Kurumsal Bilgi Sistemleri Mimarisi Yol Haritası

25.02.2015

İçindekiler

Kurumsal Mimari Çalışmasının Amacı

Kurumun icra ettiği faaliyetler ile bilgi sistemlerini ortak bir dil, yapı ve süreç ile etkin biçimde konuşturarak kurumsal faaliyetlerin sağlıklı ve verimli bir biçimde yürütülmesine imkan sağlayacak ortamı inşa etmektir. Ayrıca bu inşa sürecini bir kurumsal mimari vizyonu ışığında yürütmeyi sağlayacak, kurumun mevcut durumundan gelecekteki hedeflenen durumuna ulaşmasını sağlayacak stratejik yol haritasını da ortaya koymaktır.

Kurumsal Mimari Vizyonu

Mimari ve Kurumsal Mimari Nedir?

Mimari, bir sistemin temellerini oluşturan yapısal organizasyonunu ifade eder. Bu sistemi oluşturan bileşenleri ve bu bileşenlerin birbirleri ve çevreleri ile olan entegrasyonu ortaya koyar. Sistemin bütüncül biçimde ortaya çıkması ve idame ettirilebilmesi için yapılması gereken tasarım ve dönüşüm faaliyetlerinin belirli bir takım prensipler üzerine oturtulmasını sağlar.

Kurumsal mimari ise, yukarıda bahsedilen mimari tanımındaki sistem olarak karşımıza çıkan yapı tüm kurum ve organizasyonun kendisidir. Kurumsal mimari, kurumun veya organizasyonun bütün iş süreçlerini, faaliyetlerini yerine getirmek için kullandığı teknolojileri ve bilgi sistemlerini kapsar.

Kurumsal Mimari Katmanları

Kurumsal mimari oluşturulması kapsamlı ve uzun soluklu bir süreç yönetimidir. Organizasyonun kurumsal mimarisini katmanlara ayrıştırarak ele almak bu sürecin adım adım başarılı biçimde yürütülmesini ve büyük resmin daha anlaşılır olmasını sağlayacaktır.

Kurumsal mimari temel olarak dört ana katmana ayrıştırılarak ele alınabilir.

1. İş Mimarisi Katmanı
2. Uygulama Mimarisi Katmanı
3. Veri Mimarisi Katmanı
4. Teknoloji Mimarisi Katmanı

İş Mimarisi Katmanı

Kurumun yürüttüğü faaliyetleri, verdiği hizmetleri tanımlayan bütün süreçleri kapsar. Bu katmanda kurumun stratejisi ve hedefleri doğrultusunda gerçekleştirdiği ve gerçekleştireceği faaliyetler ortaya konur. Bu faaliyetlerin birbirleri ile etkileşimi incelenir. Bu faaliyetleri oluşturan süreçler tespit edilir. Kurumun iş kuralları, yapısal modeli, çalışanları, müşterileri ve iş ortakları incelenir.

Uygulama Mimarisi Katmanı

Kurum bünyesinde yer alan ve alacak kurumsal faaliyetleri yürütmeye hizmet eden bütün uygulamaları kapsar. Bu uygulamalar kurum içerisinde çalışanlara veya kurumun müşterilerine, vatandaşlara, iş birliği yaptığı diğer kurum ve kuruluşlara çok çeşitli hizmetler sunabilir.

İş ve uygulama katmanına odaklanırken, kuruma daha çok fonksiyonel bir perspektiften bakılması gerekir. Kurumun fonksiyonlarının ve aktivitelerinin tanımlanması ve modellenmesi ana hedeftir.

İş katmanında zaman içerisinde ortaya çıkan gereksinimlerin uygulama katmanında farklı uygulamalarca karşılanması, bu uygulamaların birbirleri ile entegrasyon halinde olmasını gerektirir. Uygulamalar arasında kurulan entegrasyon altyapısı sayesinde herhangi bir uygulamada başlatılan bir süreç bir diğer uygulama tarafından devam ettirilebilir, ya da herhangi bir uygulama tarafından üretilen veya saklanan veri başka bir uygulama tarafından kullanılabilir. Böylece veri mimarisi içerisinde oluşturulan ortak veri modelinin farklı kısımları farklı uygulamalarca yönetilebilir hale gelir.

Veri Mimarisi Katmanı

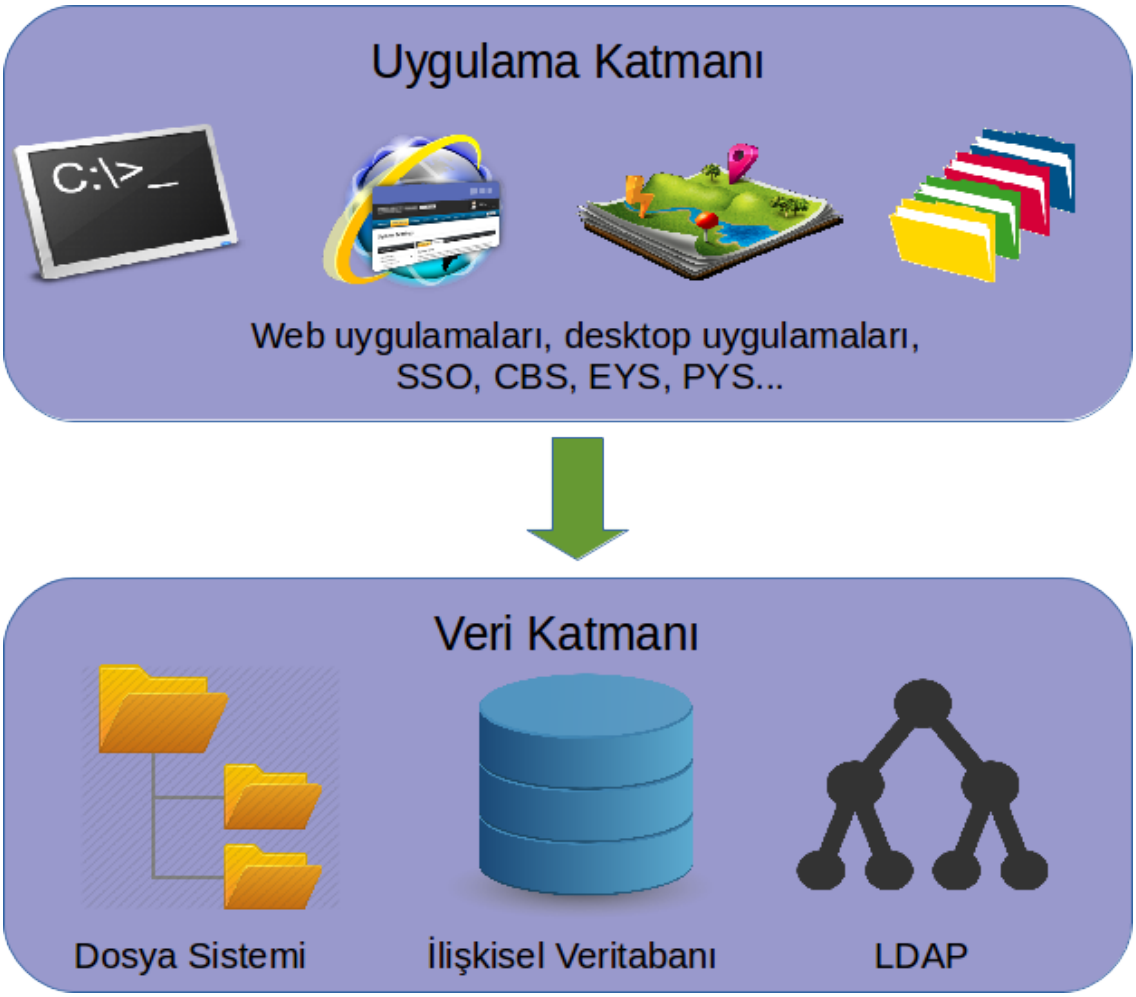
Kurumun sahip olduğu bütün veri ve bilgiyi, bu verinin ve bilginin nasıl ele alınacağını, yapılandırılacağını ve saklanacağını belirler. Kurumun sunacağı faaliyetler sırasında ihtiyaç duyulan veya bu faaliyetler sonucu ortaya çıkan verinin ve bilginin mantıksal ve yapısal bir modeli oluşturulur. Ana ve kritik veri tipleri, bunlar arasındaki ilişkiler, uygulama katmanındaki uygulamaların çalışırken veya birbirleri ile iletişimlerinde kullanacakları veri tespit edilerek, yapılandırılır.

Bu katmanda daha çok kurumun sahip olduğu veri ve bilgiye, ortak bir veri modeli ve ver

sözlüğü oluşturulmasına, uygulamalar ve kurumlar arasında veri alış verişine, verinin mantıksal ve fiziksel olarak nasıl yapılandırılacağına odaklanılır. Kurumun işleyişine ve yapısına daha çok organizasyonel bir perspektiften bakılmalıdır.

Kurumsal bilgi sistemi içerisinde yönetilen veri, veri katmanında farklı veri yapıları içerisinde tutulabilir. Örneğin kişi ve kullanıcı bilgileri LDAP içerisinde tutulurken organizasyon ağacı ilişkisel bir veritabanında tutulabilir. Benzer şekilde uygulama katmanında bir elektronik belge yönetim sistemi üzerinden takip edilen doküman ve belgeler dosya sisteminde saklanırken bu belgelerin öznitelikleri veya iş akış tanımları ilişkisel veri tabanında saklanabilir. Dahası, ilişkisel veri tabanı sistemleri içerisinde tutulan verilerin bir kısmı bir veri tabanı içerisinde tutulurken başka bir kısmı da ayrı bir veri tabanı içerisinde tutulabilir. Bu dağıtık yapıya kurumsal veri güvenliği politikası, uygulama katmanındaki farklı uygulamalar ya da kullanılan farklı teknolojik altyapı gereksinimleri neden olabilir.

Veri katmanında verinin farklı veri yapıları içerisinde dağıtık bir şekilde tutulması beraberinde bazı detaylar üzerinde düşünmeyi gerektirir. Bunlardan biri de veri sahipliğidir. Kurumsal veri mimarisi içerisinde tutulan her bir verinin uygulama katmanı üzerinden yönetildiği ayrı bir uygulama olmalıdır. Veriler bu uygulamalar tarafından yaratılır, güncellenir ve gerektiğinde silinir. Veriyi oluşturan, güncelleyen ya da silen uygulama söz konusu verinin sahibidir (master). Kurumsal veri mimarisi oluşturulurken hangi verinin sahibinin hangi uygulama olacağına dikkat edilmelidir.



