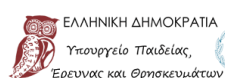


# ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΗΡΕΣΙΑ ΑΠΟΚΤΗΣΗΣ ΑΚΑΔΗΜΑΪΚΗΣ ΤΑΥΤΟΤΗΤΑΣ

## Οδηγός Διαχείρισης Ακαδημαϊκής Ταυτότητας

---

Λειτουργικό Σύστημα: Windows



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

## ΠΕΡΙΕΧΟΜΕΝΑ

1. Εγκατάσταση Λογισμικού (Classic Client) .....	4
2. Drivers Αναγνώστη/Εγγραφέα .....	6
3. Διαχείριση PIN .....	7
3.1. Αλλαγή PUK.....	8
3.2. Αλλαγή PIN.....	10
3.3. Αποδέσμευση PIN .....	12
4. Προαπαιτούμενες Ενέργειες .....	14
5. Έκδοση Ψηφιακών Πιστοποιητικών .....	18
6. Χρήση Ψηφιακών Πιστοποιητικών σε Mozilla Thunderbird .....	24
6.1. Φόρτωση Συσκευής Ασφαλείας .....	24
6.2. Ψηφιακή Υπογραφή E-mail .....	26
6.3. Κρυπτογράφηση / Αποκρυπτογράφηση E-mail .....	30
7. Χρήση Ψηφιακών Πιστοποιητικών σε Microsoft Outlook 2013.....	31
7.1. Ψηφιακή Υπογραφή E-mail .....	31
7.2. Κρυπτογράφηση / Αποκρυπτογράφηση E-mail .....	34
8. Υπογραφή PDF .....	35

Η ακαδημαϊκή ταυτότητα που έχετε στην κατοχή σας, φέρει πλινθίο αποτελούμενο από επεξεργαστή (CPU), μνήμη (ROM, EEPROM, RAM), ειδικό λογισμικό (Card Operating System) και ειδικά χαρακτηριστικά ασφαλείας.

Έχετε την δυνατότητα να ενσωματώσετε στην ακαδημαϊκή σας ταυτότητα Ψηφιακά Πιστοποιητικά, τα οποία μπορούν να χρησιμοποιηθούν:

- για την ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων (e-mail) ή εγγράφων (αρχεία .pdf)
- για την κρυπτογράφηση/αποκρυπτογράφηση ηλεκτρονικών μηνυμάτων

Συγκεκριμένα, η ακαδημαϊκή σας ταυτότητα έχει ελεύθερο χώρο για την ενσωμάτωση 12 πιστοποιητικών. Πιο αναλυτικά, υπάρχει χώρος για:

- 4 πιστοποιητικά με μέγεθος 2048bits, με δυνατότητα υπογραφής και αποκρυπτογράφησης
- 4 πιστοποιητικά με μέγεθος 2048bits, με δυνατότητα υπογραφής αλλά όχι αποκρυπτογράφησης
- 2 πιστοποιητικά με μέγεθος 1024bits, με δυνατότητα υπογραφής και αποκρυπτογράφησης
- 2 πιστοποιητικά με μέγεθος 1024bits, με δυνατότητα υπογραφής αλλά όχι αποκρυπτογράφησης

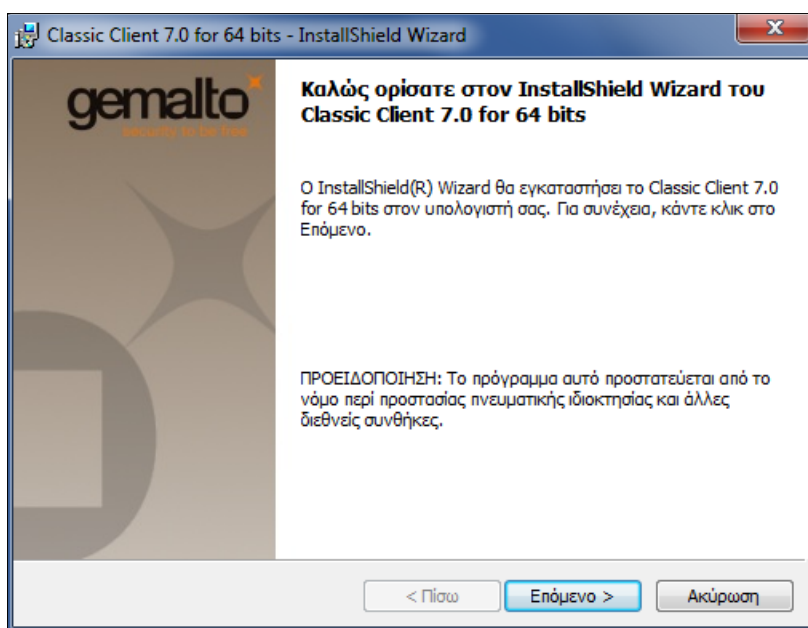
## 1. Εγκατάσταση Λογισμικού (Classic Client)

Για τη διαχείριση της Ακαδημαϊκής Ταυτότητας σε περιβάλλον Windows, είναι απαραίτητη η εγκατάσταση του διαθέσιμου λογισμικού (Classic Client) για τον αναγνώστη/εγγραφέα της ταυτότητας. Μέσω του Client μπορείτε να αλλάξετε το PIN/PUK της κάρτας και να διαχειριστείτε τα ψηφιακά πιστοποιητικά αυτής.

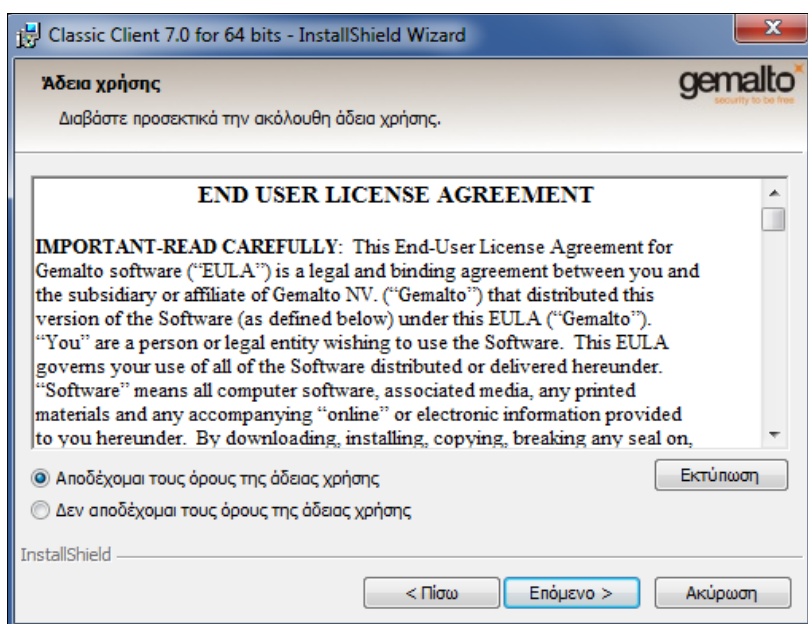
Αρχικά θα πρέπει να πραγματοποιήσετε λήψη του διαθέσιμου Client από [εδώ](#).

Σημείωση: Οδηγίες για να βρείτε αν τα Windows είναι 32 ή 64 bit υπάρχουν [εδώ](#).

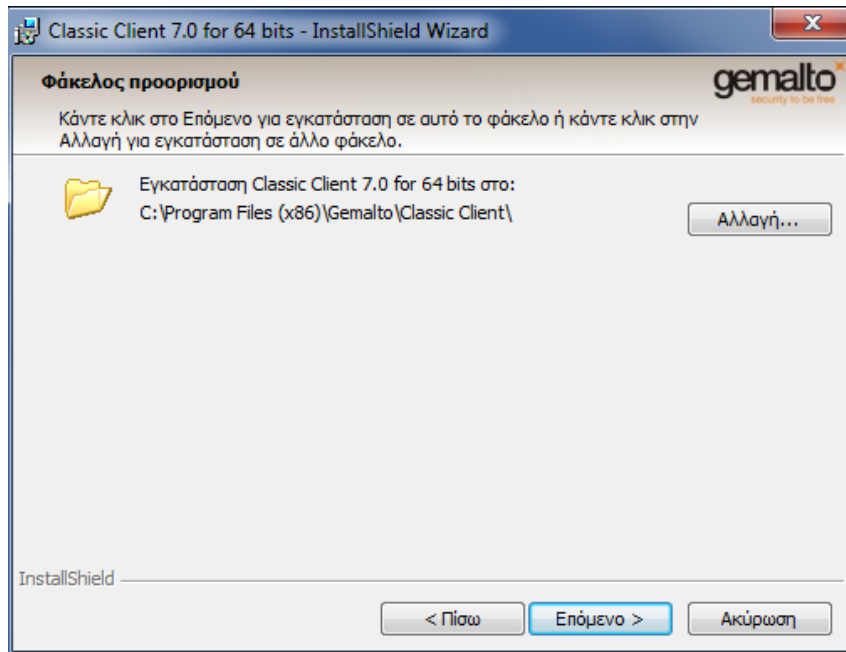
Έπειτα, αφού βρείτε το αρχείο που κατεβάσατε μπορείτε να ξεκινήσετε την εγκατάσταση κάνοντας διπλό κλικ πάνω σε αυτό. Στην οθόνη που θα εμφανιστεί πατήστε «Επόμενο» για να προχωρήσετε.



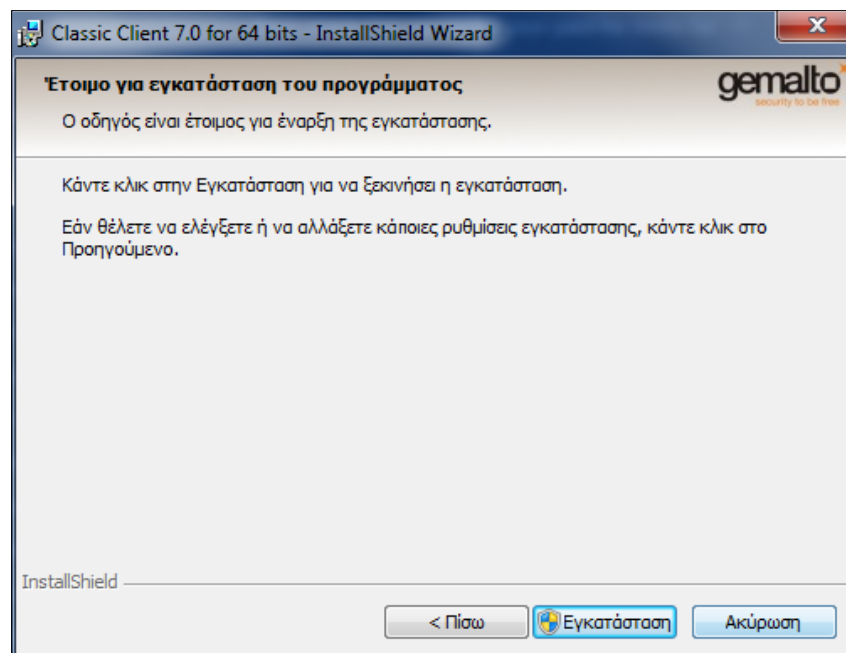
Αφού αποδεχτείτε τους όρους της άδειας χρήσης πατήστε «Επόμενο» για να προχωρήσετε.



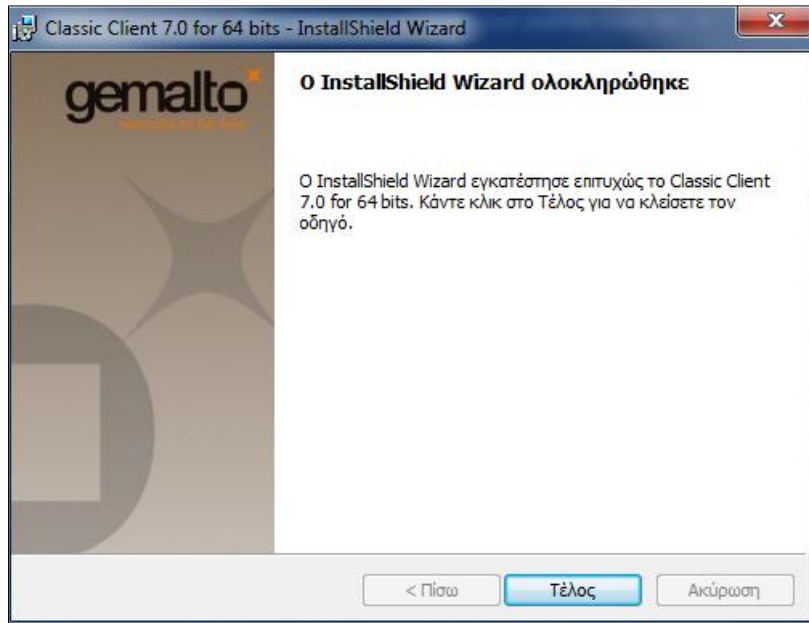
Στο επόμενο παράθυρο που θα εμφανιστεί μπορείτε να επιλέξετε σε ποιον φάκελο επιθυμείτε να γίνει η εγκατάσταση του προγράμματος πατώντας στο κουμπί «Αλλαγή» ή να προχωρήσετε επιλέγοντας τον προκαθορισμένο φάκελο που έχει επιλεγεί πατώντας «Επόμενο».



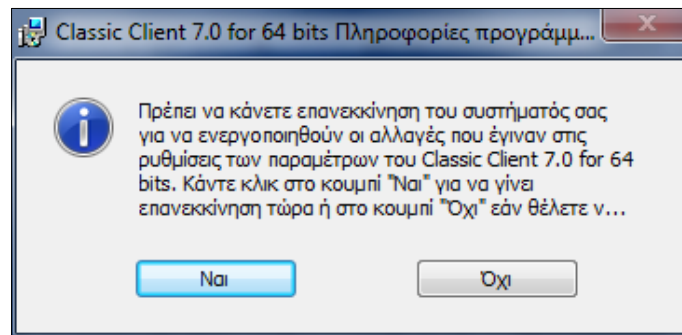
Στο τελευταίο βήμα της εγκατάστασης, εφόσον δεν επιθυμείτε να κάνετε κάποια αλλαγή στις προηγούμενες ρυθμίσεις εγκατάστασης, πατήστε το κουμπί «Εγκατάσταση» για να ολοκληρωθεί η διαδικασία.



Μόλις ολοκληρωθεί η εγκατάσταση μπορείτε πλέον να κλείσετε το πρόγραμμα εγκατάστασης πατώντας στο κουμπί «Τέλος».



Προκειμένου να ενεργοποιηθούν οι αλλαγές που έγιναν στις ρυθμίσεις των παραμέτρων του Classic Client θα πρέπει να κάνετε επανεκκίνηση του συστήματός σας. Αυτό μπορεί να γίνει επιλέγοντας «Ναι» στο πλαίσιο διαλόγου που θα εμφανιστεί ή να κάνετε επανεκκίνηση αργότερα οπότε και θα πρέπει να επιλέξετε «Όχι» στο ίδιο πλαίσιο.



## 2. Drivers Αναγνώστη/Εγγραφέα

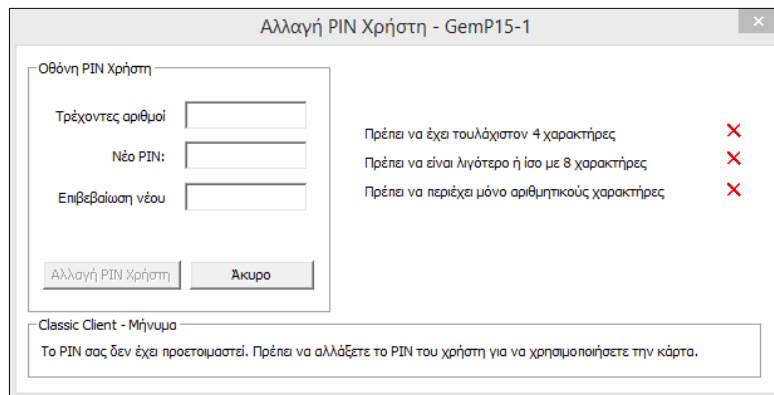
Για να χρησιμοποιήσετε την Ακαδημαϊκή Ταυτότητα θα πρέπει να συνδέσετε τον αναγνώστη/εγγραφέα στον υπολογιστή σας.

