ELPROMA ELEKTRONIKA

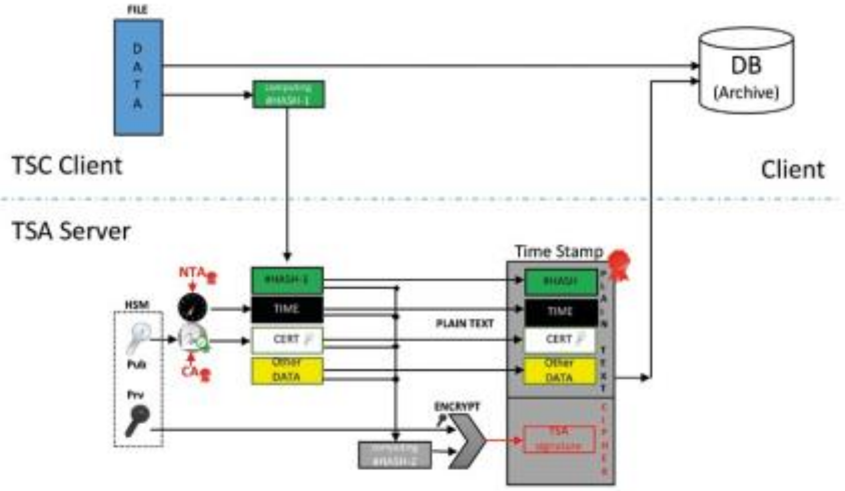
How RFC3161 Trusted Time Stamping works

Stamping files

The process of the Trusted Time Stamping of any file format (e.g. system LOG) starts on the client side, who forms on its basis a fingerprint, which is a unique sequence of bytes that identifies the original data stream included in input file (marked on right side picture "HASH-1 computing"). The calculation of the fingerprint (HASH-1) file is performed using one of many available mathematical functions; e.g. SHA-1, SHA-256 or SHA-512 etc. The most common and therefore best compatible one is SHA-1. From now on, any change, even a single bit of information in the originally labelled data (original file), will require the start of operations from the very beginning. This is so-called "sealing information" and it is a part of functionality recognized as property "DATA integrity". Therefore, until the full RFC3161 time stamp is received back from the TSA server (*Time Stamping Server Authority*), the original data should remain in an undisturbed original form. The fingerprint (HASH-1) is extended by additional information and sent through the network to TSA. The sent stream length is approximately a 500 bytes.

After receiving a request from client, the TSA completes the received data, adding information about the time and date (TIME), a cryptographic certificate with a TSAs public key (CERT), and the new fingerprint (HASH-2) of the prepared response is computed. The result is signed with TSA private key (according to PKI algorithms) and 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.

Except for PDF, all other file formats require RFC3161 time stamp to be stored in the separate file. The PDF format is exception. It includes special extra internal descriptors in accordance with RFC3161 reference, allowing in a very elegant way to store both (the original document and a timestamp) in a single PDF output file.



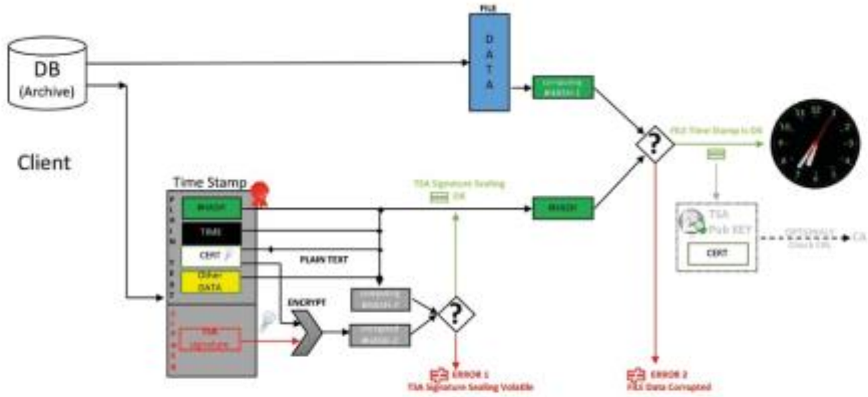
Verification of the Time Stamp

The 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 and the time stamp file containing the certificate along with the TSA public key are required.

The verification process includes testing of TSA identity (authentication) and the integrity of the time stamp data (integrity). It is done with the use of a TSA public key contained in the certificate (CERT) that is sent in the stamp to client. Independently, the client re-checks and re-calculates the HASH-2 fingerprint code. If it matches (with the previously sent HASH-2 code) the TSA authentication and data integrity of the stamp are preserved and reliable. Otherwise, an error is returned.

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 HASH-1 fingerprint code based on the archived copy of the original data and compares the result with the HASH-1 code taken from the stamp, which is calculated while preparing the request to TSA. Only this match ensures that the stamp 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 time stamp.

September 2016 ELPROMA


DB
(Archive)
Client
FILE
DATA
computing #HASH-1
FILE Time Stamp is OK
Time Stamp
#HASH
TIME
CERT
Other DATA
PLAIN TEXT
TSA Signature Sealing OK
#HASH
ENCRYPT
computing #HASH-2
computing #HASH-2
TSA signature
TSA Pub KEY
CERT
OPTIONALLY Check CRL
CA
ERROR 1
TSA Signature Sealing Volatile
ERROR 2
FILE Data Corrupted