THE DECALOGUE OF TIMESTAMPING

Version 1.0

1. What is timestamping and why should I use it?

Timestamping is used to specify the time when a digital signature was made. This is needed to properly validate the signature. If the signature timestamp is present, the application that validates (verifies) the signature will check whether the certificates involved in the signature validation were valid at the time of signing. If there's no timestamp for the signature, the certificate validity is checked for the time of the signature validation, which is not always acceptable.

Example:

- The certificate is valid from: 1st of January, 2019 to 31th of December, 2019
- The signature was made on: 5th of December, 2019 and verified on 6th of April, 2020

With timestamp: The signature is OK.

Without timestamp: The signature is not valid.

As you know, the certificate is not eternal. If you use a certificate that has expired to sign the data, such a signature will not be accepted as valid. If the signature validator finds a timestamp, the validator will know when the signature was made and will check if the certificate was valid at that moment in time. If there's no timestamp, **then nobody knows when the signature was made**, and it's assumed that it could have been made at any moment in time, possibly after the certificate had expired.

2. What key properties does Timestamping provide?

Legal properties
From a legal point of view, the accuracy of the date and time in a qualified time stamp and the integrity of the corresponding time stamped data are legally presumed and recognised as such all over the EU.

Security properties
The accuracy of the date and the time indicated in a qualified time stamp is ensured.

Data integrity
The integrity of the data to which the date and time are bound in a qualified time stamp is ensured via the hash value and the signature/seal on the time stamp. In other words, it is guaranteed that any alteration to the time stamped data can be detected.

Functional properties
From a functional point of view, a qualified electronic time stamp is a kind of time attestation in electronic form which binds whatever kind of electronic data to a particular time establishing evidence that the latter data existed at that time.

Identification of the qualified time stamp provider
Furthermore, the qualified time stamp itself:
- Allows the identification of the qualified trust service provider to which it is uniquely linked, and
- Is also protected for integrity as the time stamp is signed/sealed in such a way that any subsequent change in the time stamp itself is detectable. The QTSP name, its postal and electronic address can in fine be found in the national trusted list when validating the qualified status of the time stamp and of its provider.

3. What properties can Timestamping **not** provide?

No prevention of document alteration
While a qualified time stamp guarantees that any alteration to the time stamped data can be detected, it provides no guarantee that such alteration will not happen.

Confidentiality
A qualified time stamp provides no guarantee that the time stamped data will remain confidential when sent over to recipients. There is however no need to disclose the data to be time stamped towards the time stamp provider as the time stamp request is only including a **hash value** of that data.

No proof of sending/receipt
The qualified time stamp provides no guarantee that the time stamped document has been effectively sent to a certain recipient or has been received by a certain recipient. .

No proof of origin on the time stamped data
The qualified time stamp provides no guarantee that the time stamped document origins from a certain party (no p roof of origin of the document).
Note: For obtaining a proof of origin on the time stamped data, a user should create a qualified electronic signature as a natural person (or qualified electronic seal as a legal person) as such signature (seal) may be combined with the use of qualified time stamp.

No signing or content commitment on time stamped data
The qualified time stamp provides no guarantee that the document owner or time stamp requester is clearly identified.The time stamp is not a signature from the document owner and does not bear itself any commitment on the content of the time stamped document (no electronic signature of the document).
Note: For obtaining a proof of commitment on time stamped data, qualified time stamps may be combined with qualified electronic signatures not only to time stamp the data but to sign it as well.

