Entrust Timestamping Authority (TSA)

On-premises timestamping server

Highlights

Digital timestamping proves that specific data existed from a given time, including documents and code. Entrust TSA (Timestamping Authority) is an on-premises server designed for the deployment of a service for:

- The generation of a proof when a document or code signature is applied or validated
- The verification of digital signatures after the certificate revocation or expiry
- The prevention of code rejection, ensuring that the signature was valid at the time of signing

Entrust TSA is easy to deploy and manage. It provides maximum security and trustworthiness for your document and code signatures.

FEATURES

- Based on the IETF RFC 3161 timestamp protocol standard, widely recognized by the industry
- Aligned with ETSI for qualified timestamps under the EU eIDAS Regulation
- Deploys timestamping services for executable use cases, proven for Microsoft and Java code signing.
- Monitors time source to prevent timestamp generation in case of time drift
- Manages one or more timestamping units (TSUs) from a single server
- Compatible with Entrust FIPS- and Common Criteria-certified HSMs, ensuring maximum private key protection
- Meets the highest load requirements and high transactional response times
- Delivered in virtual appliance format, including the OS and the management tools

Learn more about the Entrust Timestamping Authority at Entrust.com

Entrust Timestamping Authority

How it works

Functionality

Entrust TSA takes care of:

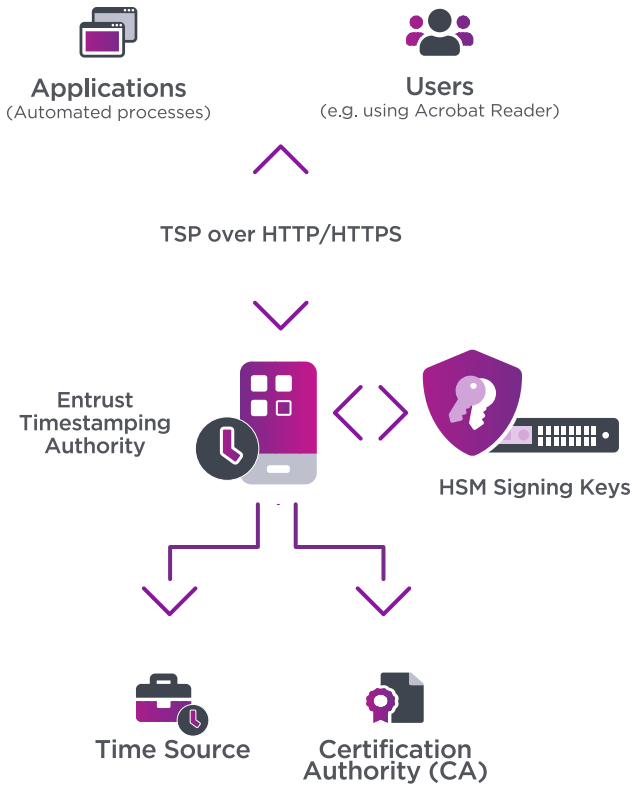
- Generating the timestamping units' key pairs in a hardware security module (HSM) and managing the certificates issued by the issuing certification authority (CA)
- Connecting with external time sources to detect time drifts or jumps out of synchronization with Universal Time Coordinated (UTC)
- Assigning timestamping policies, including hash algorithms, time accuracy information, and URLs for TSUs
- Receiving timestamp requests via the internet from users or applications that need to add timestamps to data
- Generating timestamp responses that include the time of the request and the information that securely binds the stamp to the data
- Generating logs so operators can monitor the status of the system, its security, and whether corporate specifications are being met
- Providing exportable logs to external systems for audit and archiving purposes

Architecture

The figure below illustrates the general architecture of Entrust TSA and how it interrelates with the network components (under the IETF RFC 3161 timestamp protocol).

Entrust TSA operates with external HSMs and requires connecting with one or more external NTP (Network Time Protocol) servers.

External CAs provide TSU certificates operated by Entrust TSA.



Learn more about the Entrust Timestamping Authority at Entrust.com

Entrust Timestamping Authority

TECHNICAL SPECIFICATIONS

- **Timestamp protocols:** IETF RFC 3161 and RFC 5816
- **Timestamp profile and policies:** Aligned with 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 approved by Entrust
- **Cryptographic algorithms:** RSA 2048, RSA 3072, RSA 4096, SHA-256, SHA-384, SHA-512, ECDSA P-256, ECDSA P-384, ECDSA P-521
- **Time synchronization:** Operating system's time synchronized with an external NTP source
- **Event monitoring:** Grafana dashboards, alerts, and Loki log display

SYSTEM REQUIREMENTS

- **Operating systems:** Entrust Deployment Manager on Linux
- **Hardware:** Physical machine or VMware (Nodes 4 cores with 8GB RAM); future versions: AWS, Azure
- **HSM support:** PKCS#11 devices approved by Entrust
- **Certification authority:** External CA, which provides TSU certificates operated by Entrust TSA
- **Time source:** Operating system's time synchronized with an external source; NTP required for compliance with ETSI EN 319 421
- **High availability:** Requires external load balancing
- **Log archiving:** EDM implements log rotation; logs can be pushed securely to external logging systems (e.g., Splunk, Graylog, etc.)

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223