



TÜBİTAK
KAMU SERTİFİKASYON MERKEZİ
EĞİTİM KATALOĞU
(2012)
Sürüm 1.0

Kamu Sertifikasyon Merkezi
TÜBİTAK Yerleşkesi, P.K. 74,
Gebze, 41470 Kocaeli
Tel: (0262) 648 18 18, Faks: (0262) 648 18 00
<http://www.kamusm.gov.tr>
bilgi@kamusm.gov.tr

Kamu SM Eđitimleri

| | |
|----------------------------------------------|---|
| 1. Temel Kriptoloji ve Bilgi Gvenliđi | 3 |
| 2. Aık Anahtar Altyapısı | 4 |
| 3. E-imza Mevzuatı..... | 5 |
| 4. E-imza Veri Formatları | 6 |
| 5. E-imza Kullanıcı Eđitimi..... | 7 |

1. Temel Kriptoloji ve Bilgi Güvenliđi

a. Katılması Gereken Kişiler

Elektronik imza uygulamaları yazacak veya yazdıracak olan kişiler, Kurum ve kuruluşlarda elektronik imza konusunda karar verici yetkili kişiler. Ayrıca ilgi duyan herkes katılabilir.

b. Ön Şartlar

Yok.

c. Ana Konular

- Kriptoloji Nedir
- Elektronik Tehditler ve Güvenlik
- Basit Şifreleme - Güvenli Şifreleme
- Simetrik Kriptografi - Gizli Anahtarlı Sistemler
- Asimetrik Kriptografi - Açık Anahtarlı Sistemler
- E-İmza Nasıl Atılır

d. Eğitimin Süresi

8 saat

e. Eğitim Sonunda Elde Edilecek Birikim

Katılımcılar simetrik-asimetrik algoritmalar ve özet algoritmaları hakkında bilgi sahibi olacaklar ve elektronik ortamda imzalama ve imza doğrulama, şifreleme ve şifre çözme işlemlerinin nasıl yapıldığını öğrenmiş olacaklardır.

2. Açık Anahtar Altyapısı

a. Katılması Gereken Kişiler

Elektronik imza uygulamaları yazacak veya yazdıracak olan kişiler, Kurum ve kuruluşlarda elektronik imza konusunda karar verici yetkili kişiler. Ayrıca ilgi duyan herkes katılabilir.

b. Ön Şartlar

“Temel Kriptoloji ve Bilgi Güvenliği” eğitimi almış olmak.

c. Ana Konular

- AAA Neden Gereklidir
- Açık Anahtar Sertifikaları (Elektronik Sertifika Nedir)
- Sertifika İptal Listeleri (CRL)
- Çevrimiçi Sertifika Durum Protokolü (OCSP)
- AAA Uygulamaları (SSL, Zaman Damgası)

d. Eğitimin Süresi

8 saat

e. Eğitim Sonunda Elde Edilecek Birikim

Katılımcılar Açık Anahtar Altyapısının detaylarını, neden gerekli olduğunu, elektronik sertifika kullanıcıları için neden olmazsa olmaz olduğunu, SSL, Zaman Damgası gibi PKI uygulamalarını öğrenmiş olacaklardır.

3. E-imza Mevzuatı

a. Katılması Gereken Kişiler

Elektronik imzanın hukuki yönüyle ilgilenen tüm e-imza kullanıcıları. Ayrıca ilgi duyan herkes katılabilir.

b. Ön Şartlar

“Temel Kriptoloji ve Bilgi Güvenliği” ve “Açık Anahtar Altyapısı” eğitimlerini almış olmak tercih sebebidir.

c. Ana Konular

- Yasal Altyapı ve Düzenlemeler
 - E-imza Kanunu
 - Tebliğ
 - Yönetmelik
 - Genelgeler
- Nitelikli Elektronik Sertifika Sahiplerinin Yükümlülükleri
- Üçüncü Tarafların Yükümlülükleri
- Mevzuata Göre E-imza Yazılımlarının Sağlaması Gereken Şartlar
- Kamu Sertifikasyon Merkezi

d. Eğitimin Süresi

2 saat

e. Eğitim Sonunda Elde Edilecek Birikim

Katılımcılar e-imzanın hukuki boyutunu öğrenmiş olacaklardır.

4. E-imza Veri Formatları

a. Katılması Gereken Kişiler

Kurumların elektronik imza ile ilgili politikalarını belirleyen kişiler. Ayrıca ilgi duyan herkes katılabilir.

b. Ön Şartlar

“Temel Kriptoloji ve Bilgi Güvenliği” ve “Açık Anahtar Altyapısı” eğitimlerini almış olmak.

c. Ana Konular

- E-imza Veri Formatları
- Birleşik ve Ayrık İmza
- İmzaya Eklenebilecek Bilgiler
- Çoklu İmza
 - Paralel İmza
 - Seri İmza
- İmza Formatı Tipleri
 - Temel Tipler
 - İmza Doğrulama Verilerini İçeren Tipler
 - Arşivleme

d. Eğitimin Süresi

2 saat

e. Eğitim Sonunda Elde Edilecek Birikim

Katılımcılar hangi tip e-imza formatları olduğunu öğreneceklerdir. Bu sayede kendi uygulamalarında hangi formatı kullanmaları gerektiğini belirleyebileceklerdir.

5. E-imza Kullanıcı Eğitimi

a. Katılması Gereken Kişiler

Elektronik imza kullanan kişiler. Ayrıca ilgi duyan herkes katılabilir.

b. Ön Şartlar

Yoktur.

c. Ana Konular

- E-imzanın Detaylı Tanımı ve Önemi
- Elektronik İmza İle Bir Doküman Nasıl İmzalanır?
- Elektronik İmzalı Bir Dokümanın İmzası Nasıl Doğrulunur?
- Akıllı Kartınızın (USB token) İçinde Neler Vardır?
- İmzalama Açık (Public) ve Özel (Private) Anahtar Nedir?
- NES Nedir?
- Elektronik İmza ve NES Arasındaki Fark Nedir?
- Kullanıcılar Tarafından Merak Edilen Diğer Konular

d. Eğitimin Süresi

4 saat

e. Eğitim Sonunda Elde Edilecek Birikim

Katılımcılar e-imzanın ne olduğunu, bir dokümanın elektronik olarak nasıl imzalandığını ve elektronik imzalı bir dokümanın imzasının nasıl doğrulandığını öğreneceklerdir. Ayrıca katılımcılar bu konuda merak ettikleri diğer konularda bilgi edineceklerdir.