

Χρήση εργαλείου **Adobe Acrobat Reader DC** για την προσθήκη Ψηφιακής Υπογραφής σε αρχεία PDF σε MacOS

(Μάιος 2026)



Περιεχόμενα

1. Εισαγωγή	3
2. Εγκατάσταση εργαλείου Adobe Acrobat Reader DC.....	3
3. Παραμετροποίηση εργαλείου Adobe Acrobat Reader DC.....	4
3.1. Ρυθμίσεις επαλήθευσης ψηφιακών υπογραφών	4
3.2. Δημιουργία και Εμφάνιση Υπογραφής	6
3.3. Πάροχοι Υπηρεσιών Εμπιστοσύνης	8
3.4. Ρύθμιση για TokenME Evo v2 (chip NXP)	9
3.5. Ρύθμιση για Safenet 5110cc/ Gemalto/ Thales/ TokenME EVO (MD 940).....	13
3.6. Ρύθμιση για Oberthur/ IDEMIA/ TokenME EVO (Cosmo v8.1 R2)	14
3.7. Χρονοσήμανση.....	17
4. Υπογραφή εγγράφου με τη χρήση Adobe Acrobat Reader DC	19

1. Εισαγωγή

Στο παρόν εγχειρίδιο περιγράφεται η διαδικασία, την οποία θα πρέπει να ακολουθήσει ο χρήστης προκειμένου να υπογράψει ψηφιακά ένα έγγραφο PDF. Πιο συγκεκριμένα γίνεται εκτενής περιγραφή της παραμετροποίησης του λογισμικού Adobe Acrobat Reader DC σε MacOS προκειμένου να είναι δυνατή τόσο η προσθήκη ψηφιακής υπογραφής όσο και η προσθήκη ασφαλούς χρονοσήμανσης. Ο Adobe Acrobat Reader DC πέραν της επαλήθευσης των ψηφιακών υπογραφών επιτρέπουν και τη δημιουργία αυτών. Το βασικότερο πλεονέκτημα είναι η δυνατότητα δημιουργίας υπογραφών που μπορούν να επαληθευτούν ακόμα και μετά τη λήξη ή ανάκληση του πιστοποιητικού, χωρίς να παρουσιάζεται πρόβλημα στον χρήστη που κάνει την επαλήθευση. Βασική προϋπόθεση η σωστή παραμετροποίηση της εφαρμογής.

2. Εγκατάσταση εργαλείου Adobe Acrobat Reader DC

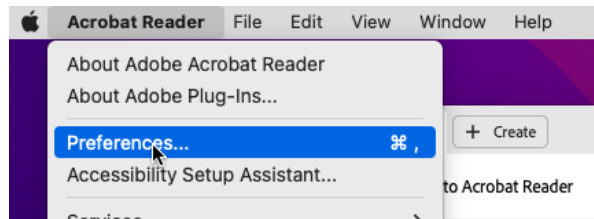
Το λογισμικό Adobe Acrobat Reader είναι ελεύθερα διαθέσιμο στην ιστοσελίδα:

<https://get.adobe.com/reader/>

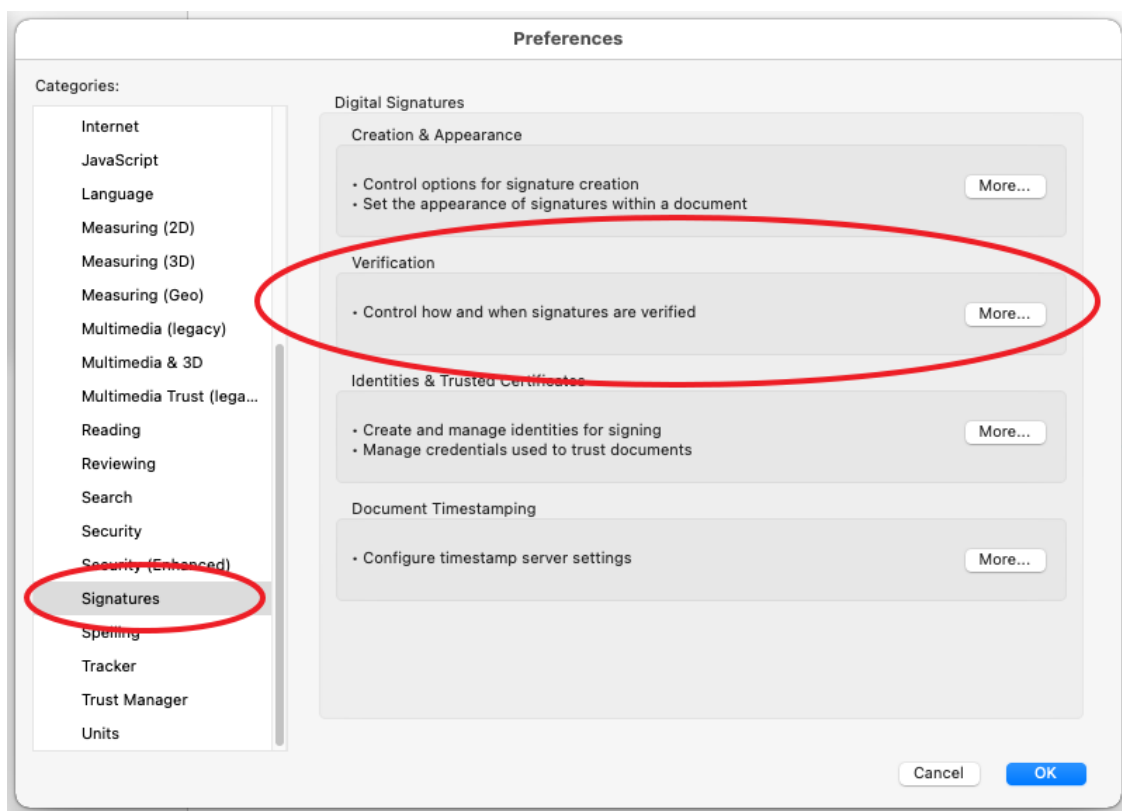
3. Παραμετροποίηση εργαλείου Adobe Acrobat Reader DC

3.1. Ρυθμίσεις επαλήθευσης ψηφιακών υπογραφών

Από το μενού εφαρμογής του προγράμματος επιλέγουμε **Acrobat Reader** ---> **Preferences**



Στην συνέχεια επιλέγουμε **Signatures** και στο **Verification** επιλέγουμε **More...**



Στο παράθυρο που εμφανίζεται, θα πρέπει να είναι ενεργοποιημένες οι επιλογές :

- ✓ Verify signature when the document is opened

Verification Behavior

- ✓ Require Certificate revocation checking to succeed whenever possible during signature verification
- ✓ Use expired timestamps

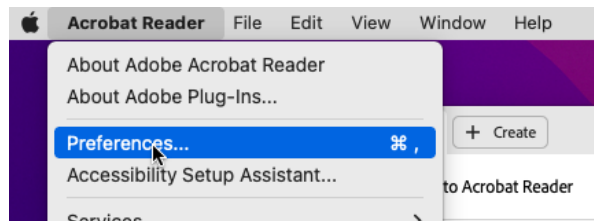
Verification Time – Verify Signatures Using:

- ✓ Secure time (timestamp) embedded in the signature

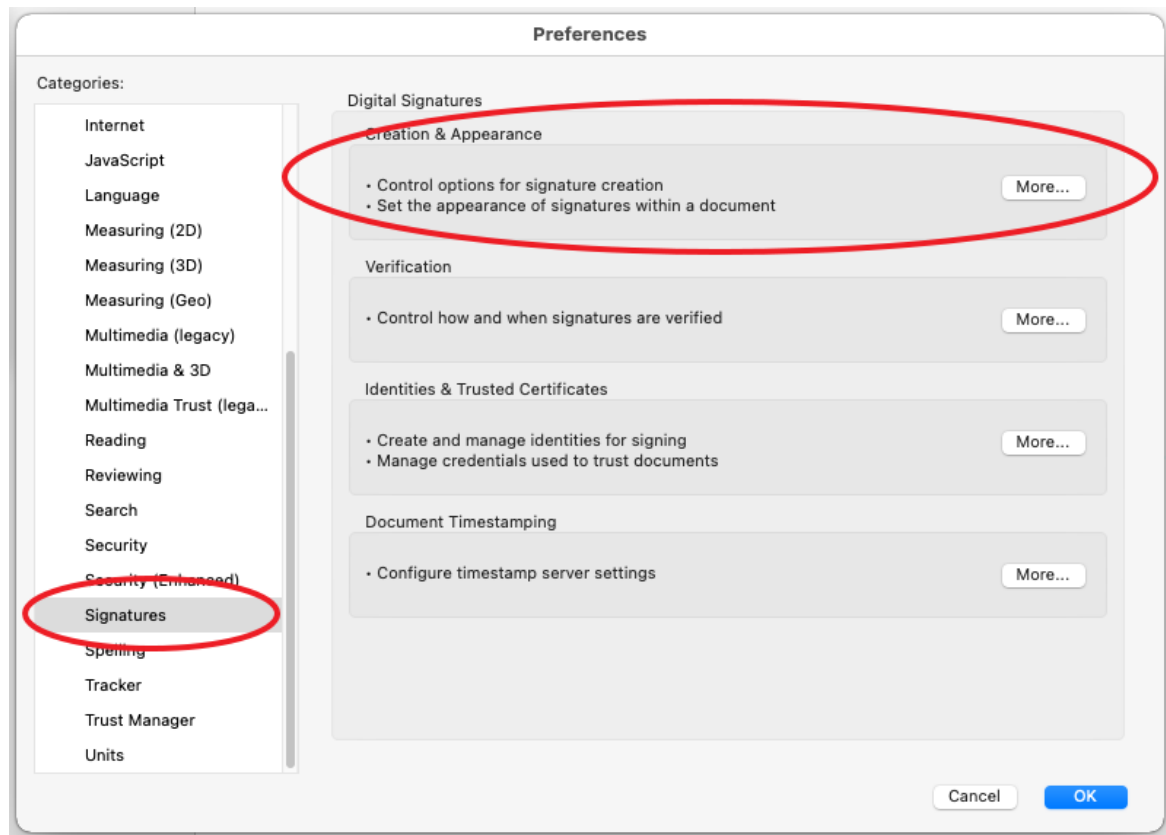


3.2. Δημιουργία και Εμφάνιση Υπογραφής

Από το μενού εφαρμογής του προγράμματος επιλέγουμε **Acrobat Reader** ---> **Preferences**