Εάν η συσκευή δεν αναγνωριστεί αυτόματα στον υπολογιστή σας, πιθανώς χρειάζεται να εγκαταστήσετε τους τελευταίους drivers για την συσκευή. Μπορείτε να κατεβάσετε τους drivers από την ακόλουθη σελίδα σύμφωνα με το λειτουργικό σύστημα του υπολογιστή σας:

[http://support.gemalto.com/index.php?id=pc\\_usb\\_tr\\_and\\_pc\\_twin#.VPQ9GOFGRfl](http://support.gemalto.com/index.php?id=pc_usb_tr_and_pc_twin#.VPQ9GOFGRfl)

### 3. Διαχείριση PIN

Την πρώτη φορά που θα συνδέσετε την Ακαδημαϊκή σας Ταυτότητα στον υπολογιστή σας μέσω του αναγνώστη/εγγραφέα θα σας ζητηθεί να αλλάξετε το PIN της κάρτας.



Η διαχείριση του PIN σας επιτρέπει να πραγματοποιείτε αλλαγές στο PIN που σχετίζεται με την κάρτα που έχετε στην κατοχή σας. Σας επιτρέπει επίσης να κάνετε επισκόπηση της πολιτικής του PIN που έχει ήδη οριστεί για αυτή την συγκεκριμένη εγκατάσταση.

Στην προκειμένη περίπτωση, η πολιτική για τον ορισμό του PIN περιλαμβάνει τους ακόλουθους κανόνες:

- Θα πρέπει να αποτελείται από τουλάχιστον 4 χαρακτήρες
- Δεν θα πρέπει να αποτελείται από περισσότερους από 8 χαρακτήρες
- Θα πρέπει να περιέχει μόνο αριθμητικούς χαρακτήρες

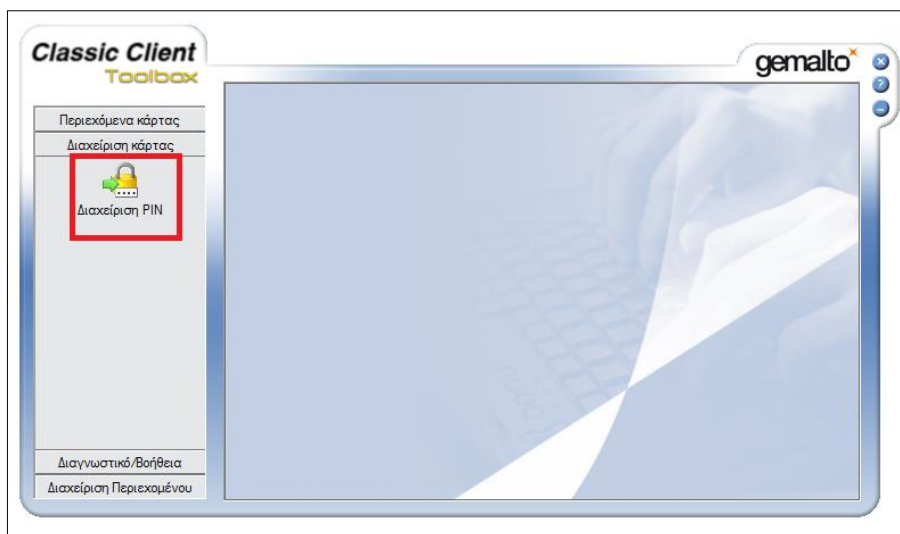
Για να αποκτήσετε πρόσβαση στην διαχείριση του PIN αρχικά θα πρέπει να έχετε συνδέσει την κάρτα σας στον αναγνώστη. Έπειτα από τον φάκελο εγκατάστασης του Classic Client θα πρέπει να εκτελέσετε την εφαρμογή "Classic Client Toolbox". Την εφαρμογή αυτή θα την βρείτε στον φάκελο εγκατάστασης και συγκεκριμένα, στον υποφάκελο "Classic Client".

Μόλις ανοίξει η εφαρμογή θα δείτε την ακόλουθη οθόνη, από την οποία θα πρέπει να πατήσετε στην επιλογή «Διαχείριση κάρτας».

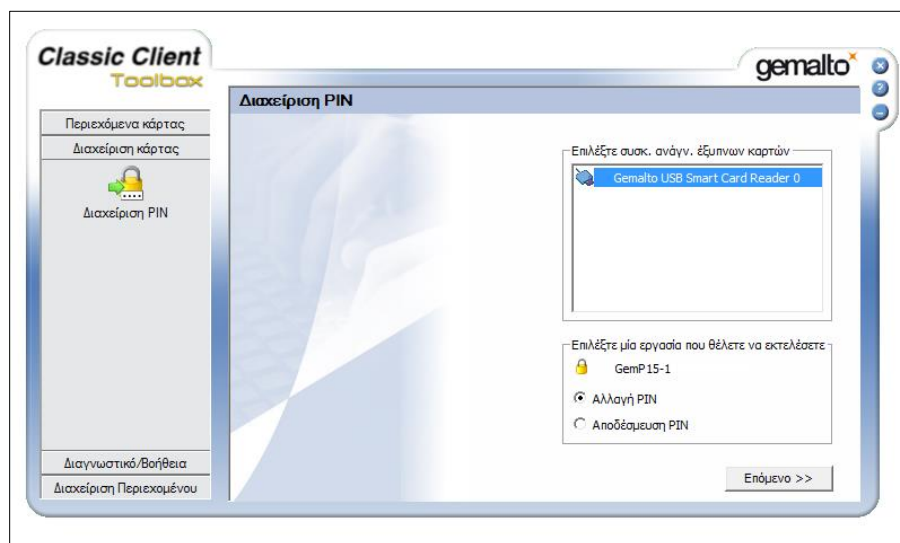




Έπειτα πατήστε πάνω στο εικονίδιο «Διαχείριση PIN» προκειμένου να συνεχίσετε.



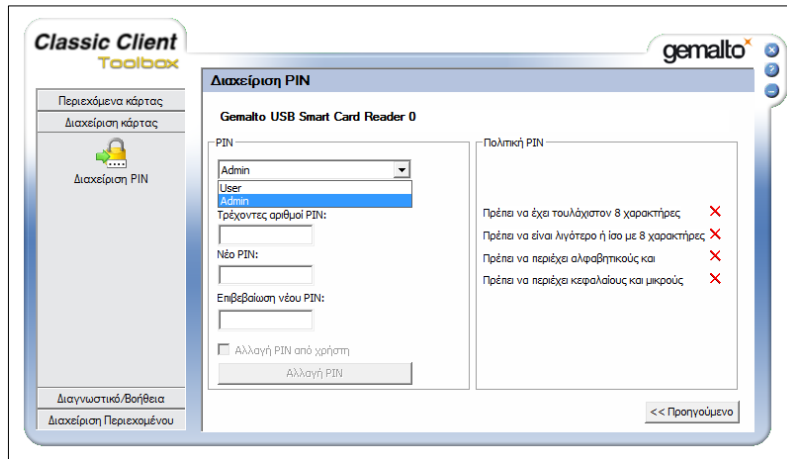
Στην επόμενη οθόνη σας δίνονται δύο δυνατότητες. Αρχικά μπορείτε να πραγματοποιήσετε αλλαγή του PIN σας ή να κάνετε αποδέσμευση του PIN εάν έχει δεσμευτεί μετά από 3 μη επιτυχημένες προσπάθειες σύνδεσης. Επιλέξτε λοιπόν ποια ενέργεια θέλετε να πραγματοποιήσετε και πατήστε στο κουμπί «Επόμενο».



### 3.1. Αλλαγή ΡΥΚ

Για την αλλαγή του ΡΥΚ (Admin PIN) και εφόσον έχετε ακολουθήσει τα παραπάνω βήματα, θα πρέπει να επιλέξετε αρχικά την επιλογή "Admin" από τη λίστα που εμφανίζεται.

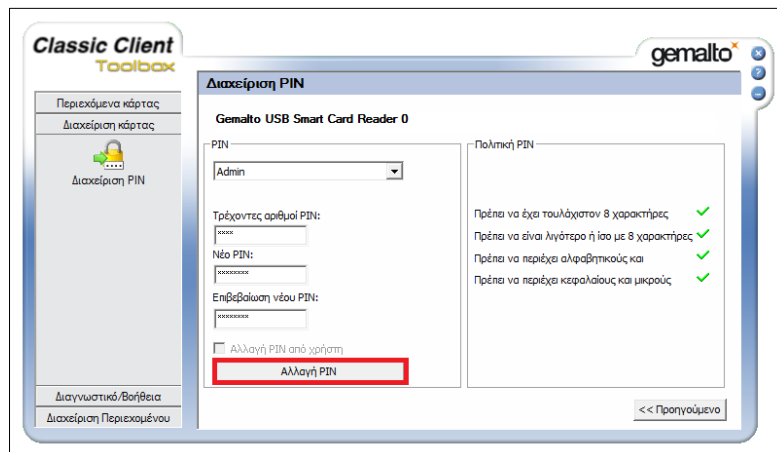




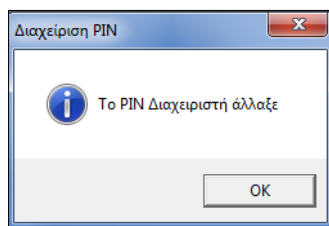
Στη συνέχεια θα πρέπει να συμπληρώσετε το τρέχον ΡΥΚ σας στο πεδίο «Τρέχοντες αριθμοί PIN», το νέο ΡΥΚ που επιθυμείτε στο πεδίο «Νέο PIN» καθώς και μια επιβεβαίωση του νέου ΡΥΚ, στο πεδίο «Επιβεβαίωση νέου PIN», για λόγους ασφαλείας. Επισημαίνεται ότι η πολιτική για τον κωδικό ΡΥΚ διαφέρει σε σχέση με αυτή που είχε αναφερθεί παραπάνω και αφορούσε το PIN σας. Συγκεκριμένα σε αυτή την περίπτωση θα πρέπει να ισχύουν οι ακόλουθοι κανόνες:

- Θα πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες
- Δεν θα πρέπει να ξεπερνάει τους 8 χαρακτήρες
- Θα πρέπει να περιέχει αλφαβητικούς και
- Θα πρέπει να περιέχει κεφαλαίους και μικρούς χαρακτήρες

Μόλις συμπληρώσετε τα απαραίτητα πεδία πατήστε το κουμπί «Αλλαγή PIN» για να ολοκληρωθεί η αλλαγή.



Εάν η ενέργεια πραγματοποιηθεί επιτυχώς εμφανίζεται σχετικό παράθυρο επιβεβαίωσης.



### 3.2. Αλλαγή PIN

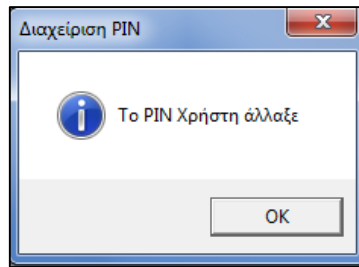
Η διαδικασία που πρέπει να ακολουθήσετε για την αλλαγή του PIN (User PIN) είναι παρόμοια με αυτή που παρουσιάστηκε παραπάνω για το PUK (Admin PIN). Εφόσον έχετε επιλέξει να κάνετε αλλαγή του PIN, θα πρέπει να επιλέξετε αυτή την φορά την επιλογή "User".

Έπειτα θα πρέπει να συμπληρώσετε το τρέχον PIN σας και το νέο με το οποίο επιθυμείτε να το αντικαταστήσετε καθώς επίσης και μια επιβεβαίωση αυτού. Για την αντικατάσταση του PIN ως απλός χρήστης ισχύουν οι παρακάτω κανόνες:

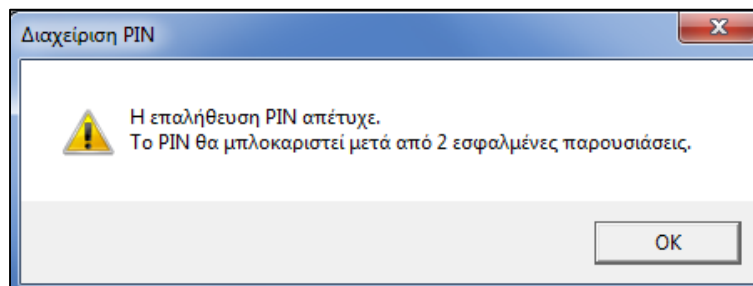
- Θα πρέπει να αποτελείται από τουλάχιστον 4 χαρακτήρες
- Δεν θα πρέπει να ξεπερνάει τους 8 χαρακτήρες
- Θα πρέπει να περιέχει μόνο αριθμητικούς χαρακτήρες

Μόλις συμπληρώσετε τα απαραίτητα πεδία πατήστε στο κουμπί «Αλλαγή PIN» για να πραγματοποιηθεί η αλλαγή.

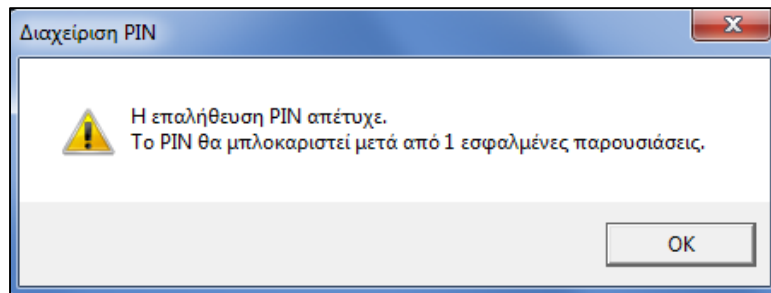
Όμοια με πριν ένα παράθυρο επιβεβαίωσης θα εμφανιστεί σε περίπτωση που η ενέργεια σας ολοκληρωθεί επιτυχώς.



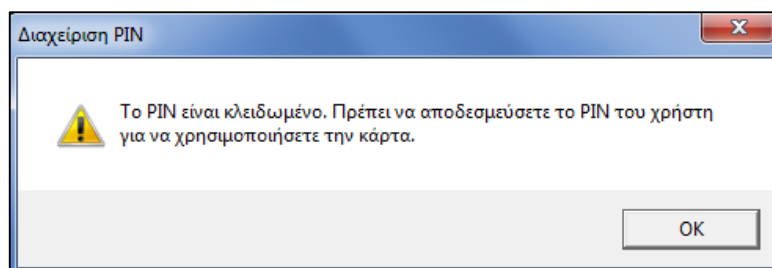
Σε περίπτωση που το τρέχον PIN που θα συμπληρώσετε δεν είναι σωστό, εμφανίζεται προειδοποιητικό μήνυμα το οποίο σας ενημερώνει για την αποτυχία επαλήθευσης του PIN καθώς επίσης και για τις υπολειπόμενες προσπάθειες που έχουν απομείνει. Σημειώνεται ότι εάν συμπληρώσετε λανθασμένα το PIN σας 3 διαδοχικές φορές, το PIN δεσμεύεται και θα πρέπει να ακολουθήσετε την διαδικασία αποδέσμευσης που περιγράφεται παρακάτω.



Όπως φαίνεται και στις αντίστοιχες εικόνες, σε κάθε αποτυχημένη συμπλήρωση του PIN σας, εμφανίζεται σχετικό μήνυμα.