Her ne kadar verinin bir sahibi olsa da bu veriyi kullanan farklı uygulamalar da olabilir. Bu uygulamalar veriye sadece okuma amaçlı erişebildiği gibi, çok tercih edilmesede değiştirme veya silme yetkisine de sahip olabilir. Ayrıca kurumsal bilgi güvenliği politikası gereği bu uygulamaların verinin tümüne ya da belirli bir kısmına erişim yetkisi verilebilir. Bu durum, verinin farklı kopyalarının farklı sistemlerce tutulması gereksinimini beraberinde getirebilir. Bu işleme veri replikasyonu adı verilir.

Veri replikasyonunda en çok dikkat edilmesi gereken noktalardan birisi de veri senkronizasyonudur. En başından itibaren dikkatli kurgulanmamış bir veri mimarisi içerisinde zaman içerisinde farklı veri yapılarında bir bilginin birden çok farklı ifadesine rastlamak olasıdır. Bunlar farklı

veri yapıları üzerinde farklı biçimlerde tutulan veriler olsa da iş katmanından bakıldığında aslında aynı bilgiyi barındırabilir. Bu durumun temel sebepleri şunlardır:

1. Veri sahipliğinin açıkça ortaya konmaması
2. Veriyi kullanan uygulamalarca tutulan replikasyonların düzgün yönetilmemesi
3. Farklı veri yapılarında tutulan verinin farklı kopyalarının senkronize edilmemesi

Yukarıda bahsi geçen problemlerin ortaya çıkmaması için gerekli önlemler veri mimarisi kurulurken en başından itibaren alınmalıdır. Buna master veri yönetimi adı verilir. Master veri yönetimi kapsamında dikkat edilmesi gereken noktalar şunlardır:

- Veri mimarisi içerisinde tutulması planlanan kullanıcı, bilgileri, organizasyonel birimler gibi kurumun temel verileri (master veri) analiz edilmelidir,
- Söz konusu verilerin nasıl bir veri yapısında ve nerede tutulacağına karar verilmelidir.
- Master veri üzerinde kurumsal veri güvenliği politikalarına göre erişim izinleri belirlenmelidir.

Bu verilerin diğer sistemlerce kullanımı için hangi kısmının hangi şekilde entegrasyona açılacağı belirlenmelidir.

Teknoloji Mimarisi Katmanı

Kurumun bilgi sistemlerinin çalışması için gerekli bütün yazılımsal ve donanımsal bileşenleri ve ortamı tanımlar. Bu aşamada kurumun bilgi sistemleri alt yapısına odaklanılır. Altyapıyı oluşturan donanımın özellikleri, kurulumu, konfigürasyonu, bu donanımın nasıl ve nerede idame ettirileceği, ağ yapısı, sunucular, veritabanları, son kullanıcı bilgisayarları, bunların fiziksel ve işletimsel güvenliği ele alınır.

Kurumsal Mimari Geliştirme Metodu

Kurumsal mimari çalışmalarında belirli fazlardan oluşan bir geliştirme metodunu izlemek önemlidir. Bu metodun her fazında yapılması gereken çalışmalar ve ortaya çıkacak yan ürünler net biçimde tespit edilmelidir. Genel olarak böyle bir çalışmayı oluşturacak fazlar şu şekilde tanımlanabilir.

1. Mevcut durumun tespit edilmesi, mimari vizyonunun ortaya konması, hedeflerin ve prensiplerin belirlenmesi
2. Güvenlik mimarisinin oluşturulması
3. Kurum organizasyon yapısının modellenmesi
4. İş katmanı üzerinde çalışma
5. Uygulama katmanı üzerinde çalışma
6. Veri katmanı üzerinde çalışma
7. Teknoloji katmanı üzerinde çalışma
8. Mevcut durumdan hedeflere ulaşmak için bir takvim oluşturulması ve uygulama sürecine geçilmesi
9. Uygulama sürecinde edinilen deneyimlerin ve ortaya çıkan ürünlerin değerlendirilmesi ve mimarisel çalışmaya geri besleme yapılması

Kurumsal mimari oluşturma daha önce de belirtildiği gibi bir süreçtir ve sürekli devam eder. Hedeflenen aşamaya gelindiğinde elde edilen sonuçlar ve deneyim, ortaya çıkan yeni ihtiyaçlar doğrultusunda yukarıdaki adımlar sürekli biçimde işletilerek mimarinin gelişim süreci devamlılık arz eder.

Kurumsal Güvenlik Mimarisi

Kurumsal güvenlik mimarisi, kurumsal bilgi sistemleri mimarisinin temel bir yapı taşıdır. Kurumsal bilgi sistemleri mimarisini oluştururken ilk aşamadan itibaren güvenlik gereksinimleri üzerinde durmak, bu gereksinimleri karşılayacak bir mimari yapı oluşturmak kurumun faaliyetlerini emniyetli ve kesintisiz biçimde sürdürebilmesi için oldukça önemlidir. Güvenlik mimarisinin ilk aşamada oluşturulması ile kurumsal mimarinin içerisinde yer alacak bileşenlerin sahip olması gereken güvenlik fonksiyonları, bu bileşenlerin devreye alındığı andan itibaren güvenli biçimde işletilebilmelerini sağlayacaktır. Zaman içerisinde sisteme dahil edilen farklı uygulamaların ve hizmetlerin kendine özgü veya eksik güvenlik kabiliyetleri nedeni ile kurumun bilgi sistemleri altyapısının zafiyete uğraması ihtimali azalacaktır. Uçtan uca tutarlı bir güvenlik modeli kurumsal mimariye hakim kılınabilecektir.

Herhangi bir kurum veya organizasyonun güvenlik gereksinimleri kurumun yerine getirdiği iş faaliyetleri, dışarıdan veya içeriden kaynaklanacak güvenlik tehditleri, kurumun uyması veya yerine getirmesi gereken yasal düzenlemeler ve standartlar tarafından belirlenmektedir. Kurumsal güvenlik mimarisinin temel amacı kuruma ait verinin ve bilginin gizli kalmasını, tutarlılığının korunmasını ve erişiminin sürekli kılınmasını sağlamaktır.

Güvenlik çözümlerinde sistem kullanıcılarını gerçekleştirdikleri faaliyetler ile ilgili yasal olarak mesul kılma (accountability) temel bir yaklaşımdır. Bir kullanıcının gerçekleştirdiği herhangi bir faaliyetle ilgili mesul tutulabilmesi için öncelikle kullanıcının kimliğinin tespit edilmesi gerekir. Daha sonra kullanıcının sistem üzerinde sadece belirli bir takım işlemlere yetkili kılınması gerekir. Son olarak sistem üzerinde gerçekleşen her türlü işlemin takip edilmesi ve denetlenmesi gerekir. Gerçekleşen her işlem ile bu işlemi gerçekleştiren kullanıcı tespit edilmelidir. Ancak bu şekilde kullanıcı ilgili faaliyeti gerçekleştirmekten mesul tutulabilir. Mesul kılma kabiliyetini hayata geçirebilmek için sistemin güvenlik mimarisinin şu üç ana kabiliyeti sunması gerekir

1. Kimliklendirme (Authentication)

2. Yetkilendirme (Authorization)
3. Denetim (Audit)

Bu üç kabiliyete güvenlik mimarisinin “altın standartı” denir. Herhangi bir kurumsal bilgi sisteminde güvenlik mimarisini ele alırken de bu kabiliyetlerle bağlantılı olarak kurumsal güvenlik mimarisi üç ana bölümde ele alınabilir.

1. Kimliklendirme ve kimlik yönetim sistemi
2. Yetkilendirme ve erişim kontrol sistemi
3. Denetim ve iz sürme sistemi

Kimliklendirme ve Kimlik Yönetim Sistemi

Kullanıcı kimliği, kullanıcıyı tanımlayan öznitelikler kümesidir. Her bir öznitelik kullanıcı ile ilgili bir özelliği veya ifadeyi ifade eder. Kullanıcıyı ifade eden özniteliklerden, onu diğer bütün kullanıcılardan ayırt etmeye yarayan öznitelik tanımlayıcı/benzersiz niteleyici (identifier) olarak adlandırılır. Kimliklendirme herhangi bir sisteme veya uygulamaya erişen kullanıcının kimliğinin tespit edilmesi sürecidir. Her sistemin veya uygulamanın kendine ait kullanıcıları mevcuttur. Bu kullanıcıların birbirlerinden ayrıştırılabilmesi için sistem genelinde benzersiz bir niteleyici bilgiye (identifier) ihtiyaç vardır. Kullanıcı sisteme erişmek istediği vakit bu benzersiz niteleyici bilgisini, sadece kendisinin bildiği, sadece kendisinin sahip olduğu bir gizli bilgi – özniteliklerden biri veya birkaçı- ile birlikte sunarak sisteme giriş yapar. Sistem, verilen niteleyici ve gizli bilgiyi kendi kayıtları ile eşleştirerek kullanıcının gerçekten niteleyici ile belirttiği kullanıcı olup olmadığını denetler.

Kimliklendirme Yöntemleri

Güvenlik düzeyi, maliyeti ve kullanım kolaylığı açısından farklı düzeyde güvenlik sağlayan üç çeşit kimliklendirme yöntemi mevcuttur.

1. Biyometrik kimliklendirme: parmak izi veya retina taraması gibi. Bu tür kimliklendirme yöntemlerinde sadece kullanıcının biyolojik olarak sahip olduğu , onu diğerlerinden benzersiz kılan bir özelliği (something you are) kullanılır.
2. Donanımsal bir kart veya jeton ile kimliklendirme: akıllı kartlar, USB token'lar gibi. Bu tür kimliklendirme yöntemlerinde ise sadece kullanıcının edinebileceği, veya sadece onun mülkiyetinde olan bir araçtan (something you have) yararlanılır.
3. Kullanıcı parolası ile kimliklendirme: Şifre, parola gibi. Bu tür kimliklendirme yöntemlerinde ise sadece kullanıcının bildiği gizli bir bilgi (something you know) kullanılır.

Kurumun güvenlik ihtiyaçları doğrultusunda bu üç kritere göre en uygun kimliklendirme yöntemini tercih edilmelidir. Bu yöntemlerden herhangi ikisini veya üçünü birlikte kullanarak sistem güvenliği artırılabilir. Örneğin akıllı kart ve kullanıcı şifresini birlikte kullanmak, yada kullanıcı şifresinin

yanında birde kullanıcıya tek kullanımlık bir şifrenin cep telefonuna gönderilmesi gibi. İki kimliklendirme yöntemini aynı anda kullanarak gerçekleştirilen kimliklendirme işlemine iki faktörlü kimliklendirme (two factor authentication) denmektedir.

