**Erişim Denetin Modelleri**

•Rol Tabanlı Erişim Denetimi

•Öznitelik Tabanlı Erişim Denetimi

•İçerik Tabanlı Erişim Denetimi

•Zaman Tabanlı Erişim Denetimi

•Konum Tabanlı Erişim Denetimi

•Amaç Tabanlı Erişim Denetimi

•Yaratıcı Kontrollü Erişim Denetimi

**Rol Tabanlı Erişim Denetimi - Role-Based Access Control(RBAC)**

Yetkilendirme yönetimi maliyetlerinin düşürülmesini amaçlamaktadır. Klasik erişim denetimlerinde yetkilendirme sayısı yüksek olmaktadır.

-Örneğin 1000 kullanıcı, 100.000 nesne ve 10 erişim hakkı olan bir sistemde 10.9 olası yetkilendirme

Rol kavramı kullanılarak kullanıcılar ve izinler arasında aracı olarak davranmaktadır. İzinler kullanıcılar yerine rollere atanmaktadır. Haliyle az sayıda ki roller sayesinde denetim kolaylaşacaktır.

RBAC Terimleri : -**U Kullanıcı (user) kümesi, -P İzinler (permission) kümesi, -R Roller(roles) kümesi**

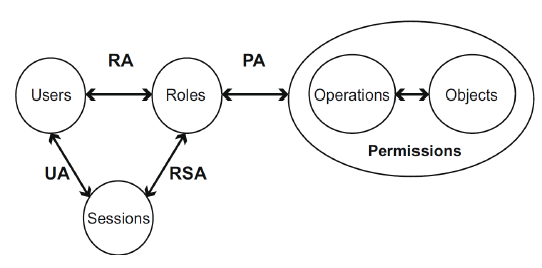
Kullanıcı: Bölüm Başkanı, Profesrö, Öğrenci gibi  
İzin: Genellikle nesne-eylem çöifti olarak kabul edilir.  
Örnek: İlişkisel sql: -Nesne İlişkiler ve veritabanı nesneleri, -Eylemler : sql komutları (select…)

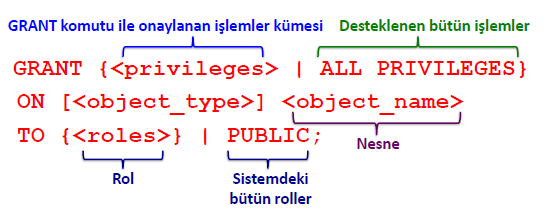
**Rol:** kullanıcılar, roller ile ilişkilidir. Kullanıcı-rol ataması için **UA ilişkisi kullanılır (u,r)**

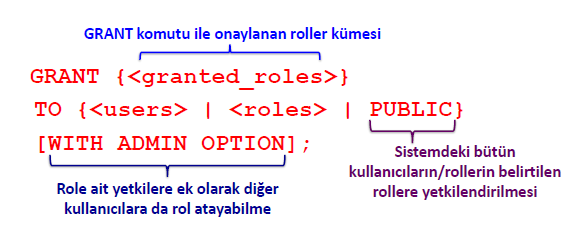
İzinler rollere atanır ve rollerden geri alınır **–PA:** hangi iznin hangi role atandığını belirtir.

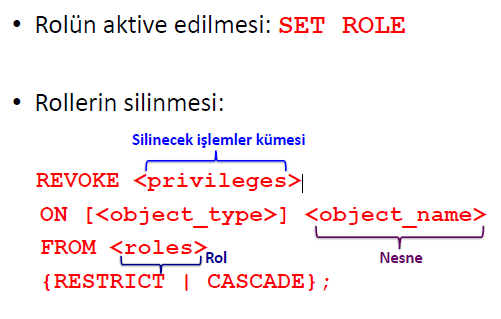
\***RBAC, role hiyerarşisi kavramını kullanarak yönetimsel masrafları düşürmektedir. Üst seviyedeki direk alttakilerin hakkına sahiptir.**

