ZAMANE
Teknik Özellikleri

İşletim Sistemi

Windows 7+, Linux, Mac

Donanım Gereksinimi

- Java 1.8+

Desteklenen Standartlar

- RFC 3161 (Internet X.509 PKI Zaman Damgası Protokolü)
- ETSI TS 102 023 Zaman Damgası Makamı İlke Gerekleri
- X.509 v3 Sertifikalar
- X.509 v2 Sertifika İptal Listeleri (SİL/CRL)
- Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP)

Açık Anahtar Altyapısı (AAA) Hizmetleri

- Zaman damgası doğrulama işleminde sertifika ve sertifika iptal listesi (SİL/CRL) kontrolü
- Çevrimiçi Sertifika Durum Protokolü (ÇİSDUP/OCSP) desteği

Temel Güvenlik Hizmetleri

- X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak zaman damgası doğrulama işlemlerini yapma
- PKCS 5 kullanarak istemci kimliği oluşturma

Sertifika ve Kripto Özellikleri

- Zaman damgası imza doğrulaması için RSA ve ECDSA algoritmaları desteği
- AES şifreleme algoritmalarının kullanımı
- SHA-1/224/256/384/512 mesaj özeti algoritmalarının kullanımı

Diğer Hizmetler

- Zaman damgası verisinin işlenip detaylarının gösterilmesi

Milli Özellikler

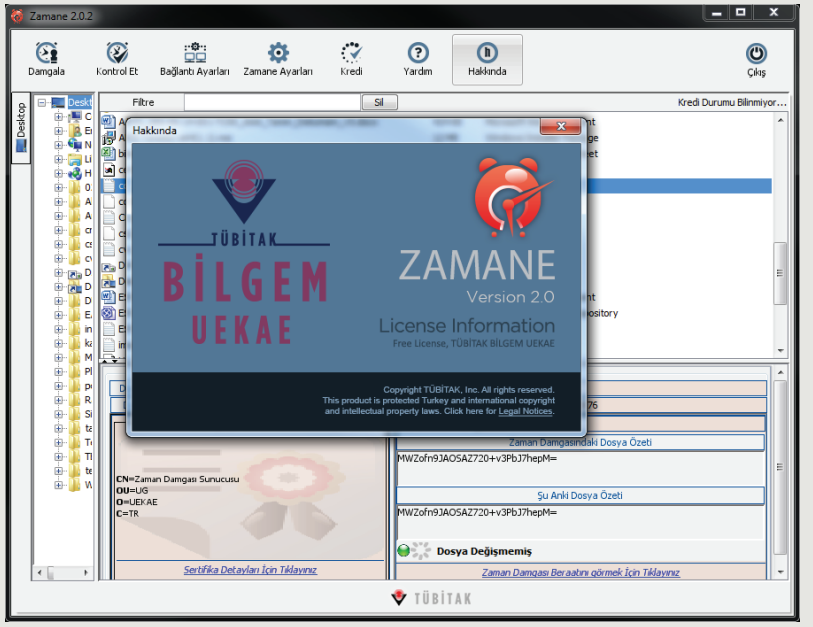
- Tüm yazılımlar TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiştir.

TÜBİTAK
BİLGEM

AÇIK ANAHTAR ALTYAPISI ARAÇLARI

ZAMANE

Zaman Damgası, elektronik verilerin belirtilen bir tarihte var olduğunu kanıtlamak amacıyla uluslararası bir standart ile tanımlanmış ve kanuni geçerliliği bulunan bir güvenlik protokolüdür. Zaman Damgası İstemcisi, zaman damgası alınmak istenen dosyanın özetini alarak zaman damgası isteği oluşturur ve bu isteği belirlenen bir zaman damgası sunucusuna gönderir. Sunucudan gelen zaman damgasının geçerliliğini kontrol edip doğrulayarak kaydeder. 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 alınması gereklidir. 5070 sayılı Elektronik İmza Kanununa göre Zaman Damgası, "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, melektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı" ifade eder.



Zamane Özellikleri

Zamane aşağıdaki özellikleri sunmaktadır:

- Damgalanmak istenen dosyanın özetini alarak zaman damgası isteği oluşturur ve bu isteği belirtilen zaman damgası sunucusuna gönderir.
- Gelen zaman damgasını damgalanmak istenen dosya ile eşleştirir ve zaman damgasının geçerliliğini kontrol eder.
- Geçmişte alınmış zaman damgalarının geçerliliğini kontrol edebilir.
- Politika dosyası kullanarak zaman damgası sunucusunun sertifikasını doğrulayabilir.
- Her türlü elektronik veri için zaman damgası isteği oluşturabilir.
- Vekil sunucusu (Proxy Server) kullanarak zaman damgası isteği gönderilebilir.
- Kullanıcılar için kredi (kontör) sorgulama özelliği sunulmaktadır.

Getirilen Çözümler

Gelişmiş Özet Algoritmaları Desteği

Zaman Damgası İstemcisi kullanılarak SHA-1 ve SHA-2 özet algoritmaları ailesinden istenilen biri seçilerek zaman damgası isteği oluşturulabilir.

Sertifika Doğrulama Desteği

Gelen zaman damgası cevabının geçerliliği doğrulanırken zaman damgasını imzalayan sertifika da doğrulanabilir.

Kullanıcı Dostu Arayüz

Kullanıcı alışkanlıklarını değiştirmeyen bir yaklaşımla hazırlanmış kolay anlaşılır kullanıcı dostu arayüze sahiptir.