KeyOne

Time Stamping Authority

Description

Electronic time-stamping is the only way to guarantee that a transaction occurred or an electronic document was signed at a given time. KeyOne TSA, the Safelayer secure time-stamping service, is designed to:

- Guarantee, objectively and precisely, the registering of the moment a transaction occurs
- Protect the time-stamp records
- Allow the connection, easily and securely, with the corporate control systems, minimizing installation and maintenance costs

Benefits

Maximum security

KeyOne TSA complies with the ETSI EN 319 421 “Protection Profile for trustworthy systems supporting time stamping” (replaces TS 102 023) and ETSI TS 319 422 “Time-stamping protocol and time-stamp profiles” (replaces TS 119 422 and TS 101 861) standards that define the requirements for qualified time-stamps in the eIDAS Regulation.

KeyOne products support defining the roles and events required to operate in compliance with the CEN TS 419 261 “Security Requirements for Trustworthy Systems Managing Certificates and Time-Stamps (replaces CWA14167-1). KeyOne TSA supports separation of roles between the security operator, system administrator and system auditor.

Reliability and control

The reliability of a TSA (Time Stamping Authority) registration system is vital for ensuring the traceability of the issued time-stamps and auditing their operation. The KeyOne registration mechanism incorporates a data protection system and an emergency system that ensures logs cannot be lost. KeyOne also supports selecting automatic events (with different levels of severity) and defining manual events (for registering actions that occur outside the application).

Maximum performance and scalability

Connected to cryptographic accelerators, KeyOne TSA meets the highest load requirements, can be integrated in high availability architectures and guarantees the fastest-possible transactional response times.

Easy to integrate and accounting

KeyOne TSA includes a workflow engine to define the interaction with information systems. It is possible to customize the system, incorporate new functions, connect to access-control systems and access internal information systems (to complement the information generated).

KeyOne
Time Stamping Authority

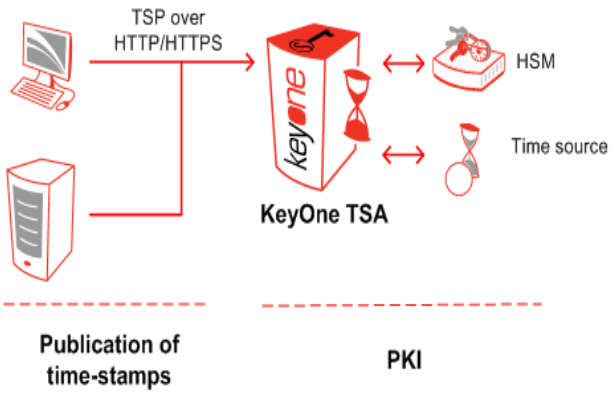
Functions

The main functions of KeyOne TSA are to:

- Receive time-stamp requests via the Internet from users and service providers that want to add time stamps to electronic documents or transactions.
- Generate a digitally-signed time-stamp that includes the time of the request; the information that securely binds the stamp to the electronic document; and a unique registration number for auditing purposes.
- Generate audit logs so operators can monitor the status of the system, its security and to what extent the corporate specifications are being met.
- Optionally, keep track of and limit each client's use of the OCSP service. To do this, KeyOne TSA assigns a service usage quota or restricts use for a specific time period (i.e., billing).

Architecture

The following figure illustrates the general architecture of KeyOne TSA and how it interrelates with the network components (under the IETF time-stamp protocol). KeyOne TSA can operate with a HSM (network or internal) and requires access to a database and a network time source (e.g., via NTP).



Technical Specifications

- **Time-stamp protocols:** IETF RFC 3161 and RFC 5816.
- **Time-stamp profile and policies:** ETSI EN 319 421 (replaces TS 102 023) and ETSI TS 319 422 (replaces TS 119 422 and TS 101 861).
- **Cryptographic devices:** RSA PKCS #11.
- **Connectivity:** SQL, LDAP/SLDAP, Microsoft Active Directory, HTTP/HTTPS, REST and SOAP Web Services, POP3 and SMTP.
- **Event monitoring:** SNMP v1, v2c and v3.
- **SIEM integration and audit:** Syslog protocol or Windows Event Log.

System Requirements

- **Operating systems:** Windows or Solaris SPARC.
- **SMTP mail server:** Recommended for implementing customized event notification.
- **Database systems:** Oracle, Microsoft SQL Server, MySQL or Maria DB.
- **Optional HSM:** Thales nCipher and SafeNet. Contact Safelayer to find out which models are homologated.
- **Time source:** Operating system time synchronized with an external source.

Safelayer Secure Communications S.A.
Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izquierda Ofi. B
28023 Madrid (Spain)
Tel. +34 917 080 480 Fax +34 913 076 652

www.safelayer.com
World Trade Center (Edif. Sud- 4ª Planta). Moll de Barcelona s/n
08039 Barcelona (Spain)
Tel. +34 935 088 090 Fax +34 935 088 091

SAFELAYER