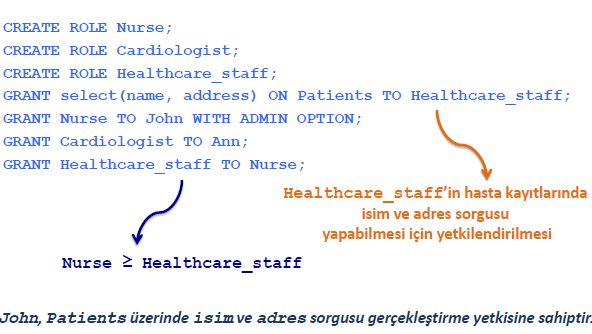
**Böylece, kıdeli rollere atanması gereken izin sayısı azalır, yönetimsel yükler azalır. Ama kullanılan algoritmanın yükü artar. Alttakileri de kontrol etmek için**

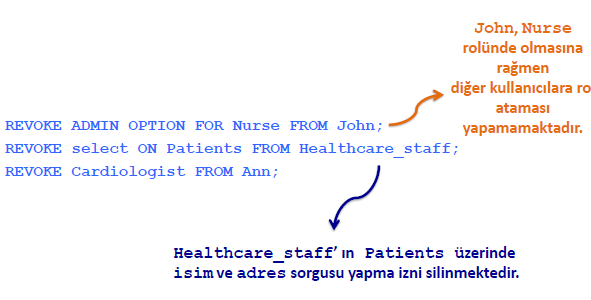
****

****

****

****

****

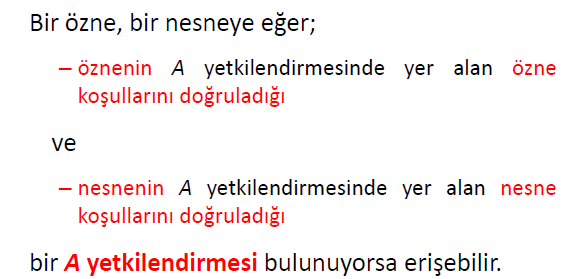
****

**Öznitelik Tabanlı Erişim Denetimi** – Attribute-Based Access Control (ABAC)

–Öznelerinvenesnelerinözniteliklerkümesiiletanımlanması,

–Öznelerinvenesneleringüvenlikileilgiliözelliklerininkodlanması,

–Yetkilendirmedekiöznelerinvenesnelerinözniteliklerinkoşullarıileifadeedilmesidir.



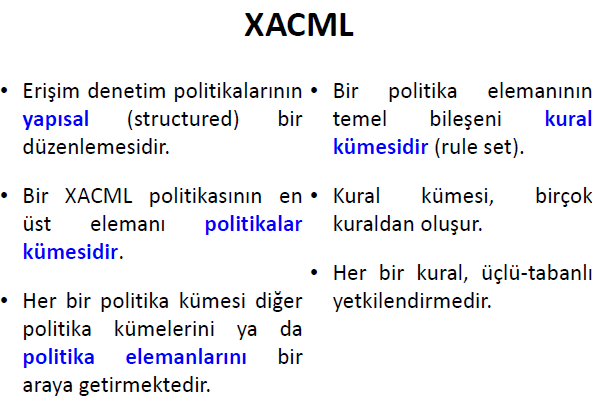
Örneğin yetişkinlere yönenlik mpeg filmler sadece 18 ve 18 yaşından büyük olan kşiler tarafından indirilebilir.

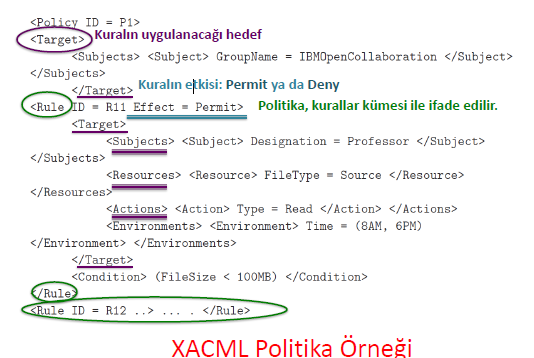
Herhangi bir kullanıcı kimliği doğrulama işlemi yok, sadece yaşı 18 ve daha büyük kullanıcılar koşulu doğrulamaktadır.

