Yazılımlar için web servis destekli bütünleşik hesap yönetimi

Güncel Sarıman[1], Onur KARASOY[2], Fatih Tarlacı[3], Bilal Durmuş[4]

[1] Süleyman Demirel Üniversitesi, Elektronik ve Haberleşme Mühendisliği Bölümü, Isparta

[2,3,4] Muğla Sıtkı Koçman Üniversitesi, Bilgi İşlem Dairesi, Muğla

guncelsariman@mu.edu.tr, okarasoy@mu.edu.tr, fatihtarlaci@mu.edu.tr, bilal@mu.edu.tr

Özet: Yazılımlar için web servis destekli bütünleşik hesap yönetimi: Yazılımların günlük hayatta kullanımının giderek yaygınlaşması daha hızlı ve kullanılabilir yazılımların geliştirilmesini zorunlu hale getirmiştir. Yazılımlar geliştirilirken dikkat edilmesi gereken en önemli konuların başında otomasyondan yararlanacak kullanıcıların belirlenmesi ve yönetilmesi gelmektedir. Özellikle üniversite ve kamu kuruluşları gibi kendi yazılımlarını geliştiren bilgi işlem merkezlerinde yazılımların kullanıcı yönetimlerine olan önem giderek artmaktadır. Aynı kullanıcılar, geliştirilen otomasyonları farklı yetkilerde kullanmaktadır. Fakat her otomasyon için belirlenen kullanıcı adı ve şifre, kullanıcılar üzerinde gereksiz bir yük ve şifre karmaşasına yol açmaktadır. Kullanıcı yönetimi karmaşası aynı zamanda yazılımı geliştiren uzmanlar için de büyük bir zaman kaybına neden olmaktadır. Bu çalışmada Muğla Sıtkı Koçman Üniversitesi bünyesinde geliştirilen yazılımlara tek bir kullanıcı adı ve şifre ile girilebilmesi amacıyla SSL (Secure Socket Layer) güvenlik protokolü destekli bir web servis mimarisi geliştirilmiştir. Geliştirilen web servisi Ldap protokolüne çeşitli sorgulamalar yaparak kullanıcıya ait giriş bilgilerini iletmektedir. Web servis sayesinde giriş işlemleri için kullanıcılar farklı uygulamalara ait veri tabanlarında sadece yetkileriyle tutulmaktadır. Çalışma kapsamında Muğla Sıtkı Koçman Üniversitesi bünyesinde geliştirilen yazılımlar bu projeye entegre edilmekte ve tek bir sistem üzerinden kullanıcı yönetimleri gerçekleştirilmektedir. Web servis mimarisi geniş bir yapıda geliştirilerek Ldap protokolünü kullanan diğer üniversite ve kurumlar için de bir model oluşturmaktadır. Bu çalışmanın amacı bütünleşik bir kullanıcı yönetim modelinin Ldap protokolü ile kurulabileceğini bu sayede hem kullanıcılara hem de yazılım geliştiricilerine büyük rahatlık sağlayacağını göstermektir.

Anahtar Sözcükler: Web Servis, Ldap, Kullanıcı Yönetimi.

Integrated account management with web services for software

Abstract: Integrated account management with web services for software: The increased use of software in daily life have made it necessary development of faster and more usable software. Management and identification of users who will benefit from automation,the most important issues to be considered when developing software. Especially in public institutions such as universities and computing centers that develop their own software,management of software users are increasingly important. Same users use developed automations with different authority. But, the specified user name and password for every automation,can lead to an unnecessary burden password complexity on users. User management complexity also has led to a huge waste of time for software developers. In order to login with single user name and pasword to the developed software within the University of Muğla Sıtkı Koçman, in this study SSL (Secure Socket Layer) security protocol supported web service architecture has been developed. The developed web service transmits the user's login information by various inquiries to ldap protocol. Through the Web service, users only kept with just authority in different application's databases for login operations. Study of work,developed software within the University Muğla Sıtkı Koçman, integrated to this project and user management are carried out in a single system. Web Service architecture by developing a broad structure,a model for

other universities and institutions which are using the LDAP protocol. The purpose of this study, an integrated user management model can be established with the LDAP protocol in this way, both users and software developers is to show how to provide great comfort.