Στην συνέχεια επιλέγουμε **Signatures** και στο **Digital Signatures** επιλέγουμε **More...**



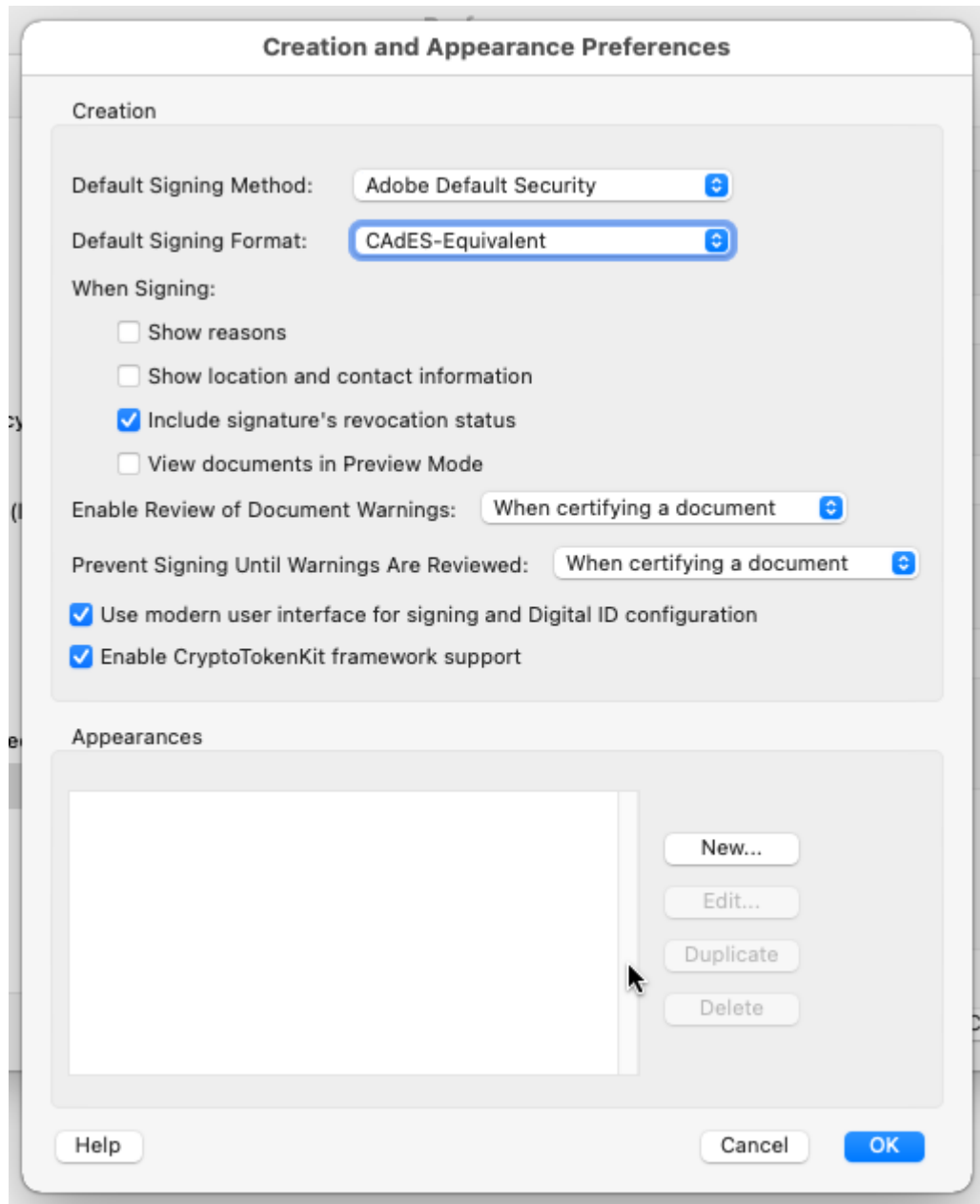
Στο παράθυρο που εμφανίζεται, θα πρέπει να είναι ενεργοποιημένες οι επιλογές :

Default Signing Format :

- ✓ CAdES-Equivalent

When Signing :

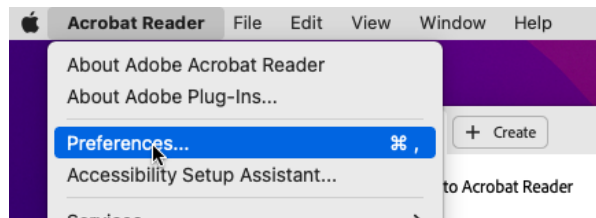
- ✓ Include signature's revocation status



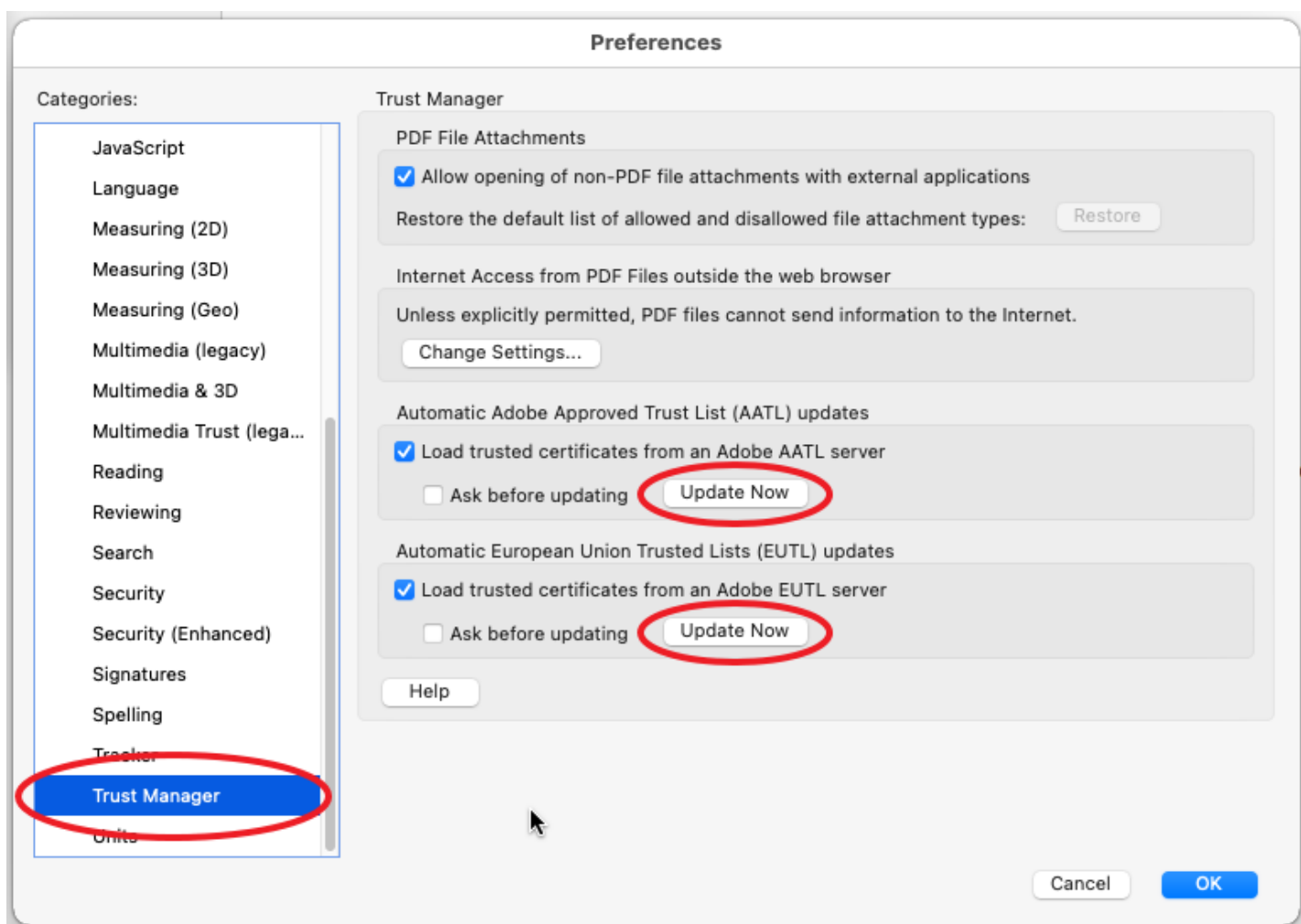
Προαιρετικά δημιουργούμε συγκεκριμένο τρόπο απεικόνισης της υπογραφής επιλέγοντας *New...* στο πεδίο *Appearances*.

3.3. Πάροχοι Υπηρεσιών Εμπιστοσύνης

Από το μενού εφαρμογής του προγράμματος επιλέγουμε **Acrobat Reader** ---> **Preferences**



Στην συνέχεια επιλέγουμε **Trust Manager** και ελέγχουμε να είναι ενεργοποιημένες οι επιλογές όπως η παρακάτω εικόνα. Επίσης πατάμε τα δύο κουμπιά “Update Now”, ώστε να ενημερωθεί η εφαρμογή με τους τελευταίους καταλόγους Παρόχων Υπηρεσιών Εμπιστοσύνης.

