Kurumsal Kimlik Yönetiminde Güncel Sorunlar

Ayhan Alkan[1], Melih Kırlıdoğ[2]

[1] Sun Microsystems, İstanbul

[2] Marmara Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul

ayhan.alkan@sun.com, melihk@marmara.edu.tr

Özet: Kurumsal bilişim altyapılarının gittikçe karmaşıklaşması ve kurumların iş ortaklarına, müşterilerine sundukları çevrim-içi (on-line) servislerin gitttikçe çeşitlenmesi, sayısal ortamda oluşan sanal kimliklerin hızla birikmesi, değişik sistemlere dağılan bu kimliklerin tutarlılığının korunması ve güvenlik açıkları yaratma riski doğurması sorunlarını da beraberinde getirmiştir. Kurumlar, sistem/uygulama yöneticilerinin yükünü hafifletmek, kimlik yönetim maliyetlerini düşürmek, güvenlik risklerini azaltmak, hizmet kalitesini ve kullanıcı memnuniyetini artırmak, kimlik yönetim süreçlerini iş süreçlerine entegre etmek için son on yılda hızla kimlik yönetim sistemleri kurmaya yöneldiler. Bu makalede, alan deneyimlerimizden de yararlanarak, kurumsal kimlik yönetimine geçişte yaşanan sorunlar, izlenen stratejiler ve elde edilen kazanımlar üzerinde durulacak ve Türkiye'deki bir uygulama anlatılacaktır.

Anahtar Sözcükler: Kimlik Yönetimi, İş Akışı, Erişim Denetimi, Rol-Temelli Erişim Denetimi, Tanıma, Yetkilendirme, Proje Yönetimi

Contemporary Problems in Enterprise Identity Management

Abstract: The last few decades witnessed ever-increasing complexity of information infrastructures and escalating variety of on-line services offered to customers and business partners. These developments resulted in high number of virtual identities for individuals. As a result, it became a major problem to maintain the integrity and security of virtual identities in various platforms. Organizations developed identity management systems with the aim of easing the burden of the system managers, reducing identity management costs, increasing service quality and user satisfaction, and aligning identity management processes with other business processes. This article will focus on the strategies and problems in development and implementation of identity management systems. An identity management application in Turkey will also be explained.

Keywords: Identity Management, Workflow, Access Control, Role-based Access Control, Authorization, Authentication, Project Management

1. Giriş

Bireylerin resmi kimlikleri ile sanal kimlikleri arasında ilk önemli fark, bir resmi kimliğe karşılık çok sayıda, hatta baş etmekte güçlük çekmemize neden olacak kadar çok sayıda, sayısal kimliğe sahip olunmasıdır. Daha tuhafı, aynı kurum içinde bile bir kişi, eriştiği sistem ve uygulamalarda birbirinden farklı kimliklere sahip olmakta, pek çok kullanıcı adı ve şifreyi ezberlemek zorunda kalmaktadır. Bu durum, kişiler için can sıkıcı olduğu gibi, kurumlar açısından baktığımızda da ciddi sorunlar yaratır. Örneğin, insan kaynaklarında E1 koduyla kayıtlı bir çalışanın ERP, CRM, Muhasebe uygulamaları, Windows alanı, Unix sistemleri, e-posta sunucusu ve bina güvenlik sistemindeki kullanıcı karşılıkları nedir, bölüm değişikliği ya da terfi durumunda yetkileri yeni pozisyonuna uygun olarak ne sürede güncellenebilecektir, kişi işten ayrılırsa bir güvenlik açığı oluşmaksızın sahip olduğu bütün erişim hakları iptal edilebilecek midir? Orta ve büyük olçekli kurumların kaçı bu soruları rahatlıkla yanıtlayabilir? Kimlik yönetimi ve erişim denetimi uygulamaları bu sorunları çözmeyi amaçlarlar.

Kimlik yönetimi ve bilişim güvenliği ile ilgili sorunları iki alanda inceleyeceğiz:

- **Kimlik Yönetim Sistemleri** (KYS) [Identity Management – IdM]
- **Erişim Denetimi** (ED) [Access Control - AC] : Bu konu da iki alanda incelenecektir:
  - **Tanıma** [Authentication]
  - **Yetkilendirme** [Authorization]

