



ATHEXGROUP
Όμιλος Χρηματιστηρίου Αθηνών

Ο ΔΕΚΑΛΟΓΟΣ ΤΗΣ ΧΡΟΝΟΣΗΜΑΝΣΗΣ



Version 1.0



1. Τι είναι η Χρονοσημανση και γιατί είναι απαραίτητη ;

Η χρονοσημανση χρησιμοποιείται για να καθορίσει την ώρα που δημιουργήθηκε μια ψηφιακή υπογραφή. Αυτό είναι απαραίτητο για την ορθή επικύρωση της υπογραφής. Εάν η ψηφιακή υπογραφή φέρει επιπλέον και χρονική σήμανση τότε, η εφαρμογή που επικυρώνει (επαληθεύει) την υπογραφή θα ελέγξει αν τα πιστοποιητικά που εμπλέκονται στην επικύρωση υπογραφής ήταν έγκυρα κατά τη στιγμή της υπογραφής. Αν δεν υπάρχει χρονική σφραγίδα για την υπογραφή, η εγκυρότητα του πιστοποιητικού ελέγχεται για την ώρα της επικύρωσης υπογραφής, η οποία δεν είναι πάντοτε αποδεκτή.

Παράδειγμα:

- Το πιστοποιητικό ισχύει από : 1η Ιανουαρίου, 2019 έως 31 Δεκεμβρίου, 2019
- Η υπογραφή δημιουργήθηκε την : 5η Δεκεμβρίου 2019
- Η υπογραφή επαληθεύτηκε την : 6η Απριλίου 2020

Με Χρονοσημανση : Η υπογραφή είναι έγκυρη την 6/4/2020
Χωρίς Χρονοσημανση : Η υπογραφή δεν είναι έγκυρη την 6/4/2020

Είναι γνωστό ότι, κανένα πιστοποιητικό δεν είναι αιώνιο. Εάν χρησιμοποιείτε πιστοποιητικό που έχει λήξει για την υπογραφή των δεδομένων σας, η υπογραφή αυτή δεν θα γίνει αποδεκτή ως έγκυρη. Εάν η εφαρμογή επικύρωσης υπογραφής εντοπίζει χρονοσημανση, γνωρίζει τότε δημιουργήθηκε η υπογραφή και θα ελέγξει εάν το πιστοποιητικό ήταν έγκυρο εκείνη τη χρονική στιγμή. Αν δεν υπάρχει χρονική σήμανση, τότε κανείς δεν ξέρει τότε δημιουργήθηκε η υπογραφή και υποτίθεται ότι θα μπορούσε να γίνει οποιαδήποτε στιγμή, πιθανώς ακόμα και μετά τη λήξη του πιστοποιητικού.

2. Τι μπορεί να μας εξασφαλίσει η Χρονοσημανση ;

Νομικές ιδιότητες

Από νομικής απόψεως, η ακρίβεια της ημερομηνίας και ώρας μιας αναγνωρισμένης χρονοσφραγίδας καθώς και η ακεραιότητα των αντίστοιχων χρονοσφραγισμένων δεδομένων θεωρούνται νομικώς αkéραια και αναγνωρίζονται ως τέτοια σε όλη την ΕΕ.

Ιδιότητες ασφαλείας

Η ακρίβεια της ημερομηνίας και της ώρας που αναφέρονται σε μια αναγνωρισμένη χρονική σφραγίδα θεωρούνται δεδομένα και είναι εξασφαλισμένα

Ακεραιότητα δεδομένων

Η ακεραιότητα των δεδομένων τα οποία δεσμεύονται με την ημερομηνία και ώρα μιας αναγνωρισμένης χρονικής σφραγίδας εξασφαλίζεται μέσω της τιμής κατακερματισμού αυτών (hash value data) και της υπογραφής / σφραγίδας της ίδιας της χρονικής σφραγίδας. Με άλλα λόγια, είναι εγγυημένο ότι μπορεί να ανιχνευθεί οποιαδήποτε μεταβολή στα δεδομένα με την χρήση της χρονικής σφραγίδας.