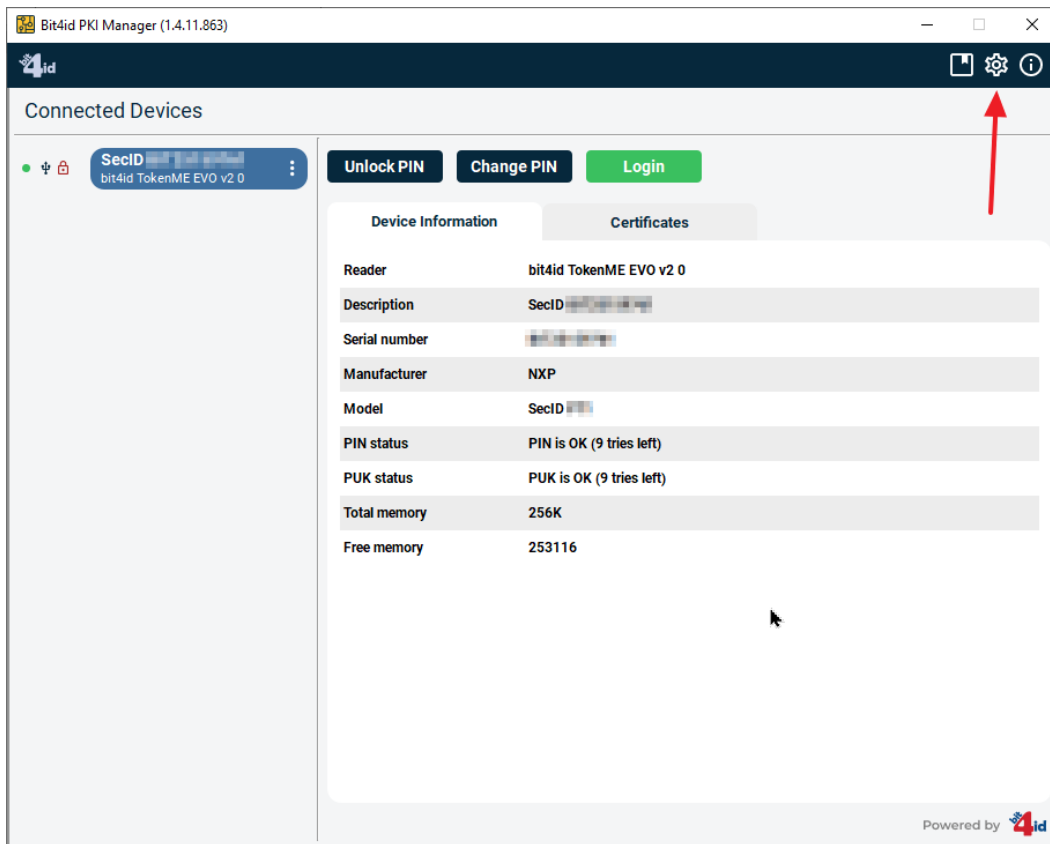


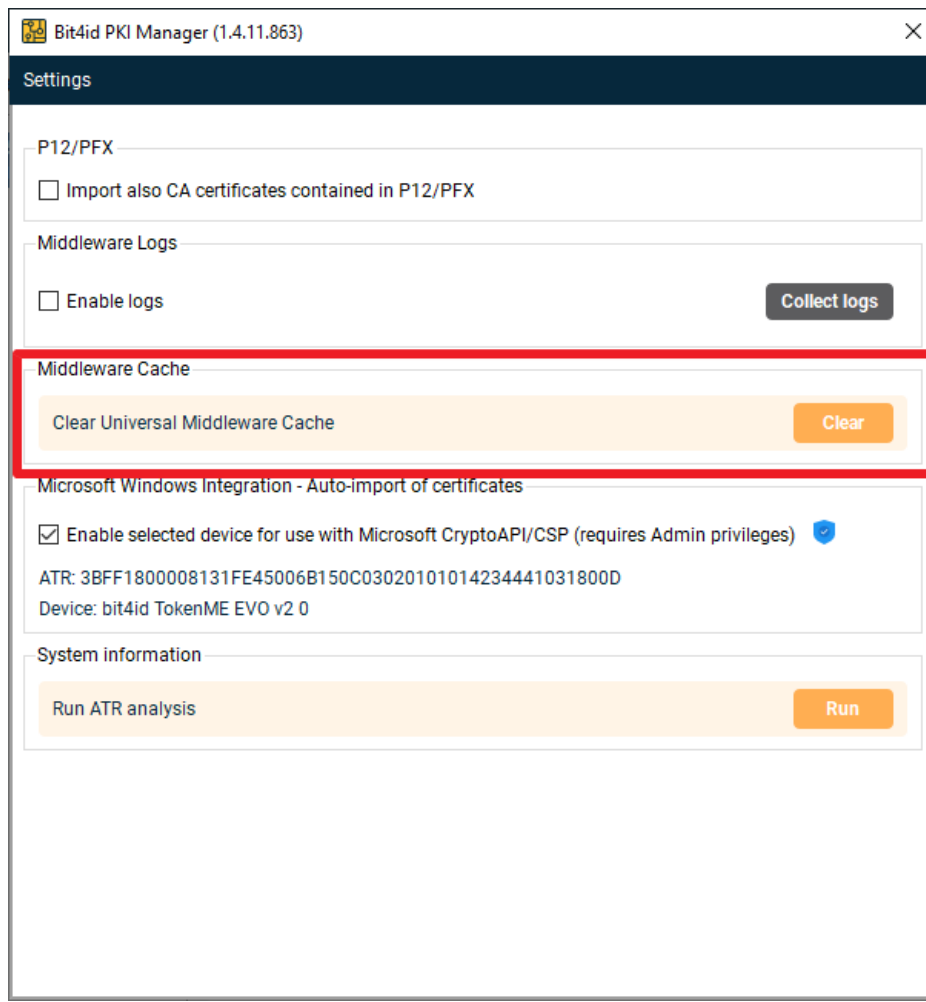
3.4. Ρύθμιση για TokenME Evo v2 (chip NXP)

Για το TokenME Evo v2 (chip NXP) θα πρέπει να εγκατασταθεί ο driver από τη σελίδα:

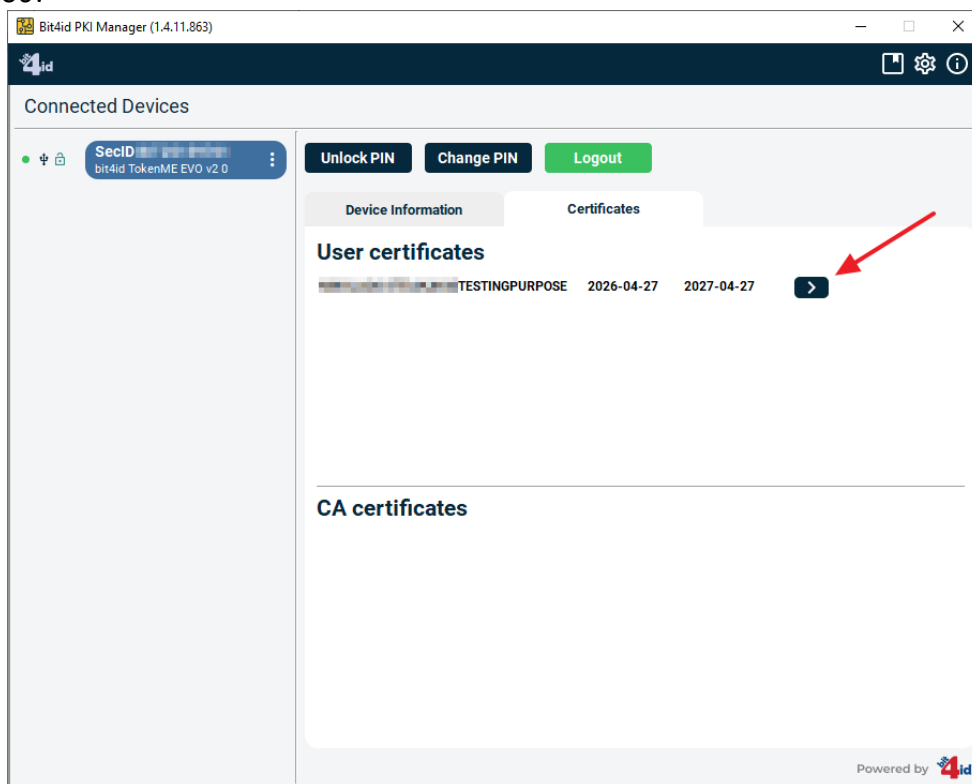
<https://aped.gov.gr/procedures/pos-tha-ypograpso-psifiaka-ena-ilektroniko-engrafo-morfi-pdf/>

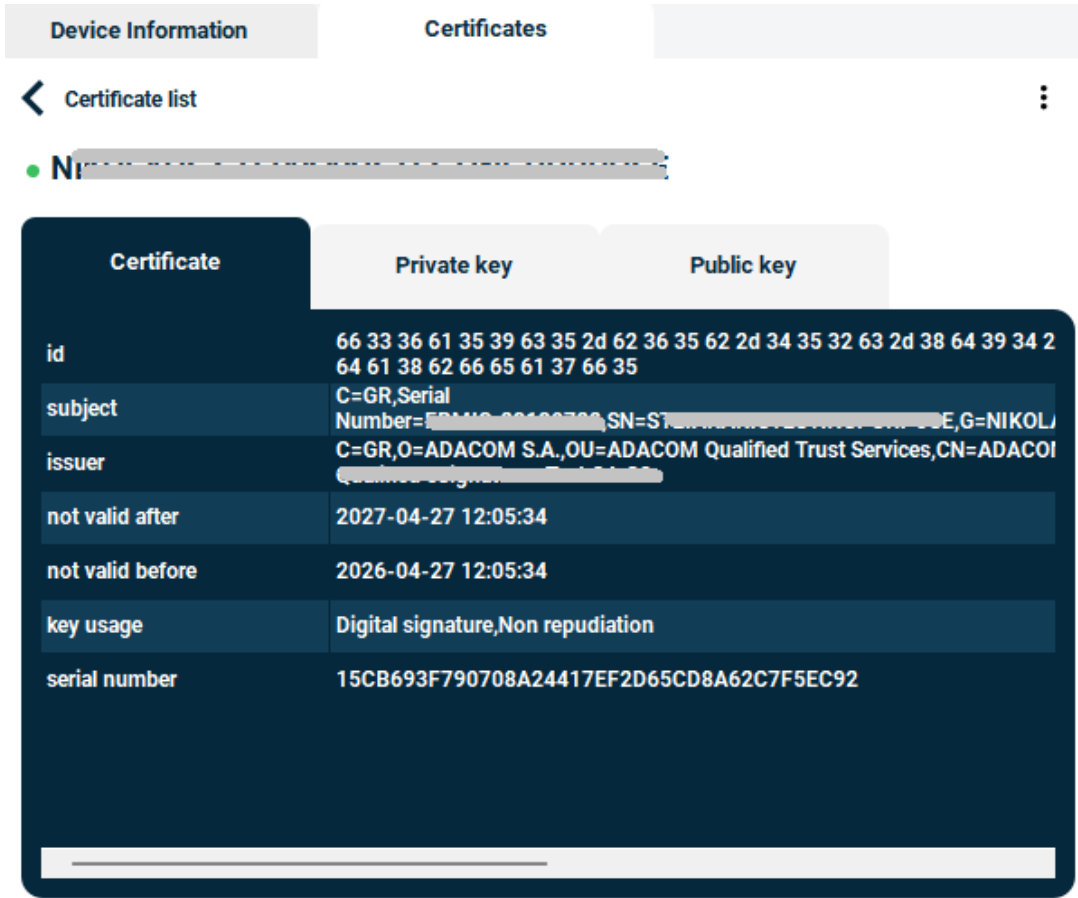
Επιβεβαιώνουμε ότι ο driver μπορεί να διαβάσει το πιστοποιητικό στη συσκευή. Ανοίγουμε την εφαρμογή “Bit4id-PKI Manager”, πατάμε settings (γρανάζι) και πατάμε Clear στο “Middleware Cache”



