak/providers/component/src/webapp/W
EB-INF/jldap-beans.xml

```
<import resource="jldap-beans.xml" />
```

3. Son olarak jldap-beans.xml dosyasında LDAP parametreleri düzeltilmelidir.

ldapHost: LDAP servis adı

basePath: OU ve DC ayarlarının yapılacağı yer

ldapUser: Eğer LDAP servisine erişim bir hesap ile gerçekleşiyorsa yani herkese açık değilse, bunun için oluşturulan hesap tanımlanmalıdır.

ldapPassword: LDAP servisine erişim için oluşturulan ldapUser şifresi.

LDAP ile Sakai hesap alanlarının eşleştirilmesi

```
<property name="attributeMappings">
<map>
<entry key="login"><value>cn</value></entry>
<entry key="distinguishedName">
<value>distinguishedName</value></entry>
<entry key="firstName">
<value>givenName</value></entry>
<entry key="lastName">
<value>sn</value></entry>
<entry key="email">
<value>mail</value></entry>
</map>
</property>
```

Eşleştirme alanlarında <value> alanına sahip olunan LDAP alanları yazılmalıdır.

Sakai-kaynak/providers bileşeni tekrar derlenmelidir. Servis başlatılmadan önce

sakai.properties dosyasında aşağıdaki özellikler eklenerek olası hata vb. loglar elde edilebilir.

```
log.config.count=1
log.config.1 =
DEBUG.edu.amc.sakai.user.JLDAPDirectoryProvider
```

6. Sonuç ve Öneriler

Günümüze kurumların hesap yönetimleri ile başa çıkabilmeleri için sistemlerin birbiri ile entegre olması son derece önem arz etmektedir. Gerek açık kaynak kodlu, gerekse ticari birçok öğrenme yönetim sisteminin entegrasyon ayarları farklılık göstermektedir. Özellikle Sakai öğrenme yönetim sistemi ile ilgi yapılandırma deneyimleri oldukça sınırlıdır. Sakai öğrenme yönetim sistemi ile tek şifre yönetimi bütünleştirilmesi gerçekleştirecek olan kurumlar öncelikle LDAP servisinin sağlıklı hizmet verdiğine emin olmalı ardından yapılandırma işlemine geçmelidirler. Ayrıca Sakai'nin LDAP desteği için gerekli bileşenler devreye alınmalı ve yerel hesap oluşturmaktan kaçınılmalıdır. Şifre yönetimi entegrasyonu sonrasında Sakai öğrenme yönetim sisteminde derslere hesapların eklenmesi kullanıcı adı araması üzerinden gerçekleştirilmelidir.