Keywords: Web Service, Ldap, User Management.

1. Giriş

Teknolojik gelişmeler son zamanlarda mobil cihazlar başta olmak üzere birçok elektronik cihazda yeni uygulamalarla karşımıza çıkmaktadır. Yenilikler genel olarak yazılım tabanlı olmaktadır. Özellikle bankacılık işlemleri başta olmak üzere birçok alışveriş sitesinin kullanımı mobil cihazlarla yapılıyor olması günlük hayatta çok büyük bir kolaylık sağlasa da uygulamaları kullanmak için oluşturulan kullanıcı bilgileri gün geçtikçe artmaktadır. Tüm bu uygulamalar ise kullanıcılar için büyük bir şifre karmaşası oluşturmaktadır. Özellikle üniversite ve kamu kuruluşları gibi kendi yazılımlarını geliştiren bilgi işlem merkezlerinde yazılımların kullanıcı yönetimlerine olan önem giderek artmaktadır. Kullanıcı adı ve şifre karmaşasının giderek arttığı günümüzde üniversite öğrencilerinin ve personelinin kurumlarında kullanmış oldukları yazılımların sayısı da gün geçtikçe artmaktadır. Her otomasyon için belirlenen kullanıcı adı ve şifre, kullanıcılar üzerinde gereksiz bir yük ve şifre karmaşasına yol açmaktadır. Üniversite bünyesinde çalışan akademik ve idari personel yanında ön lisans, lisans ve lisansüstü öğrencileri de bu tür uygulamalardan zarar görmektedir. Kullanıcı yönetimi karmaşası aynı zamanda yazılımı geliştiren uzmanlar için de büyük bir zaman kaybına neden olmaktadır. Her uygulamada ayrı bir kullanıcı tanımlama ve şifre hatırlatma sistemi geliştirilmesi gerekmektedir. Bu çalışmada Muğla Sıtkı Koçman Üniversitesi bünyesinde geliştirilen yazılımlara tek bir kullanıcı adı ve şifre ile girilebilmesi amacıyla SSL destekli bir web servis mimarisi geliştirilmiştir. Çalışma kapsamında kullanıcılara ait şifre bilgilerinin ele geçirilmemesi amacıyla geliştirilen web servisi, SSL (Secure Socket Layer) güvenlik protokolü ile korunmuştur. Web servisi kullanılarak farklı yazılım dillerinde geliştirilen uygulamalar için programlama dili bağımsız bağlantı sağlanmıştır. Web servisleri xml mesajlaşma apilerdir. Farklı sistemleri birbirleriyle haberleştirebilmektedir [8]. Web servis mimarisi asp.net ile 3 katmanlı mimari yapısında geliştirilmiştir. Geliştirilen proje kapsamında üniversite otomasyonlarında kullanılan web servisleri aynı çatı altına toplanmıştır. Personel otomasyonu, öğrenci işleri otomasyonu, geçiş kontrol sistemi, santral veri tabanlarına ait web servisleri tek bir domain altına toplanarak bütünleşik bir yapı oluşturulmuştur. Ayrıca Merkezi Nüfus İdaresi Sistemi (Mernis) kullanılarak ldap tan gelen tc numarasına göre kişinin kimlik bilgileri de ayrı bir entity yapısında verilmektedir.

Dulay vd. yapmış oldukları çalışmada politikaların belirlenmesi, yönetimi ve uygulanması için ponder dilinde tümleşik bir araç seti uygulamasını sunmuşlardır. Esnek bir yaşam döngüsü ve dağıtım modeli sunan Ponder politikaları dağıtık sistemleri yönetmek adına güçlü bir framework sunar. Geliştirilen araç, güvenlik platformları için eklenebilecek bir kod üretir [1]. Wang vd. yapmış oldukları çalışmada ise ldap dizinlerinin çeşitli erişim desenlerindeki performanslarını ölçen bir araç geliştirmişlerdir [2]. Bugüne kadar yapılan çalışmalarda ise ldap protokolünün yazılım uygulamalarında kullanıcı yönetimi olarak kullanıldığına rastlanmamıştır. Çalışma kapsamında Muğla Sıtkı Koçman Üniversitesi bünyesinde geliştirilen yazılımlar bu projeye dâhil edilmekte ve tek bir sistem üzerinden kullanıcı yönetimleri gerçekleştirilmektedir. Böylece kurumsal yapıdaki merkezlerin farklı