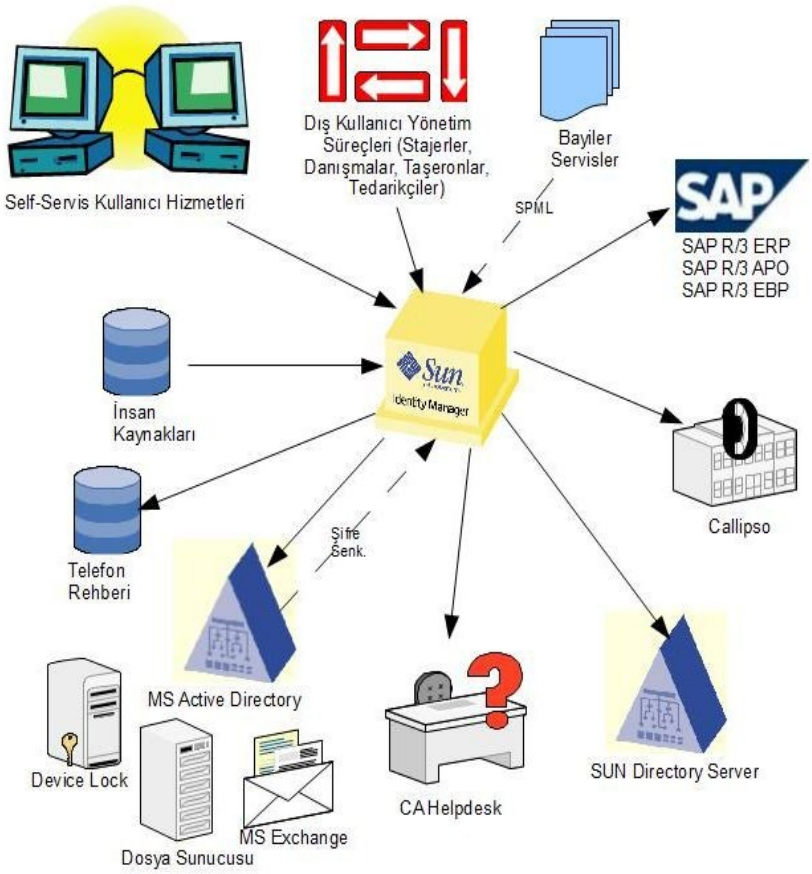
Bu makalede hem kurumsal kimlik yönetimi kavramlarını olası kimlik yönetimi projeleri bağlamında tanıtmayı, hem de karşılaşıkabilecek sorunlara karşı alınması gereken önlemleri aktarmayı hedefliyoruz.

2. Kimlik Yönetim Sistemleri (KYS)

KYS kişinin kurama girişinden (işe giriş, öğrenci kaydı, geçici danışmanlık, vb.) kurumdan çıkışına (işten ayrılma, mezuniyet, emeklilik, vb.) kadar geçen süre boyunca kurum içindeki sanal kimliği ile onlarca sisteme dağılmış kullanıcı hesaplarını iş süreçleriyle eşgüdümlü yönetmeyi

amaçlayan yazılım sistemleridir. Bazı kaynaklarda bu alan yalnızca kullanıcı yönetimi [user management] diye anılsa da [8] bizce çok daha zengin bir işlevselliği barındırır.

Çizim-1'de gerçek bir KYS uygulamasının ana bileşenleri görülmektedir. İlerleyen bölümlerde KYS bileşenleri tanıtıldıkça bu kuşbakışı görüntü daha da anlam kazanacaktır.



Çizim 1: Ana bileşenleriyle bir KYS uygulaması

2.1. Tek Sanal Kimlik

Bir KYS projesi ile öncelikle merkezi bir **kimlik veritabanı** [repository] kurulur. Burada her gerçek kimliğe karşılık yalnızca bir sanal kimlik tutulur. Bu veritabanındaki her bir sanal kimlik, temel olarak ait olduğu kişiye ait genel bilgileri (özlük bilgileri), hangi sistemlerde hesapları bulunduğu, bu hesaplara ait bilgileri taşır. Bazı KYS uygulamalarında kişinin organizasyon içindeki konumu, sahip olduğu idari ve teknik yetkiler (roller) gibi bilgileri de içerir.

Bu sanal kimlik veritabanlarının hangi teknolojiler üzerine kurulacağı kullanılan KYS ürününe ve bazen ürün içinde kurumsal tercihlere göre değişir. Çoğunlukla bir **ilişkisel veritabanı** [RDBMS] ya da bir **dizin sunucusu** [Directory Server] (yaygın olarak **LDAP** [Lightweight Directory Access Protocol] sunucuları diye anılır) tercih edilir. Eğer kullanılacak KYS uygulaması seçme olanağı sunuyorsa, genellikle dizin sunucuları kullanılması önerilir.

2.2. Kaynaklar ve Kullanıcı Hesapları

KYS'ler yönettikleri sistemlerin yalnızca kullanıcı kayıtlarıyla ilgilenirler, dolayısıyla onları kullanıcı kaynağı olarak görürler. Bu yüzden KYS uygulamalarında bu sistemler **kaynak** [resource] olarak adlandırılırlar. Bu kaynaklardaki her bir kullanıcı kaydı ise, KYS için ilişkili sanal kimliğe ait bir **kullanıcı hesabı**dır [user acount].

