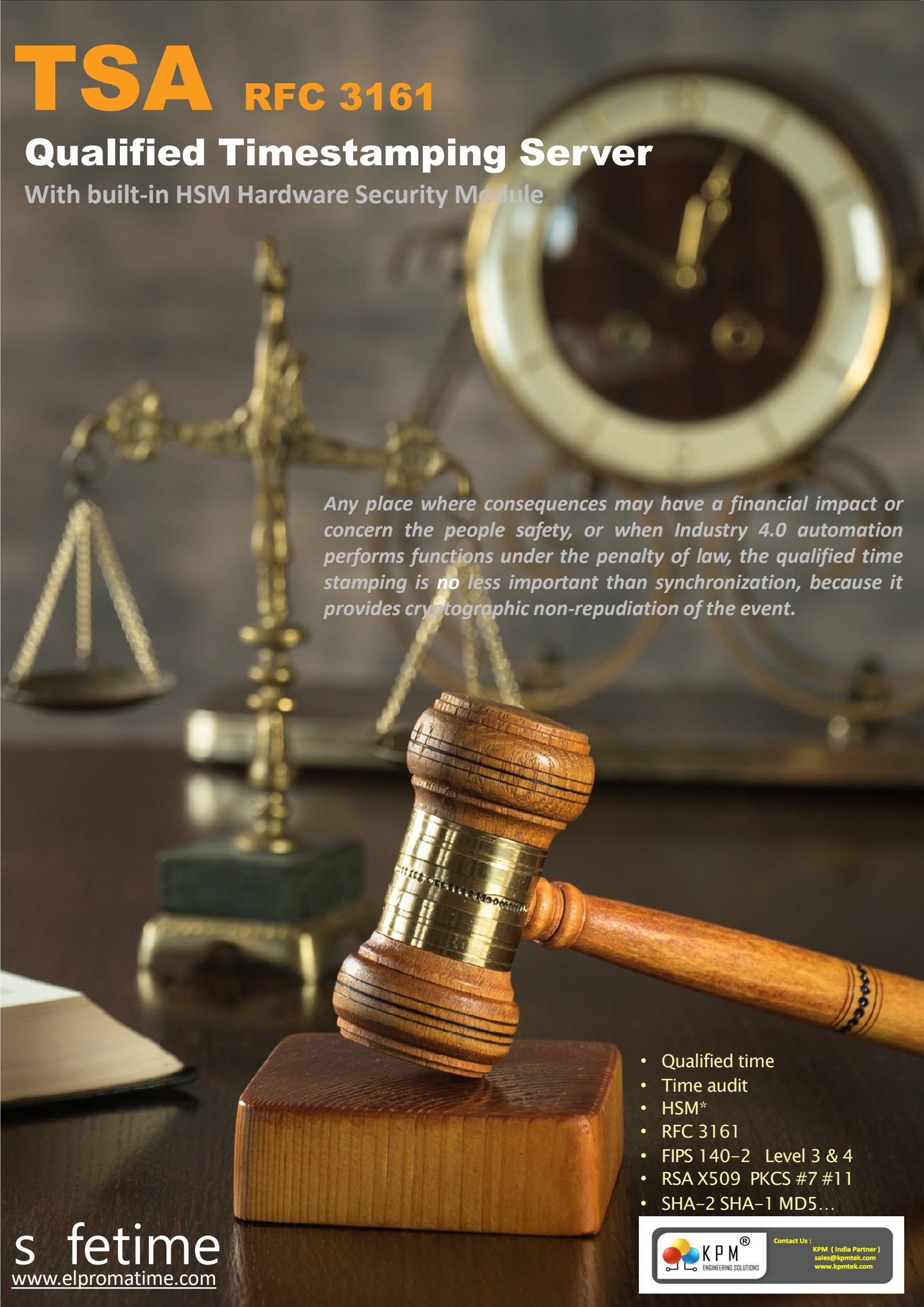
TSA RFC 3161

Qualified Timestamping Server

With built-in HSM Hardware Security Module



Any place where consequences may have a financial impact or concern the people safety, or when Industry 4.0 automation performs functions under the penalty of law, the qualified time stamping is no less important than synchronization, because it provides cryptographic non-repudiation of the event.

