Zamane Technical Specifications

Operating System

Windows 2000, Windows XP, Windows 2003, Windows Server 2008, Windows 7, Windows 8, Linux

Hardware Requirements

- Intel/AMD Processor
- Java 1.6 +

Supported Standards

- RFC 3161 (Internet X.509 PKI Timestamp Protocol)
- ETSI TS 102 023 Timestamp Authority Principle Requirements
- X.509 v3 Certificates
- X.509 v2 Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP)

Public Key Infrastructure (PKI) Services

- Control for certificate and certificate revocation list in verification process of timestamp
- Online Certificate Status Protocol Support

Basic Security Services

- Signing timestamps by using X.509 certificates and public key algorithms
- Verifying client identity by using PKCS 5

Certificate and Crypto Features

- RSA and ECDSA algorithms support for timestamp signature
- Use of AES encryption algorithms
- Use of SHA-1 and SHA-2 family of hash algorithms

Other Services

- Processing timestamp request and displaying details

National Features

- Developed by TÜBİTAK BİLGEM UEKAE

TÜBİTAK
BİLGEM

Electronic Certificate Management Infrastructure

Zamane

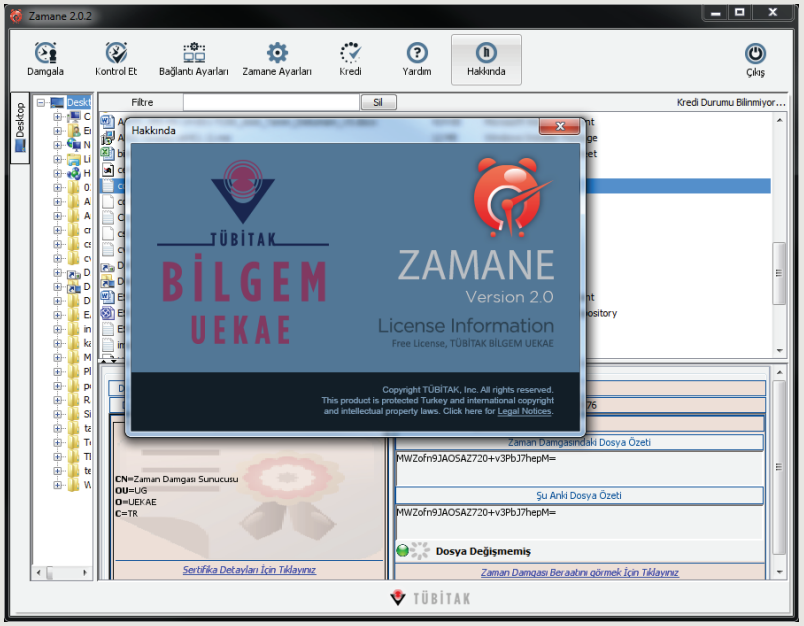
Timestamp is defined as a security protocol by international standards which provides legal proof of existence of a digital data at a particular time. Timestamp Client creates timestamp request by getting hash of the file to be timestamped and sends this request to a particular timestamp server. Afterwards it receives timestamp response from the server and stores to local file system after validation and verification processes. For digital data such as a signed agreement, a transaction or an application etc., proof of the existence for a particular time is very crucial for current e-trade and e-government applications. Nevertheless timestamp is required for varying kinds of digital data that need copyright including a new idea, photograph, model, drawing, research, formula or an algorithm.

According to the Turkish Electronic Signature Law published on January 15, 2004, Timestamp refers to a record verified with a secure electronic signature given by an authorized Electronic Certificate Service Providers in order to retain the exact time of creating, altering, sending, receiving or/and storing a digital data.

Timestamp Client Properties

Timestamp Client provides following features:

- Creates timestamp request by getting hash of the file and sends to the timestamp server.
- Checks received timestamp response with corresponding file and validate it.
- Validates timestamp responses taken before.
- Verifies the certificate of timestamp server by using a policy file.
- Creates timestamp requests for all kind of files or digital data.
- Connects to the server by using proxy on request.
- Users can request the remaining credits.



Solutions

Hash Algorithm Support

Timestamp Client provides the flexibility for timestamp requests to be created by any hash algorithm from SHA-1 and SHA-2 family.

Certificate Verification Support

In addition to validate receiving timestamp responses, timestamp client can verify the certificate of timestamp server.

User Friendly Interface

Timestamp Client comes with a user friendly interface that promotes ease of use.