Username	Email Address	Role
1000000001	1000000001@edu.amc.sakai.edu.tr	Student
1000000002	1000000002@edu.amc.sakai.edu.tr	Student
1000000003	1000000003@edu.amc.sakai.edu.tr	Student
1000000004	1000000004@edu.amc.sakai.edu.tr	Student
1000000005	1000000005@edu.amc.sakai.edu.tr	Student
1000000006	1000000006@edu.amc.sakai.edu.tr	Student
1000000007	1000000007@edu.amc.sakai.edu.tr	Student
1000000008	1000000008@edu.amc.sakai.edu.tr	Student
1000000009	1000000009@edu.amc.sakai.edu.tr	Student
1000000010	1000000010@edu.amc.sakai.edu.tr	Student
1000000011	1000000011@edu.amc.sakai.edu.tr	Student
1000000012	1000000012@edu.amc.sakai.edu.tr	Student
1000000013	1000000013@edu.amc.sakai.edu.tr	Student
1000000014	1000000014@edu.amc.sakai.edu.tr	Student
1000000015	1000000015@edu.amc.sakai.edu.tr	Student
1000000016	1000000016@edu.amc.sakai.edu.tr	Student
1000000017	1000000017@edu.amc.sakai.edu.tr	Student
1000000018	1000000018@edu.amc.sakai.edu.tr	Student
1000000019	1000000019@edu.amc.sakai.edu.tr	Student
1000000020	1000000020@edu.amc.sakai.edu.tr	Student
1000000021	1000000021@edu.amc.sakai.edu.tr	Student
1000000022	1000000022@edu.amc.sakai.edu.tr	Student
1000000023	1000000023@edu.amc.sakai.edu.tr	Student
1000000024	1000000024@edu.amc.sakai.edu.tr	Student
1000000025	1000000025@edu.amc.sakai.edu.tr	Student
1000000026	1000000026@edu.amc.sakai.edu.tr	Student
1000000027	1000000027@edu.amc.sakai.edu.tr	Student
1000000028	1000000028@edu.amc.sakai.edu.tr	Student
1000000029	1000000029@edu.amc.sakai.edu.tr	Student
1000000030	1000000030@edu.amc.sakai.edu.tr	Student
1000000031	1000000031@edu.amc.sakai.edu.tr	Student
1000000032	1000000032@edu.amc.sakai.edu.tr	Student
1000000033	1000000033@edu.amc.sakai.edu.tr	Student
1000000034	1000000034@edu.amc.sakai.edu.tr	Student
1000000035	1000000035@edu.amc.sakai.edu.tr	Student
1000000036	1000000036@edu.amc.sakai.edu.tr	Student
1000000037	1000000037@edu.amc.sakai.edu.tr	Student
1000000038	1000000038@edu.amc.sakai.edu.tr	Student
1000000039	1000000039@edu.amc.sakai.edu.tr	Student
1000000040	1000000040@edu.amc.sakai.edu.tr	Student
1000000041	1000000041@edu.amc.sakai.edu.tr	Student
1000000042	1000000042@edu.amc.sakai.edu.tr	Student
1000000043	1000000043@edu.amc.sakai.edu.tr	Student
1000000044	1000000044@edu.amc.sakai.edu.tr	Student
1000000045	1000000045@edu.amc.sakai.edu.tr	Student
1000000046	1000000046@edu.amc.sakai.edu.tr	Student
1000000047	1000000047@edu.amc.sakai.edu.tr	Student
1000000048	1000000048@edu.amc.sakai.edu.tr	Student
1000000049	1000000049@edu.amc.sakai.edu.tr	Student
1000000050	1000000050@edu.amc.sakai.edu.tr	Student

Şekil 4: Sakai'de LDAP ile bütünleştirilen ve derse eklenen kullanıcı listesi

Kaynakça

- AuthenticationWorld. (2012, Aralık 30). *Single Sign On*. Authentication World: <http://www.authenticationworld.com/Single-Sign-On-Authentication/> adresinden alınmıştır
- Liang, Z., & Chen, Y. (2012). The Design and Implementation of Single Sign-on Based on Hybrid Architecture. *Journal of Networks*, 7(1), 165-173.
- Ozarslan, Y., Süral, İ., & Ozan, Ö. (2011). Yüksek Öğretime Özelleşmiş Öğrenme Yönetim Sistemi Çözümü:Açık Kaynak Kodlu Sakai İşbirliği ve Öğrenme Ortamı. *Akademik Bilişim 2011*, (s. 865-871). Malatya.
- Özarslan, Y. (2012). Sakai OAE : Açık Akademik Ortam. *Akademik Bilişim 2012*. Uşak.

- SakaiProject. (2012). *Sakai Project*. Aralık 25, 2012 tarihinde <http://www.sakaiproject.org/> adresinden alındı
- Şen, Ç. F. (2001). *LDAP Nedir ?* Aralık 25, 2012 tarihinde Enderunix.org: http://www.enderunix.org/docs/ldap_fundamentals/ adresinden alındı
- Vikipedi. (2013, Ocak 02). *Vikipedi, özgür ansiklopedi*. Active Directory: http://tr.wikipedia.org/wiki/Active_Directory adresinden alınmıştır