Λειτουργικές ιδιότητες

Από λειτουργικής απόψεως, μια ηλεκτρονική χρονική σφραγίδα είναι ένα είδος χρονικής βεβαίωσης σε ηλεκτρονική μορφή που δεσμεύει οποιοδήποτε είδος ηλεκτρονικών δεδομένων σε μια συγκεκριμένη χρονική στιγμή που αποδεικνύει ότι τα δεδομένα αυτά υπήρχαν εκείνη την περίοδο.

Αναγνώριση του κατάλληλου Παρόχου Χρονικής Σήμανσης (QTSP)

Η αναγνωρισμένη χρονική σφραγίδα επιπλέον, επιτρέπει τον εντοπισμό του Αναγνωρισμένου Παρόχου Υπηρεσιών Εμπιστοσύνης με τον οποίο συνδέεται αποκλειστικά και επίσης εξασφαλίζεται η ακεραιότητας της καθώς είναι υπογεγραμμένη / σφραγισμένη κατά τέτοιο τρόπο ώστε να είναι ανιχνεύσιμη οποιαδήποτε μεταγενέστερη αλλαγή της ίδιας της χρονικής σφραγίδας. Η επωνυμία του QTSP, η ταχυδρομική και ηλεκτρονική του διεύθυνση μπορούν να βρεθούν στην Εθνική Έμπιστη Λίστα (EETT) κατά την επικύρωση της κατάστασης της χρονικής σφραγίδας (qualified status of the time stamp) και του παρόχου της.



3. Τι ΔΕΝ μπορεί να μας εξασφαλίσει η Χρονοσημανση;

Δεν υπάρχει πρόληψη στην αλλαγή περιεχομένου των εγγράφων

Παρόλο που σε μια αναγνωρισμένη χρονική σφραγίδα εγγυάται ότι μπορεί να εντοπιστεί οποιαδήποτε μεταβολή στα δεδομένα που φέρουν χρονική σφραγίδα, δεν παρέχει καμία εγγύηση ότι δεν θα συμβεί αυτό.

Εμπιστευτικότητα

Μια αναγνωρισμένη χρονική σφραγίδα δεν παρέχει καμία εγγύηση ότι τα δεδομένα με σφραγίδα χρόνου θα παραμείνουν εμπιστευτικά όταν αποστέλλονται στους παραλήπτες. Ωστόσο, δεν αποκαλύπτεται η χρονική σφράγιση των δεδομένων προς τον πάροχο χρονικής σήμανσης καθώς το αίτημα της σφραγίδας χρόνου περιλαμβάνει μόνο μια τιμή κατακερματισμού αυτών των δεδομένων.

Δεν υπάρχουν αποδείξεις αποστολής / παραλαβής

Η αναγνωρισμένη χρονική σφραγίδα δεν παρέχει καμία εγγύηση ότι το έγγραφο με σφραγίδα χρόνου έχει αποσταλεί αποτελεσματικά σε συγκεκριμένο παραλήπτη ή έχει παραληφθεί από συγκεκριμένο παραλήπτη.

Δεν υπάρχουν αποδείξεις προέλευσης σχετικά με τα δεδομένα φέρουν σφραγίδα χρόνου

Η αναγνωρισμένη χρονική σφραγίδα δεν παρέχει καμία εγγύηση ότι το χρονοσφραγισμένο έγγραφο προέρχεται από ένα συγκεκριμένο μέρος (δεν υπάρχει απόδειξη προέλευσης του εγγράφου).

Σημείωση: Για την απόδειξη προέλευσης στα δεδομένα με χρονική σφραγίδα, ο χρήστης θα πρέπει να δημιουργήσει μια αναγνωρισμένη ηλεκτρονική υπογραφή ως φυσικό πρόσωπο (ή αναγνωρισμένη ηλεκτρονική σφραγίδα ως νομικό πρόσωπο), καθώς η υπογραφή/σφραγίδα μπορεί να συνδυαστεί με τη χρήση αναγνωρισμένων χρονικών σφραγίδων.