Εάν το PIN δεσμευτεί, θα εμφανιστεί το ακόλουθο μήνυμα το οποίο σας ενημερώνει για την διαδικασία που πρέπει να ακολουθήσετε.



### 3.3. Αποδέσμευση PIN

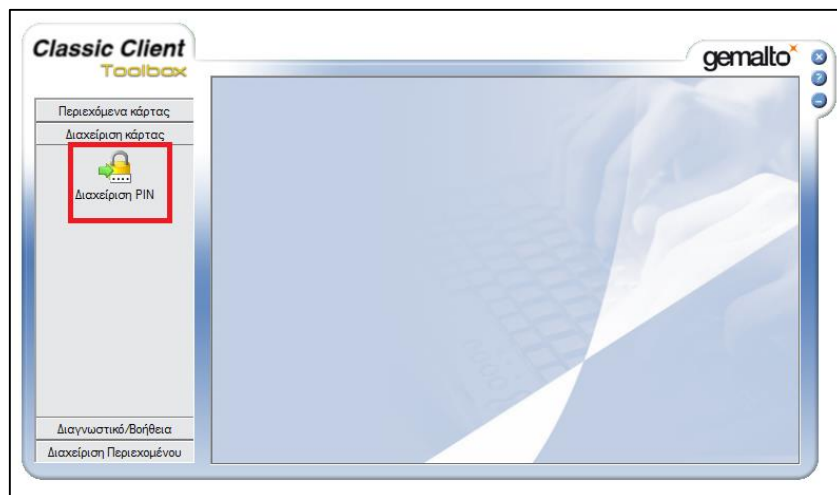
Ως διαχειριστής μπορείτε να χρησιμοποιήσετε την εφαρμογή αυτή για να αποδεσμεύσετε το PIN σας μέσω του ΡΥΚ, το οποίο μπορεί να δεσμευτεί μετά από συνεχόμενες αποτυχημένες προσπάθειες εισαγωγής του σωστού PIN.

Για να αποδεσμεύσετε λοιπόν το PIN που χρησιμοποιείτε ως χρήστης θα πρέπει να ακολουθήσετε τα παρακάτω βήματα:

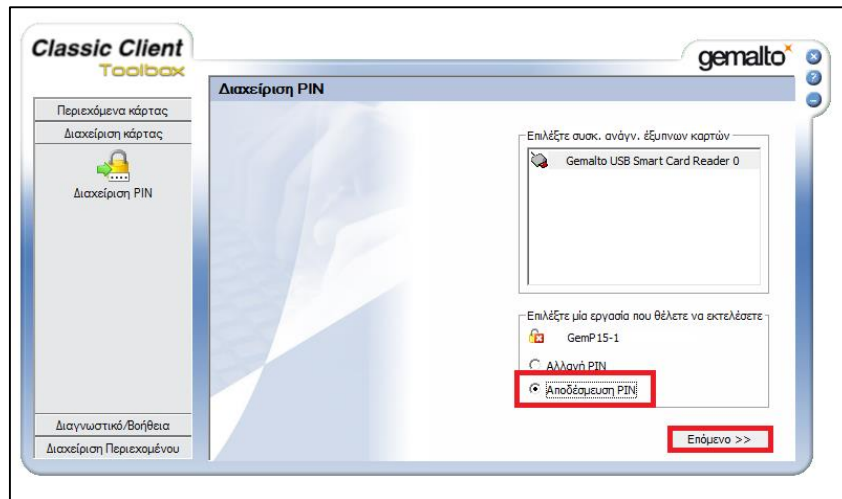
1. Επιλέξτε «Διαχείριση κάρτας»



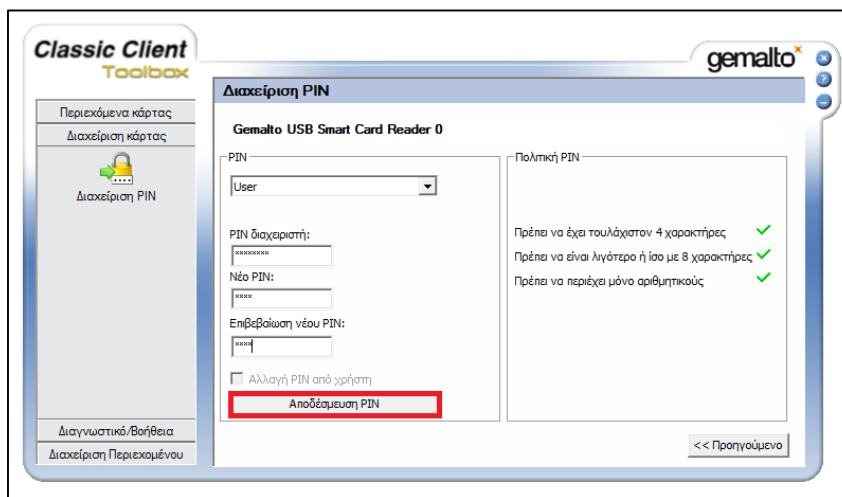
2. Επιλέξτε «Διαχείριση PIN»



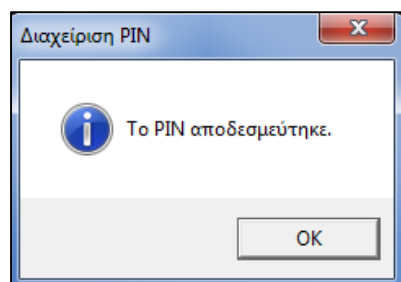
3. Επιλέξτε ως εργασία την «Αποδέσμευση PIN» και πατήστε «Επόμενο» για να συνεχίσετε.



4. Συμπληρώστε το PUK στο πεδίο «PIN διαχειριστή», το νέο PIN που επιθυμείτε να χρησιμοποιείτε ως χρήστης, μια επιβεβαίωση αυτού και πατήστε το κουμπί «Αποδέσμευση PIN».



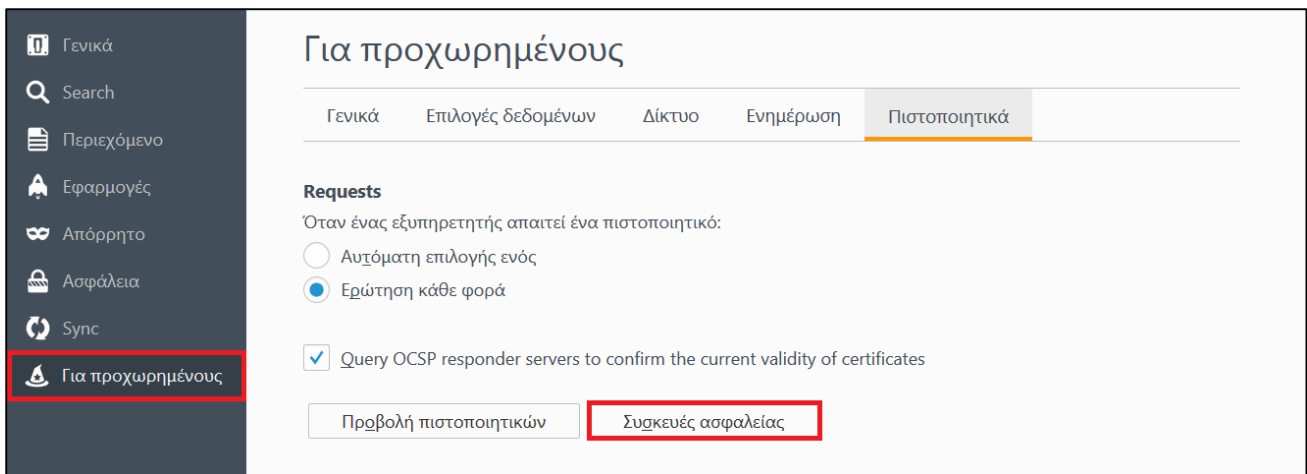
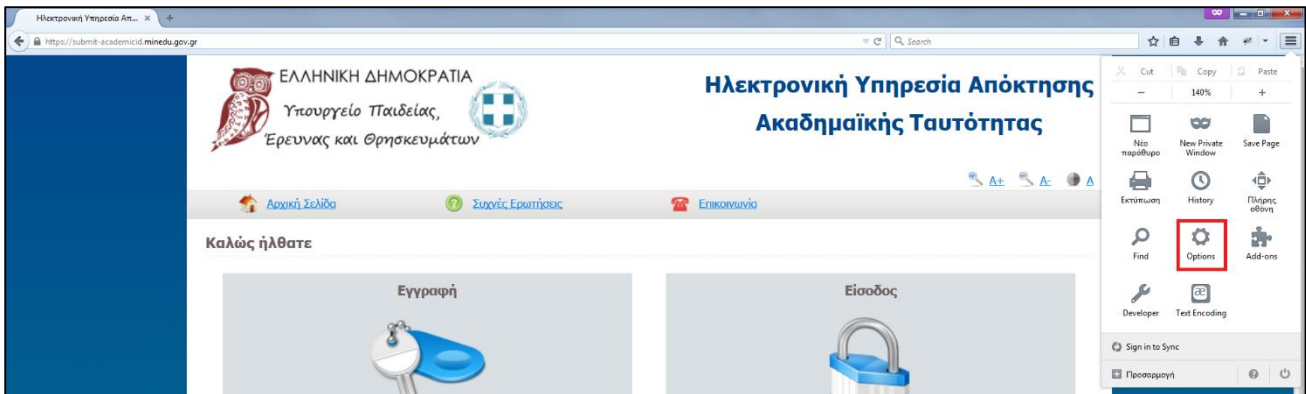
Εφόσον ολοκληρώσετε επιτυχώς την αποδέσμευση του PIN θα εμφανιστεί σχετικό ενημερωτικό μήνυμα.



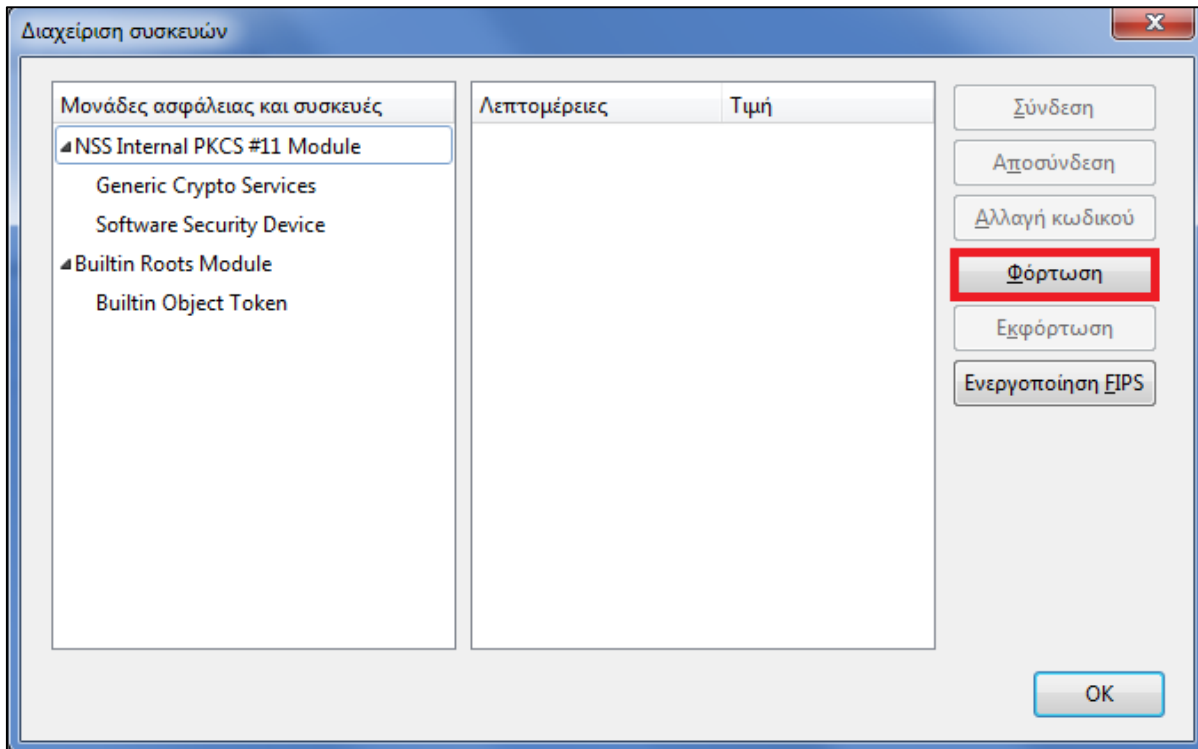
## 4. Προαπαιτούμενες Ενέργειες

Στην παράγραφο αυτή περιγράφονται οι ρυθμίσεις που θα πρέπει να γίνουν στον περιηγητή **Mozilla Firefox** ώστε να είναι δυνατή η ενσωμάτωση ψηφιακών πιστοποιητικών υπογεγραμμένων από την αρχή πιστοποίησης DigiCert στην ακαδημαϊκή ταυτότητα.

Αρχικά θα πρέπει να μεταβείτε στις ρυθμίσεις του Mozilla Firefox και στη συνέχεια στην επιλογή «Συσκευές ασφαλείας» όπως φαίνεται και στις εικόνες παρακάτω.

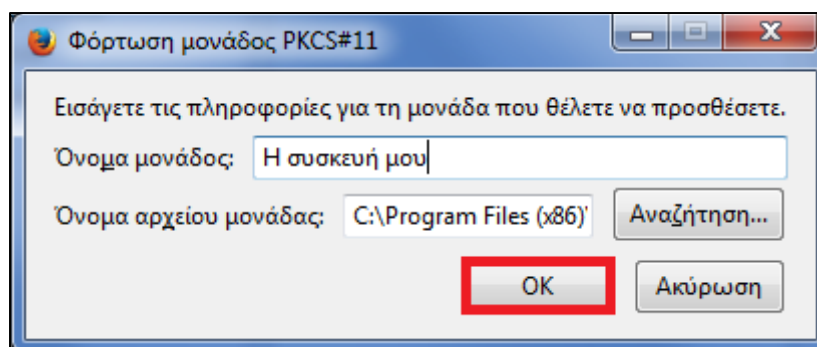


Στο νέο παράθυρο που θα ανοίξει, πατήστε «Φόρτωση» προκειμένου να φορτώσετε τη συσκευή ανάγνωσης που έχετε στην κατοχή σας.



