ESYA
Sertifikasyon Makamı
Teknik Özellikleri

İşletim Sistemi
•Windows Server 2016+ •Linux
Minimum Donanım Gereksinimleri
•Intel/AMD işlemci
•En az 16 GB RAM
•En az 100 GB boş disk alanı
Minimum Yazılım Gereksinimleri
•Oracle 11g veya PostgreSQL 9.4 ve üstü veritabanı sunucusu
•Java 1.8+
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
•Sertifika Şeffaflığı (Certificate Transparency-CT)
Dizin Hizmetleri
•X.500 uyumlu tüm dizin sunucularıyla çalışma (TÜBİTAK Directory Server, Fedora Directory Server, Active Directory vb.)
•Birden fazla dizin ile aynı anda çalışabilme
•Sertifikaların üretildikten sonra otomatik olarak dizinde yayınlanması
Açık Anahtar Altyapısı (AAA) Hizmetleri
•X.509 v3 sertifika yayınlama
•X.509 v2 sertifika iptal listesi yayınlama
•Şifreleme anahtarlarını sunucuda üretme ve yedekleme
•Anahtar geri kazanma ve yenileme
Hiyerarşi ve Çapraz Sertifikasyon Desteği
•Kök Sertifikasyon Makamı altında kesin hiyerarşi içinde dikey ve yatay olarak istenen sayıda Sertifikasyon Makamı yaratma
•Kök Sertifikasyon Makamı ile başka bir Sertifikasyon Makamı arasında çapraz sertifikasyon yapma
Sertifika Tipleri
Sertifika şablonu tanımlama özelliği sayesinde:
•Nitelikli Elektronik Sertifika,
•Şifreleme Sertifikası,
•SSL/TLS, VPN,
•Code Signing,
•Windows Smartcard Logon, Windows Domain Controller gibi X.509 v3 sertifikaları üretme
SSL Sertifika Özellikleri
•Sertifika Şeffaflığı (CT), SSL sertifika sistemindeki çeşitli yapısal kusurları ortadan kaldırmayı amaçlayan, Google tarafından başlatılan bir projedir. ESYA CT'e uygun sertifika üretimi yapabilmektedir.
•Domain Validation (DV) SSL, Organization Validation (OV) SSL, Individual Validation (IV) SSL, Extended Validation (EV) SSL tipleri desteklenmektedir.
•Single Domain SSL, Multi-Domain SSL, Wildcard SSL desteği bulunmaktadır.
Kripto Özellikleri
•RSA algoritması (1024, 2048, 4096 bit anahtar uzunluğu)
•ECDSA algoritması (256, 384, 521, 571 bit anahtar uzunlukları)
•SHA1, SHA256, SHA384, SHA512 mesaj özeti algoritmaları
Kripto Donanımı Desteği
•PKCS 11 uyumlu akıllı kartlarla ve çubuklarla çalışma
•Donanım güvenlik modülü (HSM) kullanımı
Milli Özellikler
•Tüm yazılımlar TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiştir.
Web Servis Hizmetleri
•Müşeri ihtiyaçlarına göre RESTFul web servis hizmeti,
•Müşeri ihtiyaçlarına göre SOAP web servis hizmeti,
•X.509 v2 sertifika iptal listesi yayınlama
•Şifreleme anahtarlarını sunucuda üretme ve yedekleme
•Anahtar geri kazanma ve yenileme
Hiyerarşi ve Çapraz Sertifikasyon Desteği
•Kök Sertifikasyon Makamı altında kesin hiyerarşi içinde dikey ve yatay olarak istenen sayıda Sertifikasyon Makamı yaratma
•Kök Sertifikasyon Makamı ile başka bir Sertifikasyon Makamı arasında çapraz sertifikasyon yapma
Sertifika Tipleri
Sertifika şablonu tanımlama özelliği sayesinde:
•Nitelikli Elektronik Sertifika
•SSL (Sunucu ve istemci), VPN
•Windows Smartcard Logon, Windows Domain Controller gibi X.509 v3 sertifikaları üretme
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
•PKCS 11 uyumlu akıllı kartlarla ve çubuklarla çalışma
•"M of N" anahtar paylaşım desteği
•Donanım güvenlik modülü (HSM) kullanımı
Milli Özellikler
•Tüm yazılımlar TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiştir.

TÜBİTAK
BİLGEM

ELEKTRONİK SERTİFİKA YÖNETİM ALTYAPISI

ESYA Sertifikasyon Makamı

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.

SERTİFİKASYON MAKAMI BİLEŞENLERİ

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.

RESTful Web Servisleri

Müşterilerin ihtiyaçlarına göre geliştirilen RESTful Web Servislerdir. CRM, ERP ...vb sistemler ile entegrasyon için kolaylık sağlar.

SOAP Web Servisleri

Müşterilerin ihtiyaçlarına göre geliştirilen SOAP Web Servislerdir. CRM, ERP ...vb sistemler ile entegrasyon için kolaylık sağlar.

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.

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.

SUNULAN AVANTAJLAR

Yüksek Teknoloji

- Güvenliği üst seviyeye çıkarmak için HSM, akıllı kart kullanımı
- Uluslararası güvenlik standartlarına uyumlu milli yazılım

Çoklu Sertifikasyon Makamı Oluşturma/Yönetme

- Birden fazla sertifikasyon makamını aynı arayüz üzerinde oluşturabilme ve yönetebilme imkanı

Kullanım ve Entegrasyon Kolaylığı

- Sertifikasyon makamının bütün bileşenlerinin internet tarayıcı üzerinden kolay kullanım ve yönetimine imkan veren modern tasarımlı arayüz
- CRM/ERP sistemlerine sunulan webservisler aracılığıyla kolaylıkla entegrasyon
- Çoklu dil desteği (Türkçe/İngilizce/Azerice/Rusça/Türkmence)

Uluslararası Güvenlik Sertifikası

- Certificate Issuing and Management Components (CIMC) Protection Profile uyumlu Common Criteria EAL 4+ sertifikasyonu

Akıllı Kart Yazıcıları ile Çalışabilme

- Toplu sertifika üretiminde desteklenen akıllı kart yazıcıları ile çalışabilme ve yeni yazıcılara kolay entegrasyon altyapısı