

Kurumsal PKI Uygulamaları



Tolga KILIÇLI
tolga@deepnight.org



Açık Anahtarlı Şifreleme

1.  = 011011010011010
PRE HASH CODE
MESSAGE

2. 011011010011010
PRE HASH CODE +  → Ciphertext A

3.  + Ciphertext A +  → Ciphertext B
SECRET KEY

4.  ←  + DIGITAL
SENDER CERTIFICATE


5.  +  → Ciphertext C
SECRET KEY

1. Ciphertext C +  = 
SECRET KEY

2. Ciphertext B +  = [Ciphertext A + 

3.  ←  + DIGITAL
RECIPIENT CERTIFICATE

4. Ciphertext A +  → 011011010011010
PRE HASH CODE

5.  = 011011010011010
POST HASH CODE

6. 011011010011010
POST HASH CODE = 011011010011010
PRE HASH CODE



Neden PKI?

- "Güvenilir Birim" ihtiyacı
- PKCS kullanan servislerin birbiri ile çalışabilmesi
 - ✓ Protokoller
 - ✓ Anahtar formatları
 - ✓ API'ler



Uygulama Aşamaları

- Karar
 - Durum Analizi
 - “Bilgi Güvenliği Grubu”nun kurulması
 - “Güvenlik Politikası”nın oluşturulması
- Kurulum
 - CA kurulması
 - Sistem içi kullanılan uygulamaların yenilenmesi
- Yönetim
 - Kurum İmza Anahtarının güvenliği
 - Yedekleme
 - Sertifika verilmesi ve CRL yayımlanması



Durum Analizi

- İş Kriterleri
 - E-iş ve güvenli transfer
 - İletişimde “Özel”lik ve “Gerçek”lik
 - Bürokrasi
 - Güvenlik
 - Kullanıcı sorunları
- Uygulama Kriterleri
 - Güvenli iletişim
 - Tek üyelik
 - Fiziksel güvenlik
- Uygulama Mimarisi
 - Güven Modeli
 - Veritabanı



BGG ve Güvenlik Politikası

- BGG'nin Amacı
- Güvenlik Politikası neden gereklidir?
- BGG'nin görevleri neler olmalıdır?

