ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΗΡΕΣΙΑ ΑΠΟΚΤΗΣΗΣ ΑΚΑΔΗΜΑΪΚΗΣ ΤΑΥΤΟΤΗΤΑΣ

Οδηγός Διαχείρισης Ακαδημαϊκής Ταυτότητας

Λειτουργικό Σύστημα: Windows



ΠΕΡΙΕΧΟΜΕΝΑ

1.	Еүк	ατάσταση Λογισμικού (Classic Client)	4
2.	Driv	vers Αναγνώστη/Εγγραφέα	6
3.	Δια	αχείριση PIN	7
3	.1.	Αλλαγή ΡυΚ	8
3	.2.	Αλλαγή ΡΙΝ	10
3	.3.	Αποδἑσμευση ΡΙΝ	12
4.	Πρ	οαπαιτούμενες Ενέργειες	14
5.	Έκδ	δοση Ψηφιακών Πιστοποιητικών	18
6.	Xpr	ήση 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.	Xpr	ήση Ψηφιακών Πιστοποιητικών σε Microsoft Outlook 2013	31
7	.1.	Ψηφιακή Υπογραφή E-mail	31
7	.2.	Κρυπτογράφηση / Αποκρυπτογράφηση E-mail	34
8.	Υπα	ογραφή PDF	35



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

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.

Άδεια χρήσης Διαβάστε προσεκτικά την ακόλουθη	άδεια χρήσης.	gema
END USER I	LICENSE AGREEME	NT
IMPORTANT-READ CAREFULLM Gemalto software ("EULA") is a leg the subsidiary or affiliate of Gemalt version of the Software (as defined "You" are a person or legal entity w governs your use of all of the Softw "Software" means all computer soft materials and any accompanying "or to you hereunder. By downloading	V: This End-User License A gal and binding agreement b o NV. ("Gemalto") that distr below) under this EULA (" vishing to use the Software. vare distributed or delivered tware, associated media, any online" or electronic informa g, installing, copying, breaki	greement for etween you and ibuted this Gemalto"). This EULA I hereunder. y printed ation provided ing any seal on,
 Αποδέχομαι τους όρους της άδειας χ 	ρήσης	Εκτύπωση
🔘 Δεν αποδέχομαι τους όρους της άδει	ας χρήσης	
nstallShield		
	< Πίσω Επόμ	ιενο > Ακύρωση

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».

🛃 Classic Cli	ient 7.0 for 64 bits - InstallShield Wizard	×
Φάκελος ι Κάντε κλι Αλλαγή γ	προορισμού ικ στο Επόμενο για εγκατάσταση σε αυτό το φάκελο ή κάντε κλικ στην για εγκατάσταση σε άλλο φάκελο.	gemalto
	Eγκατάσταση Classic Client 7.0 for 64 bits στο: C:\Program Files (x86)\Gemalto\Classic Client\	Αλλαγή
InstallShield —	< Πίσω Επόμενο >	Ακύρωση

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.

🛃 Classic Client 7.0 for 64 bits - InstallShield Wizard	×
Έτοιμο για εγκατάσταση του προγράμματος Ο οδηγός είναι έτοιμος για έναρξη της εγκατάστασης.	jemalto*
Κάντε κλικ στην Εγκατάσταση για να ξεκινήσει η εγκατάσταση. Εάν θέλετε να ελέγξετε ή να αλλάξετε κάποιες ρυθμίσεις εγκατάστασης, κάντε κλικ Προηγούμενο.	: ото
InstallShield < Πίσω 😤 Εγκατάσταση 🗾	Ακύρωση

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



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

🛃 Classic Client 7.0 for 64 bit	s - InstallShield Wizard
gemalto	Ο InstallShield Wizard ολοκληρώθηκε
	Ο InstallShield Wizard εγκατέστησε επιτυχώς το Classic Client 7.0 for 64 bits. Κάντε κλικ στο Τέλος για να κλείσετε τον οδηγό.
	< Πίσω Τέλος Ακύρωση

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



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

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 ΡΙΝ της κάρτας.

