



# TÜBİTAK UEKAE Elektronik Sertifika Yönetim Altyapısı



## Masaüstü Güvenlik Modülü

### Kişisel Bilgisayarların Önemi

Günümüzde tüm kurum/kuruluşlar çalışanlarına kişisel bilgisayarlar vermektedir. Kişisel bilgisayarlar hem şahsi işlerin hem de kurum/kuruluşla ilgili işlerin yapılmasında büyük kolaylıklar sağlamaktadır. Bunun sonucu olarak **kişisel bilgisayarlarda çok değerli ve önemli bilgiler saklanmaktadır**. Ne yazık ki bu bilgiler çoğu zaman yetkisiz kişilerin erişimine ve müdahalesine karşı korumasız bırakılmaktadır. Kurum/kuruluşlara özgü rapor, plan ve tasarım gibi çok önemli bilgilerin kötü niyetli kişilerce ele geçirilmesi durumunda ticari kayıplar oluşabilmekte ve bunun yanısıra kurum/kuruluşun güvenilirliği ve marka değeri de zarar görebilmektedir. Bu sebeplerden dolayı kurum/kuruluşların iş istasyonları, masaüstü ve taşınabilir bilgisayarlar için güvenlik çözümlerine kesinlikle ihtiyaç duyduğu görülmektedir.

### Güvenlik İhtiyaçları

Bilgilerin güvenli bir şekilde saklanması ve kullanılması için ESYA Masaüstü Güvenlik Modülü aşağıdaki özellikleri sunmaktadır:

- Önemli bilgi içeren dosya ve dizinleri şifreleme ve imzalama
- Kişisel bilgisayarlarda ve sunucularda saklanan dosyalara ve dizinlere erişimin kontrol edilebilmesi
- Kullanıcıya iş yükü getirilmeden güvenlik hizmetleri sunabilme
- Kolayca kurulabilme ve yönetilebilme
- Üst düzey güvenlik için akıllı kart ve çubuk kullanabilme
- Güvenlik altyapısıyla uyum içinde çalışma

### ESYA Masaüstü Güvenlik Çözümü

ESYA Masaüstü Güvenlik Modülü, Elektronik Sertifika Yönetim Altyapısı'nın diğer bileşenleri olan Sertifikasyon Makamı, Kayıt Makamı, Sertifika Yardımcısı vb. ile tam bir uyum içinde çalışır. Bu sayede kullanıcılara bilgisayarlarındaki tüm bilgileri güvenli bir şekilde saklama ve paylaşma olanağını sunar.

### Getirilen Çözümler

#### Dosya ve Dizin

#### Şifreleme/İmzalama:

Şifreli dosya ve dizinlere sadece yetkisi olan kişiler erişebilir. İmzalı dosya ve dizinlerin kime ait olduğundan emin olunur. Şifreleme ve imzalama için sertifikalar kullanılır.

#### Otomatik ve Şeffaf Çalışma:

İstenen dizinlerin içeriği otomatik olarak, kullanıcı müdahalesi gerekmeden şifrelenir ve imzalanır. İmzalı/şifreli dosyalar otomatik olarak çözülüp çalışma bittiğinde otomatik olarak tekrar şifrelenir/imzalanır.

#### Güvenli Dosya/Dizin Silme:

Silinen dosya ve dizinlerin hiç kimse tarafından geri kazanılamaması sağlanır.

### Sunulan Avantajlar

#### Güvenlik Altyapısına

#### Tam Entegrasyon:

ESYA Açık Anahtar Altyapısı'na tam uyum, sertifika ve anahtar hizmetlerine zahmetsizce erişim.

#### Yüksek Teknoloji:

Güvenliği üst seviyeye çıkarmak için akıllı kart/çubuk kullanımı. Uluslararası güvenlik standartlarına uyumlu milli yazılım.

#### Kullanım Kolaylığı:

Kullanıcı alışkanlıklarını değiştirmeyen yaklaşım. İşletim sistemine tam entegrasyon. Türkçe için tam destek. Kolay anlaşılır arayüz.