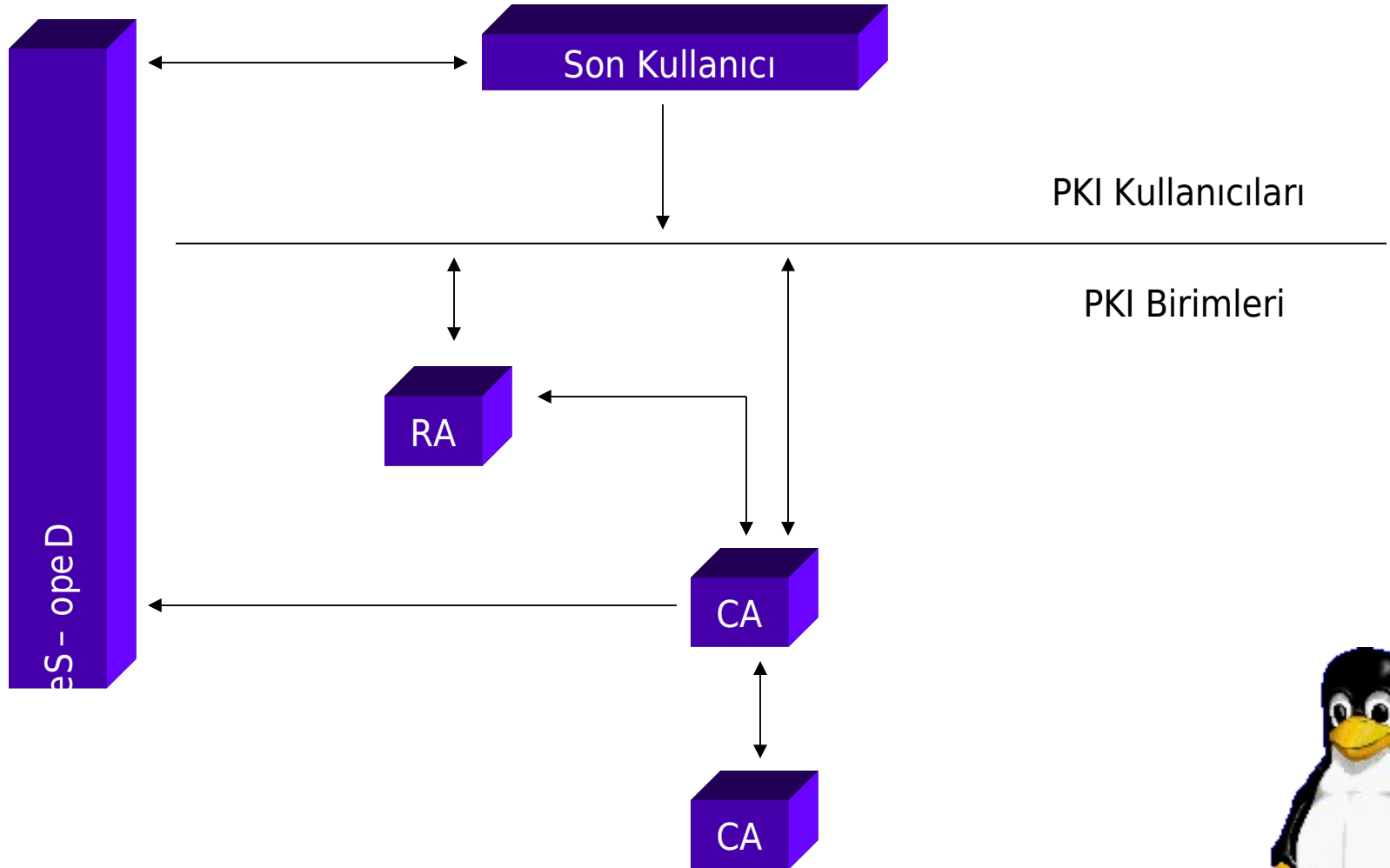


Yönetim

- Kurum İmza Anahtarının Güvenliği
- Yedekleme
- Sertifikasyon ve CRL yayımlanması



PKI Birimleri ve İşleyişi

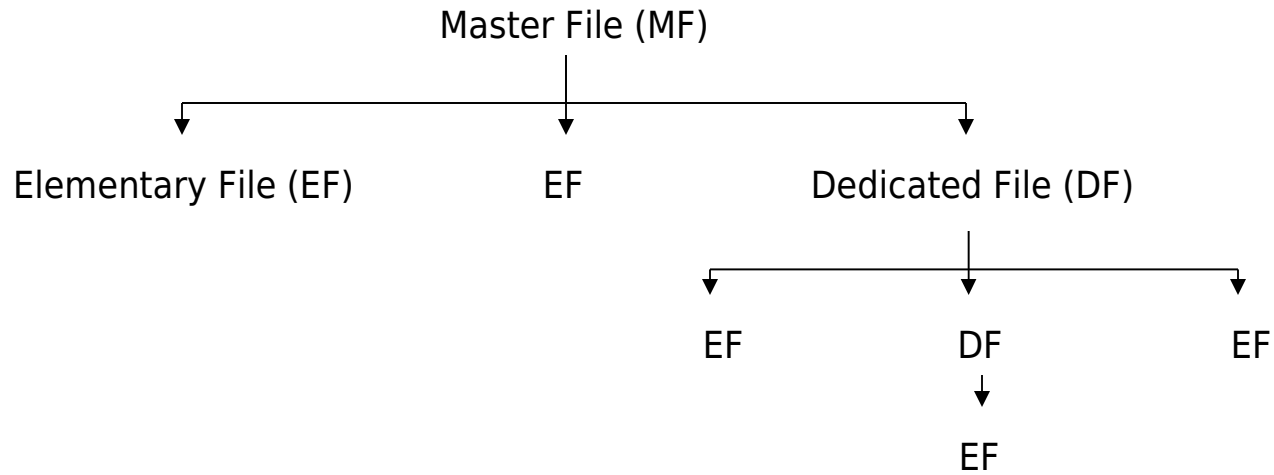


PKI ve Akıllı Kartlar

- Akıllı Kart Nedir?
- Neden Akıllı Kart?
 - Anahtarların güvenli oluşturulması ve saklanması
 - Kullanım kolaylığı
 - Birden fazla uygulamada tek kart kullanılabilmesi



Akıllı Kartların Yapısı



Kurum İçi Uygulamalar

- Kimlik
 - Güvenli elektronik erişim
 - Fiziksel erişim
 - İş-istasyonu güvenliği
 - Kredili sistemler (Boncuk sistemi)
 - E-cüzdan
 - Özel sağlık sigortası
 - Çalışma saatlerinin düzenlenmesi
- ... ve dahası



Özetle ...

PKI + Akıllı Kart =

- Daha az bürokrasi
- Daha az kullanıcı - sistem yöneticisi tartışmaları
- Daha geniş güven ağı
- Diğer kurumlar ile daha kolay işbirliği