platformlarda geliştirmiş oldukları birçok yazılımın kullanıcı yönetiminde ldap protokolünü kullanarak daha etkin ve hatası eksik bir model kurulması amaçlanmıştır. Böylece uygulamalardaki şifre karmaşasının önüne geçilerek tekil kullanıcı adı ve şifre kullanılmış olunacaktır. Çalışmanın ikinci bölümünde kurulacak web servis model tasarımı, güvenlik sertifikası, web servis mimarisi, üçüncü bölümde ise geliştirilen web servis mimarisi ile ilgili bilgiler verilmiştir. Son bölümde ise çalışmayla ilgili sonuç ve öneriler aktarılmıştır.

2. Bütünleşik Hesap Yönetim Modeli

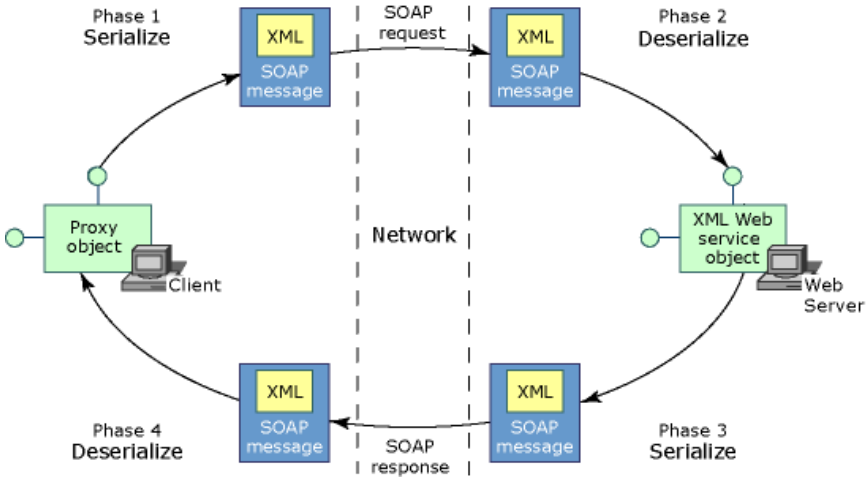
Bütünleşik hesap yönetim modeli uygulama kullanıcılarının tek bir sistem üzerinden yönetimini sağlamaktadır. Kullanıcılar Ldap protokolü üzerinde tutularak hesap bilgileri web servisleri aracılığı ile çağrılmaktadır.Güvenli bağlantıyı sağlamak için SSL güvenlik protokolü uygulama sunucusuna kurulmuştur.

2.1 Web Servis Mimarisi

Servis yönelimli programlama tanımlanan, keşfedilen ve kullanılan standart protokollerin yeniden bloklar halinde kullanılmasını sağlamaktadır. Servis yönelimli programlamayı anlamak için ortak teknolojik seçim web servisleridir [4]. Ağ üzerindeki makineler arası haberleşmenin çalışabilmesi amacıyla tasarlanan web servisleri aynı zamanda yazılım bileşenleridir. Web servislerinin yaygınlaşması ve benimsenmesi dinamik iş süreçlerinin kurulmasında tekil uygulamaların dinamik bir yapıya dönüşmesi sürecinde yeni bir paradigma olarak benimsenmiştir. Son yıllarda web hizmetleri sanayi ve akademinin geniş ilgisini çekmekte ve kamusal web hizmetlerinin sayısı giderek artmaktadır [5]. Web servisler modern internet döneminin XML mesajlaşma tabanlı entegrasyon yöntemi veya api'leridir. Web servisler çok amaçlı kullanılabilirler. Öncelikli amaçlar arasında, farklı sistemlerin birbirine entegrasyonu – mesajlaşması bulunmaktadır. Veri alışveriş yöntemine ait standartlar olduğundan dolayı web servisleri platform bağımsızdır [6]. Servis için SOAP (Simple Object Access Protocol) UDDI (Universal Description, Discovery and Integration) WSDL (Web Services Description Language) elementleri kullanılmaktadır.