Δεν υπάρχει υποχρέωση υπογραφής ή δέσμευσης περιεχομένου για δεδομένα με χρονική σφραγίδα

Η αναγνωρισμένη χρονική σφραγίδα δεν παρέχει καμία εγγύηση ότι ο κάτοχος του εγγράφου ή ο αιτών σφραγίδας χρόνου είναι σαφώς προσδιορισμένος. Η χρονική σφραγίδα δεν αποτελεί υπογραφή από τον κάτοχο του εγγράφου και δεν φέρει καμία δέσμευση σχετικά με το περιεχόμενο του χρονοσφραγισμένου εγγράφου (δεν υπάρχει ηλεκτρονική υπογραφή το έγγραφο).

Σημείωση: Για την απόκτηση απόδειξης δέσμευσης σε δεδομένα με χρονική σφραγίδα, τα χρονικά αυτά σήματα μπορούν να συνδυαστούν με αναγνωρισμένες ηλεκτρονικές υπογραφές όχι μόνο για τη χρονική σφράγιση αυτών αλλά και για την υπογραφή τους.

4. Είναι πάντα απαραίτητη η χρήση της Χρονοσημανσης ;

Όχι. Η χρονική σήμανση δεν είναι απαραίτητη όταν στέλνετε, για παράδειγμα, μια σύντομη υπογεγραμμένη σημείωση σε έναν συνάδελφο και αυτή η σημείωση αναμένεται να διαβαστεί και να 'χει ισχύ μόνο για την ίδια ημέρα που έχει γραφτεί. Από την άλλη πλευρά, η χρονική σήμανση είναι απαραίτητη όταν δημιουργείτε υπογεγραμμένα έγγραφα για ευρεία διανομή ή για μακροχρόνια αποθήκευση και αρχειοθέτηση. Εάν η υπογραφή πρόκειται να χρησιμοποιηθεί (για να αποδειχθεί η αυθεντικότητα του δημιουργού του εγγράφου ή του δημιουργού των δεδομένων) περισσότερο από μία ή περισσότερες ημέρες, τότε θα πρέπει να χρησιμοποιηθεί η χρονική σήμανση.

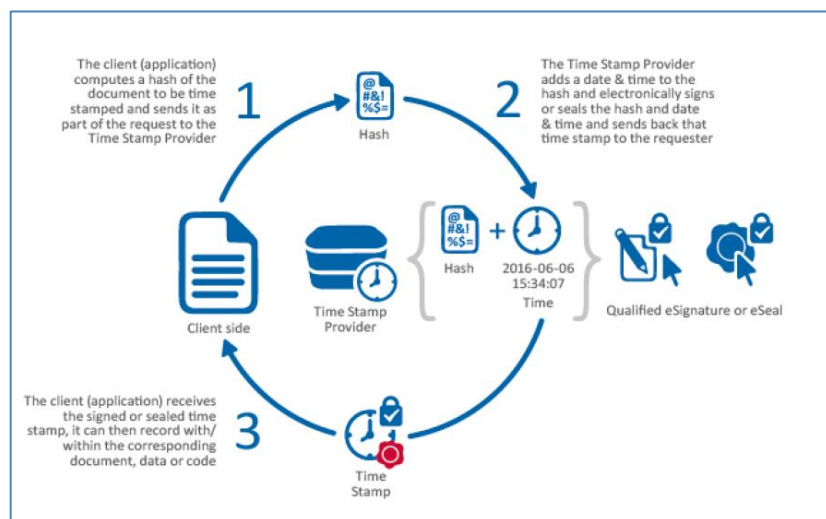


5. Πως λειτουργεί η Χρονοσήμανση ;

Η Ευρωπαϊκή Ένωση έχει παράσχει ένα πολύ εκτεταμένο σύνολο απαιτήσεων για τον έλεγχο της χρήσης αναγνωρισμένων ηλεκτρονικών χρονοσημάνσεων στο πλαίσιο του eIDAS. Αυτός είναι ο κανονισμός της ΕΕ αριθ. 910/2014. Το Χρηματιστήριο Αξιών Αθηνών είναι Πάροχος Υπηρεσιών Πιστοποίησης (CSP) καταχωρημένος στην Αξιόπιστη Λίστα (<http://tlbrowser.tsl.website/tools/index.jsp>) των Καταχωρημένων Παροχών Υπηρεσιών Πιστοποίησης που είναι εγκατεστημένοι στην Ελλάδα, έχοντας συμπληρώσει κατάλληλη έκθεση συμμόρφωσης σύμφωνα με τον ανωτέρω κανονισμό. Τα πιστοποιητικά TSA της ATHEX εκδίδονται από την Αρχή Χρονοσήμανσης της ATHEX Timestamping Qualified Athex (<https://webgate.ec.europa.eu/tl-browser/#/tl/EL/2/3>).