Yönetilen kaynaklardaki bütün kullanıcı işlemlerinin KYS sistemin devreye alınmasından sonra yalnızca KYS üzerinden güncellenmesi esastır. Eğer bu tür kaynaklarda başka bir kanaldan güncelleme yapılacaksa [native change] bu değişikliklerin KYS'ye hızla yansıtılması için gerekli önlemler alınmalıdır.

Kaynaklardan en az biri (ki bu çoğunlukla kurumun İnsan Kaynakları sistemi olur), yönetilen sanal kimliklerin içeriğini belirleyen **yetkili kaynak**tır [authoritative resource]. KYS bir **etkin senkronizasyon** [active sync] mekanizmasıyla bu kaynaktaki değişiklikleri (örneğin işe giriş, terfi, bölüm değişikliği) algılar ve KYS'deki kimlik süreçlerini tetikler.

2.3. Kimlik süreçleri

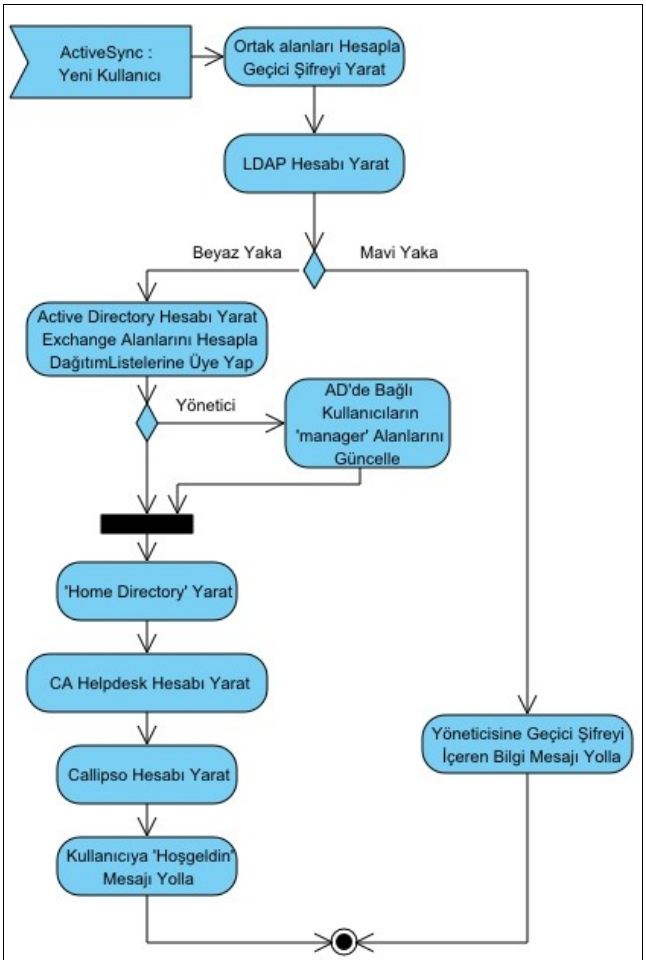
Sanal kimlikler ve ilgili kullanıcı hesaplarını etkileyecek değişiklikler genellikle karmaşık işlemleri gerektirirler. Bu değişiklikler aynı anda birden fazla kaynağı ilgilendirdiği gibi, gerekli kişilere uyarı mesajları yollama, bazı sistemlerde o kişi için düzenlemeler yapma, yetki atama/silme, yönetici onaylarını alma, eğer yönetici onayından geçmezse işlemi geri alma gibi pek çok kurumsal iş süreçlerini de içerir. Dolayısıyla her türlü **kimlik işlemleri** [provisioning] **iş akışları** [workflow] yapısında yürütülür. Bu iş akışları kurumsal iş süreçleri ve politikalarla uyumlu olmak zorundadır.

Çizim-2'de büyük bir sanayi şirketinde uygulanan bir KYS sisteminin işe giriş iş akışının UML diyagramı görülmektedir.

2.4. Self-servis hizmetler

KYS'de sanal kimlikleri tutulan kullanıcılara doğrudan sunulan hizmetler **self-servis hizmetler** terimiyle anılır. Bu hizmetler, kurumsal ihtiyaçlara göre büyük farklılıklar gösterir. En sık kıllanılan self-servis hizmetler şunlardır:

- Şifre değiştirme
- Unutulan şifrelerin güvenli bir yöntemle yenilenmesi
- Sistemlere / uygulamalara erişim talebi
- Yetki / rol talebi



Çizim 2: Örnek bir işe alma işleminin KYS iş akışı

- Geçici yetki devri talebi
- Gelen onay taleplerini değerlendirme
- Mevcut taleplerinin durumunu sorgulama
- Bazı kişisel bilgileri (telefon numarası, ev adresi gibi) güncelleme