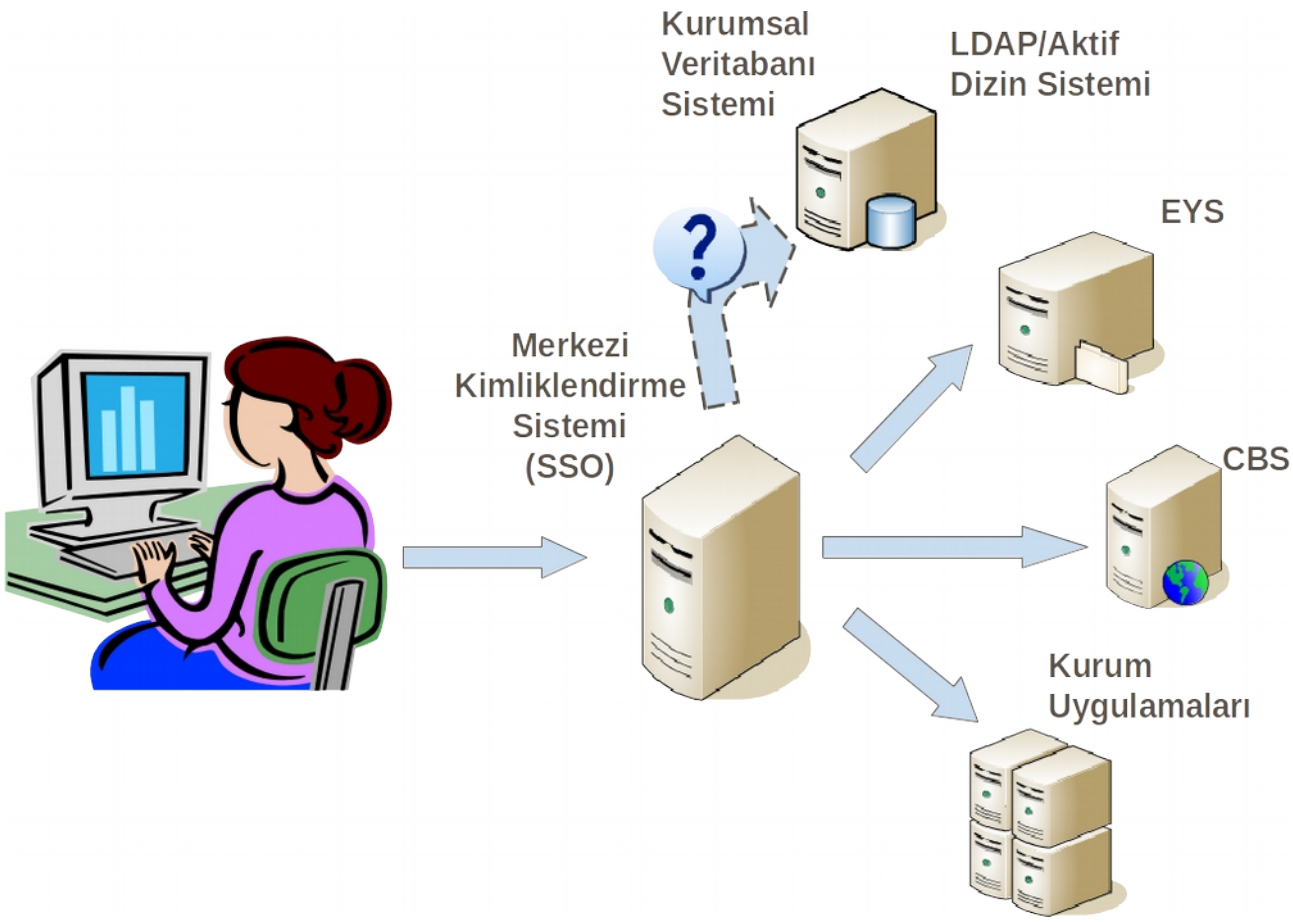
Kimliklendirmenin Kapsamı

Kurumun bilgi sistemi içerisinde farklı kapsamda etkinliğe sahip kimliklendirme işlemleri gerçekleştirilebilir.

1. Kurumsal ağ ortamında kimliklendirme
2. İşletim sistemi ortamında kimliklendirme
3. Uygulama ve servisler düzeyinde kimliklendirme

Örneğin, kullanıcının masasındaki bilgisayara ve diz üstü bilgisayara erişmek istediğinde işletim sistemi düzeyinde kimliklendirme yapılmaktadır. Eğer kurumun bilgi sistemlerine uzaktan erişim mümkün ise kurumsal ağa erişim sırasında da ağ ortamında kimliklendirme yapılmaktadır. Ya da kurum içindeki herhangi bir uygulamaya erişim söz konusu olduğunda kullanıcın uygulama tarafından kimliği denetlenmektedir.

Merkezi Kimliklendirme Sistemi



Herhangi bir kurumda hizmet veren pek çok farklı uygulama ve servis mevcuttur. Kullanıcılar bu uygulamalara eriştiğinde her bir uygulamanın kendi kimliklendirme işlemini kendisinin yapması yerine kimliklendirme hizmetinin merkezi bir kimliklendirme sunucusu tarafından sağlanması da mümkündür. Bu sayede farklı uygulamaların kullanıcıya ait gizli kimliklendirme bilgisine erişmesi ihtiyacı ortadan kalkacaktır. Kurum genelinde kimliklendirme hizmeti standartlaşacak ve daha emniyetli bir hal alacaktır.

Merkezi Kimlik Yönetim Sistemi

Kurumsal bilgi sistemindeki farklı işletim sistemlerinin, ağ cihazlarının, sunucuların ve uygulamaların kullanıcı bilgilerinin ortak bir sistem tarafından yönetilmesini sağlar. Kullanıcı

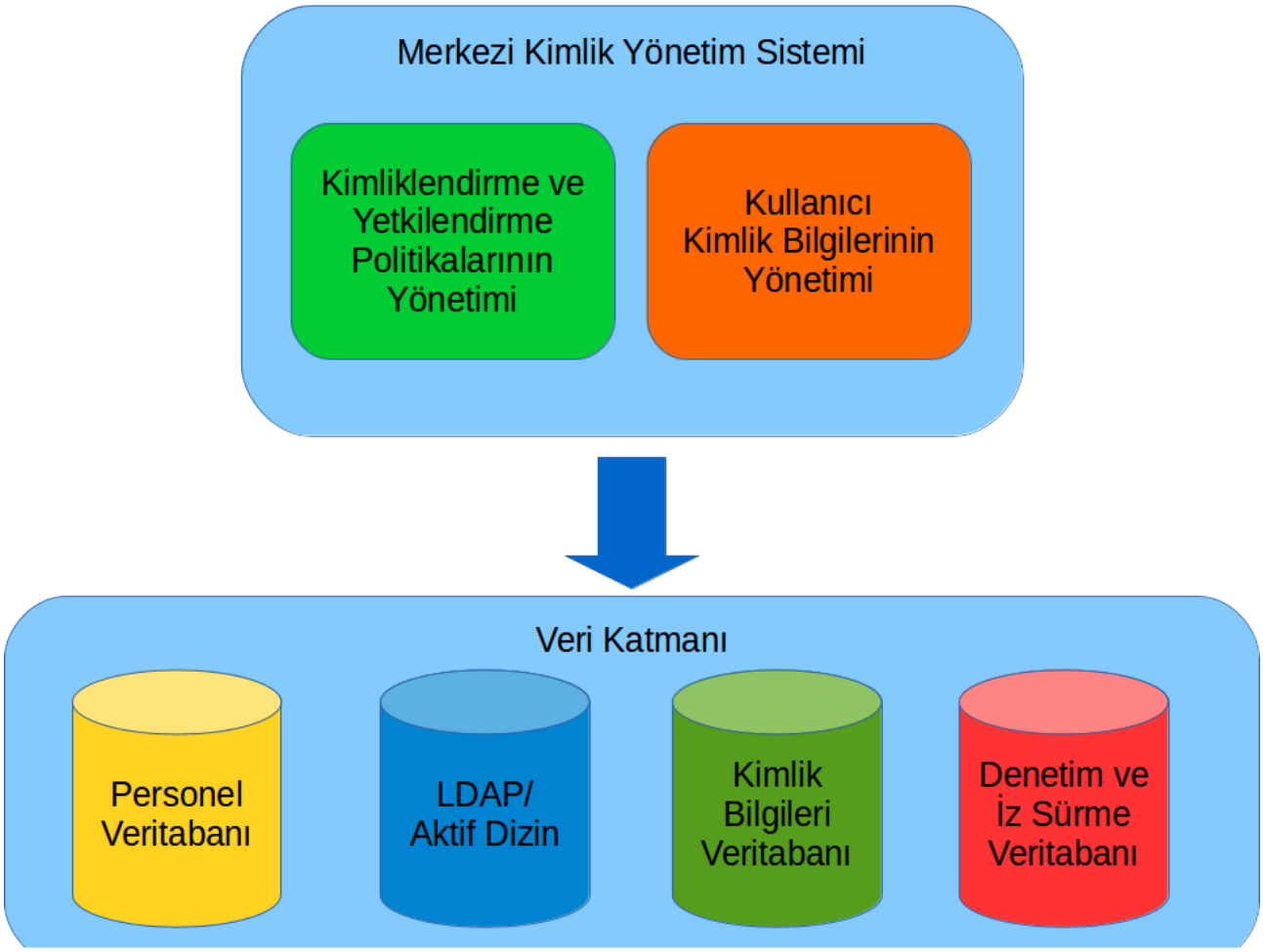
bilgilerinin yanında kullanıcının kurum içindeki farklı sistemlere ve hizmetlere erişim yetkileri de bu sistem tarafından yönetilebilmektedir.

Kurumun kullanıcı bilgisinin depolama alanı olarak LDAP veya LDAP uyumlu Microsoft Aktif Dizin kullanımı yaygın bir pratiktir. LDAP ile kurum kullanıcı bilgisi, organizasyon hiyerarşisi ile beraber merkezi bir yerde depolanarak yönetilebilir. LDAP üzerinde kullanıcının, görev, ünvan, telefon, adres gibi değişik öznitelikleri tutulur. Bu öz niteliklerden bir kısmı, -isim, e-posta, ünvan gibi- statik, diğer bir kısmı -lokasyon, IP gibi- dinamik olarak nitelendirilmektedir. LDAP türevi bir sistem kimliklendirme sürecinde yaygın içimde kullanılmasına rağmen, uygulama ve hizmetlerin erişim yetkilerinin yönetimi için uygun bir ortam değildir. Bu tür veriler genellikle ilişkisel veritabanında tutularak, çalışma zamanında LDAP üzerinden elde edilen veri ile birleştirilmektedir.