Web Servisinin Çalışma Prensibi

İstemci uygulama XML ile biçimlendirilen bir SOAP (Simple Obect Access Protocol – Basit Nesne Erişim Protokolü) mesajı hazırlar. SOAP sayesinde Web servislere her platformdan erişilip, her türlü kodlama diline de hizmet edebilmektedir. İstemci SOAP mesajını web uygulama sunucusuna yollar. Web uygulama sunucusu, gelen SOAP mesajını parse eder ve gerekli parametreleri ayıklayarak, istenen nesnenin istenen yöntemine yönlendirir. Çalışan yöntem, sonuç mesajını web uygulama sunucusuna döner. Web uygulama sunucusu, sonuç mesajını XML ile biçimlendirerek istemci uygulamasına cevap döner. Şekil-1 de web servislerinin genel çalışma mantığı anlatılmıştır.



Şekil-1 Web Servis Mimarisi [9]

2.2. Güvenlik Sertifikası

1994 yılında Netscape tarafından geliştirilen, şifreleme esası açık anahtarlı şifrelemeye dayanan, web tarayıcısı ile web sunucusu arasındaki güvenliği HTTP üzerinden sağlamayı amaçlayan SSL (Secure Socket Layer-Güvenli Yuva Katmanı) protokolü şifrelenmiş güvenli veri iletişimini sağlar [7]. SSL, İnternet üzerinden yapılan bilgi alışverişi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir protokoldür. Bu protokol ile, İnternet gibi güvensiz ve saldırılara açık bir ortam üzerinde güvenli bir şekilde iletişim sağlanır. SSL protokolü ile veri karşı tarafa gönderilmeden önce belirli bir şifreleme algoritması ile şifrelenir ve sadece doğru alıcı tarafından bu şifre çözülerek asıl veri elde edilir [10]. SSL sistem güvenliğini korur böylece kayıtlı kullanıcının şifresi bir başkası tarafından çalınamaz ve kullanıcının hakları korunmuş olur. Hackerlar internet bankacılığı kullanıcılarının şifre bilgilerini çerezleri, tabloları veya url gibi bilgileri yakalayarak çalmaktadırlar. Bu tür problemler çerezlerde kısa oturum süreleri ile çözülmektedir fakat yeterli olamamaktadır. Bu tür problemler için en güvenilir yol ise SSL'dir [3]. SSL, istemci ile bilgilerin girildiği web sitesi arasındaki iletişimin bir takım şifreleme yöntemleriyle güvenli bir şekilde yaparak gönderilen bilginin kesinlikle doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce şifrelenir ve doğru alıcı tarafından deşifre edilir. Her iki tarafta da doğrulama yapılarak bilginin gizliliği, güvenliği ve bütünlüğü sağlanır. Veri/bilgi akışında kullanılan şifrelemenin gücü kullanılan anahtar uzunluğuna bağlıdır. SSL in çalışma mantığında ise 8 bitlik bir veri sadece 256 olası farklı anahtar içerirken bilgisayar 256 farklı olasılığı sıra ile inceleyerek bir sonuca ulaşabilir. Fakat SSL protokolünde ise 40 bit ve 128 bit şifreleme kullanılarak anahtar sayısı arttırılmaktadır ve üretilen şifrenin çözülebilmesi çok büyük bir maliyet ve zaman gerektirmektedir. Oturum tabanlı yönetim web sistemlerinde sunucu ve tarayıcı arasındaki transferi sağlaması amacıyla kullanılmaktadır.

