



TÜBİTAK UEKAE Elektronik Sertifika Yönetim Altyapısı



Sertifikasyon Makamı

Sertifikasyon Makamı'nın Açık Anahtar Altyapısı İçindeki Yeri

Açık anahtar altyapısı, elektronik sertifikalar üzerine inşa edilmiş bir teknolojidir. Bu altyapı, elektronik sertifikaları üretmek için sertifikasyon makamı ve yardımcı yazılımlara ihtiyaç duyar. Sertifikasyon makamları kendilerine bağlı alt sertifikasyon makamları, kullanıcılar, sunucular ve cihazlar için elektronik sertifikalar üretirler. Elektronik sertifikaların üretilmesinden sonra bunların sahiplerine ulaştırılması ve gerektiğinde iptal edilmesi de gereklidir. Tüm bu işlemleri yapan sistemin hiyerarşik olarak en üstünde yer alan ve güven noktası olarak kabul edilen sertifikasyon makamı Kök Sertifikasyon Makamı olarak adlandırılır.

Sertifikasyon Makamı Bileşenleri

Sertifikasyon Makamı aşağıdaki bileşenlerden oluşur:

- **Kontrol Merkezi:** Sertifikasyon Makamı yöneticileri tarafından, sertifikasyon makamının kendisini ve alt sertifikasyon makamlarını yönetmek için kullanılan yazılımdır. Kontrol Merkezi aynı zamanda sistemdeki kayıtçılarının tanımlanmasını ve yetkilerinin belirlenmesini sağlar.
- **Kayıt Makamı:** Sertifikasyon Makamı işletmenleri tarafından sertifika kullanıcılarının sisteme kayıt edilmesi ve yönetilmesi için kullanılan yazılımdır. Kayıt Makamı bir web sunucu olarak çalışır ve kayıtçılar tarafından internet tarayıcıları aracılığıyla kullanılır.
- **Sertifika Üretim Servisi:** Ağ servisi olarak çalışan ve Sertifikasyon Makamı'na gelen geçerli sertifika taleplerine sertifika üreterek cevap veren yazılımdır.
- **Sertifika İptal Listesi Servisi:** Çeşitli nedenlerle iptal edilen sertifikaların, sertifika iptal listesinde (SİL) yayınlanmasını sağlayan servis yazılımdır.
- **Sertifika Bulma Servisi:** Sadece sertifika seri numarasının bulunduğu durumlarda kullanılan ve bu numaraya sahip sertifikayı isteyen kullanıcılara veren yazılımdır.

Getirilen 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, izin ve e-posta için kimlik doğrulama, gizlilik, bütünlük ve inkâr edememezlik hizmetlerinin altyapısını şifreleme/imzalama yöntemleri kullanarak sunar.

Prensip Bazlı Yönetim:

Tüm güvenlik altyapısı, tanımlanan prensiplere uygun olarak yönetilir.

Kesin Hiyerarşi:

Kök Sertifikasyon Makamı'nın altında dikeyde ve yatayda sınırsız sayıda Sertifikasyon Makamı tanımlanabilir. Ayrıca farklı Sertifikasyon Makam'ları ile çapraz sertifikasyon da yapılabilir.

Sunulan Avantajlar

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 Sertifikasyon Makamı Teknik Özellikleri

İşletim Sistemi	Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Professional (tüm bu işletim sistemlerine High Encryption Pack yüklenmiş olmalıdır), Windows 2003. İstenirse Linux işletim sistemine de uyartılabilir.
Donanım Gereksinimi	<ul style="list-style-type: none">En az Pentium III 800 MHz hızında işlemciEn az 512 MB RAM , en az 300 MB boş disk alanı
Yazılım Gereksinimi	<ul style="list-style-type: none">Oracle 9i veya Oracle 10g veritabanıSun Java JDK 1.4Tomcat Web sunucusu veya servlet desteği olan bir web sunucusu
Desteklenen Standartlar	<ul style="list-style-type: none">X.509 v3 sertifikalar, X.509 v2 sertifika iptal listeleri (SİL/CRL)Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP)PKIX güvenli haberleşme protokolüLDAP protokolü
Dizin Hizmetleri	<ul style="list-style-type: none">Sertifikaların yaratıldıktan sonra otomatik olarak dizinde yayınlanmasıX.500 uyumlu tüm dizin sunucularla çalışma (Iplanet, DirX, Active Directory vb.)
Açık Anahtar Altyapısı (PKI) Hizmetleri	<ul style="list-style-type: none">X.509 v3 sertifika yayınlama, X.509 v2 sertifika iptal listesi yayınlamaŞifreleme anahtarlarını sunucuda üretme ve yedeklemeAnahtar geri kazanma ve yenilemeTüm kritik kayıtların ve işlemlerin veritabanında imzalı olarak tutulması
Hiyerarşi ve Çapraz Sertifikasyon Desteği	<ul style="list-style-type: none">Kök Sertifikasyon Makamı altında kesin hiyerarşi içinde dikey ve yatay olarak istenen sayıda Sertifikasyon Makamı yaratmaKök Sertifikasyon Makamı ile başka bir sertifikasyon makamı arasında çapraz sertifikasyon yapma
Sertifika Tipleri	<ul style="list-style-type: none">Sertifika Şablonu tanımlama özelliği sayesinde her türlü X.509v3 sertifikası üretme. Aşağıdakilerle sınırlı olmamak üzere örneğin:<ul style="list-style-type: none">Nitelikli Elektronik SertifikaSSL (Sunucu ve istemci), VPNWindows Smartcard Logon, Windows Domain Controller
Kripto Özellikleri	<ul style="list-style-type: none">RSA algoritması (1024, 2048, 4096 bit anahtar uzunluğu)ECDSA algoritması (163, 192, 256, 368, 431, 512 bit anahtar uzunlukları)DSA algoritması (1024 bit anahtar uzunluğu)SHA1, SHA256, SHA384, SHA512 mesaj özeti algoritmaları
Kripto Donanımı Desteği	<ul style="list-style-type: none">PKCS #11 uyumlu akıllı kartlarla ve çubuklarla çalışma"M of N" anahtar paylaşım desteğiHSM (Hardware Security Module) kullanımı
Milli Özellikler	<ul style="list-style-type: none">Tüm yazılım TÜBİTAK UEKAE tarafından geliştirilmiştir.İsteğe bağlı olarak kısa sürede özelleştirme yapılabilir.



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

Yayın: BROS-501-10-B1-0002 (1.05)

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>



UEKAE, ürünlerini çağdaş teknoloji düzeyinde tutma çabaları nedeniyle, bu broşürde belirtilen teknik özelliklerde değişiklik yapma hakkına sahiptir.