Şifrelerin Saklanması

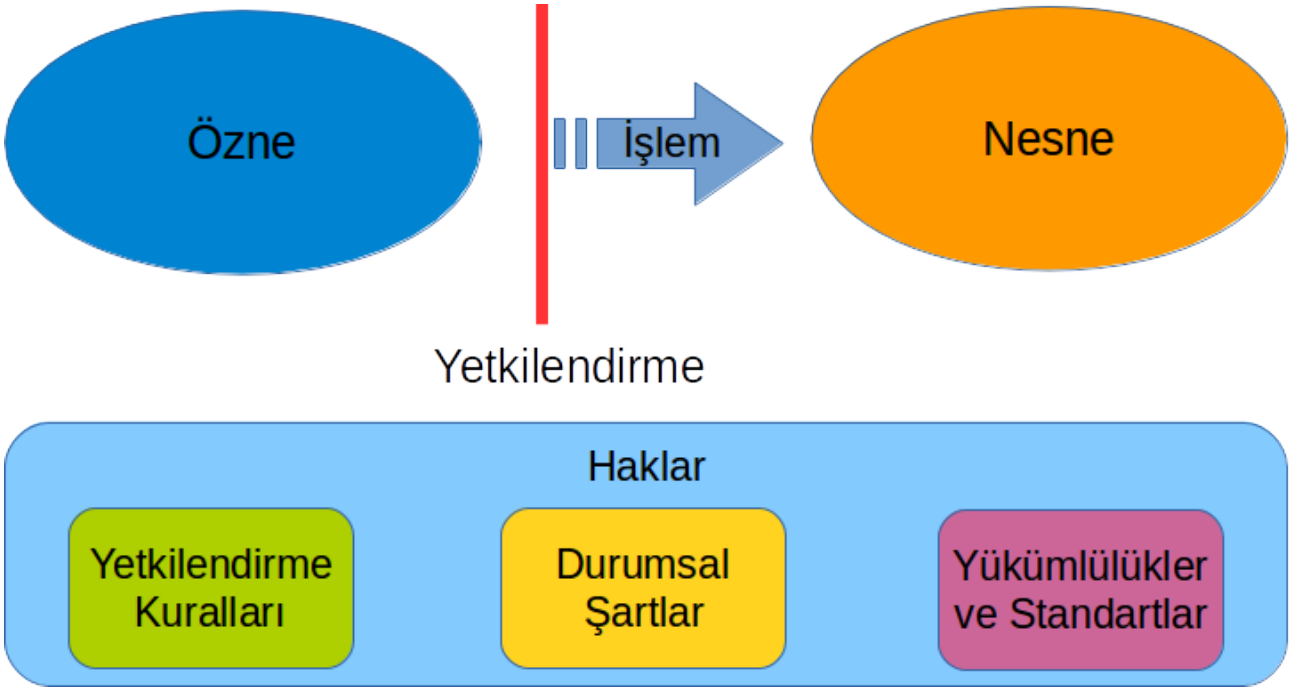
Kullanıcılara ait şifrelerin emniyetli biçimde sistem tarafından korunması gerekir. Dikkat edilmesi gereken hususlardan bazıları şunlardır:

- Şifreler düz metin şeklinde saklanmamalıdır. Tek yönlü bir kodlama algoritmasından geçirerek kriptolu biçimde saklanmalıdır.
- Kriptolama sırasında şifreye, gizli veya tek kullanımlık bir tuz değeri (salt) eklemek sözlük saldırılarından korunmak için önemlidir.
- Normal kullanıcılar kesinlikle şifrelerin saklandığı dosyaya erişmemelidir. Bu dosya üzerinde okuma veya yazma izinleri olmamalıdır.
- Kimliklendirme uygulaması şifrelerin tutulduğu dosyaya erişim hakkına sahip olmalıdır.
- Kullanıcı bilgilerini yöneten bölümlerde şifre dosyasına erişebilir, dosyayı güncelleyebilir.



Yetkilendirme ve Erişim Kontrol Sistemi

Kimliklendirmenin ardından kullanıcının sistem üzerinde sadece yetkili olduğu işlemleri yürütmesi, kurumsal veri ve bilgiye izinler dahilinde erişebilmesi, diğer yandan yetkisi dışında kalan hizmetlere ve bilgiye erişiminin kısıtlanması işlemine yetkilendirme adı verilmektedir.



Yetkilendirme işleminde özne genellikle son kullanıcı olsa bile, herhangi bir uygulama, program veya dış sistem de özne olarak ele alınabilir. Diğer yandan erişim denetimine tabi tutulan nesne çoğunlukla kurumsal veri veya bilgi olsa da, herhangi bir uygulama, süreç, disk erişimi, ağ kullanımı da nesne olarak ele alınıp erişim denetimine tabi tutulabilir. Öznenin nesne üzerinde gerçekleştirdiği işlem ise çoğunlukla veriye erişim veya veri üzerinde çalışma olsa bile, bir uygulamanın veya hizmetin çalıştırılması, bir dosyanın kopyalanması veya yazdırılması gibi herhangi bir faaliyet de yetki denetimine tabi tutulan işlem olabilir.

Öznenin nesne üzerinde gerçekleştireceği işlemin yetkilendirilmesi bir takım haklar üzerinden gerçekleştirilir. Bu haklar temelde üç ana grupta incelenebilir:

1. Yetkilendirme kuralları
2. Durumsal şartlar
3. Yükümlülükler ve standartlar

Yetkilendirme kuralları roller veya erişim kontrol listeleri şeklinde ifade edilebilir. Bu bölüm aşağıda detaylandırılmıştır. Durumsal şartlar ise nesne ve öznenin de içinde yer aldığı ortamla ilgili

durumları ve şartları tanımlar. Örneğin, işlemin gerçekleştiği zaman aralığı, erişimin gerçekleştiği uygulama, öznenin erişim lokasyonu veya terminali gibi. Yükümlülükler ve standartlar ise erişimin uygun biçimde gerçekleşmesi için gerekli olan bir takım uyulması gereken kuralları, standartları ve denetim mekanizmalarını tanımlar. Örneğin, sistemden alınan çıktı içerisine filigran yerleştirilmesi, güvenlikli ve kritik herhangi bir kaynağa erişirken iz takip loglarının üretilmesi gibi.

Kurumsal güvenlik mimarisinde yetkilendirme kurallarının uygulanmasında üç farklı metot mevcuttur:

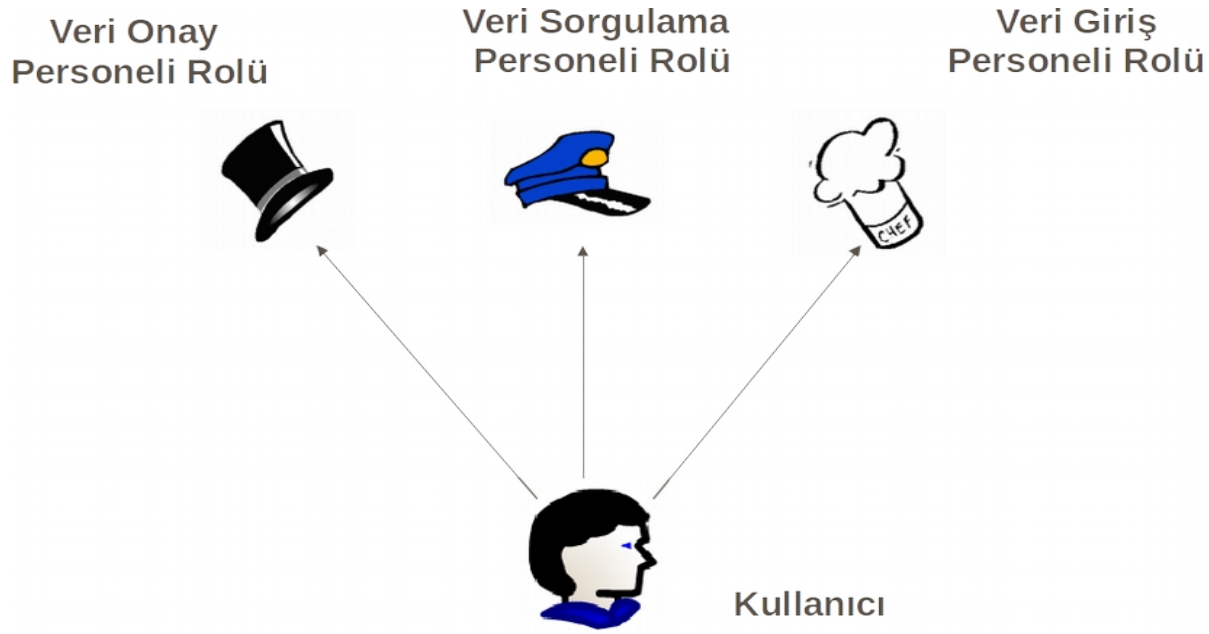
1. Rol tabanlı yetkilendirme
2. Erişim kontrol listesi tabanlı yetkilendirme
3. Durum tabanlı yetkilendirme

Rol Tabanlı Yetkilendirme

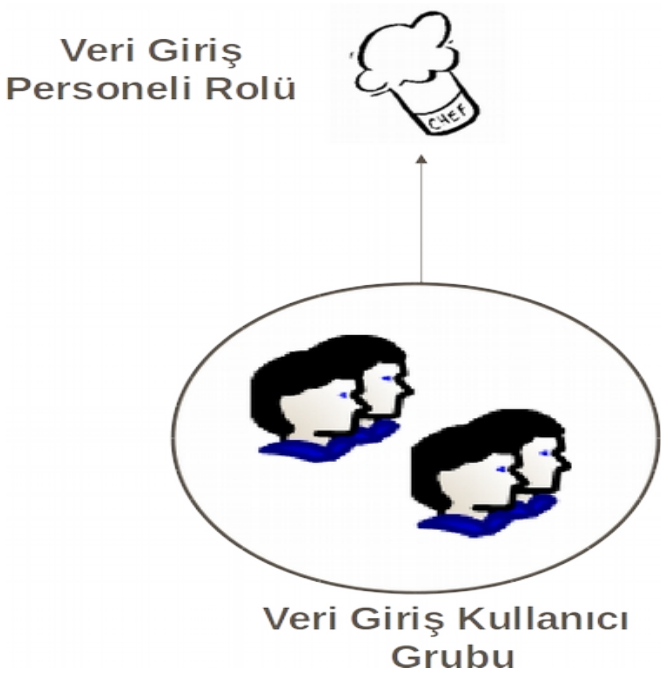
Sistem genelinde kullanıcılara veya kullanıcı gruplarına atanan bir veya birkaç rol vardır. Kullanıcılar sahip oldukları bu rollere göre bir takım işlemleri gerçekleştirebilirler. Bu yönteme rol tabanlı yetkilendirme (RBAC) adı verilmektedir. Rol tabanlı yetkilendirmede kullanıcı, rol ve kurumun organizasyon hiyerarşisi arasında birtakım yapılar temel teşkil etmektedir.