4. Is always necessary to use Timestamping?

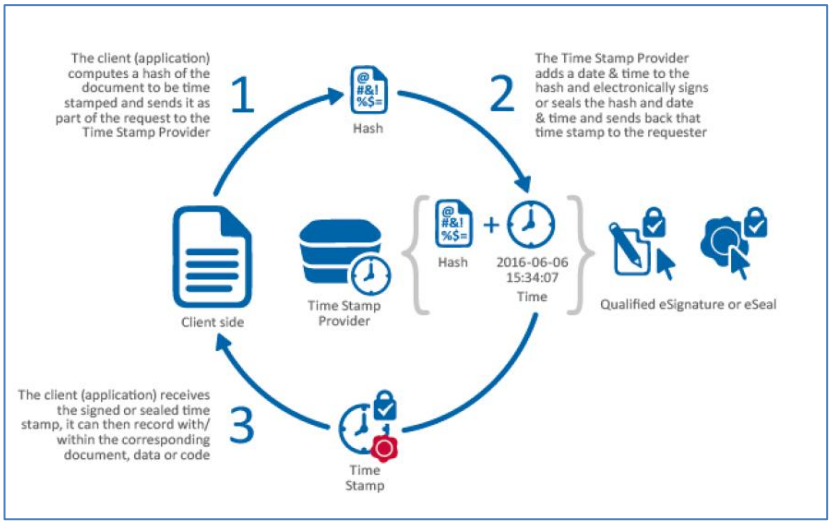
No. Timestamping is not necessary when you, for example, send a short signed note to a colleague and this note is expected to be read and disposed of the same day as it has been written. On the other hand, timestamping is a must when you create signed documents for wide distribution or for long-term storage and archival purposes. If the signature is supposed to be used (to prove the authenticity of the document author or data originator) longer than one or several days, then timestamping should be used.

5. How does timestamping work?

The European Union has provided a very comprehensive set of requirements to control the use of qualified electronic timestamps under the eIDAS. This is the EU Regulation No. 910/2014. Of course, Athens Stock Exchange is a Certification Service Provider (CSP) registered in the Trusted List (http://tlbrowser.tsl.website/tools/index.jsp) of the Registered Certification-Service Providers established in Greece, having filled a compliance report, according to the above regulation. ATHEX TSA certificates are issued by Athex Qualified Timestamping Authority (https://webgate.ec.europa.eu/tl-browser/#/tl/EL/2/3).

Timestamping involves your **electronic signed data** as a timestamping client and a timestamping server called the Timestamping Authority (**TSA**).

1. The hash of the data signature is calculated. This hash is sent to the **ATHEX TSA** for signing.
2. The ATHEX TSA signs the received hash using its TSA certificate and includes the current time on the server in this signature.
3. The signature made by the ATHEX TSA is sent back to your code and your code adds this signature to the original signature made over the initial data.



Note: The ATHEX TSA provides time with ±1 second of UTC by calibration with multiple independent time sources including GPS and National Measurement Institutes providing UTC time. "Coordinated Universal Time" or "UTC" means the time scale, based on the second, as defined by the International Telecommunications Radio Committee (ITU-R) TF.460-5 and roughly corresponding to Greenwich Mean Time (GMT).

6. Can the timestamp itself be canceled or become invalid?

If the timestamping certificate is revoked (claimed as invalid by the CA that has issued it), there are two cases possible, as per sections 4.1 and 4.2 of RFC 3161:

1. If the revocation reason code indicates that the key has not been compromised but the TSA itself will not be operating in the future, then the timestamping certificate should not be used for timestamping in the future (after revocation). Previously made timestamps, however, don't become invalid.
2. If the revocation reason code indicates code compromise, then all timestamps signed with the compromised certificate become invalid

7. Does the timestamp expire?

The timestamp itself doesn't expire. However, the timestamp is signed with a certificate issued for the specific purpose of signing timestamps. This certificate has its own expiration time and validity period. As soon as the certificate used to sign a timestamp expires, the timestamp expires as well. As per section 4.3 of RFC 3161, such a timestamp should be redone or notarized to renew the existing trust in the timestamp.

8. So, which conditions a digital signature is valid in?

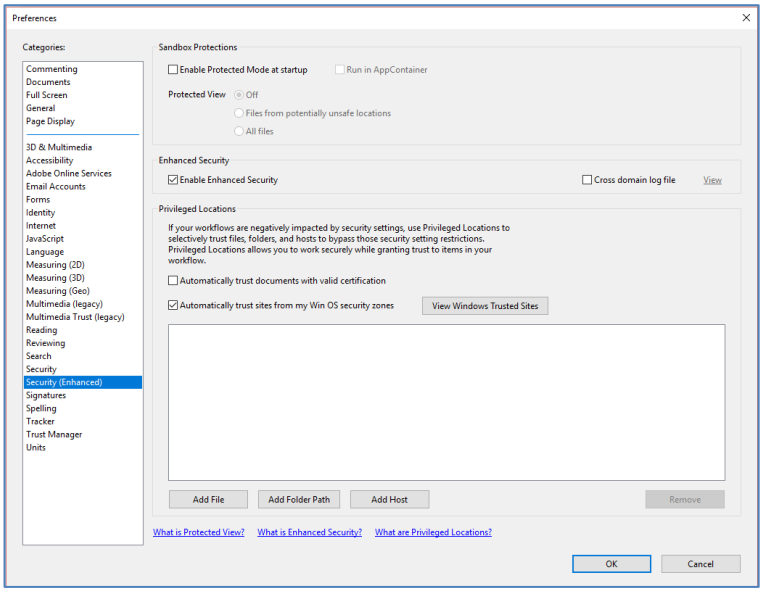
Quick table that shows signature validation status under all below described conditions.