2.2. Ldap Protokolü

LDAP (Lightweight Directory Access Protocol), bir nevi dizin servisi standardıdır. Dizin servisleri dizin yapısında, veriye merkezi olarak ulaşılması için düşünülmüş bir nevi veritabanı hizmeti veren sistemlerdir. Özellikle kurum içi organizasyon ve personelin kayıtlarının tutulabileceği elverişli bir ortam sunar. Örneğin herhangi kurumda çalışan veya bir üniversitede okuyan

öğrencilere çeşitli servisler sunulması gerekebilir. Bunun için her servisin üzerinde çalıştığı makinada ayrı ayrı kullanıcı hesapları açılması gerekebilir. LDAP sistemiyle karmaşık süreç düzeltilebilmektedir. LDAP dizinleme sisteminde her kayda ait özellikler ve bu özelliklerin değerleri vardır. Her kaydın ait olduğu bir nesne sınıfı oluşarak sınıflardam isimlendirme kullanılmıştır[11]. LDAP ile kullanılan yaygın özellikler aşağıdaki gibidir;

uid (User ID), sistemdeki kullanıcı adı,

cn (Common Name), kullanıcının adı soyadı,

sn, kullanıcının soyadı,

mail, kullanıcının e-mail adresi,

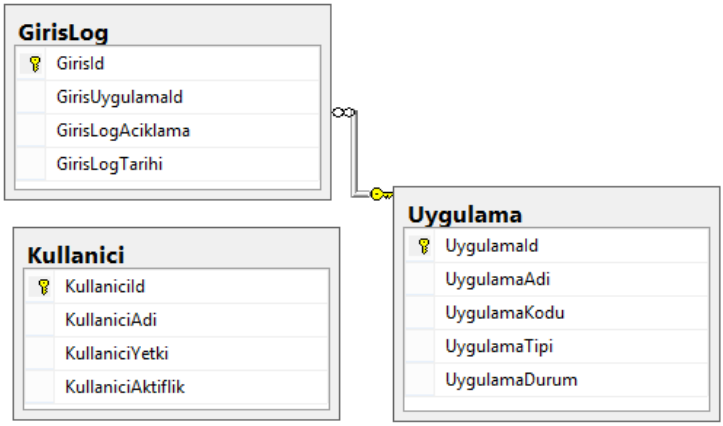
telephonenumber, kullanıcının telefonu

3. Uygulama

Bu çalışmada üniversite bünyesinde geliştirilen yazılımların kullanıcı yönetimlerine yönelik bir uygulama geliştirilmiştir. Uygulama kapsamında giriş servisi , veritabanı yapısı ve güvenlik sertifikasının sunucuya eklenmesi anlatılmıştır.

3.1. Veritabanı Yapısı

Geliştirilen yazılımlara ortak bir sistemden girilebilmesi amacıyla geliştirilen web servisi uygulamaya göre yetkilendirme yapılarak kullanılmaktadır. Bu şekilde yetkisiz kullanıcılar servisi kullanamamaktadır. Geliştirilen veritabanı yapısında uygulamaların tutulduğu uygulama tablosu ve hangi uygulamaya giriş yapıldığına dair bir log tablosu bulunmaktadır. Şekil-2 de geliştirilen veritabanı diyagramı verilmiştir. Uygulama tablosunda uygulama tipi ile geliştirilen sisteme personel veya öğrencinin erişim yetkisi belirlenmektedir. Uygulama kodu alanında ise hangi uygulamaya yetki verildiğine ait bilgiler verilmektedir. GirisLog tablosunda ise sisteme giriş yapan uygulama ve ona ait kullanıcı bilgilerinin yer almaktadır.



Şekil-2 Kimlik Yönetim Veritabanı

3.2. Giriş Servisi

Geliştirilen yazılımlara ortak bir sistemden girilebilmesi amacıyla veritabanı ile bağlantılı bir web servisi geliştirilmiştir. Web servisi ldap protokolüne bağlanarak kullanıcı doğrulamasını yapmaktadır. Ldap protokolünde kullanıcı şifreleri md5 algoritmasına göre şifrelendiği için parametre olarak girilen şifre md5 olarak ldapta sorgulanmaktadır. Sistemde tutulan veriler sınıf yapısında gönderilmektedir. Servisi kullanacak geliştiriciler de aynı şekilde bu sınıfı kullanarak kendi projelerinde kullanıcı kişisel bilgilerini kullanabilmektedirler. Ayrıca ikinci bir servis kullanılarak da giriş işleminin durumu tarih ve saat olarak Kimlik Yönetim veritabanına geri gönderilmektedir. Servis mimarisi kapsamında personel girişi, öğrenci girişi ve merkez veritabanına geri dönüş bilgisi veren fonksiyonlar geliştirilmiştir.

