Odyssey **ClockTix** is a robust, scalable, precision time stamping server that is fully standards compliant and issues time stamping tokens in accordance with RFC 3161 requests.

The need for Time Stamping

With most businesses occurring in the electronic form, constructing tamper-proof sequence of transaction events for audit trail can pave the way for many online professional services that would otherwise suffer from inadequate trust.

A time stamping server responds to requests for time stamping from clients. The data to be time stamped could be transactions, electronic documents, or digital signatures. Since the time stamping server is based on PKI technology, the time stamp is also digitally signed using the signing key of the server, thus providing tamper-proof evidence that a particular data existed before a specific time.

With a reliable time stamping server, the benefits are two-fold:

- The time stamping will help sequence and establish ownership of electronic documents and therefore ease the document verification process and other administrative tasks for agencies like the Income Tax, SEBI, RBI, etc.,

- The server can be set up as an independent Time Stamping Authority (TSA) for time stamping digital certificates. Normally, when the signing key of a CA certificate is revoked, all certificates signed by the CA become suspect. With an independent time stamping server attesting to the time a certificate was created and issued, it will be possible to distinguish between certificates issued before the CA signing key was revoked and those after, thus aiding long term verification of the certificates.

Odyssey ClockTix

Odyssey **ClockTix** is an all standards compliant, secure, scalable time stamping server that conforms to RFC 3161 specifications and can serve the time stamping needs of businesses, administrative agencies as well as commercial CAs.
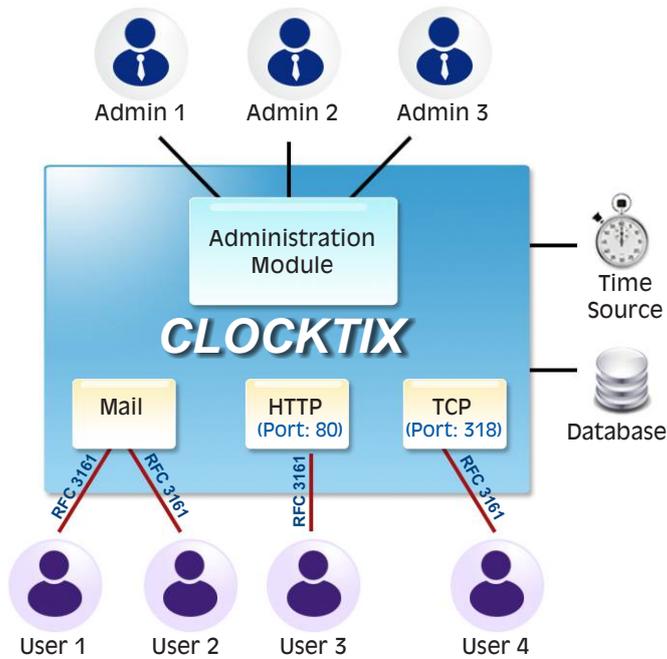
Feature Highlights

- Solution compliant with RFC 3161.
- Supports GPS, NTP and Atomic Clock.
- Supports three different transport mechanisms for time stamping request and response – E-mail, HTTP, TCP.
- Can be configured to be a universal root using a self-signed certificate or a certificate signed by another root CA for authenticating the time stamps.
- Supports signing key storage formats including PKCS #12 and M of N.
- Time stamping request includes only the digest of the data to be stamped and not the actual data itself.
- Web-based administration with client and server authenticated secure login.
- Supports a default SQLite engine for configuration and request data storage.
- Supports connecting to an external RDBMS for storing logs.

Value-Added Features

- Supports Hardware Security Module (HSM) for key security and management.
- Supports client interfaces including desktop applications, C and Java API, and web service components for connecting and obtaining time stamps over the web.

Platform Support

Processor	Operating System
(intel) AMD	Linux 64-bit

The solution can be combined with Odyssey Time Stamping Account Manager (TSAM), a versatile account management server that provides comprehensive client management including client registration, identification, authentication, and activity logging.

Standards Compliance

Standard	Description	Compliants
PKIX	Public Key Infrastructure Standards	Compliant
X509v3	Certificate Formats	Compliant
RFC 5280	X.509 V3 Certificate Profile	Compliant
PKCS #7	Cryptographic Message Syntax	Compliant
PKCS #9	Attribute Types	Compliant
PKCS #11	External Crypto modules like smart cards and HSMs	Supported and Compliant
PKCS #12	Private Keys and Certificates storage	Supported and Compliant
FIPS 180 -1	Private Keys and Certificates storage	Compliant
SSL	For secure channels	Supported
FIPS 180 -3	SHA-2 Digests	Compliant
RFC 1321	Md5 Digests	Compliant
Object Identifiers – OID standards	For Configuring Time-stamping Authority policy Id (if any)	Compliant
Support for key length up to 4096 bits (RSA)	N/A	Supported
ASN.1 (UTF-8 Encoding) and PEM	Certificate Storage Formats and Time stamping request/ response formats	Supported
Time Stamping Format	As per RFC 3161	Supported

ODYSSEY TECHNOLOGIES LTD.