Αλλαγή Ρ	IN Χρήστη - GemP15-1	×
Οθόνη ΡΙΝ Χρήστη Τρέχοντες αριθμοί Νέο ΡΙΝ: Επιβεβαίωση νέου	Πρέπει να έχει τουλάχιστον 4 χαρακτήρες Πρέπει να είναι λιγότερο ή ίσο με 8 χαρακτήρες Πρέπει να περιέχει μόνο αριθμητικούς χαρακτήρες	× × ×
Αλλαγή ΡΙΝ Χρήστη Ακαφο Classic Client - Μήνυμα Το ΡΙΝ σας δεν έχει προετοιμαστεί. Πρέπει να αλλα	άξετε το ΡΙΝ του χρήστη για να χρησιμοποιήσετε την κάρτα.	

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 ΡΙΝ 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 ΡΙΝ 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».



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



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».

assic Client		gemalto
Toolbox	Διαχείριση PIN	<u>_</u>
Περιεχόμενα κάρτας		
Διαχείριση κάρτας		Επιλέξτε συσκ. ανάγν. έξυπνων καρτών
.0		Gemalto USB Smart Card Reader 0
Διαχείριση PIN		
		Επιλέξτε μία εργασία που θέλετε να εκτελέσετε
		GemP15-1
		Αλλαγή ΡΙΝ Αλλημομομομομομομομομομομομομομομομομομομ
		C Αποδέσμευση ΡΙΝ
μαγνωστικο/Βοηθεία		Επόμενο >>
αχείριση Περιεχομένου		

3.1. Αλλαγή ΡUΚ

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



	Διαχείριση PIN	
Τεριεχόμενα κάρτας Διαχείριση κάρτας	Gemalto USB Smart Card Reader 0	
Διαχείριση PIN	PIN Admin User Admin Τρέχοντες αρθμοί PIN: Νέο PIN: Επβεβοίωση νέου PIN: Επβεβοίωση νέου PIN: Αλλαγή PIN από χρήστη Αλλαγή PIN	Πολιτική ΡΙΝ Πρέπει να έχει τουλάχιστον 8 χαρακτήρες Χ Πρέπει να είναι λιγότερο ή ίσο με 8 χαρακτήρες Χ Πρέπει να περιέχει αλφαβητικούς και Χ Πρέπει να περιέχει κεφαλαίους και μικρούς Χ
ιαγνωστικό/Βοήθεια		

Στη συνέχεια θα πρέπει να συμπληρώσετε το τρέχον PUK σας στο πεδίο «Τρέχοντες αριθμοί PIN», το νέο PUK που επιθυμείτε στο πεδίο «Νέο PIN» καθώς και μια επιβεβαίωση του νέου PUK, στο πεδίο «Επιβεβαίωση νέου PIN», για λόγους ασφαλείας. Επισημαίνεται ότι η πολιτική για τον κωδικό PUK 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.



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

3.2. Αλλαγή ΡΙΝ

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".

1001002		
	Διαχειριση ΡΙΝ	
ριεχόμενα κάρτας ιαχείριση κάρτας	Gemalto USB Smart Card Reader 0	
Διαχείριση PIN	PIN	Πολιτική ΡΙΝ Πρέπει να έχει τουλάχιστον 4 χαρακτήρες Χ Πρέπει να είναι λιγότερο ή ίσο με 8 χαρακτήρες Χ Πρέπει να περιέχει μόνο αριθμητικούς Χ
γνωστικό/Βοήθεια		

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.