Personel ve Öğrenci giriş servislerine ait nesne tanımları

mail=Mail Kulanıcı Adı,
tckimlik=T.C. Numarası
bölüm=Çalıştığı Bölüm/okuduğu fakülte
cn=Ad,Soyad
description=Akademik veya İdari personel tipi
givenname=Ad
hesapAktif=ldap hesabının aktiflik durumu
sn=soyad,
unvan=Kadro Ünvanı
proxy=ldap durumu
Şekil-3 de servisin döndürdüğü sınıf yapısı verilmiştir.

```
public class LdapBilgi
   {
      public bool Durum { get; set; }
      public string mail { get; set; }
      public string tckimlik { get; set; }
      public string bolum { get; set; }
      public string cn { get; set; }
      public string description { get; set; }
      public string displayname { get; set; }
      public string givenname { get; set; }
      public string hesapaktifligi { get; set; }
      public string sn { get; set; }
      public string mesaj { get; set; }
      public string unvan { get; set; }
   }
```

Şekil-3 LdapBilgi Sınıfı

Geliştirilen servisin genel güvenliğini sağlamak adına parametre olarak kullanıcı adı ve şifre gönderilerek güvenlik doğrulaması yapılmaktadır. Parametre olarak gönderilen şifre eğer md5e çevrilerek gönderilirse sistem bu şekilde işlem yapmaktadır. Şifrelenmemişse servis içerisinde dönüştürme işlemi yapılmaktadır. Şifreleme işlemi için System.Security.Cryptography isim uzayı kullanılmaktadır. Servis kullanılarak gönderilen kullanıcı adı ve şifre için Ldap bilgileri kullanıldığı için hem öğrenci hem de personel @mu.edu.tr uzantılı e-posta hesap bilgilerini kullanmaktadırlar.

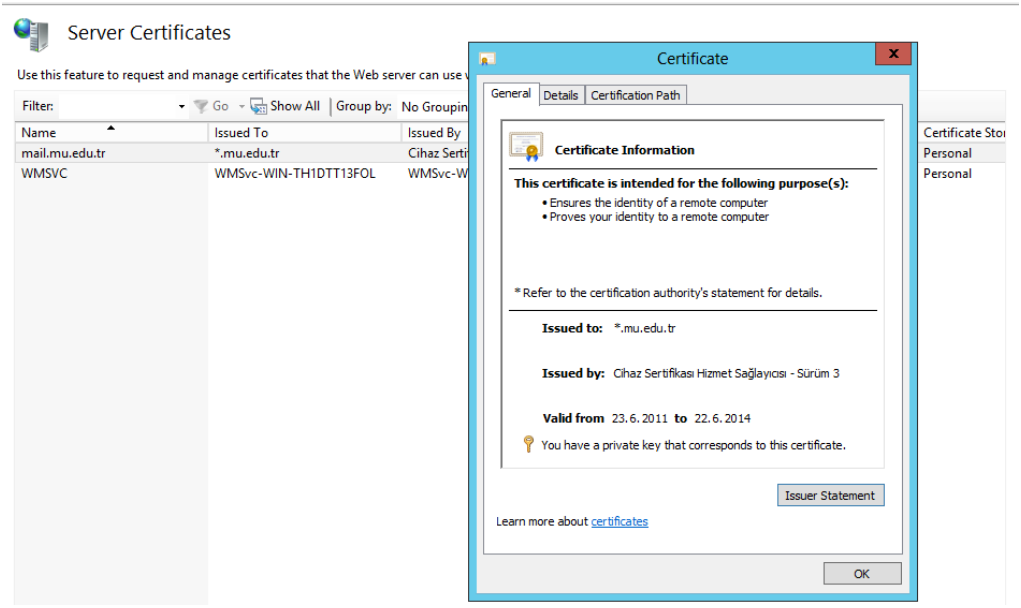
```
[WebMethod]
      public LdapBilgi GetByLdapLoginPersonel(string KullaniciAdi,string
Sifre,string ServisKullaniciAdi,string ServisSifre){
          if (Ortak.ServisKullanici.KullaniciAdiServis == ServisKullaniciAdi
&& Ortak.ServisKullanici. SifreServis == ServisSifre){string k_ad = "";
if (!KullaniciAdi.Contains("@mu.edu.tr") && !KullaniciAdi.Contains("@"))
k_ad = KullaniciAdi + "@mu.edu.tr";
              else k_ad = KullaniciAdi;
              var eskisifredogrumu = Ortak.LdapKullaniciGirisiPersonel(k_ad,
Sifre);
              if (eskisifredogrumu.Durum == true){return eskisifredogrumu;  }
              else  {LdapBilgi entity = new LdapBilgi(); entity.Durum = false;
entity.mesaj = "Kullanıcı Adı veya Şifre Yanlış Girilmiştir..."; return
entity;}}
          else  {  LdapBilgi entity = new LdapBilgi();entity.Durum =
false;entity.mesaj = "Servis Bilgileri Yanlış Girilmiştir...";return entity;} }
```

