TÜBİTAK
BİLGEM

YERLİ VE STANDARDA UYUMLU SERTİFİKA MAKAMI

ESYA SM

MİLLİ ALTYAPI VE STANDARTLARA UYGUN ENTEGRE
SERTİFİKASYON ÇÖZÜMÜ!

YERLİ VE STANDARDA UYUMLU SERTİFİKA MAKAMI

ESYA SM

Açık anahtar altyapısı (AAA/PKI), asimetrik kriptoloji üzerine inşa edilmiş bir teknolojidir. Elektronik sertifikalar, AAA teknolojisinin en önemli bileşenlerinden birisidir. Elektronik sertifikaları üretmek icin sertifikasyon makamı ve yardımcı yazılımlara ihtiyaç duyulmaktadır. Sertifikasyon makamları kendilerine bağlı alt sertifikasyon makamları, kullanıcılar, sunucular ve cihazlar için elektronik sertifikalar üretir. ESYA Sertifikasyon Makamı, Milli Açık Anahtar Altyapısı (MA3) proje grubu tarafından tamamen yerli olarak gerçeklenmiştir. ESYA Sertifikasyon Makamı, endüstriyel elektronik sertifika standartlarını (X.509, CVC, vb) destekler ve kullanıcı dostu bir arayüzle tüm elektronik sertifika yaşam döngüsü (üretim, yenileme, askıya alma, iptal, vb.) hizmetlerini sunar.

GENEL ÖZELLİKLER

Kontrol Merkezi
Sertifikasyon makamı yöneticileri tarafından, sertifikasyon makamının kendisini ve alt sertifikasyon makamlarını yönetmek için kullanılan yazılımdır. Kontrol Merkezi aynı zamanda sistemdeki kayıtçıların tanımlanması ve yetkilerinin belirlenmesini sağlar.

Kayıt Makamı
Sertifikasyon makamı işletmenleri (kayıtçılar) tarafından sertifika kullanıcılarının sisteme kayıt edilmesi ve yönetilmesi için kullanılan yazılımdır.

Sertifika Üretim Servisi
HTTP üzerinde CMP (Certificate Management Protocol) protokolü ile çalışan ve sertifikasyon makamına gelen sertifika taleplerine sertifika üreterek cevap veren yazılımdır.

Sertifika İptal Listesi Servisi
Çeşitli nedenlerle iptal edilen sertifikaların, sertifika iptal listesinde (SİL) yayımlanmasını sağlayan servis yazılımıdır.

Çevrimiçi Sertifika Durum Protokolü (OCSP) Servisi
Sertifikaların iptal durumlarının gerçek zamanlı veya en güncel SİL'den sorgulanmasına imkan veren servis yazılımıdır.

TEKNİK ÖZELLİKLER

İşletim Sistemi	Windows 2008+, Linux
Donanım Gereksinimleri	Intel/AMD işlemci En az 8 GB RAM En az 500 MB boş disk alanı
Yazılım Gereksinimleri	Oracle 11g veya PostgreSQL 9.4 ve üstü veritabanı sunucusu Java 1.8+ Tomcat Web sunucusu veya servlet desteği olan bir web sunucusu
Desteklenen Standartlar	X.509 v3 Sertifikalar X.509 v2 Sertifika İptal Listeleri (SİL/CRL) Card Verifiable Certificates Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP) PKIX güvenli haberleşme protokolü (CMP) LDAP protokolü
Kripto Özellikleri	RSA algoritması (1024, 2048, 4096 bit anahtar uzunluğu) ECDSA algoritması (163, 192, 256, 368, 431, 512 bit anahtar uzunlukları) SHA1, SHA256, SHA384, SHA512 mesaj özeti algoritmaları
Kripto Donanımı Desteği	RSA algoritması (1024, 2048, 4096 bit anahtar uzunluğu) ECDSA algoritması (163, 192, 256, 368, 431, 512 bit anahtar uzunlukları) SHA1, SHA256, SHA384, SHA512 mesaj özeti algoritmaları
Milli Özellikler	Tüm yazılımlar TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiştir.

GETİRİLEN ÇÖZÜMLER

Sertifika ve Anahtar Üretimi
Kriptografik anahtar çiftleri ve sertifikaları kullanan tüm yazılım ve donanım ürünleri için anahtar ve sertifika üretimini ve yönetimini sağlar.

Elektronik İmza Altyapısı
Elektronik (sayısal) imza kullanımı için gerekli olan altyapıyı oluşturur.

Bilgi Güvenliği Altyapısı
Dosya, dizin, e-posta gibi uygulamaların gizlilik, kimlik doğrulama, bütünlük ve inkar edilemezlik hizmetleri için gerekli olan altyapıyı şifreleme/imzalama yöntemlerini kullanarak sunar.

Prensip Bazlı Yönetim
Tüm güvenlik altyapısı, tanımlanan prensiplere uygun olarak yönetilir.

Kesin Hiyerarşi
Kök sertifikasyon makamı altında kesin hiyerarşi içinde dikey ve yatay olarak istenen sayıda sertifikasyon makamı oluşturulabilir. Ayrıca farklı sertifikasyon makamları ile çapraz sertifikasyon yapılabilir.

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