TÜBİTAK
BİLGEM

MİLLİ VE GÜVENLİ ŞİFRELEME VE İMZALAMA SİSTEMİ

KERMEN

ELEKTRONİK VERİLERİN VARLIĞINI KANITLAYAN
GÜVENLİ VE YASAL STANDART!

AÇIK ANAHTAR ALTYAPISI ARAÇLARI

KERMEN

Tamamen milli, yerli ve uluslararası standartlara uygun olarak geliştirilen KERMEN, OrtakKriterler (CC) EAL 4+ sertifikasınasahiptir. KERMEN, Açık Anahtar Altyapısı'nın (PKI) bileşenlerinden olan Sertifikasyon Makamı ve Kayıt Makamı ile tam uyumlu çalışır. Sertifika tabanlı asimetrikşifreleme ve imzalama özelliklerini kullanarak, kullanıcılara verileri güvenli bir şekilde saklama ve paylaşma olanağı sunar.

GENEL ÖZELLİKLER
Emniyetli E-posta Modülü
Masaüstü güvenlik Modülü
KERMENPortable

GETİRİLEN ÇÖZÜMLER	
KERMEN Emniyetli E-Posta Modülü	**E-posta Şifreleme ve İmzalama** Şifreli E-postaları sadece yetkisi olan kişiler açabilir. İmzalı E-postaların kimden geldiğinden emin olunur. **Outlook ile Tam Entegrasyon** Endüstri standardı haline gelmiş olan Microsoft Outlook ile tam entegrasyon sağlanır. **Gruplara Erişim** Kullanıcı gruplarına, dağıtım listelerine şifreli/imzalı e-posta göndermek mümkün olur.
KERMEN Masaüstü Güvenlik Modülü	**Dosya ve DizinŞifreleme/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
KERMEN Portable	**Kurulum Gerektirmeksizin Çalışma** KERMEN Portable ürünü, uygulama dizininin kullanıcı bilgisayarına kopyalanmasıyla ve gerekli olan lisans dongle bilgisayara takıldığında çalışır hale gelir. Herhangi bir kuruluma ihtiyaç duymaz. Bu özellik, uygulamanın harici taşınabilir bir depoda (flash disk vb.) saklanarak kullanıcı makinesine kurulmadan çalışabilmesini mümkün kılar.

TEKNİK ÖZELLİKLER	
İşletim Sistemi	Windows 7, 8, 10, 11 Pardus 23 ve üzeri Ubuntu 18.04 ve üzeri
Donanım Gereksinimi	Microsoft Outlook
Desteklenen Standartlar	X.509 v3 Sertifikalar X.509 v2 Sertifika İptalListeleri (SİL/CRL) Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP) S/MIME LDAP protokolü
Temel Güvenlik Hizmetleri	X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak dosya/dizin/E-posta şifreleme ve imzalama X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak imzalı/şifreli dosya/dizin şifreçözme ve imza doğrulama E-postaların içeriğine göre kullanıcı tarafından farklı güvenlik seviyelerine ayrılabilmesi ve her bir güvenlik seviyesi için farklı algoritmalarla şifrelenmesi Dosya/dizin güvenli silme İmzalı/şifreli dosyalar için otomatik şifre çözme ve tekrar şifreleme/imzalama Mail kullanıcı gruplarına şifreli/imzalı mail gönderebilme Masaüstü ve dosya/dizin üzerinde sağ tıklama menüsüne entegrasyon Yerel kullanıcı grupları tanımlayabilme Belirtilen dizine atılan dosyaları otomatik imzalama/şifreleme (Güvenli Dizin) Yerel güvenli sertifika deposu
Sertifika ve Kripto Özellikleri	RSA-2048/4096, EC-384/512/521 şifreleme algoritmaları DSA-4096 ve ECDSA(384/512/521) sayısal imzalama algoritmaları PKCS7/CMS için3DES veAES algoritma desteği Güvenli E-Posta (S/MIME) için RSA-2048/4096, DSA-2048/4096, EC-384/512/521 ve ECDSA algoritma desteği SHA-2 (SHA-224/256/384/512) mesaj özeti algoritma desteği
Diğer Hizmetler	PKCS11 uyumlu akıllı kart ve dongle'larla, masaüstü ve taşınabilir kart okuyucularıyla çalışabilme Akıllı kart/dongle kullanılmadığı durumlarda özel anahtarları PFX dosyaları ile alıp yerel depoda güvenli saklama/kullanma
Milli Özellikler	TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiştir.

BİLGEM
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

T: +90 262 648 1000 • F: +90 262 648 1100 • E: bilgem@tubitak.gov.tr
W: bilgem.tubitak.gov.tr • A: PK.: 74, 41470, Gebze, Kocaeli TÜRKİYE