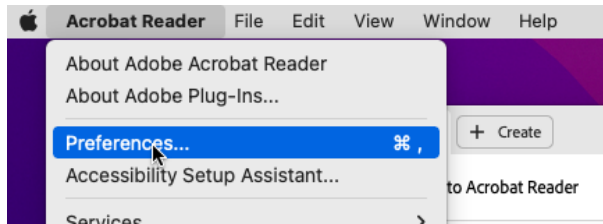


Έπειτα, αφού κλείσουμε το παράθυρο Settings, πηγαίνουμε στην καρτέλα certificates και πατάμε login. Αφού εισάγουμε το PIN, εμφανίζεται το ονοματεπώνυμο του χρήστη και πατώντας το βελάκι, βλέπουμε τα στοιχεία του πιστοποιητικού:

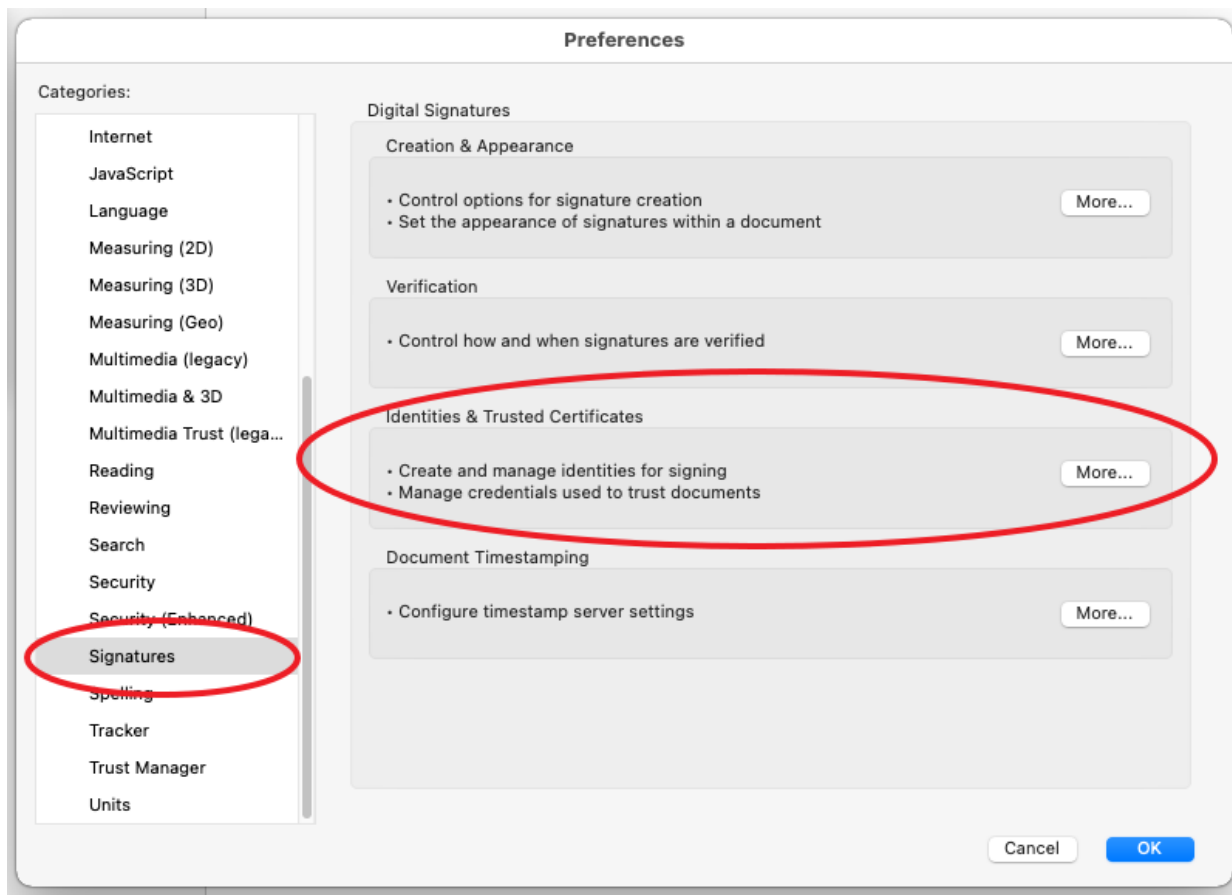




Σε περίπτωση που δεν μπορούμε να υπογράψουμε γιατί ο Acrobat δεν εντοπίζει το token, από το μενού εφαρμογής του προγράμματος επιλέγουμε **Acrobat Reader -> Preferences**



Στην συνέχεια επιλέγουμε **Signatures** και στο **Identities & Trusted Certificates** επιλέγουμε **More...**



Επιλέγουμε **PKCS#11 Modules and Tokens**, επιλέγουμε **Attach Module** και στο Library Path γράφουμε:

[*/Library/bit4id/pkcs11/libbit4xpki.dylib*](#)

και πατάμε **OK**.

Παρατήρηση:

A. Σε περίπτωση που το πλήκτρο **Attach Module** δεν μπορεί να πατηθεί, από τις ρυθμίσεις επιλέγουμε “Security (Enhanced)”, αφαιρούμε την επιλογή “Enable Protected Mode at startup”, κλείνουμε και ανοίγουμε πάλι τον Acrobat Reader

B. Σε περίπτωση που δεν μπορούμε να υπογράψουμε γιατί ο Acrobat δεν εντοπίζει πάλι το token, μετά τις παραπάνω ρυθμίσεις, ανοίγουμε πάλι τα **Identities & Trusted Certificate Settings** και εκτελούμε τα παρακάτω :

1. Κάνουμε κλικ στο **Bit4id PKCS#11**
2. Επιλέγουμε **Login**, εισάγουμε το PIN της συσκευής και κάνουμε κλικ στο **OK**.
3. Μετά το Login κάνουμε κλικ στην εγγραφή κάτω από το Bit4id PKCS#11
4. Επιλέγουμε το ψηφιακό πιστοποιητικό ---> επιλέγουμε **Usage Options** ---> επιλέγουμε **Use for Signing**

3.5. Ρύθμιση για Safenet 5110cc/ Gemalto/ Thales/ TokenME EVO (MD 940)

Αντίστοιχα, σε περίπτωση token Safenet 5110cc/ Gemalto/ Thales/ TokenME EVO (MD 940) θα πρέπει να εγκατασταθεί ο κατάλληλος driver από την [ιστοσελίδα της ΑΠΕΔ](#)

θα πρέπει να εκτελέσουμε τα παρακάτω :

- Κάντε κλικ στο εικονίδιο Launchpad  στο Dock, πληκτρολογήστε «Τερματικό» στο πεδίο αναζήτησης και μετά κάντε κλικ στο «Τερματικό» ή στο Finder , ανοίξτε τον φάκελο /Εφαρμογές/Βοηθήματα και μετά κάντε διπλό κλικ στο «Τερματικό».
- Στο τερματικό (terminal) γράφουμε την παρακάτω εντολή
`sudo nano /etc/etoken.conf`
- Πατάμε **Enter**
- Γράφουμε τον κωδικό Mac
- Στο παράθυρο συμπληρώνουμε :
[GENERAL]
EnablePrompt=1
- Πατάμε **CTRL+O** και **Enter**
- Πατάμε **CTRL+X**

Παρατήρηση:

Α. Σε περίπτωση που δεν μπορούμε να υπογράψουμε γιατί ο Acrobat δεν εντοπίζει το token (MD 940), μετά τις παραπάνω ρυθμίσεις, εκτελούμε τα παρακάτω :

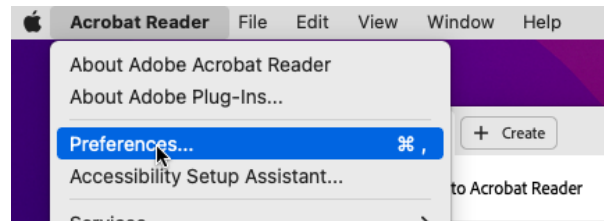
- Από το μενού εφαρμογής του προγράμματος επιλέγουμε **Acrobat Reader ---> Preferences ---> Signatures ---> Identities & Trusted Certificates ---> more...**
- Επιλέγουμε **PKCS#11 Modules and Tokens**
- Επιλέγουμε **Attach Module**
- Στο Library Path γράφουμε:
`/usr/local/lib/libeTPkcs11.dylib`
- Πατάμε **OK**
- Κάνουμε κλικ στο **SafeNet eToken PKCS#11**
- Επιλέγουμε **Login** και εισάγουμε το PIN της συσκευής
- Πατάμε **OK**
- Μετά το Login κάνουμε κλικ στο **Token** σας κάτω από το **SafeNet eToken PKCS#11**
- Επιλέγουμε το ψηφιακό πιστοποιητικό ---> επιλέγουμε **Usage Options** ---> επιλέγουμε **Use for Signing**