Kullanıcı Rol İlişkisi

Sistem kullanıcıları kendilerine atanmış rollerin izin verdiği ölçüde sistemi kullanabilirler. Bir kullanıcı birden fazla role sahip olabilir. Bir rol de birden fazla kullanıcı tarafından paylaşılabilir. Roller arasında hiyerarşi oluşturmak da mümkündür. Örneğin, ROLE_USER en düşük rol tanımı olarak bir kaynağa erişime yetkili iken, ROLE_EDITOR, hem bu kaynağa erişmeye hem de içeriğinde değişiklik yapmaya yetkili olabilir. ROLE_ADMIN'e ise kaynak üzerinde silme de dahil olmak üzere her türlü işlemi yapmasına izin verilebilir. Bu durumda ROLE_ADMIN rolüne sahip bir kullanıcının aynı zamanda ROLE_USER ve ROLE_EDITOR rollerine de sahip olduğu söylenebilir. Rol tabanlı yetkilendirme de isteğe bağlı olarak UNIX sistemlerdeki gibi sistem üzerinde her türlü işlem yapmaya yetkili root kullanıcısı da tanımlamak mümkündür.



Kullanıcı, Rol ve Kullanıcı Grubu İlişkisi

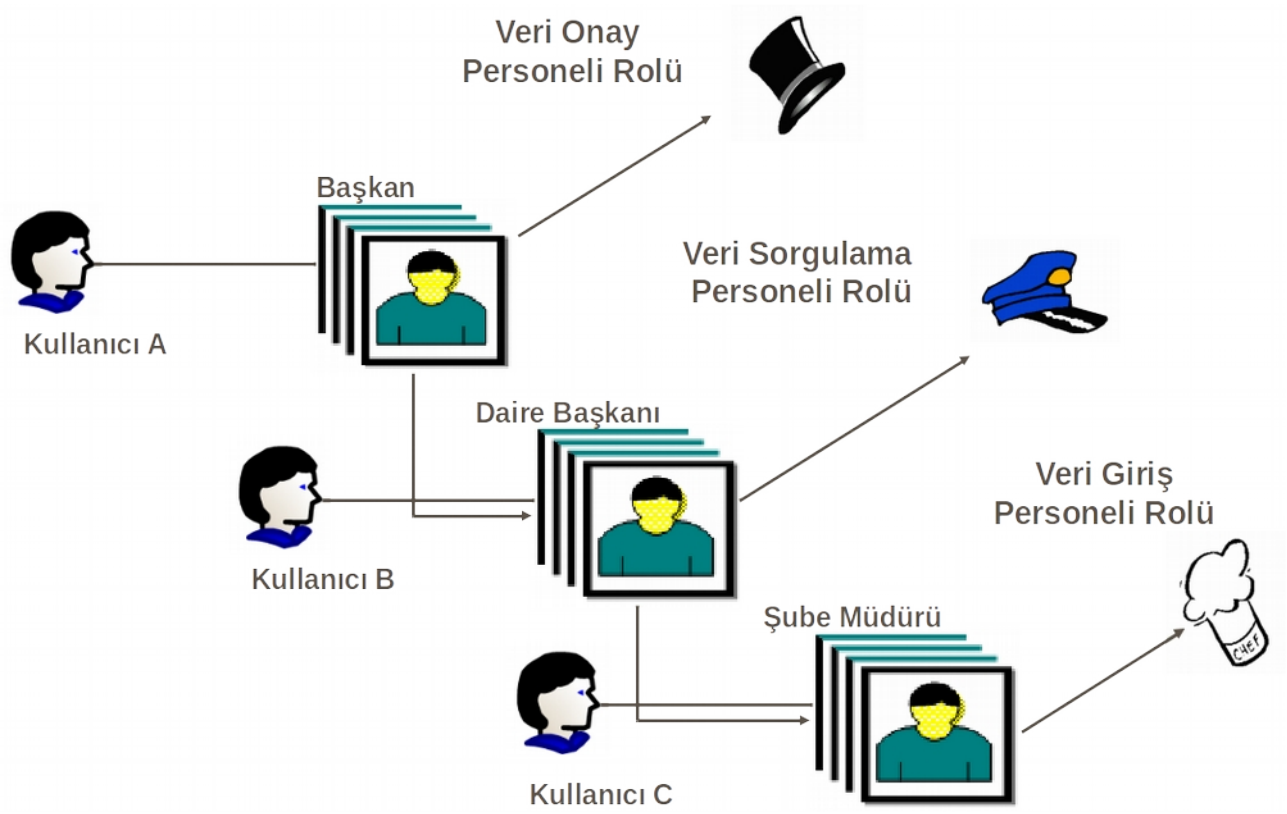


Kullanıcı grupları, bir grup kullanıcının bir araya getirilmesinden oluşur. Rolleri teker teker kullanıcılara atamak yerine doğrudan bu kullanıcı gruplarına rol ataması yapılabilir. Bu durumda o gruba dahil kullanıcıların hepsi atanan role sahip olurlar. Kullanıcının gruptan çıkarıldığı vakit role

sahip olması da sona ermiş olur. Ayrıca kullanıcı grupları arasında da hiyerarşi olabilir. Örneğin, bir grubun bağlı olduğu bir üst grup olabilir. Birden fazla grup bir gruba bağlı olabilir. Bu gibi bir durumda üst grup üyeleri kendisi altındaki bütün grupların rollerine de sahip kabul edilebilir.

Kullanıcı, Organizasyon Hiyerarşisi, Makam ve Rol İlişkisi

Kurumun organizasyon hiyerarşisindeki her bir birim bir makam olarak ele alınabilir. Her makamın sahip olduğu bir takım roller olabilir. Bir rol birden fazla makama da atanabilir. Organizasyon hiyerarşisinde üstteki bir makam alttaki makamların sahip olduğu rollere otomatik olarak sahip olabilir. Her makama asaleten veya vekaleten atanmış kullanıcılar olabilir. Kullanıcı aynı anda birden fazla makama atanmış olabilir.



Erişim Kontrol Listesi Tabanlı Yetkilendirme

Erişim kontrol listesi tabanlı yetkilendirme ise UNIX işletim sisteminin yetkilendirme modeline benzer. Bu yönteme isteğe bağlı erişim kontrolü (DAC) adı da verilmektedir. UNIX işletim sisteminde

özne kendimiz, ait olduğumuz gruplar veya diğerleri şeklinde üçe ayrılmaktadır. Nesne ise burada dosya veya uygulamadır. Dosya veya uygulama üzerinde gerçekleştirilebilecek işlemler okuma, yazma, silme ve çalıştırma olarak tanımlanmıştır. Nesnenin sahibi ilgili öznelere bu yetkilerden uygun gördüklerini atamadan sorumludur. Atanan bu yetkiler dahilinde özne de nesne üzerinde izin verilen işlemleri gerçekleştirebilir. Nesne üzerinde kimin hangi izinlere sahip olduğu bilgisine de erişim kontrol listesi (ACL) adı verilir.

Özne	İşlem	Nesne
Kendi	R	dosya
Grup üyeleri	W	proses
Diğer herkes	X	

Nesne sahibinin, nesne üzerinde uygun yetkileri ataması kendi sorumluluğundadır. Eğer sadece kendisinin görmesini istediği bir dosya için herkese erişim izni verirse bu hatanın sorumluluğu da kendisindedir. Büyük sistemlerde kullanıcıların yetki atama işlemlerinde yapabilecekleri hataları azaltmak ve atama işlemine birtakım sınırlar getirmek amacı ile zorunlu erişim kontrol yöntemi (MAC) uygulanabilir. Bu yöntemde erişim izinlerinin atanmasında kullanıcılar tamamen bağımsız ve özgür değillerdir. Kendilerine verilen izin doğrultusunda yetkiler atayabilirler. Bu yöntemde, erişim denetimine tabi tutulacak nesnelerin kendilerine has özellikleri tanımlanır. Bu özelliklere etiket adı da verilmektedir. Etiketler de bölümlere göre kendi aralarında gruplanabilirler. Bu bölümleme, domain, kategori, veya kademe şeklinde olabilir. Örneğin üst kademeden alt kademeye veri akışına izin verilmeyebilir. Ya da farklı domain'lerdeki kullanıcılar arasında veri akışı kısıtlanabilir. Bu şekilde yetkilerin atanmasında belirli bir takım kuralların zorlandığı yapıya kapsama alanı (protection domain) adı verilir.

Durum Tabanlı Yetkilendirme

Sistem ve kullanıcı ile ilgili bir takım durumsal ifadeleri kontrol ederek yapılan yetkilendirmedir. Kullanıcının erişim IP'si 192.168.1.0/24 aralığında ise, erişim zamanı 08:00 ile 17:00 arası ise veya kullanıcı BMO üyesi ise, dokümanın günlük print etme sayısı aşılmamış ise, gibi ifadeler durumsal ifadelere örnek olarak verilebilir. İki veya daha fazla durumsal ifade mantıksal operatörler

(ve, veya, değil) yardımı ile bir araya getirilerek bileşke durumsal ifadeler de oluşturulabilir. Bu durumsal ifadeler çalışma zamanında kullanıcının o anki erişim bilgisi, sistem zamanı, dokümana erişim sayısı gibi bilgiler ile değerlendirilerek istenen işlemin çalıştırılıp çalıştırılmamasına karar verilir. Literatürde bu tür yetkilendirme yöntemine claims based veya proof carrying authorization isimleri de verilmektedir. Ancak bu tür yetkilendirmeyi Türkçe'de en iyi durum tabanlı yetkilendirme karşılamaktadır.

