



Elektronik Bilgi Hizmetleri ve Erişim Yönetimi

Yaşar Tonta

H.Ü. Kütüphanecilik Bölümü

tonta@hacettepe.edu.tr

<http://yunus.hacettepe.edu.tr/~tonta/tonta.html>

Erişim Yönetimi Sorunu

- Dijital kütüphaneler, e-yayınlar, güvenlik, gizlilik, ticari sırlar, tıbbi kayıtlar vs.
- Kütüphane elektronik kaynak için lisans anlaşması yapıyor
- Lisans kullanıcılara bu kaynağı (e-dergi, veri tabanı vs.) kullanım hakkı sağlıyor
- Kullanıcı sunucu üzerindeki kaynağa tarayıcı (browser) ile erişiyor
- Sunucu kullanıcının erişim hakkı olup olmadığını kontrol ediyor
- Daha karmaşık senaryolar da olabilir
 - Birden fazla web sunucusu - farklı yayınevlerinin birden fazla kaynağı
 - Birden fazla üniversiteye mensup öğrencilerin bir üniversiteden aldıkları derse ait e-rezerv kaynakları
 - Kullanım sıklığı ve kullanıcı gereksinimlerine göre bazı kaynakların CD ağı aracılığıyla erişilebilmesi vs.

Erişim Yönetimi

- ➡ Kolay olmalı
- ➡ Alt yapının bir parçası olmalı
- ➡ Kaynak ekleme/değiřtirmeye engel olmamalı
- ➡ Kullanıcı grubunu tanımlamak da zor (ziyaretçi öğretim üyeleri, uzaktan kullanım, vs.)
- ➡ Ama sorun iki bilgisayar arasında: Ev sahibi bilgisayar kaynađa erişmek isteyen bilgisayarın tanımlanan kullanıcı grubuna dahil olup olmadığına nasıl karar verecek?
- ➡ Kullanım hakları belirlendikten sonra bu haklar nasıl gözetilecek?



Belli Başlı Sorunlar

- ➔ Erişim yönetimi programının yazılması ve yaşatılması
- ➔ Tarayıcı ve web sunucusu uyumluluğu
- ➔ Erişim kısıtlamalarının yönetimi ve yaşatımı
- ➔ Erişim kısıtlamalarının etkinliği
- ➔ Kullanıcı arabiriminin kullanım kolaylığı
- ➔ Gizlilik

Kullanıcı Kodu ve Şifre I

Yönetimsel sorunlar

- Ölçeklenebilirlik (her sunucunun kendi modülü olacak)
- Esneklik (her yeni dizin servisi web sunucusu üzerinde değişiklik yapılmasını gerektiriyor)
- Kullanıcı kodu ve şifrelerin yönetimi zor (kütüphane-yayıncı arasındaki iletişim/eşgüdüm ve güncelleme sorunları)
- Ağ güvenliği (kullanıcı kodu ve şifrelerin korunması)
- SSL yetenekli web sunucularında sertifika yönetimi gerekli

Kullanıcı arabirimi sorunları/Mimari sorun

- Farklı yayınevlerine ait farklı kaynaklara erişim için birden çok kullanıcı kodu ve şifre gerekli (anımsamak zor)
- Farklı kimlikler ve kaynaklar arasında karmaşa yaşanması
- Şifreyi girmek ne zaman güvenli belli değil
- Çıkış zor



Kullanıcı Kodu ve Şifre II



Mimari sınırlılıklar

- Üçüncü parti hizmet sağlayıcılara yer yok
- Herkese açık terminallerden erişim sorunu



Gizlilik

- Kullanıcı kodları ve tüm özellikler web sunucusunda
- Kullanıcı bilgilerinin CGI’lerde yer almasını önleyecek bir mekanizma yok



IP Numaraları

- Elektronik “yer” kullanıcı grubunu tanımlıyor
- Ağ sahipliği sık değişmiyor
- Geçerli ağ numaraları listesini yayıncıya göndermek kullanıcı kodu ve şifre listesini göndermekten daha kolay
- IP no’ları gizli değil
- Basit ve saydam bir yol
- Ama...Kullanıcılar kaynaklara tanımlanan ağ aracılığıyla erişmek zorunda
- Çevirmeli bağlantıların yerini ISS’ler alıyor
- Kablo TV modemleri var
- Uzaktan eğitim öğrencileri var

Simsar (Broker) Modeli I

☞ Yönetimsel sorunlar

- Ölçeklenebilirlik daha gelişmiş
- Esneklik daha gelişmiş
- Kullanıcı kodu ve şifrelerin yönetimi zor (kütüphane-yayıncı arasındaki iletişim/eşgüdüm ve güncelleme sorunları)
- Ağ güvenliği (kullanıcı kodu ve şifrelerin korunması)
- SSL yetenekli web sunucularında sertifika yönetimi gerekli
- Simsar ve müşterileri için de sertifika yönetimi gerekli