Özneleri ve korunan nesneleri tanımlayan **özniteliklerin kullanımını** temel almaktadır.  
Kurumsal güvenlik politikalarından **yetkilendirmelerin elde edilmesini** kolaylaştırmaktadır.  
-İçeriden gelebilecek tehditlere yönelik korunmayı sağlayacak  **yetkilendirmeyi kolaylaştırmaktadır.**

**\*XACML (eXtensible Access Control Markup Language)  
Genişleyebilen, XML olarak kodlanmıştır, politikaların, erişim isteklerinin ve erişim denetim kararlarının tanımlandığı bir dil. <Kaynak, özne, Eylem>**

Farklı kurum etki alanları arasında **işbirliği verisinin paylaşım ihtiyacı** sonucunda geliştirilmiştir.



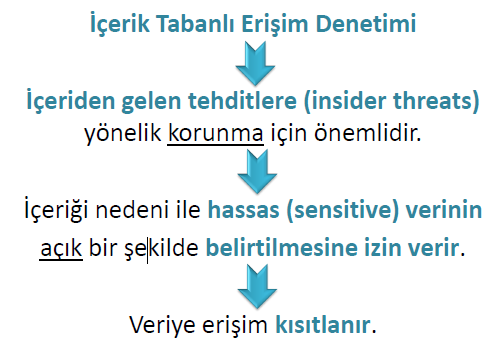


**İstek: öznenin, kaynağın, eylemin ve çevrenin ilişkili olduğu öznitelikleri** içerir.

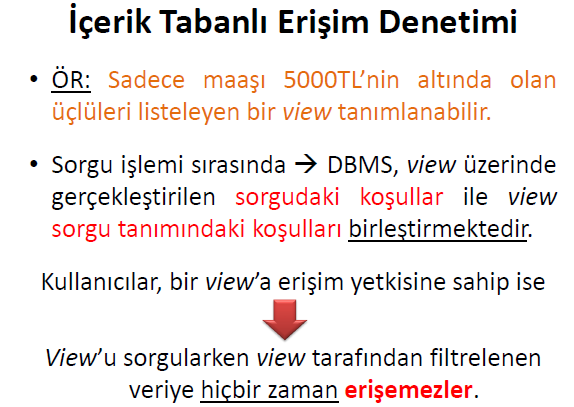
**Yanıt: 4 karardan birini içerir. İzin, Red, Uygulanamaz, Belirsiz.**

**İçerik Tabanlı Erişim Denetimi**

Korunan veri nesnelerine erişim, nesnelerin içeriklerini temel almaktadır. Örneğin maaş verisi 5000 tl ve üzerinde olan verilere sadece insan kaynakları yönetici tarafından erişilebilsin gibi..

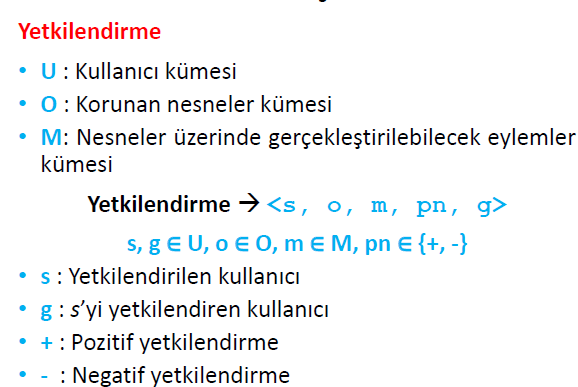


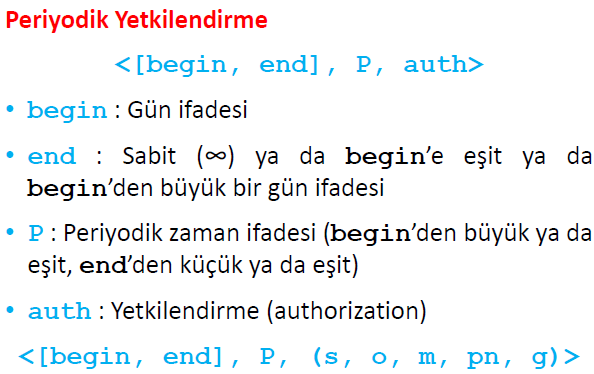
İlişkisel veritabanında verinin içeriği değiştiğinde eğer verinin yeni versiyonları erişim denetim politikasının koşularını sağlıyorsa sistem politikayı otomatik olarak uygular.

