



TÜBİTAK UEKAE Elektronik Sertifika Yönetim Altyapısı



Emniyetli E-posta Modülü

E-postanın Önemi

İnternet'in ve bilgisayar sistemlerinin yaygın kullanımı sonucunda kurum ve kuruluşlar, ofisleri ve çalışanları birbirinden ayrı yerlerde bulunsalar bile, onları beraber iş yapmaya ve bilgi paylaşmaya yönlendirebilmektedir. Bunun için kullanılan en önemli araçlardan birisi de elektronik posta hizmetidir. E-postanın kullanımı ve taşıdığı bilginin miktarı ve önemi her gün gittikçe artmaktadır. Her gün e-posta sunucularından akan posta iletilerinin içinde kurum/kuruluşlara özgü rapor, plan ve tasarım gibi çok önemli bilgilerin bulunması artık sıradan hale gelmiştir. Bu **e-postalar ve içerdiği bilgiler çoğu zaman yetkisiz kişilerin erişimine ve müdahalesine karşı korumasız bırakılmaktadır**. Kötü niyetli kişilerce ele geçirilmesi durumunda ticari kayıplara ve kurum/kuruluşun güvenilirliğinin ve marka değerinin zayıflamasına neden olabilecek bu tip değerli e-posta iletilerinin korunması için güvenlik çözümlerine kesinlikle ihtiyaç olacaktır.

Güvenlik İhtiyaçları

E-posta iletilerinin güvenli bir şekilde saklanması ve iletişimi için ESYA Emniyetli E-Posta Modülü aşağıdaki özellikleri sunmaktadır:

- Önemli bilgi içeren e-postaları şifreleme ve imzalama
- Kullanıcıya iş yükü getirmeden güvenlik hizmetleri sunabilme
- Kolayca kurulabilme ve yönetilebilme
- Üst düzey güvenlik için akıllı kart ve token kullanabilme
- Güvenlik altyapısıyla uyum içinde çalışma

ESYA E-posta Güvenlik Çözümü

ESYA Emniyetli E-Posta Modülü, Elektronik Sertifika Yönetim Altyapısı'nın diğer bileşenleri olan Sertifikasyon Makamı, Kayıt Makamı, Sertifika Yardımcısı vb. ile tam bir uyum içinde çalışır. Bu sayede kullanıcılar arasında güvenli bir şekilde e-posta haberleşmesi yapma olanağını sunar.

Getirilen Çözümler

E-posta Şifreleme ve İmzalama:

Şifreli e-postaları sadece yetkisi olan kişiler açabilir. İmzalı e-postaların kimden geldiğinden emin olunur.

Ofis Programlarına

Tam Entegrasyon:

Endüstri standardı haline gelmiş ofis programlarına tam entegrasyon sağlanır.

Gruplara Erişim:

Kullanıcı gruplarına ve dağıtım listelerine şifreli/imzalı e-posta göndermek mümkün olur .

İçerik Sınıflandırma:

E-postalar içeriklerine göre kullanıcı tarafından sınıflandırılabilir ve emniyet seviyesine göre farklı algoritmalarla şifrelenebilir.

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. Türkçe için tam destek. Kolay anlaşılır arayüz.

ESYA Emniyetli E-posta Modülü Teknik Özellikleri

İşletim Sistemi	Windows 98, Windows NT, Windows 2000 (Bu işletim sistemlerine High Encryption Pack yüklenmiş olmalıdır), Windows XP, Windows 2003
Donanım Gereksinimi	<ul style="list-style-type: none">En az Celeron/Pentium II 500 MHz hızında işlemciEn az 64 MB RAM, en az 20 MB boş disk alanı
Desteklenen Yazılımlar	<ul style="list-style-type: none">Microsoft Outlook 2000 Türkçe/İngilizceMicrosoft Outlook XP/2003 Türkçe/İngilizceMicrosoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003
Desteklenen Standartlar	<ul style="list-style-type: none">X.509 v3 sertifikalarX.509 v2 sertifika iptal listeleri (SİL/CRL)Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP)S/MIMELDAP protokolü
Dizin Hizmetleri	<ul style="list-style-type: none">Kullanıcı sertifikalarının dizinden otomatik olarak çekilmesi ve yerel Windows sertifika deposuna yerleştirilmesiX.500 uyumlu tüm dizin sunucularına bağlantı (Iplanet, DirX, Active Directory vb.)
Açık Anahtar Altyapısı (PKI) Hizmetleri	<ul style="list-style-type: none">Tüm işlemlerde sertifika ve sertifika iptal listesi (SİL/CRL) kontrolü, OCSP desteğiÇapraz sertifikasyon desteği
Temel Güvenlik Hizmetleri	<ul style="list-style-type: none">X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak e-posta şifreleme ve imzalama işlemlerini yapmaX.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak e-posta şifre çözme ve imza doğrulama işlemlerini yapmaE-posta şifreleme ve imzalama işlemlerini kullanıcı grupları için otomatik olarak yapma (Microsoft Exchange Server sunucu ile çalışırken)
Diğer Hizmetler	<ul style="list-style-type: none">E-postanın içeriğine göre kullanıcı tarafından sınıflandırılabilmesi ve emniyet seviyesine göre farklı algoritmalarla şifrelenmesiŞifreli gönderilen e-postaların gönderen kişinin de açabileceği şekilde şifrelenmesiİmzalı e-postalarda imzalama için kullanılan sertifikanın e-postayla beraber gönderilmesiHTML e-posta içeriği desteği
Sertifika ve Kripto Özellikleri	<ul style="list-style-type: none">RSA veya DSA algoritmaları ile hazırlanmış X.509 v3 sertifikalar ile çalışmaS/MIME için DES, 3DES, RC2, RC4 algoritmalarının kullanımıMD5 ve SHA-1 mesaj özeti algoritmaları
Kripto Donanımı Desteği	<ul style="list-style-type: none">PKCS #11 uyumlu akıllı kartlarla ve akıllı çubuklarla çalışmaAkıllı kart/çubuk kullanılmadığı durumlarda asimetrik anahtarları bilgisayarın sabit diskinde saklama/ kullanma
Milli Özellikler	<ul style="list-style-type: none">Tüm yazılım TÜBİTAK UEKAE tarafından geliştirilmiştir.İsteğe bağlı olarak kısa sürede özelleştirme yapılabilir.İsteğe bağlı olarak milli kripto algoritması desteği verilebilir.



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

Yayın: BROS-501-10-B1-0006 (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>