	Διαχείριση PIN	
Τεριεχόμενα κάρτας Διαχείριση κάρτας	Gemalto USB Smart Card Reader 0	
Διαχείριση PIN	PIN User Τρέχοντες αριθμοί PIN: στικα Νέο PIN: στικα Επιβεβαίωση νέου PIN: κοικα	Πολτική ΡΙΝ Πρέπει να έχει τουλάχιστον 4 χαρακτήρες Πρέπει να είναι λιγότερο ή ίσο με 8 χαρακτήρες Πρέπει να περιέχει μόνο αριθμητικούς
	Αλλαγή ΡΙΝ από χρήστη Αλλαγή ΡΙΝ	
ιγνωστικο/Βοηθεια		<< Προηγούμενο
κείριση Περιεχομένου		

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Περιφερειακής

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 ΡΙΝ καθώς επίσης και για τις υπολειπόμενες προσπάθειες που έχουν απομείνει. Σημειώνεται ότι εάν συμπληρώσετε λανθασμένα το PIN σας 3 διαδοχικές φορές, το ΡΙΝ 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.





Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ερευνας και Θρησκευμάτω

3.3. Αποδέσμευση ΡΙΝ

Ως διαχειριστής μπορείτε να χρησιμοποιήσετε την εφαρμογή αυτή για να αποδεσμεύσετε το PIN σας μέσω του PUK, 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.



Toolbox	gernauu
Διαχείριση ΡΙΝ	1
εριεχόμενα κάρτας	
Διαχείριση κάρτας	Επιλέξτε συσκ. ανάγν. έξυπνων καρτών
	Gemalto USB Smart Card Reader 0
	Επιλέξτε μία εργασία που θέλετε να εκτελέσετε -
	6E3 GemP15-1
	C Αλλανή ΡΙΝ
	Αποδέσμευση ΡΙΝ
αννωστικό/Βοήθεια	
nío m Bronno á ma	Επόμενο >>

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».

	v
Διαχείριση ΡΙΝ	
οιεχόμενα κάρτας	
αχείριση κάρτας Gemalto USB Smart Card Reader 0	
PIN User	Πολιτική ΡΙΝ
ΡΙΝ διαχειριστή:	Πρέπει να έχει τουλάχιστον 4 χαρακτήρες 🗸 Πρέπει να είναι λιγότερο ή ίσο με 8 χαρακτήρες 🗸
Néo PIN:	Πρέπει να περιέχει μόνο αριθμητικούς 🗸 🗸
Αλλαγή ΡΙΝ από χρήστη Αποδέσμευση ΡΙΝ	

Εφόσον ολοκληρώσετε επιτυχώς την αποδέσμευση του ΡΙΝ 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.

Hitertpovený Ytanpeolo An X +			8	- 0 ×
A https://submit-academicid minedu.gov.gr	V C Q Search	☆自	+ +	* - =
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ	Ηλεκτρονική Υπηρεσία Απόκτησης	X Cut 1	Copy 1	Paste +
Υπουργείο Παιδείας, Ερευνας και Θρησκευμάτων	Ακαδημαϊκής Ταυτότητας	Νέο Ν παράθυρο	CC lew Private Window	Save Page
	<u> Δ+</u> <u>Δ</u> Φ Δ		0	↓ ⊕
🤧 Αρχική Σελίδα 🛛 👩 Συχνές Ερωτήσεις	🖀 Επικοινωνία	Εκτύπωση	History	Πλήρης οθόνη
Καλώς ἠλθατε		р Find	Ö Options	Add-ons
Εγγραφή	Είσοδος	Developer Te	æ ext Encoding	
	Q	 G) Sign in to Sync Προσαρμογή 		0 U