Β. Σε περίπτωση που το πλήκτρο **Attach Module** δεν μπορεί να πατηθεί, από τις ρυθμίσεις επιλέγουμε “Security (Enhanced)”, αφαιρούμε την επιλογή “Enable Protected Mode at startup”, κλείνουμε και ανοίγουμε πάλι τον Acrobat Reader

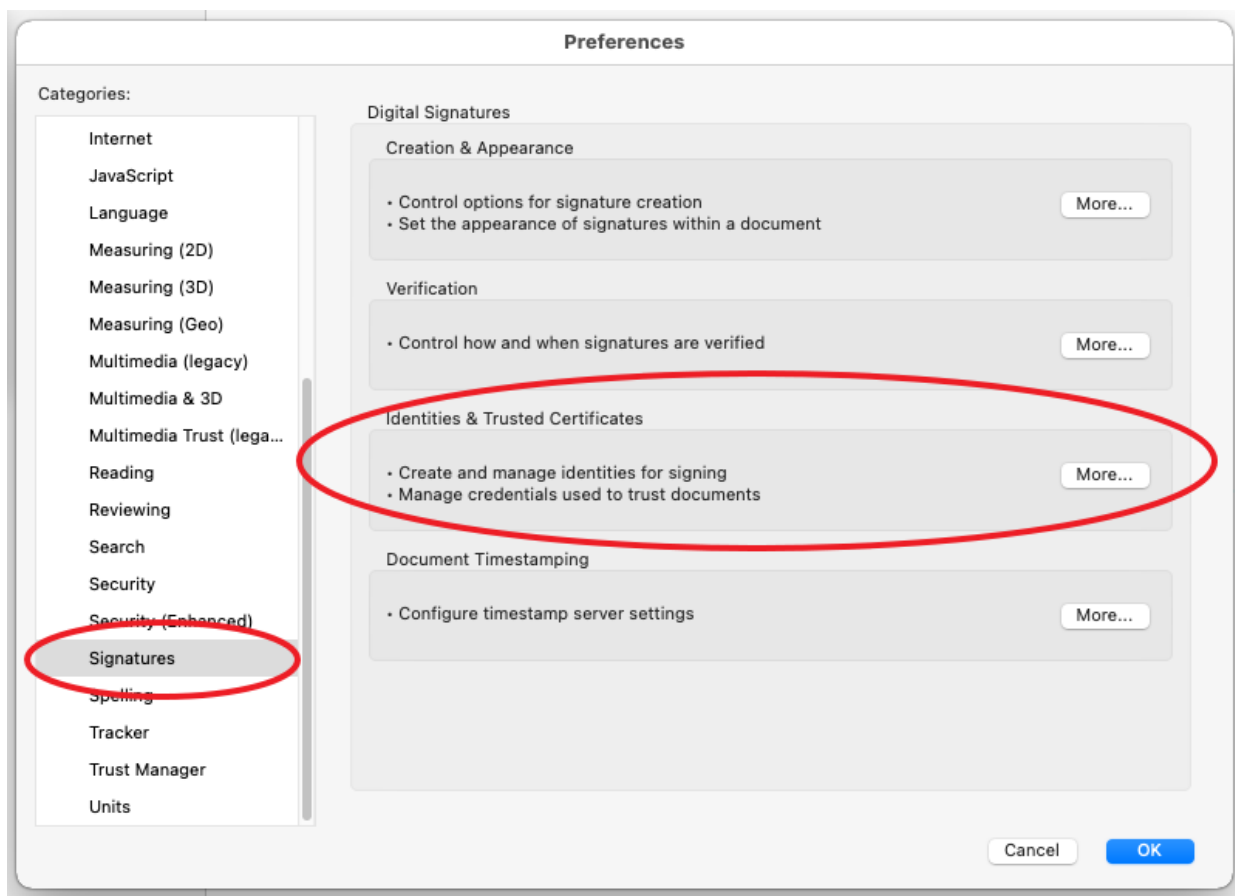
3.6. Ρύθμιση για Oberthur/ IDEMIA/ TokenME EVO (Cosmo v8.1 R2)

Σε περίπτωση token Oberthur / IDEMIA/ TokenME EVO (Cosmo v8.1 R2) θα πρέπει να εγκατασταθεί ο driver [AWP 5.2.0 SR2](#)

Έπειτα, από το μενού εφαρμογής του προγράμματος επιλέγουμε **Acrobat Reader -> Preferences**



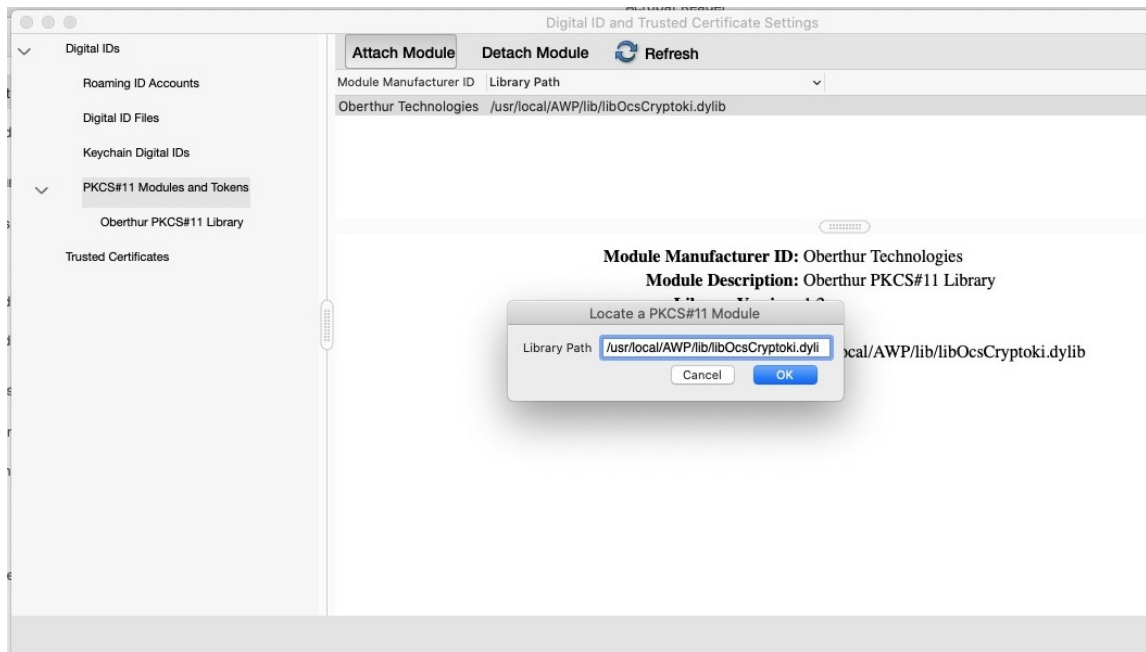
Στην συνέχεια επιλέγουμε **Signatures** και στο **Identities & Trusted Certificates** επιλέγουμε **More...**



Επιλέγουμε **PKCS#11 Modules and Tokens**, επιλέγουμε **Attach Module** και στο Library Path γράφουμε:

[*/usr/local/AWP/lib/libOcsCryptoki.dylib*](#)

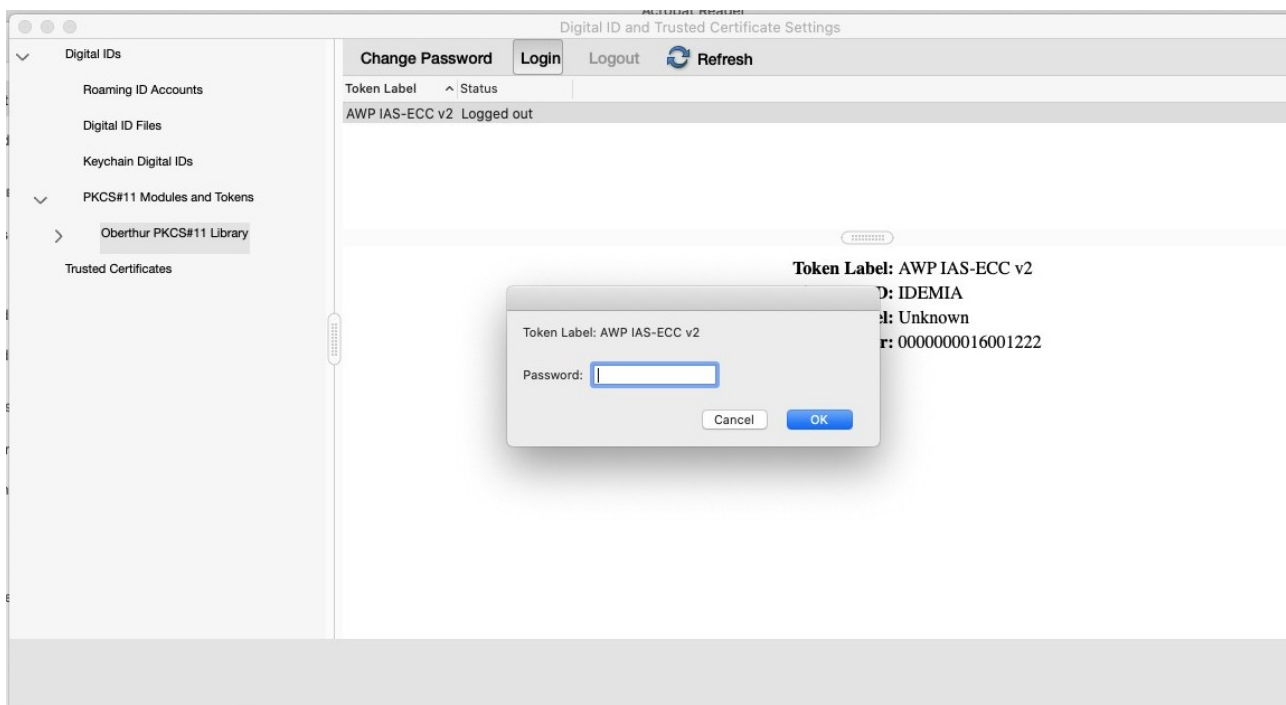
και πατάμε **OK**.