2.5. Olay izleme

KYS'lerin sanal kimlikler ve ilgili süreçleri merkezileştirmesi, hem BT hem de idari yöneticilere önemli olanaklar sağlar. Öncelikle, tek bir noktadan bakarak kişilerin kurum sistemlerine dağılmış hesapları, bu hesapların durumları ve ayrıntıları görülebilir. Onay gerektiren talepte bulunanlar, taleplerinin ne aşamada olduğunu görebilirler. Bütün kimlik işlemleri tek kanaldan geçtiğinden olağan olayların olduğu gibi ihlal girişimlerinin de izini sürmek kolaylaşır. Kurumun kimlik yönetimiyle ilgili uyması gereken yasal ya da meslek organizasyonlarının koyduğu kurallar varsa KYS'nin raporlarıyla yapılan işlemlerin kurallara uyumluluğu denetlenebilir ve kanıtlanabilir.

3. Erişim Denetimi (ED)

ED bilişim kaynak ve servislerine kişi ve uygulamaların erişip erişemeyeceklerini, erişebileceklerin hangi yetkilerle çalışabileceğini belirleme işlemidir. İki aşamada ele alınabilir: 1) Öncelikle erişim talebinde bulunan kullanıcı ya da uygulamanın kimliğinin tanınması, erişim hakkına sahip geçerli bir kimlikle eşleştirilmesi, 2) Eriştiği sistem ya da serviste yapabileceği işlerin sınırlanması. Birbirini tamamlayan süreçler olmasına karşın bu iki alan farklı kavram ve standartlarla ele alınır. Bu makalede de öyle yapılacaktır.

3.1. Tanıma

Tanıma [authentication] işlemi, insanlar için biyolojik varlığımızın, resmi kimliğimizin kullanıcı veritabanındaki sanal kimliğimizle eşleştirilmesidir. Weitzner'e göre [1] bunun için üç yol vardır: Sisteme giriş şifresi gibi "**bilinen bir şey**", akıllı kart veya geçici şifre gönderilen cep telefonu gibi "**sahip olunan bir şey**" veya iris kontrolu, parmak izi gibi değiştirilemez biyometrik özelliklerle "**olunan bir şey**". Kimi daha fazla güvenlik riski olan durumlarda bu yöntemlerin ikisi ya da üçü bir arada da kullanılabilir.

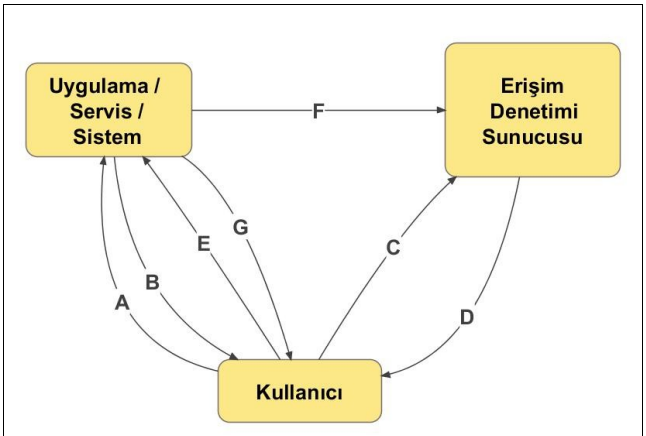
Günümüzde bilgisayarların birbirlerinin servislerinden yararlanmak üzere erişimleri de çok yaygındır ve hiç kuşkusuz zamanla daha da yaygınlaşacaktır. Sistemlerin/ uygulamaların birbirini tanımasında da insanlar için sayılan yöntemlerden ilk ikisi -biraz farklı protokol ve teknikler kullanılsa da- geçerlidir.

Tanıma konusunda günümüzün en popüler konusu, hiç kuşkusuz, kullanıcının ilk eriştiği sistemde kendini bir kez tanıttıktan sonra o kurum dahilindeki diğer uygulamalara erişirken yeniden kendini tanıtma ihtiyacı duymadan giriş yapabilmesini sağlayan **Tek Girişle Erişim** (TGE) yöntemidir.

3.1.1. Tek Girişle Erişim (TGE)

Tek Girişle Erişim [Single-Sign-On – SSO], kullanıcı deneyimleri açısından büyük önem taşır. Çünkü bu yöntemle kullanıcı bir uygulamadan diğerine geçerken yeniden kendini tanıtmak zorunda kalmaz, birden fazla kullanıcı adı/şifre bilmesi gerekmez, zaman kazanır, kullanıcı gözünde kurum servisleri bir bütünlük arz eder.

TGE yöntemi hem Web, hem de masaüstü uygulamalarda kullanılabilir. Ancak, Web uygulamalarının tersine, masaüstü TGE uygulamaları çok sorunlu ve masraflı (kurulum, bakım, destek masrafları) olduğundan kurumların masaüstü TGE'ye geçmeden önce sözkonusu uygulamaları Web ortamına taşımayı düşünmeleri önerilir.



