



TÜBİTAK

ULAKBİM

Ulusal Akademik Ağ  
ve Bilgi Merkezi



---

# ULUSAL GRID ÇALIŞTAYI 2005

## Güvenlik ve Sertifika Otoritesi

**Aslı Zengin**

asli@ulakbim.gov.tr

21-22 Eylül ANKARA

---

- Güvenlik Nedir?
- Grid Uygulamalarında Güvenlik
- Çözüm: Sertifika Otoritesi
- EUGridPMA ve Diğer Uluslararası Kurumlar
- TR-GRID Sertifika Otoritesi
  - Sertifika Politikası ve Minimum Koşullar
  - TR-GRID Sertifika Otoritesi Onaylanma Süreci

- Güvenlik ihtiyacı: Artan sanal bilgi paylaşımı ve haberleşme
- Bilgi değerli!
  - Servis sağlayıcıların sorumluluğu
  - Kullanıcıların güveninin sağlanması
- Güvenlik ve kişisel gizlilik dengesinin kurulması

Güvenlik konusunda üç temel kavram:

- Kimlik doğrulama

“Sistemdeki kullanıcı kim?”

- Yetkilendirme

“Kullanıcının yapacağı işe yetkisi var mı?”

- Sorumluluk

“Kullanıcı ne zaman, nerde, ne yaptığından sorumludur”

## Tehlikeler:

- Geniş dağıtık bilgisayar kümeleri - yabancı sitelerden giriş
- Yüklü dağıtık depolama kapasitesi - uygunsuz veri dağıtımı, yetkisiz erişim
- Karmaşık, heterojen ve dinamik bir ortam - güvenlik açıklarının kullanılması
- Geniş bilgisayar ağı, yeni bir altyapı - virüs, solucan tehlikesi

Grid kullanıcıları:

- Geniş ve dinamik kullanıcı kitlesi
  - Farklı sitelerde farklı kullanıcılar
  - Kişisel ve gizli veriler
  - Heterojen yapıda öncelikler

Grid siteleri:

- Heterojen dağılmış kaynaklar
- Sitelere erişim yolları
- Yerel politikalar
- Üyelik

## Sayısal sertifika nedir?

- Sayısal sertifika, ya da sayısal kimlik, günlük hayatta kullanılan ehliyet, pasaport gibi kimlik kartlarının elektronik ortamdaki karşılığıdır.
- Sayısal sertifika kişinin kimliğini ve söz konusu bilgiye veya online hizmete ulaşım hakkını kanıtlamak için geliştirilmiştir.

## Asimetrik Şifreleme Yöntemi

### - Açık anahtar:

Sertifika otoritesi güvenilir bir kaynak olarak, bir kurum ya da kişiyi bir açık anahtar ile eşleştirir. Açık anahtar ise sayısal imzaların doğrulanması için kullanılır.

### - Gizli anahtar:

Gizli anahtar sadece sahibi olan kişi ya da kurum tarafından bilinir ve sayısal imzayı oluşturmak için kullanılır.

## Sayısal sertifika hangi bilgileri içerir?

- Kullanıcıya ait açık anahtar
- Kullanıcının adı
- Sertifikanın son kullanma tarihi
- Sertifika Otoritesinin adı
- Sertifika Otoritesinin seri numarası

## Sayısal sertifikanın özellikleri nelerdir?

- Mesajların şifrelenmesi ve deşifre edilmesindeki güvenlik ve gizliliği sağlar.
- Mesajı gönderenin ve mesajı alanın doğru yerler olduğunu garanti eder.
- İletilen belgelerin tarih ve zamanını doğrular.
- Belge arşivi oluşturulmasını kolaylaştırır.

## Sertifika Otoritesi

- Sertifika otoritesi, sayısal sertifikaların oluşturulması, yönetilmesi, gerektiği durumlarda sertifikaların dünyaya duyurulmasını sağlayan sertifika hizmet sağlayıcısıdır.
- Sertifika otoriteleri, oluşturdukları sertifikaların güvenliğini sağlayarak, gerektiği durumlarda sertifikaları yenilemek ile sorumludur.

## PKI-Public Key Infrastructure (Açık Anahtarlama Yapısı)

- Sertifikaların, anahtar ikililerinin yönetimini sağlayan yazılımsal ve yordamsal bütünlüktür.
- PKI Sertifika Otoritesi tarafından yönetilir.

## PKI'in İşlevleri

- Anahtar ve sertifika üretimi
- Gizli anahtarın korunması
- Belli durumlarda sertifikaların iptal edilmesi
- Anahtar yedeklenmesi ve yeniden elde edebilme
- Anahtar ve sertifika güncelleme
- Sertifika arşivi

## European Policy Management Authority for Grid Authentication in e-Science

- Avrupa'da Grid sağlayıcılarının güvenlik ve sertifika otoritelerini denetleyen uluslararası bir üst kuruldur.
- Grid ortamında kullanıcıların güvenli bir şekilde dağıtık kaynaklara ulaşması için gereken minimum şartları belirler.
- IGTF (International Grid Trust Federation) aracılığıyla diğer kuruluşlardan APGridPMA (Asia-Pacific) ve TAGPMA (America) ile iletişim ve işbirliği içindedir.

- TR-GRID Sertifika Otoritesi (TR-GRID CA)  
Türkiye'deki ulusal Grid uygulamalarında güvenlik altyapısını sağlamaktan sorumludur.

- Ulusal Grid Sertifikasyon Politikası-CP/CPS Belgesi  
(Certification Policy/Certificate Practice Statement) :

<http://www.grid.org.tr/servisler/sertifika/policy>

- CP/CPS belgesi >> EUGridPMA

- Web sayfasından veya e-posta yoluyla sertifika başvurusu:

[http://www.grid.org.tr/servisler/sertifika/cert\\_request](http://www.grid.org.tr/servisler/sertifika/cert_request)  
[ca@grid.org.tr](mailto:ca@grid.org.tr)

- E-posta yoluyla sertifika iptali:

[ca@grid.org.tr](mailto:ca@grid.org.tr)

- Sertifika Otoritesi Kök Sertifikası:

[http://www.grid.org.tr/servisler/sertifika/ca\\_cert](http://www.grid.org.tr/servisler/sertifika/ca_cert)

- Geçerli sertifikalar listesi:

[http://www.grid.org.tr/servisler/sertifika/valid\\_cert](http://www.grid.org.tr/servisler/sertifika/valid_cert)

- Sertifika iptal listesi:

<http://www.grid.org.tr/servisler/sertifika/crl>

- Sertifika Otoritesinin Sorumlulukları
- Kayıt Merkezinin Sorumlulukları
- Sertifika Otoritesi Makinası Güvenlik Ayarları
- Sertifikasyon Politika Belgesi
- Sertifika Otoritesi Gizli Anahtarı:
  - 2048 bit anahtar uzunluğu
  - Geçerlilik süresi < 20 yıl
  - Yedekleme şifresi > 15 karakter
- Sertifika İptali ve Sertifika İptal Listesiyle İlgili Kısıtlamalar
- Sertifika Otoritesi Web Sayfası

- EUGridPMA elektronik haberleşme listesine üyelik
- CP/CPS belgesinin listeye gönderilmesi
- 2 PMA üyesinin başkan tarafından belgeyi incelemek için görevlendirilmesi
- **Belgenin son halinin sıradaki EUGridPMA toplantısında sunulması**
- 2 hafta oylama süreci
- Tüm liste üyelerinin onayının alınması

TEŞEKKÜRLER...