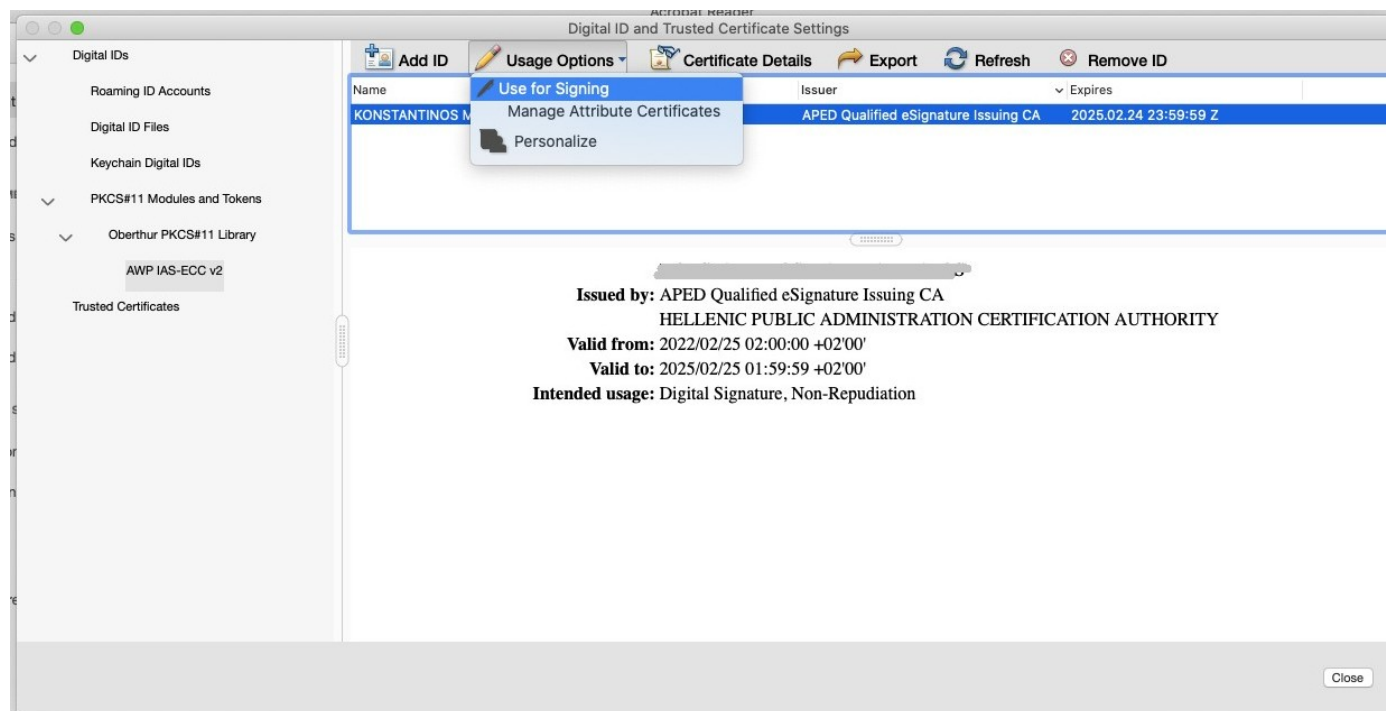
Παρατήρηση:

Σε περίπτωση που δεν μπορούμε να υπογράψουμε γιατί ο Acrobat δεν εντοπίζει το token (Cosmo v8.1 R2), μετά τις παραπάνω ρυθμίσεις, ανοίγουμε πάλι τα **Identities & Trusted Certificate Settings** και εκτελούμε τα παρακάτω :

1. Κάνουμε κλικ στο **Oberthur PKCS#11 Library**
2. Επιλέγουμε **Login**, εισάγουμε το PIN της συσκευής και κάνουμε κλικ στο **OK**.

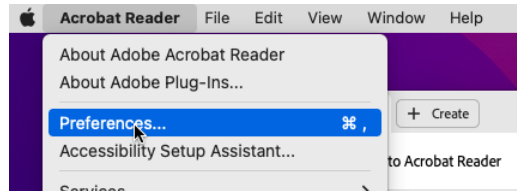


- Μετά το Login κάνουμε κλικ στο token **AWP IAS-ECC v2** κάτω από το Oberthur PKCS#11 Library
- Επιλέγουμε το ψηφιακό πιστοποιητικό ---> επιλέγουμε **Usage Options** ---> επιλέγουμε **Use for Signing**

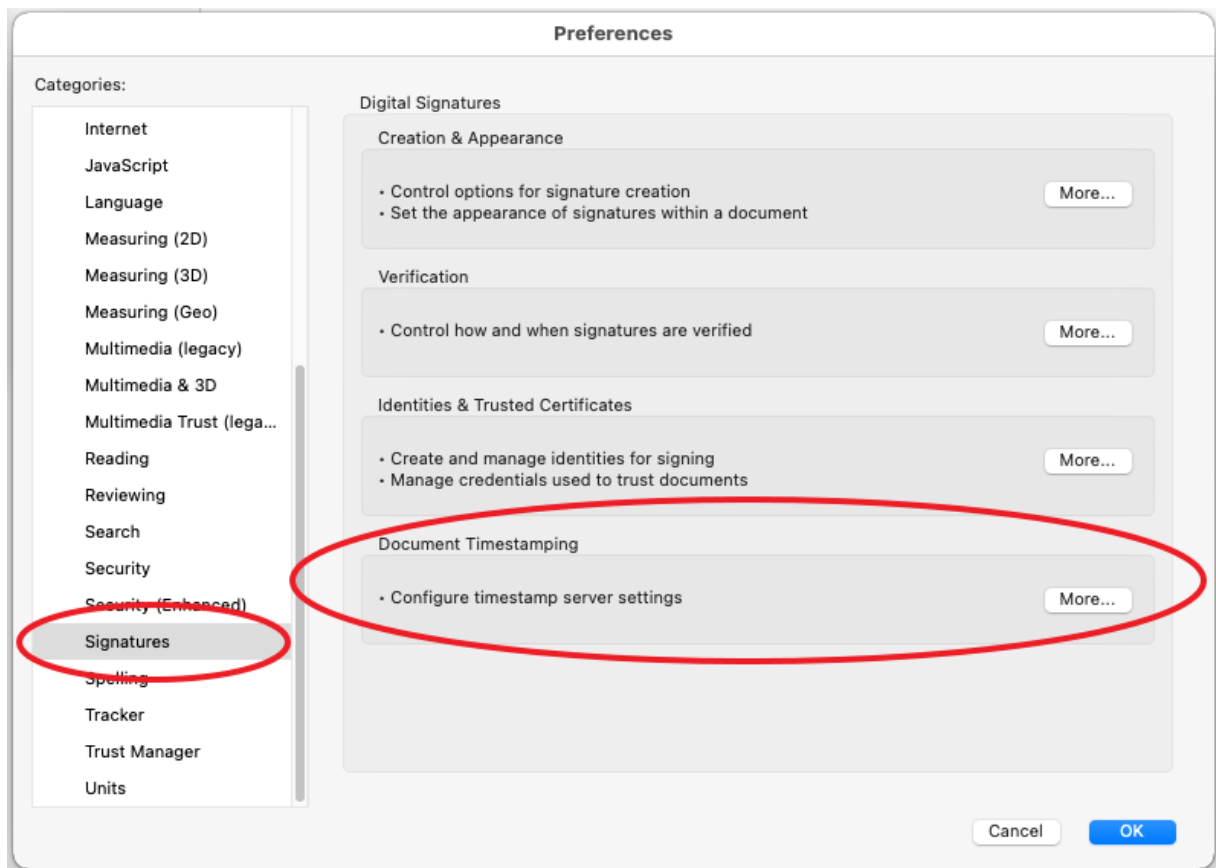


3.7. Χρονοσήμανση

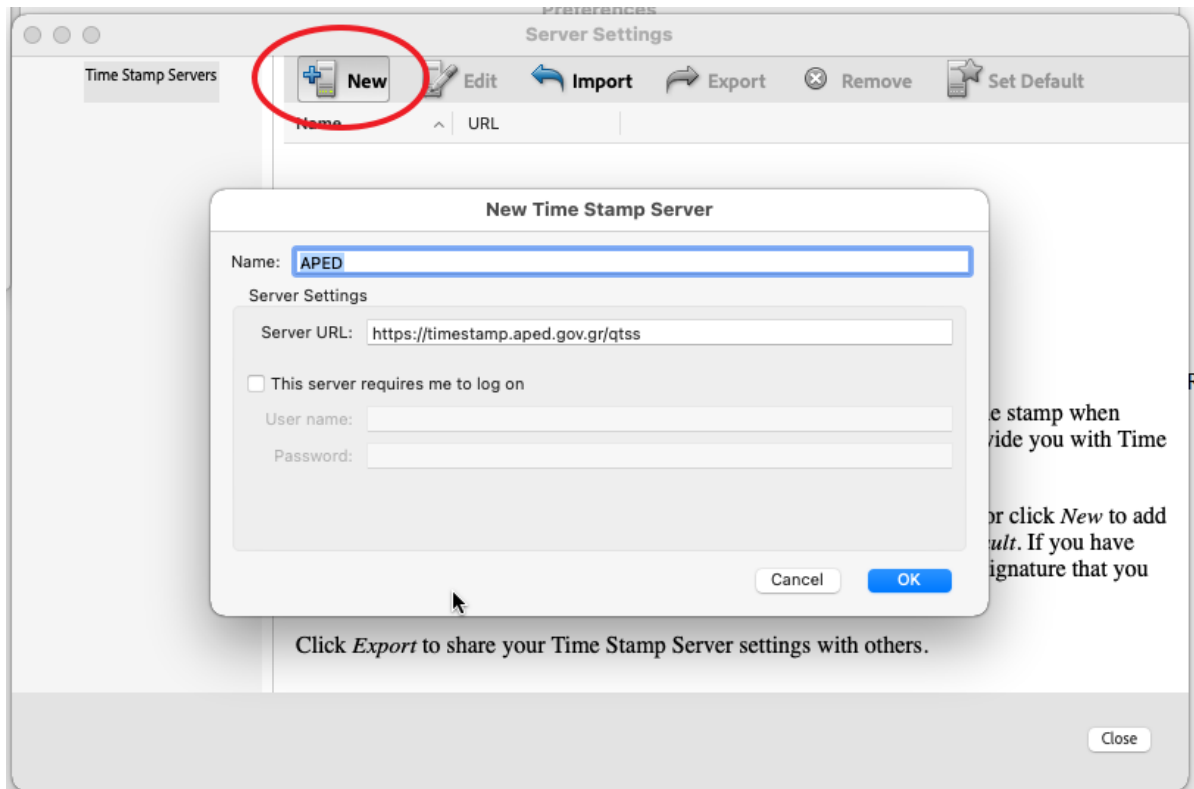
Από το μενού εφαρμογής του προγράμματος επιλέγουμε **Acrobat Reader** ---> **Preferences**