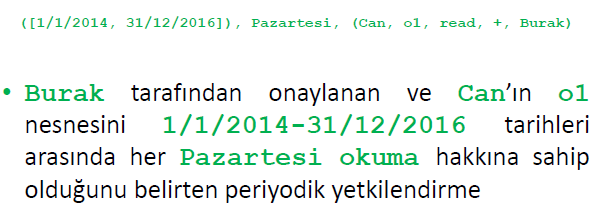


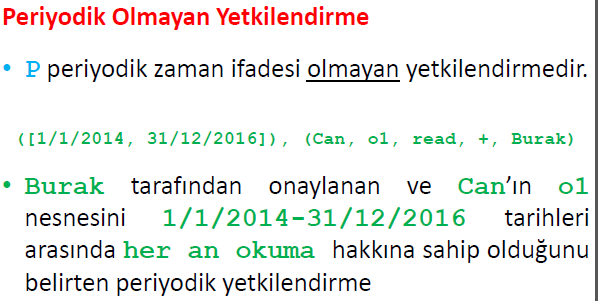
**Zaman Tabanlı Erişim Denetimi**

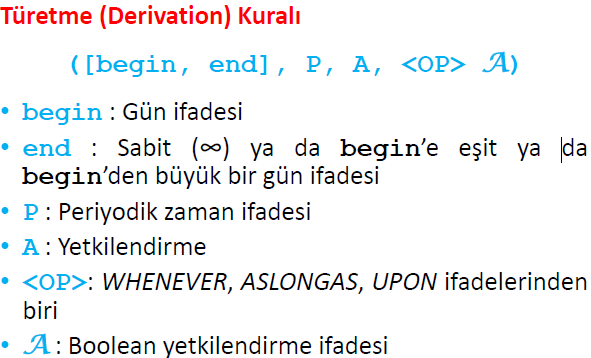
Erişim denetim düzeneğindeki en önemli ihtiyaçlardan biri korunmada izinlerin zaman boyutudur. Kullanıcılar verilen yetkilendirmeler, kullanıcıların kurum içersindeki etkinliklerine bağlı olmaldıır.

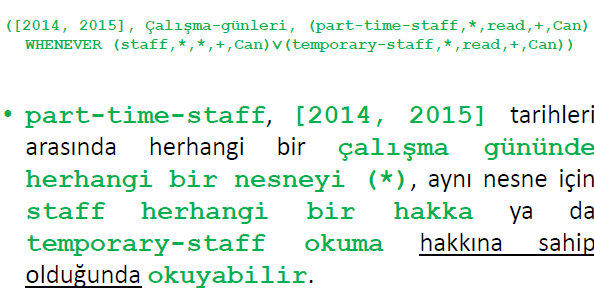


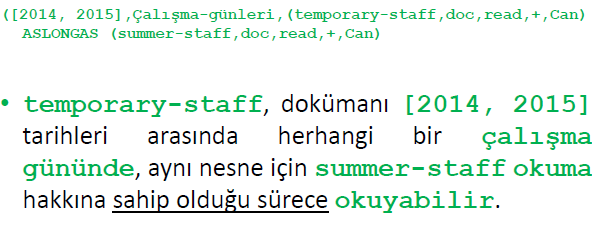


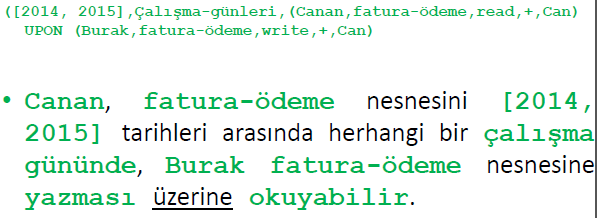








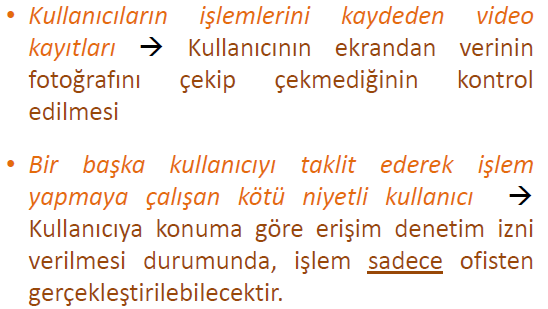




RBAC modeline zaman boyutunun uygulanması ile **Temporal RBAC** – TRBAC modeli geliştirilmiş. Rollere atanan izinler, belirli zaman periyodları için geçerlidir.