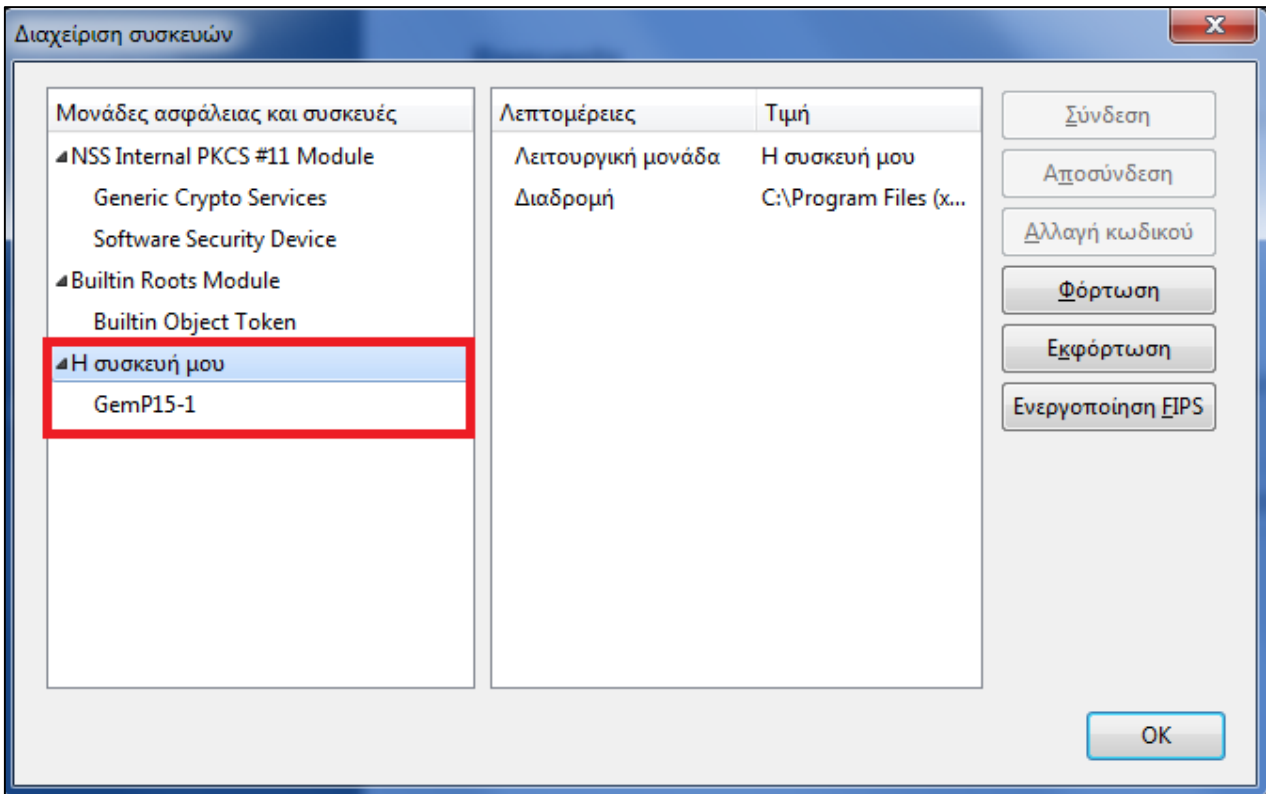
Στη συνέχεια καλείστε αρχικά να συμπληρώσετε ένα αναγνωριστικό όνομα για τη συσκευή και στη συνέχεια να επιλέξετε το αρχείο "gclib.dll" από τον φάκελο εγκατάστασης του Classic Client. Το αρχείο αυτό βρίσκεται στο μονοπάτι "\install dir\BIN". Εάν χρησιμοποιείτε 32-bit έκδοση των Windows, τότε ο προεπιλεγμένος φάκελος εγκατάστασης του αρχείου αυτού είναι ο "C:\Program Files\Gemalto\Classic Client\".

Διαφορετικά, εάν η έκδοση των Windows είναι 64 bit, ο φάκελος εγκατάστασης είναι ο "C:\Program Files (x86)\Gemalto\Classic Client\BIN". Αφού συμπληρώσετε τα παραπάνω πεδία πατήστε "OK" για να προχωρήσετε.

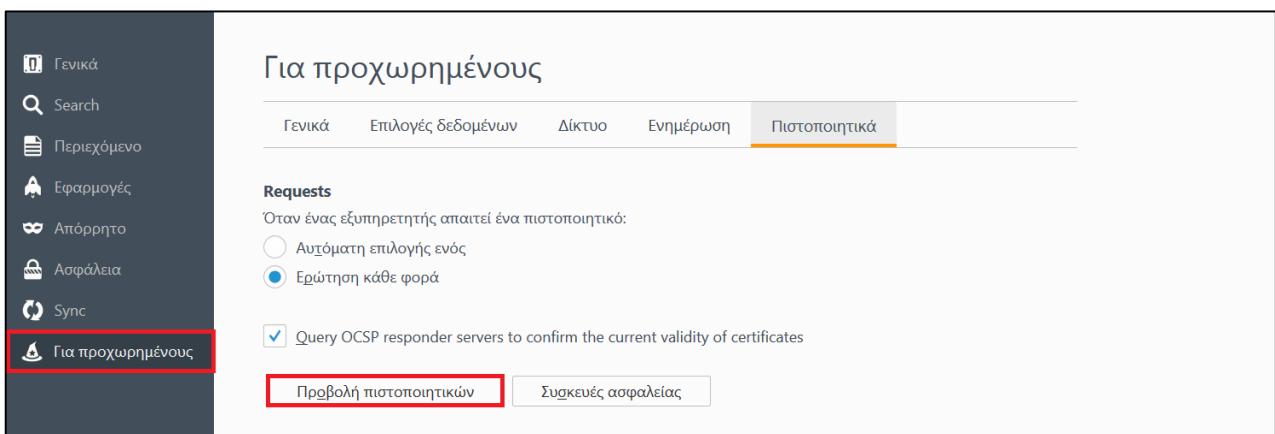




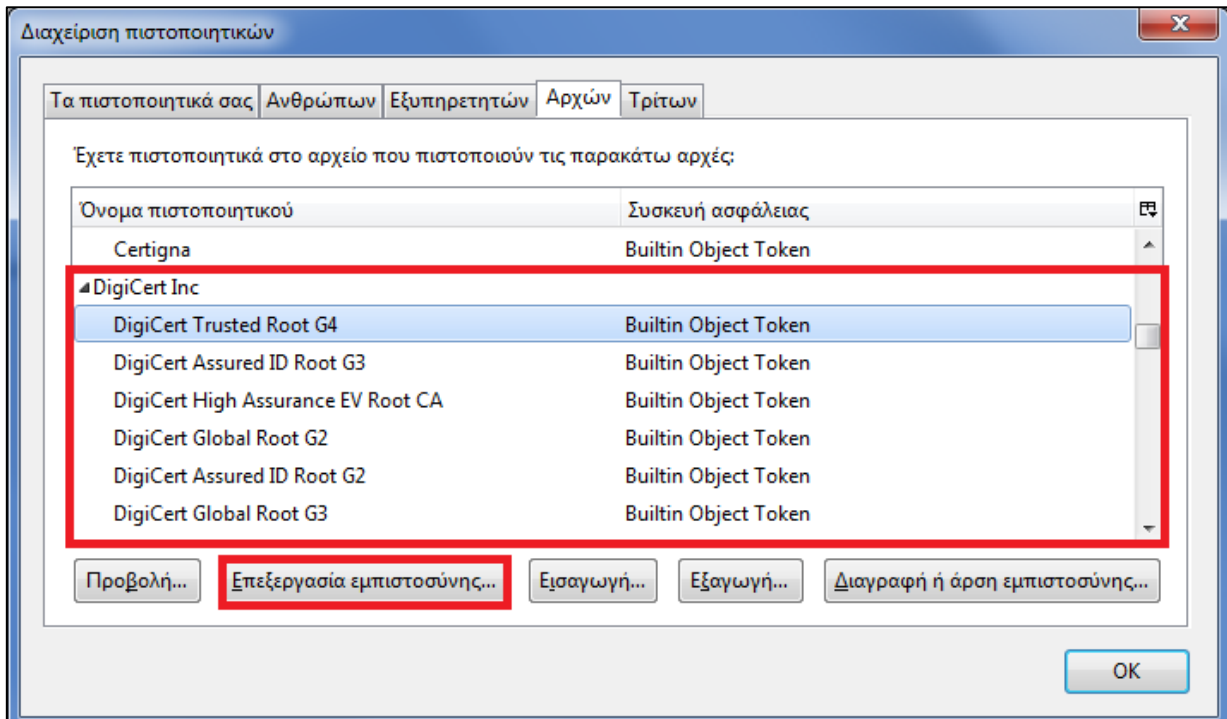
Εφόσον η ενέργεια έχει πραγματοποιηθεί επιτυχώς, θα πρέπει να βλέπετε τη συσκευή που προσθέσατε στα αριστερά της λίστας με τις συσκευές ασφαλείας. Στο παράθυρο αυτό πατήστε ξανά “OK” για να το κλείσετε.



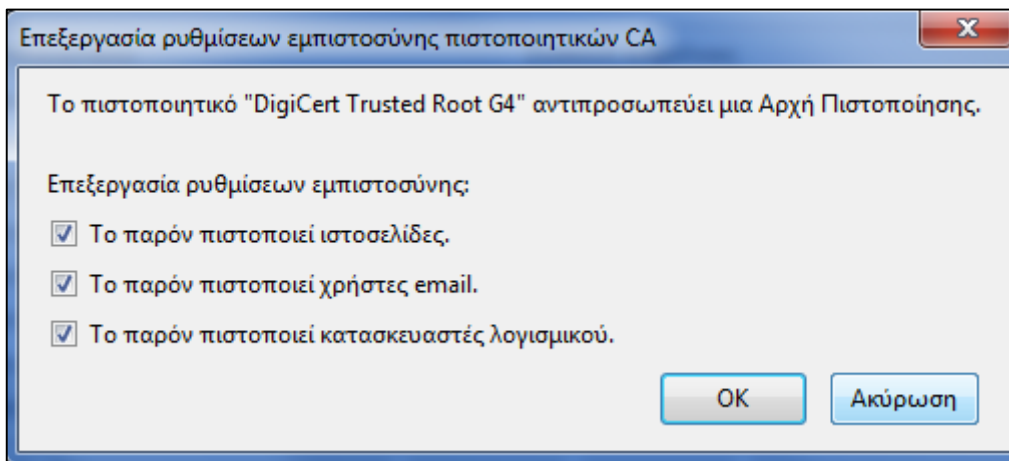
Έπειτα πατήστε στο κουμπί «Προβολή πιστοποιητικών» για να συνεχίσετε. Θα σας ζητηθεί να εισάγετε το PIN της κάρτας για την διαχείριση των πιστοποιητικών.



Στη συνέχεια θα πρέπει ανάλογα με την αρχή πιστοποίησης που εκδίδει το εν λόγω πιστοποιητικό να τροποποιήσετε τις ρυθμίσεις εμπιστοσύνης για κάθε πιστοποιητικό του που έχει ενσωματωθεί στον Mozilla Firefox. Στην προκειμένη περίπτωση, για την αρχή πιστοποίησης “Digicert Inc” επιλέξτε κάθε πιστοποιητικό που βρίσκεται κάτω από την αρχή Digicert Inc και πατήστε στο κουμπί «Επεξεργασία εμπιστοσύνης...».



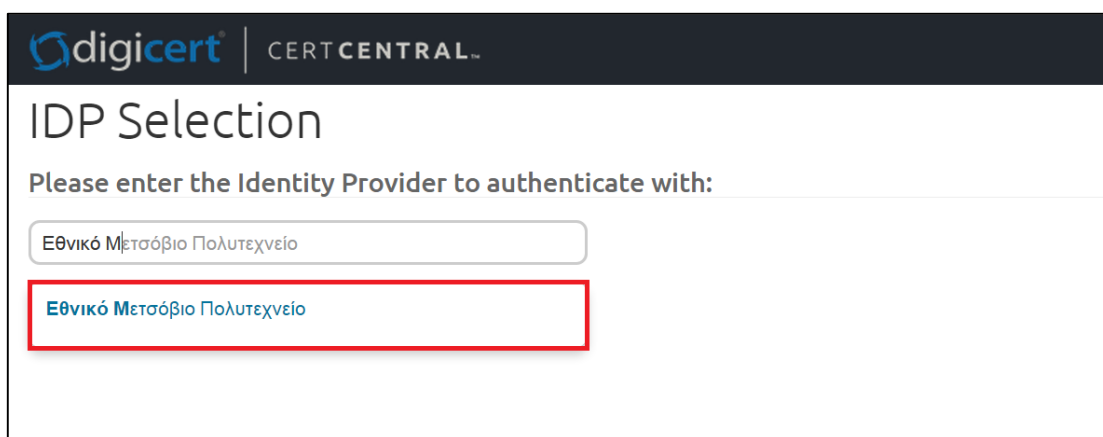
Στο παράθυρο που θα ανοίξει, φροντίστε και οι τρεις ρυθμίσεις εμπιστοσύνης να είναι επιλεγμένες και πατήστε «OK». Αφού πραγματοποιήσετε την ενέργεια αυτή για κάθε πιστοποιητικό, μπορείτε να κλείσετε το παράθυρο ρυθμίσεων του Mozilla Firefox.



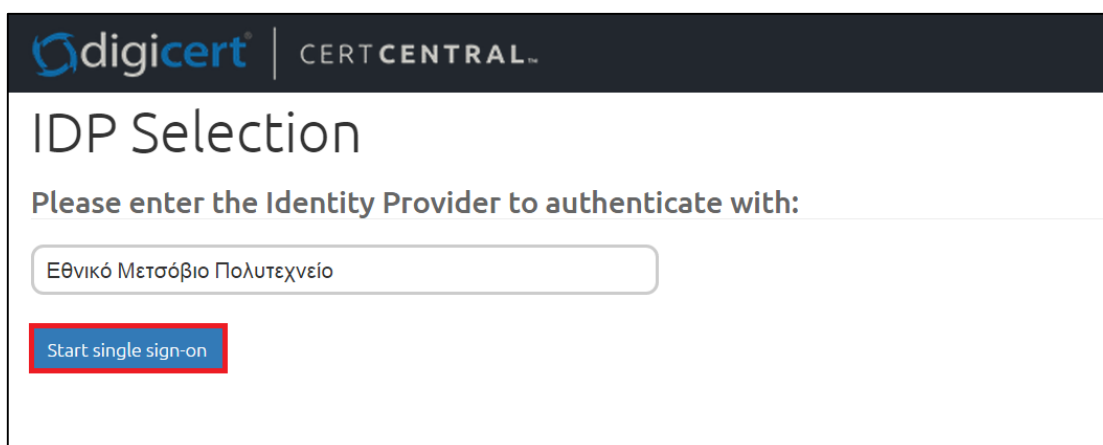
## 5. Έκδοση Ψηφιακών Πιστοποιητικών

Η δυνατότητα έκδοσης Ψηφιακών Πιστοποιητικών υπογεγραμμένων από την αρχή πιστοποίησης DigiCert είναι διαθέσιμη από εδώ: <https://www.digicert.com/sso>. Παρακάτω ακολουθούν αναλυτικές οδηγίες για δημιουργία και λήψη του προσωπικού σας ψηφιακού πιστοποιητικού προκειμένου να το χρησιμοποιήσετε σε λειτουργίες που περιγράφονται σε επόμενες ενότητες.

Πατώντας λοιπόν στον σύνδεσμο παραπάνω για τη δημιουργία και λήψη του προσωπικού σας ψηφιακού πιστοποιητικού εμφανίζεται η ακόλουθη σελίδα στην οποία θα πρέπει να πληκτρολογήσετε το Ίδρυμα/Φορέα στο οποίο ανήκετε και να το επιλέξετε στη λίστα που εμφανίζεται από κάτω.



Στη συνέχεια θα πρέπει να πατήσετε στο κουμπί “Start single sign-on” για να συνεχίσετε με τη σύνδεση σας μέσω του ιδρυματικού σας λογαριασμού.



Στη νέα σελίδα που θα ανοίξει θα πρέπει να εισάγετε τα ακαδημαϊκά σας διαπιστευτήρια για να συνεχίσετε.