- Qualified time
- Time audit
- HSM*
- RFC 3161
- FIPS 140–2 Level 3 & 4
- RSA X509 PKCS #7 #11
- SHA–2 SHA–1 MD5…

s fetime

www.elpromatime.com

Elproma TSA ensures the tamper-proof creation and authenticity of timestamps. It is the ideal Hardware Security Module (HSM) network appliance for business applications that require proving the existence and status of a document or data at a specific point in time. The timestamp server (TSA) ensures that timestamped data is authentic for these and similar applications. Timestamps are able to verify at all times, whether or not the timestamped data matches the exact same form at the point in time it was logged by the timestamp. Furthermore, the timestamps (if survive over time longer than TSA) are still able to be verified without TSA authenticating for data (document file or data streaming):

1) *Originality of any document, video streaming, picture etc.*
2) *Integrity – say nothing can be changed since the moment of data sealing*
3) *Non-repudiation of chronology – proving existence in a moment of history*

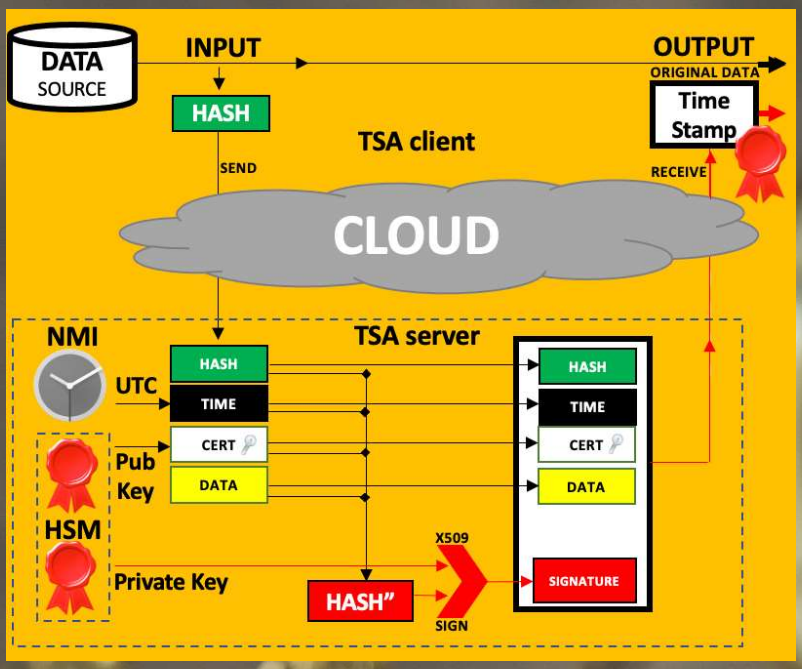
Fields of TSA application

- Long-term document archiving
- Electronic certification / e-signature
- Tender electronic platforms
- TAX authority software platforms
- Notary & legal software platforms
- Lottery, online betting & gaming
- Blockchain/tokens smart-contracts
- New crypto monetary systems, w/ limited time to spend money
- Pharma production labelling
- Global distribution of vaccines
- Global distribution of food, chemistry, water

Qualifeid Time is not less important than the power of RSA algorithm used by at TSA. Currently time from GNSS is very easy to manipulate providing false date & time inside timestamp. Following US directive EO13905 ref. time should be provided from NIST or National Institute of Metrology NMI.

safetime
www.elpromatime.com

PART #1 - The theory of timestamping operation. The process of the Qualified Time Stamping RFC3161 of any data starts on the client side, who forms on its basis a [HASH] fingerprint, which is a unique sequence of bytes that identifies the original data to prevent for non-repudiation. The calculation of the fingerprint HASH is performed using one of many available mathematical functions; e.g. SHA-256 or SHA-512 etc. From now, on any change, even a single bit of information in the originally data, will require the start of operations from the very beginning. This is so-called a "sealing" the information and it is a part of functionality recognized as property integrity of data. Therefore, until the full RFC3161 time stamp is received back from the TSA (Time Stamping Authority) server, the original client data should remain waiting in an undisturbed original form.