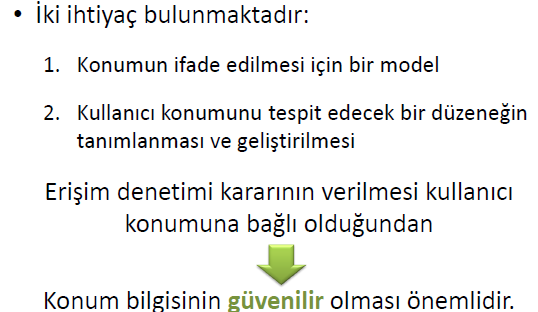
**Konum Tabanlı erişim Denetimi**

Verinin güvenli kullanımı için konum önemli bir boyuttur. Kurumlar hassas veriye sadece kurum içinden ulaşılmasını istemektedir.



Konum tabanlı erişim denetimi-> Yetkilendirmeler, erişimin onaylanacağı konumu belirten ek parametre içermektedir.

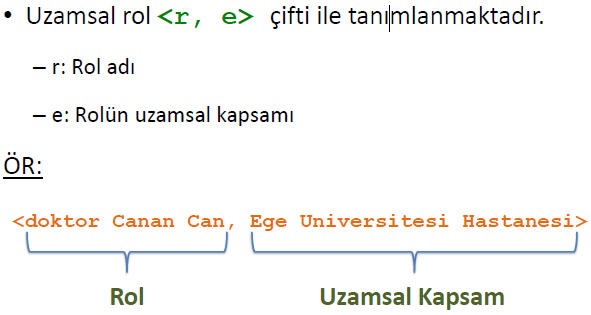
Yetkilendirme, kullanıcı yetkilendirmede belirtilen konumda bulunmadığı sürece aktif değildir.



**GEO-RBAC ->** Konumun ifade edilmesi için bir modeldir. Model uzamsal rol(spatial role) kavramını temel almaktadır.

**Uzamsal kaplam/kapsam(spatial extent)**

Rolüntanımlandığısınır(yol,şehir,kurum,vs.)  
Kullanıcının,rolünükullanabilmesiiçinkonumlanabileceğibölge

****

**Geo-RBAC ->** Genel politikaların tanımlanabilmesi için **rol şeması** kavramını sağlamaktadır.

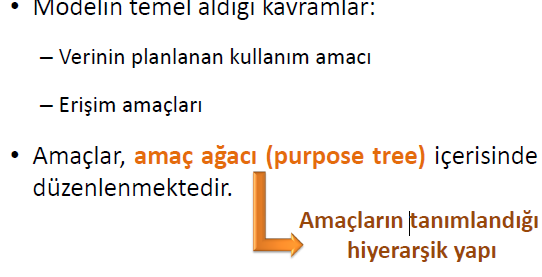
Bir hastane ile ilişkilendirilmiş bir doktor, hastanede olduğu zaman tıbbi veriler üzerinde yetkilendirmeye sahiptir. <Doktor, Hastane>

**Near Filed Communication (NFC) ->** Kullanıcı konumunu tespit edecek bir düzeneğin tanımlanmasına ve geliştirilmesine yönelik bir modeldir.

**Amaç Tabanlı Erişim Denetimi**

Mahremiyet-hassas verinin korunması için verinin kullanım amacını belirten erişim denetim politikları önem kazanmaktadır.

Politikalar, **kişisel verinin toplanmasındaki amacı** belirtmelidir. Belirtilen amacın dışındaki kullanımlar **anomali** olarak işaretlenir ve ek kontroller tetiklenir.



**Yaratıcı Kontrollü Erişim Denetimi**

ORiGinator CONtrolled Acces Control (ORGCON/ORCON) Özne diğer özneye, sadece nesnenin yaratıcının izni ile nesneye erişim için haklar vermektedir.

AvrupaBirliğiKomisyonusekreterihazırladığıdokümanlarıyorumlamalarıiçinyardımcılarınagönderir.

•Yardımcılardokümanısekreterinizniolmadandağıtamaz.

•Sekreter,dağıtımıkontroletmektedir.

•ORCON,erişimdenetimindağıtılmış(decentralized)birsistemidir.

•Heryaratıcı,veriyekiminihtiyacıolduğunubelirler.

•Veriyeerişimimerkezikurallarkümesidenetlemez.

•Erişimtamamenyaratıcınınkontrolündedir.