☞ Kullanıcı arabirimi sorunları/Mimari sorun

- Farklı yayınevlerine ait farklı kaynaklara erişim için birden çok kullanıcı kodu ve şifre gerekli (anımsamak zor)
- Farklı kimlikler ve kaynaklar arasında karmaşa yaşanması
- Şifreyi girmek ne zaman güvenli belli değil
- Çıkış zor



Simsar (Broker) Modeli II

➔ Mimari sınırlılıklar

- Üçüncü parti hizmet sağlayıcılara yer yok
- Herkese açık terminallerden erişim sorunu

➔ Gizlilik

- Kullanıcı kodları ve tüm özellikler web sunucusunda
- Kullanıcı bilgilerinin CGI’lerde yer almasını önleyecek bir mekanizma yok

Vekil (Proxy) Yaklaşımı I

- Kütüphane bir iç otantikasyon sistemi geliştirir.
- Kaynaklara erişmek isteyen kullanıcılar bu iş için ayrılan özel bir makineye (proxy) yönlendirilir
- Ağa erişme hakkı olup olmadığı doğrulandıktan sonra kaynaklara erişmesine izin verilir
- Yayınevi isteğin sadece kaynaklara erişim hakkı olan bir makineden gelip gelmediğini denetler

Vekil (Proxy) Yaklaşımı II

Artıları

- Otantikasyon kütüphanenin bir iç sorunu
- Şifreleri vekil web sunucusu kontrol ediyor, yayıncı değil
- Vekile erişim için tek kullanıcı kodu yeterli (yayıncıların ortak erişim politikaları varsa)
- Yayınevleri kullanıcı kodu/şifre gibi ayrıntılarla ilgilenmiyor
- Kimin hangi kaynaklara erişeceğine kütüphane karar veriyor
- Ölçeklenebilirlik ve esneklik iyi

Eksileri

- Vekil makine sürekli çalışmalı (kesinti, kapasite sorunları vs.)
- Kurulum yönetimi ve yaşatımı karmaşık ve emek yoğun
- Her kullanıcının tüm dış kaynaklara erişme hakkı olmayabilir
- Vekil için sertifika yönetimi gerekli
- Simsar ve müşterileri için sertifika yönetimi gerekli
- Şifreyi girmek ne zaman güvenli
- Herkese açık terminallerden erişim ve çıkış zor



Elektronik Kimliğe Dayalı Yaklaşım I

- ➔ Kütüphane/kurum her kullanıcıya bir elektronik numara (sertifika) verir
- ➔ Kullanıcı üçüncü parti yayınevının elektronik kaynağa erişmek istediğinde bu numarayı girer
- ➔ Yayıncı kütüphaneye ilişkiye geçerek bu numarayı doğrular (kredi kartlarında olduğu gibi)
- ➔ Doğrulama sisteminde bir hata olursa tüm elektronik kimliklerin yeniden verilmesi gerekir
- ➔ Ölçeklenebilir ve esnek
- ➔ Tek kullanıcı kodu yeterli; herkese açık terminallerden erişim mümkün
- ➔ Vekil sertifika yönetimi gerekli



Elektronik Kimliğe Dayalı Yaklaşım II

➔ Sorunlar

- Elektronik kimliklerin güvenliği yayınevleri - kütüphane arasında bir sorun
- Doğrulama sistemleri için standartlar ve bunu destekleyen hazır yazılımlar yok
- Açık kriptografik sertifika teknolojisine dayanan (X509) hazır yazılımlara yöneliş var
- X509 kişisel bilgisayarlar için daha güvenli (herkese açık bilgisayarlarda IP denetimi yapılabilir)
- Yazılımın tarayıcılarla bütünleştirilmesi (kullanıcılara elektronik kriptografik sertifikaların verilmesi, açık anahtar sertifikalarının doğrulanması, maliyet, vd.)
- Kurulumu zor



Politikayla İlgili Sorunlar: Gizlilik

- Kütüphanenin gizlilik (mahremiyet) politikası (yasal)
- Kullanım bilgilerinin toplanması (teknik)
 - Yayıncıların içeriği kullananlar hakkında bilgi toplaması çok kolay
 - Kimliğe dayalı sistemlerde kullanım bilgisiyle kullanıcı arasında ilişki kurulabilir
 - Lisans anlaşmasında kullanım bilgisinin toplanması, saklanması, kullanımı ve açıklanması ile ilgili hususlar yer almalı
 - Kullanıcı başka hizmetlerden yararlanmak (e-postaya dayalı güncel duyuru hizmeti) için kimliğini açık edebilir



Politikayla İlgili Sorunlar:

Hesap Verme

- ➡ Lisans anlaşmasında kullanım koşulları belirlenir
- ➡ Anlaşma koşullarının sağlanmasından taraflar sorumlu (kaynaklara erişim, kullanıcı eğitimi, vd.)
- ➡ Taraflar arasında işbirliği

Politikayla İlgili Sorunlar: Yönetim Bilgisi

- ➔ Elektronik kaynakları kim kullanıyor?
- ➔ Hangi kaynaklar daha sık kullanılıyor?
- ➔ En çok hangi makaleler indiriliyor?
- ➔ Kullanım bilgilerinin demografik bilgilerle eşleştirilmesi (gizlilik sorunu)
- ➔ Kullanım bilgileri yayıncıda, demografik bilgiler kütüphanede (yayıncı sadece kod-şifre gibi “yalancı isimler”i biliyor)
- ➔ Yayıncı kullanım bilgilerini paylaşmak istemeyebilir



Pratik Kısa Dönem Çözümler

- ➔ Otantikasyon yönetiminin önemi
- ➔ Kimliğe dayalı erişim yönetiminin kurulması için yayıncılara çok iş düşüyor
- ➔ Yayıncılar IP kaynaklı çözümleri yeğliyor
- ➔ Kurumlar bir süre “vekil”e dayalı çözümleri desteklemek durumunda
- ➔ Kurumsal otantikasyon aynı zamanda ağ güvenliğini de artırıyor
- ➔ Bazı kurumlar hem politika hem de teknik alt yapı olarak kurum ağına ve hizmetlerine erişimi yasaklıyor



Ulusal Erişim Yönetimi: ATHENS

The screenshot shows a Netscape browser window titled "Athens access management system - Netscape". The address bar shows "http://www.athens.ac.uk/". The browser's menu bar includes "File", "Edit", "View", "Go", "Communicator", and "Help". Below the menu bar, there are several icons and labels: "Bookmarks", "Location:", "Members", "WebMail", "Connections", "BizJournal", "SmartUpdate", and "Mktplace".

The main content area of the browser displays the Athens access management system website. On the left side, there is a large image of a classical Greek bust with the text "Athens access management system" overlaid. On the right side, there are four menu items, each with a radio button:

- General Information
- Data Service Providers
- List of subscribing Athens sites
- Domain Administrator Registration form

At the bottom of the page, there is a "Login to" section. Below this, there is a horizontal line and the text: "Athens - A nationwide Access Management System (AMS) service : The Athens technology has been developed by NISS, a division of EduServ, to".

The browser's status bar at the bottom shows "Document: Done". The Windows taskbar at the very bottom includes the Start button, several application icons (including "Ath...", "Inbo...", "Expl...", "Micr...", "Athe...", "Micr..."), and the system tray showing the time "15:36".



The screenshot shows a Netscape browser window titled "Athens - General information - Netscape". The address bar contains "http://www.athens.ac.uk/info/". The browser's menu bar includes "File", "Edit", "View", "Go", "Communicator", and "Help". Below the address bar are several toolbars: "Bookmarks", "Location" (with a dropdown menu), and a row of icons for "Members", "WebMail", "Connections", "BizJournal", "SmartUpdate", and "Mktplace". The main content area displays the Athens website with the following text:

Athens

access management service

General information

The Athens service enables access to numerous datasets and information services throughout the UK and overseas. Further datasets and services continue to be added and include a wide range of services both from the academic and publishing communities. The key features of the service include "single password sign-on" to multiple resources and fully distributed management of user accounts. The service is used by all UK HE institutions and an increasing number of users in allied sectors and is supported by the JISC. A brief overview and history of Athens is at [Athens - the only national access management service around?](#)

General

Document: Done

The Windows taskbar at the bottom shows the Start button, several open applications (Athens, Inbo..., Expl..., Micr..., Athe..., Micr...), and the system tray with the date and time "15:38".



ATHENS

- Birleşik Krallık yüksek öğretim kurumlarınca birçok elektronik kaynağa erişmek için kullanılan otantikasyon servisi
- Tek kullanıcı numarası/şifre
- Kullanıcı numaraları/şifreler ve çevrimiçi kaynakların merkezi veri tabanı



Tarihçe

- Birden çok kullanıcı numarası ve şifre gereksinimi
- Kampus dışı kullanıcılar
- Kullanıcıların tek tek tanınması
- Ortak raporlama
- 1994’te ilk sürüm
- Webe dayalı yönetsel servis
- Güvenilir, ölçeklenebilir, esnek, destek hizmeti var