## ESYA Masaüstü Güvenlik Modülü Teknik Özellikleri

<b>İşletim Sistemi</b>	Windows 98, Windows NT, Windows 2000 (Bu işletim sistemlerine High Encryption Pack yüklenmiş olmalıdır), Windows XP, Windows 2003
<b>Donanım Gereksinimi</b>	<ul style="list-style-type: none"><li>En az Celeron/Pentium II 500 MHz hızında işlemci</li><li>En az 64 MB RAM</li><li>En az 20 MB boş disk alanı</li></ul>
<b>Desteklenen Standartlar</b>	<ul style="list-style-type: none"><li>X.509 v3 sertifikalar</li><li>X.509 v2 sertifika iptal listeleri (SİL/CRL)</li><li>Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP)</li><li>PKCS7 / CMS dosya formatı</li><li>LDAP protokolü</li></ul>
<b>Dizin Hizmetleri</b>	<ul style="list-style-type: none"><li>Kullanıcı sertifikalarının dizinden otomatik olarak çekilmesi ve yerel Windows sertifika deposuna yerleştirilmesi</li><li>X.500 uyumlu tüm dizin sunucularına bağlantı (Iplanet, DirX, Active Directory vb.)</li><li>Dizinde arama yapan özel tarayıcı arabirim</li></ul>
<b>Açık Anahtar Altyapısı (PKI) Hizmetleri</b>	<ul style="list-style-type: none"><li>Tüm işlemlerde sertifika ve sertifika iptal listesi (SİL/CRL) kontrolü, OCSP desteği</li><li>Çapraz sertifikasyon desteği</li></ul>
<b>Temel Güvenlik Hizmetleri</b>	<ul style="list-style-type: none"><li>X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak dosya/dizin şifreleme ve imzalama işlemlerini yapma</li><li>X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak dosya/dizin şifre çözme ve imza doğrulama işlemlerini yapma</li><li>İmzalı/şifreli dosyalar için otomatik çözme ve tekrar şifreleme/imzalama desteği</li><li>Dosya/dizin şifreleme ve imzalama işlemlerini istenen dizinler üstünde otomatik olarak yapma</li></ul>
<b>Diğer Hizmetler</b>	<ul style="list-style-type: none"><li>Parola tabanlı dosya/dizin şifreleme (sertifika kullanmadan)</li><li>Güvenli dosya/dizin silme</li><li>Dosya/dizinleri güvenli olarak çöp kutusuna atma</li><li>Kullanıcı grupları yaratma ve tüm işlemlerde kullanma</li></ul>
<b>Sertifika ve Kripto Özellikleri</b>	<ul style="list-style-type: none"><li>RSA veya DSA algoritmaları ile hazırlanmış X.509 v3 sertifikalar ile çalışma</li><li>PKCS7 / CMS için DES, 3DES, RC2, RC4 algoritmalarının kullanımı</li><li>MD5 ve SHA-1 mesaj özeti algoritmaları</li></ul>
<b>Kripto Donanımı Desteği</b>	<ul style="list-style-type: none"><li>PKCS #11 uyumlu akıllı kartlarla ve çubuklarla çalışma</li><li>Akıllı kart/çubuk kullanılmadığı durumlarda asimetrik anahtarları bilgisayarın sabit diskinde saklama/ kullanma</li></ul>
<b>Milli Özellikler</b>	<ul style="list-style-type: none"><li>Tüm yazılım TÜBİTAK UEKAE tarafından geliştirilmiştir.</li><li>İsteğe bağlı olarak kısa sürede özelleştirme yapılabilir.</li><li>İsteğe bağlı olarak milli kripto algoritması desteği verilebilir.</li></ul>



**Türkiye Bilimsel ve Teknolojik Araştırma Kurumu**  
**Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**

Yayın: BROS-501-10-B1-0005 (1.04)

Elektronik Sertifika Yönetim Altyapısı ürünleri için iletişim adresi:

TÜBİTAK UEKAE P.K.74, 41470 Gebze, Kocaeli - TÜRKİYE

Tel: (262) 648 1244 Faks: (262) 648 1100 Web: <http://www.uekae.tubitak.gov.tr>