Durum tabanlı yetkilendirme diğer iki yetkilendirme yöntemi ile birlikte, bunları tamamlayıcı biçimde de kullanılabilir. Örneğin, kullanıcının herhangi bir doküman üzerinde işlem yapıp yapamayacağı ilk etapta rol tabanlı yetkilendirme veya erişim kontrol listesi tabanlı yetkilendirme ile tespit edildikten sonra, durumsal ifadeler üzerinden kullanıcının o an için o doküman üzerinde belirtilen işlemi yapıp yapamayacağına karar verilebilir.

Denetim ve İz Sürme Sistemi

Kurumsal bilgi sistemlerinde kullanıcıların gerçekleştirdiği işlemlerinin takibinin ve izinin sürülmesini sağlar. Kurumsal güvenlik mimarisinde önemli bir ayaktır. Kurum içerisinde meydana gelebilecek güvenlik problemlerinin sorumlularını tespit edebilmek için bu sistem tarafından üretilen kayıtlara ihtiyaç duyulur. Bazı durumlarda bu sistem gerçekleşen işlemlerle ilgili detaylı bir iz kaydı oluşturmakla yetinebildiği gibi, diğer bazı durumlarda sistem yöneticisinin anlık olarak bilgilendirilmesi de söz konusu olabilmektedir.

Sistemin iz kaydı oluşturacağı veya sistem yöneticisini anlık olarak uyaracağı durumlar şu şekilde sıralanabilir:

- Güvenlikli veya hassas veri üzerinde gerçekleşen okuma, yazma veya silme işlemleri
- Erişim kontrol verisi ile ilgili değişiklikler
- Sistem konfigürasyonu üzerinde yapılan işlemler

Üretilen iz kayıtları kim, ne, nerede, ne zaman ve nasıl sorularına cevap verebilecek detayda bilgi içermelidir. Bu bilgi örneğin, erişim zamanı, kullanıcı adı, kullanıcının IP adresi, işlem türü, işlem

sonucu, ve üzerinde işlem yapılan veriden oluşabilir. Şifre gibi bazı hassas verinin kriptolu biçimde bile olsa iz kayıtları içerisinde yer almaması gerekebilir. Ayrıca kullanıcıların mahremiyetine de dikkat etmek gerekebilir. Bazı bilgiler kullanıcının mahrem özellikleri arasına olabilir, bu durumda ilgili özellikler iz kayıtlarında yer almamalıdır.

Üretilen iz kayıtlarının güvenliği de önemlidir. Bu kayıtlar sistemden farklı ayı bir veya birkaç alanda birlikte toplanmalı, zaman damgalı olmalı, başkaları tarafından kesinlikle değiştirilememeli, sıkıştırma ve arşivleme işlemlerine tabi tutulabilmelidir. Log kayıtları merkezi tek bir yer yerine farklı lokasyonlarda tutuldukları için herhangi birinde meydana gelebilecek bir saldırı ve kayıtların değiştirilmesi aksiyonu, diğer replikeler üzerindeki kayıtları inceleyerek tespit edilebilir.

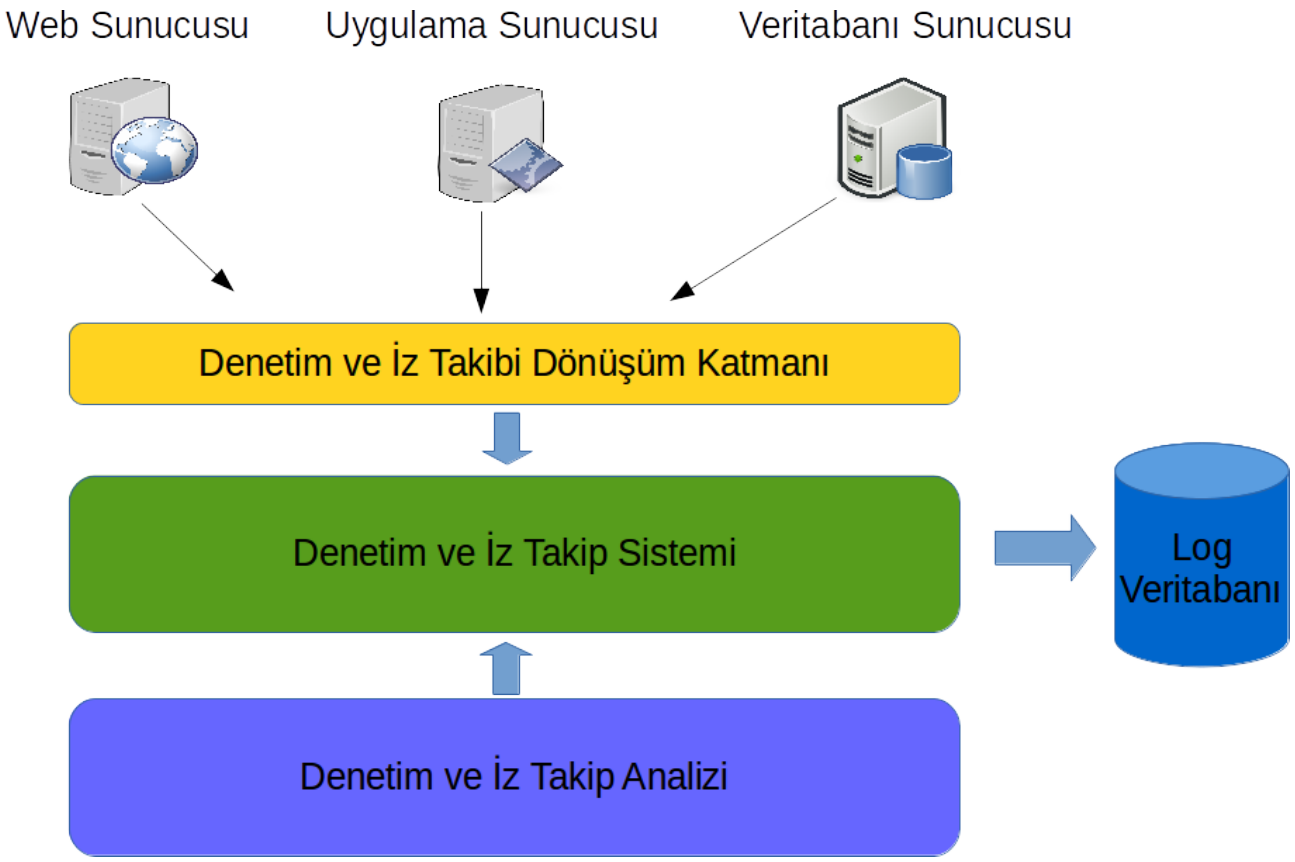
İz kayıtlarının erişimi de oldukça sıkı denetlenmelidir. İlgisiz kullanıma izin verilmemelidir. İz kayıtlarını inceleyen admin kullanıcıların dahi iz kayıtlarına erişimleri de ayrıca kayıt altına alınmalıdır.

İz kayıtlarının veritabanında kriptolu biçimde tutulması da gerekebilir. Böylece ilgisiz veya kötü niyetli kimselerin eline geçmesi durumunda bu kriptolu içeriğin de kırılması gerekecektir.

Farklı sistemlerden anlık olarak denetim ve iz sürme kayıtları üretilebilir. Bu sistemler ve merkezi denetim ve iz sürme sistemi arasında zaman senkronizasyonu da önemlidir.

Denetim ve İz Kayıtlarının Analizi

Üretilen denetim ve iz kayıtlarının geriye dönük olarak farklı kriterler ile incelenebilmesi ve yapılan işlemlerle ilgili kullanıcılara istatistiki bilgi sunması da önemlidir. Böyle bir analiz mekanizmasında belirli kriterlere göre filtreleme, sıralama, arama gibi özelliklerin yanı sıra, işlemlerle ilgili averaj değerleri veya işlenen veri miktarını, işlem sayısını sunan istatistik kabiliyetleri, farklı iz kayıtları arasındaki ilişkileri gösteren analiz kabiliyetleri de mevcut olmalıdır.

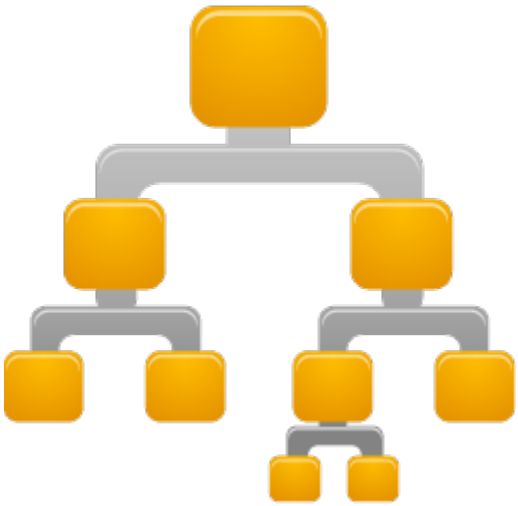


Denetim ve iz takip katmanı farklı noktalardan gelen log mesajlarının denetim ve iz takip sistemine aktarılmasını sağlar. Bunun için farklı sistemlere özgü ajan veya adaptörlerin geliştirilmesi söz konusu olabilir. Denetim ve iz takip sistemi, log mesajlarının toplanmasından, bu mesajların ortak bir yapıya dönüştürülmesinden ve normalizasyonundan, mesajların sıkıştırılarak uygun biçimde saklanmasından ve arşivlenmesinden sorumlu katmandır. Log mesajları güvenlik nedeni ile ayrı bir log veritabanında saklanmalıdır. Denetim ve iz takip analiz katmanı ise toplanan logların farklı kriterlerle aranması, incelenmesi ve analiz edilmesi ile ilgili fonksiyonlar sunabilir.