**Θα πρέπει να σημειωθεί ότι αν η σύνδεσή σας δεν είναι εφικτή, πιθανώς το οικείο σας Ίδρυμα/Φορέας δεν έχει προβεί στις απαραίτητες ενέργειες ώστε να είναι δυνατή η έκδοση ψηφιακών πιστοποιητικών μέσω της συγκεκριμένης αρχής πιστοποίησης από τα μέλη του προσωπικού.**

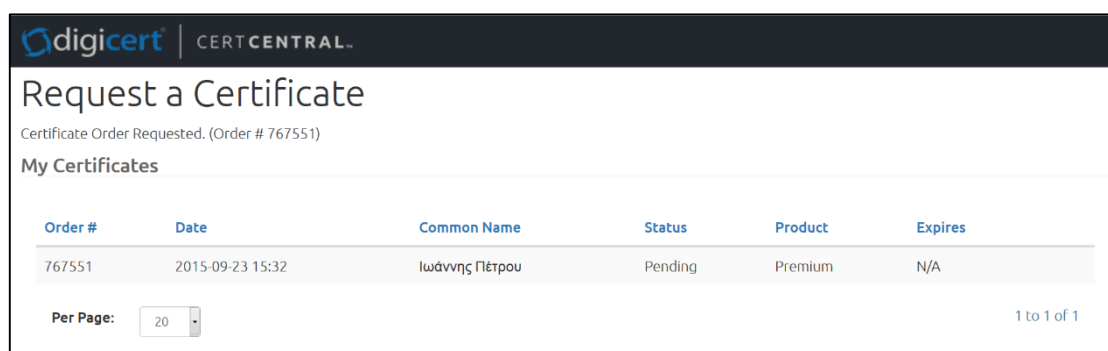
Αφού συνδεθείτε, μπορείτε να προχωρήσετε στην δημιουργία και έπειτα στη λήψη του προσωπικού πιστοποιητικού σας. Στο πεδίο “Product” που εμφανίζεται θα πρέπει να επιλέξετε την κατηγορία “Premium” και να αφήσετε κενό το πεδίο “CSR”.

Order #	Date	Common Name	Status	Product	Expires
No Certificates Found.					

Παρακάτω εμφανίζονται τα στοιχεία σας (Όνομα και E-mail) όπως αυτά επιστρέφονται από το οικείο σας Ίδρυμα/Φορέα. Για να δημιουργήσετε το πιστοποιητικό σας αρκεί να πατήσετε στο κουμπί “Request Certificate”.

Order #	Date	Common Name	Status	Product	Expires
No Certificates Found.					

Στη νέα σελίδα που θα ανοίξει μπορείτε να δείτε το πιστοποιητικό το οποίο ζητήσατε να δημιουργηθεί. Παράλληλα θα λάβετε ένα e-mail στο e-mail που εμφανίζεται και στα στοιχεία σας σύμφωνα με την προηγούμενη εικόνα.



Order #	Date	Common Name	Status	Product	Expires
767551	2015-09-23 15:32	Ιωάννης Πέτρου	Pending	Premium	N/A

Για να κάνετε λήψη του πιστοποιητικού και το φορτώσετε στην ταυτότητά σας, θα πρέπει αρχικά να έχετε συνδέσει την κάρτα στη συσκευή ανάγνωσης και τη συσκευή στον υπολογιστή σας. Έπειτα μόλις ανοίξετε το e-mail που λάβατε θα πρέπει να επιλέξετε τον σύνδεσμο προκειμένου να φορτώσετε το πιστοποιητικό στην κάρτα σας.



**Virtual Home Organization**

Hi Ιωάννης Πέτρου,

You have been approved to create a DigiCert Personal ID Certificate (Premium).

**Create your DigiCert Personal ID Certificate now by going to:**

<https://www.digicert.com/link/pid-install.php?token=ccr1n3lcv8496cm526>

Thanks!

The DigiCert Team

Στην σελίδα που θα ανοίξει καλείστε να αποδεχτείτε τους όρους χρήσης και για να συνεχίσετε θα πρέπει να πατήσετε στο κουμπί "Generate Certificate".

### Generate your DigiCert Premium Certificate

For technical assistance or to make corrections, contact your administrator.

**DigiCert Personal ID Details**

**Name:** Ιωάννης Πέτρου

**Email Addresses:** academicid@callc.grnet.gr

**Organization:** Greek Research and Technology Network

**Subscriber Agreement:**

CERTIFICATE SUBSCRIBER AGREEMENT  
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING. YOU MUST CHECK "I AGREE" BELOW TO ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT ORDER OR APPROVE THE ISSUANCE OF A DIGITAL CERTIFICATE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973. THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE  
These certificate terms of use are between DigiCert, Inc., a Utah corporation ("DigiCert") and the entity applying for a Certificate, as identified in the account or issued certificates.  
"Certificate" means a digitally signed electronic data file issued by DigiCert to a person, group, or role in order to confirm your authorization for use of the Private Key corresponding to the Public Key contained in the certificate. You and DigiCert agree as follows:  
1. Use  
1.1. Applicability. These terms cover each Certificate issued by DigiCert to you, regardless of (i) the Certificate type (email, code signing, Direct, or TLS/SSL), (ii) when you request the

I agree to the terms of the subscriber agreement

Your Personal ID will be valid for 1 year from the time it is issued. You have until October 21, 2015 to generate this certificate or you will need to contact your organization administrator to request a new email.

If your web server is configured to require "Client Authentication", you may need to configure it to allow client certs issued by DigiCert SHA2 Assured ID CA, as well as DigiCert Assured ID CA-1.

Due to new security standards, any SSL certificate expiring on or after January 1, 2017, will be issued using SHA-2 regardless of whether SHA-2 is chosen.

**Generate Certificate**

Στο νέο πλαίσιο που θα ανοίξει θα πρέπει να επιλέξετε την συσκευή ανάγνωσης που διαθέτετε και αφού πατήσετε "OK" να εισάγετε το PIN της κάρτας σας.

Επιλογή διαλόγου token

Επιλέξτε ένα token

GemP15-1

OK Ακύρωση

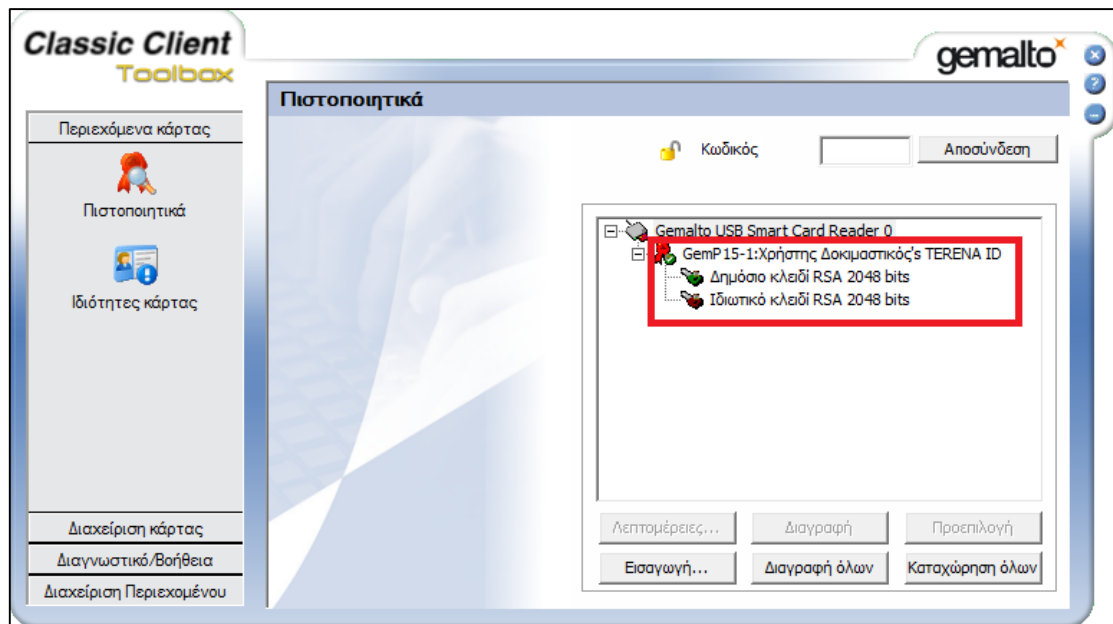
Απαιτείται κωδικός πρόσβασης

Εισάγετε τον κύριο κωδικό για το GemP15-1.

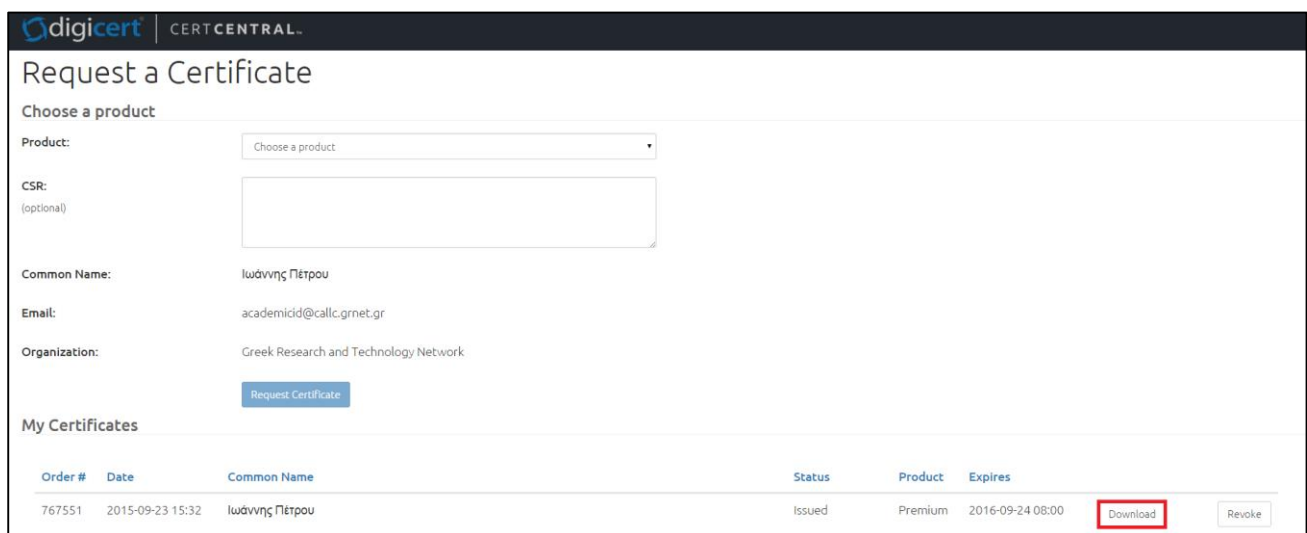
.....

OK Ακύρωση

Μόλις ανοίξετε το πρόγραμμα Classic Client για την διαχείριση της κάρτας σας και εισάγετε το PIN σας, θα πρέπει να εμφανίζεται το πιστοποιητικό το οποίο δημιουργήσατε.



Παράλληλα, αφού ολοκληρώσετε τις παραπάνω ενέργειες, υπάρχει και η δυνατότητα λήψης του πιστοποιητικού σε ξεχωριστό αρχείο μέσω της επιλογής "Download".

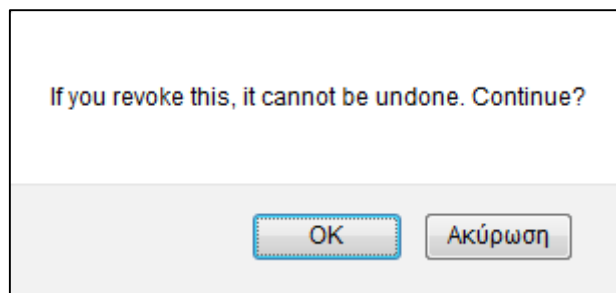


Εάν θέλετε να ακυρώσετε την ισχύ του συγκεκριμένου πιστοποιητικού, μπορείτε να προχωρήσετε σε ανάκληση αυτού πατώντας το κουμπί "Revoke".



Order #	Date	Common Name	Status	Product	Expires	
767551	2015-09-23 15:32	Ιωάννης Πέτρου	Issued	Premium	2016-09-24 08:00	Download Revoke

Για την ολοκλήρωση της ανάκλησης θα πρέπει να επιβεβαιώσετε την ενέργεια αυτή στο πλαίσιο διαλόγου που εμφανίζεται.



Εφόσον η ενέργεια πραγματοποιηθεί επιτυχώς εμφανίζεται σχετικό μήνυμα.

## 6. Χρήση Ψηφιακών Πιστοποιητικών σε Mozilla Thunderbird

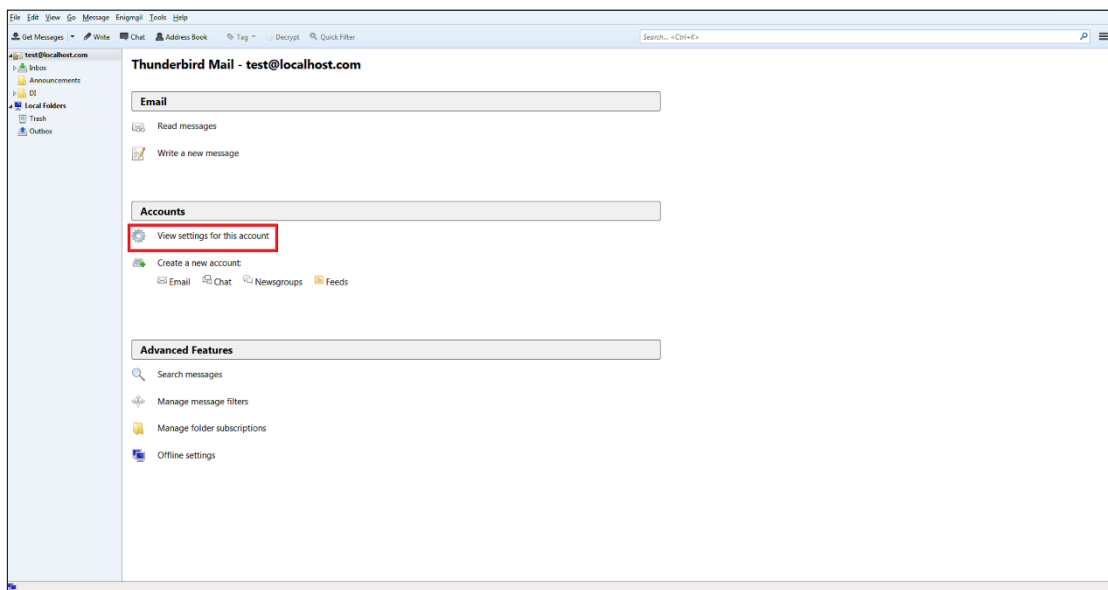
Στο κεφάλαιο αυτό περιγράφεται πώς να ρυθμίσετε και να στέλνετε e-mail με ασφαλή τρόπο χρησιμοποιώντας το πρόγραμμα Mozilla Thunderbird. Συγκεκριμένα δίνονται οδηγίες σχετικά με το πως να:

- Φορτώσετε τον αναγνώστη ως συσκευή ασφαλείας στο πρόγραμμα αυτό.
- Επιλέξετε τα πιστοποιητικά με τα οποία επιθυμείτε να υπογράψετε ψηφιακά και να κρυπτογραφήσετε τα e-mail σας.
- Στείλετε τα παραπάνω e-mail.

