

# How to independently verify Certified timestamping of archived email with RFC3161

Welcome to our comprehensive knowledge base, where we provide a detailed guide on how to independently verify the certified timestamping of archived emails using RFC3161.

## Prerequisites

- sha256sum and openssl installed
- To obtain the Archiver CA certificate, follow these simple steps:
  - Access your Archiver account and navigate to the menu: **Archiver > Compliance > Certified Timestamp**.
  - Look for the option labeled “**Download CA certificate**” and click on it.
  - Once you click the button, you will instantly receive your Archiver CA certificate in the form of a file named “**cert.pem**”.
- Download archive file (zip format) containing email to verify from volumes page: **Archiver > Storage > Volume**.

## Validation steps

1. Upon extracting the archive file contents, (**Note:** If tenant is encrypted you must use “Tenant encryption key” as extraction parameter), you’ll obtain the following files:
  1. signature (Openssl signature file)
  2. signature.json (hash list of each EML signed)
  3. list of EML files signed
2. Calculate “signature.json” HASH with sha256, obtaining signature file sha256 hash.  
ex: `sha256sum signature.json`
3. Verify signature with command:

```
openssl ts -verify -digest SIGNATURE_JSON_HASH_RESULT -sha256 -  
in SIGNATURE_FILE -CAfile cert.pem  
ex:openssl ts -verify -digest  
'02e40e87e86c71f22e68cd4213a3f7a4a1ee04de00dcffc94cac549f5ddd714  
d' -sha256 -in signature -CAfile cert.pem
```

4. IF response indicates “**Verification: OK**” it means that the JSON signature validation has been successfully verified and you can continue with validation procedure.

5. Calculate EML file hash with sha256, obtaining EML sha256 hash.

```
ex: sha256sum 9.eml
```

6. Retrieve the EML JSON hash from the signature.json file, where “filename” represent EML file name and “hash” is its related EML hash

```
... {  
  "filename": "9.eml",  
  "hash":  
    "e38d0fbcd9ad059ee85f37ee5342ebc2db35cb3cf63a746e98043b6ed4374d  
0"  
}...
```

7. Compare signature.json HASH (step 6) with calculated EML HASH (step 5).  
If two hashes are identical, it indicates a **SUCCESSFUL** validation of your EML file.