Kurumsal Organizasyon Hiyerarşisinin Yönetilmesi

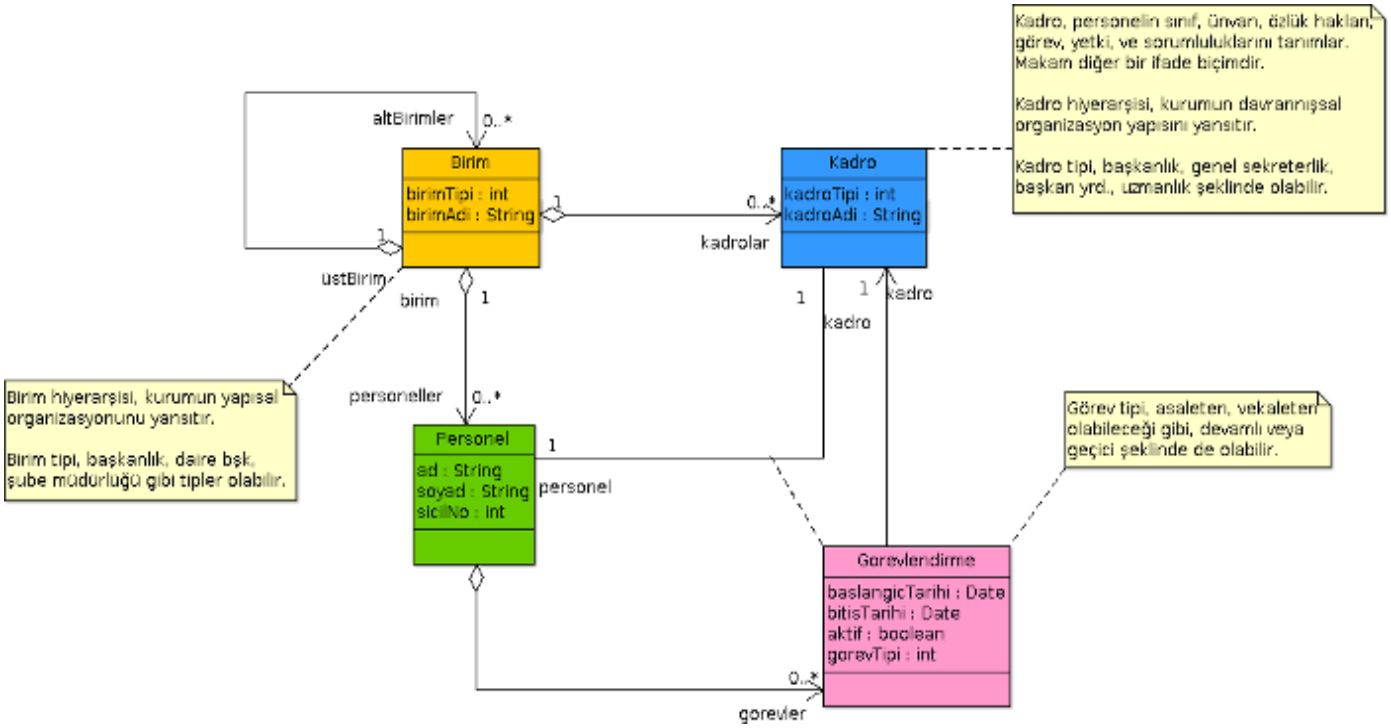
Kurumsal uygulamaların pek çoğunda kurumun sahip olduğu organizasyon hiyerarşisi önemli bir rol oynamaktadır. Kullanıcıların kurum içerisindeki uygulamalara erişmelerine, hangi veriye ne yetkilerle erişebileceklerine, hangi yetki ve sorumluluklara sahip olduklarına genellikle organizasyon hiyerarşisinde bulundukları konuma göre karar verilir.

Kurumun organizasyon yapısı en tepe birim en üstte, en alt birimler ise en altta olacak biçimde ters dönmüş bir ağacın dallarına benzetilir. Genellikle her birim, en üst birim haricinde, başka bir üst birime bağlıdır. En üst birime kök birim adı verilir. En alttaki birimlerin ise kendilerine bağlı alt birimleri olmadığı için bunlara da uç birimler adı verilir.

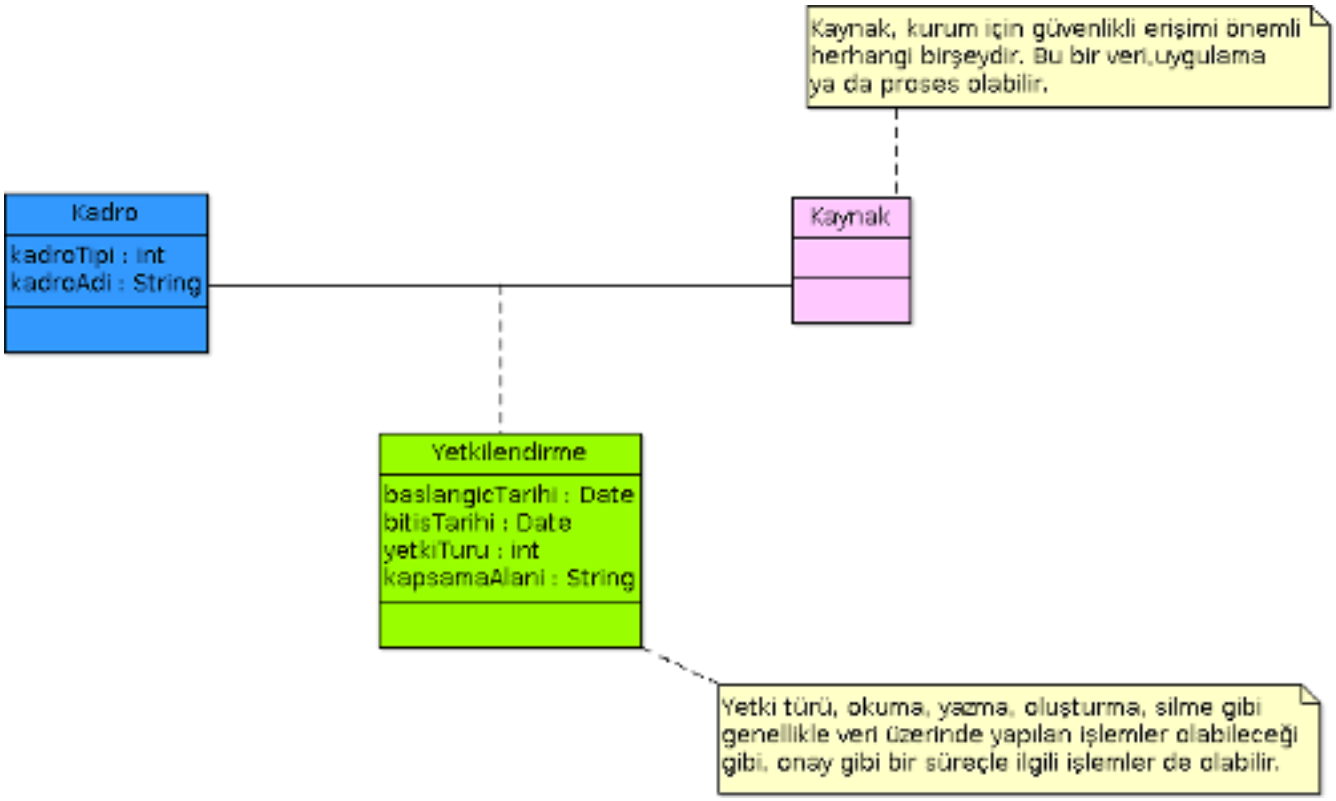


Kurum personelinin her biri organizasyon hiyerarşisindeki herhangi bir birimin altında yer alırlar. Kurum içerisindeki personelin görev, yetki ve sorumluluklarına göre sahip oldukları statü genellikle makam veya kadro olarak ifade edilir. Kadro/makam personelin sınıf, ünvan, görev, özlük hakları, yetki ve sorumluluklarını tanımlayan temel bir yapıdır. Organizasyon hiyerarşisindeki her birime tahsis edilmiş kadro veya kadrolar mevcuttur. Kadrolar arasında da ast üst ilişkisi olabilir. Herhangi bir kadro başka bir kadroya bağlı olabilir. Bağlı bulunduğu kadronun mutlaka kendi bağlı bulunduğu birime ait olması da şart değildir. Personel bu kadrolardan herhangi birisine yerleştirilir.

Personelin kadroya yerleştirilmesine veya atanmasına görevlendirme adı verilir. Görevlendirmeler belirli bir zaman aralığı için veya süresiz olabilir. Ayrıca bazı personeller atandıkları kadronun dışında başka kadrolara ait görev ve sorumlulukları da icra edebilirler. Bu nedenle görevlendirmeler asaleten veya vekaleten yapılabilir.

