Certified timestamping of archived email with RFC3161

What is Certified Timestamping

Certified Timestamping, or Trusted Timestamping, is a standard to prove the existence of data at a specific time and to verify it's integrity. RFC 3161 is an open and widespread implementation of this process.

By applying a certified timestamp the Libraesva Email Archiver also certifies the integrity of the email. Any modification of the email content invalidates the signature and the certified timestamp provides legal proof of authenticity and integrity for each email.

Timestamps are automatically applied by the Libraesva Email Archiver to every archived email. No configuration is needed, this is a feature that is provided out of the box by every Libraesva Email Archiver appliance.

How is it implemented in the Libraesva Email Archiver

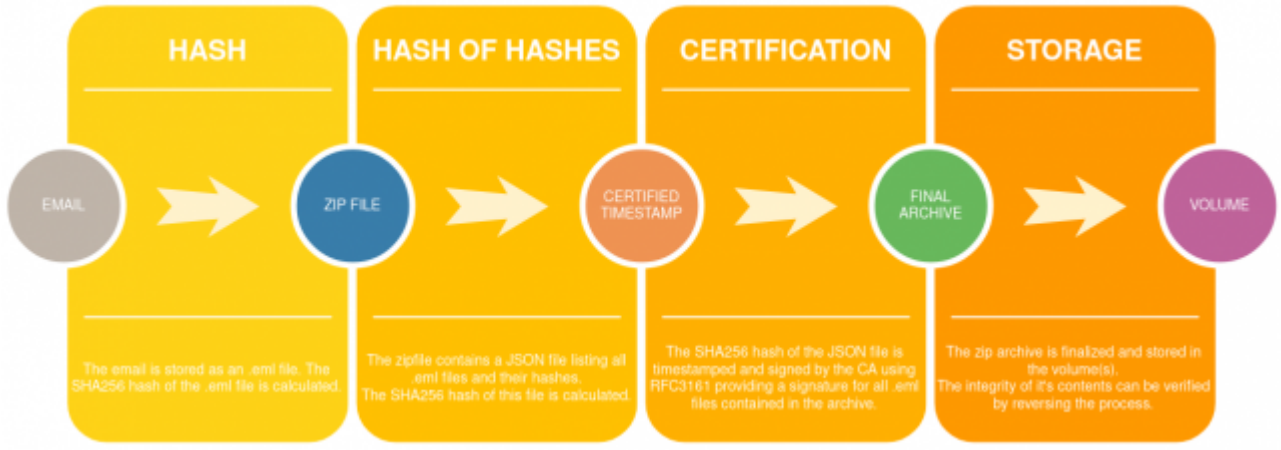
In the Libraesva Email Archiver emails are stored as .eml files contained within a zip file. The .eml file guarantees that the email is stored without any modification, ensuring maximum compliance. The zip container provides compression and de-duplication without any data loss.

The use of common and widespread standards (.eml and .zip) for storing email guarantees that the archived email can be read and recovered at any time in the future even without our software. Moreover, the .eml files contain, through the use of extra-headers added by the archiver, all the information needed in order to completely rebuild the email index.

For every .eml file a SHA256 hash is calculated. A JSON file, also contained in the .zip file, lists all the .eml files and their hashes. The SHA256 hash for this json file is calculated and this is the hash that is timestamped and signed in compliance with RFC 3161. The signature is also added to the .zip file, which is then finalized and stored.

This process guarantees that all the .eml files contained in the .zip archive are timestamped and signed. Given that a .zip file can contain up to 4000 .eml files (or 512MB of cumulative

email size), a single signature is needed for up to 4000 emails. Bundling signatures in this way improves both performance and costs related to the timestamping.



How and when the certified timestamp is verified?

The process can be reversed for verification: the SHA256 file of the JSON file is calculated and the certified timestamp verified. In turn, every .eml file can be hashed and it’s hash verified against the content of the JSON file. Using an open standard like RFC 3161 ensures that the verification process can be performed by independent parties with their tools of choice.

The Libraesva Email Archiver automatically and transparently performs this verification process every time an email is read. The user interface shows the result of the verification process to the user.

What Timestamping Authority (TSA) provides the signature?

The Libraesva Email Archiver contains it’s own Certification Authority that acts as the TSA for the certified timestamping. This internal CA is automatically initialized upon installation and it’s use requires no configuration.

The internal CA provides the timestamping for no additional cost. Any external TSA compliant

with RFC 3161 can be used, should you prefer to use an external TSA.