Η χρονική σήμανση περιλαμβάνει τα ηλεκτρονικά δεδομένα που έχετε υπογράψει ως πελάτης χρονικής σήμανσης (Timestamping Client) και ένα διακομιστή χρονικής σήμανσης (Timestamp Server) που ονομάζεται Timestamping Authority (TSA).

1. Υπολογίζεται ο κατακερματισμός της υπογραφής δεδομένων (hash of data) και αυτός (hash) αποστέλλεται στην ATHEX TSA για υπογραφή.
2. Η ATHEX TSA υπογράφει το ληφθέν hash χρησιμοποιώντας το δικό της πιστοποιητικό και τοποθετεί την τρέχουσα ώρα του διακομιστή σε αυτήν την υπογραφή.
3. Η υπογραφή της ATHEX TSA επιστρέφεται στον πελάτη (Client) και προστίθενται στην αρχική υπογραφή που έγινε στα αρχικά δεδομένα.



Σημείωση: Η ATHEX TSA παρέχει χρόνο ακρίβειας εντός ± 1 δευτερόλεπτου έναντι της UTC μέσω βαθμονόμησης με πολλαπλές ανεξάρτητες πηγές ώρας, συμπεριλαμβανομένου του συστήματος GPS και των Εθνικών Ινστιτούτων Μετρήσεων που παρέχουν ώρα UTC. Ως "συντεταγμένη παγκόσμια ώρα" ή "UTC" νοείται η χρονολογική κλίμακα, όπως ορίζεται από την Διεθνή Επιτροπή Τηλεπικοινωνιών Τηλεπικοινωνιών (ITU-R) TF.460-5 και αντιστοιχεί περίπου στο μέσο χρόνο Greenwich (GMT).



6. Μπορεί η ίδια η Χρονοσήμανση να ακυρωθεί ή να καταστεί άκυρη;

Εάν το πιστοποιητικό χρονοσήμανσης ακυρωθεί (θεωρείται άκυρο από τον ίδιο τον πάροχο που το έχει εκδώσει), υπάρχουν 2 περιπτώσεις που είναι δυνατές σύμφωνα και με τα σημεία 4.1 and 4.2 του RFC 3161:

- Εάν ο λόγος ανάκλησης υποδεικνύει ότι κλειδί δεν έχει παραβιαστεί αλλά η ίδια η TSA δεν θα λειτουργήσει στο μέλλον, τότε το πιστοποιητικό χρονικής σήμανσης δεν θα πρέπει να χρησιμοποιείται για χρονοσήμανση στο μέλλον (μετά την ανάκληση). Ωστόσο, όλες οι προηγούμενες χρονικές σφραγίδες δεν καθίστανται άκυρες.
- Εάν ο λόγος ανάκλησης υποδεικνύει ότι το κλειδί έχει παραβιαστεί (Key Compromised), τότε όλες οι χρονικές σφραγίδες που δημιουργήθηκαν με αυτό το πιστοποιητικό καθίστανται άκυρες.

7. Λήγει η Χρονοσήμανση ;

Η ίδια η χρονική σήμανση δεν λήγει. Ωστόσο, η χρονική σήμανση υπογράφεται με ένα πιστοποιητικό που έχει εκδοθεί για τον συγκεκριμένο σκοπό της υπογραφής χρονικών σημείων. Αυτό το πιστοποιητικό έχει το δικό του χρόνο λήξης και την δική του περίοδο ισχύος. Μόλις λήξει το πιστοποιητικό που χρησιμοποιείται για την υπογραφή μιας χρονικής σήμανσης, λήγει και η χρονική σήμανση. Όπως αναφέρεται στην παράγραφο 4.3 του RFC 3161, μια τέτοια χρονική σήμανση θα πρέπει να αναδιοργανωθεί ή να γίνει πράξη συμβολαιογραφίας για την ανανέωση της υπάρχουσας εμπιστοσύνης στο χρονικό σήμα.