[<mark>0]</mark> Γενικά	Για προχωρημένους						
Q Search	Γενικά Επιλογές δεδομένων Δίκτυο Ενημέρωση Πιστοποιητικά						
Περιεχόμενο							
Εφαρμογές	Requests Όταν ένας εξυπηρετητής απαιτεί ένα πιστοποιητικό:						
	Ο Αυ <u>τ</u> όματη επιλογής ενός						
Svnc	Ε <u>ρ</u> ώτηση κάθε φορά						
 Για προχωρημένους 	\checkmark Query OCSP responder servers to confirm the current validity of certificates						
	Πρ <u>ο</u> βολή πιστοποιητικών Συ <u>σ</u> κευές ασφαλείας						
 Απόρρητο Ασφάλεια Sync Για προχωρημένους 	Όταν ένας εξυπηρετητής απαιτεί ένα πιστοποιητικό: Αυ <u>τ</u> όματη επιλογής ενός Ε <u>ρ</u> ώτηση κάθε φορά Query OCSP responder servers to confirm the current validity of certificates Πρ <u>ο</u> βολή πιστοποιητικών Συ <u>σ</u> κευές ασφαλείας						

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



Διαχείριση συσκευών			×
Mονάδες ασφάλειας και συσκευές ■NSS Internal PKCS #11 Module Generic Crypto Services Software Security Device ■Builtin Roots Module Builtin Object Token	Λεπτομέρειες	Τμή	Σύνδεση Α <u>π</u> οσύνδεση Δλλαγή κωδικού <u>Φόρτωση</u> Ε <u>κ</u> φόρτωση Ενεργοποίηση <u>F</u> IPS
			ОК

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.

🥑 Φόρτωση μονάδος PKCS#11					
Εισάγετε τις πληροφορίες για τη μονάδα που θέλετε να προσθέσετε.					
Όνομα μονάδος:	Όνομα μονάδος: Η συσκευή μου				
Όνομα αρχείου μο	νάδας:	C:\Program Files (x86)'	Ανα <u>ζ</u> ήτηση		
		ОК	Ακύρωση		



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 "ΟΚ" για να το κλείσετε.

Διαχείριση συσκευών			X
Mονάδες ασφάλειας και συσκευές ANSS Internal PKCS #11 Module Generic Crypto Services Software Security Device ABuiltin Roots Module Builtin Object Token AH συσκευή μου GemP15-1	Λεπτομέρειες Λειτουργική μονάδα Διαδρομή	Τιμή Η συσκευή μου C:\Program Files (x	Σύνδεση Α <u>π</u> οσύνδεση <u>Α</u> λλαγή κωδικού <u>Φ</u> όρτωση Ε <u>κ</u> φόρτωση Ενεργοποίηση <u>F</u> IPS
			ОК

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

η Γενικά	Για ποργωρημένους
	Για προχωρημένους
Q Search	Γενικά Επιλονές δεδοιιένων Δίκτρο Ενριμέρωση Πιστοποιητικά
📄 Περιεχόμενο	
🚔 Εφαρμογές	Requests
🗴 Απόρρητο	Όταν ένας εξυπηρετητής απαιτεί ένα πιστοποιητικό:
	Ο Αυ <u>τ</u> όματη επιλογής ενός
📥 Ασφάλεια	Ε <u>ρ</u> ώτηση κάθε φορά
🚯 Sync	
🧕 Για προχωρημένους	\checkmark Query OCSP responder servers to confirm the current validity of certificates
	Προβολή πιστοποιητικών Συσκευές ασφαλείας

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…».



(είριση πιστοποιητικών	
α πιστοποιητικά σας Ανθρώπων Εξυπηρετητώ	υν Αρχών Τρίτων
Έχετε πιστοποιητικά στο αρχείο που πιστοποιοι	ύν τις παρακάτω αρχές:
Όνομα πιστοποιητικού	Συσκευή ασφάλειας 🛱
Certigna	Builtin Object Token
⊿DigiCert Inc	
DigiCert Trusted Root G4	Builtin Object Token
DigiCert Assured ID Root G3	Builtin Object Token
DigiCert High Assurance EV Root CA	Builtin Object Token
DigiCert Global Root G2	Builtin Object Token
DigiCert Assured ID Root G2	Builtin Object Token
DigiCert Global Root G3	Builtin Object Token 👻
Προ <u>β</u> ολή <u>Ε</u> πεξεργασία εμπιστοσύνης	Ε <u>ι</u> σαγωγή Ε <u>ξ</u> αγωγή <u>Δ</u> ιαγραφή ή άρση εμπιστοσύνης
	ОК

