Zaman Damgası Sunucusu Teknik Özellikleri

İşletim Sistemi

Windows 2003+, Linux

Donanım ve Yazılım Gereksinimi

- Intel/AMD İşlemci
- Oracle veya Postgre veritabanı Sunucusu
- Java 1.6 +

Desteklenen Standartlar

- RFC 3161 (Internet X.509 PKI Zaman Damgası Protokolü)
- ETSI TS 102 023 Zaman Damgası Makamı İlke Gerekleri
- X.509 v3 Sertifikalar

Temel Güvenlik Hizmetleri

- X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak zaman damgası imzalama işlemi
- PKCS 5 kullanarak istemci kimliğini doğrulama
- Zaman damgasının arşivlenmesi

Sertifika ve Kripto Özellikleri

- Zaman damgası imzası için RSA ve ECDSA algoritmaları desteği
- AES şifreleme algoritmasının kullanımı
- SHA-1 ve SHA-2 özet algoritma ailesinin kullanımı

Kripto Donanımı Desteği

- Zaman damgası sunucusunun imzalama işlemini güvenli donanım modülünde (HSM) yapması

Milli Özellikler

- TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiştir.
- İsteğe bağlı olarak kısa sürede özelleştirme yapılabilir.
- İsteğe bağlı olarak milli kripto algoritması desteği verilebilir.

TÜBİTAK
BİLGEM

Elektronik Sertifika Yönetim Altyapısı

Zaman Damgası Sunucusu

Zaman Damgası Hizmeti

Zaman Damgası elektronik verilerin belirtilen bir tarihte var olduğunu kanıtlamak amacıyla uluslararası bir standart ile tanımlanmış ve kanuni geçerliliği bulunan bir güvenlik verisidir. Zaman Damgası Sunucusu kendisine gönderilen elektronik veriler için bu standartlara uygun zaman damgaları üretir. 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 de zaman damgası alınması gereklidir.

5070 sayılı Elektronik İmza Kanununa göre Zaman Damgası "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı" olarak ifade edilmektedir.

Zaman Damgası Sunucusu Özellikleri

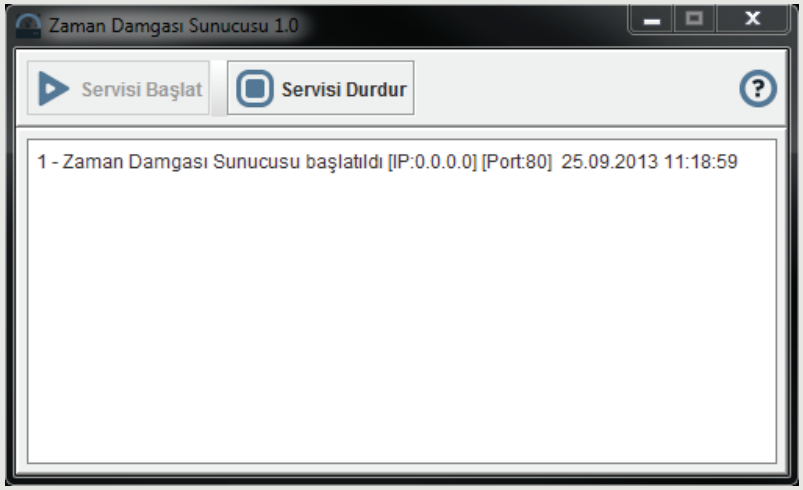
ESYA Zaman Damgası Sunucusu aşağıdaki hizmetleri sunmaktadır:

- RFC 3161 standardına uyumlu zaman damgası
- NTP protocol desteği
- HSM kullanımı ile yüksek performansta çalışma

Getirilen Çözümler

Standartlara Uyumluluk

Zaman Damgası Sunucusu PKIX RFC 3161 (Internet X.509 PKI Zaman Damgası Protokolü) güvenlik standartlarına uyumlu 5070 sayılı Elektronik İmza Kanununa göre geçerli Zaman Damgası üretir.



Gelişmiş Müşteri Yönetimi

Zaman Damgası sunucusu gelişmiş müşteri yönetimi arayüzü ile kontör bazlı olarak müşteri tanımlayabilmekte ve zaman damgası isteklerini tanımlanmış müşteri bilgilerine gore cevaplayabilmektedir.

Zaman Damgası Dosyalarının Arşivlenmesi

Zaman Damgası Sunucusu ürettiği zaman damgalarını daha sonra tekrar doğrulanabilmesi amacıyla arşivleyebilmektedir.

Gelişmiş Kriptografik Algoritma Desteği

Zaman Damgası Sunucusu RSA ve ECDSA gibi gelişmiş imzalama algoritmalarını ve SHA-2 özet algoritma ailesini destekler.

Diğer Destekler

NTP protokolü ile haberleşme ve yüksek performanslı çalışma