ATHENS Hizmeti

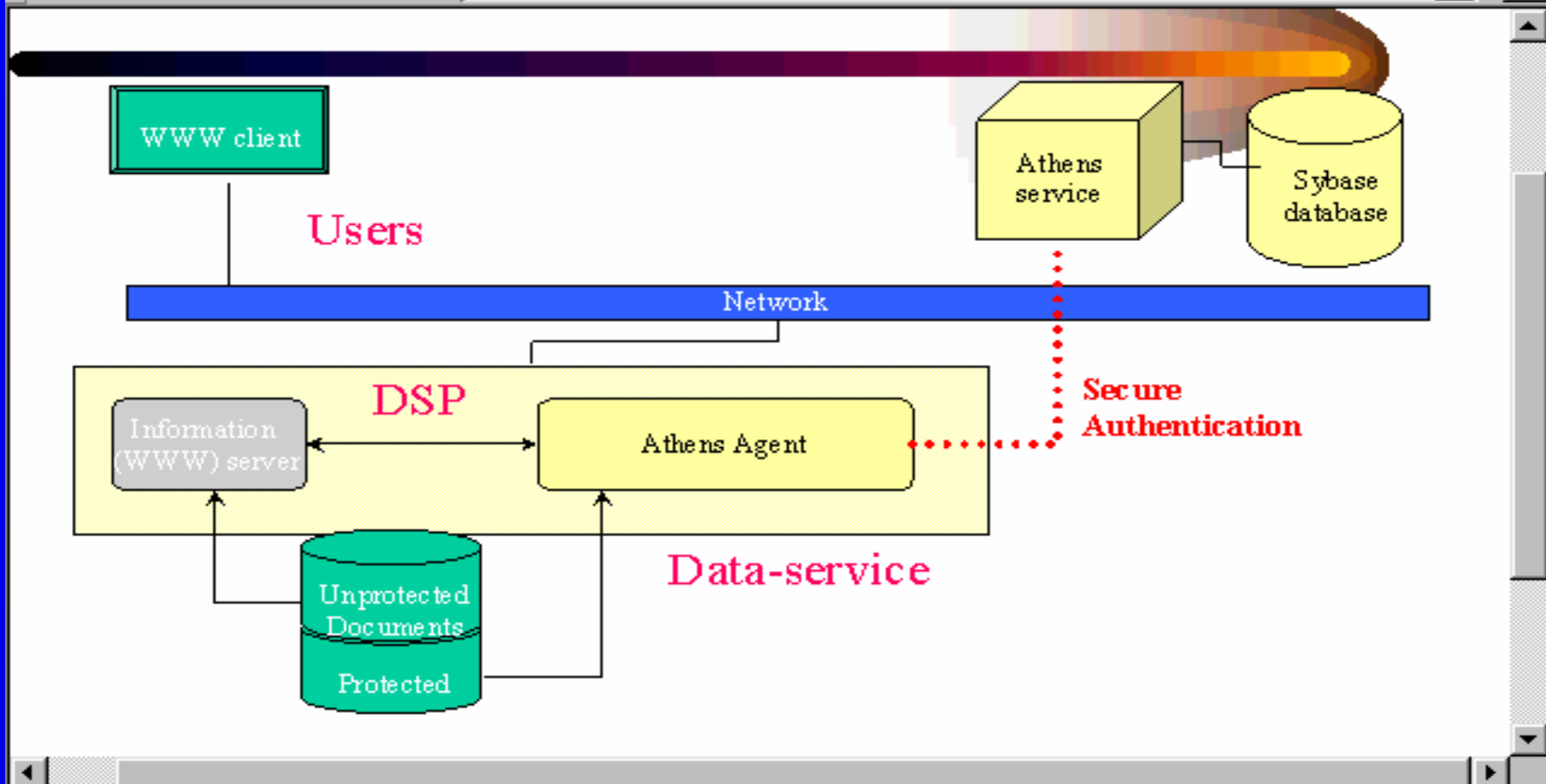
- Çekirdek ATHENS hizmeti
 - Merkezi veri tabanı
 - Hesap sunucuları
 - İstatistik sunucuları
 - Yönetim sunucusu
- Veri hizmeti sağlayıcı firmalar
- Çevrimiçi kaynaklar dermesi (Athens Ajanları)
- Alan adı yöneticileri ve alt yöneticileri
- Son kullanıcılar (750.000 kişi)



PPT Slide - Netscape

File Edit View Go Communicator Help

Bookmarks Location: <http://www.athens.ac.uk/info/candle-ath-nov99/sld006.htm>



Document: Done



Yararları

- Kullanıcılar: Tek kullanıcı numarası/şifre
- Veri hizmeti sağlayıcılar: minimum hesap tutma yükü
- Satıcılar: pazarlama kolaylığı
- Site: Düşük maliyetli merkezi yönetim
- Girişimci / Konsorsiyum:
 - işletme giderlerinin paylaşılması
 - alım gücünün artması



Elektronik Bilgi Hizmetleri ve Erişim Yönetimi

Yaşar Tonta

H.Ü. Kütüphanecilik Bölümü

tonta@hacettepe.edu.tr

<http://yunus.hacettepe.edu.tr/~tonta/tonta.html>