Çizim 3: Web üzerinde TGE işlem adımları

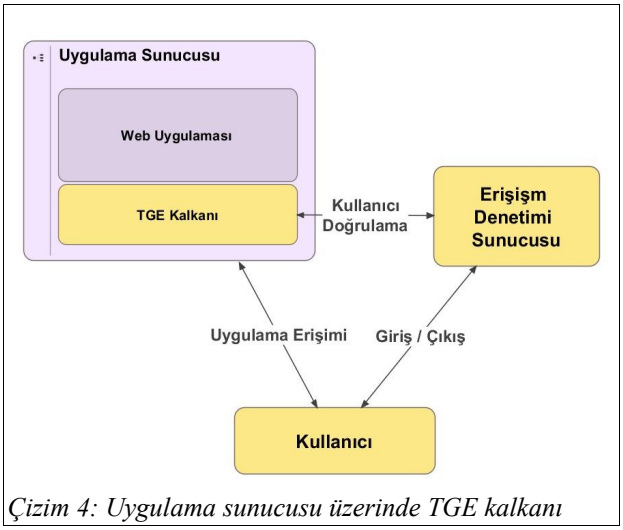
Çizim-3'te tipik bir Web TGE işleminin nasıl çalıştığı gösterilmektedir. İşlem adımları şunlardır:

A. Kullanıcı TGE ile korunan bir uygulamaya erişmeye çalışır.
B. TGE kalkanı kullanıcının giriş yapmadığını anlayınca HTTP 30x cevabı ile kullanıcıyı Erişim Denetimi Sunucusuna (EDS) yönlendirir.
C. Kullanıcı EDS üzerindeki giriş mekanizmalarından birini (kullanıcı adı/şifre, sertifika gibi) kullanarak giriş işlemini tamamlar.
D. EDS bir **geçiş bileti** [token] vererek kullanıcıyı yine HTTP 30x cevabı ile geldiği sunucuya geri gönderir.
E. Kullanıcının tarayıcısı uygulama sunucusundan A adımındaki talebini yineler.
F. TGE kalkanı kullanılan protokole göre gerek duyarsa kullanıcının giriş biletini doğrulamak üzere EDS'ye başvurur.
G. TGE kalkanı geçişe izin verir ve uygulama ile kullanıcı tarayıcısı arasında olağan trafik akışı başlar.

Web TGE uygulamalarında kullanıcıyı kabul edecek uygulama hiçbir zaman kullanıcı tanıma işine girişmez, bunu ED sunucusuna bırakır ve oradan gelen kullanıcı bilgisine güvenir. Uygulamayı korumak için bir **TGE kalkanı** [SSO-agent] kullanılır. Bu kalkanı oluşturmanın üç yöntemi aşağıda açıklanmaktadır.

3.1.1.1. Hazır TGE Kalkanı

Web uygulamaları bir taşıyıcı [container] ortam içinde çalışır. TGE yazılımı sağlayıcıları belli başlı Web uygulama sunucuları (taşıyıcıların bütünlüklü bir servis yazılımı hali) için hazır kalkan bileşenleri sunarlar. TGE işlevini bir Web uygulamasına kazandırmanın en kolay yolu, Çizim-4'te görüldüğü gibi, hazır bir TGE kalkanını uygulama sunucusuna yükleyip uygulama üzerindeki bütün giriş ve koruma önlemlerini kaldırmaktır.



Çizim 4: Uygulama sunucusu üzerinde TGE kalkanı

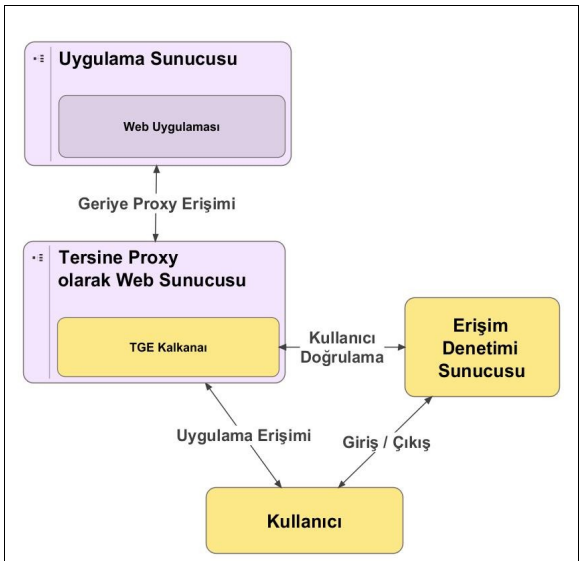
3.1.1.2. Geriye Proxy Kalkanı

Eğer kullanılan uygulama sunucusu için hazır bir TGE kalkanı yoksa ya da çok sayıda uygulama sunucusuna TGE kalkanı yüklemek, bunların ayrı ayrı bakımıyla uğraşmak istenmezse, TGE kalkanı '**geriye proxy**' [reverse proxy] modunda çalışan bir Web sunucusuna (örneğin, en yaygın kullanımı olan Apache Web Server) kurulur; uygulamalara erişim yalnızca bu geriye proxy üzerinden sağlanır.