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

Επεξεργασία ρυθμίσεων εμπιστοσύνης πιστοποιητικών CA
Το πιστοποιητικό "DigiCert Trusted Root G4" αντιπροσωπεύει μια Αρχή Πιστοποίησης.
Επεξεργασία ρυθμίσεων εμπιστοσύνης:
📝 Το παρόν πιστοποιεί ιστοσελίδες.
📝 Το παρόν πιστοποιεί χρήστες email.
📝 Το παρόν πιστοποιεί κατασκευαστές λογισμικού.
ΟΚ Ακύρωση



5. Έκδοση Ψηφιακών Πιστοποιητικών

Η δυνατότητα έκδοσης Ψηφιακών Πιστοποιητικών υπογεγραμμένων από την αρχή πιστοποίησης DigiCert είναι διαθέσιμη από εδώ: <u>https://www.digicert.com/sso</u>. 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.

Gdigicert CERTCENTRAL.
IDP Selection
Please enter the Identity Provider to authenticate with:
Εθνικό Μετσόβιο Πολυτεχνείο
Εθνικό Μ ετσόβιο Πολυτεχνείο

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

Gdigicert Certcentral.
IDP Selection
Please enter the Identity Provider to authenticate with:
Εθνικό Μετσόβιο Πολυτεχνείο
Start single sign-on

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



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

<u>Θα πρέπει να σημειωθεί ότι αν η σύνδεσή σας δεν είναι εφικτή, πιθανώς το οικείο σας Ίδρυμα/Φορέας</u> 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".

Gdigicert CERTCENTRAL							
Request a Ce	Request a Certificate						
Choose a product							
Product:	Premium		•				
CSR: (optional)							
Common Name:	Χρήστης Δοκιμα	στικός					
Email:	academicid@cal	lc.grnet.gr					
Organization:	Εικονικός Οικείο	ς Φορέας					
	Request Certifica	te					
My Certificates		_					
Order #	Date	Common Name		Status	Product	Expires	
			No Certificate	s Found.			
Per Page: 20 -							

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".

Gdigicert CE	RT CENTRA	L.				
Request a C	ertifica	te				
Choose a product						
Product:	Premium		•			
CSR: (optional)						
Common Name:	Χρήστης Δο	κιμαστικός				
Email:	academicid@	@callc.grnet.gr				
Organization:	Εικονικός Οι	κείος Φορέας				
	Request Cer	tificate				
My Certificates						
Order #	Date	Common Name	Status	Product	Expires	
			No Certificates Found.			
Per Page: 20 •						



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.

٢	Gdigicert CERTCENTRAL.						
F	Request a Certificate						
M	Certificate Order Requested. (Order # 767551) My Certificates						
Order# Date Common Name Status Product E				Expires			
	767551	2015-09-23 15:32	Ιωάννης Πέτρου	Pending	Premium	N/A	
	Per Page:	20 •					1 to 1 of 1

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.

grnet Gdigicert				
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 DigiCer	rt Premium Certificate corrections, contact your administrator.					
DigiCert Personal ID Details	DigiCert Personal ID Details					
Name:	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 ARV 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, issued by DigiCert to you, regardless of () the Certificate type (email, code signing, Direct, or TLS/SSL), (ii) when you request the 1. Jagree to the terms of the subscriber agreement						
Your Personal ID will be valid for certificate or you will need to cor	1 year from the time it is issued. You have until October 21, 2015 to generate this atact your organization administrator to request a new email.					
If your web server is configured to DigiCert SHA2 Assured ID CA, as	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 "ΟΚ" να εισάγετε το PIN της κάρτας σας.

