FreeTSA (www.freetsa.org) Certification Practice Statement

Trusted timestamping is the process of securely keeping track of the creation and modification times of a document. Security here means that no one - not even the owner of the document - should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.

FreeTSA trusted timestamping Software as a Service (SaaS) provides an easy method to apply RFC 3161 trusted timestamps to time-sensitive transactions through independently verified and auditable date and UTC (Coordinated Universal Time) sources.

- Homepage: https://www.freetsa.org

- FreeTSA CA Primary Root Certificate: https://freetsa.org/files/cacert.pem
- Timestamping (TSA) Certificate: https://freetsa.org/files/tsa.crt

- FreeTSA - Guide / Tips: https://freetsa.org/guide

For multiple files, the general concept is that timestamping a single file that contains an aggregate list of fingerprints of other files, also proves that these other files must have existed before the aggregate file was created, provided that both the aggregate file and the referenced file are available during verification process. Freetsa also offers the possibility of URLs timestamps (do not abuse).
If you are interested in implementing timestamps on your project / company using the FreeTSA service, you can contact me for specific requirements. Freetsa can also be used within the Tor anonymity network.

Web online Signature: The files are NEVER uploaded to the FreeTSA server, the browser generates a hash (TSR) and FreeTSA signs it. FreeTSA respects the user's privacy 100%.

Request Digest: md4 / md5 / rmd160 / sha / sha1 / sha224 / sha256 / sha384 / sha512.

Freetsa TSA Certificate: tsa.crt
Key modulus (sha256): 899ba3d9f777e2a74bdd34302bc06cb3f7a46ac1f565ee128f79fd5dab99d68b

Freetsa CA Certificate: cacert.pem
Key modulus (sha256): a4b1a0a81aef68be1cc985d0f83bd6539cfe84174587f900e15ffe3f65433056

Service availability: All certificate status services are made available at all times (24x7x365) if possible.

Intellectual property rights.

Certificate and revocation information are the property of FreTSA.
Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

Disclosure pursuant to judicial or administrative process.

FreeTSA may not disclose personal information if compelled to do so by court order or other compulsory legal process because freetsa does not request or save information.

Revocation information for all certificates is made available via OCSP / CRL. OCSP / CRL responses are available at all times (24x7x365) if possible.

- OCSP profile: http://www.freetsa.org:2560
- CRL: https://www.freetsa.org/crl/root_ca.crl

Version number(s): All certificates use X.509 version 3.

Freetsa implements reasonable network security safeguards and controls to prevent unauthorized access to CA systems and infrastructure. FreeTSA network is multi-tiered and utilizes the principle of defense in depth. Firewalls and other critical CA systems are configured based on a necessary-traffic-only whitelisting policy whenever possible.

Contact person: busilezas@gmail.com