TÜBİTAK
BİLGEM

TAŞINABİLİR KRİPTOGRAFİK GÜVENLİK MODÜLÜ

KERMEN PORTABLE

UEKAE
Kermen

KRİTİK ALTYAPILAR İÇİN TAŞINABİLİR,
MİLLİ GÜVENLİK MODÜLÜ!

TAŞINABİLİR KRİPTOGRAFİK GÜVENLİK MODÜLÜ

KERMEN PORTABLE

Tamamen milli, yerli ve uluslararası standartlara uygun olarak geliştirilen KERMEN'in kurulum gerektirmeyen belirli özellikleri limitlenmiş bir versiyonu olan KERMEN Portable, Açık Anahtar Altyapısı'nın (PKI) bileşenlerinden olan Sertifikasyon Makamı ve Kayıt Makamı ile tam uyumlu çalışır. Sertifika tabanlı asimetrik şifreleme ve imzalama özelliklerini kullanarak, kullanıcılara verileri güvenli bir şekilde saklama ve paylaşma olanağı sunar.

GENEL ÖZELLİKLER
Önemli bilgi içeren dosyaları şifreleme ve imzalama
Kullanıcıya iş yükü getirmeden güvenlik hizmetleri sunabilme
Kolayca kurulabilme ve yönetilebilme
Üst düzey güvenlik için sadece belirlenmiş dongle ile çalışma
PKCS11 uyumlu akıllı kartlar ile çalışabilme
Güvenlik altyapısıyla uyum içinde çalışabilme

GETİRİLEN ÇÖZÜMLER
Dosyave DizinŞifreleme/İmzalama Şifreli dosyalara sadece yetkisi olankişiler erişebilir. İmzalı dosyaların kime ait olduğundan emin olunur. Şifreleme ve imzalama için sertifikalar kullanılır.
Kurulum Gerektirmeksizin Çalışma KERMEN Portable ürünü, uygulama dizininin kullanıcı bilgisayarına kopyalanmasıyla ve gerekli olan 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.
Güvenli Dosya Silme Silinen dosyaların hiçkimse tarafından geri kazanılamaması sağlanır.

TEKNİK ÖZELLİKLER	
İşletim Sistemi	Windows 7, 8, 10, 11 Pardus 23 ve üzeri Ubuntu 18.04 ve üzeri
Dizin Hizmetleri	Kullanıcı sertifikalarının dizinden otomatik olarak çekilmesi ve yerel depoya eklenmesi X.500 uyumlu tüm dizin sunucularına bağlantı (CP, OpenLDAP, Active Directory vb.)
Desteklenen Standartlar	IX.509 v3 Sertifikalar X.509 v2 Sertifika İptalListeleri (SİL/CRL) Çevrimiçi Sertifika Durum Protokolü (ÇiSDuP/OCSP) LDAP protokolü
Temel Güvenlik Hizmetleri	X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak dosya şifreleme ve imzalama X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak imzalı/şifreli dosyanın şifresini çözme ve imzadoğrulama Dosya güvenli silme Sürükle bırak yöntemi ile dosyaşifreleme ve imzalama 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 için 3DES, AES algoritma desteği SHA-2 (SHA-224/256/384/512) mesaj özeti algoritma desteği
Kripto Donanımı Desteği	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