	Simple signature	**Timestamped signature**
Signing certificate (or certificate chain) is valid and not revoked	✅	✅
Signing certificate (or certificate chain) is valid and is revoked before signing	❌	❌
Signing certificate (or certificate chain) is valid and is revoked after signing	❌	✅
Signing certificate (or certificate chain) is expired after signing	❌	✅
Timestamping certificate (or certificate chain) is revoked before signing	**N/A**	❌
Timestamping certificate (or certificate chain) is revoked with **Key Compromise** reason	**N/A**	❌
Timestamping certificate (or certificate chain) is revoked with any other reason after signing	**N/A**	✅
Timestamping certificate (or certificate chain) is revoked with any other reason before signing	**N/A**	❌
Timestamping certificate (or certificate chain) is expired after signing	**N/A**	✅

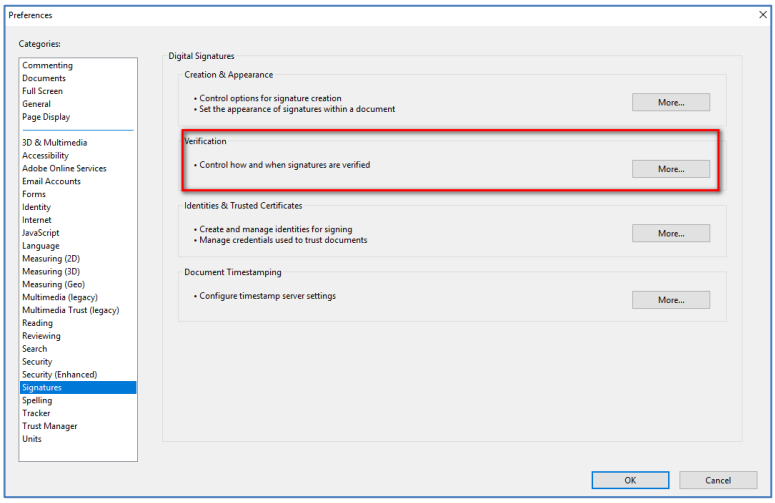
as you see there is only one case when simple signature remains valid — while the certificate is time valid and is not revoked. In all other cases the signature will become invalid. But timestamped signature remains considered as a valid even if all certificates in the signing and timestamping chains are expired. Therefore **you should timestamp your signatures each time you sign something as it is possible**

9. How to configure ATHEX Time Stamp Server to Acrobat Reader?

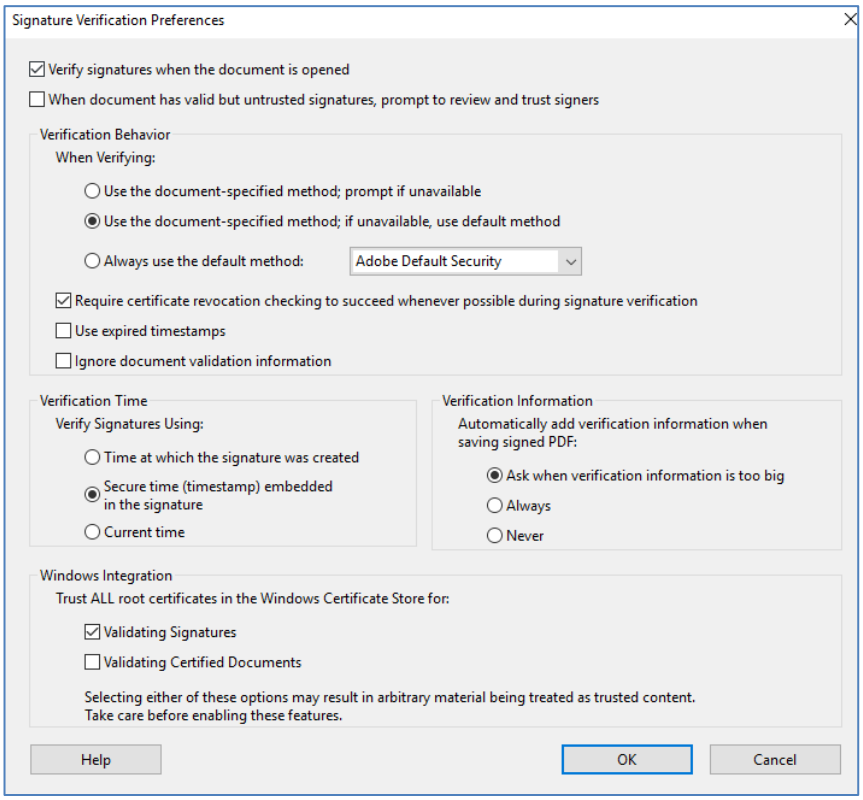
- Install ATHEX_TSA Certificate
- Open Adobe Reader
- From menu bar choose **Edit**
- Open the **Preferences** dialog box.
- Under **Categories**, select **Security (Enhanced) ,uncheck the Enable Protected Mode at startup**



