



TÜBİTAK UEKAE Elektronik Sertifika Yönetim Altyapısı



Zaman Damgası Sunucusu

Zaman Damgası Hizmeti

Zaman Damgası Sunucusu, günlük hayatımızın ihtiyaçlarını karşılamak için tasarlanan yeni nesil Açık Anahtar Altyapısının (PKI) bir parçasıdır. Zaman Damgası Sunucusu'nun temel görevi, istemcilerden gelen taleplere göre elektronik imzalı zaman damgası üretmektir. **Zaman Damgaları belli bir verinin belirtilen bir tarihte var olduğunu kanıtlarlar.** Zaman Damgası Sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisini kullanarak, verinin bütünlüğünü ve belirli bir tarihteki varlığını onaylar.

Bir sözleşmenin imzalandığı, paranın transfer edildiği, başvurunun yapıldığı vs. tarih ve saati kanıtlama ihtiyacı günümüz e-ticaret, e-devlet uygulamaları için hayati önem taşımaktadır. Bununla birlikte yeni bir çizim, tasarım, fotoğraf, düşünce, araştırma, formül, algoritma, kitap gibi fikri ve mülki kullanım hakkı elde edilmek istenen her türlü elektronik veri için zaman damgası alınabilir.

Özellikler

ESYA Zaman Damgası Hizmeti aşağıdaki özellikleri sunmaktadır:

- Zaman damgası, veri özeti ile zaman bilgisinin, zaman damgası sunucusu tarafından imzalanması ile oluşan elektronik veridir.
- Zaman damgası alınacak veri içeriği gizli kalmakta, sadece verinin özeti kullanılmakta ve veri özetinden veriyi elde etmek mümkün olmamaktadır.
- Zaman bilgisi, Ulusal Metroloji Enstitüsü (UME) atom saati vb güvenilir zaman kaynaklarından alınmaktadır.
- Zaman Damgası Sunucusu, zaman damgası yapısını güvenli donanım modülünde(HSM) imzalamaktadır.
- Her türlü bilgisayar dosyası, elektronik veri için zaman damgası alınabilmektedir.
- Verilen herbir zaman damgasının tekil bir numarası vardır. İstenildiğinde zaman damgasının geçerliliği kontrol edilebilmektedir.

Getirilen Çözümler

Ücretsiz Zaman Damgası İstemci Uygulaması:

Zaman Damgası Sunucusuna internet üstünden bağlanarak her türlü bilgisayar dosyası için kolaylıkla zaman damgası alma imkanı.

Zaman Damgası Dosyalarının Arşivlenmesi:

Zaman Damgası İstemcisi kullanılarak alınan zaman damgalarının arşivlenip, daha sonra tekrar doğrulanabilmesi imkanı

Geniş API desteği:

Farklı uygulamalarla entegrasyon için Java, C, C++ API desteği.

Sunulan Avantajlar

Yüksek Teknoloji:

Uluslararası güvenlik standartlarına uyumlu milli yazılım.

Kullanım Kolaylığı:

Kullanıcı alışkanlıklarını değiştirmeyen yaklaşım. Kolay anlaşılır arayüz.

ESYA Zaman Damgası Sunucusu Teknik Özellikleri

İşletim Sistemi	<ul style="list-style-type: none">Windows 2000Windows XP (Sadece istemci)Windows 2003Linux
Donanım / Yazılım Gereksinimi	<ul style="list-style-type: none">En az Pentium IV, 2.0 GHz hızında işlemciEn az 512 MB RAMEn az 20 MB boş disk alanıOracle veritabanı sunucusuJava 1.4/1.5
Desteklenen Standartlar	<ul style="list-style-type: none">RFC 3161 – Internet X.509 PKI Zaman Damgası ProtokolüETSI TS 102 023 – Zaman Damgası Makamı İlke GereklereX.509 v3 sertifikalarX.509 v2 sertifika iptal listeleri (SİL/CRL)Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP)
Açık Anahtar Altyapısı (PKI) Hizmetleri	<ul style="list-style-type: none">Zaman damgası doğrulama işleminde sertifika ve sertifika iptal listesi (SİL/CRL) kontrolüÇevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP) desteğiÇapraz sertifikasyon desteği
Temel Güvenlik Hizmetleri	<ul style="list-style-type: none">X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak zaman damgası imzalama işlemlerini yapmaX.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak zaman damgası doğrulama işlemlerini yapmaPKCS #5 kullanılarak istemci kimliğini doğrulama
Diğer Hizmetler	<ul style="list-style-type: none">Zaman damgasının arşivlenmesiZaman damgası verisinin işlenip detaylarının gösterilmesiZaman damgası verisinin sertifika formatında gösterilip, yazdırılabilmesi
Sertifika ve Kripto Özellikleri	<ul style="list-style-type: none">1024 – 2048 – 4096 bit RSA algoritması desteğiZaman Damgası imzası için RSA algoritmasının kullanımıAES 128, 192, 256 bit simetrik şifreleme algoritması kullanımıSHA-1, SHA-256, SHA-512 mesaj özeti algoritmaları
Kripto Donanım Desteği	<ul style="list-style-type: none">Zaman Damgası sunucusunun imzalama işlemini güvenli donanım modülünde(HSM) yapması
Milli Özellikler	<ul style="list-style-type: none">Tüm yazılım TÜBİTAK UEKAE tarafından geliştirilmiştir.İsteğe bağlı olarak milli kripto algoritması desteği verilebilir.



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

Yayın: BROS-501-10-B1-0006 (1.04)

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>



AQAP-110
2003 / 20