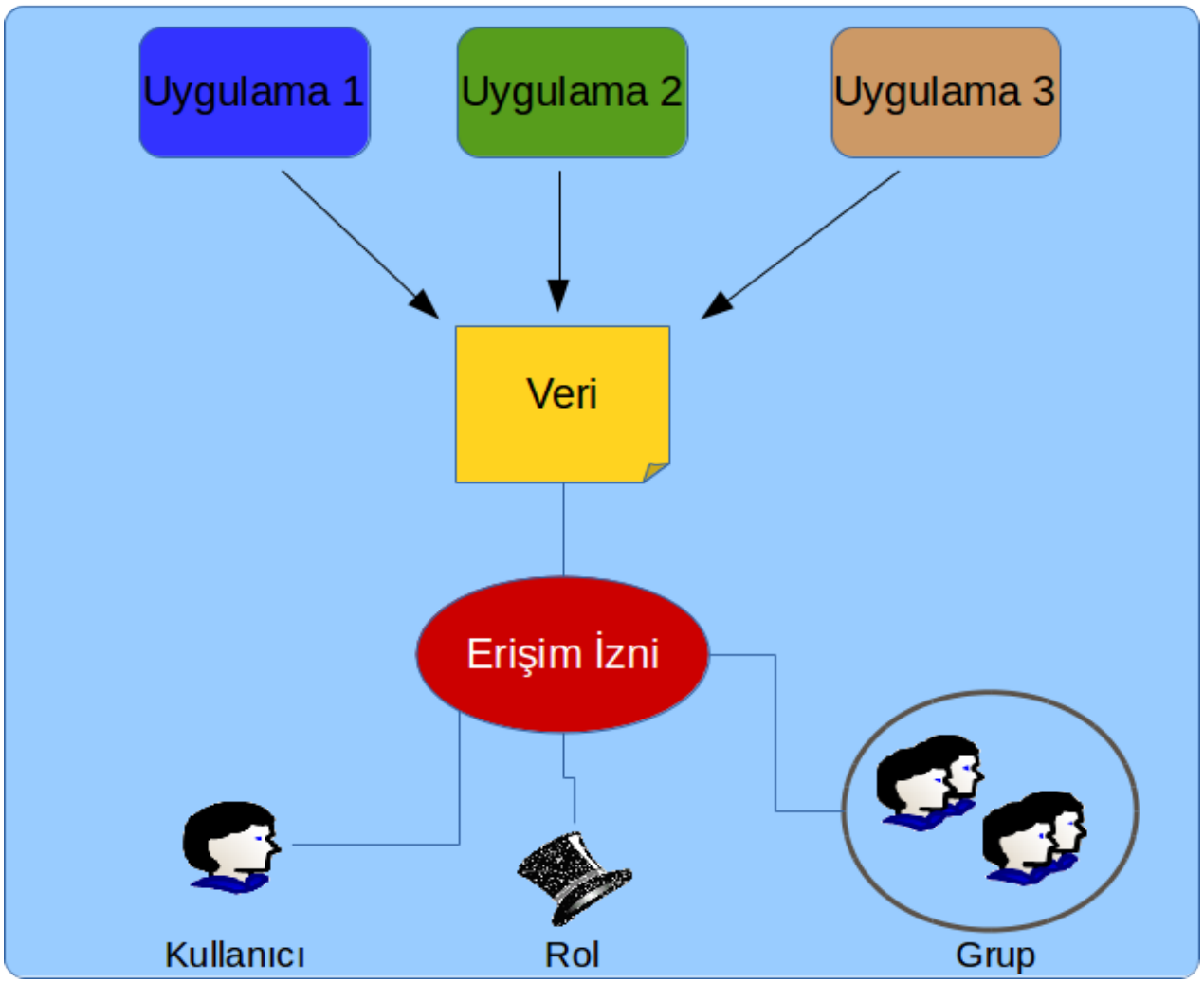


Kurum için güvenli erişim gerektiren herhangi bir kaynak üzerinde işlem yapma yetkisi ilgili kadrolara verilir. Kaynak genellikle veri olur. Ancak veri dışında kurum içindeki herhangi bir servis, proses veya uygulama da kaynak olarak ele alınabilir. Yetkilendirmenin süresi, ve kapsama alanı olabilir. Kapsama alanı, kurum içerisindeki uygulamalar veya domain olabilir.


Kaynak, kurum için güvenlikli erişimi önemli herhangi birşeydir. Bu bir veri,uygulama ya da proses olabilir.
Kadro
kadroTipi : int
kadroAdi : String
Kaynak
Yetkilendirme
baslangicTarihi : Date
bitisTarihi : Date
yetkiTuru : int
kapsamaAlani : String
Yetki türü, okuma, yazma, oluşturma, silme gibi genellikle veri üzerinde yapılan işlemler olabileceği gibi, onay gibi bir süreçle ilgili işlemler de olabilir.

Kurumsal Verinin Güvenliği

Kurumsal mimari de kurumun sahip olduğu verinin güvenli biçimde yönetilmesi hayati öneme sahiptir. Pek çok organizasyon için kurumsal mimari de odak noktası veridir. Kurumun sahip olduğu değişik uygulamalar ortak bir veri katmanı üzerinden kabiliyetlerini sunarlar. Farklı uygulamalar ortak veri setleri üzerinde işlem yapabilirler. Bu verinin gizliliği, tutarlı biçimde değiştirilmesi ve sürekli olarak erişilebilir kılınması için uygulamalardan bağımsız biçimde veriyi odak noktasına alan bir güvenlik mimarisine ihtiyaç vardır.



Kurumsal veri bir uygulama tarafından üretildikten sonra diğer pek çok uygulama tarafından kullanılabilir. Verinin uygulamalar arasında paylaşılması söz konusu olacaktır. Dolayısı ile veri düzeyinde hangi kullanıcıların ne türde yetkilere sahip olduğu bilgisinin de tek bir noktadan yönetilmesi yetkilendirme politikalarının ve veri üzerindeki yetkilendirme işlemlerinin kurumun sahip olduğu uygulamalar arasında paylaşılmasının sağlar. Bu nedenle veri üzerinde yapılan yetki tanımlarının uygulamalar arasında tekrarının önüne geçilmiş olunur.

Kurumsal uygulamalarda genellikle, kullanıcılara atanan yetkilerin sadece belirli bir koruma alanı kapsamında aktif ve geçerli kılınması söz konusudur. Atanan yetkilerin geçerli olduğu kapsama alanları genellikle kurum düzeyinde uygulamalar, uygulama içerisinde ise modüller veya kod blokları şeklinde ifade edilebilir. Ya da dokümanların hiyerarşik bir yapıda, hizmete özel, gizli, çok gizli gibi sınıflandırılması söz konusu olabilir. Çalışma zamanında erişim gerçekleştiği anda kullanıcının talep ettiği işlemi yürüten thread'in ilişkilendirildiği bir koruma alanı bilgisi söz konusudur. Bu bilgi çerçevesinde belirtilen işlemin yapılıp yapılamayacağına karar verilebilir. Ya da benzer biçimde erişilen dokümanın sınıflandırma bilgisi ile o andaki aktif kullanıcıya atanmış hangi sınıftan dokümanlara erişebileceğini tanımlayan bilgi karşılaştırılabilir.

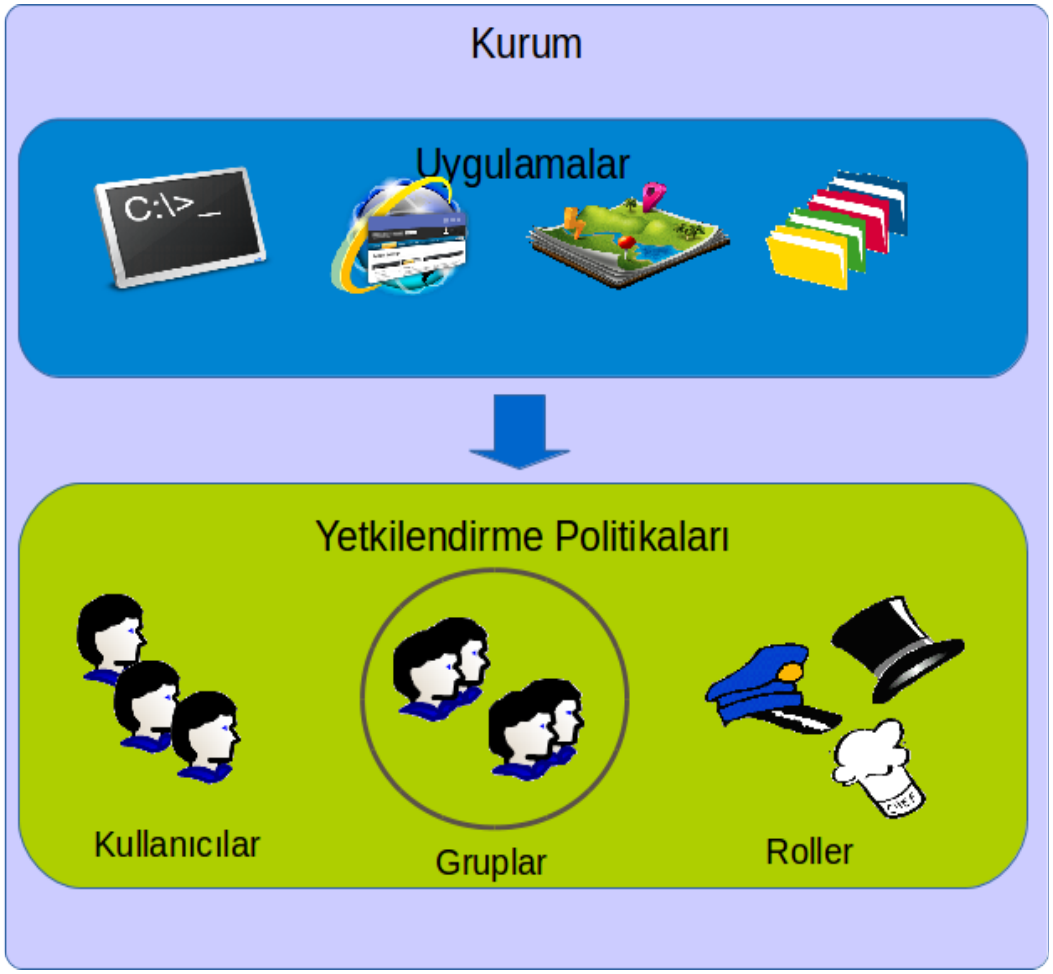
Nesne (OID)	Özne (SID)	İzin	Etki Alanı
Doküman:101	user1	R	app1
Doküman:555	user1	R,W	app2,app3
Doküman:101	user2	D,R,W	app1,app2,app3

Yukarıdaki örnekte 101 id'li Doküman nesnesi üzerinde user1'e okuma (R) yetkisi verilmiştir. Ancak bu yetki sadece app1 isimli uygulama için geçerlidir. Kullanıcı Doküman:101'e sadece app1

uygulaması üzerinden erişebilecektir. Aynı dokümana user2 kullanıcısı ise app1, app2 ve app3 uygulamalarından erişebilecek şekilde yetkilendirilmiştir. User2'nin Doküman:101 üzerinde okuma dışında silme (D) ve güncelleme (W) yetkileri de mevcuttur.

Kapsama alanının kurum içerisindeki uygulamalar ve uygulamaların içindeki modüller düzeyinde ele alınması durumunda kapsama alanı bilgisini ifade etmek için DNS'den yararlanılabilir. Örneğin, yetki tanımında kapsama alanı harezmi.com.tr olarak tanımlandığında bu kapsama alanı Harezmi genelinde bütün uygulamalar için geçerli bir yetki tanımı anlamına gelebilir. Benzer biçimde app1.harezmi.com.tr, app2.harezmi.com.tr şeklinde bir kapsama alanı bilgisi ise yetkinin sadece harezmi.com.tr alanındaki app1 ve app2 uygulamaları için geçerli olduğu anlaşılır. Uygulamanın altında ise modul1.app1.harezmi.com.tr, modul2.app1.harezmi.com.tr alan adından ise yetkilendirmenin sadece app1 için ve bu uygulamanın içinde de sadece modul1 ve modul2 için verildiği anlaşılır. Birden fazla müşterinin olduğu durumlarda, eğer kullanıcı o an için spesifik bir müşterinin dokümanına erişebiliyor ise, bu durumda o müşterinin rakibi olan diğer bir müşterinin dokümanına erişimi de engellenebilir.

Kurumsal güvenlik mimarisi ile ortaya konan kullanıcı, grup ve rol bilgilerinin uygulama ve iş katmanlarından bağımsız biçimde tanımlanabilmeleri ve yönetilebilmeleri gerekir. Kurumsal güvenlik mimarisinin kullanıcı ve yetki yönetim tarafında yetkilendirme politikalarının kurum genelinde geçerli olacak biçimde düzenlenmesi faydalı olacaktır.


Kurum
Uygulamalar
C:\>_
Yetkilendirme Politikaları
Kullanıcılar
Gruplar
Roller

Referanslarımız