Bu yöntemin en zayıf tarafı, geriye proxy ile uygulama sunucusu arasındaki güvenliğin sağlanmasıdır. Ancak güvenli ağ yönetimi ve uygun uygulama sunucusu konfigürasyonları ile bu güvenli ortamı oluşturmak mümkündür. Bu yöntemle çalışma örneği Çizim-5'te gösterilmmektedir.

3.1.1.3. Özel Geliştirilen Kalkan

Eğer sağlanan hazır kalkan seçenekleri beklediğimiz bazı karmaşık işlemleri karşılayamıyorsa bu kalkan bileşenini kendimiz yazıp uygulamaya entegre edebiliriz. Bu seçenek, yazılım hataları ve unutulan ayrıntılar gibi olası riskleri barındırır. Eğer bu yöntemi izlemek zorundaysak, kullandığımız TGE protokolünü baştan yazmak yerine ED sunucusunu sağlayan firmanın API'lerini kullanmak tercih edilmelidir.



Çizim 5: Geriye proxy üzerinde TGE kalkanı

3.1.2. Web Alanları Arası TGE

Kurumlar sağladıkları servislerde birden fazla Web Alanı [domain] kullanabilirler. Bu durum, bir çok katma değerli servisi üçüncü parti firmalarla birlikte sunan kurumlarda (özellikle telekom ve içerik sağşayıcı kurumlar) çok yaygındır. Bu durumlarda kullanılacak TGE ürün ve protokollerinin **alanlararası TGE** [cross-domain SSO] desteğinin olup olmadığı sorgulanmalıdır.

3.1.3. Kurumlararası TGE

Kurumlararası TGE [Federated SSO] ilk bakışta kurumsal TGE'nin genelleştirilmiş hali gibi görünse de kendine özgü karakteristikler ve sorunlar içerir.

Başlangıçta birbirini tamamlayan işler yapan kurumların (örneğin bir havayolu şirketi, bir oto kiralama şirketi, bir otel zinciri) bir **güven çemberi** [circle of trust] içinde müşterilerine ortak bir TGE ortamı sağlaması fikrinden yola çıkılmıştı. Ancak standartların karmaşıklığı ve uygulama güçlükleri nedeniyle fazla yaygınlaşamadı. Günümüzde ise, çok farklı bir alandan, sosyal ağlardan, gelen motivasyon ve büyük Internet şirketlerinin (Google, AOL, Yahoo) desteği ile OpenID gibi çok daha basit protokoller kullanılarak hızla yaygınlaşmaktadır.

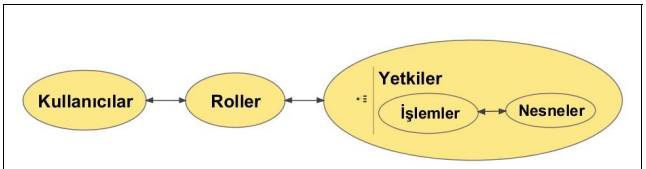
Bundan öte, bugün artık küçük ölçekli kurumların kendi TGE servislerini kurup yönetmek yerine, bu servisi dışarıdan almaları bile gündemdedir ve şimdiden pazarda bu servisleri ticari olarak sağlayan şirketler mevcuttur.

3.2. Yetkilendirme

Yetkilendirme [authorization], bir sisteme/servise giriş yapmış kişi ya da uygulamaların hangi nesmeler üzerinde neleri yapıp neleri yapamayacağını belirleme ve denetleme işidir. Yetkilendirme kimlik yönetimi işlemlerinin en güç alanıdır, çünkü:

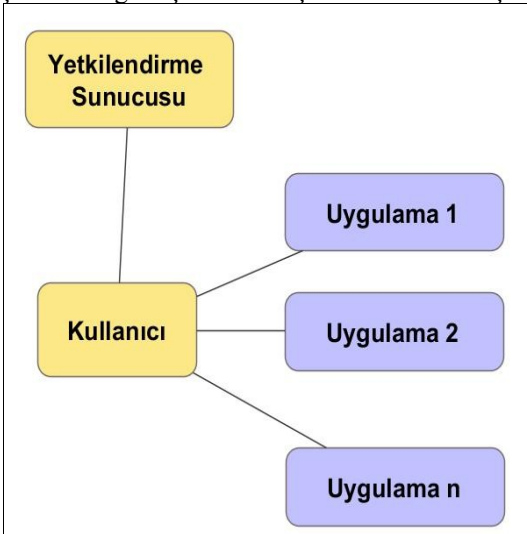
- Pratikte çok büyük çeşitlilik gösterir.
- Çoğunlukla işleyen yetki mekanizmaları dokümante edilmemişlerdir.
- Tanımlamaya çalışınca o zamana kadar farkında olunmayan pek çok muğlaklık ortaya çıkar.
- Aynı yetki farklı sistemlerde farklı adlarla geçtiği gibi, farklı sistemlerde aynı adla kullanılan yetkiler aslında çok farklı yetkileri ifade edebilir.
- Organizasyon şeması oturmuş ve pozisyona göre yetki dağılımları iyi tanımlanmış kurumlarda bile şaşırtıcı miktarda istisna bulunur.
- Geçici yetki atamaları çok yaygındır, bazen geçici yetkiler unutulup kalıcı görünümü kazanırlar.
- Çok sayıda standart tanımı içinde hangisinin kullanılacağına karar vermek oldukça güçtür.

En yaygın yetkilendirme yaklaşımı **Rol-Temelli Erişim Denetimi**'dir (RTED) [Role-Based Access Control – RBAC]. Çizim-6'da görülebileceği gibi, bu yaklaşımda kişilere doğrudan yetki verilmez. İş gören yetkiler rollerle ilişkilendirilir, kişiye bu roller atanır [10] [11]. Yetkiler ise, yetkinin geçerli olacağı nesne(ler) ile o nesne üzerinde yapılabilecek işlemlerin bileşimiyle oluşur.



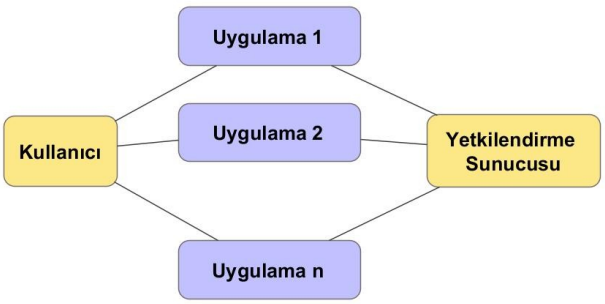
Çizim 6: Rol temelli erişim denetimi

Burada söz edilen nesneler, veri tabanındaki bir tablodan bir yönetici raporuna, kullanıcı ekranındaki bir düğmeden disk üzerindeki bir dosyaya kadar neredeyse sonsuz çeşitliliktedir. Yetkiler ise, bu nesnelere uygulanacak çalıştırabilme, onaylayabilme, görebilme, silebilme, değiştirebilme gibi işlemlerle ilişkilendirilecek oluşturulur.



Çizim 7: RTED - Kullanıcı kendi rollerini sunması

Tüm rol ve yetki tanımları ED sunucusu üzerinde tanımlanır ve yönetilir. Uygulamalar ise, yetkilendirme kararlarını verirken ya Çizim-7'de görüldüğü gibi kullanıcının getirdiği rollerini kullanırlar (örneğin, rol TGE bileti içinde gelebilir), ya da Çizim-8'de görüldüğü gibi kullanıcı adından ED üzerinde sorgulama yaparak tanımlanmış rol/yetki bilgilerine erişirler.



Çizim 8: RTED - Sunucunun sorguyla kullanıcı rollerine erişmesi

4. Kurumsal Kimlik Yönetimi Projeleri Özellikleri

4.1. Proje Yönetimi ve Liderlik

Kurumsal kimlik yönetimi projeleri her zaman kurumun bütün birimlerini -teknik açıdan bakarsak bütün sistemlerini- ilgilendiren/etkileyen projelerdir. Yürüten ekibin çok yönlü olması, diğer bir deyişle hem idari hem de teknik süreçlere ve sistemlere hakim olması gerekir. Projede yer alacak birim ve ekiplerin (bunlara kuruma servis ve yazılım sağlayan üçüncü parti ekipler de dahildir) etkili bir şekilde motive edilebilmesi, uygun ve yeterli katkılarının sağlanması için güçlü bir liderlik gerekir. Bunun anlamı projenin kurum içinde güçlü bir sahibinin

olması gerekir. Bu liderlik ve proje ekibi etkin bir proje planlaması ve yönetimi ile desteklenmelidir.