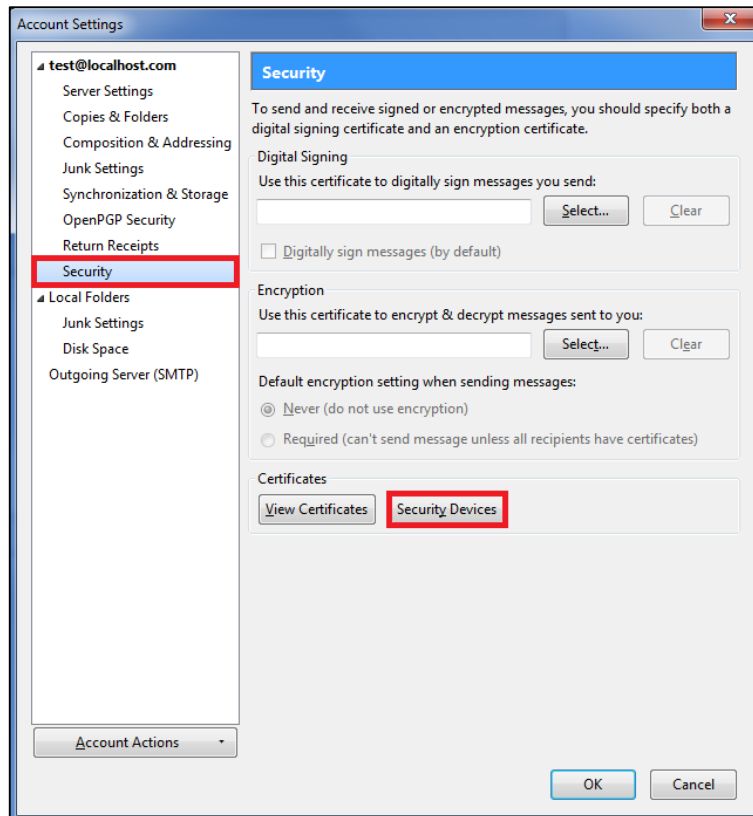
### 6.1. Φόρτωση Συσκευής Ασφαλείας

Για να φορτώσετε τον αναγνώστη της κάρτας ως συσκευή ασφαλείας στον Mozilla Thunderbird θα πρέπει να ακολουθήσετε τα παρακάτω βήματα:

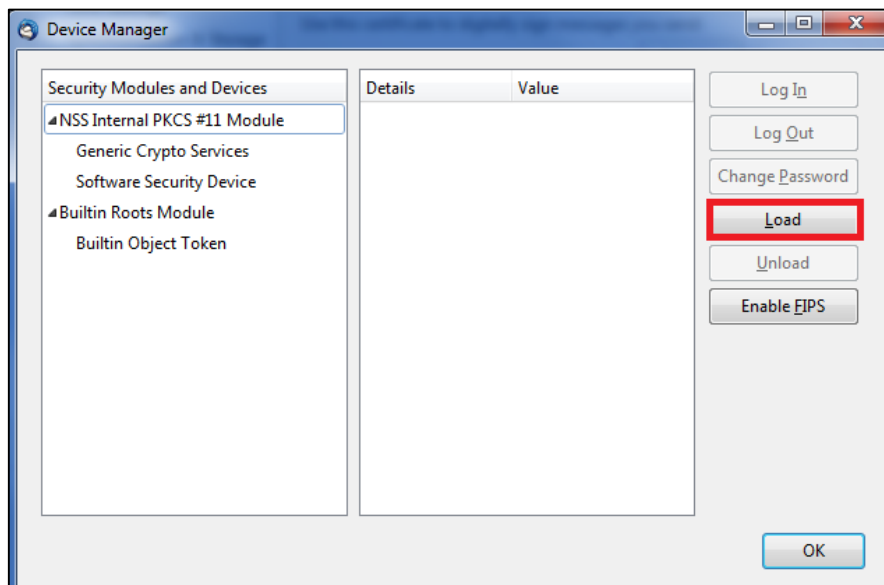
1. Επιβεβαιώστε ότι δεν έχετε συνδεδεμένη την κάρτα σας στη συσκευή ανάγνωσης.
2. Εκκινήστε το πρόγραμμα Mozilla Thunderbird.
3. Επιλέξτε «View settings for this account».



4. Στο παράθυρο που θα ανοίξει, επιλέξτε "Security" και στη συνέχεια πατήστε πάνω στο κουμπί «Security Devices».

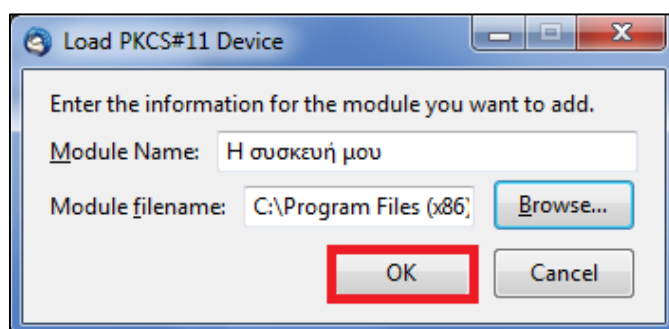


5. Στο νέο παράθυρο που θα ανοίξει, θα πρέπει να πατήσετε στο κουμπί “Load” προκειμένου να φορτώσετε τη συσκευή ανάγνωσης που έχετε στην κατοχή σας.

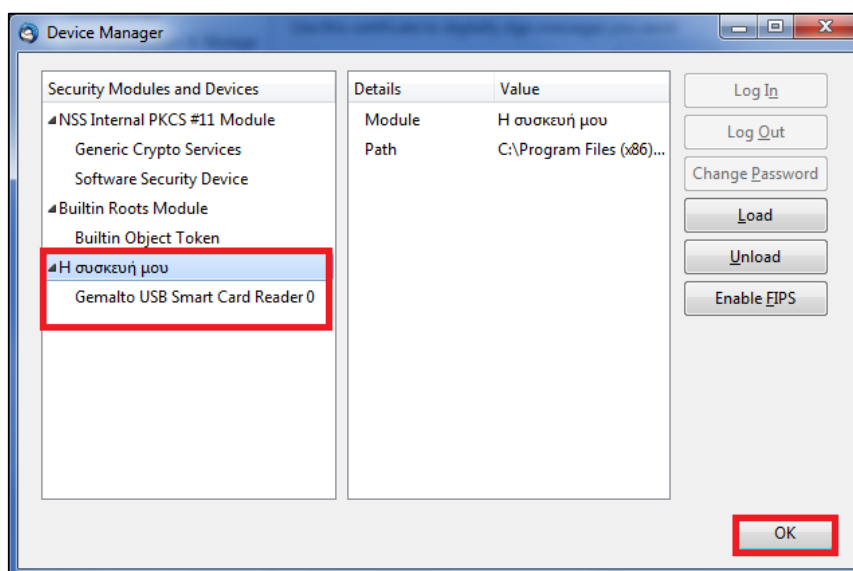


6. Στη συνέχεια καλείστε αρχικά να συμπληρώσετε ένα αναγνωριστικό όνομα για τη συσκευή και στη συνέχεια να επιλέξετε το αρχείο “gclib.dll” από τον φάκελο εγκατάστασης του Classic Client. Το αρχείο αυτό βρίσκεται στο μονοπάτι “\install dir\BIN”. Εάν χρησιμοποιείτε 32-bit έκδοση των Windows, τότε ο προεπιλεγμένος φάκελος εγκατάστασης του αρχείου αυτού είναι ο “C:\Program Files\Gemalto\Classic Client\”.

Διαφορετικά, εάν η έκδοση των Windows είναι 64 bit, ο φάκελος εγκατάστασης είναι ο “ C:\Program Files (x86)\Gemalto\Classic Client\BIN ”. Αφού συμπληρώσετε τα παραπάνω πεδία πατήστε “OK” για να προχωρήσετε.



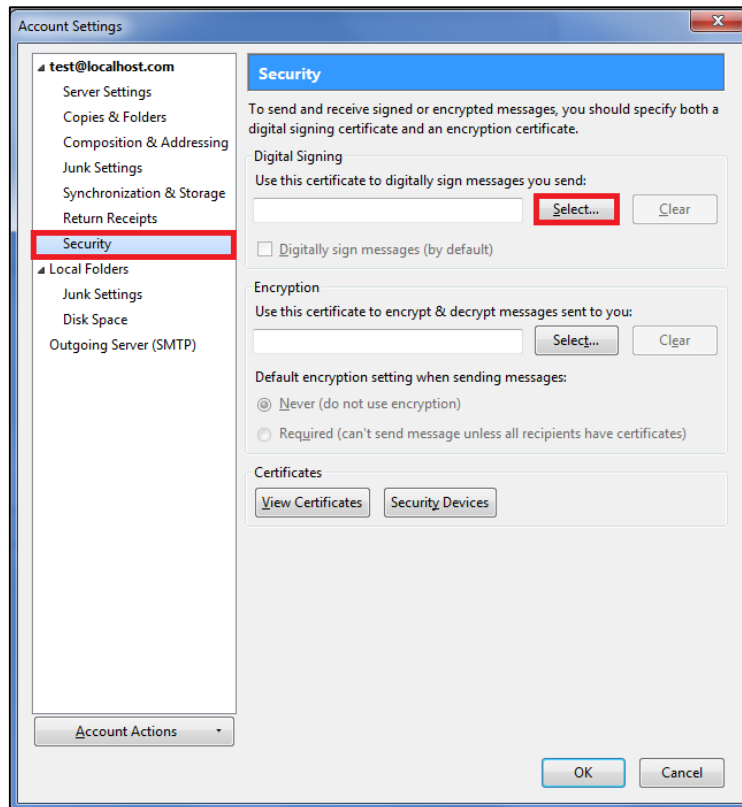
Εφόσον η ενέργεια έχει πραγματοποιηθεί επιτυχώς, θα πρέπει να βλέπετε τη συσκευή που προσθέσατε στα αριστερά της λίστας με τις συσκευές ασφαλείας. Στο παράθυρο αυτό πατήστε ξανά “OK” για να το κλείσετε.



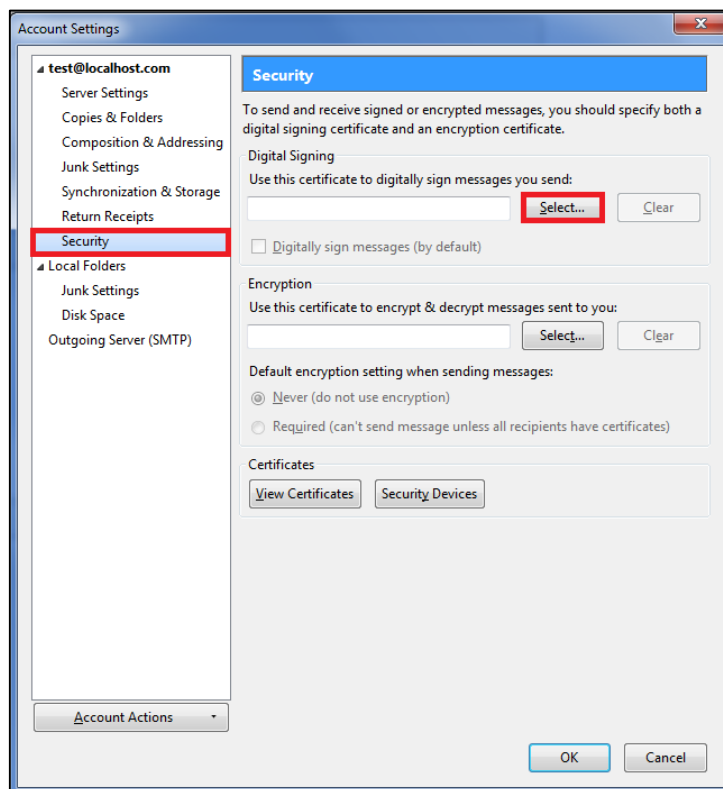
## 6.2. Ψηφιακή Υπογραφή E-mail

Εφόσον ακολουθήσετε τις παραπάνω οδηγίες και έχετε πλέον προσθέσει τον αναγνώστη ως συσκευή ασφαλείας στο Mozilla Thunderbird, τώρα έχετε τη δυνατότητα να στείλετε e-mail ενσωματώνοντας σε αυτό την ψηφιακή σας υπογραφή. Για να το πετύχετε αυτό θα πρέπει αρχικά να κάνετε τις ακόλουθες ρυθμίσεις:

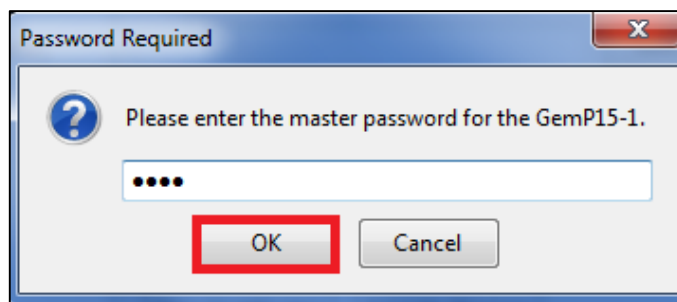
1. Συνδέστε την κάρτα στη συσκευή ανάγνωσης.
2. Εκκινήστε το πρόγραμμα Mozilla Thunderbird.
3. Ανοίξτε τις ρυθμίσεις του λογαριασμού σας όπως κάνατε και παραπάνω επιλέγοντας “Security”.



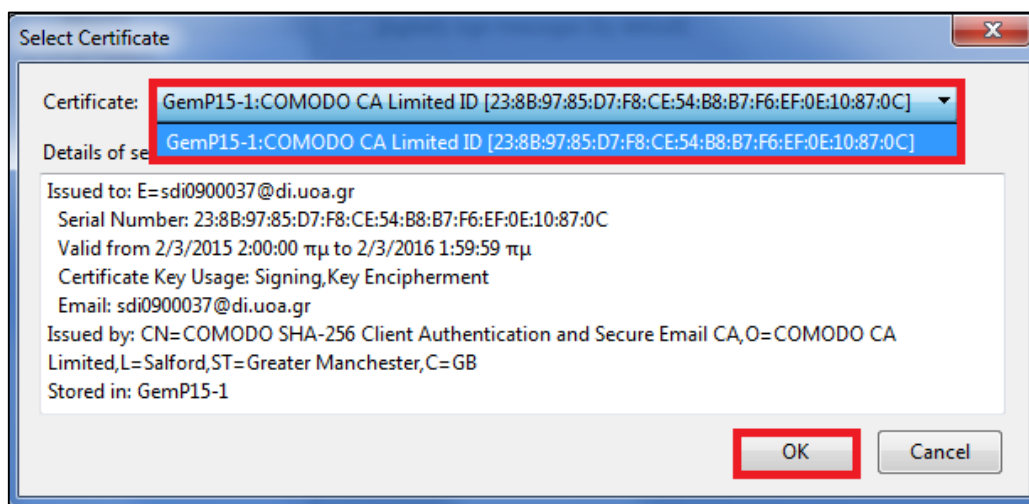
4. Στη συνέχεια θα πρέπει να επιλέξετε με ποιο πιστοποιητικό από την κάρτα σας επιθυμείτε να ενσωματώσετε την ψηφιακή υπογραφή σας στα e-mail. Επομένως θα πρέπει να πατήσετε στο κουμπί “Select” στο πλαίσιο “Digital Signing”.



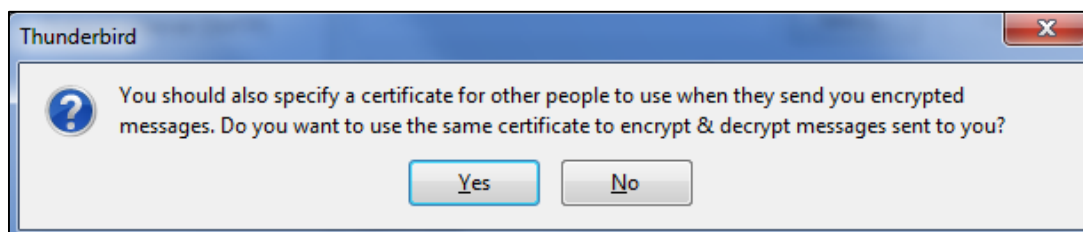
5. Προκειμένου να συνεχίσετε θα πρέπει να συμπληρώσετε το PIN της κάρτας σας στο πλαίσιο διαλόγου που εμφανίζεται και να πατήσετε “OK”.