The [HASH] fingerprint is extended by additional information and sent through the network to TSA server. The sent stream length data is approximately a 500 bytes. It is send using HTTPS protocol. After receiving a request with [HASH] fingerprint from TSA client, the TSA server completes the received data, adding information about the reference UTC date & time [TIME]. To ensure the Qualified Time Stamping, the reference UTC should be supported from National Metrology Institute (NMI) using authenticated NTP or IEEE1588 protocol. The reference UTC time can also be taken from GNSS satellites under several restrictions. According to US directive EO13905, the GPS stays constantly at risk of jamming and spoofing attack and therefore using it for synchronization of critical infrastructures is requiring the traceability to UTC of NMI again. In case of USA this procedure is under responsibility of NIST. The next step the TSA adds the certificate with a public key [CERT] and the other extra [DATA], and the new fingerprint [HASH"] of the prepared response is computed. Finally the TSA reads a PRIVATE key from internal HSM (Hardware Secured Module) and it e-signs all prepared data [HASH] + [TIME] + [CERT] + [DATA] + [HASH"] creating the Qualified Time Stamp. The result is sent via network back to the client. The answer has about 1500 bytes and is stored by the client as a separate file together with original data file.

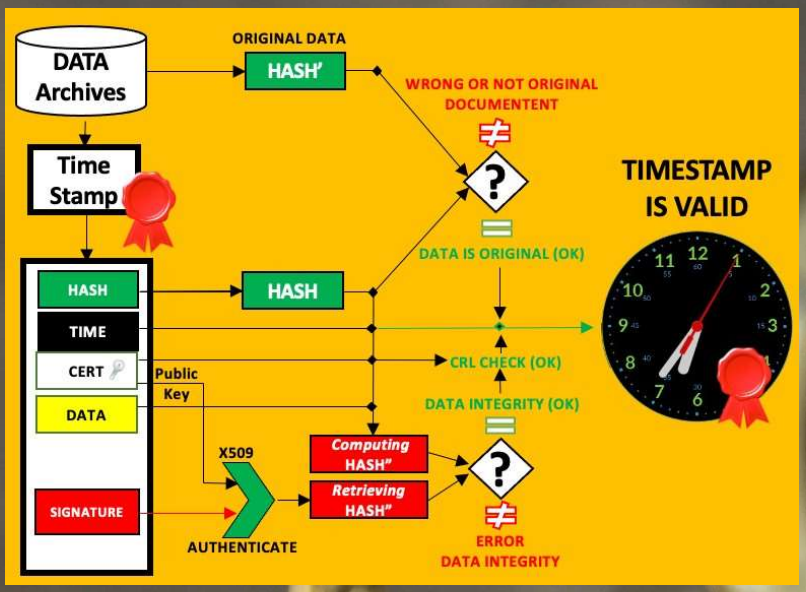
IMPORTANT NOTE - To avoid strong RSA cypher over false or tampered date & date the input UTC ref. should be traceable to National Institute of Metrology.

PART #2 – The theory of timestamp verification. The timestamp verification process may be executed at any time, even after many years, and the verification does not require a TSA server. For verification, the original document (file, picture, movie) and the timestamp file containing the certificate along with the public key are required.

The verification process includes testing of TSA identity (authentication) and the integrity of the timestamp data. It is done with the use of a TSA public key contained in the certificate [CERT].

Independently, the client computes (re-calculates) [HASH'] fingerprint from stored original timestamp data. If it matches (with the previously sent) retrieved [HASH"] one the TSA authentication and timestamp data integrity are preserved and reliable. Otherwise, an error is returned "ERROR DATA INTEGRITY".

Finally, there is the need to check if the verified time stamp refers to the original data (file), which is essentially the subject of the verification process. Therefore, the client re-calculates the new [HASH'] prime fingerprint code based on the archived, unchanged copy of the original data (file) and compares the result with the [HASH] code taken from the timestamp.



Only this match ensures that the timestamp and original file document correspond with each other. In this way, a complete verification is achieved based on PKI properties, TSA authentication, the integrity of the timestamp, the originality of the document and the stamp, as well as the non-repudiation that the document existed in a given form in a moment of history reliably specified by the timestamp.