Şekil-4 Personel Login İşlemi Servis Fonksiyonu

Bütünleşik hesap yönetimi için geliştirilen web servisi asp.net platformunda üç katmanlı mimaridedir. Proje kapsamında. Net Framework teknolojisi kullanılmıştır.

3.3. Güvenlik Sertifikası

Uygulama kapsamında geliştirilen servis üzerinden kullanıcı doğrulaması yapılacağından dolayı parametre olarak gönderilen şifre ve kullanıcı adları güvenli bir ortamda gönderilmelidir. Bunun için web servislerinde ayrıca bir kullanıcı adı ve şifre istense dahi hackerler ve robot yazılımlar web servisinin parametrelerini url içerisinde dinleyebilmektedir. Bunu önlemek amacıyla son yıllarda giderek yaygınlaşan güvenlik sertifikası kullanılmakta ve önemli bir güvenlik aracı olarak projelerde yer almaktadır. Bu çalışmada web servisi asp.net platformunda geliştirildiği için iis platformuna ilk olarak kurumun satın aldığı sertifika kurulmuştur. Pfx uzantılı dosya import özelliği kullanılarak ilgili iis sunucusuna yüklenmiştir. Şekil-5 de sunucuya eklenen sertifika bilgileri verilmiştir.



Şekil-5 Sunucuya Yüklenen Sertifika Bilgileri

Eğer aynı iis içerisinde aynı ip üzerindeki farklı siteler https özelliği kullanacaksa herhangi bir site üzerinde bindings özelliği kullanılarak sertifika eklenir.
Kod satırı kullanılarak servise komut satırından https sertifikasyon özelliği kazandırılır.

Cd C:\Windows\System32\inetsrv\appcmd set site /site.name: login /+bindings.[protocol ='https',bindingInformation='*:443:servis adresi']

4. Sonuç ve Öneriler

Bütünleşik hesap yönetiminin kurumların bilgi işlem merkezleri tarafından geliştirilen uygulamalarda uygulanması zaman, kullanılabilirlik ve maliyet açısından önemli bir tasarruf sağlamaktadır. Teknolojinin güncel hayatımızda yaygınlaşması beraberinde kullanılan uygulamaları da arttıştır. Her uygulamaya girişte sorulan kullanıcı adı ve şifre büyük bir karmaşaya neden olmaktadır. Birçok kez şifreler birbirine karıştırılmaktadır. Yaşanan sıkıntılar kaşısında bilgi işlem merkezlerinde kurum için geliştirilen yazılımları tek bir kullanıcı adı ve şifre ile yönetmek kullanıcıların kurum için tek bir şifre bilmelerini sağlayacaktır. Bu çalışmada Muğla Sıtkı Koçman Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından geliştirilen bütünleşik hesap yönetimi anlatılmıştır. Sistem ile kullanıcılar üniversite bünyesinde geliştirilen farklı yazılımlara aynı hesap bilgileriyle girebilmektedir. Şifreler ise sms ve e-posta desteği ile değiştirilebilmektedir [12]. Geliştirilen sistem ile web servisinin adresine dışardan erişilse dahi hangi uygulama tarafından kullanılacağı veritabanına belirtilmediği sürece kullanıcı doğrulaması çalışmayacaktır. Servisin güvenliğini sağlamak amacıyla fonksiyonların aldığı kullanıcı parametrelerinin yanında servis kullanıcı adı ve şifresi de güvenliği önemli ölçüde sağlamaktadır. Kullanıcı doğrulama için Ldap protokolü kullanılmıştır. Üniversiteye hem personel hem de öğrenci