Επιλογή διαλ	ιόγου token	n			×	
Επιλέξτε GemP15	ένα token -1				•	
				DK AI	ໜ່ρωση	
	Απαιτείται	ι κωδικός πρόσβασης Εισάγετε τον κύριο κωδ •••• ΟΚ	δικό για το GemP15 Ακύρωση	X		
ΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ Ιουργείο Παιδείας, νας και Θρησκευμάτων		пе тур Ереман кан мул Еленайская	Ευρωπαϊκή Ένωση Ευρωπαϊκό Ταμείο Περιφεριακήs Ανάπτυξηs		ακήελλάδα είναι δυνατά ησιακό Γρόγραμμα ησική Σύγκλιση*	ΕΣΠΑ 2007-201

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

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.

Toolbox		gemaito
	Πιστοποιητικά	
Περιεχόμενα κάρτας		🚽 Κωδικός Αποσύνδεση
Πιστοποιητικά		
5		Gemalto USB Smart Card Reader 0 Gemalto USB Smart Card Reader 0 GemP15-1:Χρήστης Δοκιμαστικός's TERENA ID GemP15-1:Χρήστης Δοκιμαστικός's TERENA ID Gemalto USB Smart Card Reader 0
Ιδιότητες κάρτας		μικό κλειδί RSA 2048 bits
Διαχείριση κάρτας		Λεπτομέρειες Διαγραφή Προεπιλογή
Διαγνωστικό/Βοήθεια		Εισαγωγή Διαγραφή όλων Καταχώρηση όλων

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

Gdigicert CERTCENTRAL.						
Request a Cer	Request a Certificate					
Choose a product						
Product:	Choose a product •					
CSR: (optional)						
Common Name:	Ιωάννης Πέτρου					
Email:	academicid@callc.grnet.gr					
Organization:	Greek Research and Technology Network					
	Request Certificate					
My Certificates						
Order # Date	Common Name	Status	Product Expires			
767551 2015-09-23 15:32	Ιωάννης Πέτρου	Issued	Premium 2016-09-24 08:00 Download Revoke			

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



Gdigicert CERT	CENTRAL.					
Request a Cer	Request a Certificate					
Choose a product						
Product:	Choose a product					
CSR: (optional)						
Common Name:	Ιωάννης Πέτρου					
Email:	academicid@callc.grnet.gr					
Organization:	Greek Research and Technology Network					
	Request Certificate					
My Certificates						
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.

lfy	you revoke thi	s, it cannot be und	done. Continue?
		ОК	Ακύρωση

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».

<u>Eile Edit View Go M</u> essage Er	igmgil Icols Help	
🕭 Get Messages 👻 🖉 Write 🛛	🗮 Chat 🔹 Address Book 🔋 🗞 Tag 🐃 😓 Decrypt 🔍 Quick Filter	Search <ctrl+k></ctrl+k>
▲ test@localhost.com > ★ Inbox Announcements	Thunderbird Mail - test@localhost.com	
DI Local Folders	Email	
1 Trash		
📤 Outbox	Ligiji Kead messages	
	Write a new message	
	Accounts	
	View settings for this account	
	Create a new account:	
	🖾 Email 🖓 Chat 🦓 Newsgroups 🔼 Feeds	
	and and a second group of a second	
	Advanced Features	
	Q Search messages	
	Manage message filters	
	Anage folder subscriptions	
	Giffine settings	
1		

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



Account Settings	
	Security To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate. Digital Signing Use this certificate to digitally sign messages you send: <u>Select</u> <u>Clear</u> Digitally sign messages (by default) Encryption Use this certificate to encrypt & decrypt messages sent to you: Select Clear Default encryption setting when sending messages: <u>Never</u> (do not use encryption) Required (can't send message unless all recipients have certificates) Certificates <u>View Certificates</u> View Certificates Security Devices
Account Actions •	OK Cancel

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.