8. Άρα, υπό ποιες συνθήκες / καταστάσεις μια υπογραφή θεωρείται έγκυρη ;

Συνοπτικός Πίνακας

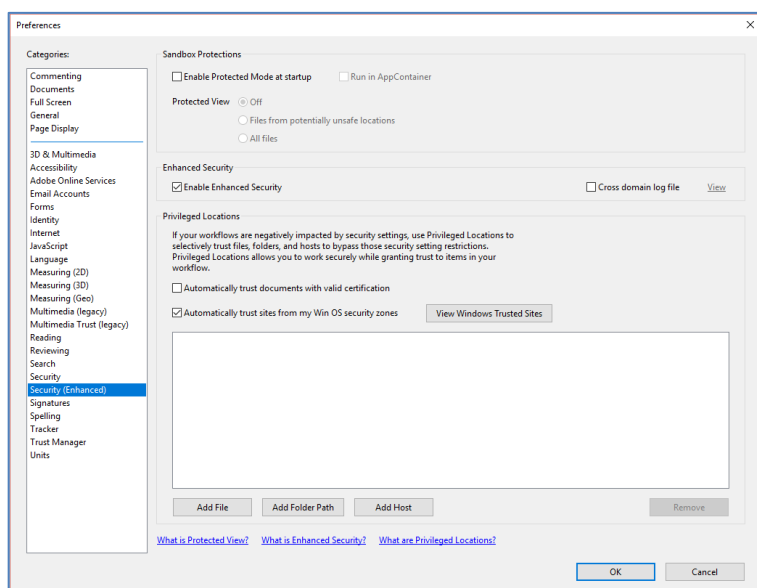
Συνθήκη / Κατάσταση	Απλή Υπογραφή	Υπογραφή με Χρονοσήμανση
Signing certificate (or certificate chain) is valid and not revoked		
Signing certificate (or certificate chain) is valid and is revoked before signing		
Signing certificate (or certificate chain) is valid and is revoked after signing		
Signing 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	



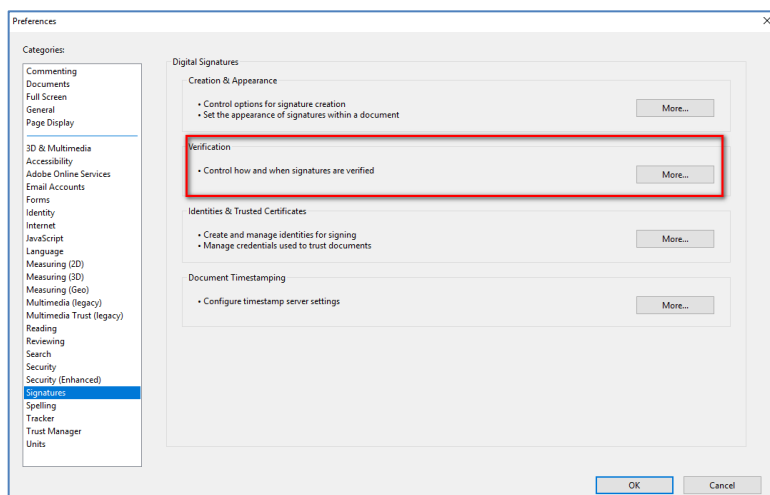
Όπως φαίνεται από τον παραπάνω πίνακα , σε μία μόνο περίπτωση μια απλή υπογραφή που δεν φέρει χρονοσήμανση είναι έγκυρη – όταν το πιστοποιητικό υπογραφής είναι εν ισχύ και έγκυρο. Σε όλες τις άλλες περιπτώσεις η υπογραφή θα καταστεί άκυρη. Ωστόσο , η υπογραφή που φέρει χρονοσήμανση εξακολουθεί να είναι έγκυρη , ακόμη και αν έχουν λήξει όλα τα πιστοποιητικά στις αλυσίδες υπογραφής και χρονικής σήμανσης . Ως εκ τούτου , θα πρέπει να χρησιμοποιείται η χρονοσήμανση με κάθε ψηφιακή υπογραφή.