olarak başlayan kullanıcılara ilk olarak kişiye özel tanımlanan kullanıcı adı ve şifresi verilir. Bu sayede üniversite bünyesinde kullanılacak eduroam, öğrenci not sistemi, evrak otomasonu gibi uygulamalara tek bir kullanıcı bilgisiyle girilebilmektedir. Ldap protokolüne girilen bilgiler doğrulama sonucunda otomasyonlarda kullanılabilmektedir.Çalışma kapsamında servisin yayınlandığı iis sunucusuna güvenlik sertifası kurulmuştur. Bu sayede robot yazılımlar aracılığı ile yapılan saldırılar karşısında kullanıcı adı ve şifresi okunamamaktadır. Bu çalışmada bütünleşik hesap yönetimi modellenmiştir. İleriki çalışmalarda ise bu modelin tek bir kurum için değilde tüm kurumlarda kullanılabileceği ve ayrıca özel geliştirilen yazılımlara da eklenebileceği gösterilmiştir.

5. Kaynaklar

[1] Dulay, N., Lupu, E., Sloman, M., Tonouchi, T.,"Tools for domain-based policy management of distributed systems", **Network Operations and Management Symposium,** 203 - 217, (2002).

[2] Wang, X., Schulzrine, H., Dilip, K., Verma. D., "Measurement and analysis of LDAP performance", **International Conference on Measurement and Modeling of Computer Systems,** 232 - 243, (2008).

[3] Yun, Z., Kuihe, Y., Yanhua, W., Zhifeng, Z., "Research on Protecting the Safety in Web System With SSL", **The Eighth International Conference on Electronic Measurement and Instruments**, Xi'an, 340-343 (2007).

[4] Mateos, C., Crasso, M., Zunino, A., Coscia, J.L.O.,"Revising WSDL Documents: Why and How, Part 2", **Internet Computing, IEEE**, 46-53, (2013).

[5] Chen, X., Zheng, Z., Liu, Xudong., Huang, Z., Sun, H., " Personalized QoS-Aware Web Service Recommendation and Visualization", **IEEE Transactions on Services Computing**, 35-47, (2013).

[6] http://www.omerfarukozdemir.com/2012/05/25/web-servis-nedir-web-services/, Ömer Faruk Özdemir (Erişim Tarihi: Eylül. 2013).

[7] http://www.e-siber.com/guvenlik/ssl-secure-socket-layer-protokolu-nedir, M.Mekin Kesen (Erişim Tarihi: Kasım. 2013).

[8] http://adil.gen.tr/asp-net-web-servis-nedir-nasil-kullanilir-1/, Adil Öztaşer (Erişim Tarihi: Kasım 2013).

[9] http://muratimre.blogspot.com/2012/06/web-servis-nedir-nerelerde-kullanlr.html, Murat İmre (Erişim Tarihi: Aralık 2013)

[10]http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/sertifika-sertifika-olusturma-sertifika-turleri.html, Esma Güneyyeri (Erişim Tarihi: Aralık 2013)

[11] http://www.ulakbim.gov.tr/dokumanlar/programlama/2000php/ldap/index.html, Ulakbim (Erişim Tarihi: Kasım 2013)

[12] https://sifre.mu.edu.tr/, Muğla Sıtkı Koçman Üniversitesi Bilgi İşlem Daire Başkanlığı