9	Device Manager			
9	Security Modules and Devices NSS Internal PKCS #11 Module Generic Crypto Services Software Security Device Builtin Roots Module Builtin Object Token	Details	Value	Log I <u>n</u> Log Qut Change <u>P</u> assword Load <u>U</u> nload Enable <u>F</u> IPS
				ОК

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.

Co Load PKCS#11 Device					
Enter the information for the module you want to add.					
<u>M</u> odule Name: Η συσκευή μου					
Module <u>f</u> ilename:	C:\Program Files (x86)	<u>B</u> rowse			
	ОК	Cancel			

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 "ΟΚ" για να το κλείσετε.

Oevice Manager			
C Device Manager Security Modules and Devices NSS Internal PKCS #11 Module Generic Crypto Services Software Security Device Builtin Roots Module Builtin Object Token H συσκευή μου Gemalto USB Smart Card Reader 0	Details Module Path	Value Η συσκευή μου C:\Program Files (x86)	Log In Log Out Change Password Load Load Enable FIPS
			ОК

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".



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Account Settings	
test@localhost.com Server Settings Copies & Folders Composition & Addressing Junk Settings Synchronization & Storage Return Receipts Security Local Folders Junk Settings Disk Space Outgoing Server (SMTP)	Security To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate. Digital Signing Use this certificate to digitally sign messages you send: gelect Clear Digitally sign messages (by default) Encryption Use this certificate to encrypt & decrypt messages sent to you: Select Clear Default encryption setting when sending messages: Never (do not use encryption) Required (can't send message unless all recipients have certificates) Certificates Security Devices
Account Actions •	
	OK Cancel

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

▲ test@localhost.com Server Settings	Security
Server Settings Copies & Folders Composition & Addressing Junk Settings Synchronization & Storage Return Receipts Security Local Folders Junk Settings Disk Space Outgoing Server (SMTP)	To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate. Digital Signing Use this certificate to digitally sign messages you send: Digitally sign messages (by default) Encryption Use this certificate to encrypt & decrypt messages sent to you: Default encryption setting when sending messages: Default encryption setting when sending messages: Clear Default encryption setting when sending messages: Default encryption setting when sending messages when set the s
Account Actions •	OK Cancel

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΛΛΗΝΙΚΗ

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

Password	Required 💌
?	Please enter the master password for the GemP15-1.
	••••
	OK Cancel

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 "ΟΚ" για να συνεχίσετε.

Select Certifica	ite	x
Certificate:	GemP15-1:COMODO CA Limited ID [23:88:97:85:D7:F8:CE:54:88:87:F6:EF:0E:10:87:0C]	-
Details of se	GemP15-1:COMODO CA Limited ID [23:88:97:85:D7:F8:CE:54:88:87:F6:EF:0E:10:87:0C]	
Issued to: E Serial Nun Valid from Certificate Email: sdi(Issued by: C Limited,L= Stored in: G	=sdi0900037@di.uoa.gr nber: 23:88:97:85:D7:F8:CE:54:B8:B7:F6:EF:0E:10:87:0C 2/3/2015 2:00:00 πμ to 2/3/2016 1:59:59 πμ Key Usage: Signing,Key Encipherment 1900037@di.uoa.gr CN=COMODO SHA-256 Client Authentication and Secure Email CA,O=COMODO CA Salford,ST=Greater Manchester,C=GB iemP15-1	
	ОК Са	ncel

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 "ΟΚ" στο αρχικό παράθυρο για να κλείσει και να συνεχίσετε με την σύνταξη ενός νέου e-mail.



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

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.

😋 Write: Ψηφιακή υπογραφή	
<u>File Edit View Insert Format Options Iools Help</u>	
📰 Send 🖌 Spelling 🕆 🕲 Attach 🔻 🖨 Security 💌 🖬 Save 🔻	
From: Ioannis Petrou <sdi09000 encrypt="" message<="" th="" this=""><th>-</th></sdi09000>	-
To: To: To:	
View Security Info	
Subject: Ψηφιακή υπογραφή	
Body Text ▼ Variable Width ▼ ■ A* A* A A A III 1 III III III III III III III	



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. Ανοίξτε 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.