Στην συνέχεια επιλέγουμε **Signatures** και στο **Document Timestamping** επιλέγουμε **More...**



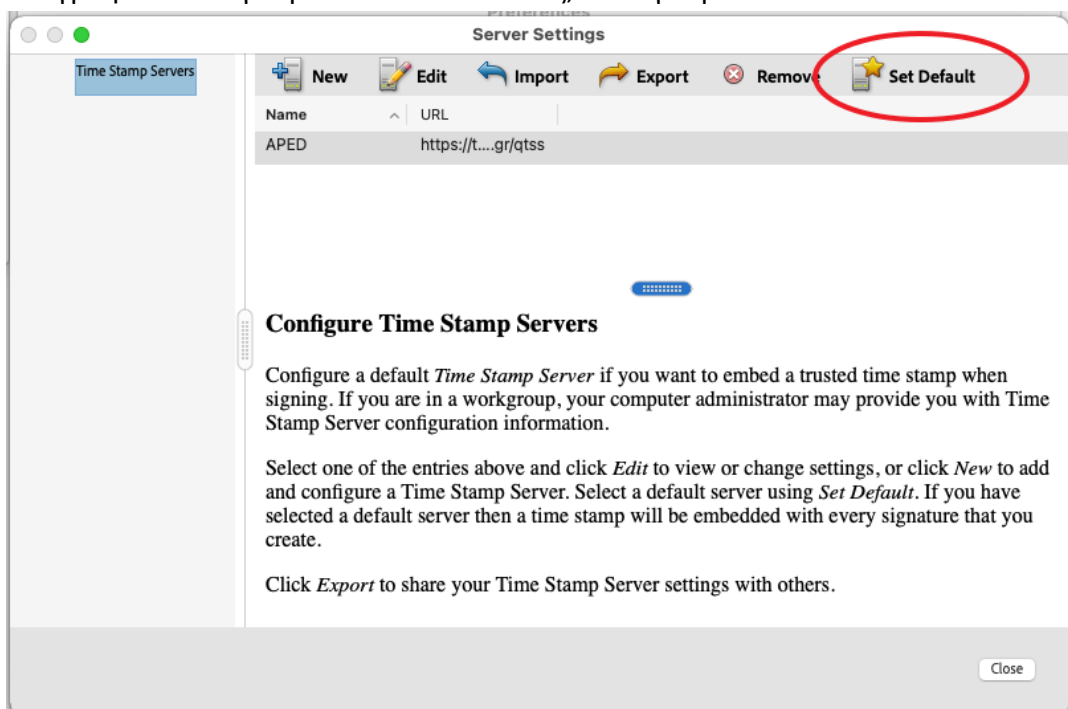
Στην οθόνη που εμφανίζεται, επιλέγουμε **New** για να εισάγουμε τα στοιχεία του εξυπηρετητή χρονοσήμανσης.



Στο Name Εισάγουμε ένα χαρακτηριστικό όνομα (π.χ. APED) και το Server URL:
<https://timestamp.aped.gov.gr/qtss>

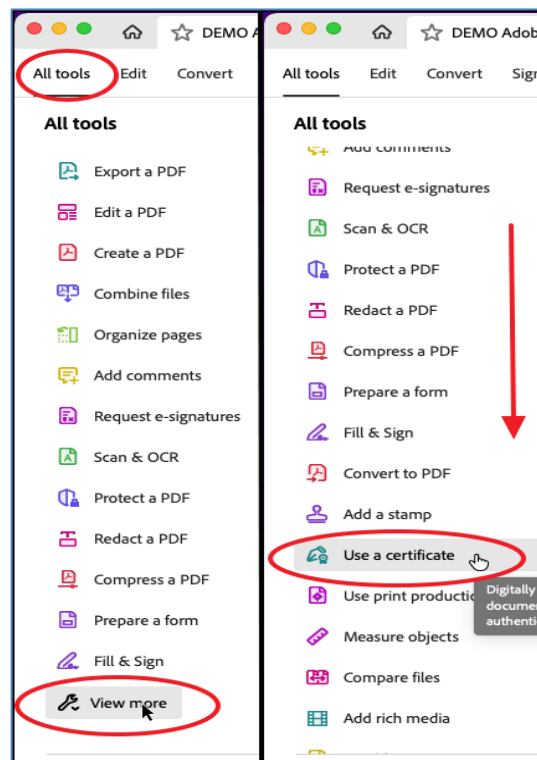
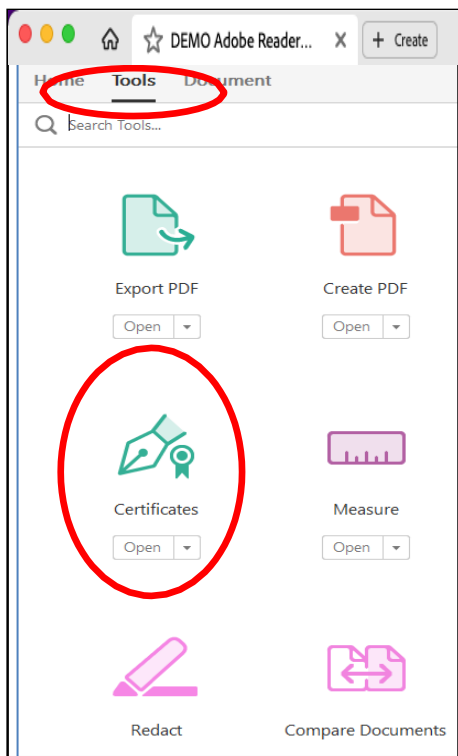
Και επιλέγουμε **OK**.

Για να ορίσουμε αυτόν τον εξυπηρετητή ως αυτόν που εξ' ορισμού θα χρησιμοποιείται κατά τη δημιουργία υπογραφών επιλέγουμε **Set Default**. Τέλος, επιλέγουμε **Close**.

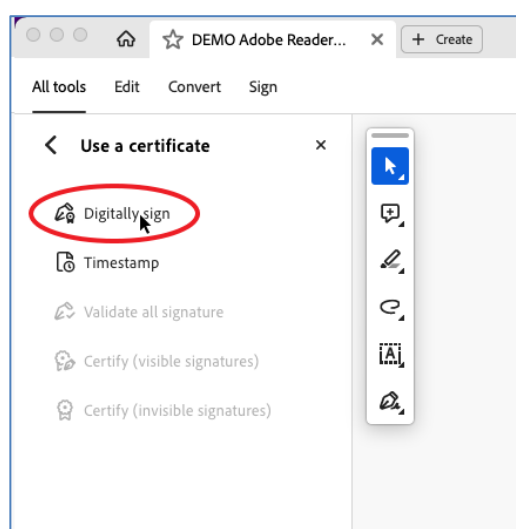
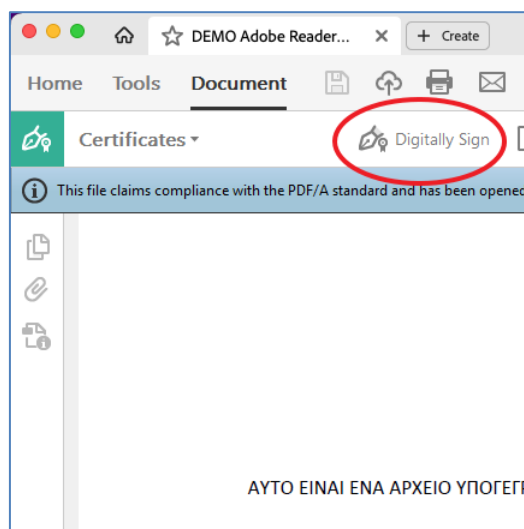