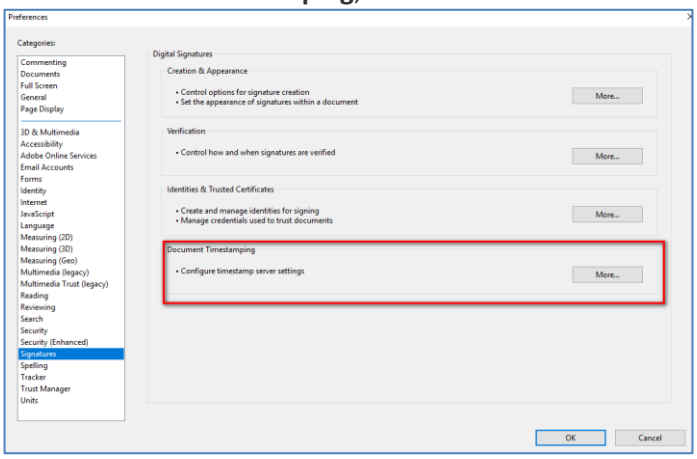
- Click OK
- Under **Categories**, select **Signatures**.
- For **Verification**, click **more**.



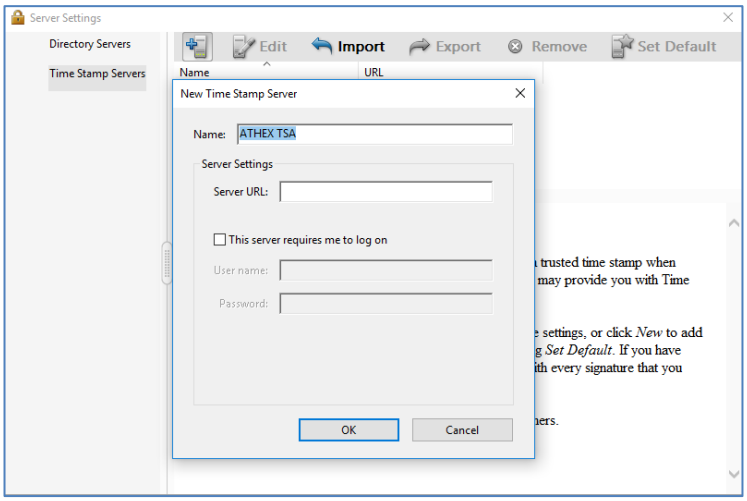
- Enable (check) the below preferences according to the picture.



- Click OK.
  - Open the **Preferences** dialog box.
  - Under **Categories**, select **Signatures**.
  - For **Document Timestamping**, click **more**.



  - Select **Time Stamp Servers** on the left
  - Click the **New** button  . Type ATHEX TSA in the Name



- Add ATHEX's URL and type it for the timestamp server, and then click **OK**.
- Select Time Stamp Servers on the left.
- Select the ATHEX TSA timestamp server, and click the **Set Default** button .
- Click **OK** to confirm your selection
- Restart Adobe Acrobat Reader .

10. What is ATHEX's TSA URL?

The use of the Athex Time-Stamping service signifies that you should be a subscriber acknowledging that you agree and accept the terms and conditions contained in a contract agreement.

For more information about please contact

http://www.athexgroup.gr/web/guest/digital-certificates-contact-info