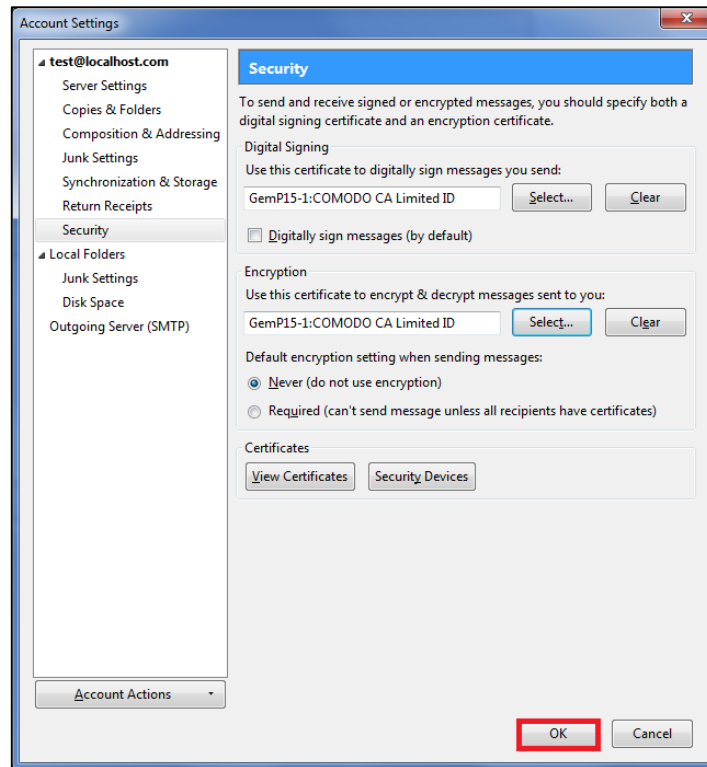
6. Στο επόμενο παράθυρο καλείστε να επιλέξετε ποιο πιστοποιητικό από την κάρτα σας επιθυμείτε να χρησιμοποιηθεί για την δημιουργία της ψηφιακής σας υπογραφής. Αφού το επιλέξετε από τη λίστα που εμφανίζεται, πατήστε “OK” για να συνεχίσετε.



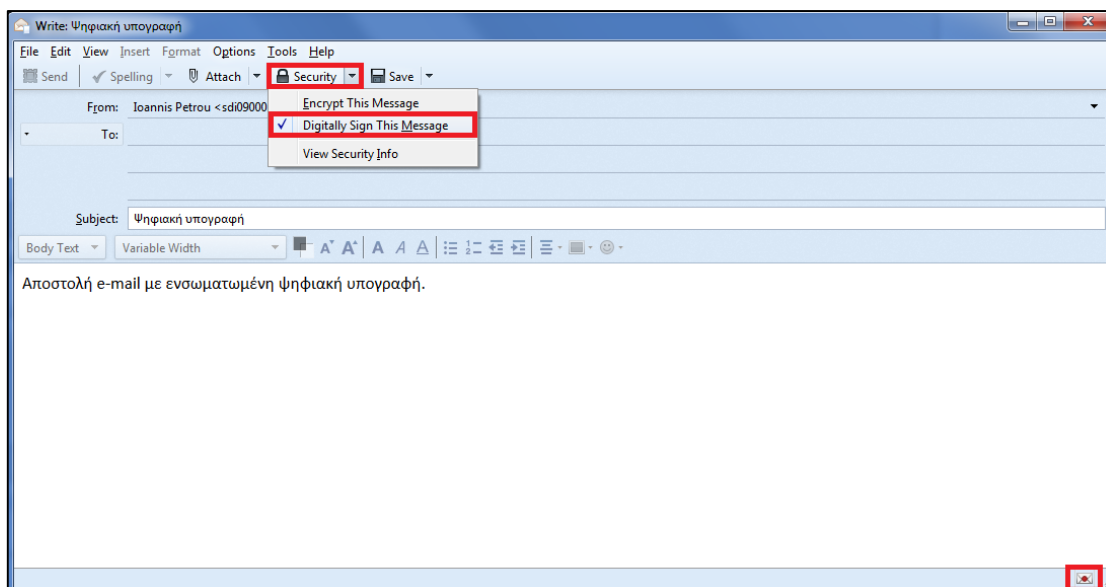
7. Για να προχωρήσετε θα πρέπει να επιλέξετε εάν επιθυμείτε να χρησιμοποιηθεί το ίδιο πιστοποιητικό και για την κρυπτογράφηση/αποκρυπτογράφηση των e-mail. Σε κάθε περίπτωση το συγκεκριμένο πεδίο μπορεί να συμπληρωθεί και αργότερα με παρόμοια διαδικασία με αυτή που περιγράφηκε παραπάνω. Επισημαίνεται όμως ότι για να αποκρυπτογραφήσετε ένα e-mail το οποίο έχει κρυπτογραφηθεί με το δικό σας δημόσιο κλειδί μέσω της ψηφιακής σας υπογραφής, θα πρέπει να έχετε συμπληρώσει αυτό το πεδίο.



8. Για να ολοκληρώσετε την προσθήκη του πιστοποιητικού, πατήστε “OK” στο αρχικό παράθυρο για να κλείσει και να συνεχίσετε με την σύνταξη ενός νέου e-mail.



9. Για να ενσωματώσετε την ψηφιακή υπογραφή σας στα e-mail σας, στο παράθυρο σύνταξης ενός νέου e-mail, θα πρέπει από την καρτέλα “Security” να επιλέξετε “Digitally Sign This Message”. Μπορείτε να επιβεβαιώσετε ότι η υπογραφή έχει ενσωματωθεί και από το σχετικό εικονίδιο που προστίθεται στην κάτω δεξιά περιοχή του παραθύρου.



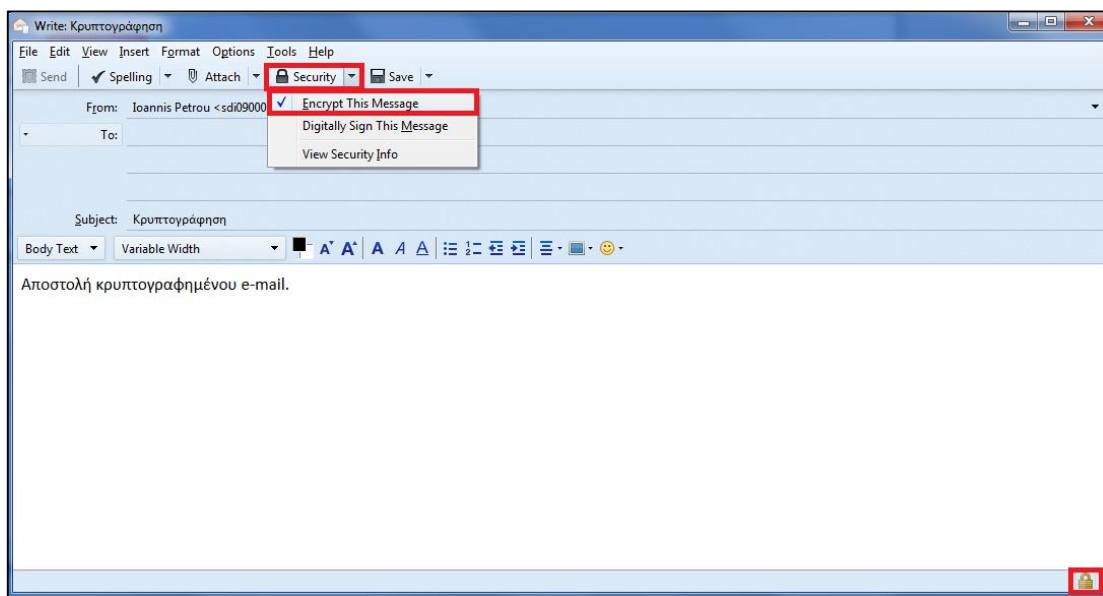


### 6.3. Κρυπτογράφηση / Αποκρυπτογράφηση E-mail

Για να κρυπτογραφήσετε ένα e-mail θα πρέπει να το κάνετε χρησιμοποιώντας το πιστοποιητικό του χρήστη που σας έστειλε ένα e-mail δηλαδή τον παραλήπτη του e-mail το οποίο θέλετε να κρυπτογραφήσετε. Επομένως θα πρέπει ο χρήστης που σας έστειλε το mail αυτό να το έχει υπογράψει ψηφιακά με το δικό του πιστοποιητικό.

Τα βήματα που πρέπει να ακολουθήσετε για την κρυπτογράφηση είναι τα εξής:

1. Ανοίξετε το e-mail που λάβατε, το οποίο ενσωματώνει την ψηφιακή υπογραφή του αποστολέα.
2. Εάν δεν το έχετε κάνει ήδη, προσθέστε τον αποστολέα στις επαφές σας προκειμένου να αποθηκευτεί το πιστοποιητικό του σύμφωνα με το οποίο θα κρυπτογραφήσετε το νέο e-mail που θα στείλετε στον ίδιο.
3. Στην σύνταξη του e-mail επιλέξτε την καρτέλα "Security" και στη συνέχεια "Encrypt This Message" προκειμένου να κρυπτογραφήσετε το e-mail με βάση το πιστοποιητικό του παραλήπτη. Το εικονίδιο που εμφανίζεται στο κάτω δεξιά μέρος της οθόνης σας μπορεί να σας επιβεβαιώσει ότι η κρυπτογράφηση έχει πραγματοποιηθεί.



Για την αποκρυπτογράφηση ενός e-mail θα πρέπει να πραγματοποιηθεί η αντίστροφη διαδικασία. Εφόσον έχετε στείλει σε κάποιο άτομο ένα e-mail με την ψηφιακή σας υπογραφή, το άτομο αυτό έχει τη δυνατότητα να κρυπτογραφήσει την απάντηση που θα σας στείλει με το δικό σας πιστοποιητικό. Επομένως όταν λάβετε το e-mail που θα σας στείλει και εφόσον έχετε πραγματοποιήσει τις παραπάνω ρυθμίσεις στον Mozilla Thunderbird θα έχετε τη δυνατότητα ανάγνωσης του αποκρυπτογραφημένου μηνύματος. Σε διαφορετική περίπτωση, αν για παράδειγμα δοκιμάσετε να ανοίξετε το e-mail που λάβατε από το Web Interface του λογαριασμού σας, το μήνυμα αυτό θα είναι κενό λόγω του ότι θα είναι κρυπτογραφημένο.

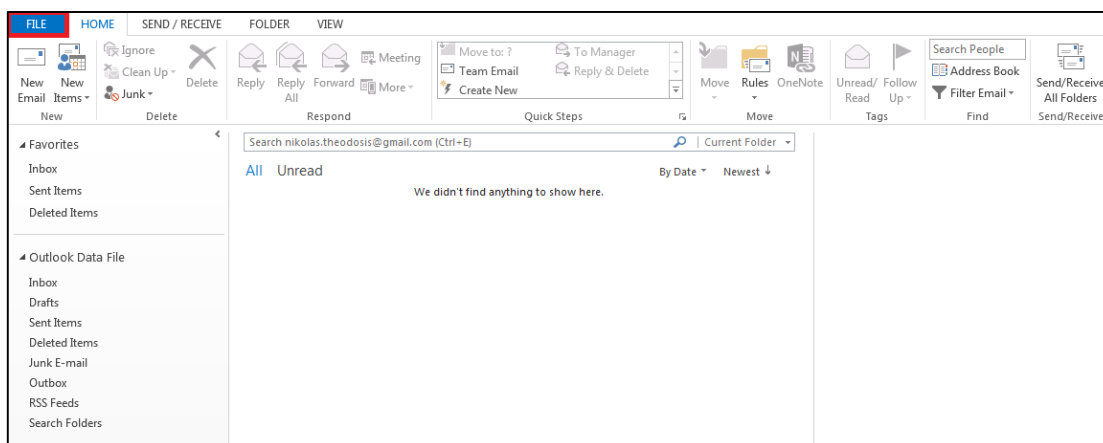
## 7. Χρήση Ψηφιακών Πιστοποιητικών σε Microsoft Outlook 2013

Η διαδικασία που πρέπει να ακολουθήσετε για να ενσωματώσετε ψηφιακές υπογραφές ή/και για να κρυπτογραφήσετε/αποκρυπτογραφήσετε e-mail είναι παρόμοια με αυτή που περιγράφηκε παραπάνω.

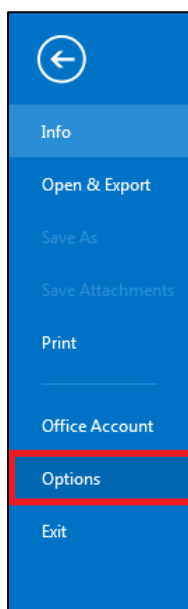
### 7.1. Ψηφιακή Υπογραφή E-mail

Για να ενσωματώσετε την ψηφιακή σας υπογραφή σε ένα e-mail θα πρέπει να ακολουθήσετε τα παρακάτω βήματα:

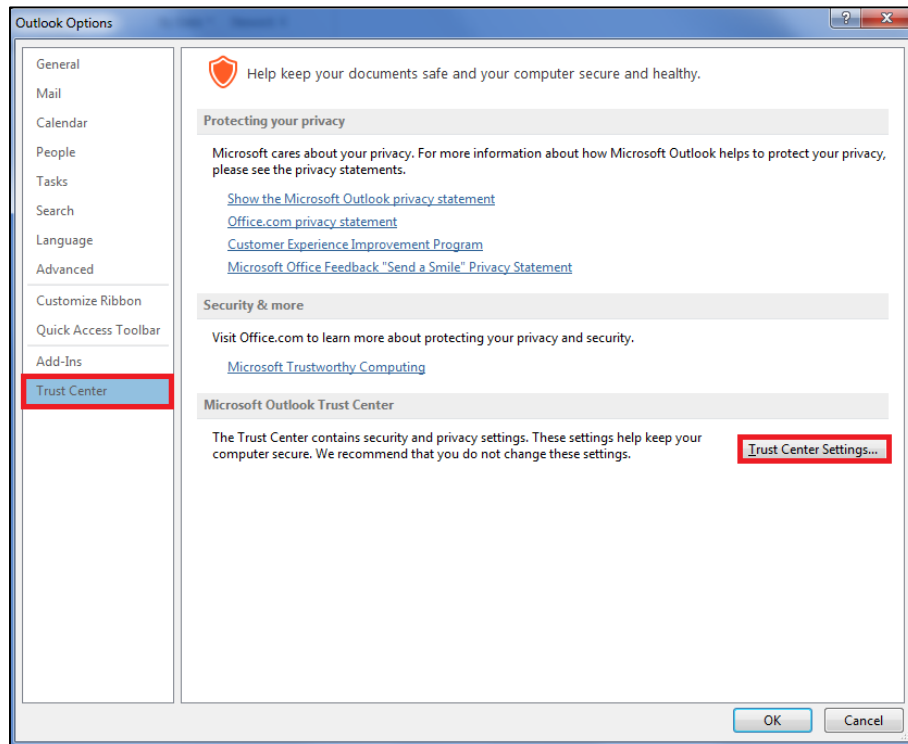
1. Πατήστε “FILE” από τις καρτέλες στο πάνω αριστερά μέρος της οθόνης σας.



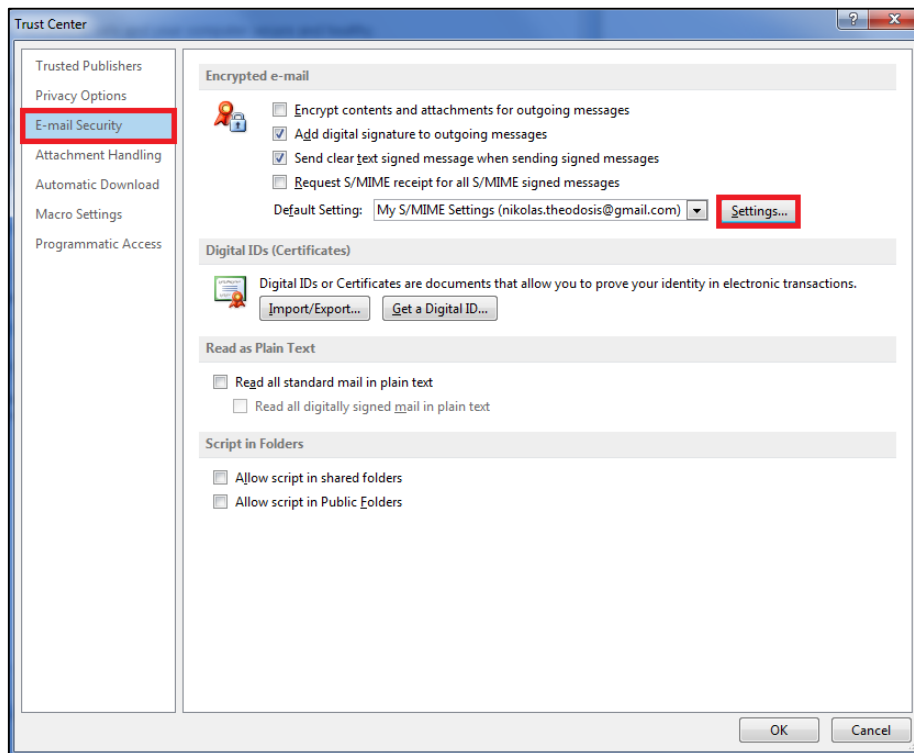
2. Από τις επιλογές που εμφανίζονται στα αριστερά της οθόνης σας επιλέξτε την επιλογή “Options”.