IMPORTANT NOTE - The retrospective successful verification of TSA timestamp does not say anything about the performance or accuracy date & time. Therefore, it is recommended that you consider keeping additional LOG file archives containing information that can be used by auditors to prove the traceability of the UTC reference source of NMI.

safetime
www.elpromatime.com

Qualified Time and the problems with GNSS. Today the GPS satellite signal is still the most common source of time today. Since 1995, the civil industry has been gradually adopting GPS or other GNSS-based solutions dependent on it. Over time, the IT industry had so many receivers that they frequently has started to interfere with each other (due to active antennas). It also became difficult to manage such an extensive number of satellite receivers. First GPS-based synchronization anomalies appeared leading IT to failures. In an increasing number of cases, it turned out that correlated IT systems synchronized by two or more independent GPS receivers showed time discrepancies and therefore providing different RFC3161 timestamps too. It became to cause very serious problems.

The Jamming/Spoofing Attacks to GNSS. Moreover, except for European GALILEO, all other GNSS systems (GPS, GLONASS, BEIDOU, IRNSS) are military systems and, depending on the geopolitical situation, do not guarantee reception of their signals. The data received from the GNSS can also be easily manipulated to create false emissions on Earth. This is called spoofing. One can also jam the original satellite signal, with this being referred to as jamming, or retransmit it with an intentional delay (this is what makes it different from interference or signal reflections), the so-called meacooning. Today, GNSS signals in the industry are highly vulnerable to such manipulation and intentional cyber-attacks. There is an increasing number of attacks on entire industrial infrastructures and infrastructures of critical nature for countries.

Nowadays, synchronization is closely related to cybersecurity, because – instead of hacking into an internal network – it is simpler to destabilize the work of an entire IT structure by remotely disrupting the synchronization process. If the system is vulnerable to it, the rest of the destruction will practically follow by itself. Time manipulation can disrupt business, contracts, and the chronology of recorded events in LOGs of any system. In such a case, the chance to analyze errors and determine the cause of failure will irretrievably be lost. This provides ideal conditions for hackers diverting attention from the real cause of attack behind the failure. Nowadays, the entire cybersecurity paradigm has changed, and hacker attacks of "time synchronization attack" and "time delay attack" class are among the most likely and dangerous for the highly automated, GNSS-dependent industry.

Qualified Time reference is from NMI

To avoid strong RSA cypher over false or tampered date & time, the input ref. UTC should be provided from National Institute Of Metrology (NMI). The US directive **EU13905** points the NIST as supplier of UTC inside USA.

safetime
www.elpromatime.com

Technical Specification

Performance
- 4mln cryptographic timestamps per day (continue 24/7 operation 365days)
- 1800 timestamps per minute w/o HSM
- 180 timestamps per minute w/ HSM
- 1GbE Ethernet (Factory Default) 2x interface std.
- 10GbE, 25GbE, 40GbE, 100GbE NIC available as option*

Protocols
- RFC 3161 timestamp protocol via HTTP/HTTPS, TCP IPv4 & IPv6 network protocol
- PTP IEEE1588, NTP SNTP, Chrony synchronization protocols with MD5 authentication

Algorithms
- RSA, key length 2048, 4096, and optionally up to 8192* bits
- Hash algorithms SHA-1, SHA-256, SHA-512, MD5

Certificates
- X509 PKCS#11 and PKCS#7 TimestampServer certificate support

Security
- Integrated Hardware Security Module HSM
- FIPS 140-2 Level 3
- FIPS 140-2 Level 4
- Met ETSI specification TS102023

Qualified Time Support
- UTC with traceability to National Institute Of Metrology
- UTC from ELPROMA NTS-5000 Rubidium or Cesium
- DEMETRA* TSI#2 Audit & Verification Facility (option)

Mechanical
- 1U rack'19 mount chassis
- Redundant power supply 100-240 VAC (min. power 60W max power 300W*)
- Operating Temperature +10*C to +50*C (Storage -10*C to +60*C)
- Humidity up to 95%
- MTBF 300,000 hours at 25*C

ORDERING INFORMATION

Elproma TSA (factory default) incl. 2x 1GbE ETH
Elproma TSA-10GbE => std. + 10GbE Ethernet Network NIC
Elproma TSA-25GbE => std. + 25GbE Ethernet Network NIC
Elproma TSA-40GbE => std. + 40GbE Ethernet Network NIC
Elproma TSA-100GbE => std.+100GbE Ethernet Network NIC

safetime
www.elpromatime.com