4. Υπογραφή εγγράφου με τη χρήση Adobe Acrobat Reader DC

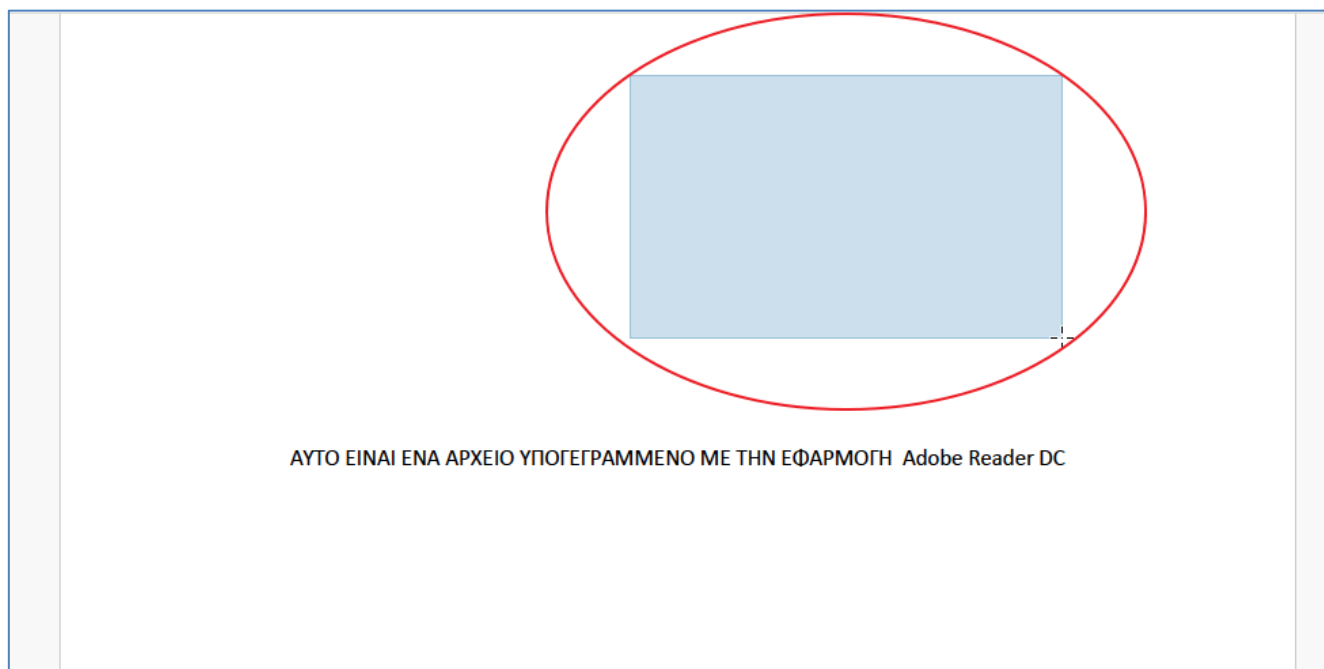
Για τη δημιουργία της υπογραφής επιλέγουμε από το μενού **Tools** και στην συνέχεια **Certificates** ή επιλέγουμε από το μενού **All Tools** και στη συνέχεια **View more** και **Use a certificate**.



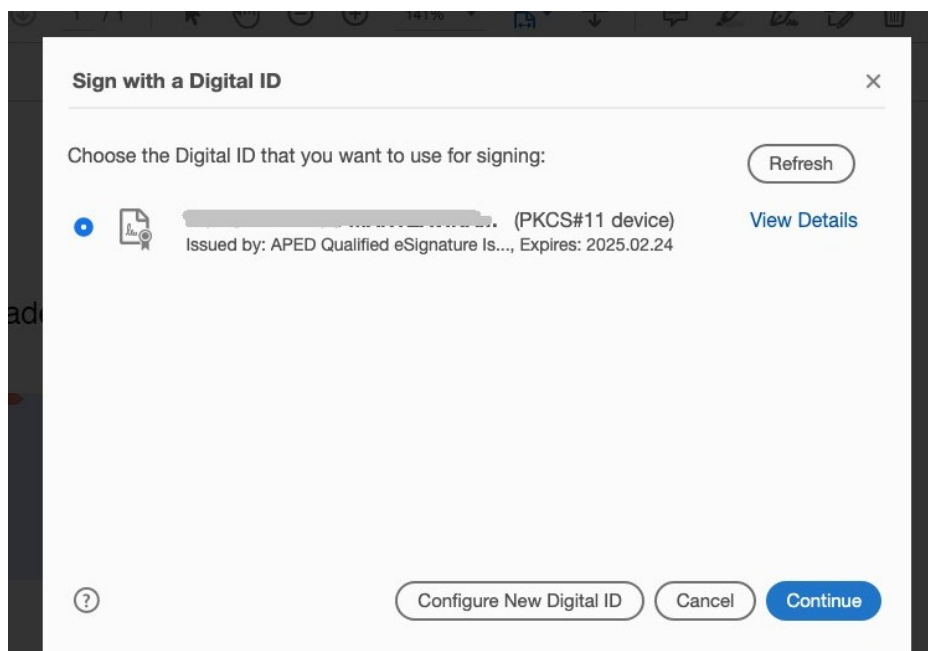
Στην οθόνη που εμφανίζεται επιλέγουμε το **Digitally Sign**



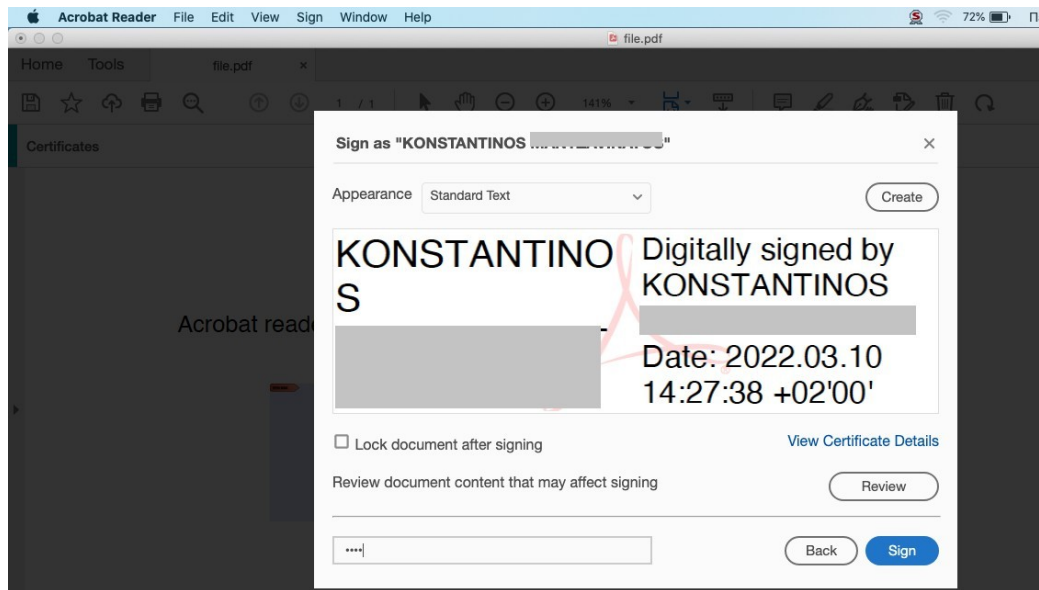
Με τη χρήση του ποντικιού ορίζουμε την περιοχή στην οποία θα μπει η υπογραφή



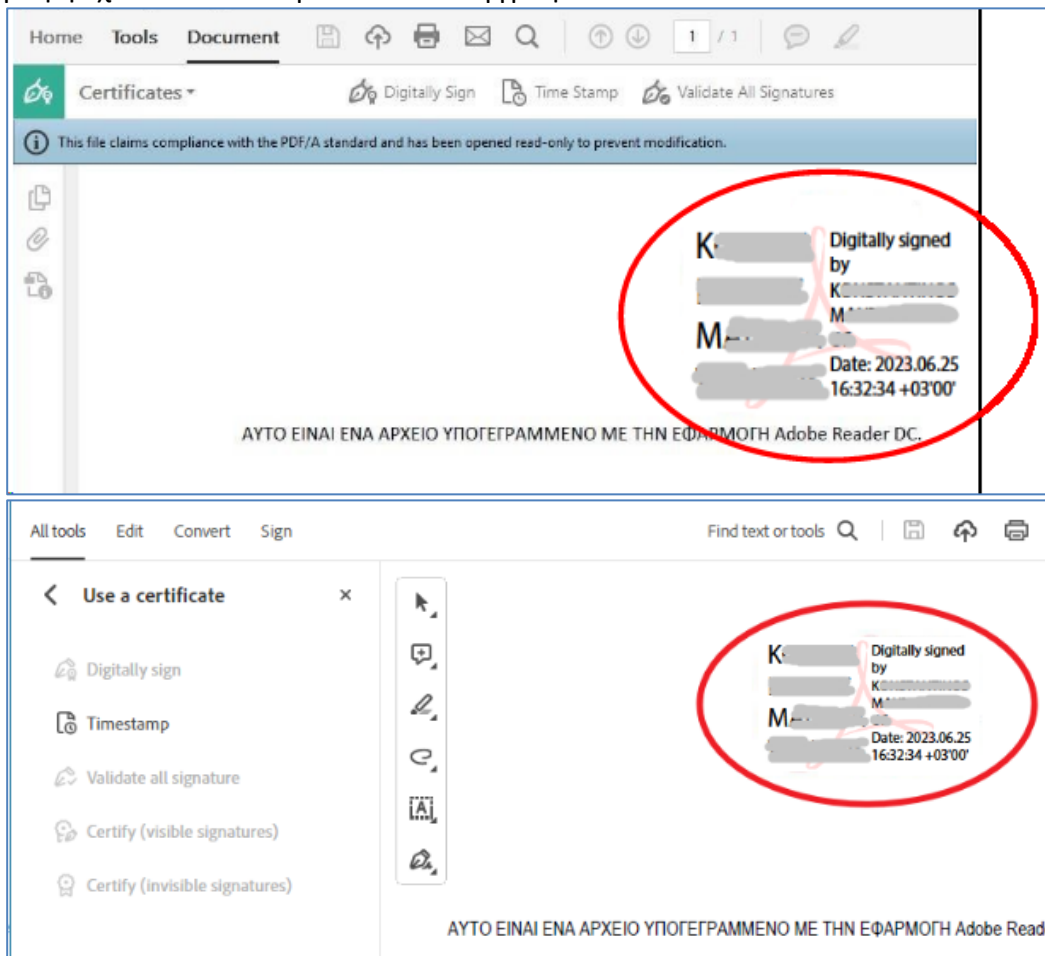
Στο παράθυρο που εμφανίζεται επιλέγουμε το ψηφιακό πιστοποιητικό που θα χρησιμοποιηθεί για την υπογραφή και πατάμε **Continue**



Προαιρετικά επιλέγουμε τη μορφή απεικόνισης της υπογραφής (Appearance), εισάγουμε το **PIN** της συσκευής και πατάμε **Sign**



Η ψηφιακή υπογραφή έχει πλέον ενσωματωθεί στο έγγραφο.



ΓΕΝΙΚΗ ΠΑΡΑΤΗΡΗΣΗ

Για υπολογιστές με **επεξεργαστές ARM** (Σειρά M) μπορείτε να δείτε οδηγίες για χρήση Acrobat Reader με Rosetta στο https://aped.gov.gr/wp-content/uploads/sign_acrobat_MacOS_M1_M2.pdf