3. Στη συνέχεια και στο νέο παράθυρο που εμφανίζεται, επιλέξτε από την λίστα που βρίσκεται στα αριστερά την επιλογή “Trust Center” και στη συνέχεια από το πεδίο “Microsoft Outlook Trust Center” πατήστε πάνω στο κουμπί “Trust Center Settings”.



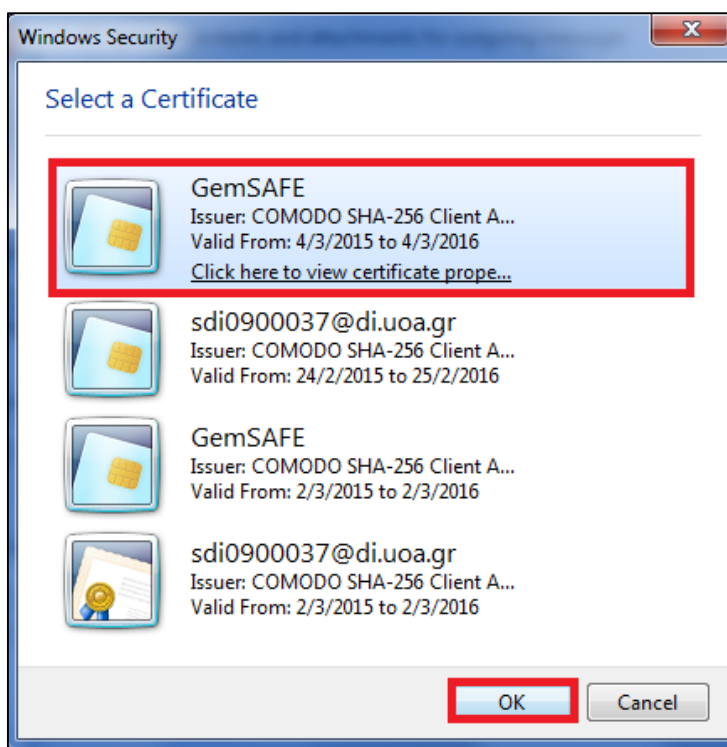
4. Στην επόμενη οθόνη που θα συναντήσετε θα πρέπει να επιλέξετε από τα αριστερά “E-mail Security” και στη συνέχεια στο πεδίο “Default Settings” θα πρέπει να πατήσετε στο κουμπί “Settings”.



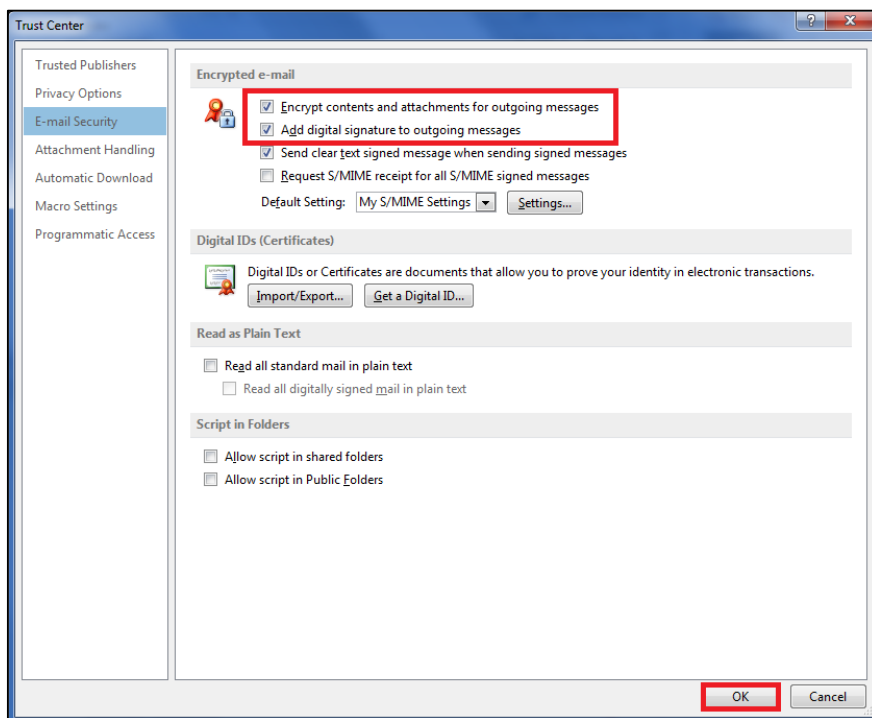
5. Έπειτα θα πρέπει να κάνετε εισαγωγή του πιστοποιητικού σύμφωνα με το οποίο επιθυμείτε να ενσωματώνετε ψηφιακές υπογραφές ή/και να κρυπτογραφείτε τα e-mail. Στο παράθυρο που εμφανίζεται πατήστε στο κουμπί "Choose" που αντιστοιχεί στο πεδίο "Signing Certificate" αν θέλετε να ορίσετε το πιστοποιητικό για ψηφιακή υπογραφή ή το αντίστοιχο κουμπί για το πεδίο "Encryption Certificate" εάν θέλετε να ορίσετε το πιστοποιητικό για κρυπτογράφηση.



6. Για να συνεχίσετε θα πρέπει να επιλέξετε το πιστοποιητικό που επιθυμείτε από τη λίστα με τα διαθέσιμα πιστοποιητικά που θα εμφανιστεί. Αφού το επιλέξετε πατήστε "OK" για να συνεχίσετε.



Αφού κλείσετε και το επόμενο παράθυρο, θα πρέπει να επιλέξετε ότι επιθυμείτε να προσθέσετε την ψηφιακή σας υπογραφή σε όλα τα εξερχόμενα μηνύματα που στέλνετε καθώς επίσης και ότι θέλετε να κρυπτογραφείτε τα εξερχόμενα μηνύματα εφόσον βέβαια έχετε λάβει την ψηφιακή υπογραφή του παραλήπτη όπως αναλύεται παρακάτω. Αφού επιλέξετε λοιπόν και το αντίστοιχο πλαίσιο, πατήστε “OK” για να αποθηκευτούν όλες οι αλλαγές.



7. Αφού κλείσετε όλα τα παράθυρα ρυθμίσεων που είχατε ανοίξει, οποιοδήποτε e-mail στέλνετε, πλέον θα ενσωματώνει αυτόματα και την ψηφιακή σας υπογραφή.

## 7.2. Κρυπτογράφηση / Αποκρυπτογράφηση E-mail

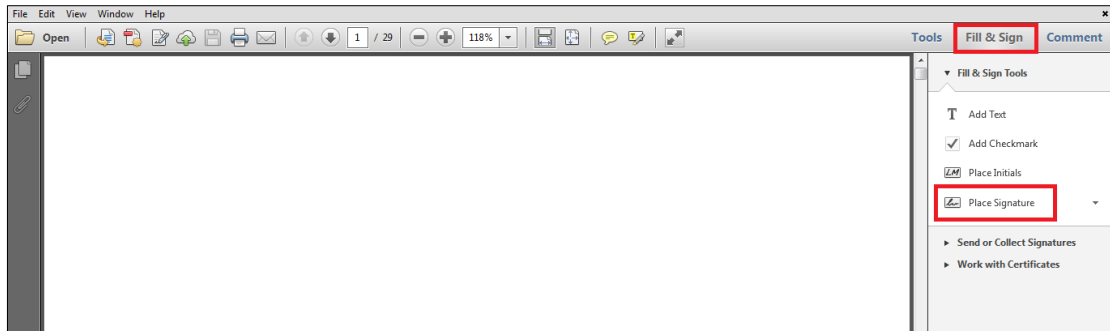
Για την κρυπτογράφηση και αποκρυπτογράφηση η διαδικασία που πρέπει να ακολουθήσετε είναι η ίδια με αυτή που έχει περιγραφεί για το Mozilla Thunderbird. Αρχικά για να κρυπτογραφήσετε ένα e-mail, θα πρέπει ο μελλοντικός παραλήπτης του κρυπτογραφημένου e-mail να σας έχει στείλει ένα e-mail στο οποίο θα έχει ενσωματώσει την ψηφιακή του υπογραφή. Στη συνέχεια μπορείτε να κρυπτογραφήσετε το e-mail που θέλετε να στείλετε στον παραλήπτη αυτόν απλά προσθέτοντας τον στις επαφές σας. Προφανώς αν λάβετε ένα e-mail το οποίο είναι κρυπτογραφημένο με βάση το δικό σας πιστοποιητικό, τότε εφόσον έχετε την κάρτα συνδεδεμένη στον αναγνώστη, θα έχετε και τη δυνατότητα ανάγνωσης του e-mail καθώς η αποκρυπτογράφηση γίνεται αυτόματα.

## 8. Υπογραφή PDF

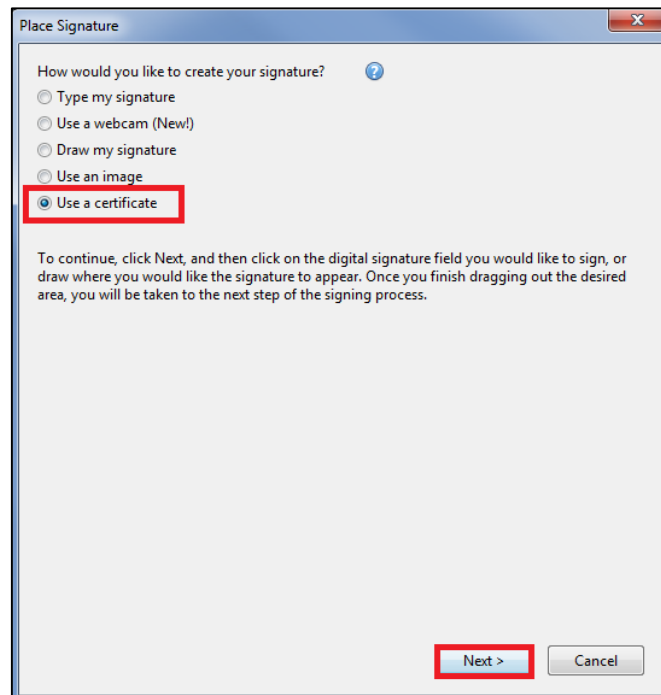
Η υπογραφή σε έγγραφα PDF μπορεί να πραγματοποιηθεί μέσω του αντίστοιχου προγράμματος ανάγνωσης της Adobe που χρησιμοποιείτε. **Οι οδηγίες που ακολουθούν αναφέρονται στην έκδοση “Adobe Reader XI”.**

Για να υπογράψετε ψηφιακά ένα PDF λοιπόν, θα πρέπει να ακολουθήσετε τα παρακάτω βήματα:

1. Ανοίξτε το PDF που επιθυμείτε να υπογράψετε.
2. Στο πάνω δεξιά μέρος της οθόνης πατήστε το κουμπί “Fill & Sign” και στη συνέχεια “Place Signature”.



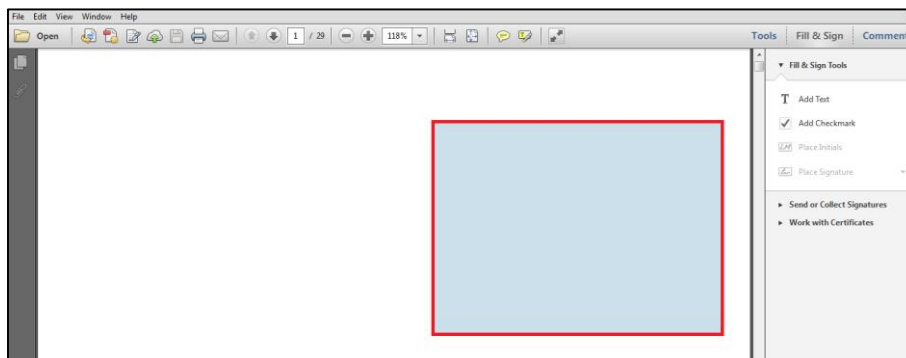
3. Στο νέο παράθυρο που εμφανίζεται, θα πρέπει να επιλέξετε να υπογράψετε με τη χρήση πιστοποιητικού. Επομένως επιλέξτε την επιλογή “Use a certificate” και πατήστε “Next”.



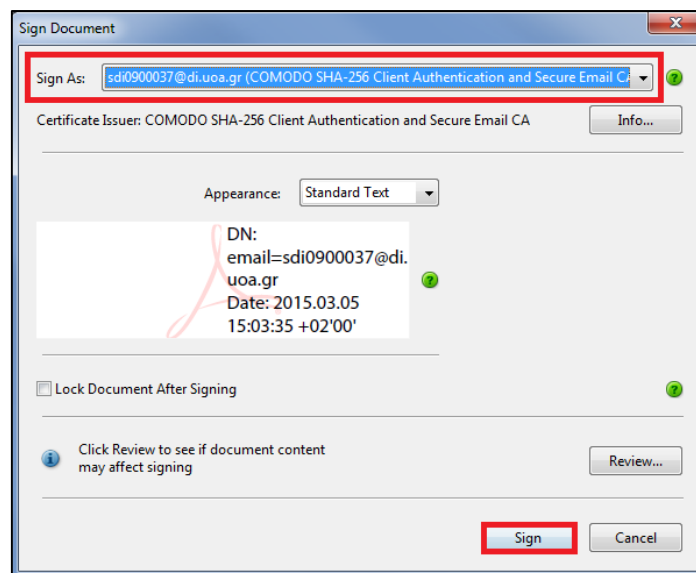
4. Το πλαίσιο διαλόγου που εμφανίζεται σας ενημερώνει ότι θα πρέπει να σχεδιάσετε στο PDF σε ποιο σημείο επιθυμείτε να φαίνεται η υπογραφή σας. Για να προχωρήσετε επιλέξτε την επιλογή “Drag New Signature Rectangle ...”.



5. Για να σχεδιάσετε λοιπόν το σημείο αυτό, κάντε κλικ και τραβήξτε το ποντίκι ώστε να επιλέξετε την περιοχή αυτή.



6. Μόλις αφήσετε τον δείκτη του ποντικιού, στο νέο παράθυρο καλείστε να επιλέξετε με ποιο πιστοποιητικό θέλετε να υπογράψετε το PDF καθώς επίσης και πως θα εμφανίζεται η υπογραφή σας σε αυτό. Αφού επιλέξετε το πιστοποιητικό αυτό από την επιλογή "Sign As" στη συνέχεια πατήστε στο κουμπί "Sign".



7. Τότε θα σας ζητηθεί να αποθηκεύσετε το νέο αυτό PDF το οποίο ενσωματώνει την ψηφιακή σας υπογραφή. Μετά την αποθήκευση, για επιβεβαίωση θα σας ζητηθεί το PIN της κάρτας σας. Στη συνέχεια θα μπορείτε να δείτε την υπογραφή στο σημείο που είχατε επιλέξει στο βήμα 5.