4.2. Kullanım Hedeflerinin Ayrıştırılması

Kimlik yönetim projeleri hem kurumun iç kullanımı (buna çoğunlukla iş ortakları da dahildir) hem de dış kullanıcıların (müşterilerin) kullanımı için uygulanabilir. Ancak bu iki alan kesinlikle ayrı projelerle ele alınmalıdır, çünkü:

- İç ve dış kullanıcı sayıları çok farklıdır. İç kullanıcı sayıları genellikle binler, on binlerle ifade edilirken dış kullanıcılarda bazen milyonlarca kullanıcıdan söz edilir. Bu ayrım sistemlerin ölçeklenmesini farklılaştırır.
- İş süreçleri çok farklıdır. Genellikle dış kullanıcılara yönelik iş süreçleri daha basit olur.
- İç ve dış kullanıcıların eriştikleri sistem ve servisler (KYS deyimiyle kaynaklar) çok farklıdır.
- Kullanıcı tanımada yararlanılan araçlar farklı olabilir.
- Yetkilendirme düzeyleri ve rol yönetimi açısından iç kullanımdaki karmaşıklık düzeyi dış kullanımla kıyaslanamayacak kadar karmaşıktır.

Her ne kadar iç içe geçmiş görünse de KYS ve ED bileşenlerinin aynı proje kapsamında ele alınması zorunlu değildir. Kimi zaman aynı projenin farklı fazlarının ya da tümüyle ayrı projelerin konusu da olabilirler.

4.3. Teknik Tercihler

Kimlik yönetimi projeleri her zaman çok ortamlı, çok aktörlü projelerdir. Farklı ortam ve araçlara sahip bileşenlerin bir arada uyumlu çalışabilmesi için standartlara uyumluluk çok önemlidir. Ayrıntıda kalmış teknik bir problemi çözerken bile büyük resmi kaybetmeden ve geçici kısa yollara başvurmadan, diğer bir deyişle standartlardan sapmadan çalışılmalıdır.

Bu sistemlerin çok merkezi bir konumda olduğu, kısa bir kesintinin bile çok geniş çaplı sıkıntılar yaratacağı düşünülerek sistemin kesintisiz çalışması için önlemler alınmalı, gerçekçi yük testleri yapılarak öngörülen ölçeklemenin uygunluğu sınanmalıdır.

Aslına uygun test ortamları sistem üretim ortamına alındıktan sonra da hazır tutulmalıdır.

Projeye başlamadan önce projenin en kritik bileşenlerini içeren bir **kavram doğrulama** [proof-of-concept] çalışması yapılmalı, karşılaşılan sorun ve güçlüklere göre gerekirse tasarım güncellenmelidir.

5. Sonuçlar

Sağladıkları zaman, emek ve maliyet avantajları bir yana, yalnızca bilgi tutarlılığı ve güvenlik gerekleri açısından bile değerlendirdiğimizde günümüzde orta ve büyük ölçekli kurumların kimlik yönetimi teknik ve uygulamalarına geçmeleri önem arzetmektedir. Öte yandan, kimlik yönetimi teknolojilerinin ve yazılımlarının artık olgunluk dönemine girdiği söylenebilir. Dünya ile birlikte Türkiye'de de çok sayıda uygulama gerçekleştirilmiş, önemli bir bilgi birikimi oluşmuş, pek çok uzman yetişmiştir. Tüm bu nedenlerden ötürü yakın zamanda ülkemizdeki kimlik yönetimi uygulamalarının artması beklenebilir.

Kaynakça

[1] Weitzner, D., "In search of manageable identity systems", **IEEE Internet Computing,** 10(6), 84-86, (2006).

[2] Djordjevic, I. and Dimitrakos, T., "A note on the anatomy of federeation", **BT Technology Journal**, 23(4), 89-106, (2005).

[3] Choo, K. K. R., "Issue report on business adoption of Microsoft Passport", **Information Management & Computer Security**, 14(3), 218-234, (2006).

[4] Windley, P. J., **Digital Identity**, O'Reilly, (2005).

[5] Scorer, A., "Identity Directories and Databases", Birch, D. G. W., Ed., **Digital Identity Management**, 41-52, Gover Publishing Ltd., (2007).

[6] Birch, D. G. W., McEvoy, N. A., "A Model for Digital Identity", Birch, D. G. W., Ed., **Digital Identity Management**, 95-104, Gover Publishing Ltd, (2007).

[7] Mackinson, P., "Large-Scale Identity Management", Birch, D. G. W., Ed., **Digital Identity Management**, 105-119, Gover Publishing Ltd, (2007).

[8] IT Governance Institute, **Enterprisewide Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment**, IT Governance Institute, http://itgi.org, (2004).

[9] Todorov, D., **Mechanics of User Identification and Authentication**, Auerbach Publications, (2007).

[10] Ferraiolo, D. F., Kuhn, D. R., Chandramouli, R., **Role-Based Access Control**, Artech House, (2003).

[11] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., Chandramouli, R., "**Proposed NIST Standardf or Role-Based Access Control**", ACM Transactions on Information Systems Security, 4(3), 224-274, (August 2001)