9. Πως ενσωματώνω την ATHEX Χρονοσήμανση στον Acrobat Reader?

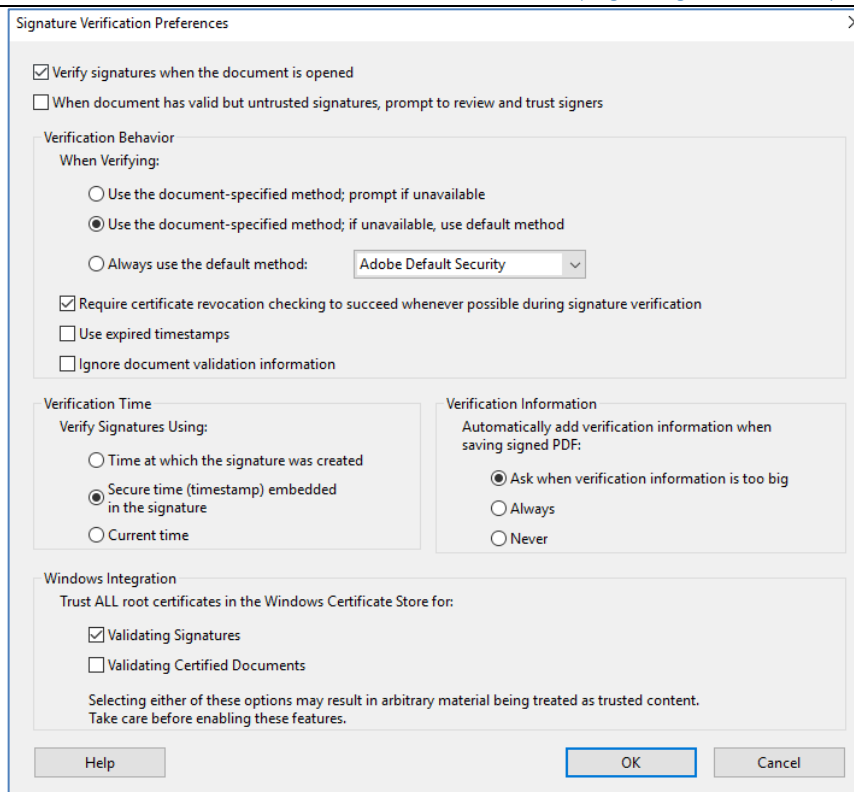
- Εγκατάσταση [ATHEX TSA Certificate](#)
- Ανοίξτε τον Adobe Reader
- Από το menu bar επιλέξτε **Edit**
- Ανοίξτε το **Preferences** από το κουτί διαλόγου
- Από το **Categories**, επιλέξτε **Security (Enhanced)** ,και **uncheck** το **Enable Protected Mode at startup**



- Click OK
- Από το **Categories**, επιλέξτε **Signatures**.
- Στο **Verification**, click **more**.



- Ενεργοποιήστε (check) τις επιλογές όπως φαίνεται στην παρακάτω εικόνα .



Signature Verification Preferences

☒ Verify signatures when the document is opened

☐ When document has valid but untrusted signatures, prompt to review and trust signers

Verification Behavior

When Verifying:

☐ Use the document-specified method; prompt if unavailable

☒ Use the document-specified method; if unavailable, use default method

☐ Always use the default method: Adobe Default Security

☒ Require certificate revocation checking to succeed whenever possible during signature verification

☐ Use expired timestamps

☐ Ignore document validation information

Verification Time

Verify Signatures Using:

☐ Time at which the signature was created

☒ Secure time (timestamp) embedded in the signature

☐ Current time

Verification Information

Automatically add verification information when saving signed PDF:

☒ Ask when verification information is too big

☐ Always

☐ Never

Windows Integration

Trust ALL root certificates in the Windows Certificate Store for:

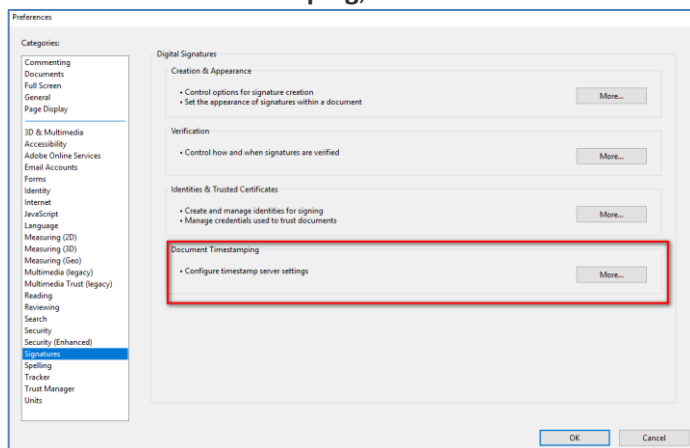
☒ Validating Signatures

☐ Validating Certified Documents

Selecting either of these options may result in arbitrary material being treated as trusted content. Take care before enabling these features.

Help OK Cancel

- Click OK.
- Ανοίξτε το **Preferences** από το κουτί διαλόγου .
- Από το **Categories**, επιλέξτε **Signatures**.
- Στο **Document Timestamping**, click **more**.



Preferences

Categories:

- Commenting
- Documents
- Full Screen
- General
- Page Display
- 3D & Multimedia
- Accessibility
- Adobe Online Services
- Email Accounts
- Forms
- Identity
- Internet
- JavaScript
- Language
- Measuring (3D)
- Measuring (Geo)
- Multimedia (legacy)
- Multimedia Trust (legacy)
- Reading
- Reviewing
- Search
- Security
- Security (Enhanced)
- Signatures**
- Spelling
- Tracker
- Trust Manager
- Units

Digital Signatures

Creation & Appearance

- Control options for signature creation
- Set the appearance of signatures within a document
- More...

Verification

- Control how and when signatures are verified
- More...

Identities & Trusted Certificates

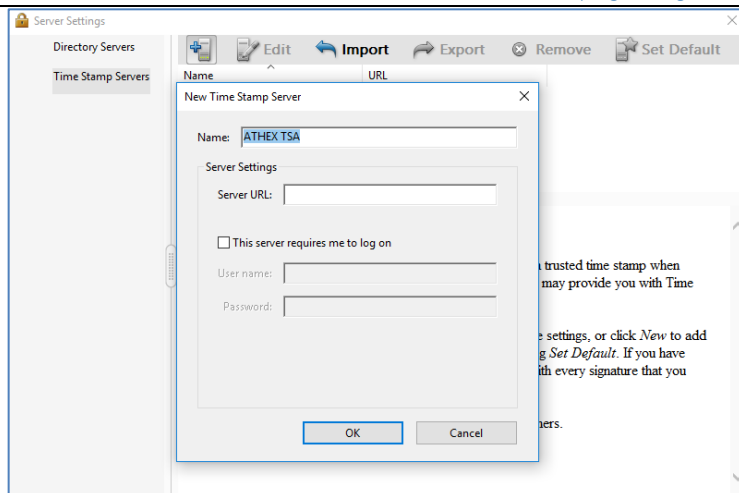
- Create and manage identities for signing
- Manage credentials used to trust documents
- More...

Document Timestamping

- Configure timestamp server settings
- More...

OK Cancel

- Επιλέξτε **Time Stamp Servers** (αριστερά)
- Click **New**  . Πληκτρολογήστε **ATHEX TSA** στο πεδίο **Name**



- Προσθέστε το ATHEX's URL στο Server URL , και click **OK**.
- Επιλέξτε Time Stamp Servers από τα αριστερά .

- Επιλέξτε το ATHEX TSA timestamp server, και click το **Set Default**  .
- Click **OK**
- Restart Adobe Acrobat Reader.

10. Ποιο είναι το ATHEX's TSA URL?

Για να γίνει χρήση της ATHEX Χρονοσήμανσης , πρέπει να είστε συνδρομητής αυτής όπου αναγνωρίζει ότι συμφωνεί και αποδέχεται τους όρους και τις προϋποθέσεις που εμπεριέχονται στη σχετική σύμβαση .

Για περισσότερες πληροφορίες επικοινωνήστε στα ακόλουθα στοιχεία :

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