🕞 Write: Κρυπτογράφηση	- 🗆 🗙
Ele Edit View Insert Format Ogtions Iools Help	
Send 🖌 Spelling 🔻 🖲 Attach 👻 🖨 Security 💌 🖬 Save 🔻	
From: Ioannis Petrou < sdi09000 🗸 Encrypt This Message	-
- To: Digitally Sign This Message	
View Security Info	
Subject: Κρυπτογράφηση	
Body Text ▼ Variable Width ▼ ■ A A A A ⊟ 1 至 1 至 2 至 2 ■ 0 -	

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.



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

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.

FILE HC	ME SEND / RECEIVE	FOLDER VIEW					
New New Email Items •	ि Ignore ≧ Clean Up - Belete	Reply Reply Forward More -	Move to: ? Team Email Create New Create New Creat	Move Rules OneNot	e Unread/ Follow Read Up ~	Search People Address Book Filter Email •	Send/Receive All Folders
New	Delete	Respond	Quick Steps	G Move	Tags	Find	Send/Receive
▲ Favorites	<	Search nikolas.theodosis@gmail.com	n (Ctrl+E)	🔎 🛛 Current Folder 🕞			
Inbox		All Unread		By Date ▼ Newest ↓			
Sent Items		W	e didn't find anything to show here.				
Deleted Items							
▲ Outlook Dat	a File						
Inbox							
Drafts							
Sent Items							
Deleted Items							
Junk E-mail							
Outbox							
RSS Feeds							
Search Folder	s						

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".

Outlook Options	2
General Mail	Help keep your documents safe and your computer secure and healthy.
Calendar	Protecting your privacy
People	Microsoft cares about your privacy. For more information about how Microsoft Outlook helps to protect your privacy, please see the privacy statements.
Search	Show the Microsoft Outlook privacy statement Office.com privacy statement Cutteres Exercises Researces
Advanced	Customer experience improvement rrogram Microsoft Office Feedback "Send a Smile" Privacy Statement
Customize Ribbo	n Security & more
Quick Access To	olbar Visit Office.com to learn more about protecting your privacy and security.
Add-Ins	Microsoft Trustworthy Computing
Trust Center	Microsoft Outlook Trust Center
	The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.
	OK Cancel

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 κρυπτογραφηση.

Change Security Settings	×
Security Setting Preference Security Settings Name:	25
Cryptography Format:	▼ S/MIME ▼
Default Security Sett	ing for this cryptographic message format
Default Security Sett	ing for all cryptographic messages
Security Labels	New Delete
Certificates and Algorit	hms
Signing Certificate:	Choose
Hash Algorithm:	· · · · · · · · · · · · · · · · · · ·
Encryption Certificate:	Choose
Encryption Algorithm:	· · · · · · · · · · · · · · · · · · ·
Send these certificat	es with signed messages
	OK Cancel

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 "ΟΚ" 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 "ΟΚ" 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.



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

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".

How would you like to create your signature?
 Use a webcam (New!) Draw my signature Use an image
• Use a certificate To continue, click Next, and then click on the digital signature field you would like to sign, or draw where you would like the signature to appear. Once you finish dragging out the desired area, you will be taken to the next step of the signing process.
Next > Cancel

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 ...".



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



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".

Sign Document
Sign As: sdi0900037@di.uoa.gr (COMODO SHA-256 Client Authentication and Secure Email Ci 🔻 🕖
Certificate Issuer: COMODO SHA-256 Client Authentication and Secure Email CA
Appearance: Standard Text
DN: email=sdi0900037@di. uoa.gr Date: 2015.03.05 15:03:35 +02'00'
Lock Document After Signing
Click Review to see if document content may affect signing Review
Sign Cancel

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.



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης