ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ
Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή εργασία

‘Διαδικασία έκδοσης ψηφιακού πιστοποιητικού για το ΤΕΙ Κρήτης’

Καγκέλη Κωνσταντίνα ΑΜ: 335
Γκλαβίνα Βασιλική ΑΜ: 223

Εισηγητής: κ. Κ.Βασιλάκης

Πρόλογος

Στην παρούσα πτυχιακή εργασία θα ασχοληθούμε με τη διαδικασία που πρέπει να ακολουθηθεί για την έκδοση ψηφιακού πιστοποιητικού για το ΤΕΙ Κρήτης, υπογεγραμμένο απο την Αρχή Πιστοποίησης HARICA. Πιο συγκεκριμμένα, το ΤΕΙ Κρήτης θα συμμετάσχει στην Υποδομή Δημόσιου Κλειδιού της HARICA και θα μπορούν να υποβάλλονται αιτήματα για έκδοση πιστοποιητικού χρήστη και διακομιστή. Θα μελετήσουμε με ποιους τρόπους μπορούν να χρησιμοποιηθούν τα πιστοποιητικά και τι εξασφαλίζει η ύπαρξή τους.

Ο σκοπός της παρούσας Πτυχιακής εργασίας είναι ανάδειξη του τρόπου έκδοσης των πιστοποιητικών και των εφαρμογών στις οποίες χρησιμοποιούνται.

Θα θέλαμε να ευχαριστήσουμε τον εισηγητή αυτής της εργασίας καθηγητή Κώστα Βασιλάκη για την συνεχή παρότρυνση καθώς και τις επισημάνσεις του σε κάθε στάδιο περάτωσης αυτής της δουλειάς. Επίσης θέλουμε να ευχαριστήσουμε τον Μιχάλη Βούρκα υπεύθυνο του ΚΕΔΔ του ΤΕΙ για τη συνεργασία και τη βοήθεια του για την πραγματοποίηση αυτής της εργασίας.

Επίσης, θέλουμε να ευχαριστήσουμε ιδιαίτερα τους γονείς μας για όλη τους την προσπάθεια όλα αυτά τα χρόνια, χάρη στην οποία βρισκόμαστε στην ευχάριστη αυτή στιγμή περάτωσης των σπουδών μας.

Ηράκλειο, Ιούνιος 2007

Κωνσταντίνα Καγκέλη
Βασιλική Γκλαβίνα

Περίληψη

Σκοπός αυτής της Πτυχιακής εργασίας είναι η έκδοση ψηφιακού πιστοποιητικού χρήστη και διακομιστή (server) για το ΤΕΙ Κρήτης, μέσω της Αρχής Πιστοποίησης HARICA(Hellenic Academic and Research Institutions Certificate Authority).

Στο 1^{ο} κεφάλαιο θα δούμε κάποιες πληροφορίες αναφορικά με την κρυπτογραφία, τους αλγόριθμους κρυπτογράφησης, την υποδομή δημόσιου κλειδιού, τα κρυπτογραφικά συστήματα, το SSL(Secure Socket Layer) και τις ψηφιακές υπογραφές .

Στο 2^{ο} κεφάλαιο θα παρουσιάσουμε κάποια στοιχεία σχετικά με το ΕΔΕΤ(Εθνικό Δίκτυο Έρευνας και Τεχνολογίας) και την υποδομή δημόσιου κλειδιού HARICA.

Στο 3^{ο} κεφάλαιο θα ασχοληθούμε με τη συνεργασία του ΤΕΙ Κρήτης με τη HARICA.

Στο 4^{ο} κεφάλαιο θα περιγράψουμε τη διαδικασία που ακολουθήσαμε για την έκδοση πιστοποιητικών για χρήστη. Έπειτα θα δούμε την εγκατάσταση του πιστοποιητικού στους browsers και σε προγράμματα ηλεκτρονικού ταχυδρομείου, καθώς και τη χρήση του, για την υπογραφή και κρυπτογράφηση email. Κατόπιν την ανάκληση πιστοποιητικού και τους λόγους για τους οποίους μπορεί να γίνει αυτό.

Στο 5^{ο} κεφάλαιο θα περιγράψουμε τη διαδικασία έκδοσης πιστοποιητικού για διακομιστή. Τις ενέργειες από την πλευρά των διαχειριστών του διακομιστή για την έκδοση και χρήση του πιστοποιητικού.

Η πτυχιακή εργασία ολοκληρώνεται με μια σύνοψη των εργασιών που εκτελέσαμε και των συμπερασμάτων που προκύπτουν. Επίσης γίνεται μια αναφορά σε πιθανή αναβάθμιση της υπηρεσίας. Τέλος επισημαίνουμε τα προβλήματα και τις δυσκολίες που υπήρχαν στη διάρκεια της υλοποίησης της εργασίας .

Στο τέλος της εργασίας υπάρχουν παραρτήματα με την αναλυτική περιγραφή όλων των διαδικασιών που ακολουθήθηκαν.

Περιεχόμενα

1

Εισαγωγή

Στο κεφάλαιο αυτό θα δούμε κάποιες πληροφορίες αναφορικά με την κρυπτογραφία, τους αλγόριθμους κρυπτογράφησης, την υποδομή δημόσιου κλειδιού, τα κρυπτογραφικά συστήματα, το SSL(Secure Socket Layer) και τις ψηφιακές υπογραφές .

1.1 Κρυπτογραφία

Κρυπτογραφία είναι η επιστήμη και η ικανότητα να γράφεις με μυστικότητα -κρατώντας τις πληροφορίες μυστικές. Όταν αναφερόμαστε σε υπολογιστές, η κρυπτογραφία προστατεύει δεδομένα έναντι της αποκάλυψης αυτών χωρίς άδεια. Μπορεί να αναγνωρίσει την ταυτότητα του χρήστη και φανερώνει την πλαστογραφία χωρίς άδεια.

1.2 Τι είναι κρυπτογράφηση

Κρυπτογράφηση είναι μια διεργασία με την οποία ένα μήνυμα (που ονομάζεται *plaintext)* μετατρέπεται σε ένα άλλο μήνυμα (που ονομάζεται *ciphertext)* χρησιμοποιώντας μια μαθηματική συνάρτηση (αλγόριθμος κρυπτογράφησης) και ένα ειδικό password κρυπτογράφησης, που ονομάζεται *κλειδί.*

Αποκρυπτογράφηση είναι η ανάποδη διεργασία : το *ciphertext* μετατρέπεται στο αρχικό κείμενο *(plaintext)* χρησιμοποιώντας μια άλλη μαθηματική συνάρτηση και ένα άλλο κλειδί. Σε μερικά κρυπτογραφικά συστήματα το κλειδί κρυπτογράφησης και το κλειδί αποκρυπτογράφησης μπορεί να είναι το ίδιο. Ο μόνος τρόπος να αποκρυπτογραφήσεις ένα ciphertext είναι να γνωρίζεις το μυστικό κλειδί mycard. Εάν δεν ξέρεις το μυστικό κλειδί και δεν έχεις πρόσβαση σε έναν πολύ γρήγορο υπολογιστή, δεν μπορείς να το αποκρυπτογραφήσεις. Ακόμα εάν χρησιμοποιήσεις ένα ισχυρό αλγόριθμο κρυπτογράφησης και ένας υπέρ-υπολογιστής δεν θα μπορέσει να σε βοηθήσει.

1.3 Τι μπορούμε να επιτύχουμε με την κρυπτογράφηση.

Η κρυπτογράφηση μπορεί να παίξει σημαντικό ρόλο στις καθημερινές μας υπολογιστικές και επικοινωνιακές μας ανάγκες :

- Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες αποθηκευμένες στον υπολογιστή μας από πρόσβαση ενός τρίτου, με ή χωρίς άδεια.
- Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες κατά την διάρκεια της μεταφοράς από ένα υπολογιστικό σύστημα στο άλλο.
- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να εμποδίσει και για να εντοπίσει τυχαίες ή σκόπιμες αλλαγές στα δεδομένα μας.

- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να επικυρώσει την ταυτότητα του δημιουργού.

Πέρα από αυτά τα πλεονεκτήματα, υπάρχουν και κάποια όρια τα οποία πρέπει να γνωρίζουμε για να αποφεύγουμε τα ανεπιθύμητα αποτελέσματα :

- Η κρυπτογράφηση δεν μπορεί να προφυλάξει τα δεδομένα μας από κάποιον εισβολέα που θέλει να σβήσει τα δεδομένα μας όπως είναι.
- Ένας εισβολέας μπορεί να έχει τροποποιήσει και να εκθέτει ένα πρόγραμμα κρυπτογράφησης από μόνος του, έτσι ώστε να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα με το δικό του κλειδί. Ή μπορεί να κρατά σε ένα αρχείο όλα τα κλειδιά για να τα χρησιμοποιήσει αργότερα.
- Ένας εισβολέας μπορεί να έχει πρόσβαση στα αρχεία μας πριν τα κρυπτογραφήσουμε και αφού τα αποκρυπτογραφήσουμε.
- Ένας εισβολέας ίσως βρει έναν άγνωστο προηγούμενα και σχετικά εύκολο τρόπο να αποκρυπτογραφεί τα μηνύματα που εμείς κρυπτογραφούμε με κάποιο αλγόριθμο.

Για όλους αυτούς του λόγους, η κρυπτογράφηση θα πρέπει να θεωρείται σαν ένα μέρος της ολικής στρατηγικής ασφαλείας που έχουμε, και όχι σαν υποκατάστατο άλλων μέτρων ασφαλείας που πρέπει να έχουμε, όπως είναι ο κατάλληλος έλεγχος πρόσβασης στον υπολογιστή μας.

1.4 Στοιχεία της κρυπτογράφησης.

Υπάρχουν πολλοί διάφοροι τρόποι με τους οποίους μπορούμε να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε μια πληροφορία με έναν υπολογιστή. Παρ' όλα, αυτά όλα αυτά τα συστήματα κρυπτογράφησης μοιράζονται κοινά στοιχεία :

Plaintext

Η πληροφορία την οποία επιθυμούμε να κρυπτογραφήσουμε.

Ciphertext

Η πληροφορία αφού αυτή κρυπτογραφήθηκε.

Αλγόριθμος κρυπτογράφησης

Ο αλγόριθμος κρυπτογράφησης είναι μια συνάρτηση, συνήθως μαθηματικών αρχών, η οποία εκτελεί το έργο της κρυπτογράφησης και της αποκρυπτογράφησης των δεδομένων μας.

Κλειδιά κρυπτογράφησης

Τα κλειδιά κρυπτογράφησης χρησιμοποιούνται από τον αλγόριθμο κρυπτογράφησης για να ορίσουν πώς τα δεδομένα είναι κρυπτογραφημένα ή αποκρυπτογραφημένα. Τα κλειδιά είναι παρόμοια με τα password των υπολογιστών: όταν ένα κομμάτι πληροφορίας κρυπτογραφείται, πρέπει να έχουμε το σωστό κλειδί για να έχουμε πρόσβαση πάλι σε αυτό. Αλλά αντίθετα με ένα πρόγραμμα που χρησιμοποιεί password, ένα πρόγραμμα κρυπτογράφησης δεν συγκρίνει το κλειδί που δίνουμε με το κλειδί που αρχικά χρησιμοποιούμε για να κρυπτογραφήσουμε το αρχείο, και μετά μας παρέχει πρόσβαση εάν τα δύο κλειδιά ταιριάζουν. Αντίθετα ένα πρόγραμμα κρυπτογράφησης χρησιμοποιεί το κλειδί μας για να μετατρέψει το ciphertext στο αρχικό κείμενο. Εάν δώσουμε το σωστό κλειδί θα πάρουμε το αρχικό μήνυμα. Εάν προσπαθήσουμε να αποκρυπτογραφήσουμε ένα αρχείο με λάθος κλειδί, θα πάρουμε σκουπίδια.

Μήκος κλειδιών

Όπως και με τα password, τα κλειδιά κρυπτογράφησης έχουν ένα προκαθορισμένο μήκος. Τα μακρύτερα κλειδιά είναι περισσότερο δύσκολο να τα μαντέψει κάποιος από τα μικρότερα γιατί υπάρχουν περισσότερα πιθανά κλειδιά που πρέπει να δοκιμάσει κάποιος επιτιθέμενος, για να βρει το σωστό. Μερικά συστήματα κρυπτογράφησης μας επιτρέπουν να χρησιμοποιούμε διαφορετικό μήκος κλειδιών και μερικά μας επιτρέπουν μεταβλητού μήκους κλειδιών.

1.5 Δύναμη και αντοχή κρυπτογράφησης

Όλοι οι τύποι της κρυπτογραφίας δεν είναι ίδιοι. Μερικά συστήματα παρακάμπτονται εύκολα, ή "σπάζονται". Άλλα αντιστέκονται αρκετά ακόμα και στις ποιο καλές επιθέσεις. Η ικανότητα ενός κρυπτογραφικού συστήματος να προστατεύσει την πληροφορία από μια επίθεση ονομάζεται η αντοχή του. Η αντοχή εξαρτάται από πολλούς παράγοντες, περιλαμβάνοντας :

- Η μυστικότητα του κλειδιού.
- Η δυσκολία να μαντέψουμε το κλειδί, ή να δοκιμάσουμε όλα τα πιθανά κλειδιά. Μακρύτερα κλειδιά είναι γενικά δυσκολότερο να μαντέψεις ή να βρεις.
- Η δυσκολία να αναστρέψουμε έναν αλγόριθμο κρυπτογράφησης χωρίς να γνωρίζουμε το κλειδί (σπάσιμο του αλγόριθμου κρυπτογράφησης).
- Η ύπαρξη άλλων δρόμων, όπως λέμε "πίσω πόρτα" με τους οποίους μπορούμε να αποκρυπτογραφήσουμε ποιο εύκολα ένα αρχείο χωρίς να γνωρίζουμε το κλειδί κρυπτογράφησης.
- Η ικανότητα να αποκρυπτογραφήσεις ένα ολόκληρο κρυπτογραφημένο μήνυμα εάν γνωρίζεις τον τρόπο με τον οποίον αποκρυπτογραφήθηκε ένα μέρος αυτού (known text attack).
- Η ιδιοκτησία και η γνώση των χαρακτηριστικών του plaintext από τον επιτιθέμενο. (Για παράδειγμα, ένα κρυπτογραφικό σύστημα είναι ευπρόσβλητο σε επίθεση εάν όλα τα μηνύματα που κρυπτογραφούνται με αυτό, αρχίζουν και τελειώνουν με ένα γνωστό κομμάτι κειμένου.)

Ο στόχος στον σχεδιασμό κρυπτογραφικών συστημάτων είναι η δημιουργία ενός αλγόριθμου που θα είναι πολύ δύσκολο να αναστραφεί χωρίς το κλειδί. Η δυσκολία της αναστροφής αυτής πρέπει να είναι σχεδόν ισοδύναμη με την προσπάθεια που απαιτείται για να μαντέψουμε το κλειδί προσπαθώντας με πιθανές λύσεις κάθε φορά. Για να μπορέσουμε να κρατήσουμε την διαδικασία αναστροφής του αλγόριθμου πολύ δύσκολη χρειάζεται να χρησιμοποιηθούν μαθηματικά υψηλού επιπέδου.

Η κρυπτογραφική δύναμη δεν μπορεί σχεδόν ποτέ να αποδειχθεί θετική, μπορεί όμως να γίνει το αντίθετο. Όταν ένας καινούργιος αλγόριθμος σχεδιάζεται, οι δημιουργοί του πιστεύουν ότι είναι τέλειος. Πιστεύουν πως είναι τόσο δυνατός ώστε δεν υπάρχει περίπτωση να αποκρυπτογραφηθεί ένα ciphertext χωρίς την χρήση του κατάλληλου κλειδιού. Επίσης οι σχεδιαστές προσπαθούν να "σπάσουν" τον αλγόριθμο με είδη γνωστούς τρόπους επιθέσεων. Καθώς όμως ο χρόνος περνάει καινούργιες τεχνικές επίθεσης ανακαλύπτονται και δημοσιεύονται.

Για το λόγο αυτό είναι καλή ιδέα να είμαστε ιδιαίτερα προσεκτικοί με καινούργιους κρυπτογραφικούς αλγόριθμους. Με πολύ λίγες εξαιρέσεις, οι

περισσότεροι κρυπτογραφικοί αλγόριθμοι έχουν στοιχειώδη ελαττώματα που τους κάνουν ακατάλληλους για σοβαρό σκοπό.

1.6 Αλγόριθμοι κρυπτογράφησης και συναρτήσεις

Υπάρχουν δύο βασικά είδη κρυπτογραφικών αλγόριθμων σε χρήση σήμερα:

- **Κρυπτογραφία προσωπικού κλειδιού,** (Private key cryptography), η οποία χρησιμοποιεί το ίδιο κλειδί για να κρυπτογραφήσει και να αποκρυπτογραφήσεί το μήνυμα. Αυτός ο τύπος είναι επίσης γνωστός σαν κρυπτογραφία συμμετρικού κλειδιού (symmetric key cryptography).
- **Κρυπτογραφία δημόσιου κλειδιού,** (Public key cryptography), η οποία χρησιμοποιεί ένα δημόσιο κλειδί (public key) για να κρυπτογραφήσει το μήνυμα, και ένα προσωπικό κλειδί (private key) για να το αποκρυπτογραφήσει. Το όνομα "δημόσιο κλειδί" οφείλεται στο γεγονός ότι μπορούμε να κάνουμε το κλειδί αυτό δημοσίως γνωστό χωρίς να διακινδυνεύσουμε την μυστικότητα του μηνύματος ή του κλειδιού αποκρυπτογράφησης. Τα συστήματα δημόσιου κλειδιού είναι επίσης γνωστά σαν κρυπτογραφία ασύμμετρου κλειδιού (asymmetric key cryptography).

Η κρυπτογραφία προσωπικού κλειδιού χρησιμοποιείται συχνότερα για να προστατεύσει πληροφορίες που είναι αποθηκευμένες στον σκληρό δίσκο ενός υπολογιστή, ή για να κρυπτογραφήσει πληροφορίες που μεταφέρονται μέσω επικοινωνιακού συνδέσμου ανάμεσα σε δύο διαφορετικές μηχανές. Επίσης είναι γενικά πολύ γρηγορότερη από την κρυπτογραφία δημόσιου κλειδιού και ευκολότερη στην εφαρμογή. Δυστυχώς έχει ένα πρόβλημα που έχει περιορίσει την χρήση της : για να ανταλλάξουν δύο άνθρωποι με ασφάλεια τα μηνύματα τους, πρέπει πρώτα να ανταλλάξουν με ασφάλεια το κλειδί κρυπτογράφησης (private key).

Οι αλγόριθμοι δημόσιου κλειδιού ξεπερνούν αυτό το πρόβλημα. Οι άνθρωποι που θέλουν να επικοινωνήσουν δημιουργούν ένα δημόσιο και ένα προσωπικό κλειδί. Το δημόσιο κλειδί δημοσιεύεται, ώστε να μπορεί ο καθένας να το αποκτήσει. Εάν κάποιος κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί του παραλήπτη, τότε **μόνο** ο παραλήπτης θα μπορέσει να αποκρυπτογραφήσει και να διαβάσει το μήνυμα χρησιμοποιώντας το προσωπικό του κλειδί.

Η Κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται περισσότερο για δημιουργία ψηφιακών υπογραφών (digital signatures) στα δεδομένα, όπως στο ηλεκτρονικό ταχυδρομείο (e-mail) για να πιστοποιήσει την προέλευση και την ακεραιότητα των δεδομένων. Στην περίπτωση των ψηφιακών υπογραφών, το προσωπικό κλειδί χρησιμοποιείται για την δημιουργία της ψηφιακής υπογραφής και το δημόσιο κλειδί για την επικύρωση αυτής. Όταν ο παραλήπτης λαμβάνει ένα γράμμα, ψηφιακά υπογεγραμμένο με το προσωπικό κλειδί του αποστολέα, μπορεί να το επικύρωση χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα.

Οι αλγόριθμοι δημόσιου κλειδιού έχουν ένα σημαντικό πρόβλημα, είναι απίστευτα αργοί . Είναι 10 με 100 φορές αργότεροι από τους αλγόριθμους συμμετρικού κλειδιού. Για το λόγο αυτό υπάρχει και ένα τρίτο σύστημα κρυπτογράφησης :

- **Κρυπτογραφία διασταύρωσης δημόσιου /προσωπικού κλειδιού** (Hybrid public/private cryptosystem). Σε αυτά τα συστήματα, χρησιμοποιείται αργότερη κρυπτογραφία δημόσιου κλειδιού για ανταλλαγή ενός τυχαίου κλειδιού συνόδου

(session key), το οποίο τότε χρησιμοποιείται σαν βάση του αλγόριθμου κρυπτογράφησης προσωπικού κλειδιού . Ένα κλειδί συνόδου χρησιμοποιείται μόνο για μια μόνο περίοδο κρυπτογράφησης και μετά καταστρέφεται. Σχεδόν όλες η πρακτικές εφαρμογές της κρυπτογραφίας δημόσιου κλειδιού είναι συστήματα διασταύρωσης.
Τελικά υπάρχει ένα νέο είδος συνάρτησης που έχει γίνει δημοφιλές τα τελευταία χρόνια και χρησιμοποιείται με συνδυασμό με την κρυπτογραφία δημόσιου κλειδιού.

Συναρτήσεις αποσύνθεσης μηνύματος (Message digest functions)

Μια συνάρτηση αποσύνθεσης μηνύματος δημιουργεί ένα μοναδικό πρότυπο από bits για μία δοσμένη είσοδο. Η τιμή αποσύνθεσης υπολογίζεται με τέτοιο τρόπο ώστε να είναι αδύνατο να υπολογιστεί μια είσοδος από ένα τεμαχισμένο μήνυμα χρησιμοποιώντας την ίδια τιμή της αποσύνθεσης. Οι αποσυνθέσεις μηνυμάτων θεωρούνται συχνά σαν δαχτυλικά αποτυπώματα (fingerprint) για αρχεία.

1.6.1 Αλγόριθμοι συμμετρικού κλειδιού (Symmetric key or private key)

Οι αλγόριθμοι αυτοί χρησιμοποιούνται για μεγάλο όγκο δεδομένων ή επίσης για δεδομένα με συνεχή ροή. Είναι σχεδιασμένοι να εκτελούνται με ταχύτητα και έχουν μεγάλο αριθμό πιθανόν κλειδιών. Οι καλύτεροι αλγόριθμοι συμμετρικού κλειδιού φτάνουν το τέλειο: αν ένα δεδομένο κρυπτογραφηθεί με ένα δοσμένο κλειδί, δεν υπάρχει τρόπος να το αποκρυπτογραφήσεις χωρίς να έχεις το ίδιο κλειδί.

Οι αλγόριθμοι συμμετρικού κλειδιού μπορούν να χωριστούν σε δύο κατηγορίες Σε αυτούς που κρυπτογραφούν ένα κομμάτι δεδομένων μόνο μιας ή αλγόριθμους "μπλοκ", *{Block algorithms),* και σε αυτούς που κάνουν την κρυπτογράφηση byte παρά byte σε δεδομένα συνεχής ροής ή αλγόριθμους "συρμού", *{Stream algorithms).*

Υπάρχουν πολλοί αλγόριθμοι συμμετρικού κλειδιού σε χρήση σήμερα. Μερικοί από αυτούς που συναντάμε συνήθως για την ασφάλεια του web είναι οι παρακάτω.

DES. (Data Encryption Standard) Εφαρμόστηκε από την κυβέρνηση τον Ηνωμένων πολιτειών το 1977 και σαν ANSI πρότυπο το 1981. Είναι ένας "μπλοκ" αλγόριθμος που χρησιμοποιεί κλειδί 56-bit και έχει πολλούς τύπους λειτουργιών ανάλογα με τον σκοπό που χρησιμοποιείται. Είναι ένας δυνατός αλγόριθμος, αλλά πιθανολογείται ότι μια μηχανή που θα είναι ικανή να σπάσει ένα κρυπτογραφημένο μήνυμα σε μερικές ώρες μπορεί να κατασκευαστεί για περισσότερα από 1.000.000 δολάρια. Τέτοιες μηχανές ίσως υπάρχουν αν και καμία κυβέρνηση ή επίσημη εταιρία δεν παραδέχεται ότι έχει.

DESX. Είναι μια απλή μετατροπή του DES αλγόριθμου για να βελτιώσει την ασφάλεια και να κάνει την αναζήτηση κλειδιού δυσκολότερη.

Triple - DES. Είναι ένας τρόπος να κάνεις το DES τουλάχιστον δυο φορές ποιο ασφαλές χρησιμοποιώντας τον DES αλγόριθμο τρεις φορές με τρία διαφορετικά κλειδιά

IDEA. (International Data Encryption Algorithm) Αναπτύχθηκε στην Ζυρίχη της Ελβετίας, από τους James L. Massey και τον Xuejia Lai και δημοσιεύτηκε το 1990. Χρησιμοποιεί κλειδί 128-bit και θεωρείται ότι είναι πολύ ασφαλής. Ο IDEA χρησιμοποιείται και από το πρόγραμμα PGP.

RC2. Είναι "μπλοκ" αλγόριθμος και αναπτύχθηκε από τον Ronald Rivest και κρατείται σαν επαγγελματικό μυστικό από την RSA Data Security. Αυτός ο αλγόριθμος ανακαλύφθηκε από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet το 1996. Ο RC2 πωλείται με μια λειτουργία όπου μπορείς να χρησιμοποιήσεις κλειδιά από I-bit έως 2048-bit. Συχνά το μήκος όμως φτάνει στα 40-bit, σε εφαρμογές που εξάγονται, και αυτό είναι πολύ ευάλωτο στην επίθεση έρευνας κλειδιού.

RC4. Είναι αλγόριθμος "συρμού" και αναπτύχθηκε από τον Ronald Rivest και κρατείται σαν επαγγελματικό μυστικό από την RSA Data Security. Επίσης αυτός ο αλγόριθμος ανακαλύφθηκε από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet το 1994 και εμφανίζεται αρκετά ασφαλής. Χρησιμοποιεί κλειδιά μήκους I-bit έως 2048-bit, και συχνά περιορίζεται σε 40-bit κλειδιά για προγράμματα που εξάγονται.

Η εφαρμογή του SSL στο εξαγόμενο Netscape, χρησιμοποιεί μήκος κλειδιού 128-bit, από τα οποία τα 88 αποκαλύπτονται, παράγοντας ένα μυστικό κλειδί 40-bit. Η Netscape ισχυρίζεται ότι τα 88 bits παρέχουν προστασία εναντίον των codebook επιθέσεων, στις οποίες 2^{40} κλειδιά είναι προϋπολογισμένα και τα αποτελέσματα των κρυπτογραφημένων προτύπων φυλάσσονται. (Για την αποθήκευση των πρώτον 8 bytes από όλα τα πρότυπα χρειάζονται 900 σκληροί δίσκοι των 10-gigabyte).

1.6.2 Αλγόριθμοι δημόσιου κλειδιού (public key)

Η ύπαρξη κρυπτογραφίας δημόσιου κλειδιού πρωτοπαρουσιάστηκε το φθινόπωρο του 1975 από τους Whitfield Diffie και Martin Hellman. Οι δύο ερευνητές τότε στο Stanford University, έγραψαν ένα έγγραφο στο οποίο υποστήριζαν την ύπαρξη μιας κρυπτογραφικής τεχνικής, με την οποία μια πληροφορία που κρυπτογραφούταν με ένα κλειδί μπορούσε να αποκρυπτογραφηθεί από ένα δεύτερο, χωρίς να έχουν σχέση τα δύο κλειδιά μεταξύ τους. Ο Robert Merkle, τότε ένας απόφοιτος του Berkeley, είχε παρόμοιες ιδέες, αλλά λόγω των ιδιοτροπιών των ακαδημαϊκών εκδόσεων δεν δημοσιεύτηκαν τότε, αλλά όταν η ιδέα της κρυπτογράφησης δημοσίου κλειδιού ήταν ευρέως γνωστή.

Μέχρι τότε, μια ποικιλία από κρυπτογραφικά συστήματα δημόσιου κλειδιού είχαν αναπτυχθεί. Δυστυχώς υπήρχαν σημαντικά λιγότερα κρυπτογραφικά συστήματα δημόσιου κλειδιού από ότι συμμετρικού κλειδιού. Η αιτία έχει να κάνει με τον τρόπο που έχουν σχεδιαστεί οι αλγόριθμοι. Καλοί συμμετρικοί αλγόριθμοι απλά αλλάζουν την είσοδο ανάλογα με το κλειδί. Για να αναπτύξουμε ένα καινούργιο αλγόριθμο συμμετρικού κλειδιού θα πρέπει να βρούμε έναν νέο ασφαλή τρόπο να αλλάζουμε την είσοδο. Οι αλγόριθμοι δημοσίου κλειδιού στηρίζονται στα μαθηματικά. Αναπτύσσοντας έναν τέτοιο αλγόριθμο απαιτείται να λυθεί ένα μαθηματικό πρόβλημα με ειδικές ιδιότητες.

Diffie-Hellman key exchange. Ένα σύστημα για ανταλλαγή κρυπτογραφικών κλειδιών ανάμεσα σε ενεργά μέρη. Το Diffie-Hellman δεν είναι ακριβώς μια μέθοδος κρυπτογράφησης και αποκρυπτογράφησης, αλλά μια μέθοδος ανάπτυξης και ανταλλαγής ενός μοιρασμένου μυστικού κλειδιού σε ένα δημόσιο κανάλι επικοινωνίας. Στην πραγματικότητα, τα δύο μέρη συμφωνούν σε μερικές κοινές αριθμητικές τιμές, και τότε το κάθε μέρος δημιουργεί ένα κλειδί. Οι μαθηματικοί μετασχηματισμοί των κλειδιών ανταλλάσσονται. Κάθε μέρος

μπορεί τότε να υπολογίσει ένα τρίτο κλειδί συνόδου (session key) το οποίο δεν μπορεί εύκολα να παραχθεί από έναν επιτιθέμενο που γνωρίζει και τον δύο τις αριθμητικές τιμές.

RSA. Ο RSA είναι ένα πολύ γνωστό κρυπτογραφικό σύστημα αναπτυγμένο από καθηγητές του MIT, τους Ronald Rivest, Adi Shamir και Leonard Adleman. Ο RSA μπορεί να χρησιμοποιηθεί και για να κρυπτογραφεί πληροφορίες αλλά και σαν βάση του συστήματος ψηφιακών υπογραφών. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για να αποδείξουν την πατρότητα και γνησιότητα της ψηφιακής πληροφορίας. Το κλειδί μπορεί να είναι οποιουδήποτε μήκους, ανάλογα με την εφαρμογή που χρησιμοποιείται.

EIGamal. Ο δημιουργός αυτού του αλγόριθμου είναι ο Taher ELGamal, είναι ένα κρυπτογραφικό σύστημα δημόσιου κλειδιού που είναι βασισμένο στο πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Hellman. Ο ELGamal χρησιμοποιείται για κρυπτογράφηση και για ψηφιακές υπογραφές με τον ίδιο τρόπο όπως ο RSA.

DSS. (Digital Signature Standard). Αναπτύχθηκε από την National Security Agency (NSA) και εφαρμόστηκε σαν ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών FIPS (Federal Information Processing Standard) από την NIST (National Institute for Standards and Technology). Ο DSS είναι βασισμένος στον αλγόριθμο ψηφιακών υπογραφών (DSA). Αν και ο DSA επιτρέπει κλειδιά οποιουδήποτε μήκους, μόνο κλειδιά ανάμεσα σε 512 και 1024 bits επιτρέπονται στον DSS. Όπως αναφέρθηκε, ο DSS μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, αν και είναι πιθανό να χρησιμοποιήσει DSA εφαρμογές για την κρυπτογράφηση επίσης.

1.7 Υποδομή δημόσιου κλειδιού(Public Key Infrastructure)

Το τελευταίο κομμάτι του puzzle της κρυπτογραφίας είναι ένα σύστημα για να αποδεικνύει την ταυτότητα των ανθρώπων που κρατούν κρυπτογραφικά κλειδιά.

Στην κρυπτογράφηση δημόσιου κλειδιού κάθε χρήστης απαιτείται να φτιάξει δύο κλειδιά:

- Ένα δημόσιο κλειδί το οποίο χρησιμοποιείται για να στέλνουμε κρυπτογραφημένα μηνύματα στον παραλήπτη, και για να επικυρώνουμε την ψηφιακή υπογραφή του αποστολέα.
- Ένα προσωπικό κλειδί, το οποίο χρησιμοποιείται από τον παραλήπτη για να αποκωδικοποιήσει τα κρυπτογραφημένα μηνύματα που λαμβάνει, και για να υπογράψει με την ψηφιακή υπογραφή του ο αποστολέας.

Ενώ τα προσωπικά κλειδιά είναι σχεδιασμένα να κρατιούνται μυστικά, τα δημόσια κλειδιά είναι σχεδιασμένα να δημοσιεύονται και να διανέμονται ευρέως.

Ένας απλός τύπος δημόσιου και προσωπικού κλειδιού περιέχει ελάχιστη πληροφορία εκτός από τις πραγματικές τιμές που χρειάζονται για να γίνει η κρυπτογράφηση και αποκρυπτογράφηση. Θα μπορούσαμε να πούμε ότι χρειαζόμαστε περισσότερες πληροφορίες να αποθηκεύονται σε κάθε δημόσιο κλειδί. Μαζί με την πληροφορία κρυπτογράφησης, ίσως επιθυμούμε να αποθηκεύσουμε το όνομα του χρήστη ή κάποια άλλη πληροφορία ταυτότητας. Για παράδειγμα αν έχουμε τρία δημόσια κλειδιά για τρείς ανθρώπους είναι δύσκολο να τα ξεχωρίσουμε. Αν όμως αποθηκεύσουμε περισσότερη πληροφορία στου καθένα το προσωπικό κλειδί, θα έχουμε τρόπο να ξέρουμε ποιο προσωπικό

κλειδί ανήκει σε ποιανού το δημόσιο κλειδί.Η περιοχή του ονόματος μπορεί να συμπληρωθεί με οποιδήποτε στοιχείο που θέλουμε. Άπαξ κα το κλειδί δημιουργηθεί με ένα όνομα, αυτό μπορεί να υπογραφτεί από ένα τρίτο πρόσωπο. Τα τρίτα πρόσωπα που επικυρώνουν την πληροφορία του κλειδιού πριν αυτό υπογραφτεί ονομάζονται αρχές πιστοποίησης(C.A Certification Authorities).

1.8 Λειτουργίες της κρυπτογράφησης στο WEB

Οι επαγγελματίες που ασχολούνται με την ασφάλεια έχουν ταυτίσει τέσσερις λέξεις για να περιγράφουν όλες τις λειτουργίες που εκτελεί η κρυπτογραφία στα σύγχρονα πληροφοριακά συστήματα. Οι διαφορετικές λειτουργίες είναι:

Confidentiality - **Εμπιστευτικότητα**

Η κρυπτογραφία χρησιμοποιείται για να μεταμορφώνει την πληροφορία που στέλνεται μέσω του Internet και αποθηκεύεται στους servers, έτσι ώστε να μην μπορούν να δουν το περιεχόμενο των δεδομένων αυτοί που κρυφοκοιτάνε. Μερικοί ονομάζουν αυτή την ιδιότητα **μυστικότητα (privacy)** αλλά οι περισσότεροι χρησιμοποιούν αυτή τη λέξη για να αναφέρονται στην προστασία της ατομικής πληροφορίας.

Authentication - **Επικύρωση - Απόδειξη γνησιότητας**

Οι Ψηφιακές Υπογραφές χρησιμοποιούνται για να εξακριβώνουν την ταυτότητα του αποστολέα ενός μηνύματος. Οι παραλήπτες ενός μηνύματος μπορούν να ελέγξουν την ταυτότητα του αποστολέα, ο οποίος υπέγραψε ψηφιακά το μήνυμα. Μπορούν να χρησιμοποιηθούν σε συνδυασμό με τα password ή και να τα αντικαταστήσουν.

Integrity -Ακεραιότητα

Υπάρχουν μέθοδοι που ελέγχουν αν ένα μήνυμα έχει μεταβληθεί την στιγμή της μεταφοράς. Συχνά αυτό γίνεται με τους κώδικες αποσύνθεσης μηνυμάτων ψηφιακά υπογεγραμμένων.

Nonrepudiation - **Απαγόρευση απάρνησης**

Οι κρυπτογραφικές αποδείξεις δημιουργούνται έτσι ώστε ο αποστολέας να μην μπορεί να απαρνηθεί το γεγονός της αποστολής του μηνύματος του.

1.9 Κρυπτογραφικά συστήματα σήμερα

Τα τελευταία χρόνια έχουν αναπτυχθεί και χρησιμοποιηθεί αρκετά κρυπτογραφικά συστήματα για το Internet. Μπορούμε να τα χωρίσουμε σε δύο κατηγορίες. Η πρώτη είναι προγράμματα και πρωτόκολλα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων του ηλεκτρονικού ταχυδρομείου (e-mail). Τα ποιο δημοφιλή είναι τα παρακάτω :

- **PGP**
- **S/MIME**

Η δεύτερη κατηγορία είναι πρωτόκολλα δικτύου που χρησιμοποιούνται για να παρέχουν εμπιστευτικότητα, ακεραιότητα, αναγνώριση ταυτότητας σε περιβάλλον δικτύου. Τέτοια συστήματα χρειάζονται αλληλεπίδραση πραγματικού χρόνου ανάμεσα στο client και ενός server για να δουλέψουν σωστά. Τα ποιο δημοφιλή είναι ταπαρακάτω:

- **SSL**
- **PCT**

- **S-HTTP**
- **SET and CyberCash**
- **DNSSEC**
- **IPsec and IPv6**
- **Kerberos**
- **SSH**

1.9.1 PGP (Pretty Good Privacy)

Το PGP είναι το πρώτο πρόγραμμα κρυπτογράφησης δημόσιου κλειδιού, γραμμένο από τον Phil Zimmerman που κυκλοφόρησε στο Internet τον Ιούνιο του 1991. Το PGP είναι ένα ολοκληρωμένο σύστημα που προσφέρει κρυπτογραφική προστασία των e-mails και των αρχείων γενικότερα. Το PGP επίσης είναι ένα σύνολο από standards που περιγράφουν τα formats των κρυπτογραφημένων μηνυμάτων, των κλειδιών και των ψηφιακών υπογραφών.

Το PGP είναι ένα κρυπτογραφικό σύστημα διασταύρωσης που χρησιμοποιεί τον RSA αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού για την διαχείριση των κλειδιών και τον IDEA συμμετρικό αλγόριθμο για την κύρια κρυπτογράφηση των δεδομένων.

Το PGP προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος που χρησιμοποιεί είναι ο IDEA. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης που χρησιμοποιεί είναι η MD5. Προσφέρει αναγνώριση γνησιότητας με την χρήση των δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

Το PGP είναι διαθέσιμο με δυο τρόπους, σαν μια μεμονωμένη εφαρμογή και σαν ένα ολοκληρωμένο πρόγραμμα ηλεκτρονικού ταχυδρομείου διαθέσιμο από την PGP Inc. Το μεμονωμένο πρόγραμμα "τρέχει" σε πολύ περισσότερα συστήματα από ότι το ολοκληρωμένο πρόγραμμα, αλλά είναι περισσότερο δύσχρηστο. Ένα τέτοιο παράδειγμα που ήταν πολύ διαδεδομένο είναι η εκδόσεις του PGP για περιβάλλον DOS. Επίσης η PGP Inc. αναπτύσσει διάφορα plug-ins για δημοφιλή προγράμματα ηλεκτρονικού ταχυδρομείου για να επιτρέψει σε αυτά να στέλνουν και να λαμβάνουν κρυπτογραφημένα μηνύματα με το PGP.

Ένα πρόβλημα με το PGP είναι η διαχείριση και πιστοποίηση των δημόσιων κλειδιών. Τα δημόσια κλειδιά δεν έχουν ημερομηνία λήξης, αντί αυτού, όταν τα κλειδιά εκτεθούν, εξαρτάται από τον ιδιοκτήτη εάν αυτός θέλει να διανέμει σε όλους αυτούς με τους οποίους είχε επικοινωνία μια ειδική PGP πιστοποίηση απόσυρσης (ακύρωσης). Οι ανταποκριτές που δεν μαθαίνουν το γεγονός αυτό και χρησιμοποιούν το εκτιθέμενο κλειδί για εβδομάδες, μήνες και χρόνια αργότερα για να στείλουν κρυπτογραφημένα μηνύματα ρισκάρουν την ασφάλεια των μηνυμάτων. Αυτό έχει σαν αποτέλεσμα, εάν δημιουργήσουμε και διανέμουμε ένα δημόσιο κλειδί, πρέπει να κρατήσουμε το μυστικό κλειδί για πάντα επειδή το κλειδί αυτό δεν λήγουν (expire) ποτέ.

Η πρόσφατη έκδοση του PGP5 χρησιμοποιεί ένα νέο τύπο κλειδιών με κρυπτογραφικούς αλγόριθμους τον DSS και τον Diffie-Helman.

1.9.2 S/MIME (Multipurpose Internet Mail Extensions)

Το MIME είναι ένα standard για αποστολή αρχείων με binary attachments μέσω του Internet. Το Secure/MIME είναι μια επέκταση του MIME standard για την αναγνώριση των κρυπτογραφημένων e-mail. Αντίθετα από το PGP, το S/MIME δεν εφαρμόσθηκε σαν ένα αυτόνομο πρόγραμμα, αλλά σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομείου.

Επειδή αυτό το εργαλείο προέρχεται από την RSA Data Security και περιλαμβάνει άδειες για όλους τους απαιτούμενους αλγόριθμους και όλες τις πατέντες, και επειδή οι μεγαλύτερες εταιρίες που πουλούν συστήματα e-mail ήδη έχουν επιχειρηματική σχέση με την RSA Data Security, είναι πιθανό το S/MIME θα υιοθετηθεί περισσότερο από το PGP, από τους πωλητές e-mail προγραμμάτων.

Το S/MIME προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώριση γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων. Το σύστημα μπορεί να χρησιμοποιηθεί με δυνατή ή αδύνατη κρυπτογράφηση.

Για να στείλουμε κρυπτογραφημένα μηνύματα σε κάποιον με το S/MIME, πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού του. Τα περισσότερα προγράμμαχα που χρησιμοποιούν το S/MIME κάνουν χρήση των X.509 v3 Public key infrastructures σαν και αυχές που δημιουργούνται από την VeriSign και από άλλες αρχές πιστοποίησης.

1.9.3 SSL (Secure Socket Layer)

Το SSL είναι ένα κρυπτογραφικό πρωτόκολλο για ασφαλή κανάλια επικοινωνίας διπλής κατεύθυνσης. Το SSL χρησιμοποιείται συχνά με το TCP/IP πρωτόκολλο του Internet. Το SSL είναι το κρυπτογραφικό σύστημα που χρησιμοποιείτε από τους web browsers όπως είναι ο Netscape Navigator και ο Microsoft Internet Explorer, αλλά μπορεί να χρησιμοποιηθεί σε οποιοδήποτε υπηρεσία TCP/IP.

Οι SSL συνδέσεις συχνά ξεκινούν από την πλευρά του web browser εξαιτίας της χρήσης ενός ειδικού προθέματος στην URL διεύθυνση. Για παράδειγμα το πρόθεμα "https://" χρησιμοποιείται για να υποδείξει μια SSL-κρυπτογραφημένη HTTP σύνδεση, ενώ "snews://" χρησιμοποιείται για να υποδείξει μια SSL-κρυπτογραφημένη NNTP σύνδεση.

Το SSL προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώριση γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

1.9.4 PCT (Private Communications Technology)

Το PCT είναι ένα ασφαλές πρωτόκολλο επιπέδου μεταφοράς, παρόμοιο με το SSL, το οποίο αναπτύχθηκε από την Microsoft. Το PCT αναπτύχθηκε σαν απάντηση στα προβλήματα που παρουσίασε το SSL 2.0, αλλά και στο SSL 3.0.

Αν και η Microsoft υποστηρίζει το SSL 3.0 και το TLS, το καινούργιο Transport Layer Security μοντέλο, η Microsoft σκοπεύει να συνεχίσει να υποστηρίζει το PCT γιατί χρησιμοποιείται από πολλούς μεγάλους πελάτες της Microsoft, στα εταιρικά τους δίκτυα (corporate intranets).

1.9.5 S-HTTP

Το S-HTTP είναι ένα σύστημα για υπογραφή και κρυπτογράφηση πληροφοριών που στέλνονται μέσω του HTTP πρωτοκόλλου. Το S-HTTP σχεδιάστηκε πριν να κυκλοφορήσει δημόσια το SSL. Περιλαμβάνει μερικά κομψά χαρακτηριστικά, όπως είναι η ικανότητα να έχει προϋπογράψει κείμενα που βρίσκονται σε έναν web server. Αλλά το S-HTTP είναι ένα νεκρό πρωτόκολλο επειδή η Netscape και η Microsoft έχουν αποτύχει να το εφαρμόσουν στους browsers.

1.9.6 SET

Το SET είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο για την αποστολή κρυπτογραφημένων αριθμών πιστωτικών καρτών μέσω του Internet. Το πρωτόκολλο αυτό είναι ακόμα υπό ανάπτυξη.

Υπάρχουν τρία μέρη που αποτελούν το SET : ένα "ηλεκτρονικό πορτοφόλι" που υπάρχει στον υπολογιστή του χρήστη, ένας server που τρέχει στα εμπορικά web sites, και ο SET server πληρωμής που τρέχει στις διάφορες τράπεζες των εμπόρων.

Για να χρησιμοποιήσουμε το SET σύστημα, πρέπει να εισάγουμε πρώτα τον αριθμό της πιστωτικής μας κάρτας μέσα στο πρόγραμμα του "ηλεκτρονικού πορτοφολιού". Οι περισσότερες εφαρμογές αποθηκεύουν τον αριθμό της πιστωτικής κάρτας σε ένα κρυπτογραφημένο αρχείο στον σκληρό μας δίσκο ή σε μια κάρτα (smart card). Το πρόγραμμα επίσης δημιουργεί ένα δημόσιο και ένα μυστικό κλειδί για την κρυπτογράφηση διάφορων οικονομικών πληροφοριών μας που θα σταλούν μέσω του Internet.

Όταν εμείς θελήσουμε να αγοράσουμε κάτι, ο αριθμός της πιστωτικής μας κάρτας κρυπτογραφείται και στέλνεται στον έμπορο. Το πρόγραμμα του έμπορου υπογράφει ψηφιακά το μήνυμα πληρωμής και το προωθεί στην τράπεζα όπου επεξεργάζεται. Έτσι ο SET server πληρωμής αποκρυπτογραφεί όλες τις πληροφορίες και χρεώνει την πιστωτική κάρτα. Τελικά, μια απόδειξη είσπραξης στέλνεται πίσω και σε εμάς, τους πελάτες, αλλά και στον έμπορο.

Οι Τράπεζες που επεξεργάζονται τις πιστωτικές κάρτες είναι ενθουσιασμένες για το SET επειδή αυτές κρατούν τους αριθμούς των πιστωτικών καρτών μακριά από χα χέρια των εμπόρων. Αυτό θα περιόριζε σημαντικά τις απάτες που γίνονται, γιατί είναι έμποροι, και όχι νεαροί hackers, που αυτοί είναι υπεύθυνοι για τις απάτες των πιστωτικών καρτών σήμερα.

Το SET προσφέρει εμπιστευτικότητα για τους αριθμούς των πιστωτικών καρτών, καθώς κρυπτογραφούνται χρησιμοποιώντας τον RSA αλγόριθμο. Αλλά δεν προσφέρει εμπιστευτικότητα (και κατά συνέπεια μυστικότητα) για χα υπόλοιπα στοιχεία της συναλλαγής του χρήστη. Αυτή ήταν μια αναγκαία

συμβιβαστική λύση για να κερδισθεί η έγκριση για εξαγωγή του SET προγράμματος χωρίς περιορισμούς. Το SET παρέχει ακεραιότητα, αναγνώριση ταυτότητας και απαγόρευση απάρνησης χρησιμοποιώντας συναρτήσεις αποσύνθεσης μηνύματος και ψηφιακές υπογραφές.

1.9.7 CyberCash

Το CyberCash είναι ένα πρωτόκολλο ηλεκτρονικής πληρωμής παρόμοιο στο σκοπό με το SET. Στην πραγματικότητα μέρη του SET είναι μοντέλα ανάπτυξης στο CyberCash. Είναι θα λέγαμε μια παραλλαγή προϊόντος.

1.9.8 DNSSEC (Domain Name System Security)

Το Domain Name System Security standard είναι ένα σύστημα που σχεδιάστηκε για να φέρει ασφάλεια στο Domain Name System Security (DNS). Το DNSSEC δημιουργεί ένα παράλληλο δημόσιο κλειδί υποδομής "χτισμένο" πάνω στο DNS σύστημα. Κάθε DNS domain καθορίζεται από ένα δημόσιο κλειδί. Ένα τέτοιο δημόσιο κλειδί μπορούμε να το αποκτήσουμε με έναν έμπιστο τρόπο από το εν λόγο domain ή αυτό μπορεί να φορτωθεί από πριν μέσα σε ένα DNS server χρησιμοποιώντας χο αρχείο "boot" του server.

Το DNSSEC αναγνωρίζεται για τις ασφαλής ανανεώσεις πληροφοριών στους DNS servers, κάνοντας το ιδανικό για απομακρυσμένη διαχείριση.

1.9.9 IPsec και IPv6

Το IPsec είναι ένα κρυπτογραφικό πρωτόκολλο σχεδιασμένο από το Internet Engineering Task Force για να την παροχή πέρα για πέρα εμπιστευτικότητας για τα πακέτα που ταξιδεύουν μέσα στο Internet. Το IPsec δουλεύει με το IPv4, την έκδοση του IP standard που χρησιμοποιείται σήμερα στο Internet. Το IPv6, είναι η "επόμενη γενιά" IP, περιλαμβάνει το IPsec.

Το IPsec δεν προσφέρεται για την ακεραιότητα, την αναγνώριση ταυτότητας, ή την απαγόρευση απάρνησης, αλλά αφήνει αυτά τα χαρακτηριστικά για τα άλλα πρωτόκολλα. Πρόσφατα, η κύρια χρήση του IPsec φαίνεται να είναι ένα πρωτόκολλο για την δημιουργία εικονικών προσωπικών δικτύων (Virtual Private Networks -VPNs) μέσω του Internet. Αλλά το IPsec έχει την ικανότητα να παρέχει αναγνώριση ταυτότητας, ακεραιότητα, και προαιρετικά την εμπιστοσύνη των δεδομένων για όλες τις επικοινωνίες που παίρνουν μέρος πάνω στο Internet, έχοντας ευρέως διαδεδομένες εφαρμογές του πρωτοκόλλου και επίσης την άδεια χρήση αυτών από τις κυβερνήσεις.

1.9.10 Kerberos

Ο Kerberos είναι ένα σύστημα ασφάλειας δικτύου που αναπτύχθηκε από το MIT και χρησιμοποιήθηκε από την αρχή στις Ηνωμένες Πολιτείες. Αντίθετα με τα άλλα συστήματα που αναφέρθηκαν στο κεφάλαιο αυτό, ο Kerberos δεν χρησιμοποιεί τεχνολογία δημόσιου κλειδιού. Αντί αυτού, ο Kerberos είναι βασισμένος σε συμμετρικά κρυπτογραφήματα που μοιράζονται μεταξύ του Kerberos server και κάθε ξεχωριστού χρήστη. Κάθε χρήστης έχει το δικό του password, και ο Kerberos server χρησιμοποιεί αυτό το password για να κρυπτογραφήσει μηνύματα που στέλνονται σε αυτόν τον χρήστη έτσι ώστε να μην μπορούν να διαβαστούν από κανέναν άλλο.

Υποστήριξη με τον Kerbero πρέπει να προστίθεται σε κάθε πρόγραμμα που χρειάζεται προστασία. Συνήθως, "Kerberized" εκδόσεις προγραμμάτων όπως το Telnet, FTP, POP, και Sun RPC χρησιμοποιούνται σήμερα. Ένα σύστημα που χρησιμοποιούσε τον Kerbero για να αποδώσει εμπιστευτικότητα στο HTTP πρωτόκολλο αναπτύχθηκε αλλά ποτέ δεν βγήκε από το εργαστήριο.

Ο Kerberos είναι ένα δύσκολο σύστημα στο να διαμορφωθεί και να διαχειριστεί. Για να λειτουργήσει ένα τέτοιο σύστημα θα πρέπει η κάθε μεριά να έχει ένα Kerberos server που θα είναι φυσικά ασφαλές. Ο Kerberos server διατηρεί ένα αντίγραφο των password κάθε χρήστη. Σε περίπτωση που ο Kerberos server εκτίθεται, κάθε password χρήστη πρέπει να αλλάζεται.

1.9.11 SSH (Secure Shell)

Το SSH είναι το ασφαλές κέλυφος (Secure Shell). Παρέχει κρυπτογραφικά προστατευμένα εικονικά τερματικά (Telnet) και λειτουργίες μεταφοράς αρχείων (rcp). Μη εμπορικές εκδόσεις του SSH είναι διαθέσιμες από πολλές εκδόσεις UNIX συστημάτων.

1.10 SSL (Secure Socket Layer)

Το SSL (Secure Socket Layer), είναι ένα γενικού σκοπού πρωτόκολλο για την αποστολή κρυπτογραφημένης πληροφορίας μέσω του Internet. Αναπτύχθηκε από την Netscape και έγινε προσιτό από το πλατύ κοινό από τον web browser και server της Netscape. Η ιδέα ήταν να μιμηθούν τις πωλήσεις μιας εταιρίας με κρυπτογραφικά ενεργοποιημένους web servers διανέμοντας έναν free client ο οποίος εφάρμοζε τα ίδια κρυπτογραφικά πρωτόκολλα.

Από τότε το SSL έχει ενσωματωθεί μέσα σε πολλούς άλλους web servers και browsers, έτσι ώστε η υποστήριξη του SSL να μην είναι ένα ανταγωνιστικό πλεονέκτημα αλλά μια. αναγκαιότητα. Το SSL χρησιμοποιείται και για no-web εφαρμογές όπως είναι το secure Telnet. Το SSL είναι τώρα ένα από τα ποιο δημοφιλές πρωτόκολλα κρυπτογράφησης στο Internet.

Το Internet Engineering Task Force (IETF) είναι τώρα στην διαδικασία της δημιουργίας ενός Transport Layer Security (TLS) πρωτοκόλλου. Αυτό το πρωτόκολλο είναι βασισμένο στο SSL 3.0, με μικρές αλλαγές στις επιλογές αλγόριθμων.

1.10.1 Τι είναι το **SSL**

Το SSL είναι ένα επίπεδο (layer) που υπάρχει ανάμεσα στη σειρά του TCP/IP πρωτοκόλλου και στο επίπεδο εφαρμογής. Ενώ το κανονικό TCP/IP πρωτόκολλο απλά στέλνει ένα ανώνυμο free-error ρεύμα πληροφοριών ανάμεσα στους δύο υπολογιστές, το SSL προσθέτει πολυάριθμες λειτουργίες σε αυτό το ρεύμα, περιλαμβάνοντας :

- Απόδειξης γνησιότητας και απαγόρευση απάρνησης του server, χρησιμοποιώντας ψηφιακές υπογραφές
- Απόδειξης γνησιότητας και απαγόρευση απάρνησης του client, χρησιμοποιώντας ψηφιακές υπογραφές
- Εμπιστοσύνη δεδομένων μέσω της χρήσης της κρυπτογραφίας
- Ακεραιότητα δεδομένων μέσω της χρήσης κωδικών απόδειξης γνησιότητας μηνυμάτων

Η κρυπτογραφία είναι ένας γρήγορα αναπτυσσόμενος τομέας, και τα κρυπτογραφικά πρωτόκολλα δεν δουλεύουν αν τα δυο μέρη της επικοινωνίας δεν χρησιμοποιούν τους ίδιους αλγόριθμους. Για το λόγο αυτό το SSL είναι επεκτάσιμο και ένα πρωτόκολλο που μπορεί να προσαρμοστεί εύκολα. Όταν ένα πρόγραμμα που χρησιμοποιεί SSL προσπαθεί να επικοινωνήσει με ένα άλλο, τότε τα δύο προγράμματα ηλεκτρονικά συγκρίνουν στοιχεία και καθορίζουν ποιος είναι ο δυνατότερος κρυπτογραφικός αλγόριθμος που διαθέτουν από κοινού. Αυτή η συναλλαγή ονομάζεται *SSL Hello.*

Το SSL σχεδιάστηκε για χρήση σε παγκόσμιο επίπεδο, αλλά αναπτύχθηκε στις Ηνωμένες Πολιτείες και συμπεριλαμβάνεται μέσα στα προγράμματα που πωλούνται από εταιρίες των Ηνωμένων Πολιτειών για χρήση στο εξωτερικό. Για το λόγο αυτό, το SSL περιέχει πολλές λειτουργίες σχεδιασμένες έτσι ώστε να μπορεί να συμμορφώνεται με τις κυβερνητικές περιοριστικές πολιτικές σε θέματα εξαγωγής κρυπτογραφικών συστημάτων των Ηνωμένων Πολιτειών.

1.10.2 Εκδόσεις του **SSL**

Το SSL πρωτόκολλο σχεδιάστηκε από την Netscape για χρήση με τον Netscape Navigator. Η έκδοση 1.0 του πρωτοκόλλου χρησιμοποιήθηκε μέσα στο Netscape. Η έκδοση 2.0 συμπεριλήφθηκε με το Netscape Navigator 1 και 2. Αφού το SSL 2.0 δημοσιεύτηκε, η Microsoft δημιούργησε ένα παρόμοιο secure link πρωτόκολλο, ονομαζόμενο PCT, το οποίο ξεπέρασε μερικές αδυναμίες του SSL 2.0. Τα πλεονεκτήματα του PCT ενσωματώθηκαν στο SSL 3.0. Το SSL 3.0 πρωτόκολλο χρησιμοποιήθηκε σαν την βάση για το Transport Layer Security (TLS) πρωτόκολλο που αναπτύχθηκε από την IETF.

1.10.3 Χαρακτηριστικά

Το SSL 3.0 προσφέρει πολλά χαρακτηριστικά θεωρητικού αλλά και πρακτικού ενδιαφέροντος:

1.10.3.1 **Διαχωρισμός των καθηκόντων**

Το SSL χρησιμοποιεί ξεχωριστούς αλγόριθμους για την κρυπτογράφηση, την απόδειξη γνησιότητας και την ακεραιότητα των δεδομένων με διαφορετικά κλειδιά (που ονομάζονται "μυστικά", secrets) για κάθε λειτουργία. Το βασικό πλεονέκτημα αυτού του διαχωρισμού των καθηκόντων είναι ότι τα μεγαλύτερα κλειδιά μπορούν να χρησιμοποιηθούν για την απόδειξη γνησιότητας και για την ακεραιότητα των δεδομένων, ενώ τα μικρότερα κλειδιά να χρησιμοποιούνται για την μυστικότητα. Αυτό είναι χρήσιμο για τα προϊόντα που σχεδιάζονται με σκοπό την εξαγωγή τους από τις Ηνωμένες Πολιτείες, επειδή ομοσπονδιακές ρυθμίσεις τοποθετούν περιορισμούς στο θέμα του μήκους των κλειδιών που χρησιμοποιούνται για την εμπιστευτικότητα ενώ δεν χρησιμοποιούνται περιορισμοί για την περίπτωση της ακεραιότητας των δεδομένων και της απόδειξης γνησιότητας.

Το SSLv3 παρέχεται για τις συνδέσεις που δεν κρυπτογραφούνται αλλά αποδεικνύεται η γνησιότητα τους και προστατεύονται εναντίον προμελετημένων αλλοιώσεων από κάποιον επιτηδευμένο attacker. Αυτό ίσως είναι χρήσιμο σε περίπτωση που η κρυπτογράφηση είναι απαγορευμένη από το νόμο, όπως είναι στην Γαλλία.

Η επιλογή των αλγόριθμων και του μήκους των κλειδιών καθορίζεται από τον SSL server, αλλά περιορίζεται και από τις δυο μεριές τον server και τον client.

1.10.3.2 **Αποτελεσματικότητα**

Η κρυπτογράφηση και αποκρυπτογράφηση δημόσιου κλειδιού είναι μια χρονοβόρα διαδικασία. Πόσο μάλλον όταν επαναλαμβάνεται αυτή η επεξεργασία για κάθε επικοινωνία ανάμεσα στον client και σε έναν server. Οι SSL εφαρμογές μπορούν να αποθηκεύουν κρυφά (cache) ένα μυστικό "master secret" που διατηρείται αναλλοίωτο μεταξύ των SSL συνδέσεων. Αυτό επιτρέπει στις καινούργιες SSL συνδέσεις να ξεκινήσουν αμέσως την ασφαλή επικοινωνία, χωρίς να χρειάζεται να εκτελεστούν περισσότερες λειτουργίες δημόσιου κλειδιού.

1.10.3.3 **Πιστοποιητικό βασισμένο στην απόδειξη γνησιότητας**

Το SSL παρέχετε για την απόδειξη γνησιότητας και των δύο, του client και του server, μέσω της χρήσης των ψηφιακών πιστοποιητικών και των ψηφιακά υπογεγραμμένων προκλήσεων αναγνώρισης.

Το SSLv3 χρησιμοποιεί τα X.509 v3 πιστοποιητικά, μολονότι η IETF τυποποίηση του SSL (πιθανώς ονομάζεται TLS) ίσως χρησιμοποιεί διαφορετικά είδη πιστοποιητικών καθώς είναι τυποποιημένα. Η απόδειξη γνησιότητας είναι ένα προαιρετικό μέρος του πρωτοκόλλου, μολονότι τα πιστοποιητικά του server είναι αποτελεσματικά εξουσιοδοτημένα από τις σημερινές SSL εφαρμογές.

1.10.3.4 **Αγνωστικό πρωτόκολλο (Protocol Agnostic*)***

Αν και το SSL σχεδιάστηκε για να τρέχει στην κορυφή του TCP/IP, αυτό στην πραγματικότητα μπορεί να τρέξει στην κορυφή κάθε αξιόπιστου connection-oriented πρωτοκόλλου, όπως είναι το X.25 ή το OSI. Το SSL πρωτόκολλο *δεν μπορεί* να "τρέξει" στην κορυφή ενός μη αξιόπιστου πρωτοκόλλου όπως είναι το IP User Datagram Protocol (UDP).

Όλη η SSL επικοινωνία παίρνει μέρος πάνω σε ένα απλό διπλής κατεύθυνσης ρεύμα.

1.10.3.5 **Προστασία ενάντια στις man-in-the-middle και replay επιθέσεις.**

Το SSL πρωτόκολλο είναι ειδικά σχεδιασμένο για να προστατεύει ενάντια στις man-in-the-middle και replay επιθέσεις. Σε μια man-in-the-middle επίθεση, ο επιτιθέμενος παρεμβάλλεται και υποκλέπτει όλες τις επικοινωνίες ανάμεσα στα δύο μέρη, κάνοντας τον καθένα να νομίζει ότι αυτός επικοινωνεί με τον άλλον.

Το SSL δίνει προστασία ενάντια στην man-in-the-middle επίθεση κάνοντας χρήση ψηφιακών πιστοποιητικών για να επιτρέψει στον web χρήστη να μάθει το επικυρωμένο (validated) όνομα του web site. Δυστυχώς, ο Netscape Navigator κρύβει αυτή την πληροφορία, κάνοντας την προσιτή μόνο στους χρήστες που επιλέγουν την "View Document Info" εντολή. Ένα καλύτερο περιβάλλον χρήστη θα εμφάνιζε τα επικυρωμένα ονόματα των web sites στην "title bar" του web browser, ή σε κάποιο άλλο εμφανή σημείο.

ΣΗΜΕΙΩΣΗ

Το SSL δεν προστατεύει ενάντια στην man-in-the-middle επίθεση όταν χρησιμοποιείται σε "encrypt-only" mode με κάθε SSLDHanon συνοδεία

κρυπτογράφησης. Αυτό συμβαίνει επειδή αυτό το mode δεν επιτρέπει ούτε στον server αλλά ούτε στον client να αποδείξουν την γνησιότητα τους ο ένας στον άλλον.
Σε μια replay επίθεση, ο επιτιθέμενος αντιγράφει (capture) τις επικοινωνίες ανάμεσα στα δύο μέρη και επαναλαμβάνει τα μηνύματα. Για παράδειγμα, ένας επιτιθέμενος ίσως αντιγράψει ένα μήνυμα ανάμεσα σε ένα χρήστη και ένα οικονομικό ίδρυμα (τράπεζα) έχοντας πληροφορηθεί ότι μια ηλεκτρονική πληρωμή ίσως να γίνει. Επαναλαμβάνοντας αυτό το μήνυμα, μπορεί να προκαλέσει πολλές άλλες ηλεκτρονικές πληρωμές.

1.10.3.6 **Υποστήριξη για συμπίεση**

Επειδή τα κρυπτογραφημένα δεδομένα δεν μπορούν να συμπιεστούν, το SSL εξασφαλίζει για το μέλλον την ικανότητα να συμπιέζει τα δεδομένα του χρήστη πριν αυτά κρυπτογραφηθούν. Το SSL υποστηρίζει πολλούς αλγόριθμους συμπίεσης. Ωστόσο δεν υπάρχει σήμερα κάποια SSL εφαρμογή που να ενσωματώνει την συμπίεση.

ΣΗΜΕΙΩΣΗ

Τα κρυπτογραφημένα δεδομένα δεν μπορούν να συμπιεστούν επειδή η καλή κρυπτογράφηση μετακινεί δραστικά κάθε επανάληψη ή ομοιότητα που είναι μετακινημένη κατά την διάρκεια της συμπίεσης. Εάν τα κρυπτογραφημένα δεδομένα μας μπορούν να συμπιεστούν, τότε η κρυπτογράφηση μας δεν είναι πολύ καλή.

1.10.3.7 **Συμβατότητα με το SSL 2.0**

Οι SSLv3.0 servers μπορούν να δέχονται συνδέσεις από SSLv2.0 clients και να χειρίζονται το μήνυμα αυτόματα χωρίς να υπάρχει ανάγκη να ξανασυνδεθεί ο client.

1.11 Ψηφιακά Πιστοποιητικά

Το SSL κάνει εκτεταμένη χρήση των πιστοποιητικών δημοσίου κλειδιού για την απόδειξη γνησιότητας τόσο του client όσο και του server στις SSL συναλλαγές. Το SSL κάνει χρήση των X.509 v3 πιστοποιητικών για τον έλεγχο των RSA ζεύγος κλειδιών, και ένα τροποποιημένο X.509 πιστοποιητικό για τον έλεγχο δημόσιων κλειδιών που χρησιμοποιούνται από το U.S. Department of Defense Forteza/DMS πρωτόκολλο ανταλλαγής κλειδιών
Το SSL υποστηρίζει τα παρακάτω είδη πιστοποιητικών:

- RSA πιστοποιητικά δημόσιου κλειδιού με δημόσια κλειδιά αυθαίρετου μήκους
- RSA πιστοποιητικά δημόσιου κλειδιού που περιορίζονται στα 512 bits, για χρήση στα κρυπτογραφικά λογισμικά που πρόκειται να εξαχθούν.
- RSA πιστοποιητικά μόνο για υπογραφή, τα οποία περιέχουν RSA δημόσια κλειδιά που χρησιμοποιούνται μόνο για την υπογραφή δεδομένων, και όχι για κρυπτογράφηση.
- DSS πιστοποιητικά
- Diffie-Hellman πιστοποιητικά

Η χρήση των πιστοποιητικών είναι προαιρετική. Το SSL απαιτεί πιστοποιητικά server εκτός αν οι SSL εφαρμογές και του client και του server

χρησιμοποιούν το Diffie-Hellman πρωτόκολλο ανταλλαγής κλειδιών. Σήμερα, τα προϊόντα της Netscape δεν εφαρμόζουν τους αλγόριθμους του Diffie-Hellman.

1.12 Επίδοση εκτέλεσης

Το SSL εμφανώς μειώνει την ταχύτητα μετάδοσης της πληροφορίας μέσω του Internet. Η επίδοση της επιβράδυνσης είναι κυρίως αποτέλεσμα της κρυπτογράφησης και αποκρυπτογράφησης δημόσιου κλειδιού που απαιτείται για να αρχικοποιηθεί η πρώτη SSL σύνδεση. Σε σύγκριση με αυτό, οι επιπλέον κρυπτογραφήσεις και αποκρυπτογραφήσεις δεδομένων με τους RC2, RC4, ή τον DES είναι πρακτικά ασήμαντες.

Χρήστες του SSL αναφέρουν ότι η επιβράδυνση φτάνει το +50%, συγκρινόμενη με την αποστολή πληροφορίας χωρίς την χρήση SSL. Χρήστες με SPARC Station 10s έχουν αναφέρει ότι η κρυπτογράφηση και αποκρυπτογράφηση δημόσιου κλειδιού απαιτεί περίπου τρία CPU δευτερόλεπτα ανά χρήστη με ένα κλειδί 124-bit κλειδί.

Αυτό σημαίνει ότι θα υπάρχει μια παύση τριών δευτερολέπτων ανάμεσα στο άνοιγμα μιας σύνδεσης σε έναν SSL server και στην απόκτηση μιας HTML σελίδας από τον server. Επειδή το SSL μπορεί να αποθηκεύει κρυφά (cache) ένα μυστικό "master secret", αυτή η καθυστέρηση επιδρά μόνο στην πρώτη SSL συναλλαγή μεταξύ του client και του server.

Εάν έχουμε έναν γρήγορο υπολογιστή και μια σχετικά αργή σύνδεση στο δίκτυο -ποίος δεν έχει?- το επιπλέον του SSL μπορεί να είναι ασήμαντο, εδικά εάν στέλνουμε μεγάλες ποσότητες πληροφοριών πάνω από μια απλή SSL σύνοδο ή πάνω από πολλαπλές SSL συνόδους που χρησιμοποιούν ένα κοινό "master secret".

Από την άλλη πλευρά, εάν απαιτούμε να "σερβίρουμε" μεγάλο μέγεθος SSL HTTP αιτήσεων μέσα σε ένα λεπτό, πρέπει να αποφασίσουμε είτε στην αγορά ενός εξαιρετικά γρήγορου υπολογιστή είτε στην hardware βοήθεια για τις δημόσιου κλειδιού λειτουργίες. Για να μειώσουν την επίδραση του SSL, πολλοί οργανισμοί μεταδίδουν των όγκο των πληροφοριών τους "καθαρά", και χρησιμοποιούν το SSL μόνο για κρυπτογράφηση ευαίσθητων δεδομένων. Δυστυχώς αυτό αφήνει τον χρήστη ανοιχτό σε μια επίθεση, επειδή τα μη-κρυπτογραφημένα HTML αρχεία μπορούν να τροποποιηθούν κατά την μετάδοση, καθώς αυτά στέλνονται από τον client στον server, με ένα εξεζητημένο πρόγραμμα φιλτράρισμα πακέτων και εισαγωγής νέων στοιχείων (injection).

Για παράδειγμα, θα μπορούσε να αλλαχθεί το action tag σε μια HTML form, έτσι ώστε αντί να τοποθετείται ο αριθμός της πιστωτικής κάρτας στο κατάλληλο σύστημα επεξεργασίας, αυτός να τοποθετείται σε έναν πειρατικό υπολογιστή στην Νότια Αμερική. Αν υποθέσουμε ότι ο χειριστής του πειρατικού συστήματος μπορεί να πάρει ένα ψηφιακά υπογεγραμμένο ID (signed digital ID) από τον δικό του SSL server, τότε ίσως είναι πολύ δύσκολο για έναν χρήστη που εξαπατήθηκε με αυτό το τέχνασμα να ανακαλύψει ότι ήταν θύμα μιας επίθεσης.

1.13 Ψηφιακές Υπογραφές για Αναγνώριση Ταυτότητας

Πολλά από τα συστήματα αναγνώρισης ταυτότητας που αναφέρθηκαν παραπάνω μπορούν να βελτιωθούν με την χρήση των ψηφιακών υπογραφών.

Με λίγα λόγια, κάθε χρήστης ενός συστήματος που χρησιμοποιεί ψηφιακές υπογραφές δημιουργεί ένα ζεύγος κλειδιών:

Ένα προσωπικό κλειδί

Χρησιμοποιείται για να υπογράψει κάποιος με την υπογραφή του ένα κομμάτι δεδομένων, όπως είναι ένα Html κείμενο, ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ή μια φωτογραφία.

Ένα δημόσιο κλειδί

Χρησιμοποιείται για την επικύρωση της ψηφιακής υπογραφής αφού αυτή έχει υπογραφεί.

Εάν του Α το δημόσιο κλειδί είναι ευρέως διαδεδομένο σε ένα tamper-proof format, τότε θα μπορούσε να χρησιμοποιήσει το προσωπικό του κλειδί για να αποδείξει ότι είναι στην πραγματικότητα ο Α (εξασφαλίζοντας βέβαια, ότι θα έχει προσέξει να προστατεύσει το κλειδί του από πιθανή κλοπή). Το πλεονέκτημα της χρήσης κρυπτογραφίας δημόσιου κλειδιού είναι ότι η δοκιμασία αυτή μπορεί γίνει με ασφάλεια πάνω από ένα τηλέφωνο, ή ένα δίκτυο υπολογιστών ακόμα και εάν κάποιο τρίτο πρόσωπο κρυφακούει.

Για να δούμε πώς ο Α μπορεί να χρησιμοποιήσει το προσωπικό του κλειδί για να αποδείξει την ταυτότητα του, ας φανταστούμε ότι ο Α και ο Β ανταλλάσσουν μηνύματα μέσω ηλεκτρονικού ταχυδρομείου. Αυτό που έχει να κάνει ο Β, για να αναγνωρίσει ότι η ταυτότητα του μηνύματος είναι του Α, είναι να στείλει ένα σύντομο γράμμα στον Α που θα περιέχει έναν τυχαίο αριθμό, ζητώντας του να υπογράψει ψηφιακά τον αριθμό αυτόν και να τον στείλει πάλι πίσω σε αυτόν. Όταν ο Β πάρει πίσω το γράμμα, αυτός επικυρώνει την ψηφιακή υπογραφή χρησιμοποιώντας το αντίγραφο του δημόσιου κλειδιού του Α. Εάν ο Α ήταν προσεκτικός με τα κλειδιά του, ο Β λογικά μπορεί να συμπεράνει ότι το πρόσωπο με το οποίο επικοινωνεί είναι ο Α. Χρησιμοποιώντας την ψηφιακή υπογραφή για να αποδείξεις ποιος είσαι.

Αυτή η τεχνική καταλαβαίνουμε όχι δεν μπορεί να εκτεθεί ακόμα και αν κάποιος τρίτος (όπως ο Γ) κρυφακούει ή παραποιεί χα μηνύματα. Ακόμα και αν ο Γ παρατηρεί όλα τα μηνύματα που στέλνονται μεταξύ του Α και του Β, δεν θα δει ποτέ το προσωπικό κλειδί του Α και δεν θα είναι ικανός να πλαστογραφήσει την ψηφιακή υπογραφή του Α. Ο Γ μπορεί, ωστόσο, λόγο του Β να κάνει δύσπιστο τον Α. Αυτό μπορεί να το κάνει μεταβάλλοντας το μήνυμα καθώς αυτό ταξιδεύει από τον Β στον Α. Ο Α δεν θα υπογράψει το σωστό μήνυμα, και ο Β θα αναρωτιέται γιατί ο Α δεν κάνει όχι του ζήτησε. Άλλος τρόπος είναι, ο Γ μπορεί να μεταποιήσει το υπογεγραμμένο μήνυμα. αυτό ίσως κάνει το Β να σκεφτεί όχι κάποιος προσπάθησε να προσποιηθεί όχι είναι ο Α (κάποιος που δεν είχε το σωστό κλειδί).

Έχουν αναπτυχθεί πολλοί τρόποι για να προστατεύουμε τα προσωπικά κλειδιά :

- **Κρυπτογράφηση και αποθήκευση του κλειδιού στον σκληρό δίσκο.**

Ο απλούστερος τρόπος να προστατεύσουμε ένα προσωπικό κλειδί είναι να το κρυπτογραφήσουμε χρησιμοποιώντας μια μυστική φράση (passphrase). Με αυτόν τον τρόπο τα προγράμματα όπως το PGP και ο Netscape Navigator

προστατεύουν τα προσωπικά κλειδιά. Αυτή η τεχνική είναι προσωρινή λύση. Το μειονέκτημα είναι όχι αν κάποιος έχει πρόσβαση στον υπολογιστή σου και ξέρει την μυστική φράση, τότε μπορεί να έχει και το προσωπικό κλειδί σου.

Επίσης το κλειδί πρέπει να αποκρυπτογραφείται από τον υπολογιστή και αντιγράφεται στην μνήμη του για να μπορεί να χρησιμοποιηθεί, είναι ευπρόσβλητη η επίθεση μέσα στην μνήμη του υπολογιστή με ένα κακοποιό πρόγραμμα ή ένα "δούρειο ίππο" (Trojan horse).

- **Κρυπτογράφηση και αποθήκευση του κλειδιού σε ένα μεταφερόμενο μέσο.**

Ένα λίγο ποιο ασφαλής τρόπος να αποθηκεύσουμε το προσωπικό κλειδί μας είναι να το αποθηκεύσουμε κρυπτογραφημένο σε ένα μαλακό δίσκο, η σε ένα CD-ROM, ή άλλο μεταφερόμενο μέσο. Με αυτή την τεχνική ο επιτιθέμενος χρειάζεται και την μυστική φράση αλλά και το αποθηκευμένο κρυπτογράφημα για να αποκτήσει το προσωπικό μας κλειδί. Δυστυχώς, όταν χρησιμοποιούμε το προσωπικό μας κλειδί, ο υπολογιστής αποκρυπτογραφεί το κλειδί και τοποθετεί ένα αντίγραφο στην μνήμη του. Αυτό αφήνει πάλι το κλειδί ευπρόσβλητο σε μια επίθεση από κάποιον ιό ή άλλο κακοποιό πρόγραμμα.

- **Αποθήκευση του κλειδιού σε μια "Smart Card" ή άλλη έξυπνη συσκευή**

Αυτή είναι ένας από τους περισσότερο ασφαλής τρόπους να προστατεύσουμε το προσωπικό μας κλειδί. Η έξυπνη κάρτα έχει έναν μικροεπεξεργαστή και στην πραγματικότητα δημιουργεί το δημόσιο /προσωπικό ζεύγος κλειδιών. Η έξυπνη κάρτα μπορεί να μεταφέρει το δημόσιο κλειδί στον "host" υπολογιστή και έχει έναν περιορισμένο αριθμό αποθηκευτικού χώρου για να κρατά 10 ή 20 πιστοποιητικά δημόσιου κλειδιού. Θεωρητικά, το προσωπικό κλειδί δεν απομακρύνεται από την κάρτα. Έτσι οι επιτιθέμενοι δεν μπορούν να χρησιμοποιήσουν το προσωπικό κλειδί μας, εκτός αν έχουν στην κατοχή τους την κάρτα μας. Και, αντίθετα από την περίπτωση αποθήκευσης του κλειδιού σε μια δισκέτα, ένα κακοποιό πρόγραμμα που ίσως τρέξει στον υπολογιστή μας δεν θα μπορέσει να μας κλέψει ένα αντίγραφο του προσωπικού μας κλειδιού επειδή αυτό δεν τοποθετείται ποτέ στην μνήμη του υπολογιστή μας.

Οι έξυπνες κάρτες είναι συναρπαστικά κομμάτια της τεχνολογίας σε θέματα ασφάλειας. Παίρνεις την κάρτα σου έξω από τον υπολογιστή σου, και ξέρεις ότι κανένας άλλος δεν μπορεί να έχει πρόσβαση στο προσωπικό σου κλειδί. Οι έξυπνες κάρτες επίσης μπορούν να προγραμματιστούν να ζητούν έναν PIN ή μια passphrase πριν εκτελέσουν την κρυπτογραφική διαδικασία. Αυτό βοηθά στην προστασία του κλειδιού σε περίπτωση που κλαπεί η έξυπνη κάρτα.

Επίσης μπορούν να προγραμματιστούν έτσι ώστε εάν γίνουν πολλές προσπάθειες εισαγωγής PIN's, το κλειδί αυτόματα να διαγράφεται. Έξυπνες κάρτες μπορούν να φτιαχτούν ώστε να χρησιμοποιούν και βιομετρήσεις επίσης. Για παράδειγμα, μπορεί να κατασκευαστεί ένας αναγνώστης δακτυλικών αποτυπωμάτων ή ένα μικρό μικρόφωνο μέσα σε μια κάρτα.

Οι έξυπνες κάρτες έχουν και μειονεκτήματα. Μερικές από αυτές είναι εξαιρετικά λεπτεπίλεπτες και εύθραυστες, έτσι ώστε με την συχνή χρήση τους αχρηστεύονται. Αν μια κάρτα χαθεί, κλαπεί ή καταστραφεί τα κλειδιά που περιέχει χάνονται και δεν είναι ποια διαθέσιμα στον χρήστη. Έτσι είναι απαραίτητο να υπάρχει ένα σύστημα αναπαραγωγής καρτών και ένα σύστημα ακύρωσης του κλειδιού σε περίπτωση απώλειας. Αυτό είναι ιδιαίτερα σημαντικό

για κλειδιά που χρησιμοποιούνται για να κρυπτογραφούν αποθηκευμένα δεδομένα.

- **Veritas : Ψηφιακές υπογραφές για φυσικά πιστοποιητικά ιδιότητας**

Ένας ενδιαφέρον τρόπος χρήσης της τεχνολογίας δημόσιου κλειδιού για την απόδειξη ταυτότητας είναι το σύστημα Veritas των Pitney-Bowes, το οποίο χρησιμοποιεί τις ψηφιακές υπογραφές για να αποδεικνύει την γνησιότητα φωτογραφιών και άλλων πληροφοριών που είναι αποθηκευμένα σε φυσικά έγγραφα (όπως είναι η άδεια οδήγησης αυτοκινήτου). Αυτό το σύστημα αποθηκεύει ένα *bar code,* δυο διαστάσεων και υψηλής πυκνότητας, στο πίσω μέρος μιας πλαστικής κάρτας. Αυτό το bar code περιέχει μια ωηφιοποιημένη φωτογραφία, ένα αντίγραφο της υπογραφής του οδηγού, και πληροφορίες όπως το όνομα, την ηλικία και την διεύθυνση του οδηγού. Όλες οι πληροφορίες που αποθηκεύονται στο bar code είναι υπογεγραμμένες με μια ψηφιακή υπογραφή. Το προσωπικό κλειδί που χρησιμοποιείται για να δημιουργηθεί αυτή η ψηφιακή υπογραφή ανήκει στην αρχή που εκδίδει την κάρτα.

Για να επικυρώσουμε την ψηφιακή υπογραφή που είναι αποθηκευμένη στο πίσω μέρος της κάρτας, είναι απαραίτητο να έχουμε τον κατάλληλο αναγνώστη "Veritas reader". Αυτός ο αναγνώστης σαρώνει και τις δύο διαστάσεις του bar code της κάρτας, επικυρώνει την ψηφιακή υπογραφή, και μετά εμφανίζει ένα αντίγραφο της φωτογραφίας σε μια μικρή οθόνη. Ένα μαγαζί που πουλά οινοπνευματώδη ποτά ίσως μπορούσε να χρησιμοποιεί αυτό το σύστημα για να επιβεβαιώνει την ηλικία των ανθρώπων που προσπαθούν να αγοράσουν αλκοόλ, καθώς και για να επικυρώνει τα ονόματα των ανθρώπων που υπογράφουν λογαριασμούς (checks).

Το Veritas δοκιμάστηκε για πρώτη φορά το 1994 για την παροχή IDs σε 800 φοιτητές του πανεπιστημίου New Haven. Επίσης το 1995 δοκιμάστηκε στους ειδικούς Ολυμπιακούς Αγώνες στο Connecticut. Περίπου 7.000 πιστοποιητικά ιδιότητας αθλητών εκδόθηκαν για την χρήση τους στους αγώνες. Αυτά τα πιστοποιητικά ιδιότητας περιείχαν μια φωτογραφία του αθλητή, βιογραφικά δεδομένα και ιατρικές πληροφορίες. Οι Pitney-Bowes ανέφεραν ένα 100% ρυθμό ανάγνωσης στις κάρτες, πράγμα που είχε σαν συνέπεια να "πέσει" το δίκτυο.

1.14 Public Key Infrastructure (PKI)

Όλα τα συστήματα αναγνώρισης ταυτότητας που αναφέρθηκαν προηγουμένως έχουν ένα κοινό μειονέκτημα : Επιτρέπουν στους ανθρώπους να δημιουργούν προσωπικές-ιδιωτικές σχέσεις ανάμεσα στους εαυτούς τους και ενός συγκεκριμένου υπολογιστικού συστήματος, αλλά δεν επιτρέπουν αυτές οι σχέσεις να σχηματίζονται στο πλαίσιο μιας μεγαλύτερης κοινωνίας. Είναι όλα προσωπικά συστήματα αναγνώρισης ταυτότητας, δεν είναι δημόσια, κοινής ωφέλειας.

Για παράδειγμα, ας υποθέσουμε ότι Α γίνεται μέλος με μια πανεθνική online service και δημιουργεί έναν email λογαριασμό. Όταν δημιουργεί τον λογαριασμό, παίρνει ένα username και ένα password. Όταν ο Α επιθυμεί να δει το email του, χρησιμοποιεί το password για να αποδείξει την ταυτότητα του. Αυτός ακόμα, ίσως δημιουργήσει ένα προσωπικό κλειδί για να αποδείξει την ταυτότητα του, και δώσει ένα αντίγραφο του δημόσιου κλειδιού του στην online service.

Τώρα ας φανταστούμε ότι ο Α χάνει το password του σε αυτή την περίπτωση χρειάζεται να υπογραφεί ψηφιακά το δημόσιο κλειδί του. Τότε ο Νίκος μπορεί να υπογράψει όλα τα μηνύματα του με το προσωπικό του κλειδί. Όποιος τώρα επιθυμεί να επιβεβαιώσει ότι τα μηνύματα του Νίκου στην πραγματικότητα του ανήκουν, θα πρέπει να πάρει ένα αντίγραφο του ψηφιακά υπογεγραμμένου δημόσιου κλειδιού του Νίκου και να επικυρώσει την υπογραφή του που βρίσκεται εκεί.

Πράγματι, αυτός είναι ο ακριβής τρόπος που μια υποδομή δημόσιου κλειδιού δουλεύει.

1.14.1 Αρχές Πιστοποίησης (Certification Authorities)

Μια αρχή πιστοποίησης (CA) είναι ένας οργανισμός που εκδίδει πιστοποιητικά δημόσιου κλειδιού. Αυτά τα πιστοποιητικά μοιάζουν με κάρτες κρυπτογραφικά υπογεγραμμένου περιεχομένου. Τα πιστοποιητικά, υπογράφονται από τα προσωπικά κλειδιά που ανήκουν στην αρχή πιστοποίησης, και περιέχουν το όνομα του προσώπου, το δημόσιο κλειδί αυτού του προσώπου, έναν serial number, και άλλες πληροφορίες. Το πιστοποιητικό επιβεβαιώνει ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε έναν συγκεκριμένο άτομο ή οργανισμό.

Υπάρχουν πολλοί διαφορετικοί τρόποι με τους οποίους μια αρχή πιστοποίησης μπορεί να προσφέρει υπηρεσίες:

Εσωτερική αρχή (Internal CA)

Ένας οργανισμός μπορεί να λειτουργεί μια CA για να πιστοποιεί στους εργαζομένους του, τις θέσεις τους, και το επίπεδο της εξουσίας τους. Μια τέτοια ιεραρχία πιστοποίησης μπορεί να χρησιμοποιηθεί για τον έλεγχο πρόσβασης στις εσωτερικές πηγές πληροφοριών του οργανισμού. Για παράδειγμα, κάθε εργαζόμενος σε έναν οργανισμό μπορεί να δημιουργήσει ένα κλειδί και να αποκτήσει ένα πιστοποιητικό, για αυτό το κλειδί, που να αναφέρεται μόνο στα υπολογιστικά συστήματα στα οποία θα έχει πρόσβαση ο εργαζόμενος. Οι υπολογιστές του οργανισμού μπορούν τότε να
αποφασίζουν εάν θα παρέχουν ή όχι σε έναν εργαζόμενο πρόσβαση, βασιζόμενοι στην πιστοποίηση του κλειδιού τους. Με αυτόν τον τρόπο, οι επιχειρήσεις αποφεύγουν την αναγκαιότητα τις διανομής μιας λίστας ελέγχου πρόσβασης και τις ύπαρξης αρχείου password σε όλους τους κατανεμημένους υπολογιστές

Εξωτερικής προέλευσης υπαλλήλου αρχή (Outsourced employee CA)

Μια εταιρία ίσως συμφωνήσει με μια εξωτερική φίρμα να παρέχει υπηρεσίες πιστοποίησης για τους δικούς της εργαζόμενους, όπως μια εταιρία ίσως συμφωνήσει με ένα εργαστήριο φωτογραφίας για να κατασκευάσει ταυτότητες.

Εξωτερικής προέλευσης πελάτη αρχή (Outsourced customer CA)

Μια εταιρία ίσως συμφωνήσει με μια εξωτερική φίρμα να διευθύνει μια αρχή πιστοποίησης η οποία να λειτουργήσει για τους τρέχων ή για τους πιθανούς πελάτες της εταιρίας. Βασιζόμενη στις μεθόδους πιστοποίησης της εξωτερικής φίρμας, η εταιρία θα γλιτώσει την δαπάνη της δημιουργίας δικών τις διαδικασιών πιστοποίησης.

Έμπιστου τρίτου προσώπου αρχή (Trusted third-party CA)

Μια εταιρία ή μια κυβέρνηση μπορεί να λειτουργεί μια CA η οποία να συνδέει τα δημόσια κλειδιά με τα νόμιμα ονόματα ανθρώπων ή επιχειρήσεων. Μια τέτοια CA μπορεί να χρησιμοποιηθεί για να επιτρέπει σε άτομα χωρίς καμία

προηγούμενη σχέση να αποδεικνύουν ο ένας στον άλλον την ταυτότητα του και να μετέχουν σε νόμιμες συναλλαγές

Για να χρησιμοποιήσουμε τα πιστοποιητικά που έχει εκδώσει μια CA, πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού της CA. Πρόσφατα, τα δημόσια κλειδιά διανέμονται συσσωρευμένα μαζί με τα διάφορα πακέτα προγραμμάτων, όπως είναι οι web browsers και τα λειτουργικά συστήματα. Άλλα δημόσια κλειδιά CAs μπορούν να προστεθούν χειροκίνητα από τον κάθε χρήστη.

1.14.2 Ακύρωση πιστοποιητικών

Εκτός από την έκδοση πιστοποιητικών, οι CAs χρειάζονται έναν τρόπο για την ακύρωση αυτών, για τις παρακάτω περιπτώσεις:

- Αν ο κρίκος των προσωπικών κλειδιών εκτεθεί σε τρίτους.
- Αν η CA ανακαλύψει ότι έκδωσε το πιστοποιητικό σε λάθος πρόσωπο ή ύπαρξη.
- Αν το πιστοποιητικό έχει εκδοθεί για να παρέχει πρόσβαση σε μια συγκεκριμένη υπηρεσία, και το άτομο αυτό έχει χάσει την εξουσιοδότηση για την υπηρεσία αυτή.
- Αν εκτεθούν τα συστήματα της CA κατά τέτοιο τρόπο που κάποιος να έχει την δυνατότητα να εκδώσει πλαστογραφημένα πιστοποιητικά.

Ένας τρόπος που είχε προταθεί για τον έλεγχο τον ακυρώσεων είναι η λίστα ακυρωμένων πιστοποιητικών (Certificate Revocation List, CRL). Μια CRL είναι μια λίστα που περιέχει κάθε πιστοποιητικό που έχει ακυρωθεί από την CA, το οποίο δεν έχει ακόμα λήξη για άλλους λόγους. Θεωρητικά, μια CA εκδίδει μια τέτοια λίστα CRL σε τακτά χρονικά διαστήματα. Εκτός των ακυρωμένων πιστοποιητικών μια τέτοια λίστα CRL καθορίζει το πόσο καιρό αυτή θα ισχύει και το που θα πάρουμε την επόμενη CRL.

Οι CRLs είναι ενδιαφέρουσες στην θεωρία : επιτρέπουν στους υπολογιστές που δεν είναι συνδεδεμένοι σε ένα δίκτυο να καθορίζουν εάν τα πιστοποιητικά ισχύουν ή έχουν ακυρωθεί. Στην πραγματικότητα όμως, οι CRL έχουν πολλά προβλήματα:

- Έχουν την τάση να μεγαλώνουν με πολύ γρήγορο ρυθμό.
- Υπάρχει μια περίοδος ανάμεσα στον χρόνο όπου ένα πιστοποιητικό ακυρώνεται και στον χρόνο που οι νέα CRL διανέμεται, οπότε ένα πιστοποιητικό φαίνεται να ισχύει ενώ δεν ισχύει στην πραγματικότητα.
- Η πληροφορία που περιέχεται μέσα στις λίστες αυτές μπορεί να χρησιμοποιηθεί για παράνομες αναλύσεις.

Πολλές CAs, αντί για τις CRLs, ίσως θα χρησιμοποιήσουν επικύρωση πραγματικού χρόνου (real-time) κάνοντας χρήση online συστημάτων διαχείρισης βάσεων δεδομένων συνδεδεμένα σε δίκτυο, όπως είναι το Internet. Αυτά τα συστήματα με επιδέξιο τρόπο αφήνουν κατά μέρος τα προβλήματα των CRLs, αν και απαιτούν ένα δίκτυο που να είναι αξιόπιστο και διαθέσιμο.

Μια εναλλακτική πρόταση, από τον Carl Ellison της CyberCash, είναι απλά να χρησιμοποιούμε πιστοποιητικά με πολύ μικρή ημερομηνία λήξης - ένα ή δύο λεπτά. Σαν συνέπεια, αυτό απαιτεί από τον χρήστη του πιστοποιητικού να επικοινωνεί με την CA πριν από κάθε συναλλαγή. Σε μερικές περιπτώσεις, αυτό μπορεί να είναι περισσότερο αποτελεσματικό απ' ότι να έχεις τον παραλήπτη του πιστοποιητικού να επικυρώνει αυτό με την CA.

Certification Practices statement (CPS)

Το CPS είναι ένα νομικό κείμενο που δημοσιεύει η κάθε CA, που περιγράφει τις πολιτικές και τις διαδικασίες που εφαρμόζει για την έκδοση και την ακύρωση ψηφιακών πιστοποιητικών. Αυτό το κείμενο απαντά στην ερώτηση, "Τι σημαίνει όταν αυτός ο οργανισμός υπογράφει ένα κλειδί;"

1.14.3 Το X.509 v3 Πιστοποιητικό

Το X.509 v3 πιστοποιητικό είναι ένα δημοφιλές πρότυπο για τα πιστοποιητικά δημόσιου κλειδιού. Τα X.509 v3 πιστοποιητικά είναι ευρέως χρησιμοποιημένα από πολλά μοντέρνα κρυπτογραφικά πρωτόκολλα, περιλαμβάνοντας και χο SSL. Τα X.509 πιστοποιητικά δεν χρησιμοποιήθηκαν από το πρόγραμμα PGP κρυπτογράφησης email στις εκδόσεις 2.0 έως 4.5, αλλά είναι πιθανό στο μέλλον να υποστηρίζει το X.509 v3 πιστοποιητικό.

Το κάθε X.509 πιστοποιητικό περιλαμβάνει έναν αριθμό έκδοσης, έναν σειριακό αριθμό, πληροφορίες ταυτότητας, πληροφορίες σχετικές με τον αλγόριθμο και την υπογραφή της αρχής που το εκδίδει. Στην παρακάτω Εικόνα βλέπουμε την δομή ενός τυπικού X.509 πιστοποιητικού.

Version_____
Serial Number_____
Algorithm Identifier_____
Issuer_____
Period of Validity:
- Not Before Date
- Not After Date_____
Subject_____
Subject's Public Key
- Algorithm
- Parameters
- Public Key_____
Signature_____

Η παραγωγή έχει αποδεχτεί τα X.509 v3 πιστοποιητικά, περισσότερο από τα αρχικά X.509 πιστοποιητικά, γιατί το X.509 v3 πρότυπο επιτρέπει αυθαίρετο αριθμό ζευγαριών name/value στο πρότυπο πιστοποιητικό. Αυτά τα ζευγάρια μπορούν να χρησιμοποιηθούν για πολλούς σκοπούς

1.15 Αρχές Πιστοποίησης και Πιστοποιητικά Server

Οι αρχές πιστοποίησης για συντομία έχει καθιερωθεί να αναφέρονται σαν CA (Certification Authorities).

1.15.1 Τα Πιστοποιητικά Σήμερα

Τα ψηφιακά πιστοποιητικά προσφέρουν στους ανθρώπους, στους οργανισμούς και στις επιχειρήσεις του Internet απλούς τρόπους για να πιστοποιεί ο ένας του άλλου την ταυτότητα.

Για τους καταναλωτές, μερικά πλεονεκτήματα των πιστοποιητικών είναι:

• Ένας απλός τρόπος να πιστοποιήσουμε την γνησιότητα ενός οργανισμού πριν να δώσουμε στον οργανισμό αυτό εμπιστευτικές πληροφορίες.

- Η γνώση ότι μπορούμε να αποκτήσουμε την φυσική διεύθυνση του οργανισμού και το νομικά κατοχυρωμένο όνομα του, έτσι ώστε να μπορούμε να διώξουμε ποινικά, στην χειρότερη περίπτωση, ενάντια της εταιρίας.

Για τις επιχειρήσεις χα πλεονεκτήματα είναι:

- Ένας απλός τρόπος να πιστοποιήσουν την ηλεκτρονική διεύθυνση ταχυδρομείου ενός ατόμου χωρίς να πρέπει να του στείλουν κανένα email. Αυτό μειώνει τον χρόνο συναλλαγής, μειώνοντας και το κόστος. Επίσης μπορούν να εμποδίσουν την κατάχρηση του ηλεκτρονικού ταχυδρομείου. Για παράδειγμα εάν μια εταιρία επιτρέπει την εγγραφή σε mailing lists μόνο σε άτομα που διαθέτουν ψηφιακό ID, ένας κακόβουλος χρήστης δεν θα μπορεί να εγγράψει πολλούς ανθρώπους σε αυτή την mailing list χωρίς την άδεια της.
- Ένας απλός ευρέως χρησιμοποιούμενος τρόπος για την πιστοποίηση της ταυτότητας ενός ατόμου χωρίς την χρήση usernames και passwords, τα οποία ξεχνιούνται εύκολα και μοιράζονται μεταξύ των χρηστών.
- Αντί να προσπαθούν να ρυθμίζουν λίστες χρηστών και passwords, οι επιχειρήσεις μπορούν απλά να εκδίδουν πιστοποιητικά στους εργαζόμενους και στους συνέταιρους τους. Μετά χρειάζονται μόνο χα προγράμματα που παραχωρούν την πρόσβαση στις υπηρεσίες, με την επικύρωση της υπογραφής του πιστοποιητικού.
- Σήμερα, πολλές υπηρεσίες συνδρομητών στο Internet ζητούν ένα σταθερό μηνιαίο εισόδημα από τους συνδρομητές τους, αναγνωρίζοντας την ταυτότητα τους με ένα username και ένα password. Δυστυχώς, συνεργαζόμενοι χρήστες μπορούν να καταστρέψουν την υπηρεσία αυτή απλά με το να μοιράζονται ένα κοινό username και password μεταξύ τους. Υπηρεσίες που βασίζονται στην αναγνώριση ταυτότητας με την χρήση των πιστοποιητικών έχουν λιγότερες πιθανότητες να πέσουν θύματα τέτοιας κατάχρησης, επειδή είναι περισσότερο δύσκολο να για τους συνεργαζόμενους χρήστες να μοιράζονται κλειδιά και πιστοποιητικά από ότι να μοιράζονται usernames και passwords. Πολύ περισσότερο, εάν ένα μυστικό κλειδί χρησιμοποιείται για πολλούς σκοπούς τότε οι χρήστες είναι απίθανο να συνεργαστούν. Για παράδειγμα αν ένα κλειδί χρησιμοποιείται για πρόσβαση στο web αλλά και για πρόσβαση στον λογαριασμό τράπεζας.

Πάντα πρέπει να θυμόμαστε το γεγονός ότι αυτοί που μπορούν να αποδείξουν την ταυτότητα τους χρησιμοποιώντας πιστοποιητικά, δεν είναι και πάντα αυτοί που υποστηρίζουν ότι είναι. Αυτό φανερώνει μόνο ότι έχουν στην κατοχή τους ένα μυστικό κλειδί υπογεγραμμένο από μια κατάλληλη αρχή πιστοποίησης.

Ο Michael Baum από την Verisign λεει ότι τα ψηφιακά πιστοποιητικά παρέχουν "αποδεικτικά στοιχεία" (probative evidence) - στοιχεία που είναι χρήσιμα στο να καθορίζουν την ταυτότητα η οποία μπορεί να χρησιμοποιηθεί στο δικαστήριο. Όμως αυτό απαιτεί, από τον χρήστη να μην χάσει τον "έλεγχο" του μυστικού κλειδιού του, ότι η CA ακολούθησε τις απαιτούμενες σωστές διαδικασίες για την έκδοση του συγκεκριμένου τύπου πιστοποιητικού και να μην εκτεθεί η CA στο μέλλον.

Παρ' όλα αυτά, τα ψηφιακά πιστοποιητικά είναι σημαντικά περισσότερο ασφαλής τρόπος εξακρίβωσης της ταυτότητας των ανθρώπων στο Internet, από ότι της εναλλακτικής λύσης των usernames και των passwords.

1.15.2 Διαφορετικά Είδη Πιστοποιητικών

Υπάρχουν τέσσερεις διαφορετικοί τύποι ψηφιακών πιστοποιητικών σε χρήση στο Internet σήμερα :

Πιστοποιητικά Αρχών Πιστοποίησης (Certification authority certificates)

Αυτά τα πιστοποιητικά περιλαμβάνουν το δημόσιο κλειδί της αρχής πιστοποίησης και είτε το όνομα της CA είτε το όνομα της συγκεκριμένης υπηρεσίας που πιστοποιεί. Αυτά μπορούν να υπογραφτούν από μόνα τους ή αλλιώς να υπογραφτούν από άλλη CA. Αυτά συνηθίζεται να πιστοποιούν άλλα είδη πιστοποιητικών.

Πιστοποιητικά Server (Server certificates)

Αυτά τα πιστοποιητικά περιλαμβάνουν το δημόσιο κλειδί ενός SSL Server, το όνομα του οργανισμού που "τρέχει" τον Server, το όνομα της Internet διεύθυνσης του, και το δημόσιο κλειδί του server.

Προσωπικά πιστοποιητικά (Personal certificates)

Αυτά τα πιστοποιητικά περιλαμβάνουν το όνομα ενός ατόμου και το δημόσιο κλειδί αυτού του προσώπου. Επίσης μπορούν να έχουν και άλλες πληροφορίες, όπως την ηλεκτρονική διεύθυνση του ατόμου, την ταχυδρομική διεύθυνση του, ή οτιδήποτε άλλο.

Πιστοποιητικά εκδοτών λογισμικού (Software Publisher certificates)

Αυτά τα πιστοποιητικά χρησιμοποιούνται για να υπογράφουν προγράμματα που πρόκειται να διανεμηθούν.

1.15.3 Πιστοποιητικά Αρχών Πιστοποίησης

Ένα πιστοποιητικό μιας αρχής πιστοποίησης είναι ένα πιστοποιητικό που περιλαμβάνει το όνομα και το δημόσιο κλειδί της αρχής πιστοποίησης. Αυτά τα πιστοποιητικά μπορούν να υπογραφτούν από μόνα τους (self-signed). Αυτό σημαίνει ότι η αρχή πιστοποίησης μας λεει ότι το κλειδί της είναι καλό, και εμείς πρέπει να το εμπιστευτούμε. Αλλιώς, αυτά μπορούν να υπογραφτούν από μια άλλη αρχή. Επίσης οι αρχές μπορούν να διασταυρώνουν η μια με την άλλη την πιστότητα των κλειδιών τους ή ακόμα και να υπογράφει η μια της άλλης τα κλειδιά.

Τα πιστοποιητικά αυτά διανέμονται με την προοπτική να τα εμπιστευτούμε όπως είναι, αυτό φαίνεται από το γεγονός ότι ενσωματώνονται απευθείας στους web browsers.

1.15.4 Πιστοποιητικά Server

Κάθε SSL server πρέπει να έχει ένα SSL πιστοποιητικό server. Όταν ένας browser συνδέεται σε ένα web server χρησιμοποιώντας το SSL πρωτόκολλο, ο server στέλνει στον browser το δημόσιο κλειδί του σε ένα X.509 v3 πιστοποιητικό. Το πιστοποιητικό χρησιμοποιείται για να αποδείξει την ταυτότητα του server και για να διανέμει το δημόσιο κλειδί του server, το οποίο χρησιμοποιείται για να κρυπτογραφήσει την αρχική πληροφορία που στέλνεται στον server από τον client.

1.15.4.1 Απόκτηση Πιστοποιητικού για έναν Server

Για να αποκτήσουμε ένα πιστοποιητικό για τον server μας, χρειαζόμαστε να ακολουθήσουμε τα παρακάτω βήματα :

1. Δημιουργία ενός RSA δημόσιου /προσωπικού ζεύγους κλειδιών χρησιμοποιώντας ένα πρόγραμμα που θα το προμηθευτούμε από τον πωλητή του server.
2. Αποστολή του δημόσιου κλειδιού, το διακεκριμένο και το κοινό όνομα στην αρχή πιστοποίησης που επιθυμούμε να χρησιμοποιήσουμε. Η αποστολή συνήθως γίνεται με την χρήση email.
3. Θα πρέπει να ακολουθήσουμε την διαδικασία πιστοποίησης της CA . Συμπλήρωση διαφόρων στοιχείων στο web site της CA, αποστολή εγγράφων με email-fax ή και με ταχυδρομείο. Επίσης μπορεί να χρειαστεί να πληρώσουμε και την CA.
4. Αναμονή για την επεξεργασία της αίτησης από την CA.
5. Όταν η CA πειστεί ότι η αίτηση πληρεί τις προϋποθέσεις, θα εκδώσει ένα πιστοποιητικό αποτελούμενο από το δημόσιο κλειδί μας, το διακεκριμένο όνομα μας, άλλες πληροφορίες, και την ψηφιακή υπογραφή του. Η αποστολή συνήθως γίνεται με την χρήση email.
6. Εγκατάσταση του κλειδιού χρησιμοποιώντας ένα πρόγραμμα που θα το προμηθευτούμε από τον πωλητή του server

Βέβαια όπως όλα τα έγγραφα απόδειξης ταυτότητας, έτσι και τα X.509 v3 πιστοποιητικά λήγουν και χρειάζονται τότε την κατάλληλη ανανέωση πιστοποιητικού που εκτελείται από τις CAs. Η ημερομηνία λήξης κυμαίνεται στους 3-12 μήνες για λόγους ασφάλειας.

1.15.4.2 Βλέποντας ένα Πιστοποιητικό ενός Site

Μπορούμε να δούμε τα πιστοποιητικά των διαφόρων sites επιλέγοντας την "Document info".

1.15.5 Ψηφιακά Πιστοποιητικά από την Μεριά του Χρήστη

Προηγουμένως αναφερθήκαμε σε ψηφιακά πιστοποιητικά για οργανισμούς. Τωρα θα δούμε πως τα ψηφιακά πιστοποιητικά μπορούν να πιστοποιήσουν την ταυτότητα ενός ατόμου.

1.15.5.1 Client Πιστοποιητικά

Ένα client πιστοποιητικό είναι ένα ψηφιακό πιστοποιητικό το οποίο είναι σχεδιασμένο για να πιστοποιεί την ταυτότητα ενός ατόμου. Όπως και με τα πιστοποιητικά των Web sites, τα client πιστοποιητικά συνδέουν ένα συγκεκριμένο όνομα με ένα συγκεκριμένο μυστικό κλειδί. Αυτά εκδίδονται από τις αρχές πιστοποίησης (CAs).

Τα client πιστοποιητικά έχουν πολλές χρήσεις και οφέλη:

- Τα ψηφιακά πιστοποιητικά μπορούν να απομακρύνουν την ανάγκη της απομνημόνευσης των usernames και των passwords. Απλά υπογράφουμε με την ψηφιακή υπογραφή μας οποτεδήποτε εισβάλουμε σε περιορισμένο χώρο.
- Αντί να αναπτύσσουν μια μεγάλη διασκορπισμένη βάση δεδομένων, οι οργανισμοί μπορούν απλά να χρησιμοποιήσουν ένα ψηφιακό πιστοποιητικό εκδομένο από μια ειδική CA σαν απόδειξη ιδιότητας μέλους στον οργανισμό αυτό.
- Είναι δυσκολότερο για μια ομάδα ατόμων να μοιραστούν ένα μονό ψηφιακό ID από ότι είναι να μοιραστούν ένα ζεύγος username-password. Αυτό συμβαίνει επειδή η υπογραφεί του ονόματος μας με ένα ψηφιακό πιστοποιητικό απαιτεί πρόσβαση σε ένα μυστικό κλειδί. Αυτό είναι επειδή υπάρχουν τεχνικά εμπόδια στο να μπορούν να μοιράζονται κοινά μυστικά κλειδιά οι χρήστες μεταξύ τους, και επειδή ίσως οι χρήστες να είναι απρόθυμοι να μοιράζονται ένα μυστικό κλειδί που είναι χρήσιμο για περισσότερες από μια εφαρμογές.
- Επειδή τα ψηφιακά πιστοποιητικά περιέχουν ένα δημόσιο κλειδί (που ανήκει στον ιδιοκτήτη του πιστοποιητικού), εμείς μπορούμε να χρησιμοποιήσουμε κάποιου το ψηφιακό πιστοποιητικό για να του στείλουμε κρυπτογραφημένο email.
- Τα πιστοποιητικά που δείχνουν την ηλικία ενός προσώπου μπορούν να χρησιμοποιηθούν για περιορισμούς σε πονηρού περιεχομένου δεδομένα ή και chat groups.
- Τα πιστοποιητικά που δείχνουν το φύλο ενός προσώπου μπορούν να χρησιμοποιηθούν για την ελεύθερη πρόσβαση σε χώρους μόνο για άνδρες ή μόνο για γυναίκες.

Δημιουργώντας ισχυρά συστήματα αναγνώρισης της ταυτότητας των χρηστών, τα πιστοποιητικά βοηθούν για την εξαφάνιση της ανωνυμίας. Επίσης είναι περισσότερο αποτελεσματικά και από τα «cookies». Ένα cookie απλώς αφήνει ένα ίχνος, που έχει να κάνει με τα σημεία από τα οποία εμείς περάσαμε στην επίσκεψη μας σε ένα web site. Ένα ψηφιακό πιστοποιητικό από την άλλη μεριά, αφήνει πίσω το όνομα μας, την ηλεκτρονική μας διεύθυνση, ή και άλλες πληροφορίες αναγνώρισης ταυτότητας οι οποίες έχουν την δυνατότητα να ξαναγυρίσουν σε εμάς και να μα δώσουν πληροφορίες για την ταυτότητα του site που επισκεφτήκαμε.

Επειδή τα πιστοποιητικά ελαχιστοποιούν την ανωνυμία, μερικό χρήστες του Internet είναι αντίθετοι στη χρήση τους, βασιζόμενοι στο ότι αυτά εκθέτουν την μυστικότητα του χρήστη. Αυτό κάνουν, αυτός είναι και ο σκοπός που δημιουργήθηκαν τους άλλωστε. Όπως σήμερα κατασκευάζονται, ωστόσο, τα πιστοποιητικά δεν στέλνονται ποτέ από έναν web browser χωρίς την γνώση και την άδεια του χρήστη. Επίσης, τα πιστοποιητικά δεν περιέχουν πληροφορίες που είναι άγνωστες στον χρήστη. Φυσικά, και οι δύο αυτές περιπτώσεις μπορούν να αλλάξουν στο μέλλον.

Στο μέλλον, οι χρήστες του Internet μπορεί να αλλάξουν γνώμη για τα πιστοποιητικά. Είναι αλήθεια ότι ένα σημαντικό στοιχείο ενός ολοκληρωμένου συστήματος διακυβέρνησης είναι η έκδοση καρτών απόδειξης ταυτότητας, και η ύπαρξη μεγάλων προστίμων όταν ο πολίτης δεν είναι σε θέση να αποδείξει την ταυτότητα του όταν του ζητηθεί. Αυτές οι κάρτες απόδειξης ταυτότητας, επίσης βοηθούν στη εδραίωση μιας δυνατής κοινωνίας με ανθρώπους υπεύθυνους των πράξεων τους. Με την όλο και ποιο συχνή χρήση των πιστοποιητικών στο Internet, θα αναπτυχθεί και το ασφαλής εμπόριο.

1.15.5.2 Υποστήριξη για τα Client-side ψηφιακά πιστοποιητικά

Τα client-side ψηφιακά πιστοποιητικά υποστηρίζονται από τον Internet Explorer, και τον Netscape Navigator, και άλλες εφαρμογές βασισμένες στο SSL. Η υποστήριξη αποτελείται από τέσσερα συστατικά κλειδιού:

Δημιουργία κλειδιού

Η εφαρμογή (browser) περιέχει κώδικα για την δημιουργία δημόσιου /προσωπικού ζεύγους κλειδιών, στέλνοντας το μυστικό κλειδί σε μία CA μέσα στην φόρμα μιας HTTP POST συναλλαγής.

Απόκτηση πιστοποιητικού

Η εφαρμογή (browser) μπορεί να δεχτεί ένα πιστοποιητικό από μια CA μέσω HTTP.

Κλήση / Ανταπόκριση

Η εφαρμογή μπορεί να κάνει χρήση ενός αποθηκευμένου μυστικού κλειδιού για την υπογραφεί τυχαίων κλήσεων ενός SSL server.

Ασφαλής αποθήκευση

Ο browser παρέχει ένα μέρος για την ασφαλή αποθήκευση του μυστικού κλειδιού. Οι εκδόσεις του Internet Explorer, και του Netscape Navigator επιτρέπουν στο κλειδί να αποθηκεύεται κρυπτογραφημένο. Σε μελλοντικές εκδώσεις οι εφαρμογές θα επιτρέπουν στα κλειδιά να αποθηκεύονται σε floppy disks ή σε smart cards.

2

ΕΔΕΤ & Αρχές Πιστοποίησης

2.1 Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ)

Το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας ΕΔΕΤ / GRNET παρέχει στην Ελληνική Ακαδημαϊκή, Ερευνητική και εκπαιδευτική κοινότητα προηγμένες υπηρεσίες εθνικής διασύνδεσης Ίντερνετ υψηλής χωρητικότητας εξυπηρετώντας όλα τα ΑΕΙ, ΤΕΙ, τα Ερευνητικά Κέντρα της χώρας και πάνω από 9500 σχολεία μέσω του Πανελλήνιου Σχολικού Δικτύου. Εξυπηρετεί συνολικά πάνω από 200.000 χρήστες οι οποίοι είναι ερευνητές, φοιτητές και ερευνητικό προσωπικό ΑΕΙ / ΤΕΙ, χρήστες ακαδημαϊκών και ερευνητικών ηλεκτρονικών βιβλιοθηκών, εκπαιδευτικοί και μαθητές της Πρωτοβάθμιας και Δευτεροβάθμιας Εκπαίδευσης.
Επίσης το ΕΔΕΤ:

- Διαχειρίζεται τον κόμβο Athens Internet Exchange (AIX), ο οποίος παρέχει τοπική διασύνδεση μεταξύ των μεγαλυτέρων εταιρειών παροχής υπηρεσιών Ιντερνετ στην Ελλάδα.
- Παρέχει διεθνή διασύνδεση με τα υπόλοιπα ερευνητικά δίκτυα και το Ίντερνετ μέσω του πανευρωπαϊκού ερευνητικού δικτύου GEANT.
- Διαχειρίζεται / συμμετέχει σε μια σειρά αναπτυξιακών έργων, όπως το e-Business Forum και η Εκπαιδευτική Στήριξη του προγράμματος Δικτυωθείτε, τα οποία έχουν σκοπό την προώθηση των τεχνολογιών του Ίντερνετ και των εφαρμογών τους στις ελληνικές επιχειρήσεις και τη διαμόρφωση και ανταλλαγή ιδεών και προτάσεων για το ηλεκτρονικό επιχειρείν, με έμφαση στις Μικρομεσαίες Επιχειρήσεις (ΜΜΕ).

Η Εταιρεία ΕΔΕΤ (Εθνικό Δίκτυο Έρευνας και Τεχνολογίας Α.Ε.) έχει την ευθύνη της διαχείρισης του Εθνικού Δικτύου Έρευνας & Τεχνολογίας. Το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας παρέχει, από το 1995, υπηρεσίες δικτύου κορμού στην Ελληνική Ακαδημαϊκή & Ερευνητική Κοινότητα (έργο της Γενικής Γραμματείας Έρευνας & Τεχνολογίας του Υπουργείου Ανάπτυξης).

Η εταιρεία ΕΔΕΤ Α.Ε. δημιουργήθηκε το 1998 κατά το πρότυπο των αντίστοιχων εταιρειών διαχείρισης των Εθνικών Ερευνητικών Δικτύων (National Research Networks) των χωρών της Ευρωπαϊκής Ένωσης. Συγκεντρώνοντας στις τάξεις της επιστήμονες με σημαντική τεχνογνωσία, η ΕΔΕΤ αποτελεί δυναμικό παράγοντα ανάπτυξης, αξιοποίησης και διάχυσης τεχνογνωσίας και τεχνολογικής εξέλιξης στην Ελλαδα.

2.1.1 Υπηρεσίες ΕΔΕΤ

2.1.1.1 Βασικές υπηρεσίες

- Υπηρεσία Helpdesk

Η υπηρεσία αρωγής χρηστών (Helpdesk) δέχεται, καταγράφει και δρομολογεί προς επίλυση προβλήματα των συνδέσεων του δικτύου κορμού του ΕΔΕΤ, των συνδέσεων των φορέων στους κόμβους του ΕΔΕΤ καθώς επίσης και των προσφερόμενων υπηρεσιών του ΕΔΕΤ προς τους φορείς.

- Σύνδεση νέου φορέα()

Η υπηρεσία περιλαμβάνει την διαδικασία που πρέπει να ακολουθηθεί, με τη συνεργασία 7 διαφορετικών ΔΟ(Διαχειριστικές Ομάδες), για τη σύνδεση ενός νέου φορέα στο δίκτυο του ΕΔΕΤ.

- Δρομολόγηση με το πρωτόκολλο IP (IPv4 & IPv6)

Η υπηρεσία αυτή δίνει την δυνατότητα σε φορείς από την Ελλάδα αλλά και από ολόκληρο τον κόσμο να επικοινωνήσουν μέσω του Διαδικτύου, χρησιμοποιώντας είτε την τρέχουσα έκδοση 4 του Internet Protocol ή τη νεότερη εξέλιξή του, την έκδοση 6. Το ΕΔΕΤ διαθέτει για το σκοπό αυτό δρομολογητές σε καίρια σημεία της Ελλάδας, που εξυπηρετούν τις αντίστοιχες γεωγραφικές περιοχές στις οποίες ανήκουν. Οι συγκεκριμένοι δρομολογητές φροντίζουν για τη δυναμική δρομολόγηση κίνησης IPv4 και IPv6 μέσω της χρήσης σύγχρονων πρωτοκόλλων δρομολόγησης BGP, OSPF και IS-IS.

- Χρονισμός Δικτυακών Συσκευών (NTP)

Στόχος της υπηρεσίας είναι να παρέχει ένα ή περισσότερα σημεία αναφοράς για ώρα υψηλής ακριβείας. Η περιορισμένη ακρίβεια των ρολογιών των δικτυακών συσκευών επιβάλει τον συγχρονισμό τους σε τακτά χρονικά διαστήματα με κάποια ώρα αναφοράς υψηλής ακρίβειας.

- Υπηρεσία hostmaster

Από τον Ιούλιο του 1995, το ΕΔΕΤ έχει αναλάβει από το RIPE τον ρόλο του Τοπικού Καταχωρητή Internet (Local Internet Registry - LIR). Η υπηρεσία Hostmaster έχει σαν σκοπό την διαχείριση του χώρου των IPv4 και IPv6 διευθύνσεων που έχουν δεσμευθεί για το ΕΔΕΤ (GR.GRNET LIR) από το RIPE, καθώς και την διάθεσή διευθύνσεων αυτών στους φορείς-πελάτες του ΕΔΕΤ κατόπιν σχετικής αιτήσεως.

- Υπηρεσία DNS

Η υπηρεσία Διευθυνσιοδότησης Υπολογιστών έχει σκοπό την αντιστοίχηση των ονομάτων των υπολογιστών στις Internet Protocol (IP) διευθύνσεις τους (ευθεία αντιστοίχηση) και το αντίστροφο, δηλαδή IP διευθύνσεις σε ονόματα (αντίστροφη αντιστοίχηση).

- Υπηρεσία NEWS

Η υπηρεσία άρθρων έχει σκοπό την παροχή δυνατότητας ανταλλαγής μηνυμάτων σε όλα τα μέλη που ανήκουν σε κάποιο ίδρυμα το οποίο συνεργάζεται με το ΕΔΕΤ. Με βάση την υπηρεσία NEWS, οι χρήστες μπορούν να ανταλλάσσουν μηνύματα ως συμμετάσχοντες σε ομάδες συζητήσεων (newsgroups).

- Υπηρεσίες Καταλόγου

Οι Υπηρεσίες Καταλόγου του ΕΔΕΤ παρέχουν έναν κεντρικό εξυπηρετητή καταλόγου για αιτήματα αναζήτησης στοιχείων χρηστών των ελληνικών ακαδημαϊκών και ερευνητικών ιδρυμάτων.

- Υπηρεσίες Web (Υπηρεσίες Ανάπτυξης Ερευνητικών Δικτυακών Τόπων - Οργάνωση και Ανάπτυξη Μεθόδων Ανάκτησης Πληροφοριών και Ψηφιακού Υλικού).

Η υπηρεσία συνίσταται στην ανάπτυξη και λειτουργία "Θεσμικών Δικτυακών Πυλών" (Institutional Portals), και εργαλείων για συνεργατικές δραστηριότητες στο εσωτερικό Κατανεμημένων Κοινοτήτων, και στην υποστήριξη της οργάνωσης ad hoc Ομάδων Εργασίας και Πρωτοβουλιών διαμόρφωσης πολιτικής, μέσω ειδικών λειτουργικών Δικτυακών Τόπων.

- Υπηρεσία αντιμετώπισης περιστατικών ασφαλείας

Η ομάδα GRNET-CERT (Greek Research and Technology Network Computer Emergency Response Team) ανταποκρίνεται, καταγράφει, και παρακολουθεί περιστατικά που αφορούν την ασφάλεια των πληροφοριακών συστημάτων του ΕΔΕΤ και των φορέων του.

2.1.1.2 Πρόσθετες υπηρεσίες

- Έλεγχος πρόσβασης (access control)

Η υπηρεσία αυτή έχει σκοπό να προστατέψει κατά ένα ποσοστό το δίκτυο του ΕΔΕΤ από τις πολυπληθείς απειλές του διαδικτύου. Με την βοήθεια των security access lists προστατεύονται τόσο οι δικτυακές συσκευές του ΕΔΕΤ από κακόβουλες ενέργειες, όσο και οι φορείς-πελάτες του ΕΔΕΤ εφόσον το επιθυμούν.

- Παρουσίαση κίνησης, ποιότητας και διαθεσιμότητας δικτύου

Ο στόχος της υπηρεσίας είναι να παρουσιάσει συνοπτικά την κατάσταση του δικτύου αναφορικά με τον φορτίο και τα χαρακτηριστικά ποιότητας (τρέχον φορτίο,καθυστέρηση, διακύμανση καθυστέρησης, απώλεια πακέτων.

- Παρουσίαση κίνησης και διαθεσιμότητας δικτυακών υπηρεσιών

Ο στόχος της υπηρεσίας είναι να παρουσιάσει συνοπτικά την κατάσταση των υπηρεσιών του δικτύου αναφορικά με τον φορτίο και τα χαρακτηριστικά ποιότητας τους (τρέχον φορτίο, αριθμός κλήσεων, καθυστέρηση, διακύμανση καθυστέρησης).

- Υπηρεσία web proxy, content filtering και edge networking

Η υπηρεσία web proxying, content filtering και edge networking έχει ως σκοπό την παροχή υπηρεσιών proxy/caching και content filtering σε πελάτες του ΕΔΕΤ με αντίστοιχες ανάγκες και να εξετάσει τη δυνατότητα παροχής τεχνολογιών edge networking και content delivery στο σύνολο των πελατών του ΕΔΕΤ.

- Υπηρεσία mailing lists

Πρόκειται για τη διαχείριση των discussion lists που χρησιμοποιούνται για: την επικοινωνία των Διαχειριστικών Ομάδων του Virtual NOC που διαχειρίζεται το δίκτυο και τις παρεχόμενες από την ΕΔΕΤ ΑΕ υπηρεσίες στην επικοινωνία των συνδεδεμένων φορέων.

- Backup MX

Πρόκειται για την υπηρεσία σύμφωνα με την οποία, όταν ο εξυπηρετητής mail του ιδρύματος τεθεί εκτός λειτουργίας, τα μηνύματα mail που απευθύνονται προς τους χρήστες του ιδρύματος αποθηκεύονται προσωρινά στους εξυπηρετητές του ΕΔΕΤ, ώστε να αυξάνεται η αξιοπιστία και η ταχύτητα της τελικής παραλαβής των mails όταν ο εξυπηρετητής mail του ιδρύματος επανέλθει σε λειτουργία.

- Υπηρεσίες τηλεδιασκέψεων

Σε επίπεδο υποδομών, λειτουργεί σε συνεργασία με το GUNET ο εθνικός gatekeeper που προσφέρει στους φορείς του ΕΔΕΤ διασύνδεση υπηρεσιών τηλεφωνίας πάνω από δίκτυο δεδομένων (VoIP μέσω πρωτοκόλλου H.323) και κεντρική υπηρεσία τηλεδιασκέψεων μέσω MCU.

- Υπηρεσίες Δημόσιου Κλειδιού (PKI)

Περιλαμβάνει την διαχείριση Κεντρικής Αρχής Πιστοποίησης που εκδίδει ψηφιακά πιστοποιητικά, τόσο για Δευτερεύουσες Αρχές Πιστοποίησης, όσο και για τελικούς χρήστες και εξυπηρετητές. Τα εκδιδόμενα πιστοποιητικά χρησιμεύουν για την προστασία δεδομένων και για την ασφαλή ηλεκτρονική επικοινωνία. Η υποδομή PKI είναι εγγεγραμμένη στο αντίστοιχο ευρωπαϊκό μητρώο του TERENA (TACAR).

- Video Webcasting

Το ΕΔΕΤ έχει αναπτύξει υπηρεσίες Video Webcasting μέσω της τεχνολογίας Real. Ο RealServer που έχει εγκατασταθεί στον κεντρικό κόμβο του ΕΔΕΤ είναι διαθέσιμος στους φορείς του ΕΔΕΤ για ζωντανή μετάδοση εκδηλώσεων σε μεγάλο κοινό.

- IP Τηλεφωνία

Η υπηρεσία IP τηλεφωνίας δίνει στους φορείς του ΕΔΕΤ την δυνατότητα εκτέλεσης τηλεφωνικών κλήσεων μεταξύ τους αλλά και με τους φορείς του διεθνούς δικτύου Videnet.Η υπηρεσία παρέχεται σε συνεργασία και συντονισμό με το GUNET.

- Video On Demand

Το ΕΔΕΤ έχει αναπτύξει υπηρεσίες Video On Demand μέσω της τεχνολογίας Real. Ο RealServer που έχει εγκατασταθεί στον κεντρικό κόμβο του ΕΔΕΤ είναι διαθέσιμος στους φορείς του ΕΔΕΤ για την αποθήκευση του ψηφιοποιημένου video υλικού των φορέων. Η πρόσβαση στο υλικό αυτό είναι ελεύθερη σε όλους τους τελικούς χρήστες.

- Τεχνική υποστήριξη εκδηλώσεων

Η υπηρεσία αφορά την τεχνική υποστήριξη των εκδηλώσεων (συνέδρια, κλπ.). Τα αντικείμενα της τεχνικής υποστήριξης είναι οι εργασίες για την προσωρινή διασύνδεση των συνεδριακών και άλλων χώρων με το ΕΔΕΤ και η
προσωρινή εγκατάσταση και ρύθμιση κάθε είδους εξοπλισμού που ανήκει στο ΕΔΕΤ και χρησιμοποιείται για λόγους τεχνικής κάλυψης (ενδεικτικά, δρομολογητές, modem, εξοπλισμός τηλεδιασκέψεων, μεταγωγείς, σημεία ασύρματης πρόσβασης, κλπ.).

2.1.1.3 Προηγμένες υπηρεσίες

- Παροχής Ποιότητας (QoS)

Η υπηρεσία QoS έχει ως σκοπό να δημιουργήσει, συντηρήσει και να διαχειριστεί μηχανισμούς παροχής ποιότητας υπηρεσίας στον κορμό και στην περιφέρεια του δικτύου του ΕΔΕΤ. Η υπηρεσία βασίζεται στην αρχιτεκτονική DiffServ και στοχεύει να εξασφαλίσει εγγυήσεις στην απόδοση του δικτύου για συγκεκριμένες κλάσεις κίνησης. Οι εγγυήσεις ποιότητας που παρέχει έχουν να κάνουν με την παροχή απόλυτης προτεραιότητας (συνεπώς πολύ μικρής καθυστέρησης διάδοσης) και μηδενικής απώλειας πακέτων σε κλάσεις κίνησης που είναι συμβατές με προσυμφωνημένους (και αποδεκτούς)ρυθμούς μετάδοσης ώστε να μην παραβιάζεται η διαστασιολόγηση της υπηρεσίας.

- Διαχείρισης εύρους ζώνης (MBS)

Σκοπός της υπηρεσίας είναι να παρέχει στον κορμό και την περιφέρεια του δικτύου του ΕΔΕΤ νοητά κυκλώματα point-to-point, με εγγυημένο εύρος ζώνης. Η υπηρεσία υλοποιείται με την χρήση L2 MPLS VPNs τα οποία συνδυάζουν QoS και Traffic Engineering χαρακτηριστικά (mpls traffic engineering tunnels). Η παροχή εγγυήσεων για συγκεκριμένο εύρος ζώνης επιτυγχάνεται με χρήση μηχανισμών που ανήκουν στην αρχιτεκτονική DiffServ. Για την παροχή της υπηρεσίας έχει γίνει κατάλληλη διαστασιολόγηση του δικτύου (κοινή με την υπηρεσία QoS) και η αποδοχή των αιτημάτων χρήσης της υπηρεσίας βασίζεται σε αυτή. Η υπηρεσία MBS στην ουσία "συνενώνει" τις υπηρεσίες L2 MPLS VPNs και QoS και τις επεκτείνει εισάγοντας traffic engineering χαρακτηριστικά.

- L-2 και L-3 MPLS VPNs.

Στο ΕΔΕΤ η υπηρεσία των νοητών ιδιωτικών δικτύων επιπέδου 2 ή 3 παρέχεται μέσω της τεχνολογίας MPLS. Υπηρεσίες επιπέδου 2 ορίζονται μόνο μεταξύ δύο σημείων και εξομοιώνουν την σύνδεση των σημείων αυτών πάνω από το ίδιο φυσικό μέσο (π.χ., Ethernet). Υπηρεσίες επιπέδου 3 παρέχονται μεταξύ οποιονδήποτε δύο ή περισσοτέρων σημείων και εξομοιώνουν την σύνδεση των σημείων αυτών στο ίδιο IP broadcast domain.

2.1.2 Το μέλλον του ΕΔΕΤ

Στο αμέσως προσεχές μέλλον, η ΕΔΕΤ σκοπεύει να δραστηριοποιηθεί σε όλους τους σημαντικούς εκείνους χώρους που συνδέονται με την ανάπτυξη του Internet νέας γενιάς οπτικής τεχνολογίας υπερυψηλών ταχυτήτων (1-5 Gbps).
Μεταξύ άλλων, θα προσφέρει τη δυνατότητα παροχής σε Ερευνητικές Κοινοπραξίες, Εικονικών Δικτύων (VPN), υπηρεσιών Multicast και υπηρεσιών δικτύωσης IPv6. Συγκεκριμένα, το ΕΔΕΤ στοχεύει να υποστηρίξει την ανάπτυξη και διάχυση στους Ακαδημαϊκούς και Ερευνητικούς φορείς:

- Προηγμένων Υπηρεσιών Internet νέας γενιάς.
- Προηγμένων Εφαρμογών Ηλεκτρονικής Μάθησης από απόσταση.
- Διασύνδεση υπερ-υπολογιστικών συστημάτων και GRID.

Στόχος της ΕΔΕΤ είναι να παίξει πρωτοποριακό ρόλο στη διαμόρφωση των τάσεων και εξελίξεων στο χώρο των προηγμένων τηλεπικοινωνιακών δικτύων και υπηρεσιών σε Εθνικό και Παγκόσμιο επίπεδο. Εξίσου σημαντικός σκοπός του ΕΔΕΤ είναι να εξακολουθήσει να λειτουργεί ως προπομπός και μοχλός ανάπτυξης της Ελληνικής Κοινωνίας της Πληροφορίας ενθαρρύνοντας παράλληλα τις συνεργασίες ανάμεσα στην Ακαδημαϊκή - Ερευνητική Κοινότητα και τη Βιομηχανία καθώς και να προωθεί τη διάθεση των ευρυζωνικών δικτύων σε

ολοένα μεγαλύτερη κοινότητα χρηστών στη χώρα μας, στο πλαίσιο των Ευρωπαϊκών πρωτοβουλιών e-Europe2002 & e-Europe2005.

2.2 Υποδομή Δημόσιου Κλειδιού HARICA

Η Υποδομή Δημοσίου Κλειδιού "Hellenic Academic & Research Institutions Certification Authority - (HARICA)" είναι μία έμπιστη τρίτη οντότητα που πιστοποιεί την ταυτότητα χρηστών και δικτυακών εξυπηρετητών των Ακαδημαϊκών ιδρυμάτων και Ερευνητικών φορέων της Ελλάδας.

Η Υποδομή Δημοσίου Κλειδιού της HARICA είναι μια σύμπραξη ισότιμων μελών που απαρτίζεται από Ακαδημαϊκά Ιδρύματα, Ερευνητικούς φορείς και το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας - ΕΔΕΤ, και ξεκίνησε στα πλαίσια του έργου VNOC2 (έργο χρηματοδοτούμενο από το ΕΔΕΤ μέσω του Επιχειρησιακού προγράμματος "Κοινωνία της Πληροφορίας"). Οι υπηρεσίες της είναι διαθέσιμες στα μέλη των Ελληνικών Ακαδημαϊκών και Ερευνητικών φορέων.

Σκοπός της HARICA είναι η δημιουργία υποδομής για την ασφαλή επικοινωνία των μελών των Ακαδημαϊκών και Ερευνητικών φορέων της Ελλάδας.

Η Υποδομή Δημοσίου Κλειδιού της HARICA :

- Υλοποιεί μία Ιεραρχία Δημόσιου Κλειδιού με αρχή την Κεντρική Αρχή Πιστοποίησης της HARICA, μέσω της οποίας τα μέλη της μπορούν να αποκτήσουν ενδιάμεση Αρχή Πιστοποίησης, η οποία συνεργάζεται με τις αρχές πιστοποίησης άλλων φορέων στην Ελλάδα και στο εξωτερικό με στόχο την διεύρυνση του δικτύου εμπιστοσύνης
- Παρέχει δυνατότητα δια-πιστοποίησης με Κεντρικές Αρχές Πιστοποίησης μελών του
- Εκδίδει -για λογαριασμό των μελών του- ψηφιακά πιστοποιητικά για τους διακομιστές του δικτύου, έτσι ώστε να είναι ασφαλή τα δεδομένα που ανταλλάσουν με τους χρήστες του δικτύου.
- Εκδίδει -για λογαριασμό των μελών του- ψηφιακά πιστοποιητικά για τους χρήστες του δικτύου τα οποία μπορούν να χρησιμοποιήσουν για να αποδεικνύουν την ταυτότητά τους σε υπηρεσίες δικτύου και για ασφαλή επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου.

Η Υποδομή Δημοσίου Κλειδιού της HARICA εκδίδει πιστοποιητικά σε οντότητες σύμφωνα με συγκεκριμένες διαδικασίες που περιλαμβάνονται στη "Δήλωση Διαδικασιών Πιστοποίησης" και ανάλογα με τις "Πολιτικές Πιστοποίησης" της κάθε Αρχής Πιστοποίησης.

Η Δήλωση Διαδικασιών Πιστοποίησης και η Πολιτική Πιστοποίησης του ΕΔΕΤ βρίσκονται στο Παράρτημα Ν.

2.3 Κεντρική Αρχή Πιστοποίησης HARICA

Η HARICA είναι μια Αρχή Πιστοποίησης η οποία φιλοξενείται στο Εθνικό Δίκτυο Έρευνας και Τεχνολογίας ΕΔΕΤ. Η Αρχή αυτή αποτελεί ένα κοινό σημείο αρχής της εμπιστοσύνης (trust anchor) για την ελληνική ακαδημαϊκή και ερευνητική κοινότητα. Πρόκειται για έναν οργανισμό που εκδίδει πιστοποιητικά δημόσιου κλειδιού. Τα πιστοποιητικά, υπογράφονται από τα προσωπικά κλειδιά που ανήκουν στην Αρχή Πιστοποίησης, και περιέχουν το όνομα του προσώπου, το δημόσιο κλειδί αυτού του προσώπου, έναν serial number, και άλλες πληροφορίες.

Η Αρχή Πιστοποίησης της HARICA βρίσκεται εκτός δικτύου για λόγους ασφαλείας. Υπάρχει μια διαδικασία μεταφοράς των αιτημάτων των χρηστών με χειροκίνητο τρόπο, είτε με δισκέτες είτε με flash disks από την Αρχή Καταχώρησης στην Αρχή Πιστοποίησης. Η διαδικασία αυτή πραγματοποιείται με την εκτέλεση κάποιων ειδικών scripts που έχουν φτιαχτεί για αυτό το σκοπό.

Αρχικά εκτελείται το script εξαγωγής αιτημάτων. Τα αιτήματα που είναι αποθηκευμένα στην Αρχή Καταχώρησης μεταφέρονται και εξάγονται σε κάποιον ενδιάμεσο χώρο.

Έπειτα, πάλι με την εκτέλεση κάποιου script,ενεργοποιείται η Αρχή Πιστοποίησης.

Στη συνέχεια εκτελείται το πρόγραμμα υπογραφής πιστοποιητικών. Το πρόγραμμα αρχικά ψάχνει να βρεί διάφορα αιτήματα, καθώς συνδέεται στον ενδιάμεσο χώρο που βρίσκονται τα αιτήματα πιστοποιητικών. Γίνεται έλεγχος αν το πιστοποιητικό της αίτησης συμφωνεί με τα στοιχεία που βρίσκονται στην Αρχή Καταχώρησης. Εφόσον συμφωνούν πραγματοποίται η υπογραφή του αιτήματος. Ο διαχειριστής της Αρχής Πιστοποίησης δίνει το ιδιωτικό κλειδί του, εμφανίζεται μεχρι πότε θα υπογραφεί το πιστοποιητικό και ολοκληρώνεται η διαδικασία.

Αφού το πιστοποιητικό δημιουργηθεί επιστρέφει στην Αρχή Καταχώρησης εκτελώντας ένα script εισαγωγής πιστοποιητκού και ενημερώνεται ο χρήστης ότι μπορεί να το παραλάβει.

3

Συμμετοχή του ΤΕΙ Κρήτης στην υποδομή δημόσιου κλειδιού HARICA

Σε αυτό το κεφάλαιο θα ασχοληθούμε με τη συμμετοχή του ΤΕΙ Κρήτης με τη HARICA. Θα περιγράψουμε τη διαδικασία για την ένταξη του ιδρύματος και τις υπηρεσίες που μπορεί να χρησιμοποιήσει στα πλαίσια αυτής της συνεργασίας.

3.1 Αίτηση συμμετοχής του ΤΕΙ Κρήτης στην υποδομή δημόσιου κλειδιού HARICA

Η διαδικασία ένταξης του ιδρύματος ξεκινάει με τη συμπλήρωση μιας αίτησης. Στην αίτηση αυτή περιέχονται κάποια γενικά στοιχεία για το φορέα, το όνομα του ιδρύματος , το όνομα του υπεύθυνου επικοινωνίας κτλ. Στη συνέχεια καθορίζεται το είδος της συνεργασίας με τη HARICA.

- Μπορεί κάποιο ίδρυμα να έχει ήδη δική του Αρχή Πιστοποίησης και να ζητά διαπιστοποίηση, ώστε τα πιστοποιητικά της μιας Αρχής να αναγνωρίζονται από την άλλη.
- Εναλλακτικά, μπορεί να αιτηθεί νέα Αρχή Πιστοποίησης υπογεγραμμένη από τη HARICA, της οποίας η διαχείριση θα γίνεται εξ'ολοκλήρου από τον φορέα.
- Τέλος, μπορεί να αιτηθεί νέα Αρχή Πιστοποίησης και πλήρη ή μερική τεχνική υποστήριξη από τους τεχνικούς της HARICA. Συγκεκριμένα μπορεί να χρησιμοποιούνται οι μηχανισμοί της Αρχής Πιστοποίησης της HARICA για να υπογράφονται τα αιτήματα ή να χρησιμοποιήσει την Αρχή Καταχώρησης της HARICA για να κατατίθονται τα αιτήματα των χρηστών για ψηφιακά πιστοποιητικά. Ο φορέας μπορεί να επιλέξει δυο μεθόδους πιστοποίησης των στοιχείων των αιτούντων. Η πρώτη γίνεται με αυτόματο έλεγχο των στοιχείων του χρήστη, τα οποία βρίσκονται σε κάποια υπηρεσία καταλόγου του φορέα[1] , με έλεγχο username & password που βρίσκεται στο φορέα. Η δεύτερη μέθοδος γίνεται μέσω email επιβεβαίωσης των στοιχείων. Τα στοιχεία τα εισάγει ελεύθερα ο χρήστης και θα πρέπει να επιβεβαιωθούν από το noc του φορέα. Η μέθοδος αυτή είναι

[1] Σε περίπτωση που το ίδρυμα δεν διαθέτει υπηρεσία καταλόγου, μπορεί να χρησιμοποιήσει την Εθνική υπηρεσία καταλόγου του ΕΔΕΤ που παρέχει εύκολη διαχείριση χρηστών σε web περιβάλλον, και πολλαπλά οφέλη.

χειροκίνητη και προσθέτει παρισσότερα βήματα στη διαδικασία έκδοσης πιστοποιητικού.

Αφού συμπληρωθεί κατάλληλα η αίτηση αποστέλλεται στους διαχειριστές της HARICA.

Το ίδρυμα του ΤΕΙ Κρήτης αιτήθηκε για νέα Αρχή Πιστοποίησης και χρησιμοποιεί την Αρχή Καταχώρησης της HARICA για την αποστολή των αιτημάτων των χρηστών για ψηφιακό πιστοποιητικό. Η επιβεβαίωση των στοιχείων των χρηστών, οι οποίοι αιτούνται ψηφιακό πιστοποιητικό, γίνεται μέσω της υπηρεσίας καταλόγου του Ιδρύματος (ldap.teicrete.gr).

Μετά την έγκριση της αίτησης ο υπεύθυνος του ΚΕΔΔ(Κέντρο Ελέγχου & Διαχείρισης Δικτύων) ήρθε σε συννενόηση με τον αρμόδιο της HARICA και υπήρξε ενημέρωση σχετικά με τη μορφή που πρέπει να έχει ο ldap ώστε να μπορούν να αξιοποιηθούν κατάλληλα τα στοιχεία του.

Τέλος, δημιουργήθηκε η Αρχή Πιστοποίησης του ΤΕΙ Κρήτης με διακεκριμένο όνομα 'Technological Educational Institution of Crete CA 2007', την οποία διαχειρίζονται πλήρως οι τεχνικοί της HARICA.

Η αίτηση αυτούσια βρίσκεται στο Παράρτημα Α.

3.2 Χρήση υπηρεσιών της HARICA

Για την έκδοση πιστοποιητικών χρήστη και διακομιστή τα οποία είναι υπογεγραμμένα από την Αρχή Πιστοποίησης του ΤΕΙ Κρήτης, πρέπει να χρησιμοποιήσουμε την υποδομή της HARICA.

Για να χρησιμοποιήσουμε τις υπηρεσίες της HARICA θα πρέπει πρώτα να την εμπιστευτούμε σαν Ανώτατη Αρχή Πιστοποίησης. Αυτό θα γίνει εγκαθιστώντας το ψηφιακό πιστοποιητικό της στον browser.

Από τη στιγμή που θα το εγκαταστήσουμε δηλώνουμε πως.

- Αναγνωρίζουμε οτι η διεύθυνση www.harica.gr αντιστοιχεί όντως στην ιστοσελίδα της Hellenic Academic and Research Institutions Certificate Authority.
- Αναγνωρίζουμε τη HARICA ως Αρχή Πιστοποίησης και την εμπιστευόμαστε να πιστοποιεί χρήστες, διακομιστές και λογισμικό.

Για να γίνει η εγκατάσταση επισκεπτόμαστε τη σελίδα της HARICA,στη διεύθυνση http://www.harica.gr/index.php.el και ακολουθούμε τις οδηγίες. Στο Παράρτημα Β περιγράφεται η ακριβής διαδικασία που πρέπει να ακολουθηθεί.

Έχοντας εγκαταστήσει το πιστοποιητικό της HARICA μπορούμε να αιτηθούμε ψηφιακά πιστοποιητικά.

Το ψηφιακό πιστοποιητικό, που κατέχει και επιδεικνύει ένας χρήστης, πιστοποιεί την ταυτότητα του σε τρίτους και παρέχει τα μέσα σε αυτούς να επιβεβαιώνουν, αυτή τη ταυτότητα.

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται κατά κύριο λόγο στην επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου. Το κοινό ηλεκτρονικό ταχυδρομείο δεν εξασφαλίζει την ταυτότητα του αποστολέα ούτε την ακεραιότητα του περιεχομένου του μηνύματος, σε αντίθεση με το ασφαλές ηλεκτρονικό. Το τελευταίο, βασίζεται στο πρωτόκολλο S/MIME (Secure Multipurpose Internet Mail Extensions), που υποστηρίζεται από τις τελευταίες εκδόσεις λογισμικού διαχείρισης ηλεκτρονικού ταχυδρομείου (π.χ Outlook Express, Mozilla)

Με την χρήση ψηφιακών πιστοποιητικών είναι δυνατή η πλοήγηση σε ασφαλείς δικτυακούς τόπους/ιστοσελίδες. Η προσπέλαση των δικτυακών τόπων που χαρακτηρίζονται ασφαλείς, χρησιμοποιούν ψηφιακά πιστοποιητικά εξυπηρετητών (με ενεργοποίηση πρωτοκόλλου SSL) και με τεχνολογίες κρυπτογράφησης εξασφαλίζουν το απόρρητο της επικοινωνίας. Το αποτέλεσμα είναι τα στοιχεία που ο χρήστης πληκτρολογεί και "στέλνει" προς τον ιστοχώρο να μην μπορούν να διαβαστούν από τρίτους.

Επιπλέον, υπάρχουν εξυπηρετητές ιστοσελίδων (Web Servers) που απαιτούν απόδειξη της ταυτότητας του χρήστη για να παρέχουν δικτυακές υπηρεσίες. Όλοι οι σύγχρονοι πλοηγοί (πχ Netscape, Internet Explorer, Mozilla, Safari), παρέχουν τη δυνατότητα πιστοποίησης ταυτότητας με την χρήση ψηφιακών πιστοποιητικών (Web Authentication).

4

Ψηφιακό πιστοποιητικό χρήστη

Σε αυτό το κεφάλαιο θα περιγράψουμε τη διαδικασία που ακολουθήσαμε για την έκδοση πιστοποιητικών για χρήστη. Θα δούμε τη χρήση του πιστοποιητικού για την υπογραφή και κρυπτογράφηση email, την ανάκληση πιστοποιητικού για διάφορους λόγους.

4.1 Αίτηση για ψηφιακό πιστοποιητικό χρήστη

Αφού έχουμε αποδεχτεί την Αρχή Πιστοποίησης HARICA μπορούμε να κάνουμε αίτηση για έκδοση ψηφιακού πιστοποιητικού χρήστη.

Πιστοποιητικά Χρήστη εκδίδονται σε φυσικά πρόσωπα, μέλη των φορέων - συνδρομητών της HARICA που διαθέτουν ηλεκτρονική διεύθυνση σε επίσημη υπηρεσία του φορέα τους.

Οποιοσδήποτε είναι εγγεγραμένος στην υπηρεσία καταλόγου ldap.teicrete.gr, του ΤΕΙ μπορεί να επισκεφτεί τη σελίδα της HARICA και να αιτηθεί ψηφιακό πιστοποιητικό.

Χρησιμοποιώντας τον ίδιο browser και τον ίδιο υπολογιστή συνδεόμαστε στις σελίδες της HARICA και επιλέγουμε από το menu **έκδοση πιστοποιητικού για χρήστη.**

Τα στοιχεία που χρειάζονται αρχικά είναι το ονοματεπώνυμο του χρήστη και το email του. Αφού δοθούν, γίνεται έλεγχος του email στην υπηρεσία καταλόγου του φορέα και αντλούνται τα στοιχεία του χρήστη, τα οποία εμφανίζονται όπως είναι εκεί καταχωρημένα. Έπειτα ζητείται ο κωδικός που χρησιμοποιεί ο χρήστης στο λογαριασμό του.

Στο τελικό βήμα μας ενημερώνει ότι η αίτηση πρέπει να γίνει από το browser που θα χρησιμοποιείται το πιστοποιητικό. Ζητείται να αποδεχτούμε τους όρους της δήλωσης διαδικασιών πιστοποίησης της HARICA και πατώντας **request** κατατίθεται το αίτημα για πιστοποιητικό χρήστη.

Καταθέτοντας την αίτηση για ψηφιακό πιστοποιητικό, θα δημιουργηθεί και ένα ζεύγος κλειδιών(ιδιωτικό-δημόσιο) και γι αυτό μας ζητείται να ορίσουμε ένα master password για την προστασία του ιδιωτικού κλειδιού.

Η αίτηση για πιστοποιητικό αποστέλλεται στην Αρχή Καταχώρησης . Από εκεί, χειροκίνητα μεταφέρεται στην Αρχή Πιστοποίησης, ελέγχεται και εκδίδεται το ψηφιακό πιστοποιητικό.

Η ακριβής διαδικασία αίτησης για έκδοση πιστοποιητικού, περιγράφεται στο Παράρτημα Γ.

4.2 Παραλαβή ψηφιακού πιστοποιητικού χρήστη

Αφού το αίτημα γίνει αποδεκτό και εκδοθεί το πιστοποιητικό, η υπηρεσία μας ειδοποιεί με email για την παραλαβή του. Ακολουθώντας το σχετικό σύνδεσμο που υπάρχει στο email παραλαμβάνουμε το πιστοποιητικό, το οποίο εγκαθίσταται αυτόματα στον browser. Μπορούμε να αποθηκεύσουμε το πιστοποιητικό σε base64 format & binary format. Επίσης μας δίνεται ο μυστικός κωδικός ανάκλησης τον οποίο θα χρησιμοποιήσουμε σε περίπτωση που θέλουμε να ακυρώσουμε το πιστοποιητικό.

Σχετικά με τις μορφές ενός πιστοποιητικού, μπορούμε να αποθηκεύσουμε ένα πιστοποιητικό σε δυαδική μορφή. Στην περίπτωση αυτή χρησιμοποιείται κωδικοποίηση DER (Distinquished Enconding Rules). Τα δεδομένα του πιστοποιητικού αποθηκεύονται κατευθείαν σε δυαδική μορφή. Τα πιστοποιητικά μορφής DER χρησιμοποιούνται κυρίως από τα Windows και υποστηρίζονται τόσο από το Mozilla Firefox όσο και από τον Internet Explorer. Επίσης μπορούμε να αποθηκεύσουμε ένα πιστοποιητικό σε BASE64 μορφή. Στην περίπτωση αυτή το πιστοποιητικό αποθηκεύεται με την κατάληξη .pem (Privacy Enhanced Mail). Ουσιαστικά το pem αρχείο είναι το der αρχείο το οποίο μπορεί να μεταφερθεί σε απλό κείμενο χρησιμοποιώντας κωδικοποίηση BASE64. Μπορούμε να το δούμε ανοίγοντάς το με ένα text editor. Περιέχει μια επικεφαλίδα και μια κατακλείδα. Η μορφή pem προτιμάται από τα Unix/Linux.

Αναζητώντας τα εγκατεστημένα πιστοποιητικά στο browser θα βρούμε αυτό που μόλις παραλάβαμε, αποθηκευμένο στα προσωπικά πιστοποιητικά.

Η ακριβής διαδικασία παραλαβής πιστοποιητικού, περιγράφεται στο Παράρτημα Δ.

4.3 Διαχείριση του ψηφιακού πιστοποιητικού χρήστη

4.3.1 Δημιουργία backup αρχείου του ψηφιακού πιστοποιητικού χρήστη

Ένα backup αρχείο ενός ψηφιακού πιστοποιητικού, είναι το πιστοποιητικό μαζί με το ιδιωτικό κλειδί κρυπτογραφημένο σε ένα αρχείο PKCS12. Αυτό το αρχείο το χρησιμοποιούμε για να εγκαταστήσουμε το πιστοποιητικό σαν προσωπικό πιστοποιητικό σε ένα browser ή σε κάποιο πρόγραμμα ηλεκτρονικού ταχυδρομείου. Παρακάτω περιγράφεται η διαδικασία που πρέπει να ακολουθήσουμε για τη δημιουργία αυτού του αρχείου.

Πηγαίνουμε στον browser στον οποίο έχει αρχικά αποθηκευτεί το πιστοποιητικό. Στα προσωπικά πιστοποιητικά όπου και βρίσκεται, υπάρχει η επιλογή δημιουργίας **backup** αρχείου. Μας ζητείται να ορίσουμε που και με ποιο όνομα θα αποθηκευτεί το αρχείο αυτό. Στη συνέχεια πρέπει να δώσουμε το master password που έχει οριστεί για την προστασία του ιδιωτικού κλειδιού. Έπειτα, μας ζητά να δημιουργήσουμε έναν κωδικό για την προστασία του backup αρχείου. Τέλος, μας ενημερώνει για την επιτυχή δημιουργία του αρχείου.

Η ακριβής διαδικασία δημιουργίας του, περιγράφεται στο Παράρτημα Ε.

4.3.2 Εγκατάσταση προσωπικού ψηφιακού πιστοποιητικού χρήστη σε άλλο browser.

Για να μπορέσουμε να εγκαταστήσουμε το προσωπικό μας πιστοποιητικό, σε άλλο browser από αυτόν που κάναμε την αίτηση αρχικά και στον οποίο εγκαταστάθηκε αυτόματα, πρέπει να εισαγάγουμε στα **προσωπικά πιστοποιητικά**, το backup αρχείο του.

Η ακριβής διαδικασία εγκατάστασής του περιγράφεται στο Παράρτημα Ζ.

4.3.3 Εγκατάσταση ψηφιακού πιστοποιητικού άλλου χρήστη σε browser.

Για να μπορέσουμε να χρησιμοποιήσουμε το ψηφιακό πιστοποιητικό άλλου χρήστη θα πρέπει να το εγκαταστήσουμε στα **πιστοποιητικά άλλων προσώπων** του browser. Σε αυτήν την περίπτωση αναζητούμε το πιστοποιητικό που μας ενδιαφέρει στην αντίστοιχη σελίδα της HARICA και το αποθηκεύουμε ώστε στη συνέχεια να μπορέσουμε να το εγκαταστήσουμε. Η ακριβής διαδικασία εγκατάστασής του περιγράφεται στο Παράρτημα Η.

4.3.4 Εγκατάσταση και χρήση ψηφιακού πιστοποιητικού χρήστη από προγράμματα ηλεκτρονικού ταχυδρομείου

Τα προγράμματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν τα ψηφιακά πιστοποιητικά για την υπογραφή και κρυπτογράφηση email.

Τα προσωπικά πιστοποιητικά χρησιμοποιούνται για την υπογραφή email. Μπορούμε να κάνουμε τέτοιες ρυθμίσεις ώστε όλα τα εξερχόμενα μηνύματα να περιέχουν τη ψηφιακή υπογραφή μας.

Τα πιστοποιητικά άλλων χρηστών χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων με το δημόσιο κλειδί του εκάστοτε παραλήπτη το οποίο αντλείται από το πιστοποιητικό του.

Στο Παράρτημα Θ περιγράφεται η διαδικασία εγκατάστασης και οι ρυθμίσεις για τη χρήση του ψηφιακού πιστοποιητικού από το Outlook Express και το Thunderbird.

4.4 Ανάκληση ψηφιακού πιστοποιητικού χρήστη

Το πιστοποιητικό ενός χρήστη πρέπει να ανακληθεί όταν συντρέχει κάποιος από τους ακόλουθους λόγους:

- Δεν χρησιμοποιείται πλέον.
- Έχουν αλλάξει τα στοιχεία που περιέχει. Π.χ. η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη, η σχέση του χρήστη με τον φορέα, χρήστη της HARICA, κ.α.
- Έχει εκτεθεί ή χαθεί ή υποπτευθεί ότι έχει εκτεθεί ή χαθεί το ιδιωτικό κλειδί.

Μετά την ανάκλησή του, το πιστοποιητικό παύει να ισχύει. Ο χρήστης μπορεί να αιτηθεί την έκδοση νέου πιστοποιητικού.

Για την ανάκληση του πιστοποιητικού ο χρήστης θα πρέπει να υποβάλει αίτηση από την αντίστοιχη ασφαλή ιστοσελίδα δίνοντας το μυστικό κωδικό ανάκλησης.

Η διαδικασία ανάκλησης πιστοποιητικού περιγράφεται λεπτομερώς στο Παράρτημα Ι.

5

Ψηφιακό πιστοποιητικό διακομιστή

Σε αυτό το κεφάλαιο θα περιγράψουμε τη διαδικασία που ακολουθήσαμε για την έκδοση πιστοποιητικού για το διακομιστή imap.teicrete.gr, ο οποίος είναι στημένος σε Linux. Θα δούμε επίσης τον τρόπο παραλαβής και αποθήκευσης του πιστοποιητικού καθώς και την ανάκλησή του για διάφορους λόγους.

5.1 Αίτηση ψηφιακού πιστοποιητικού διακομιστή

Πιστοποιητικά Διακομιστή εκδίδονται σε διακομιστές (servers) που ανήκουν σε φορείς - συνδρομητές της HARICA και διαχειρίζονται από μέλη των φορέων. Το μέλος του φορέα που είναι υπεύθυνος για τη λειτουργία και τη διαχείριση του διακομιστή θα πρέπει να διαθέτει Ψηφιακό Πιστοποιητικό Χρήστη.

Τα στοιχεία που χρειάζονται για την έκδοση πιστοποιητικού είναι αρχικά το πλήρες όνομα του διακομιστή(FQDN). Στη συνέχεια ζητείται η πιστοποίηση του διαχειριστή του διακομιστή. Αφού γίνει έλεγχος των στοιχείων του

Δημιουργούμε ένα αρχείο ρύθμισης με όνομα servercert.cnf με τα στοιχεία του πιστοποιητικού που θα ζητήσουμε. Με χρήση openssl δημιουργούμε το ιδιωτικό κλειδί (προστατευμένο με κωδικό) το οποίο θα χρησιμοποιηθεί για το αίτημα ψηφιακού πιστοποιητικού και στη συνέχεια για τη χρήση του τελικού πιστοποιητικού. Το κλειδί θα δημιουργηθεί στο αρχείο "server.key". Δημιουργούμε το αίτημα ψηφιακού πιστοποιητικού (Certificate Server Request). Το αίτημα θα δημιουργηθεί στο αρχείο "server.csr" . Ανοίγουμε το αρχείο "server.csr" με ένα πρόγραμμα που διαβάζει απλό ASCII κείμενο (πχ notepad), αντιγράφουμε τα περιεχόμενα του και τα επικολλούμε στο πεδίο "Αίτηση σε μορφή PKCS10" της σελίδας αίτησης για έκδοση πιστοποιητικού. Τέλος, υποβάλλουμε την αίτηση.

Στο Παράρτημα Κ περιγράφεται με λεπτομέρειες η διαδικασία υποβολής της αίτησης.

5.2 Παραλαβή και διαχείριση ψηφιακού πιστοποιητικού διακομιστή

Μετά την υποβολή της αίτησης και αφού το αίτημα γίνει δεκτό από την Αρχή Πιστοποίησης , ειδοποιείται με email ο διαχειριστής για την παραλαβή του πιστοποιητικού μέσω του σχετικού συνδέσμου που υπάρχει στο μήνυμα.

Μπορούμε να αποθηκεύσουμε το πιστοποιητικό σε base64 format & binary format. Επίσης μας δίνεται ο μυστικός κωδικός ανάκλησης τον οποίο θα χρησιμοποιήσουμε σε περίπτωση που θέλουμε να ακυρώσουμε το πιστοποιητικό.

Μετά την παραλαβή του πιστοποιητικού αποθηκεύουμε το πιστοποιητικό και το ιδιωτικό κλειδί σε ένα αρχείο με το όνομα imapd.pem και το αποθηκεύουμε στο κατάλογο etc/pki/tls/certs. Από το αρχείο αυτό έχουμε βγάλει το passphrase. Αν και αυτό μειονεκτεί από θέμα ασφάλειας, σε δημόσιους servers είναι αναγκαίο.

Στο Παράρτημα Λ περιγράφεται με λεπτομέρειες η διαδικασία για την παραλαβή και αποθήκευσή του στο server.

5.3 Ανάκληση ψηφιακού πιστοποιητικού διακομιστή

Για την ανάκληση του πιστοποιητικού διακομιστή, ο υπεύθυνος για τη λειτουργία του θα πρέπει να υποβάλει αίτηση από την αντίστοιχη ασφαλή ιστοσελίδα.

Η αίτηση αυτή περιέχει το πλήρες όνομα του διακομιστή, τον μυστικό κωδικό ανάκλησης ο οποίος δόθηκε κατά την παραλαβή του πιστοποιητικού και το λόγο που ζητάμε την ανάκληση.

Στο Παράρτημα Μ περιγράφεται με λεπτομέρειες η διαδικασία ανάκλησης του πιστοποιητικού.

6

Συμπεράσματα-Προτάσεις

6.1 Σύνοψη

Στην παρούσα πτυχιακή εργασία περιγράφεται η διαδικασία έκδοσης ψηφιακού πιστοποιητικού για το ΤΕΙ Κρήτης, από την Αρχή Πιστοποίησης HARICA(Hellenic Academic and Research Institutions Certificate Authority).

Ξεκινώντας συμπληρώθηκε μια αίτηση συμμετοχής του ΤΕΙ Κρήτης στην Υποδομή Δημοσίου Κλειδιού HARICA, η οποία περιελάμβανε τα στοιχεία του Ιδρύματος και του υπεύθυνου διαχείρισης. Επίσης διευκρίνιζε το είδος της συνεργασίας του φορέα(ΤΕΙ Κρήτης) και της HARICA. Συγκεκριμένα το ΤΕΙ Κρήτης αιτήθηκε νέα Αρχή Πιστοποίησης με πλήρη υποστήριξη με την μορφή outsourcing από τους τεχνικούς της HARICA. Αυτό σημαίνει ότι χρησιμοποιείται η Αρχή Καταχώρησης της HARICA για την αποθήκευση των αιτημάτων των χρηστών, καθώς και οι μηχανισμοί της Αρχής Πιστοποίησης της HARICA για να υπογράφονται τα αιτήματα.

Αφού εγκρίθηκε η αίτηση και η συμμετοχή μας στη HARICA, συνδέθηκε η υπηρεσία καταλόγου του ΤΕΙ (ldap) . Έπειτα έχοντας λογαριασμούς (accounts) email στο teicrete ξεκινήσαμε τη διαδικασία έκδοσης πιστοποιητικού χρήστη.

Πρώτα εμπιστεύομαστε τη HARICA ως Ανώτατη Αρχή Πιστοποίησης. Χρησιμοποιώντας τον ίδιο υπολογιστή και τον ίδιο browser(mozilla firefox) και ακολουθώντας τα βήματα στην αντίστοιχη ιστοσελίδα της HARICA, κάνουμε αίτηση για ψηφιακό πιστοποιητικό υπογεγραμμένο από την Αρχή Πιστοποίησης του ΤΕΙ Κρήτης. Δώσαμε το όνομα και το email του χρήστη, έγινε έλεγχος των στοιχείων στον ldap και αφού επιβεβαιώθηκε η ύπαρξη του στον κατάλογο του ιδρύματος, έγινε δεκτή η αίτηση. Κατόπιν ειδοποιείται ο χρήστης μέσω email για την παραλαβή του πιστοποιητικού, το οποίο αποθηκεύεται αυτόματα στον browser του υπολογιστή μέσω του οποίου έγινε η αίτηση και περιέχει διάφορες πληροφορίες, όνομα χρήστη και email από ποιον υπογράφηκε, πότε εκδόθηκε και πότε λήγει, το δημόσιο κλειδί του. Υπάρχει η δυνατότητα εξαγωγής του πιστοποιητικού μαζί με το ιδιωτικό κλειδί κρυπτογραφημένο,σε ένα αρχείο, ώστε να μπορεί να αποθηκευτεί και σε άλλο browser(πχ Internet Explorer) και σε άλλο υπολογιστή, ως προσωπικό πιστοποιητικό.

Το πιστοποιητικό χρήστη μπορεί να χρησιμοποιηθεί από διάφορα προγράμματα ηλεκτρονικού ταχυδρομείου(Outlook Express , Thunderbird). Με αυτό τον τρόπο ρυθμίζοντας κάποιες παραμέτρους σε αυτά, μπορούμε να στέλνουμε μηνύματα υπογεγραμμένα με την ψηφιακή μας υπογραφή αλλά και κρυπτογραφημένα. Σχετικά με την κρυπτογράφηση θα πρέπει και ο παραλήπτης να έχει ψηφιακό πιστοποιητικό και κρυπτογραφούμε το μήνυμα που θέλουμε να του στείλουμε, με το δημόσιο κλειδί του.

Για την έκδοση πιστοποιητικού για server ακολουθώντας τα βήματα της αντίστοιχης ιστοσελίδας της HARICA, δίνουμε το ονομα του server. Σε αυτό το

σημείο να υπογραμμίσουμε ότι τη αίτηση μπορεί να την κάνει μόνο ο διαχειριστής (administrator) και όχι απλός χρήστης, ώστε να μπορεί να έχει πρόσβαση στο ιδιωτικό κλειδί του διακομιστή. Στη συνέχεια πρέπει ο διαχειριστής να εκτελέσει κάποιες εντολές και να δημιουργήσει κάποια αρχεία, ώστε να φτιάξει την τελική αίτηση για το πιστοποιητικό. Αρχικά δημιουργούμε ένα αρχείο ρύθμισης με όνομα servercert.cnf με τα στοιχεία του πιστοποιητικού που θα ζητήσουμε. Εκτελώντας την κατάλληλη εντολή με χρήση openssl, δημιουργούμε το ιδιωτικό κλειδί (προστατευμένο με κωδικό), το οποίο θα χρησιμοποιηθεί για το αίτημα ψηφιακού πιστοποιητικού καθώς και για τη χρήση του τελικού πιστοποιητικού. Το κλειδί θα δημιουργηθεί στο αρχείο "server.key", με την κατάλληλη εντολή. Έπειτα δημιουργούμε το αίτημα ψηφιακού πιστοποιητικού (Certificate Server Request). Το αίτημα θα δημιουργηθεί στο αρχείο "server.csr", πάλι με μια εντολή του openssl. Ανοίγουμε το αρχείο "server.csr", που δημιουργήσαμε, με ένα πρόγραμμα που διαβάζει απλό ASCII κείμενο (πχ notepad), αντιγράφουμε τα περιεχόμενα του και τα επικολλούμε στο πεδίο "Αίτηση σε μορφή PKCS10" της σελίδας αίτησης για έκδοση πιστοποιητικού. Τέλος, υποβάλλουμε την αίτηση. Το πιστοποιητικό εκδίδεται και υπογράφεται από την Αρχή Πιστοποίησης. Ο διαχειριστής ειδοποιείται με email για την παραλαβή και αποθήκευση του πιστοποιητικού server. Αποθηκεύει το πιστοποιητικό και το ιδιωτικό κλειδί σε ένα αρχείο. Βγάζει το passphrase απο το αρχείο αυτό.

6.2 Συμπεράσματα

Η χρήση ψηφιακών πιστοποιητικών εξασφαλίζει την ασφαλή επικοινωνία μεταξύ χρηστών οι οποίοι μπορούν να αποδεικνύουν την ταυτότητα τους, καθώς και να επιτυγχάνουν την ασφαλή μεταφορά των ηλεκτρονικών μηνυμάτων, χωρίς να υπάρχει κίνδυνος υποκλοπής και αλλοίωσής τους.

Η χρήση ψηφιακών πιστοποιητικών εξυπηρετητών, δίνει τη δυνατότητα σε εξυπηρετητές ιστοσελίδων, ηλεκτρονικού ταχυδρομείου, κ.α. να εξασφαλίζουν ασφαλή (κρυπτογραφημένη) επικοινωνία μεταξύ των χρηστών και του εξυπηρετητή χρησιμοποιώντας τεχνολογίες όπως SSL (Secure Sockets Layer) και TLS (Transport Layer Security).

Επομένως στην εποχή μας, όπου το internet προσφέρει ευκολία και ταχύτητα και χρησιμοποιείται για κάθε είδους επικοινωνία, είτε αποστολή εγγράφων, είτε μηνυμάτων, είτε σημαντικών πληροφοριών, είναι απαραίτητο να μπορούμε να διασφαλίσουμε τη ακεραιότητα των επικοινωνιών.

6.3 Ελλείψεις προβλήματα

Στη διάρκεια υλοποίησης της εργασίας μας το βασικό πρόβλημα που υπήρχε ήταν η καθυστέρηση ανταπόκρισης από την πλευρά του ΚΕΔΔ(Κέντρο Ελέγχου & Διαχείρισης Δικτύων) λόγω του φόρτου εργασίας που υπήρχε και των πολλών αρμοδιοτήτων του υπεύθυνου.

6.4 Προτάσεις

Το ΤΕΙ Κρήτης συμμετέχοντας στην Υποδομή Δημόσιου Κλειδιού της HARICA, έχει αποκτήσει την Αρχή Πιστοποίησης με όνομα Technological Educational Institution of Crete CA 2007, η οποία είναι υφιστάμενη της Αρχής Πιστοποίησης της HARICA, Hellenic Academic and Research Institutions RootCA 2006. Στη φάση αυτή, τα αιτήματα των χρηστών και η υπογραφή τους διαχειρίζονται από τους υπεύθυνους της HARICA.

Σαν εξέλιξη αυτού, θα μπορούσε το ΤΕΙ Κρήτης να χειρίζεται το ίδιο την Αρχή Πιστοποίησης. Αυτό θα απαιτούσε τη δημιουργία μιας σελίδας μέσω της οποίας θα γίνονταν οι αιτήσεις για τα ψηφιακά πιστοποιητικά. Μέσω της σελίδας αυτής τα πιστοποιητικά θα αποθηκεύονται στην Αρχή Καταχώρησης. Έπειτα κάποιος υπεύθυνος θα ελέγχει τα αιτήματα, θα ενεργοποιεί τους μηχανισμούς της Αρχής Πιστοποίησης για υπογραφή πιστοποιητικού και θα εκδίδει το πιστοποιητικό.

7
Παραρτήματα

Παράρτημα Α

Αίτηση για συμμετοχή του ΤΕΙ Κρήτης στην υποδομή δημόσιου κλειδιού της HARICA

Hellenic Academic and Research Institutions Certification Authority
Ημ/νία Διεκπεραίωσης:...../...../.....

Στοιχεία Φορέα
Ονομασία:…..ΤΕΙ Κρήτης ……....
Ιδιότητα: Ακαδημαϊκός / Ερευνητικός Υπεύθυνος
επικοινωνίας: …..Μιχάλης Βούρκας …..
Τηλέφωνο: ….2810379801……..
E-mail: …..vourkas@teicrete.gr…….....

Προς τους Διαχειριστές της «Αρχής Πιστοποίησης Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων» (Hellenic Academic and Research Institutions Certification Authority – HARICA)

ΘΕΜΑ: «Σύνδεση με την Υποδομή Δημοσίου Κλειδιού HARICA»

[Ηράκλειο] 23/03/2007,

Παρακαλούμε για την συμμετοχή του φορέα μας στην Υποδομή Δημοσίου Κλειδιού HARICA. Τα στοιχεία του αναγνωριστικού ονόματος (Distinguished Name – DN) μας είναι:

C = GR
O = ……TEI of Crete……[1]

Παρακαλούμε σημειώστε με Χ, αν επιθυμείτε κάποιες από τις παρακάτω επιλογές:

1. Αίτηση δια-πιστοποίησης με υφιστάμενη Υποδομή Δημοσίου Κλειδιού ιδρύματος:
☐ Το ίδρυμά μας έχει ήδη ανεξάρτητη Κεντρική Αρχή Πιστοποίησης την οποία διαχειρίζεται με ιδία μέσα και αιτείται δια-πιστοποίηση με τη HARICA

2. Αίτηση νέας Αρχής Πιστοποίησης και υποστήριξη (μερική ή ολική) με μορφή out-sourcing από τεχνικούς της HARICA (επιλέξτε ενδεχομένως και τα δύο)
☐ Το ίδρυμα μας αιτείται να χρησιμοποιηθούν οι μηχανισμοί της Αρχής Πιστοποίησης της HARICA για να υπογράφονται τα αιτήματα ψηφιακών πιστοποιητικών των τελικών μας χρηστών
☒ Το ίδρυμα μας αιτείται να χρησιμοποιηθεί η Αρχή Καταχώρισης της HARICA (www.harica.gr) στην οποία οι τελικοί μας χρήστες θα καταθέτουν αιτήματα για ψηφιακά πιστοποιητικά

Επιλογή τρόπου εγγραφής νέων χρηστών:
☒ Αυτόματη εγγραφή των χρηστών του ιδρύματος με επιβεβαίωση κωδικού μέσω της υπηρεσίας καταλόγου του ιδρύματος[2].
☐ Εγγραφή με έλεγχο της e-mail διεύθυνσης των χρηστών και επιβεβαίωσή τους από εξουσιοδοτημένο προσωπικό του φορέα μας. [εάν το επιλέξτε, συμπληρώστε την e-mail διεύθυνση (alias) των "validators" του φορέα σας:……]

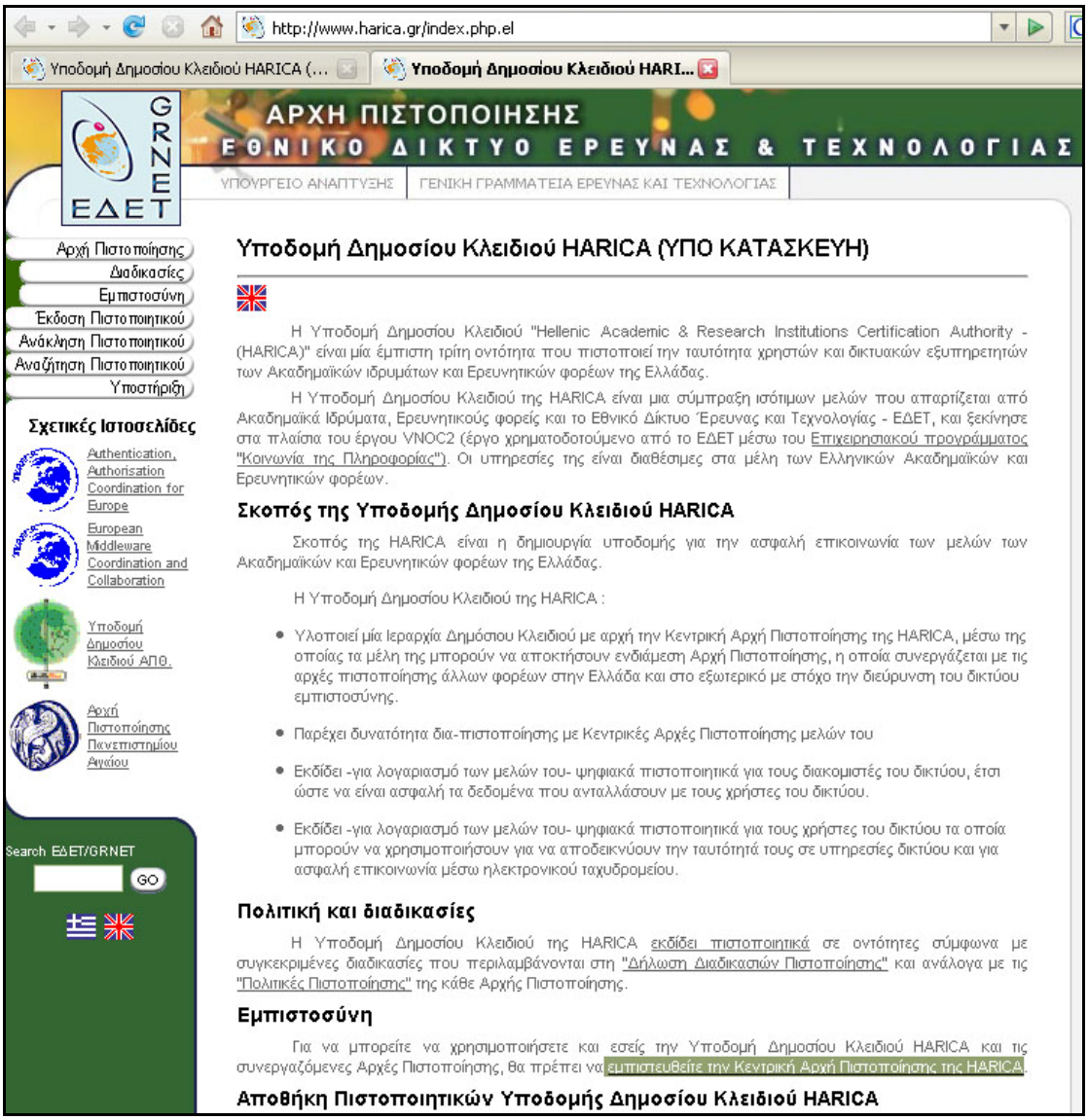
3. Αίτηση νέας Αρχής Πιστοποίησης και διαχείριση με ιδία μέσα:
☐ Το ίδρυμα μας αιτείται νέα Αρχή Πιστοποίησης υπογεγραμμένη από την Κεντρική Αρχή Πιστοποίησης της HARICA την οποία θα διαχειριστούμε με ίδια μέσα

[1] Επίσημη ονομασία του αιτούντος οργανισμού
[2] Σε περίπτωση που το ίδρυμα δεν διαθέτει υπηρεσία καταλόγου, μπορεί να χρησιμοποιήσει την Εθνική υπηρεσία καταλόγου του ΕΔΕΤ που παρέχει εύκολη διαχείριση χρηστών σε web περιβάλλον, και πολλαπλά οφέλη.

Παράρτημα Β

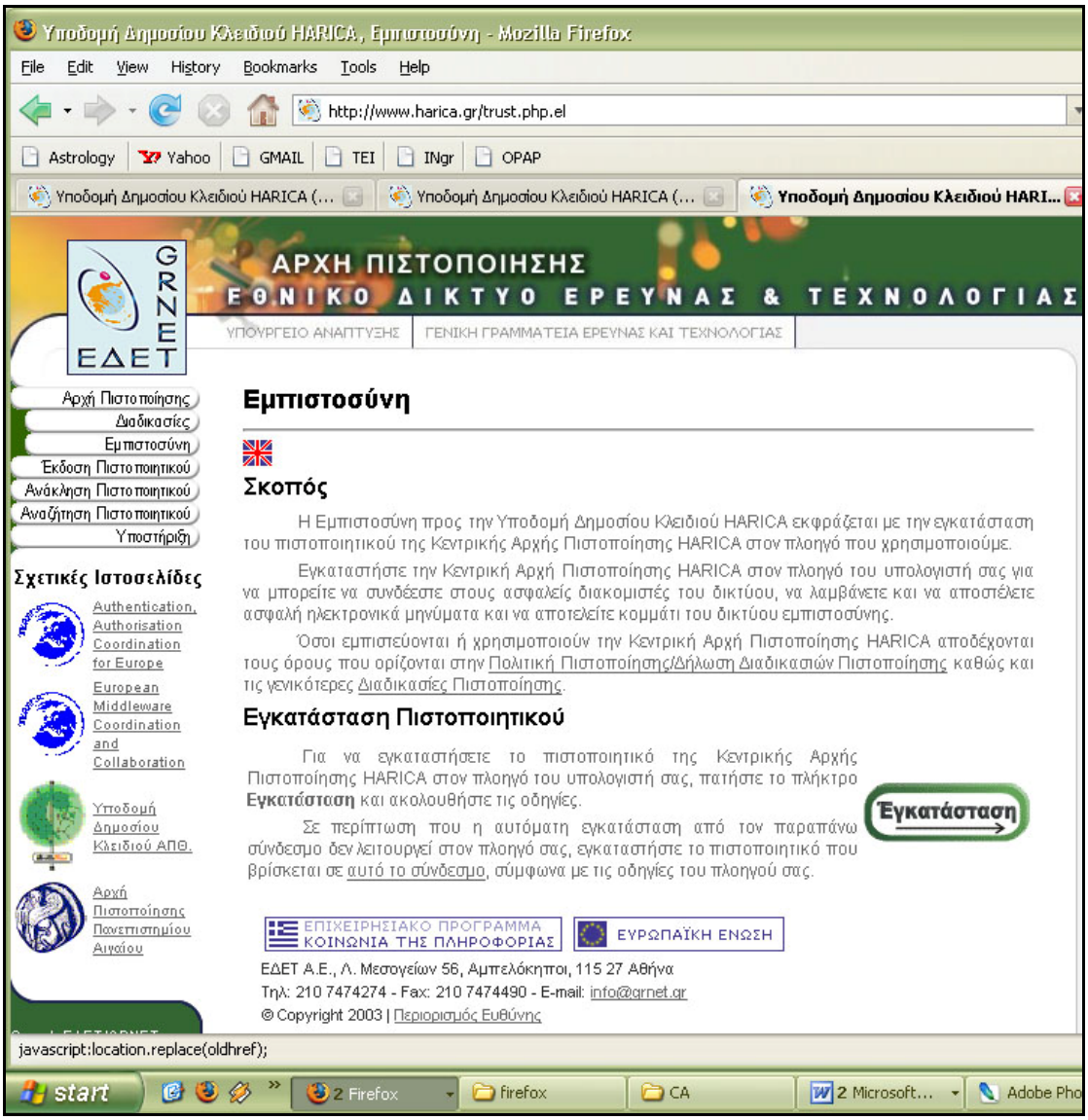
Οδηγίες για την εγκατάσταση του πιστοποιητικού HARICA στους browsers Mozilla Firefox, Internet Explorer.

Ξεκινώντας, στη σελίδα http://www.harica.gr/index.php.el , στην παράγραφο **Εμπιστοσύνη** επιλέγουμε το σύνδεσμο εμπιστευθείτε την Κεντρική Αρχή Πιστοποίησης της HARICA , ο οποίος μας μεταφέρει στη σελίδα εγκατάστασης .



Σχ 1. Εμπιστοσύνη της αρχής πιστοποίησης HARICA.

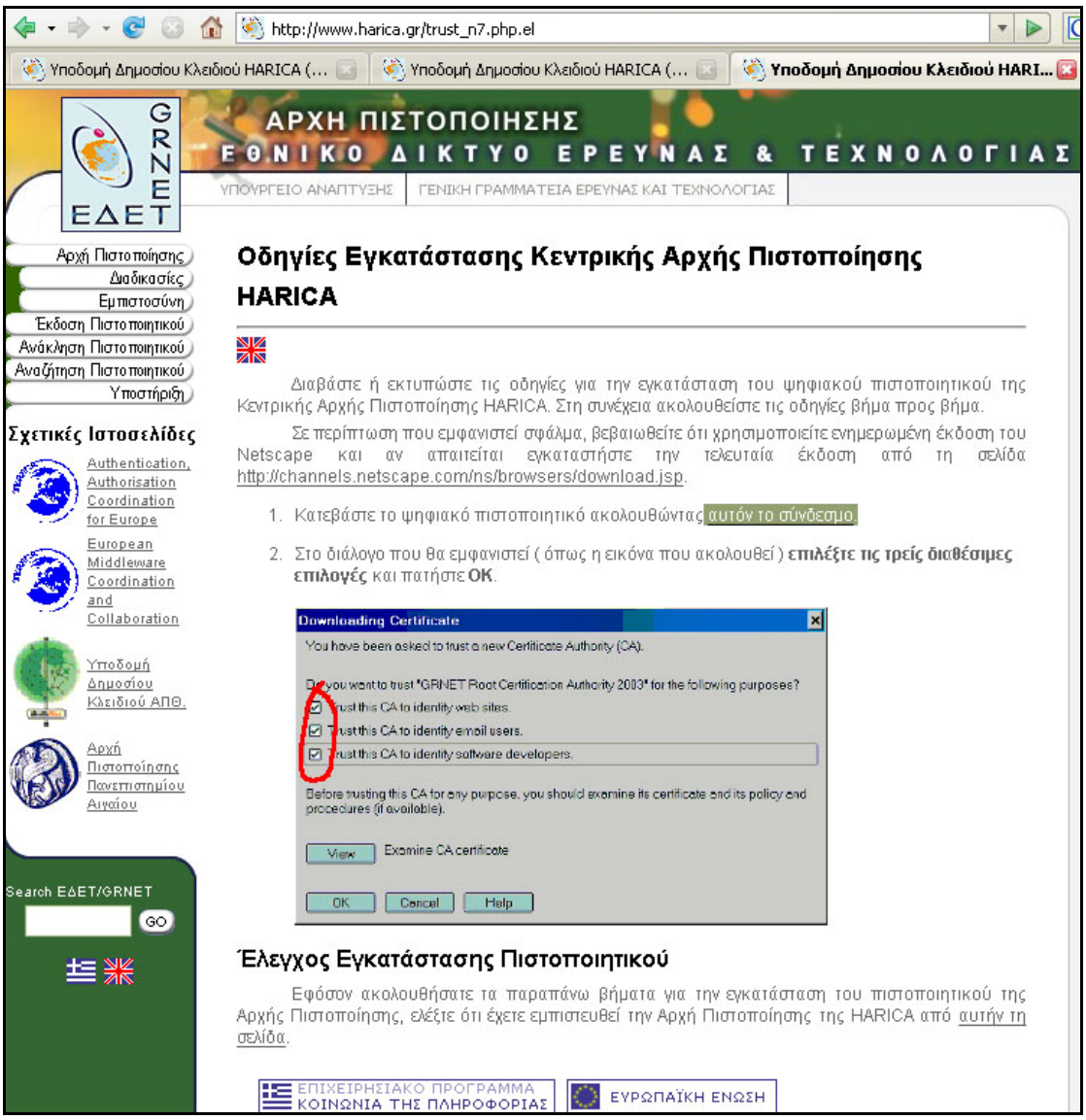
Επιλέγοντας **«Εγκατάσταση»** εμφανίζεται η σελίδα με τις οδηγίες εγκατάστασης για τον browser που χρησιμοποιούμε.



Σχ 2 Εγκατάσταση πιστοποιητικού.

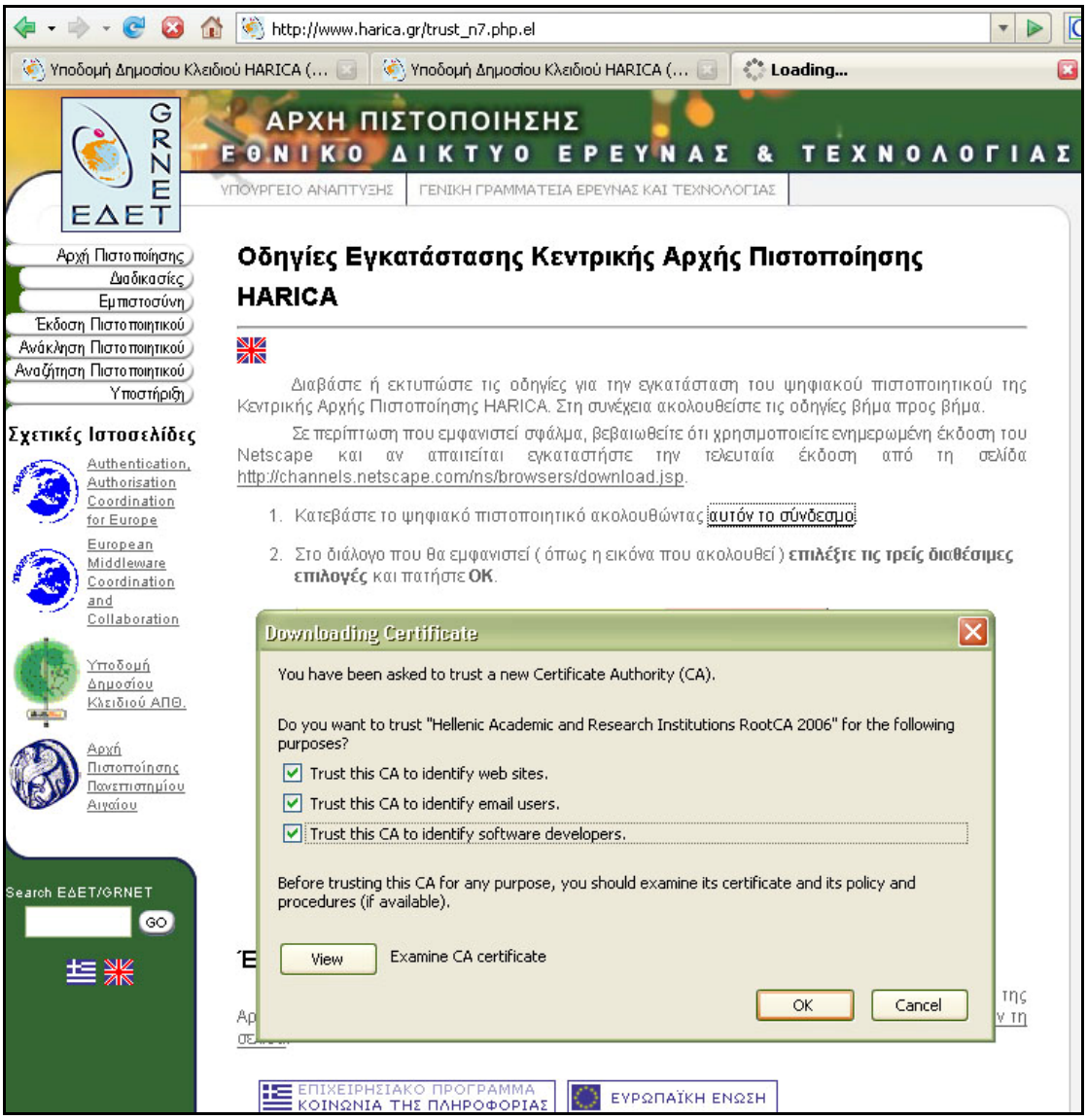
Εγκατάσταση πιστοποιητικού στο Mozilla Firefox

Η σελίδα με τις οδηγίες μας εξηγεί αναλυτικά τη διαδικασία που πρέπει να ακολουθήσουμε.



Σχ 3. Οδηγίες εγκατάστασης πιστοποιητικού.

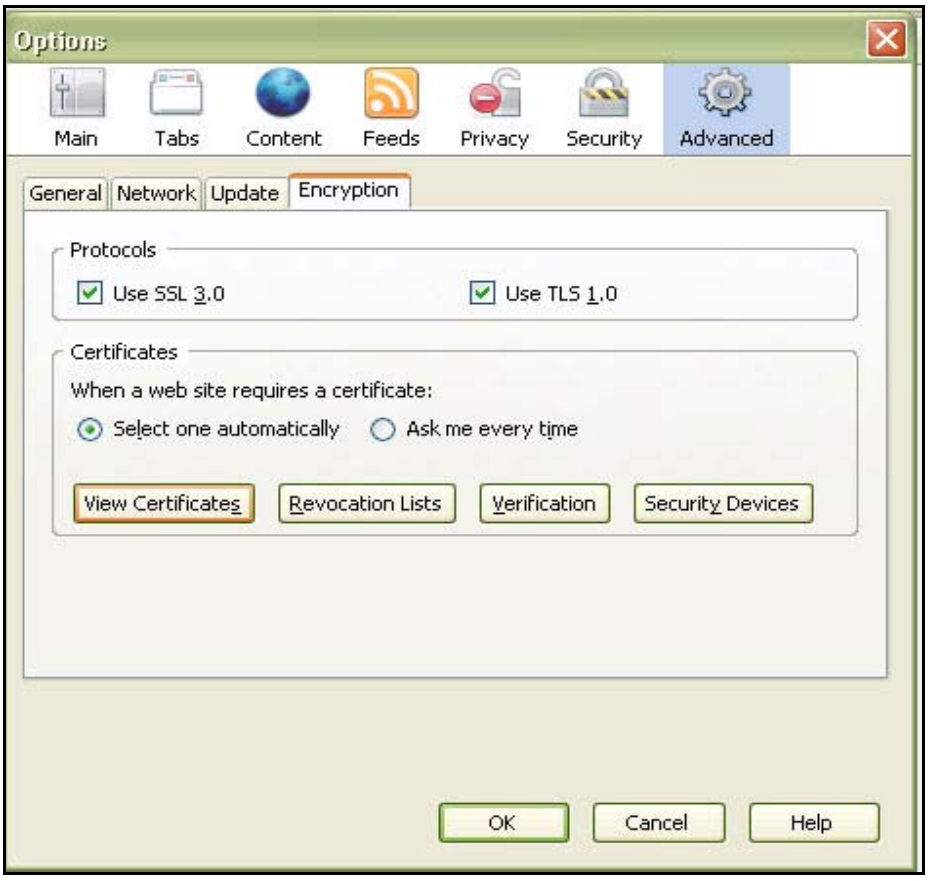
Πρώτα, κατεβάζουμε το πιστοποιητικό πατώντας το σχετικό σύνδεσμο και στο παράθυρο επιλογών που εμφανίζεται τσεκάρουμε και τις τρεις επιλογές . Πατάμε **«ok»** και η εγκατάσταση έχει πραγματοποιηθεί.



Σχ 4. Εγκατάσταση πιστοποιητικού.

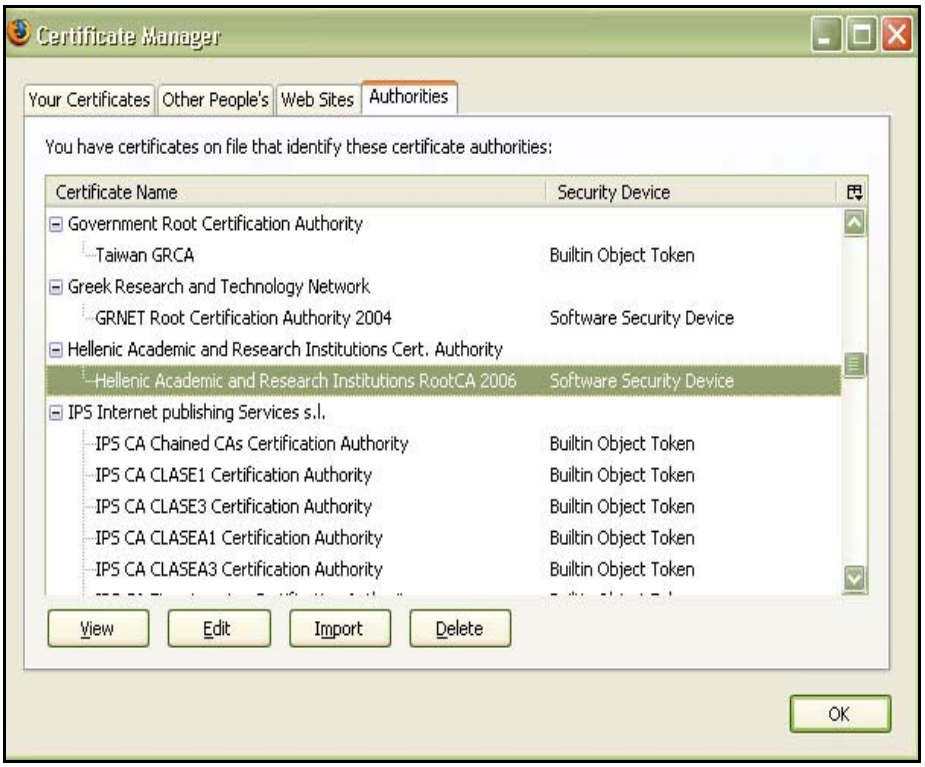
Κατόπιν από το σύνδεσμο στην παράγραφο **«Έλεγχος Εγκατάστασης Πιστοποιητικού»** παίρνουμε περαιτέρω οδηγίες για το πώς θα ελέγξουμε αν όντως έχει εγκατασταθεί το πιστοποιητικό HARICA.

Από το menu του Browser επιλέγουμε **Tools/Options**.Στο menu που εμφανίζεται επιλέγουμε το **advanced**. Στην καρτέλα **Encryption** πατάμε το κουμπί **View certificates.**



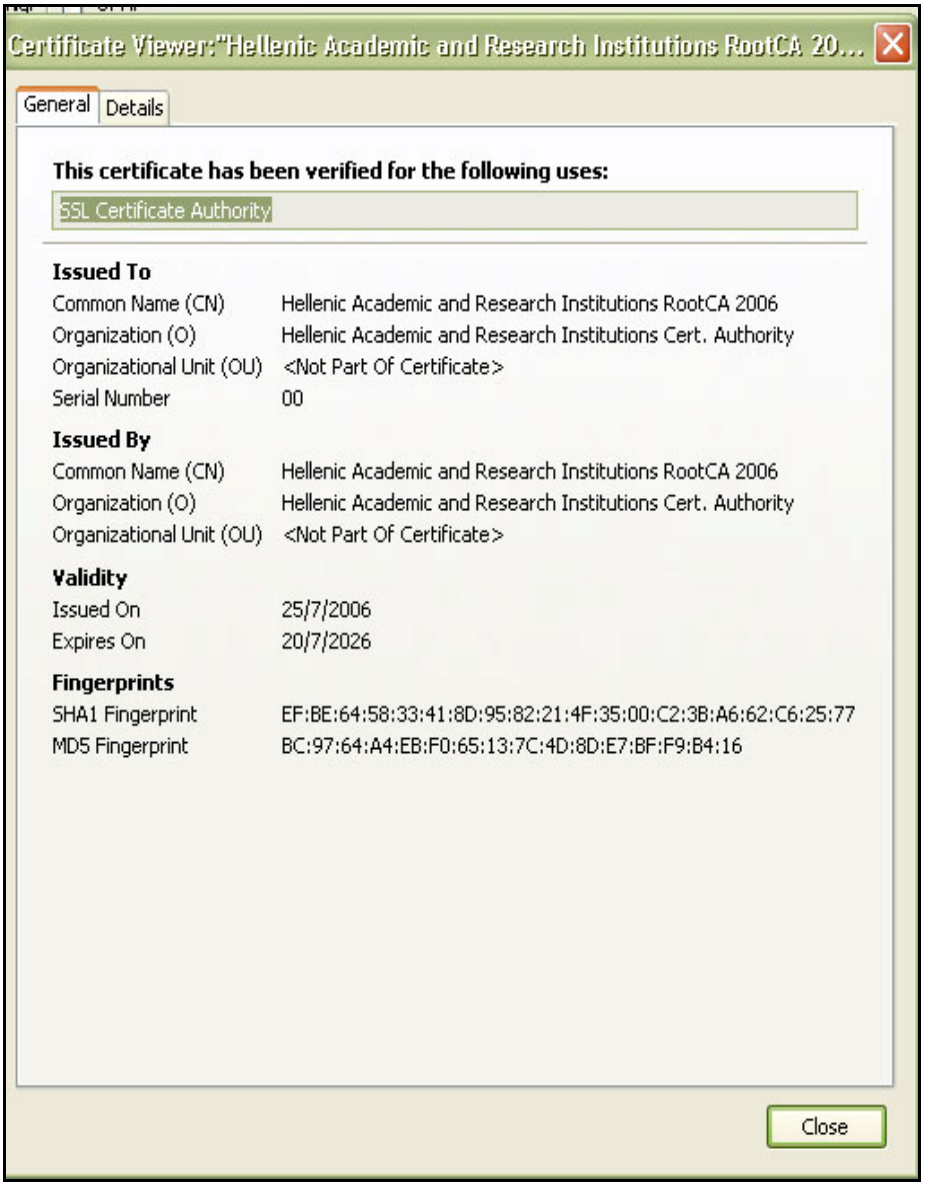
Σχ5. Έλεγχος ύπαρξης πιστοποιητικού.

Εμφανίζονται τα εγκατεστημένα πιστοποιητικά. Ανάμεσα τους και το πιστοποιητικό της HARICA. Με το κουμπί **View** βλέπουμε τα στοιχεία του πιστοποιητικού του.



Σχ 6.Εγκατεστημένα ψηφιακά πιστοποιητικά στον browser.

Στο πιστοποιητικό παρατηρούμε το όνομα της Αρχής που το εξέδωσε. Την ημερομηνία που εκδόθηκε και πότε λήγει, καθώς και το μοναδικό αποτύπωμα του πιστοποιητικού.



Σχ7. Ψηφιακό Πιστοποιητικό.

Εγκατάσταση πιστοποιητικού στο Internet Explorer

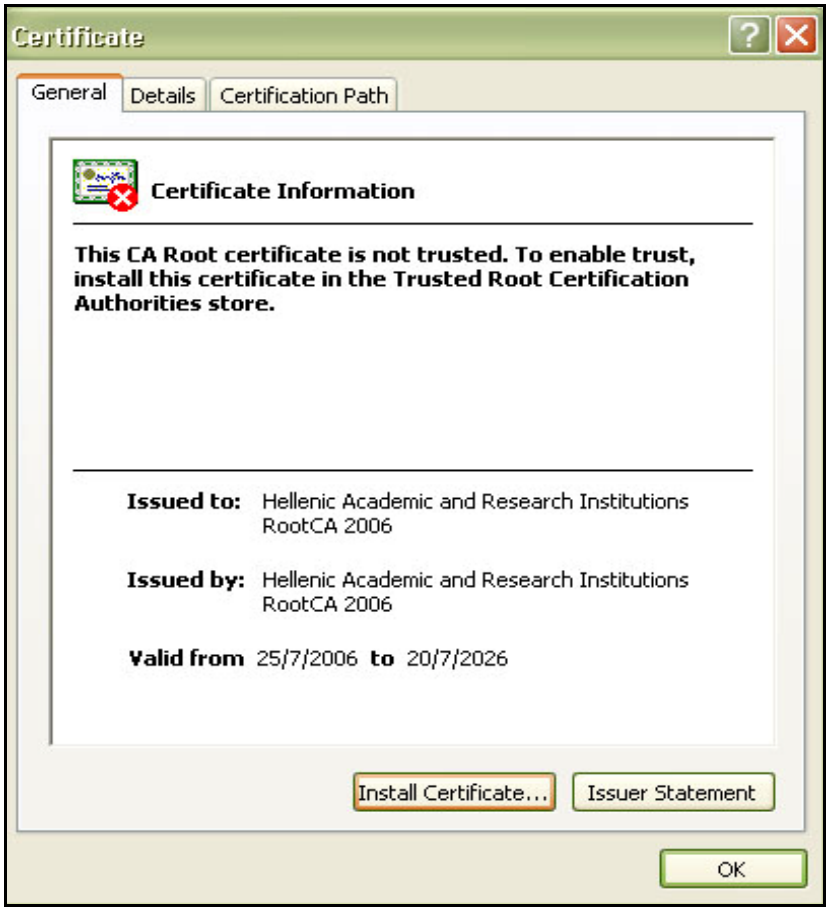
Διαβάζουμε τις οδηγίες που βρίσκονται στην αντίστοιχη ιστοσελίδα. Κατεβάζουμε το πιστοποιητικό από το σχετικό σύνδεσμο.

Σχ 8 Εγκατάσταση πιστοποιητικου για Internet Explorer(α)

Στο παράθυρο διαλόγου που ανοίγει πατάμε το κουμπί **Open :**

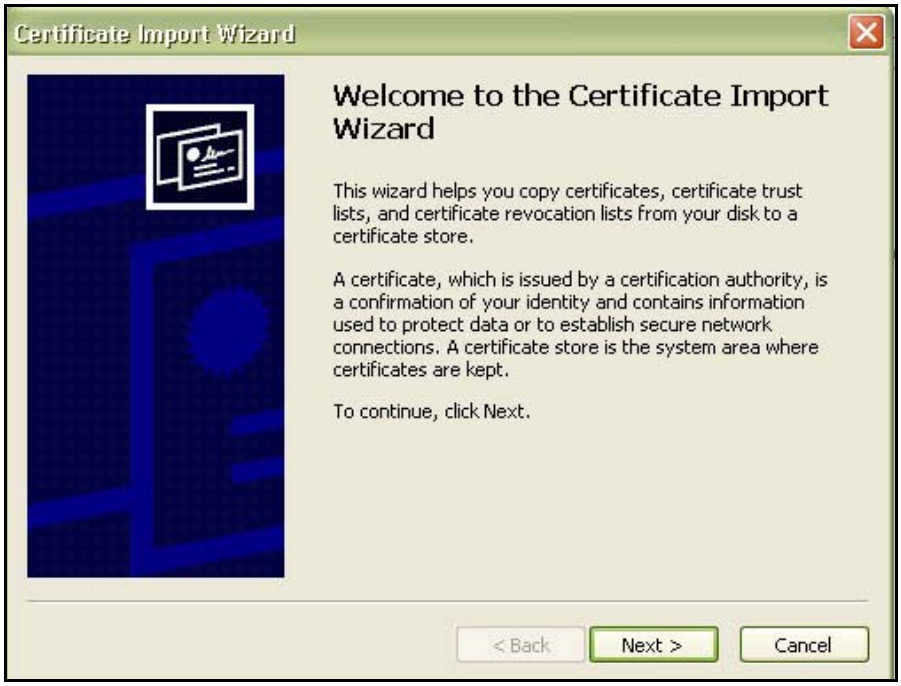
Σχ 9 Εγκατάσταση πιστοποιητικου για Internet Explorer(β)

Στη συνέχεια επιλέγουμε **Install Certificate**



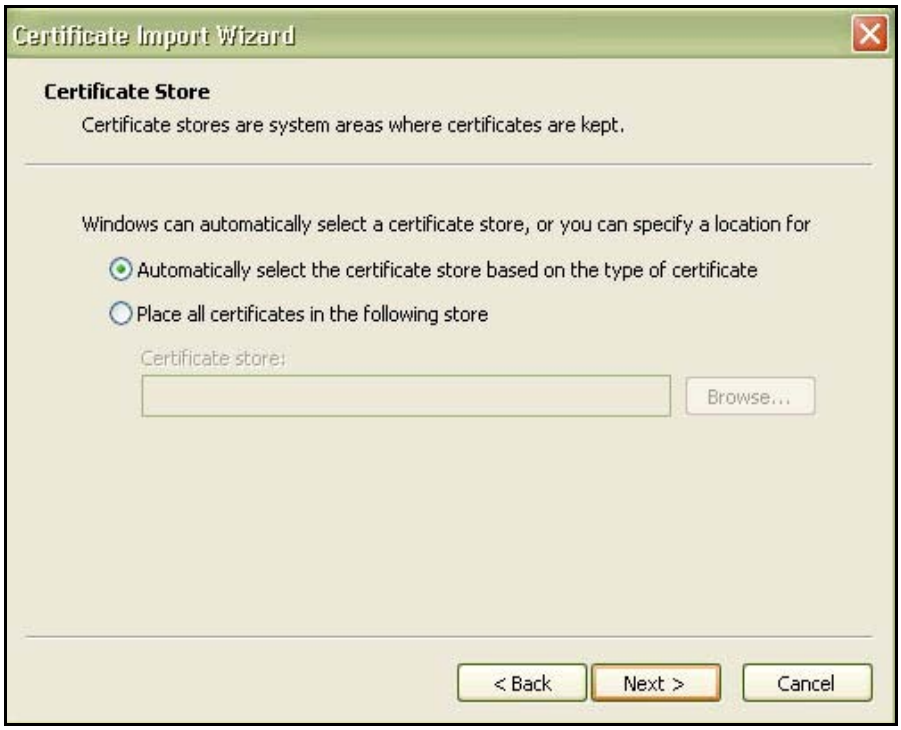
Σχ 10 Εγκατάσταση πιστοποιητικού για Internet Explorer(γ)

Ανοίγει ο οδηγός και ακολουθούμε τα βήματα εγκατάστασης. Πατάμε το κουμπί **next.**



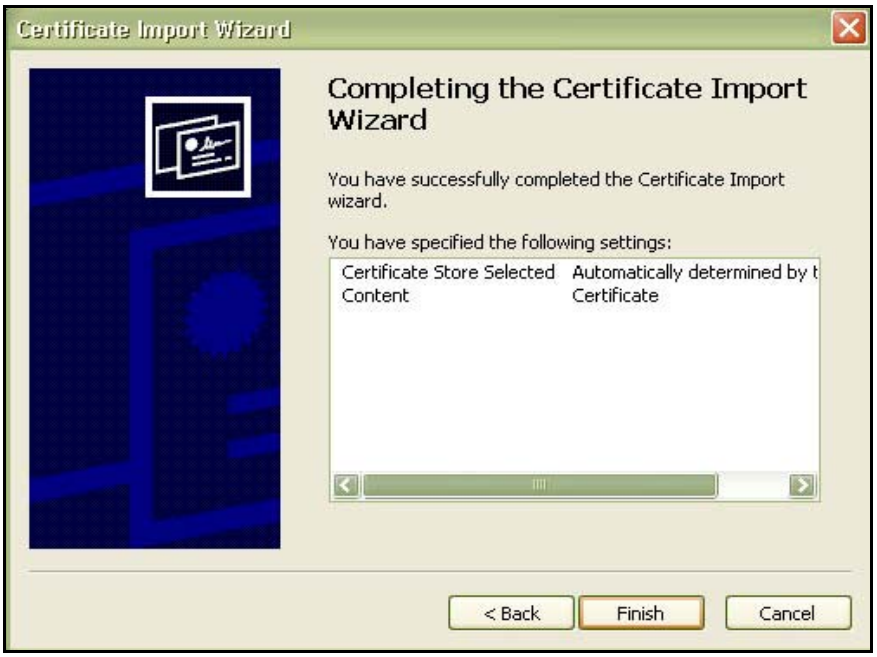
Σχ 11 Εγκατάσταση πιστοποιητικού για Internet Explorer(δ)

Συνεχίζουμε στο επόμενο παράθυρο όπου μπορούμε να επιλέξουμε αν το πιστοποιητικό θα αποθηκευτεί αυτόματα ή θα ορίσουμε εμείς την περιοχή αποθήκευσης .Επιλέγουμε αυτόματη αποθήκευση και πατάμε το κουμπί **next.**



Σχ 12 Εγκατάσταση πιστοποιητικού για Internet Explorer(ε)

Πατάμε **finish** για να τερματιστεί η διαδικασία εγκατάστασης.



Σχ 13 Εγκατάσταση πιστοποιητικού για Internet Explorer(στ)

Εμφανίζεται ένα μήνυμα προειδοποίησης οτι πρόκειται να εγκαταστήσουμε ένα πιστοποιητικό του οποίου την προέλευση δε μπορούν να εξακριβώσουν τα Windows. Αποδεχόμαστε την εγκατάσταση του πιστοποιητικού και πατάμε το κουμπί **Yes.**

Σχ 14 Εγκατάσταση πιστοποιητικού για Internet Explorer(ζ)

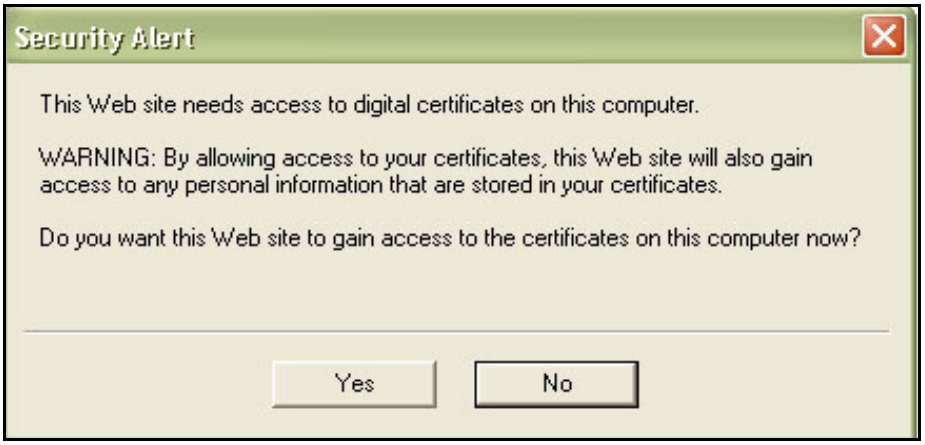
Τέλος μας εμφανίζει ένα μηνυμα οτι η εγκατάσταση είναι επιτυχής.

Σχ 15 Εγκατάσταση πιστοποιητικού για Internet Explorer(η)

Κατόπιν από το σύνδεσμο στην παράγραφο **Έλεγχος Εγκατάστασης Πιστοποιητικού»** διαπιστώνουμε αν έχουμε εμπιστευθεί την Αρχή Πιστοποίησης HARICA

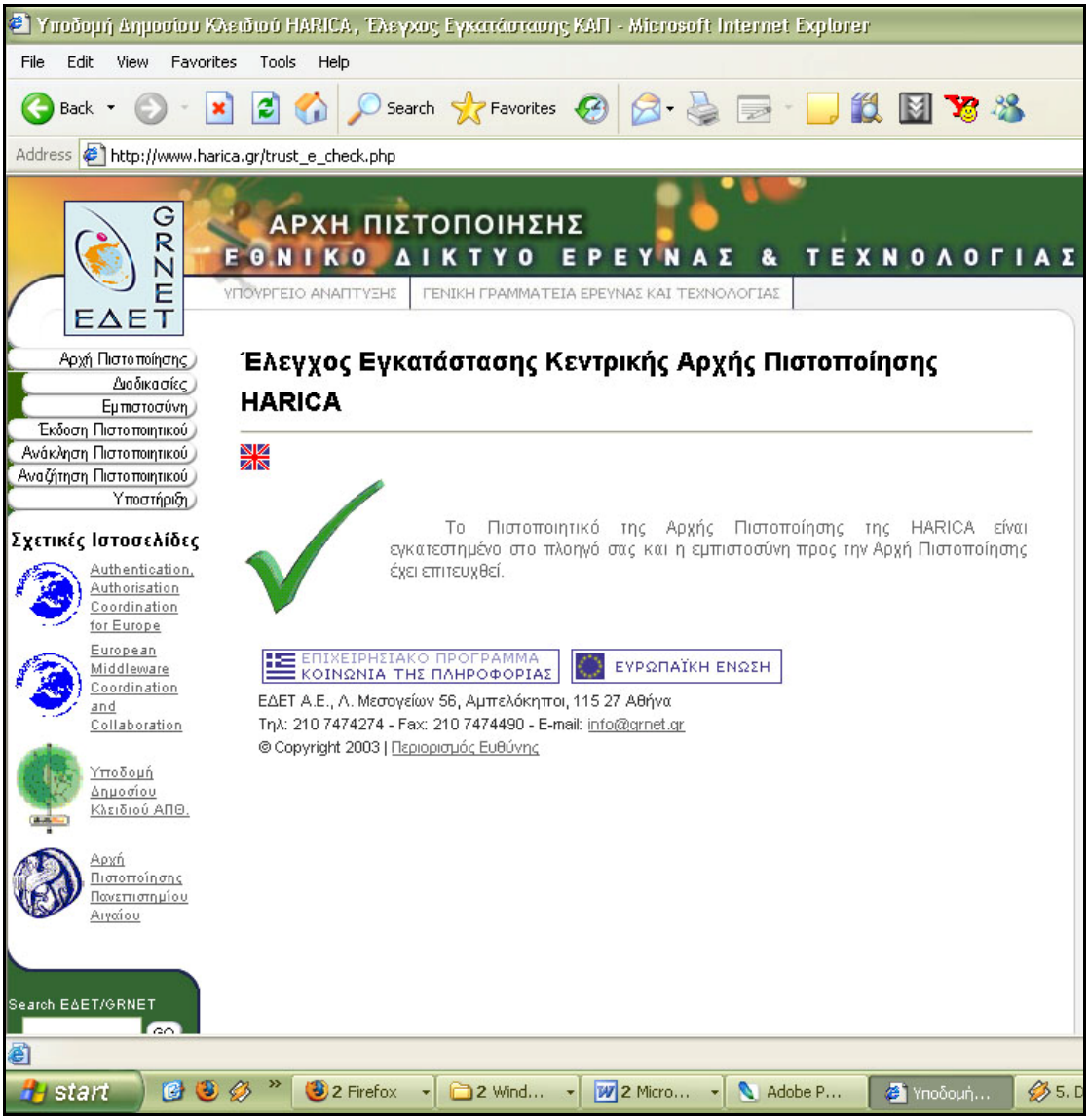
Σχ 16 Έλεγχος ύπαρξης πιστοποιητικού στο browser(α)

Εμφανίζει προειδοποιητικό μήνυμα οτι η ιστοσελίδα αυτή ζητάει πρόσβαση στα ψηφιακά πιστοποιητικά του υπολογιστή και σε όποια προσωπική πληροφορία υπάρχει σε αυτά. Επιτρέπουμε την πρόσβαση και πατάμε το κουμπί **yes.**



Σχ17. Έλεγχος ύπαρξης πιστοποιητικού στο browser(β)

Επιβεβαιώνεται τέλος η ύπαρξη του πιστοποιητικού στον browser.



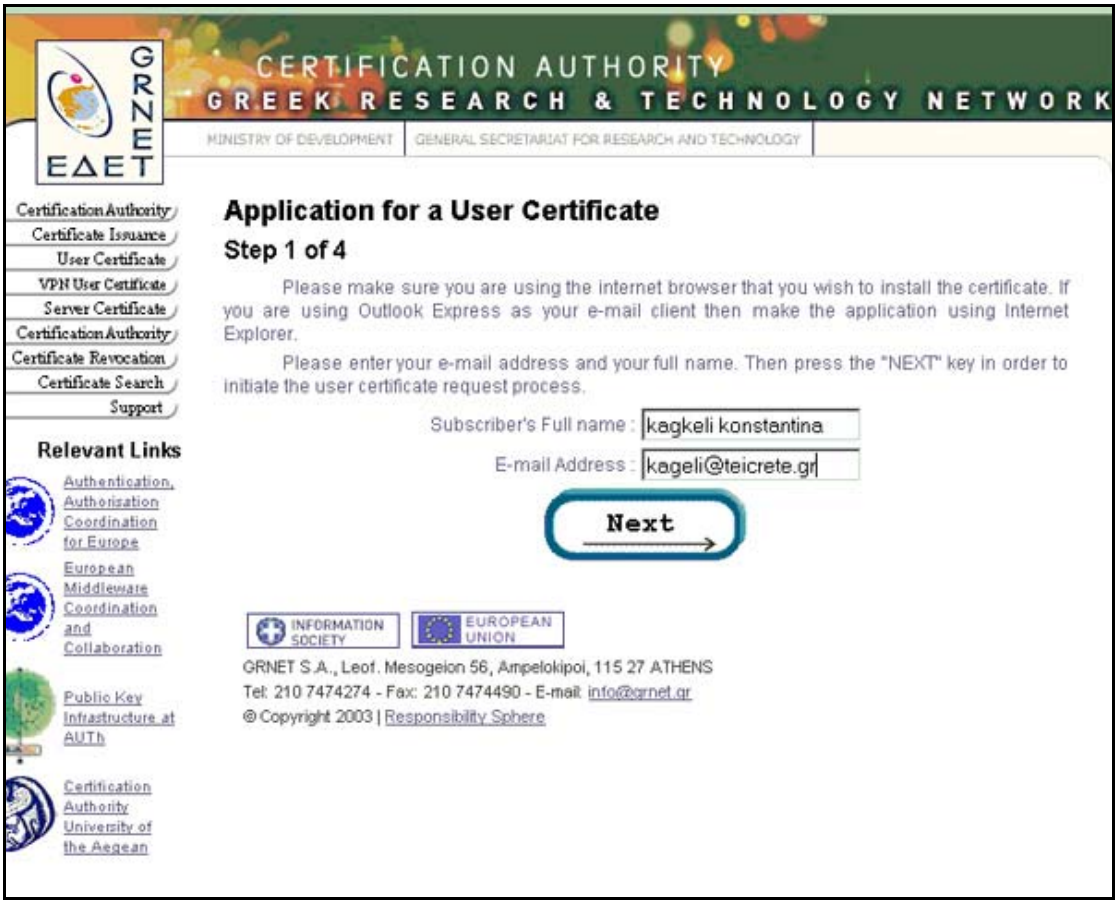
Σχ18 Επιβεβαίωση ύπαρξης πιστοποιητικού στο browser

Παράρτημα Γ

Οδηγίες για την αίτηση πιστοποιητικού χρήστη

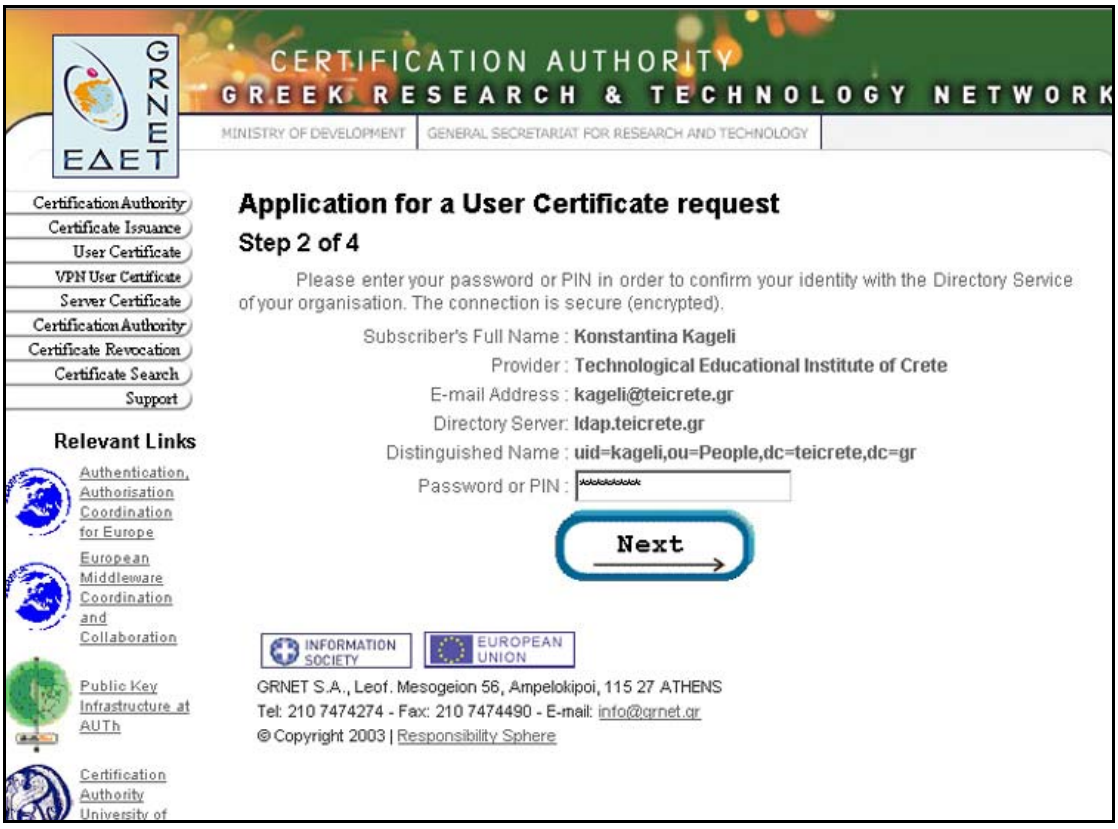
Ο browser που θα χρησιμοποιηθεί πρέπει να έχει εγκατεστημένο το πιστοποιητικό της HARICA. Στην περιπτωσή μας χρησιμοποιούμε Mozilla Firefox.

Αρχικά επισκεπτόμαστε τη σελίδα της HARICA και από το αριστερό μενού επιλέγουμε **Έκδοση πιστοποιητικού για χρήστη.** Ο σύνδεσμος αυτός μας μεταφέρει στη σελίδα με το πρώτο βήμα της αίτησης. Δίνουμε το ονοματεπώνυμο του χρήστη και το email του. Πατάμε **next** .



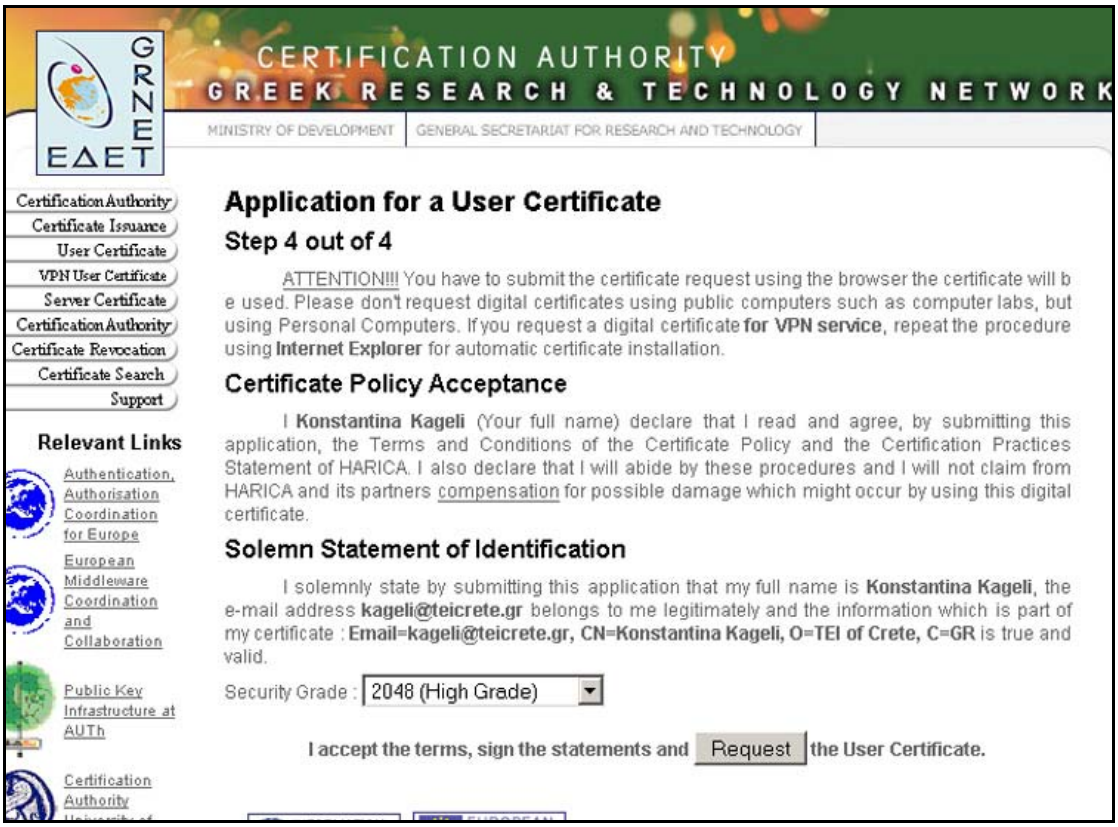
Σχήμα 1. Εισαγωγή στοιχείων χρήστη.

Αφού γίνει έλεγχος για την ύπαρξη του χρήστη στην υπηρεσία καταλόγου του ιδρύματος, εμφανίζει τα στοιχεία του όπως αυτά είναι αποθηκευμένα στον ldap.teicrete.gr. Σ᾽αυτό το βήμα δίνουμε τον κωδικό χρήστη και πατάμε **next.**



Σχήμα 2. Εισαγωγή κωδικού χρήστη.

Στο τελικό βήμα η υπηρεσία μας ενημερώνει ότι πρόκειται να αιτηθούμε πιστοποιητικό χρήστη, το οποίο θα το χρησιμοποιούμε απο το συγκεκριμένο browser. Μας ζητάει να αποδεχτούμε τους όρους της Δήλωσης Διαδικασιών Πιστοποίησης της HARICA. Επίσης μας ζητά να ορίσουμε το μέγεθος του κλειδιού που θα δημιουργηθεί και αφήνουμε την επιλογή στο *2048* για μεγαλύτερη ασφάλεια. Πατώντας **request** κατατίθεται το αίτημα.

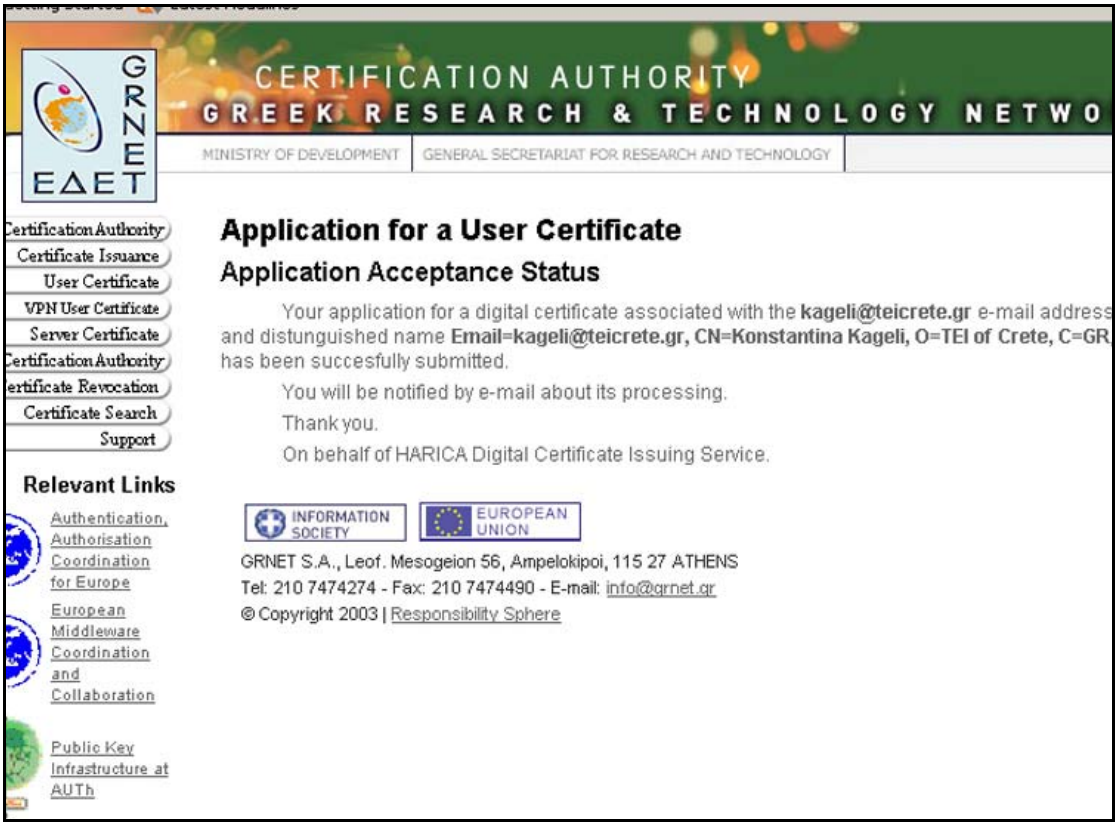


Σχήμα 3. Κατάθεση αιτήματος.

Σε αυτό το σημείο μας ζητείται από το browser να ορίσουμε ένα *master password* για την προστασία του ιδιωτικού κλειδιού, το οποίο θα αποθηκευτεί σε αυτόν. Παρατηρούμε ότι εμφανίζεται μια μπάρα που δείχνει πόσο ισχυρός είναι ο κωδικός που δώσαμε. Πατάμε **ok**.

Σχήμα 4. Δημιουργία master password.

Τέλος, μας ενημερώνει ότι υποβλήθηκε επιτυχώς το αίτημα μας και θα ειδοποιηθούμε μέσω email για την παραλαβή του πιστοποιητικού.



Σχήμα 5. Επιβεβαίωση κατάθεσης αίτησης.

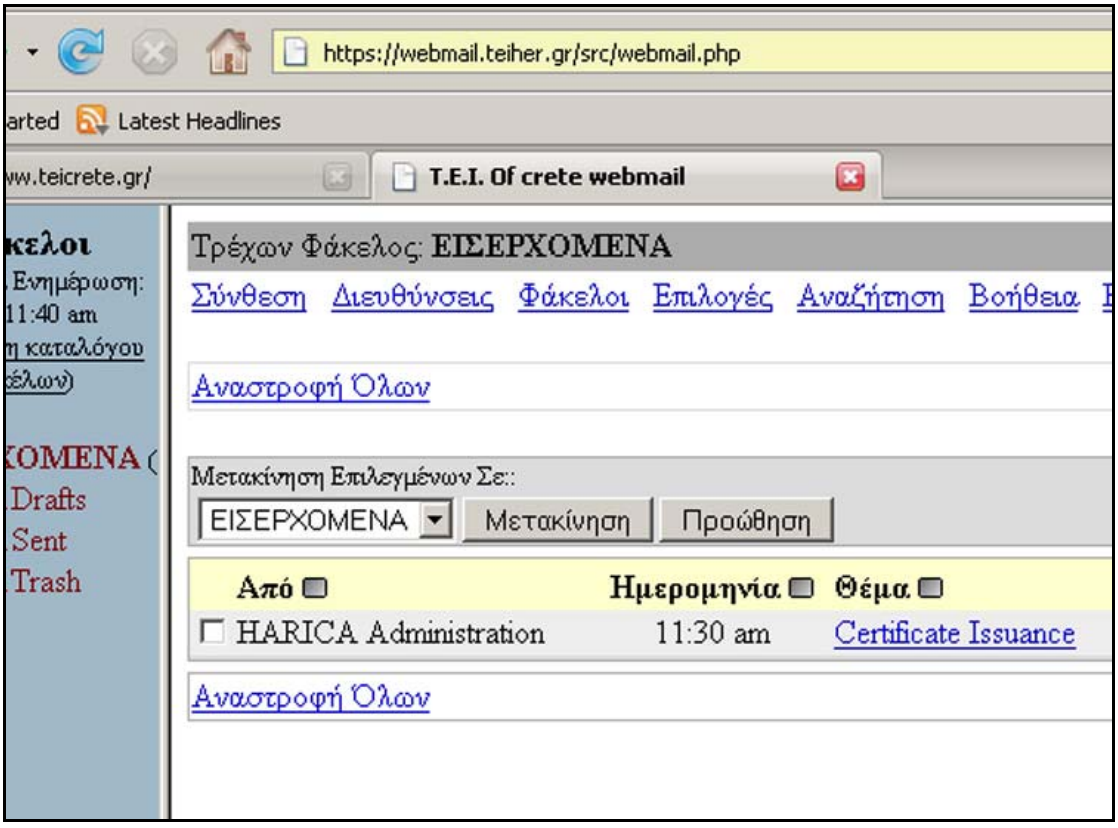
Ακολουθώντας ακριβώς την ίδια διαδικασία μπορούμε να αιτηθούμε πιστοποιητικό χρησιμοποιώντας τον Internet Explorer.

Παράρτημα Δ

Οδηγίες για την παραλαβή του πιστοποιητικού χρήστη

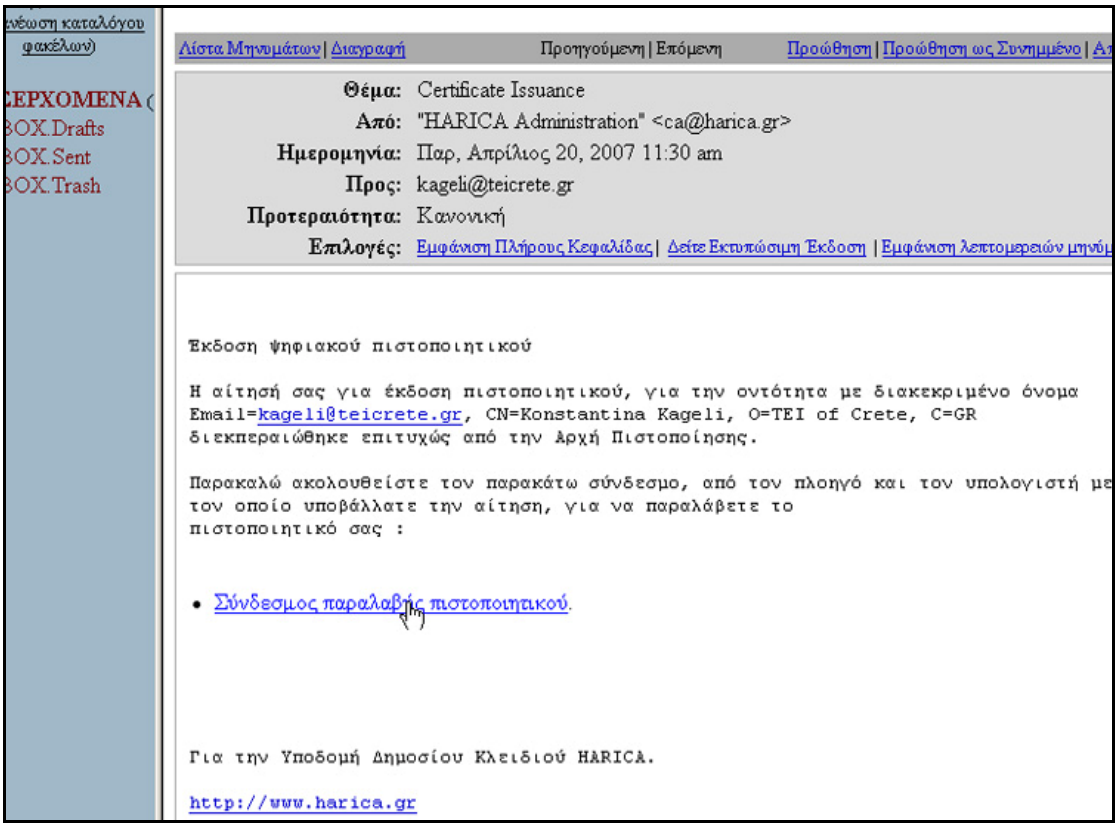
Μετά την κατάθεση της αίτησης και αφού αυτή ελέγχθηκε και υπογράφηκε από την Αρχή Πιστοποίησης, ειδοποιούμαστε με email για την παραλαβή του πιστοποιητικού.

Μπαίνουμε στο λογαριασμό email και βλέπουμε το μήνυμα που έχει έρθει από τη HARICA.



Σχήμα 1. Email παραλαβής πιστοποιητικού.

Ανοίγουμε το email και πατάμε το σύνδεσμο παραλαβής του πιστοποιητικού.



Σχήμα 2. Σύνδεσμος παραλαβής πιστοποιητικού.

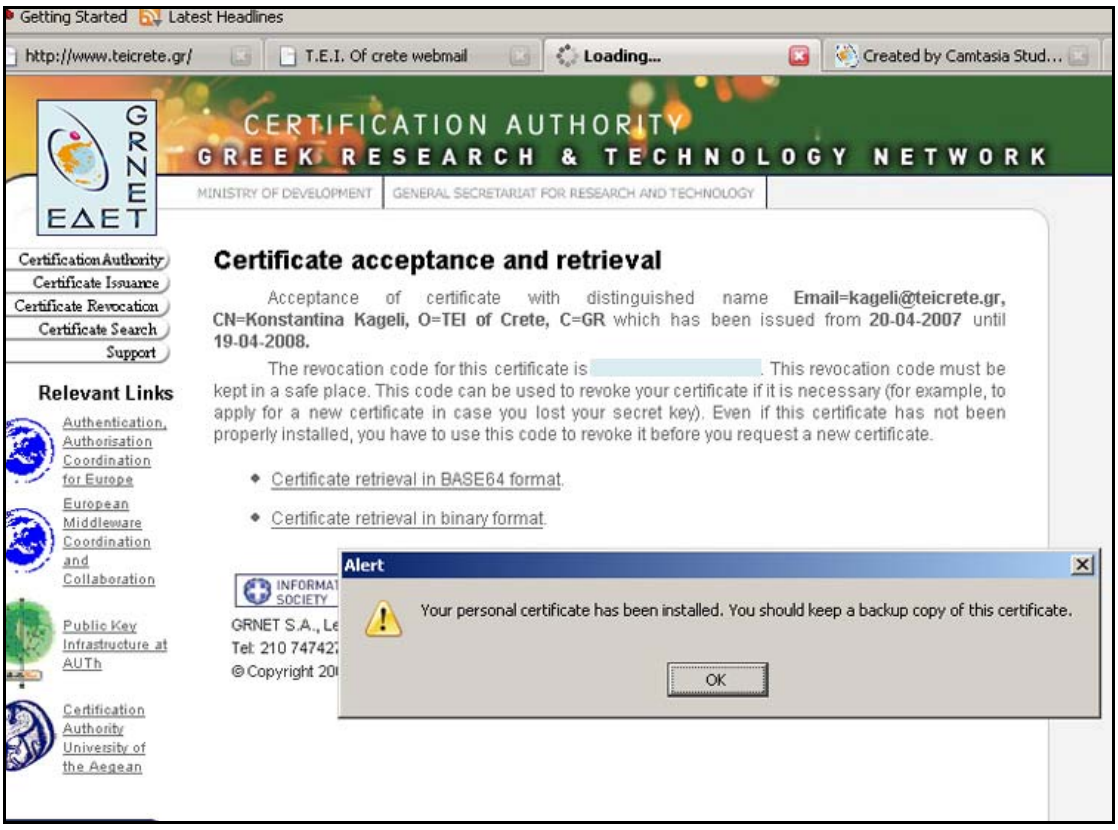
Μεταφερόμαστε στη σελίδα για την αποδοχή και παραλαβή του πιστοποιητικού.Εδώ η υπηρεσία μας ενημερώνει για τα στοιχεία του πιστοποιητικού που πρόκειται να παραλάβουμε, πότε εκδόθηκε και πότε λήγει. Από το σχετικό σύνδεσμο αποδεχόμαστε το πιστοποιητικό.

Σχήμα 3. Παραλαβή πιστοποιητικού.

Η υπηρεσία μας ενημερώνει με μήνυμα, οτι το πιστοποιητικό έχει εγκατασταθεί αυτόματα στο browser και ότι από εκεί θα πρέπει να κρατήσουμε ένα αντίγραφο ασφαλείας .

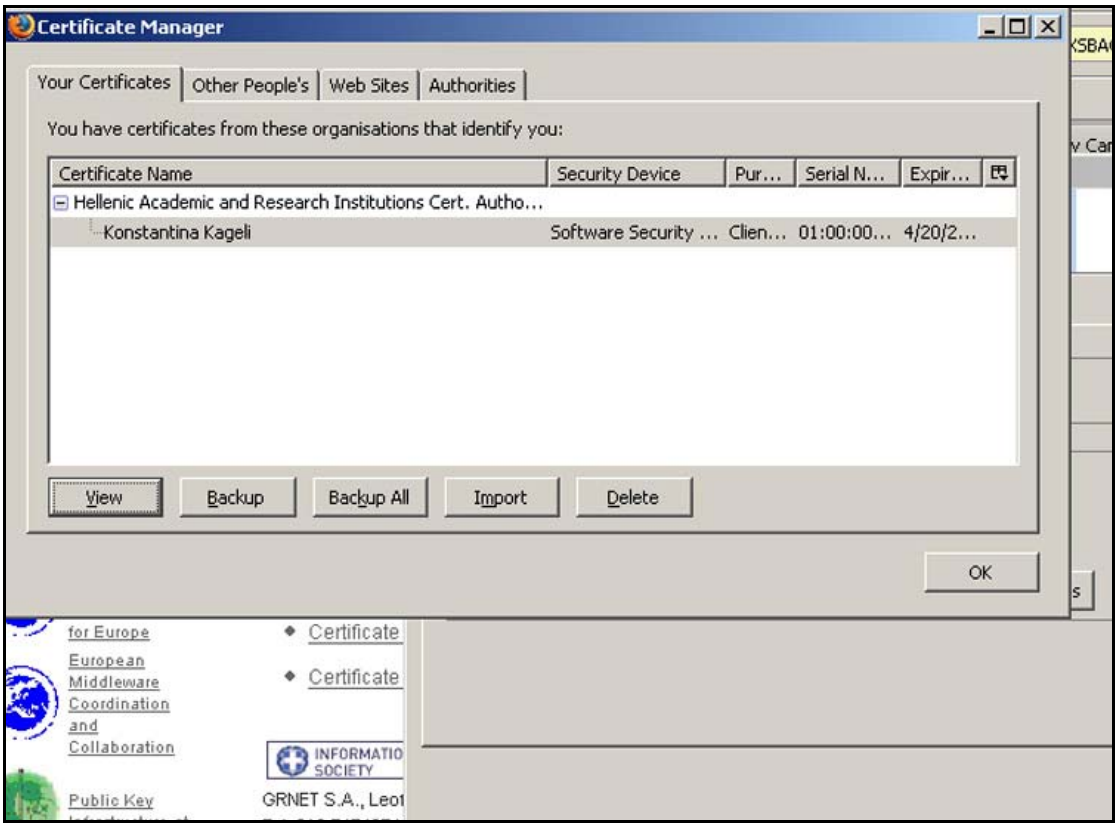
Στη σελίδα αυτή εμφανίζονται τα στοιχεία του πιστοποιητικού και ο μυστικός κωδικός ανάκλησης.

Τέλος, μπορούμε να κρατήσουμε ένα απλό αντίγραφο του πιστοποιητικού μας σε BASE64 ή δυαδική μορφή.



Σχήμα 4. Κωδικός ανάκλησης και αντίγραφο πιστοποιητικού.

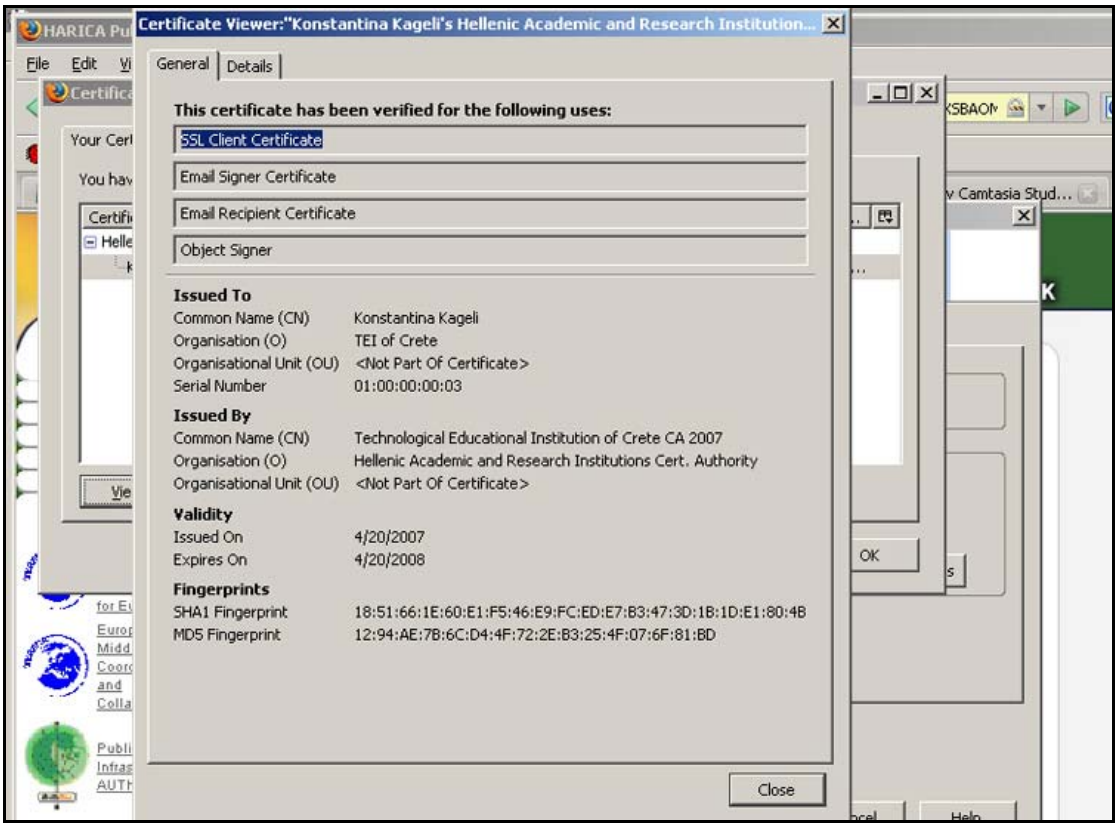
Αν θέλουμε να δούμε το πιστοποιητικό στο browser που είμαστε, πηγαίνουμε
Tools / **Options**, από το μενού επιλέγουμε **Advanced** , στην καρτέλα **Encryption**, πατάμε το κουμπί **View certificates** και βλέπουμε το πιστοποιητικό να είναι εγκατεστημένο στα προσωπικά πιστοποιητικά.



Σχήμα 5. Το πιστοποιητικό χρήστη στο browser.

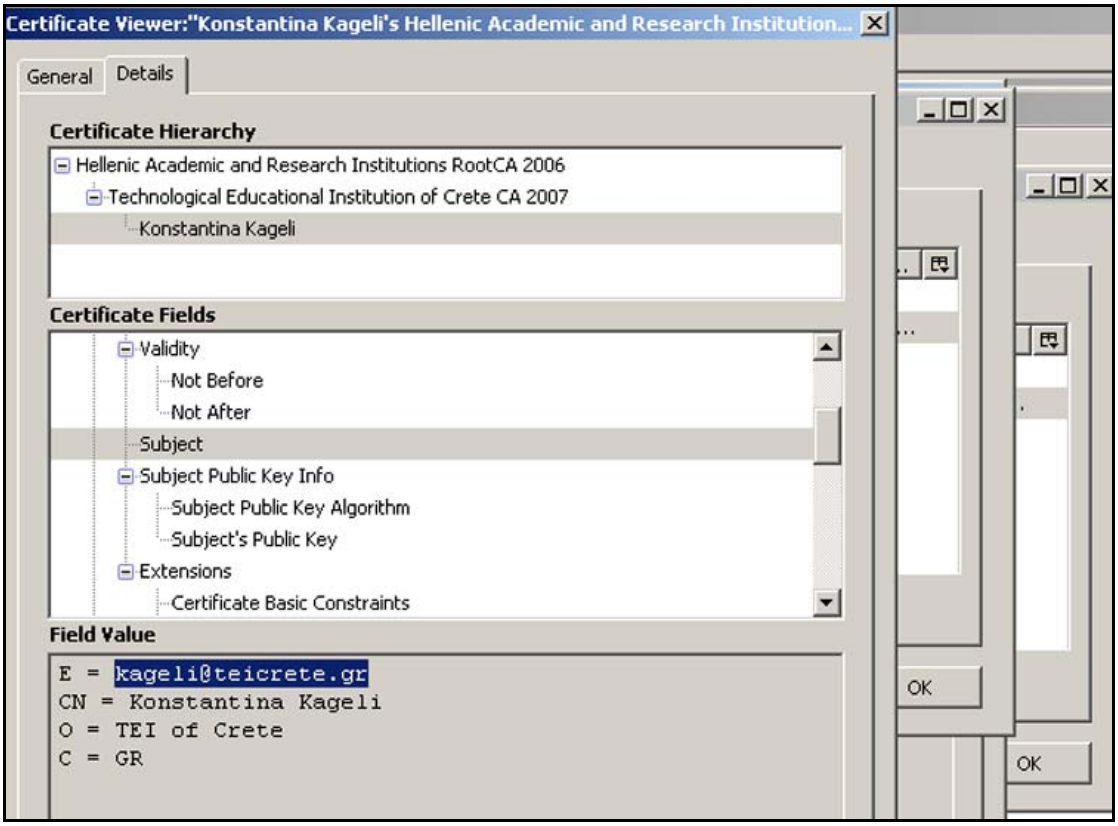
Για να δούμε τις λεπτομέρειες του πιστοποιητικού πατάμε το κουμπί **View** .

Στην καρτέλα **General** βλέπουμε για ποιον έχει εκδοθεί το πιστοποιητικό, ότι ο χρήστης ανήκει στο ΤΕΙ Κρήτης, πότε εκδόθηκε και πότε λήγει το πιστοποιητικό, από ποια Αρχή υπογράφηκε, και το μοναδικό αποτύπωμα του πιστοποιητικού.



Σχήμα 6. Στοιχεία πιστοποιητικού.

Στην καρτέλα **Details** βλέπουμε τα στοιχεία του πιστοποιητικού με περισσότερες λεπτομέρειες.



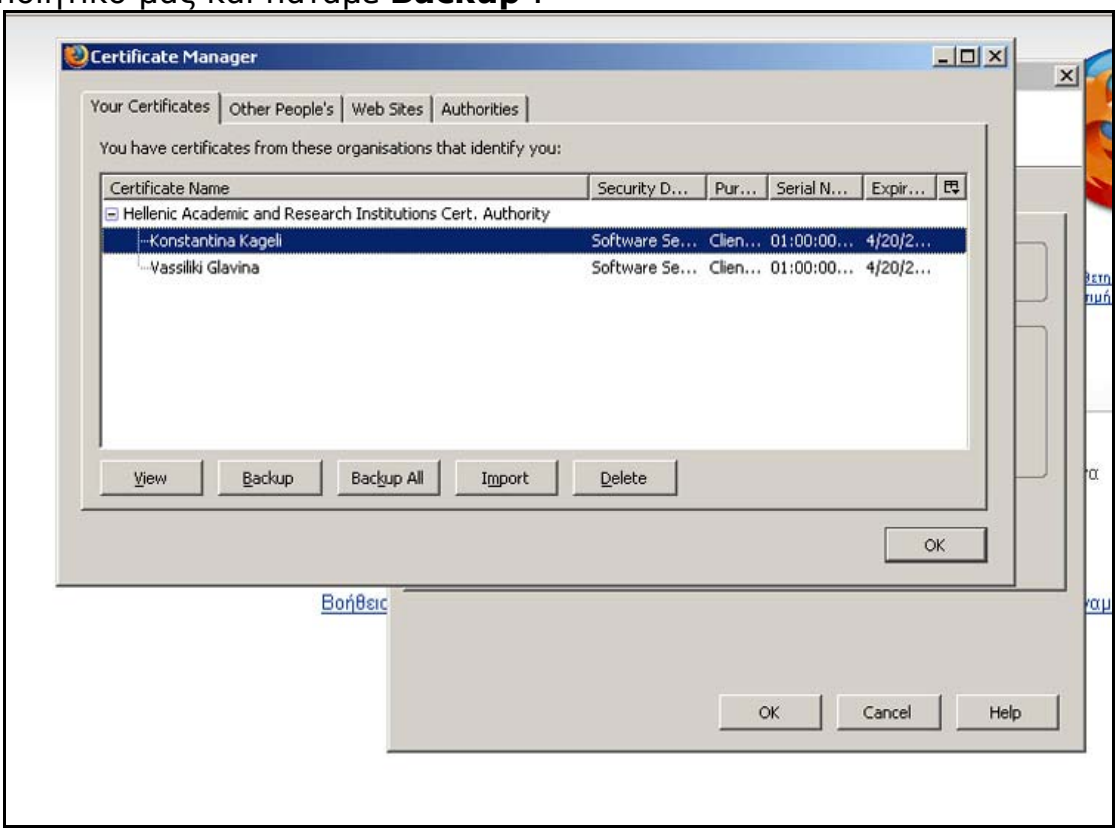
Σχήμα 7. Λεπτομέρειες πιστοποιητικού.

Παράρτημα Ε

Οδηγίες για την δημιουργία backup αρχείου του ψηφιακού πιστοποιητικού

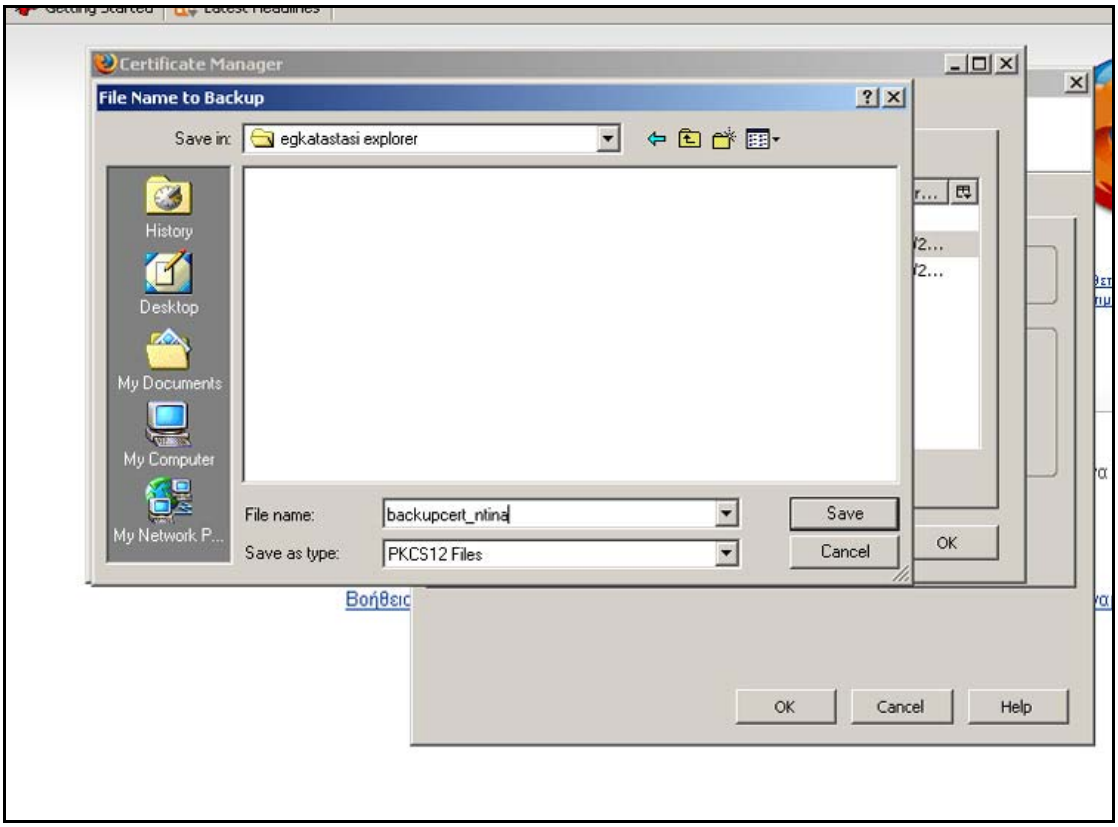
Backup αρχείο μπορούμε να δημιουργήσουμε μόνο για προσωπικά πιστοποιητικά γιατί χρειάζεται ο μυστικός κωδικός προστασίας του ιδιωτικού κλειδιού (master password).

Στο browser που έχουμε αποθηκευμένο το προσωπικό μας πιστοποιητικό, στην περίπτωσή μας το Mozilla Firefox, από το μενού πηγαίνουμε **Tools** / **Options**, επιλέγουμε **Advanced**, στην καρτέλα **Encryption** πατάμε το κουμπί **View Certificates** και στην καρτέλα **Your Certificates** . Εκεί επιλέγουμε το πιστοποιητικό μας και πατάμε **Backup** .



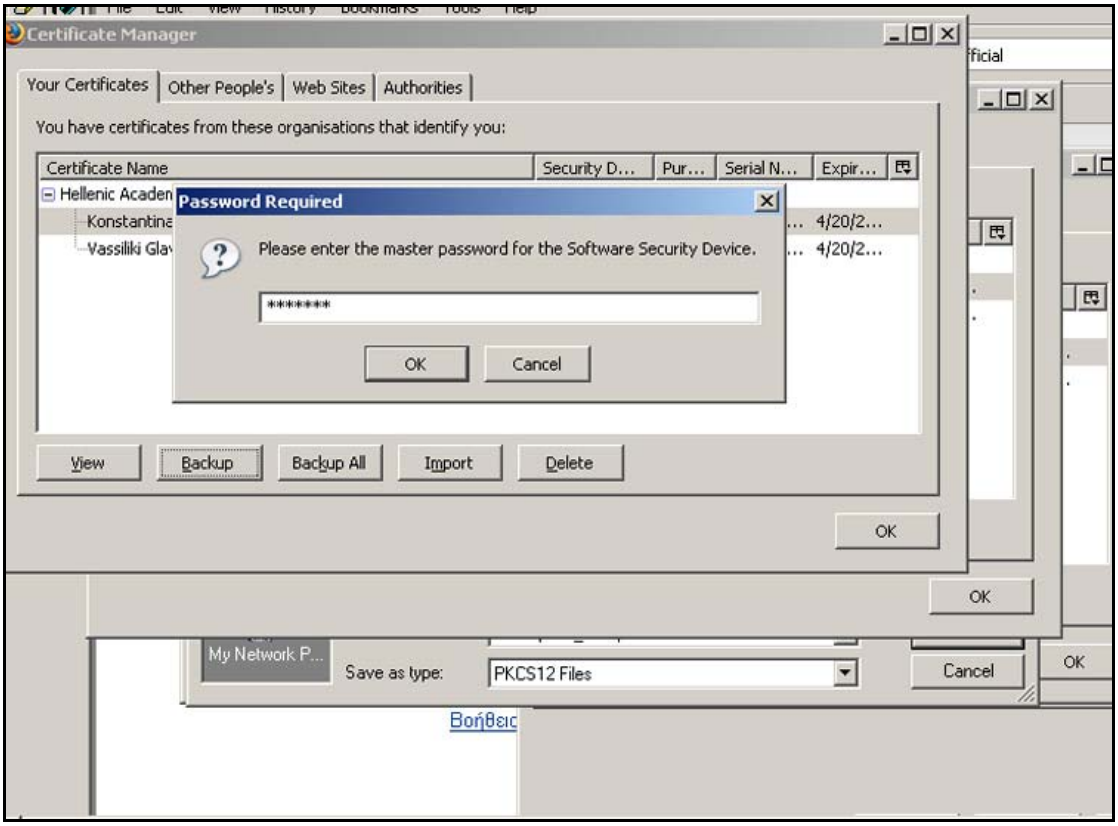
Σχήμα 1. Δημιουργία backup αρχείου.

Ορίζουμε το όνομα με το οποίο θέλουμε να αποθηκευτεί το αρχείο και την τοποθεσία που θα αποθηκευτεί. Πατάμε **Save** .



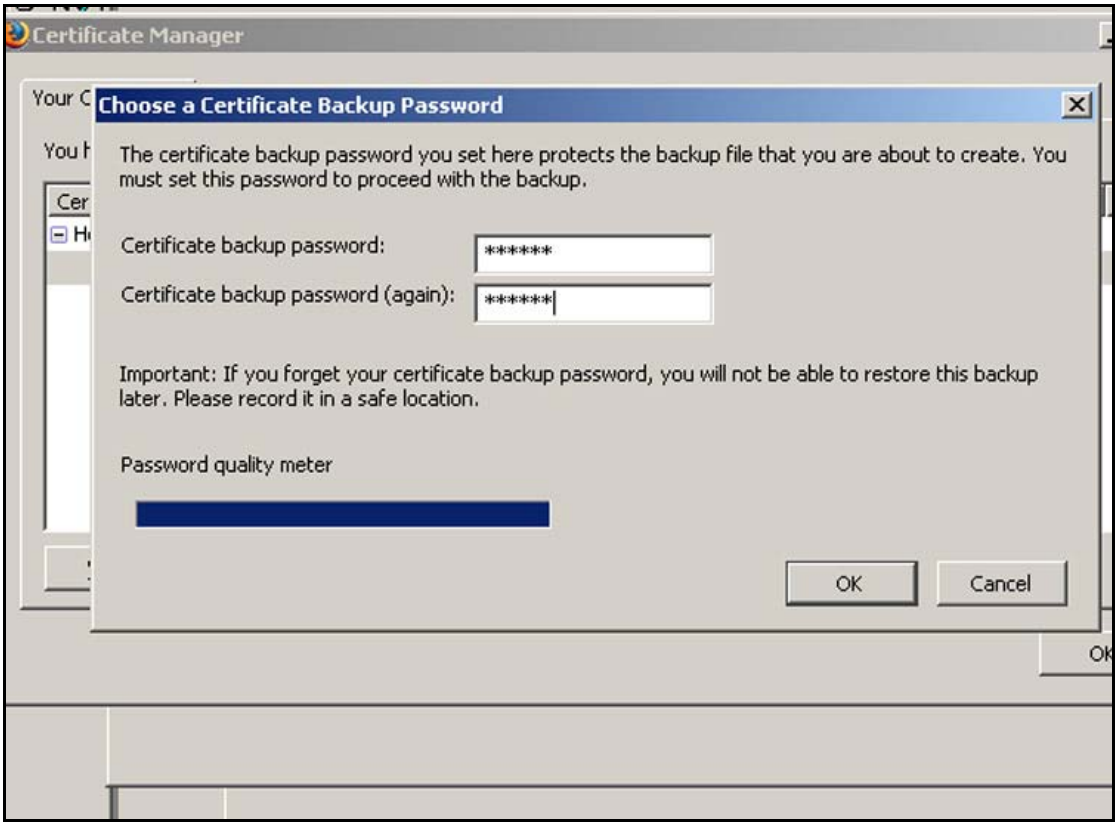
Σχήμα 2. Ορισμός ονόματος και τοποθεσίας αποθήκευσης.

Σε αυτό το σημείο πρέπει να δώσουμε το master password.



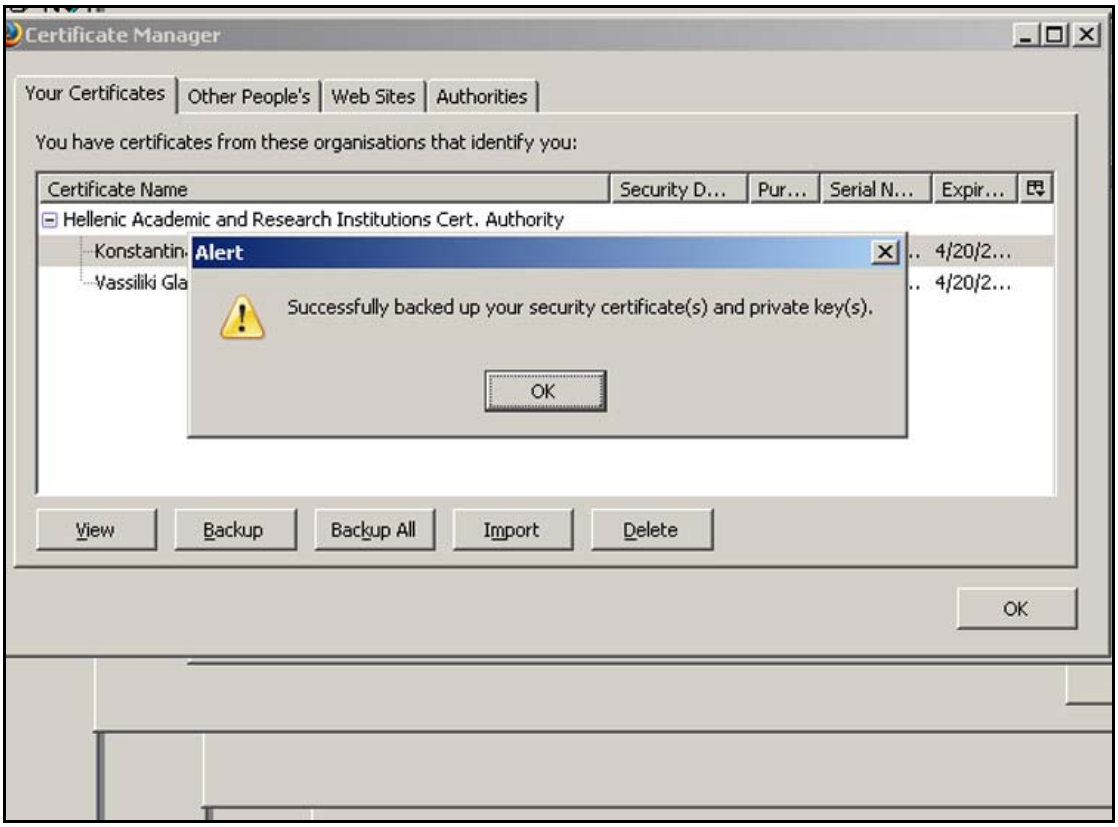
Σχήμα 3. Εισαγωγή master password.

Στη συνέχεια μας ζητείται να ορίσουμε έναν κωδικό για την προστασία του backup αρχείου. Σε περίπτωση που ξεχάσουμε αυτόν τον κωδικό δε θα μπορούμε να χρησιμοποιήσουμε το αρχείο. Για το λόγο αυτό θα πρέπει να το έχουμε σε κάποια ασφαλή τοποθεσία.



Σχήμα 4. Ορισμός Certificate backup password.

Τέλος ειδοποιούμαστε οτι το backup αρχείο του πιστοποιητικού με το ιδιωτικό κλειδί, έχει δημιουργηθεί με επιτυχία.



Σχήμα 5. Μήνυμα επιβεβαίωσης δημιουργίας backup αρχείου.

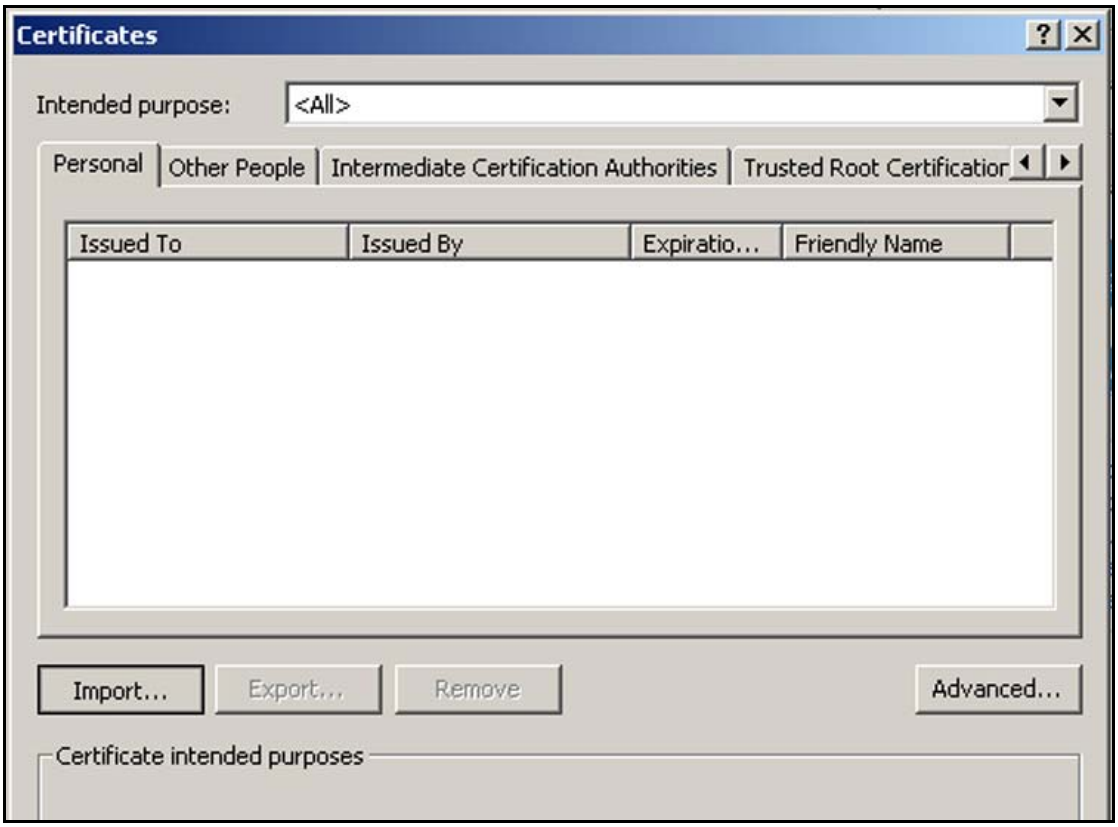
Παράρτημα Ζ

Οδηγίες εγκατάστασης προσωπικού πιστοποιητικού σε άλλο browser

Για να εγκαταστήσουμε το πιστοποιητικό μας σε κάποιον άλλο browser από αυτόν με τον οποίο το παραλάβαμε, πρέπει να χρησιμοποιήσουμε το backup αρχείο του.

- Internet Explorer

Στη συγκεκριμένη περίπτωση το εφαρμόζουμε στον Internet Explorer. Από το μενού **Tools** / **Internet Options**, επιλέγουμε την καρτέλα **Content**, πατάμε το κουμπί **Certificates** και στην καρτέλα **Personal** πατάμε **Import**.

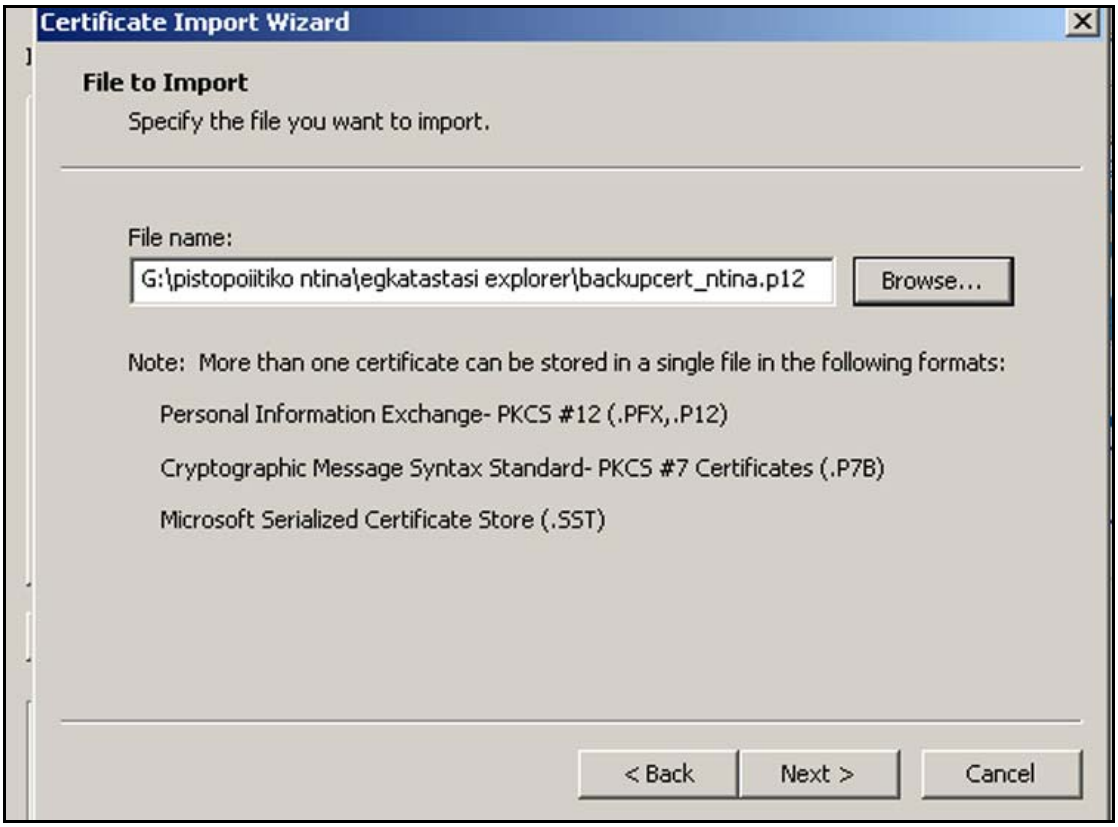


Σχήμα 1. Εισαγωγή προσωπικού πιστοποιητικού.

Έχοντας πατήσει Import ξεκινάει ο οδηγός εγκατάστασης πιστοποιητικών του Internet Explorer. Πατάμε **next.**

Σχήμα 2. Οδηγός εγκατάστασης πιστοποιητικού.

Πατώντας browse εντοπίζουμε την τοποθεσία που έχουμε αποθηκεύσει το backup αρχείο και πατάμε **Open** για να μπει το path στον οδηγό. Πατάμε **next .**

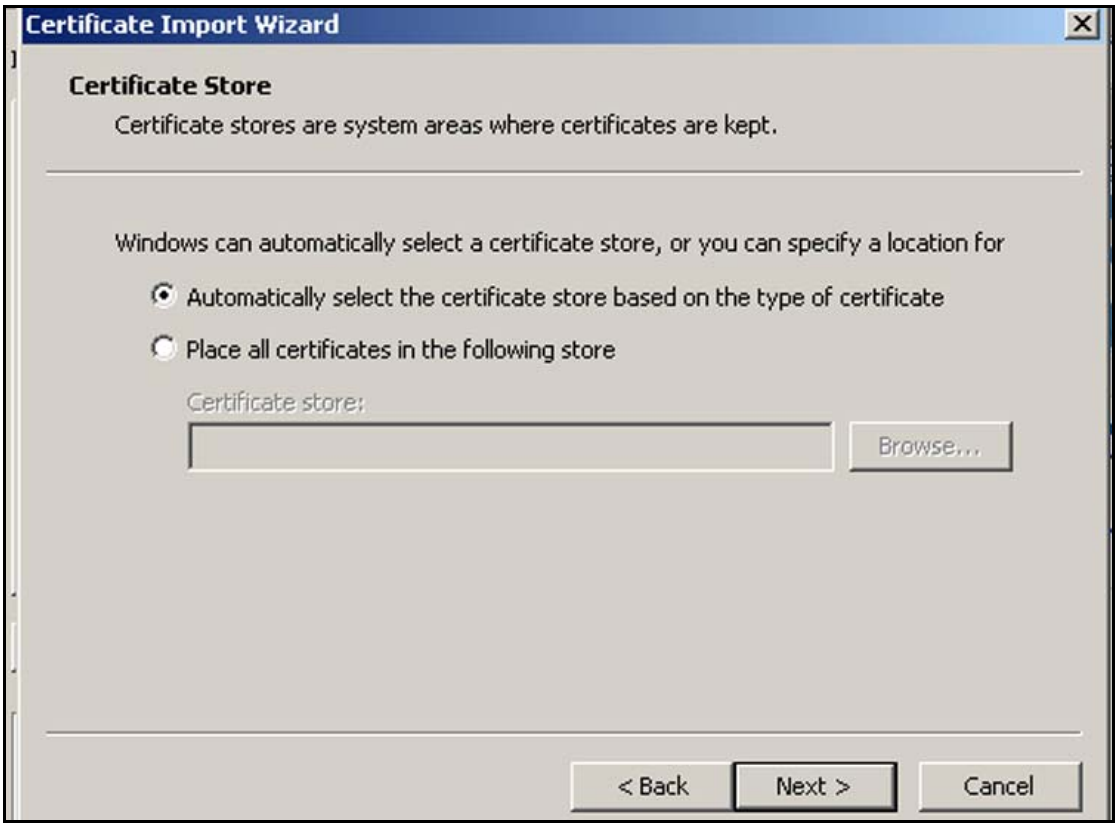


Σχήμα 3. Εισαγωγή backup αρχειου στον οδηγό εγκατάστασης.

Στη συνέχεια πρέπει να δώσουμε τον κωδικό που είχαμε ορίσει για την προστασία του backup αρχείου. Σε αυτό το σημείο μπορούμε να επιλέξουμε κάθε φορά που μια εφαρμογή χρησιμοποιεί το προσωπικό μας κλειδί να ειδοποιούμαστε με μήνυμα, τσεκάροντας την αντίστοιχη επιλογή. Ακόμα, με τον ίδιο τρόπο, μπορούμε να ορίσουμε να υπάρχει δυνατότητα εξαγωγής για το προσωπικό κλειδί.
Μετά πατάμε **next.**

Σχήμα 4. Εισαγωγή κωδικού προστασίας του αρχείου.

Ο οδηγός εγκατάστασης μας ζητάει να ορίσουμε αν η τοποθεσία αποθήκευσης θα επιλεγεί αυτόματα ή θα την ορίσουμε εμείς. Αφήνουμε την αυτόματη επιλογή. Πατάμε **next.**



Σχήμα 5. Επιλογή τοποθεσίας αποθήκευσης πιστοποιητικού.

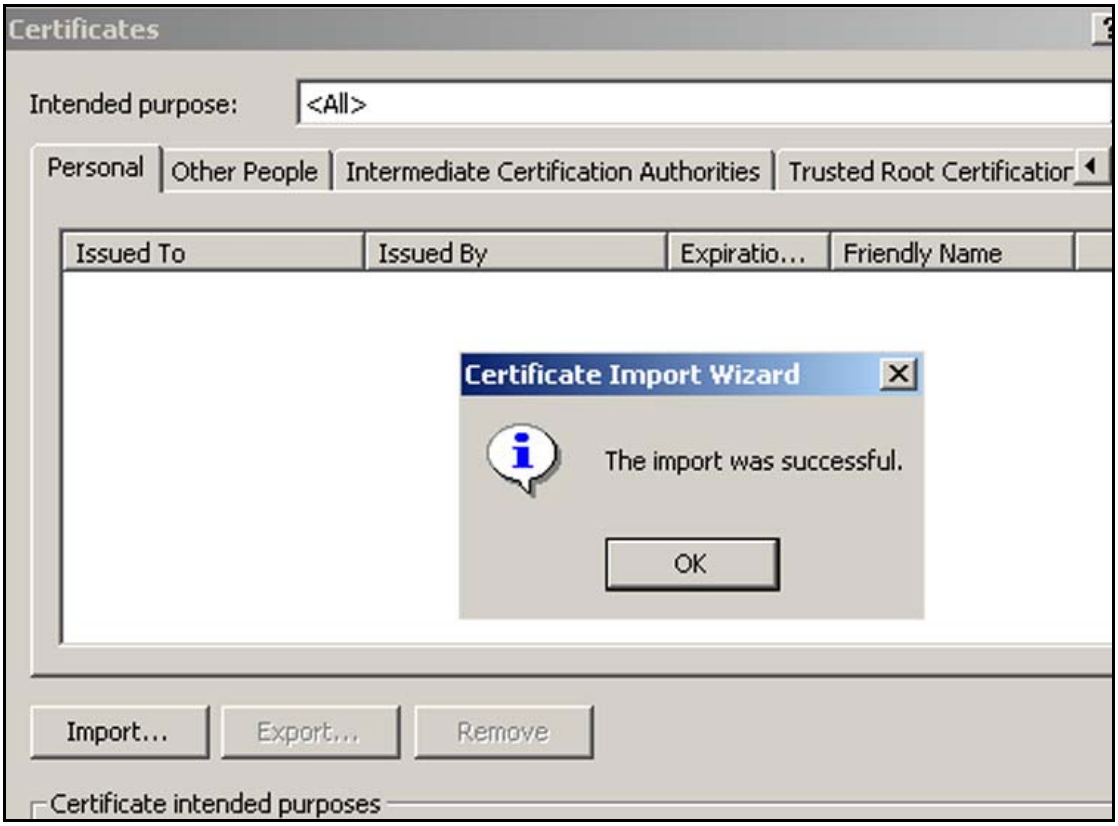
Ο οδηγός μας ενημερώνει για την ολοκλήρωση της εγκατάστασης του πιστοποιητικού. Πατάμε **Finish** .

Σχήμα 6. Ολοκλήρωση εγκατάστασης πιστοποιητικκού.

Εμφανίζεται ένα μήνυμα προειδοποίησης ότι κάποιο πρόγραμμα προσπαθεί να έχει πρόσβαση στο ιδιωτικό μας κλειδί. Μπορούμε να ορίσουμε στο **Set Security Level** το επίπεδο ασφαλείας ώστε κάθε φορά που κάποια εφαρμογή ζητάει πρόσβαση στο ιδιωτικό κλειδί να εμφανίζει απλά ένα προειδοποιητικό μήνυμα(Medium Level) ή να ζητάει και κωδικό(High Level). Αφού ορίσουμε το επίπεδο ασφαλείας πατάμε **ok.**

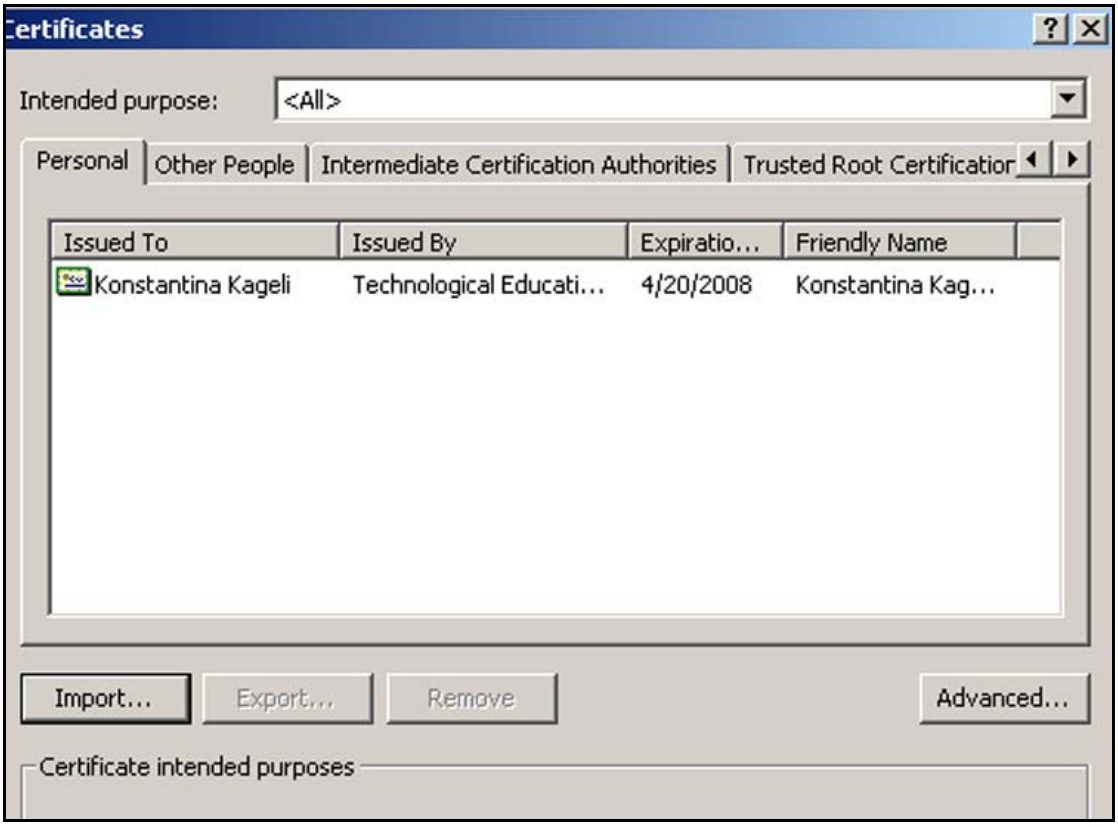
Σχήμα 7. Μήνυμα προειδοποίησης για χρήση του ιδιωτικού κλειδιού.

Ο οδηγός εγκατάστασης μας ενημερώνει για την επιτυχή εισαγωγή του πιστοποιητικού και κλείνει. Πατάμε **ok**.



Σχήμα 8. Ολοκλήρωση εισαγωγής πιστοποιητικού.

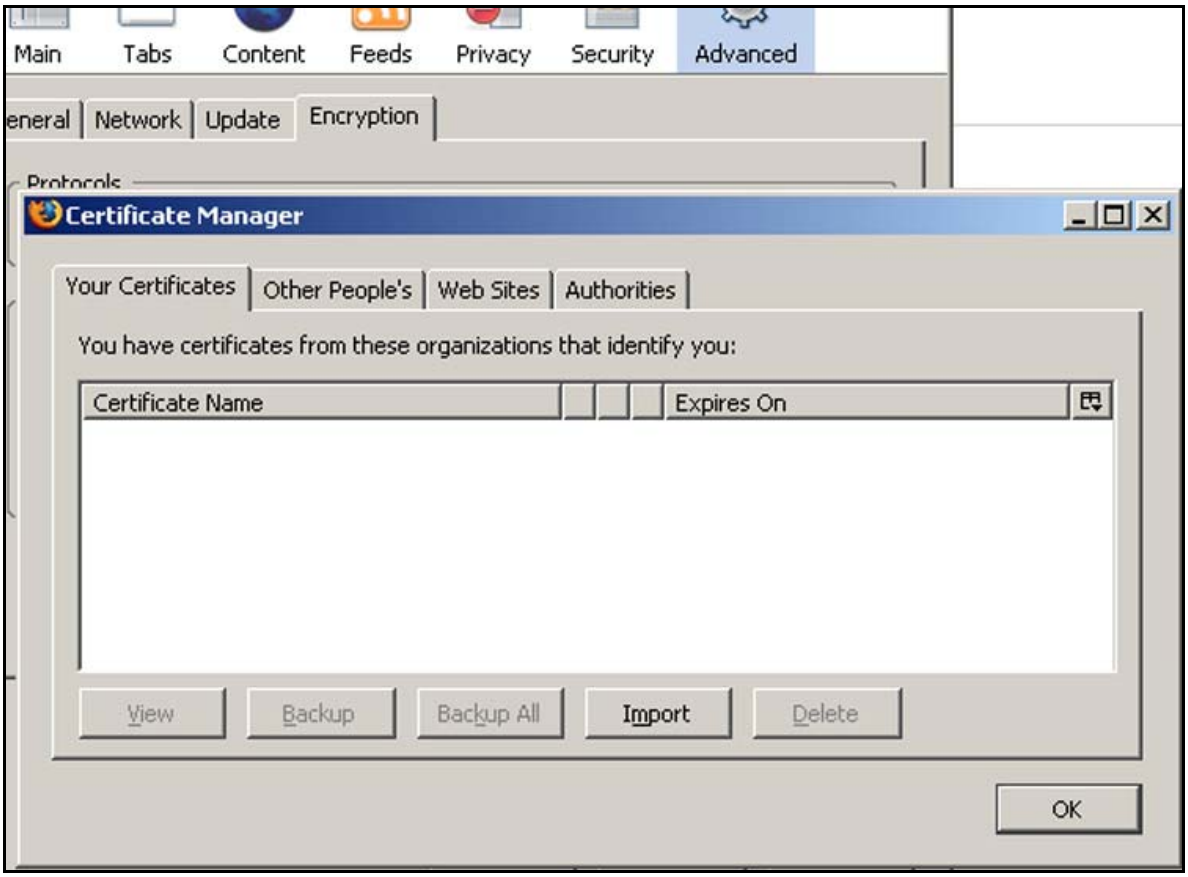
Τέλος, βλέπουμε το πιστοποιητικό εγκατεστημένο στα προσωπικά πιστοποιητικά του browser.



Σχήμα 9. Παρουσία πιστοποιητικού στα προσωπικά πιστοποιητικά.

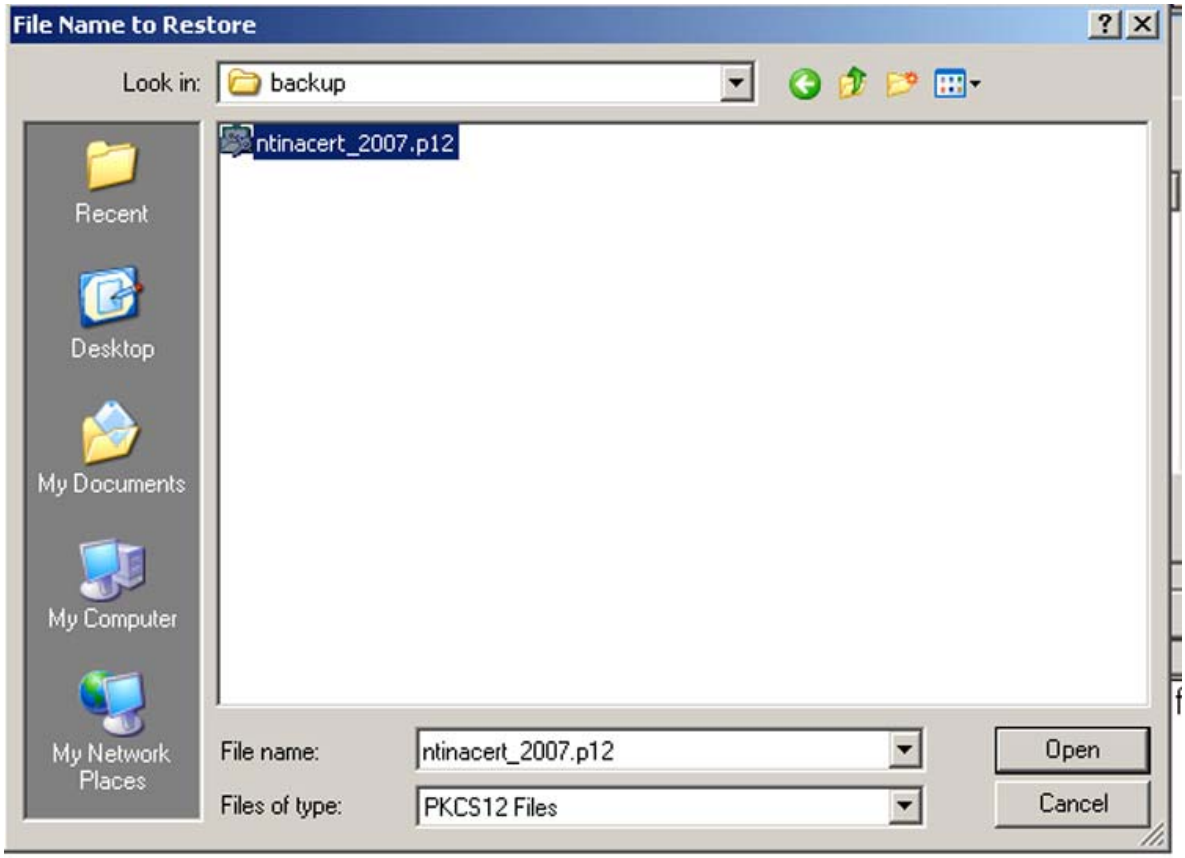
- Mozilla Firefox

Στη περίπτωση που θέλουμε να εγκαταστήσουμε το προσωπικό πιστοποιητικό του χρήστη στο Mozilla Firefox, από το μενού πηγαίνουμε **Tools** / **Options**, επιλέγουμε **Advanced**, στην καρτέλα **Encryption** πατάμε το κουμπί **View Certificates** και στην καρτέλα **Yours Certificates** πατάμε το κουμπί **Import**.



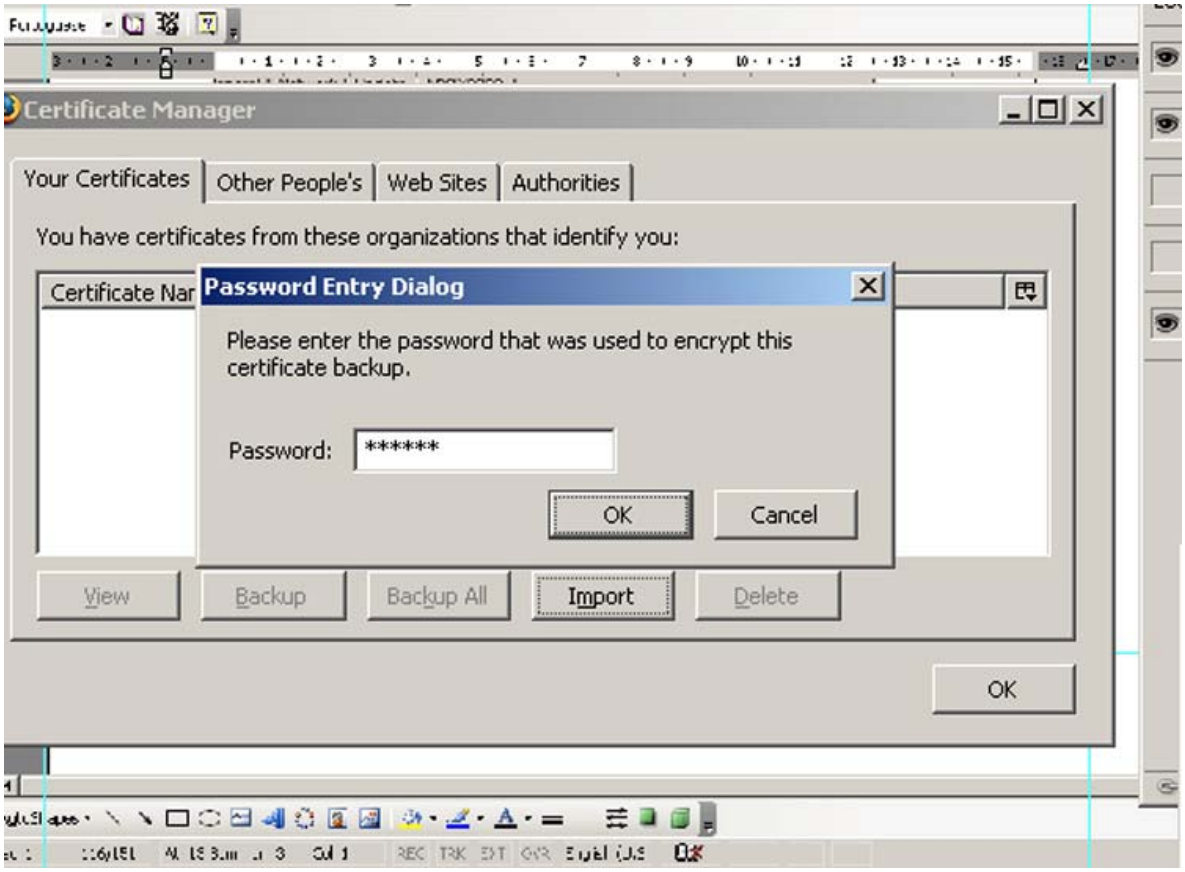
Σχήμα 10. Εγκατάσταση προσωπικού πιστοποιητικού στο Mozilla Firefox.

Εντοπίζουμε την τοποθεσία που έχουμε αποθηκεύσει το backup αρχείο και πατάμε **Open.**



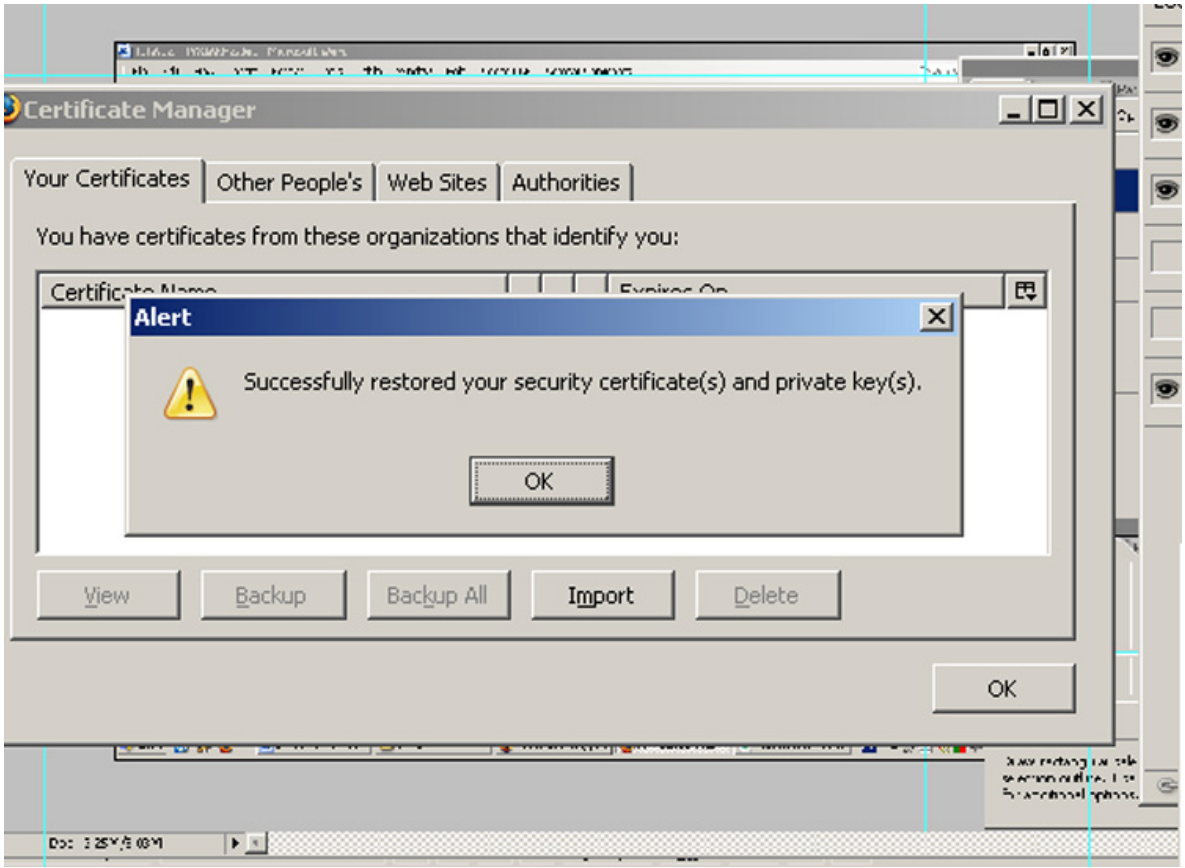
Σχήμα 11. Εισαγωγή backup αρχειου

Στη συνέχεια πρέπει να δώσουμε τον κωδικό που είχαμε ορίσει για την προστασία του backup αρχείου.



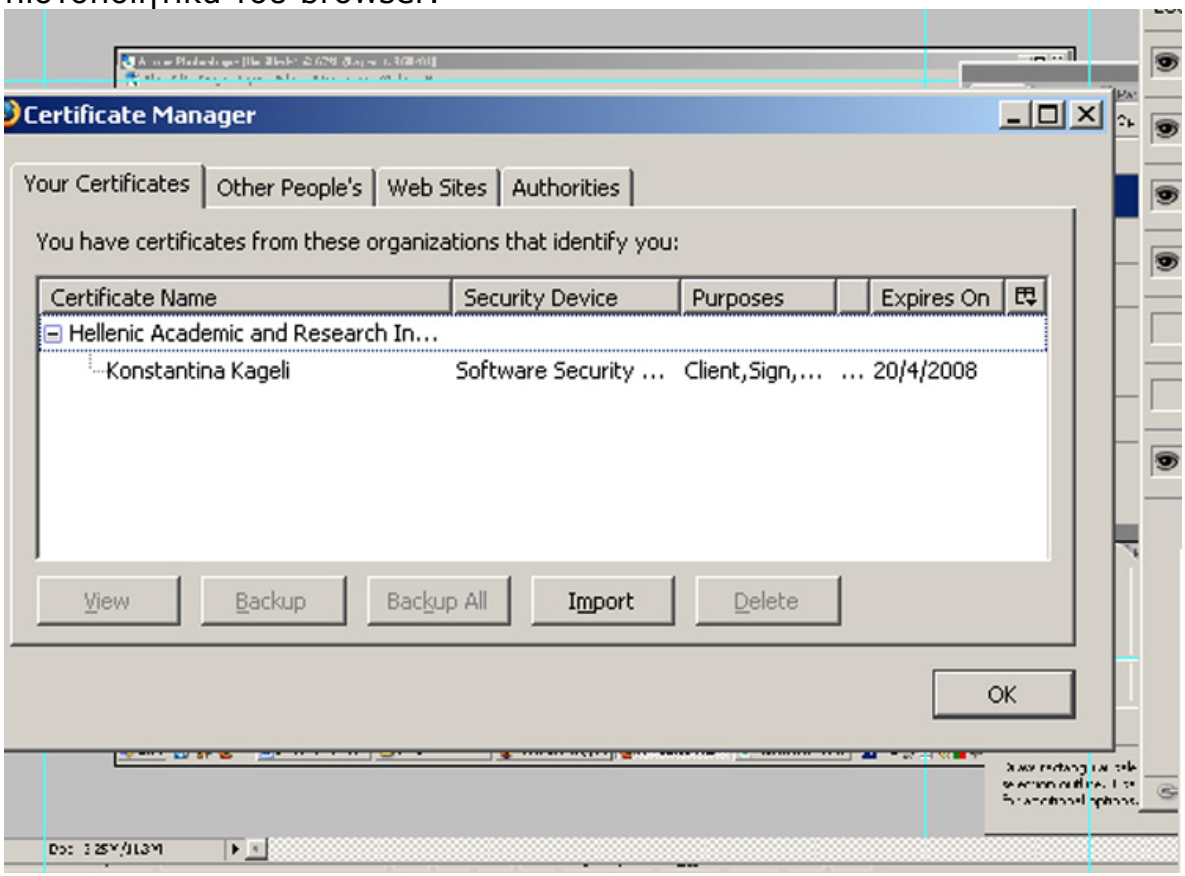
Σχήμα 12. Εισαγωγή κωδικού προστασίας του αρχείου

Εμφανίζεται μήνυμα για την επιτυχή εισαγωγή του πιστοποιητικού. Πατάμε **ok**.



Σχήμα 13. Ολοκλήρωση εισαγωγής πιστοποιητικού

Τέλος, βλέπουμε το πιστοποιητικό εγκατεστημένο στα προσωπικά πιστοποιητικά του browser.

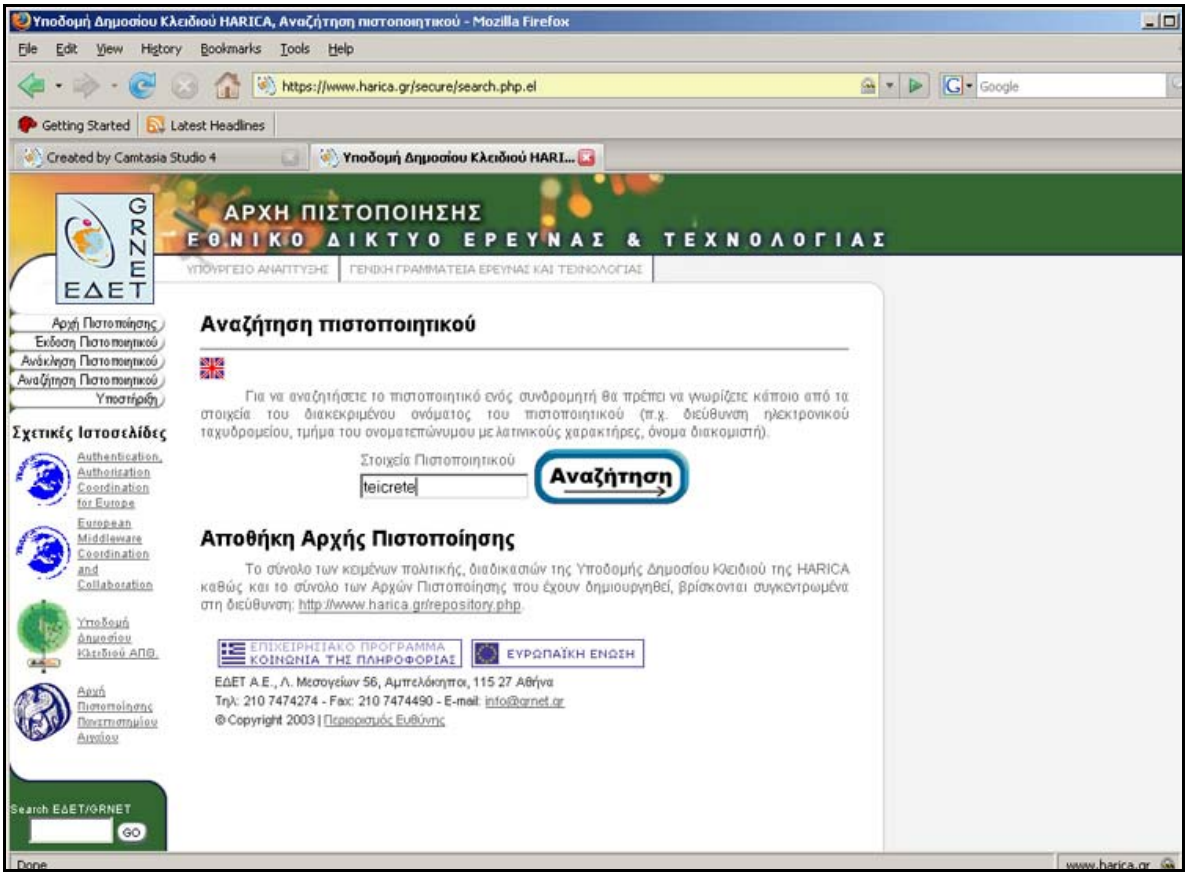


Σχήμα 14. Παρουσία πιστοποιητικού στα προσωπικά πιστοποιητικά.

Παράρτημα Η

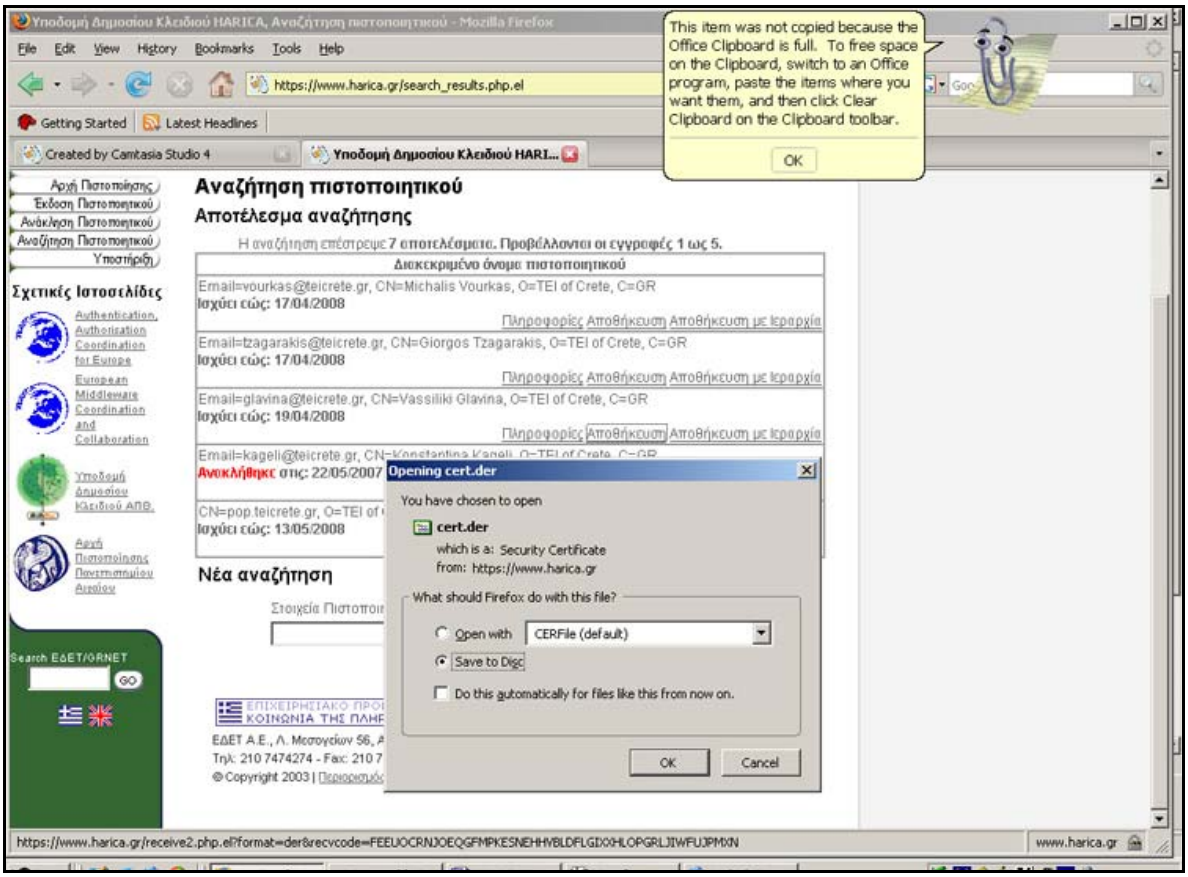
Οδηγίες για την εγκατάσταση πιστοποιητικού άλλου προσώπου στο browser.

Στην περίπτωση που θέλουμε να εγκαταστήσουμε κάποιο πιστοποιητικό άλλου χρήστη, αρχικά επισκεπτόμαστε τη σελίδα αναζήτησης πιστοποιητικών, της HARICA. Δίνουμε κάποιο στοιχείο(αυτό μπορεί να είναι είτε το όνομα του, είτε το email του, είτε το όνομα του φορέα στον οποίο ανήκει) του χρήστη του οποίου το πιστοποιητικό αναζητούμε. Πατάμε **Αναζήτηση**.



Σχήμα 1. Αναζήτηση πιστοποιητικού άλλου προσώπου.

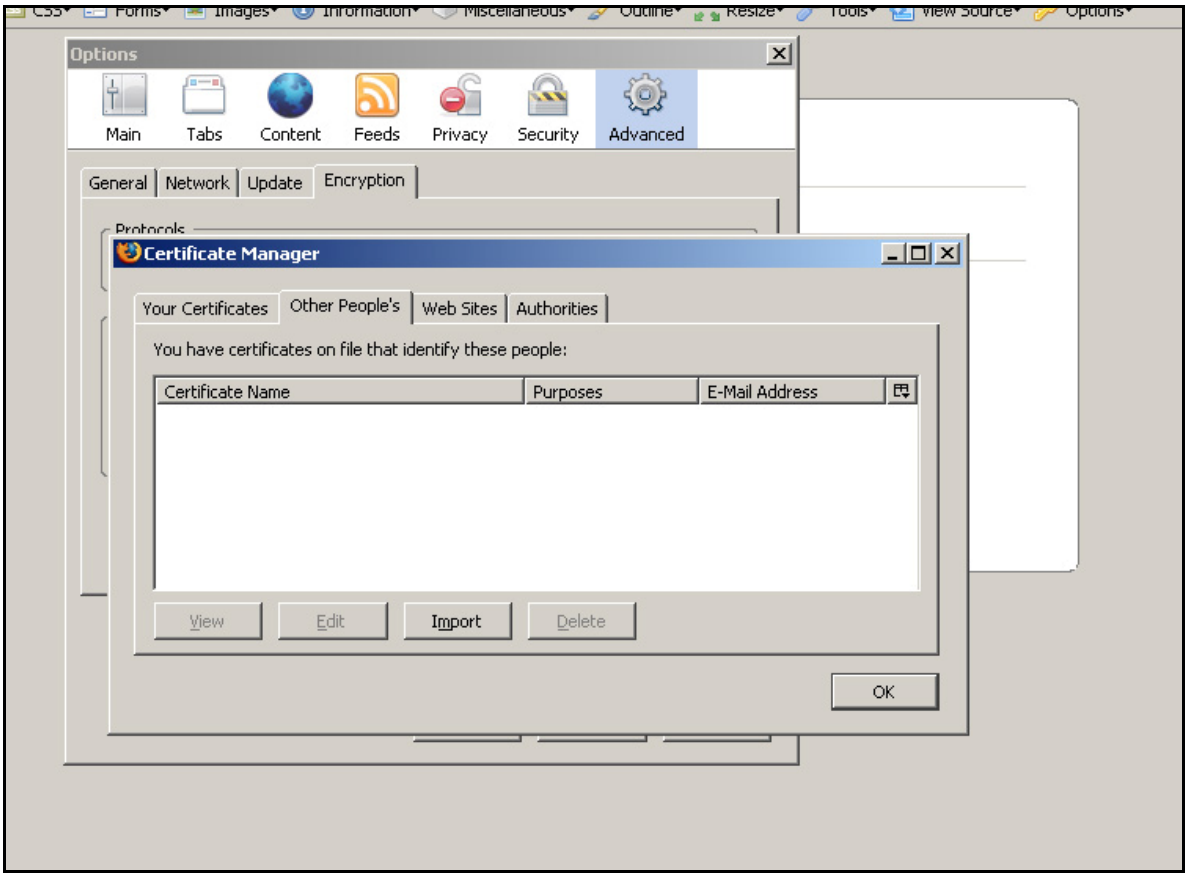
Εμφανίζονται τα αποτελέσματα της αναζήτησης με βάση την λέξη κλειδί που ορίσαμε. Εντοπίζουμε το πιστοποιητικό που μας ενδιαφέρει και το σώζουμε σε κάποια τοποθεσία πατώντας **Save**. Σε αυτό το σημείο υπάρχει δυνατότητα να σώσουμε το πιστοποιητικό με την μορφή ιεραρχικής αλυσίδας, ξεκινώντας από το πιστοποιητικό της HARICA κάτω από το οποίο βρίσκεται το πιστοποιητικό του ΤΕΙ Κρήτης, κάτω από το οποίο βρίσκεται το πιστοποιητικό του χρήστη.



Σχήμα 2. Αποθήκευση πιστοποιητικού άλλου προσώπου στον υπολογιστή μας.

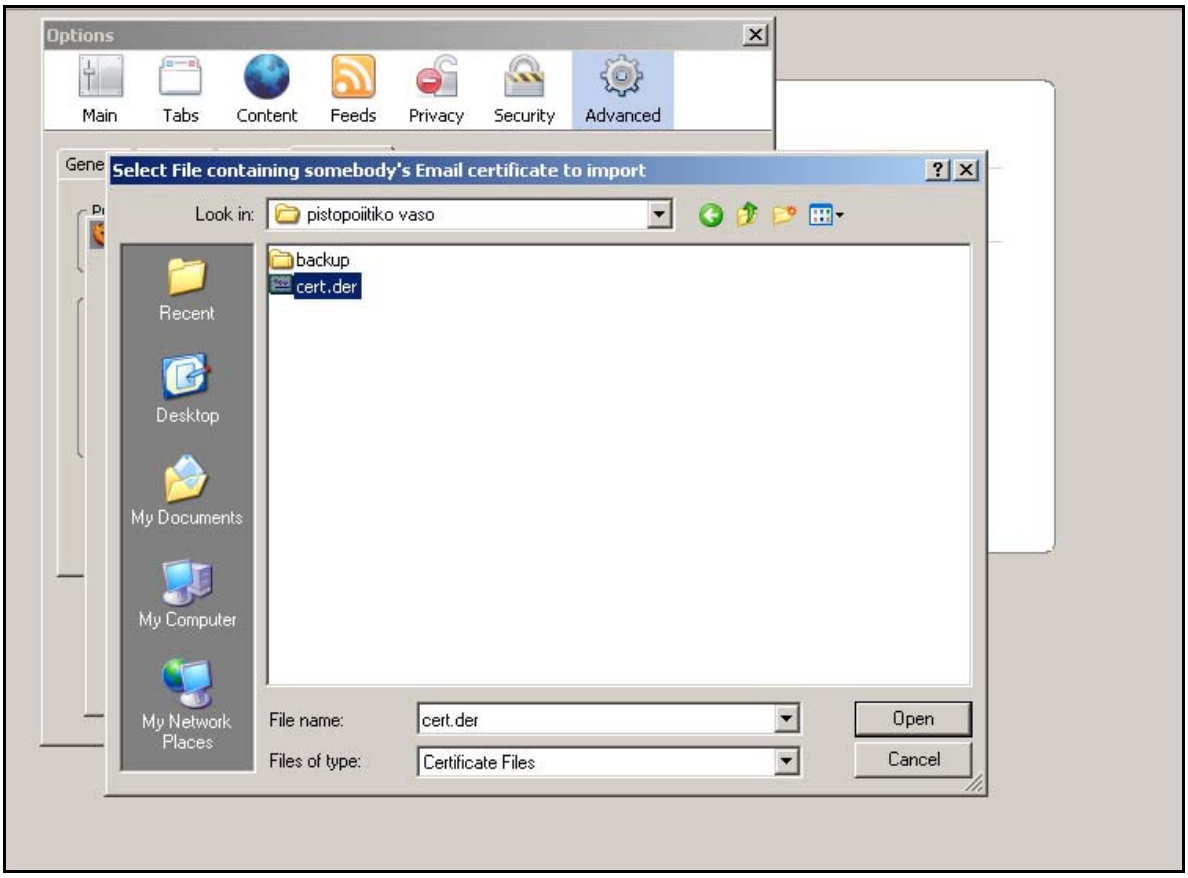
- Mozilla Firefox

Από το μενού **Tools** / **Options**, επιλέγουμε **Advanced**, στην καρτέλα **Encryption** πατάμε το κουμπί **View Certificates** και στην καρτέλα **Other People's** πατάμε το κουμπί **Import**.



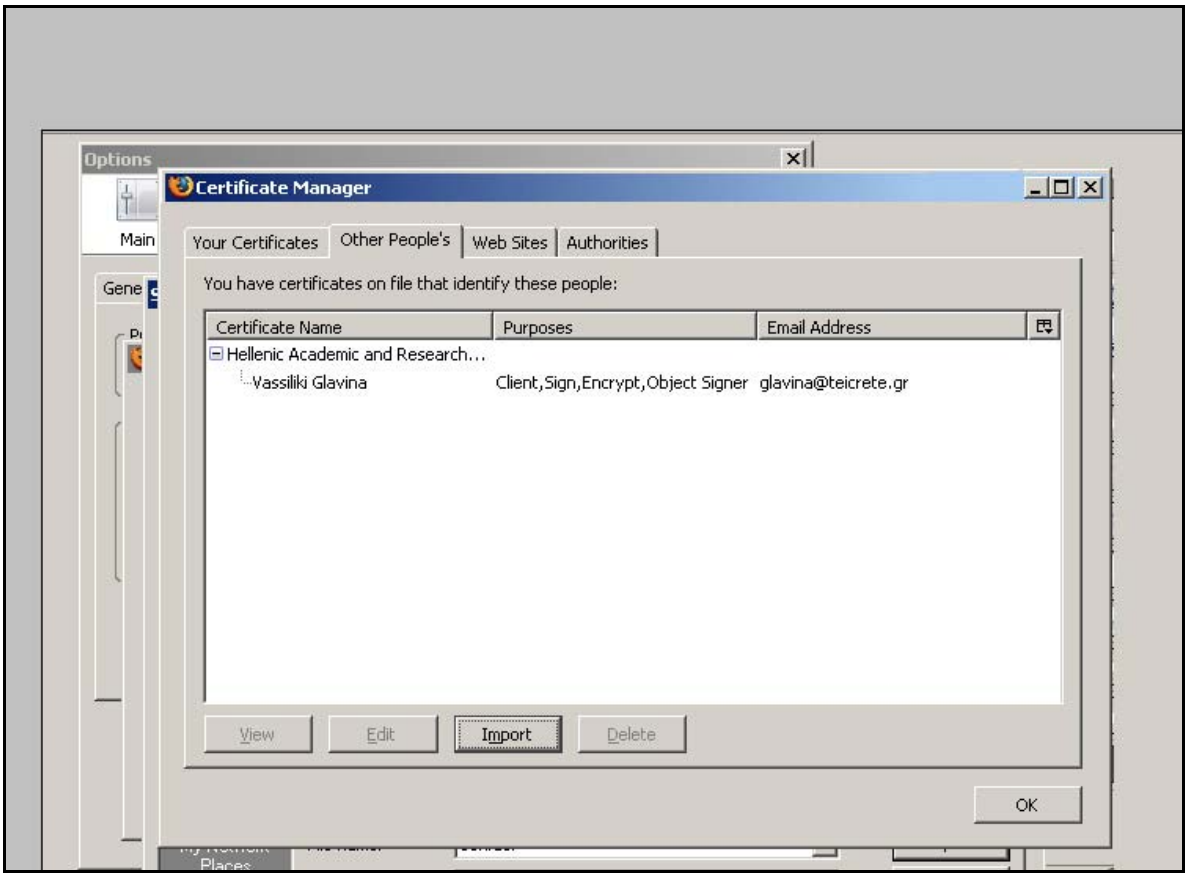
Σχήμα 3. Εγκατάσταση πιστοποιητικού άλλου προσώπου στο Mozilla Firefox.

Εντοπίζουμε την τοποθεσία που έχουμε αποθηκεύσει το πιστοποιητικό και πατάμε **Open.**



Σχήμα 4. Εισαγωγή πιστοποιητικού.

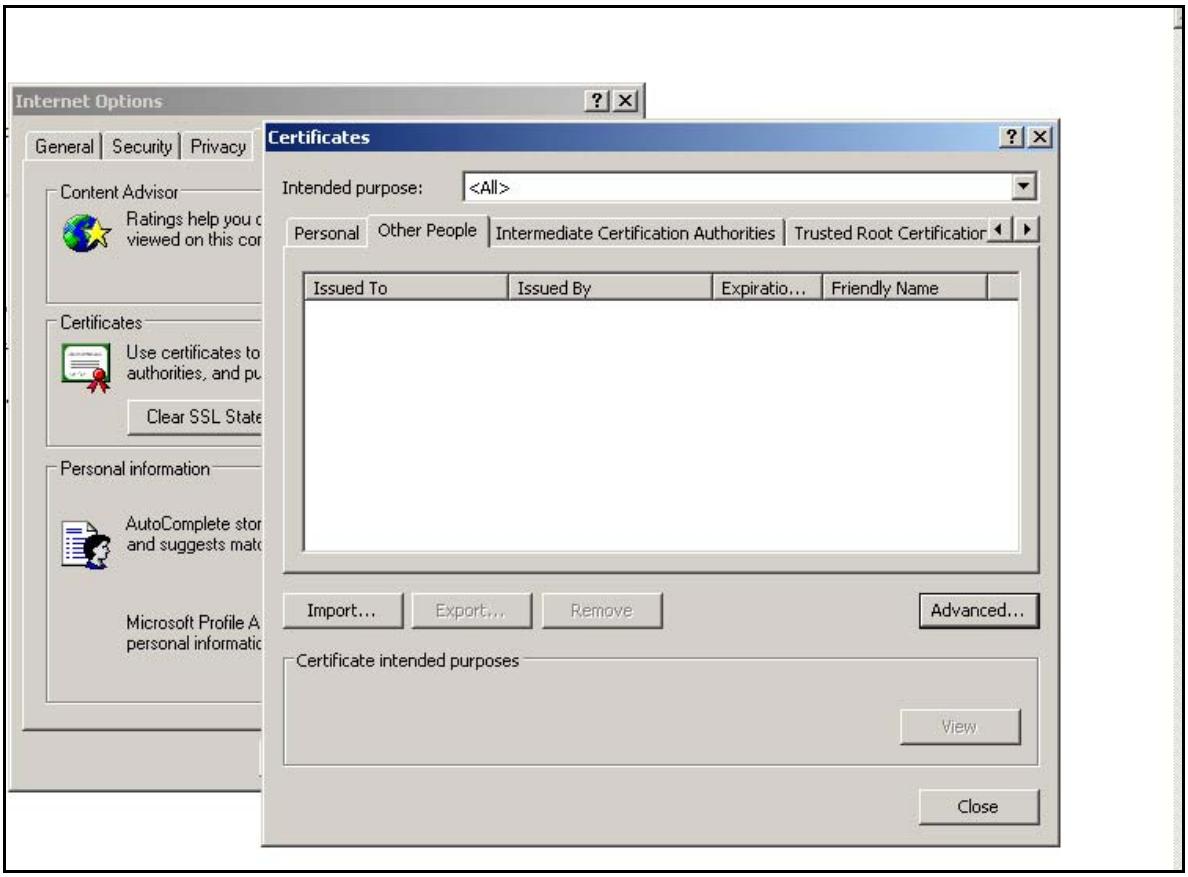
Τέλος, βλέπουμε το πιστοποιητικό εγκατεστημένο στα πιστοποιητικά άλλων προσώπων του browser.



Σχήμα 5. Παρουσία πιστοποιητικού στα πιστοποιητικά άλλων προσώπων.

- Internet Explorer

Για την εισαγωγή πιστοποιητικού άλλου προσώπου στον Internet Explorer πηγαίνουμε από το μενού **Tools** / **Internet Options**, επιλέγουμε την καρτέλα **Content**, πατάμε το κουμπί **Certificates** και στην καρτέλα **Other People** πατάμε **Import.**

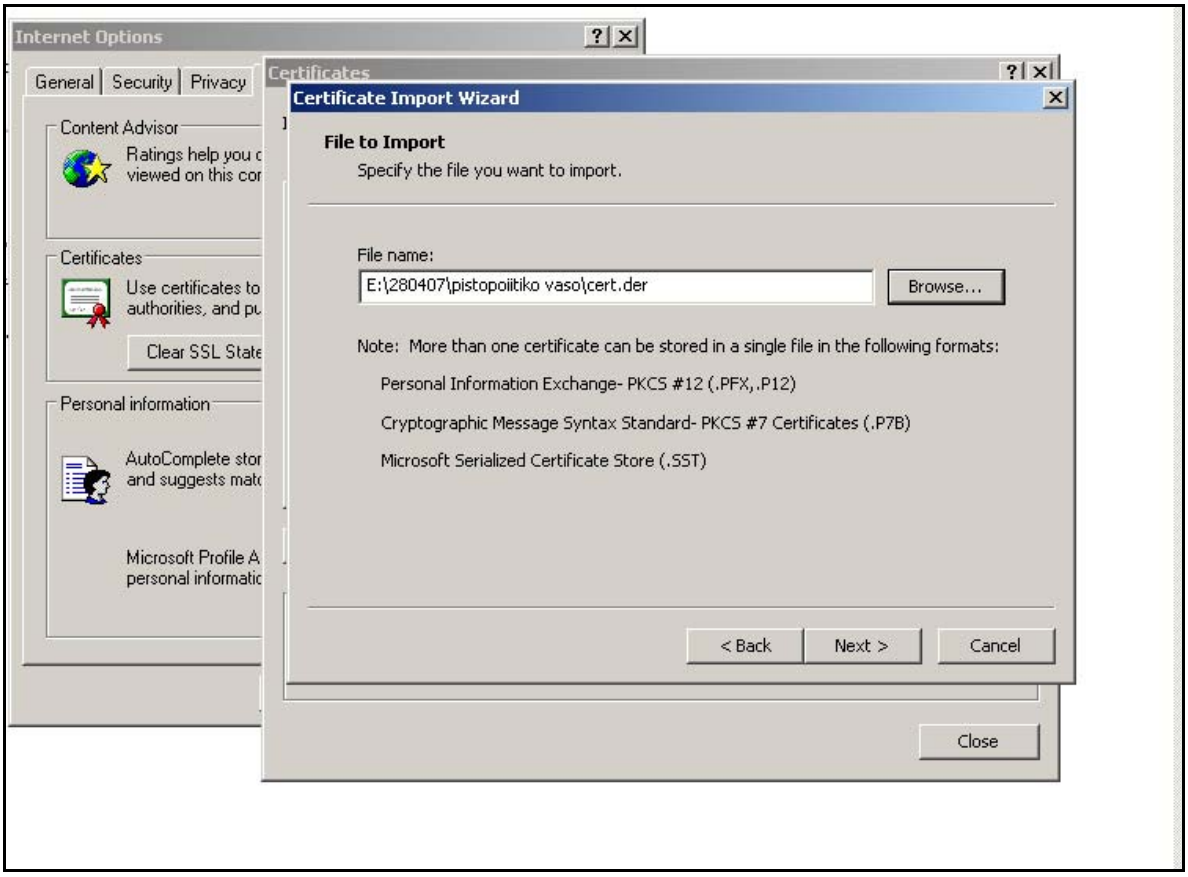


Σχήμα 6. Εισαγωγή πιστοποιητικού άλλου προσώπου.

Έχοντας πατήσει Import ξεκινάει ο οδηγός εγκατάστασης πιστοποιητικών του Internet Explorer. Πατάμε **next.**

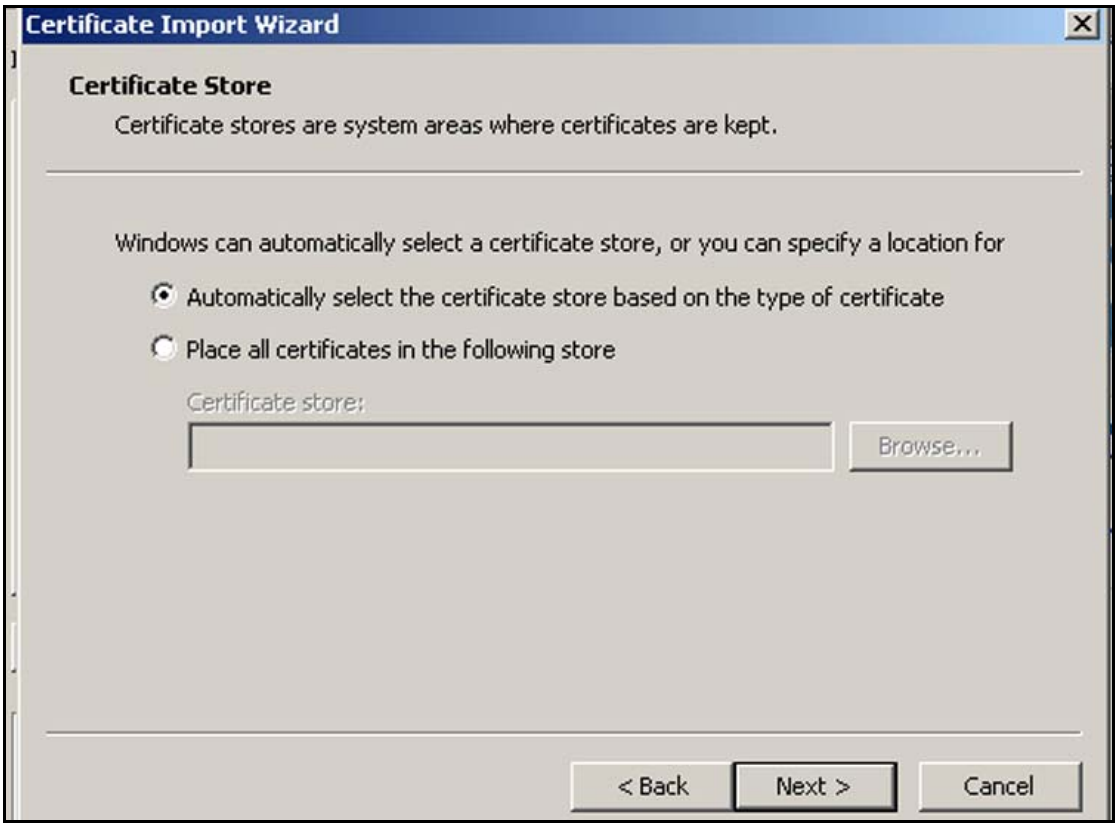
Σχήμα 7. Οδηγός εγκατάστασης πιστοποιητικού.

Πατώντας browse εντοπίζουμε την τοποθεσία που έχουμε αποθηκεύσει το πιστοποιητικό και πατάμε **Open** για να μπει το path στον οδηγό. Πατάμε **next .**



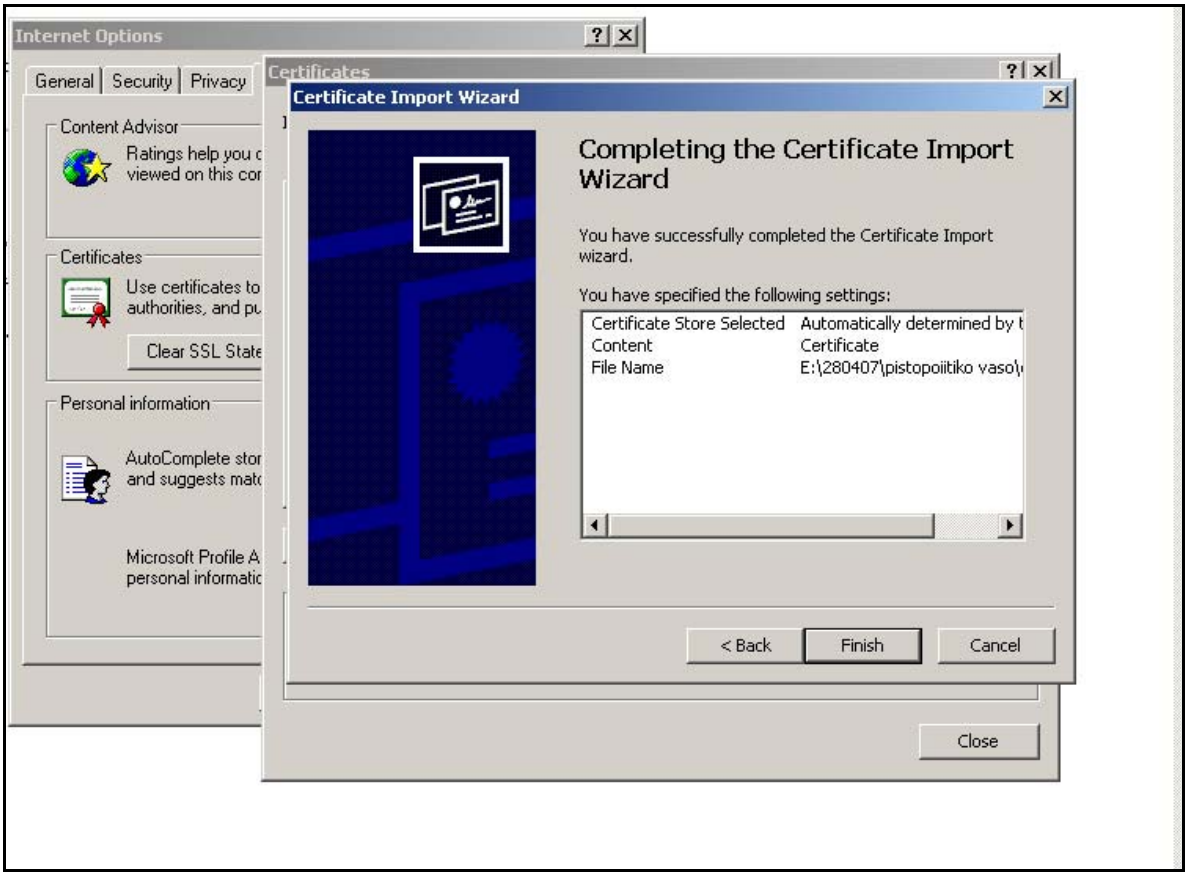
Σχήμα 8. Εισαγωγή πιστοποιητικού στον οδηγό εγκατάστασης.

Ο οδηγός εγκατάστασης μας ζητάει να ορίσουμε αν η τοποθεσία αποθήκευσης θα επιλεγεί αυτόματα ή θα την ορίσουμε εμείς. Αφήνουμε την αυτόματη επιλογή. Πατάμε **next**



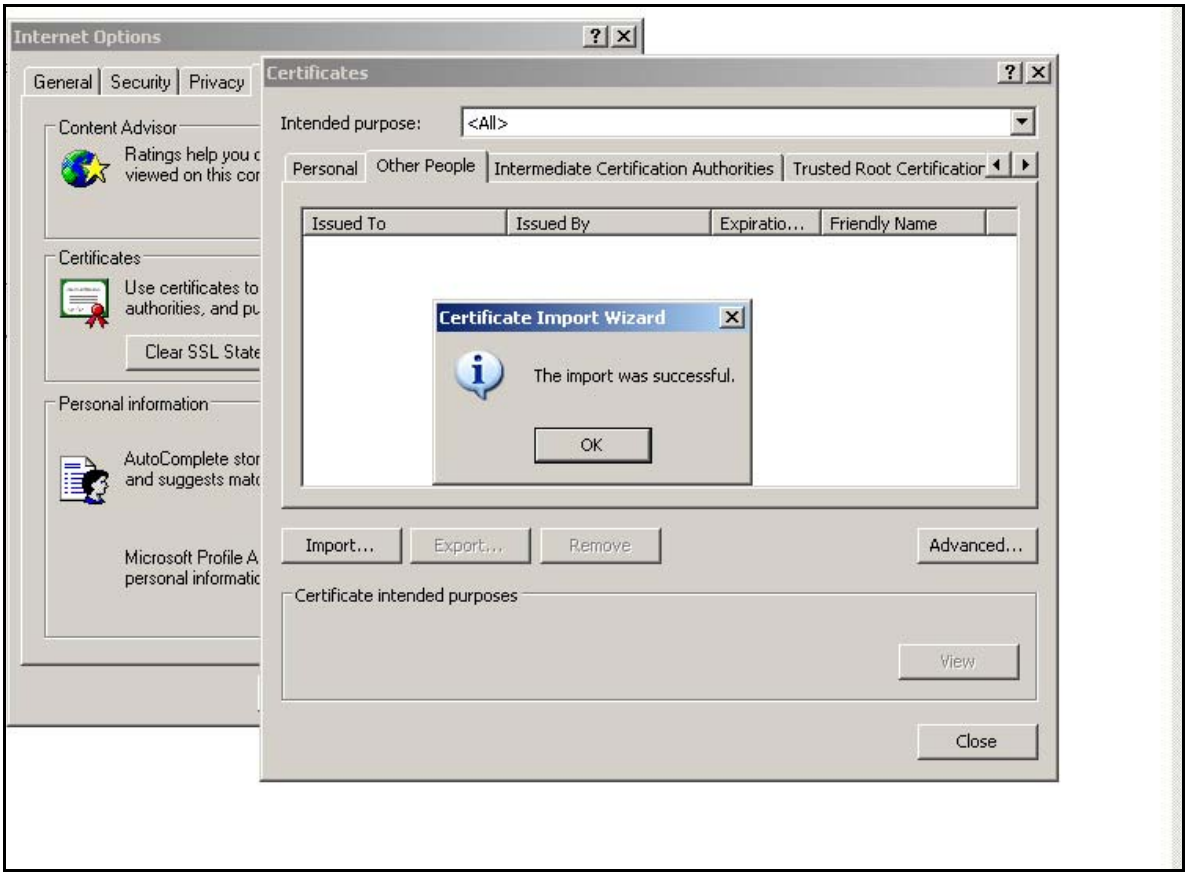
Σχήμα 9. Επιλογή τοποθεσίας αποθήκευσης πιστοποιητικού.

Ο οδηγός μας ενημερώνει για την ολοκλήρωση της εγκατάστασης του πιστοποιητικού. Πατάμε **Finish.**



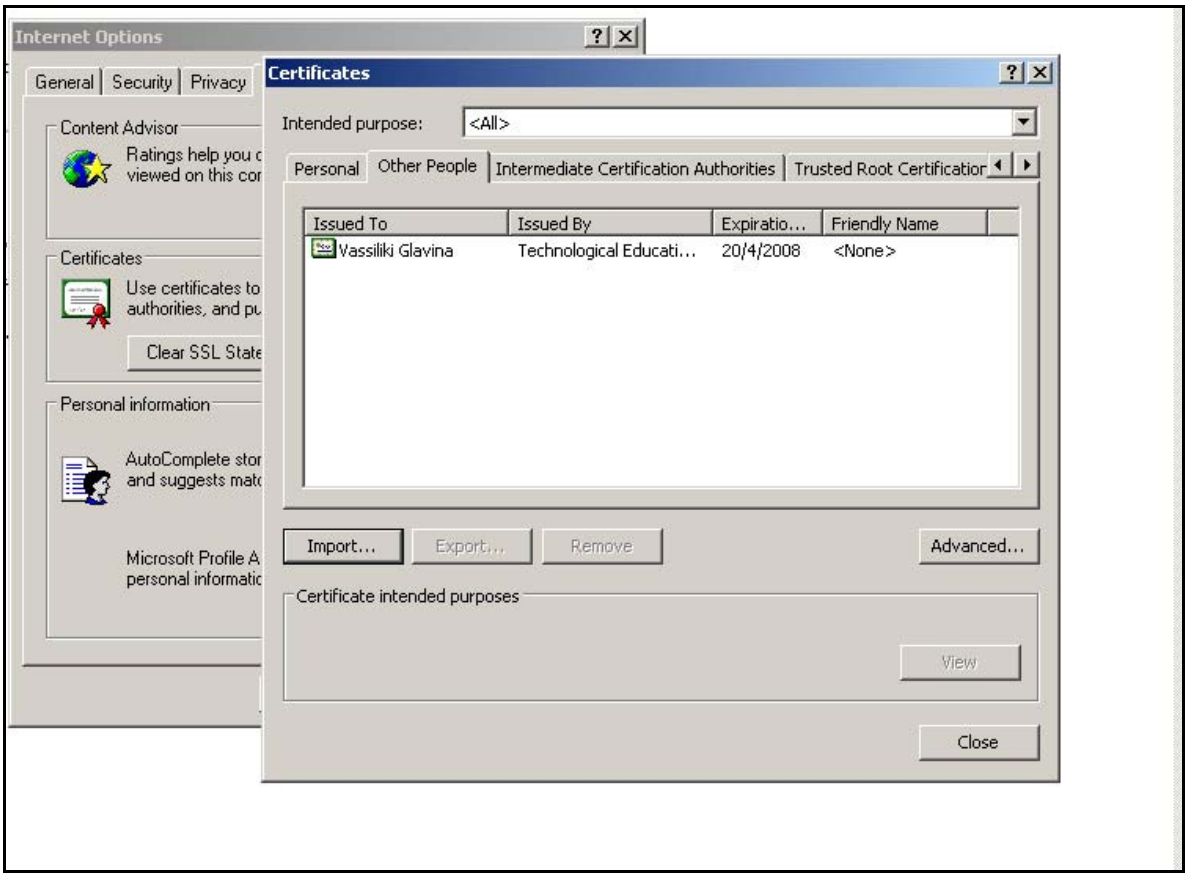
Σχήμα 10. Ολοκλήρωση εγκατάστασης πιστοποιητικού.

Ο οδηγός εγκατάστασης μας ενημερώνει για την επιτυχή εισαγωγή του πιστοποιητικού και κλείνει. Πατάμε **ok**.



Σχήμα 11. Ολοκλήρωση εισαγωγής πιστοποιητικού

Τέλος, βλέπουμε το πιστοποιητικό εγκατεστημένο στα πιστοποιητικά άλλων προσώπων του browser.



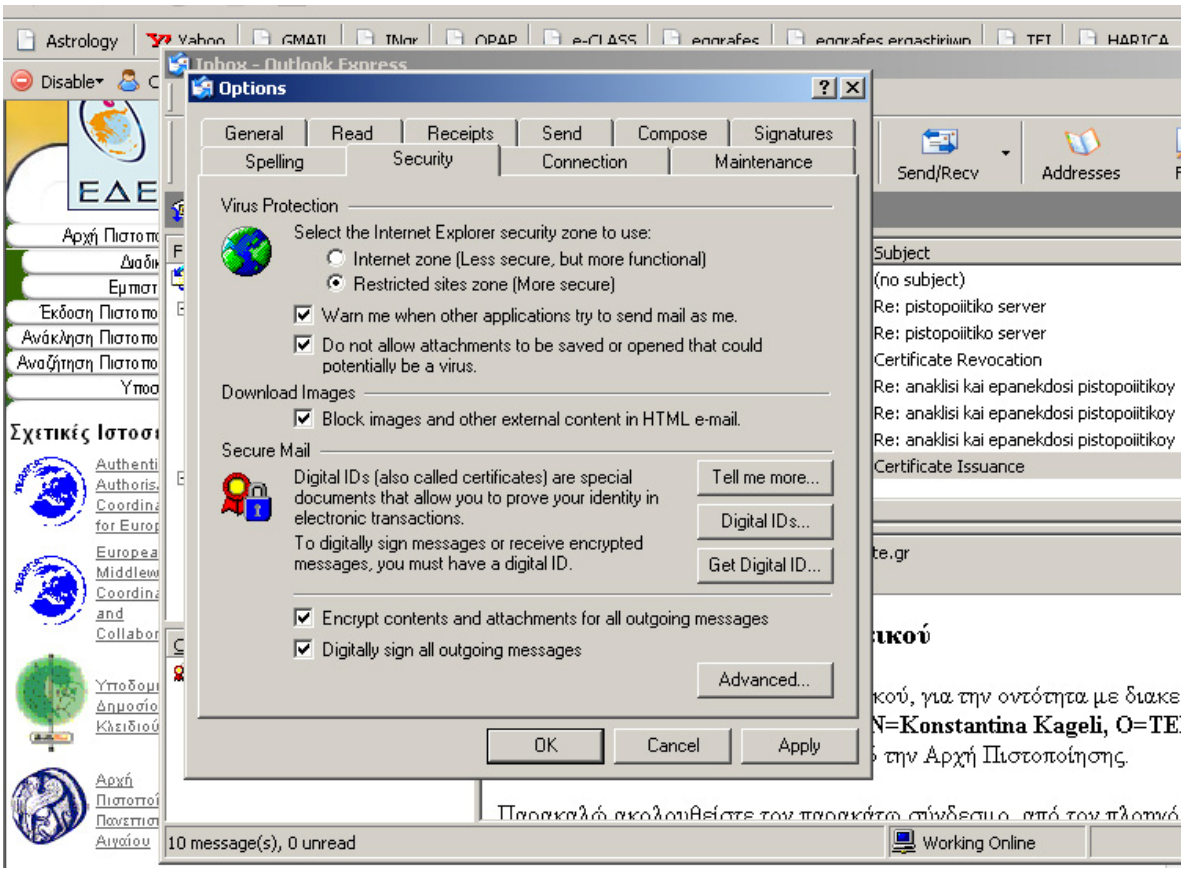
Σχήμα 12. Παρουσία πιστοποιητικό στα πιστοποιητικά άλλων προσώπων

Παράρτημα Θ

Οδηγίες για τη χρήση του ψηφιακού πιστοποιητικού από το Outlook Express και το Thunderbird

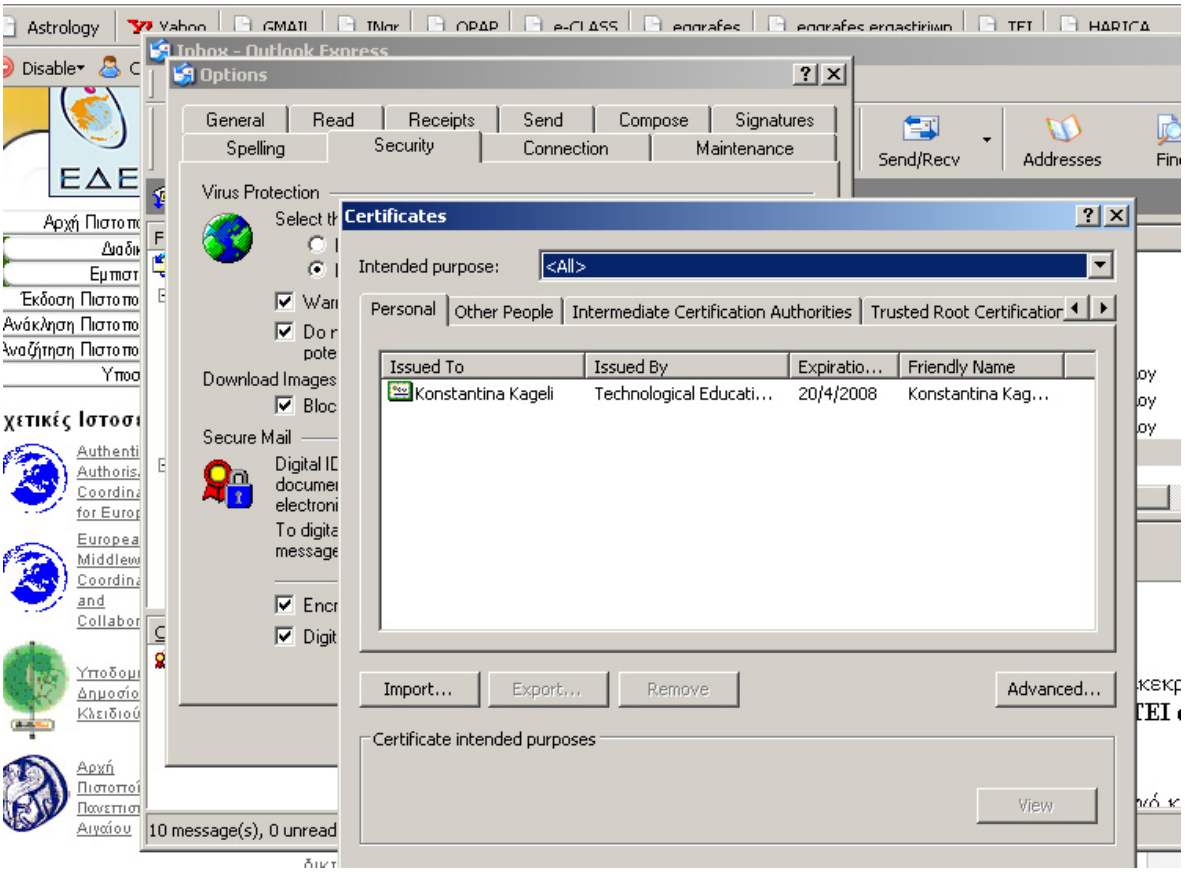
- Outlook Express

Ανοίγοντας το λογαριασμό μας, για το οποίο έχουμε πάρει το ψηφιακό πιστοποιητικό,με το πρόγραμμα ηλεκτρονικού ταχυδρομείου Outlook Express και πηγαίνοντας από το μενού **Tools / Options** στην καρτέλα **Security** πατάμε το κουμπί **Digital IDs** για να δούμε τα ψηφιακά πιστοποιητικά που είναι αποθηκευμένα.



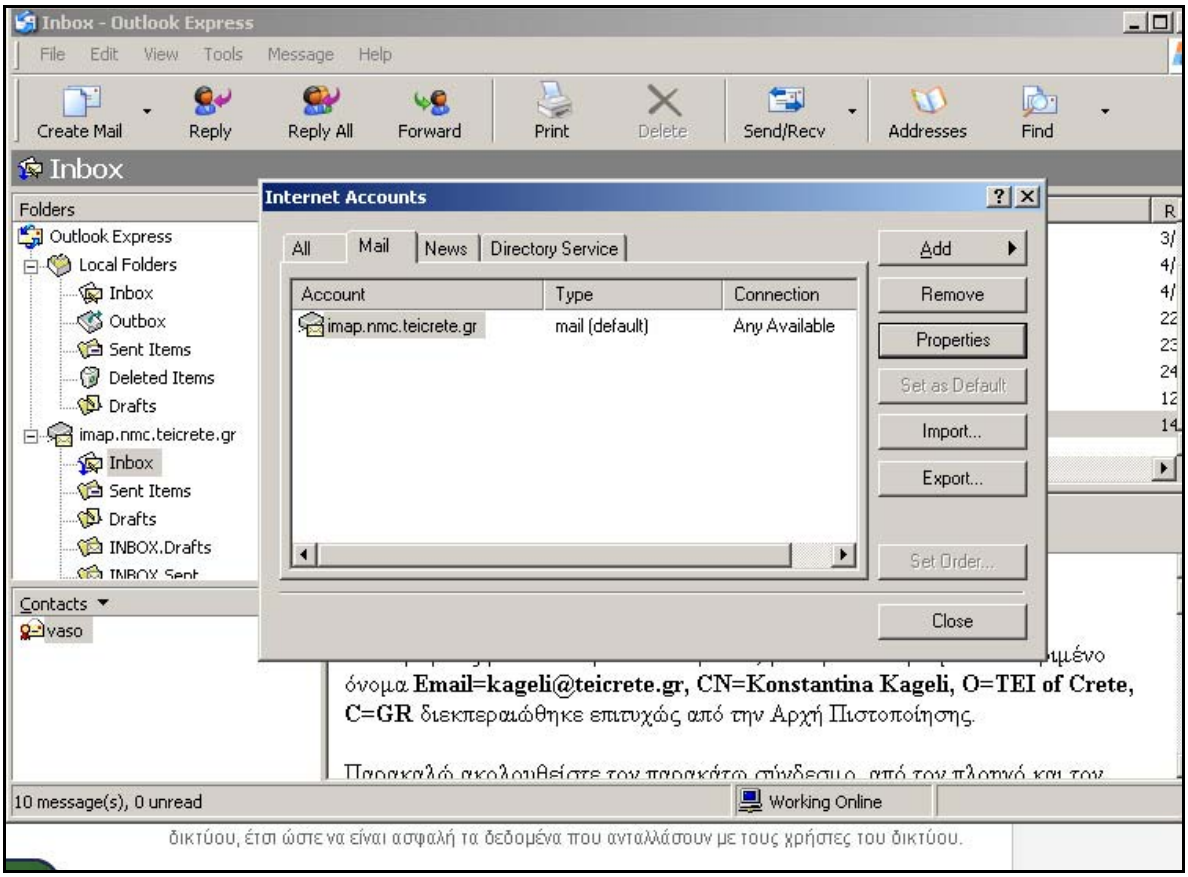
Σχήμα 1. Αποθήκη πιστοποιητικών στο Outlook Express.

Το Outlook Express επικοινωνεί με τον Internet Explorer και αντλεί τα πιστοποιητικά που είναι εγκατεστημένα εκεί. Ουσιαστικά ανοίγει η καρτέλα Certificates του Internet Explorer.



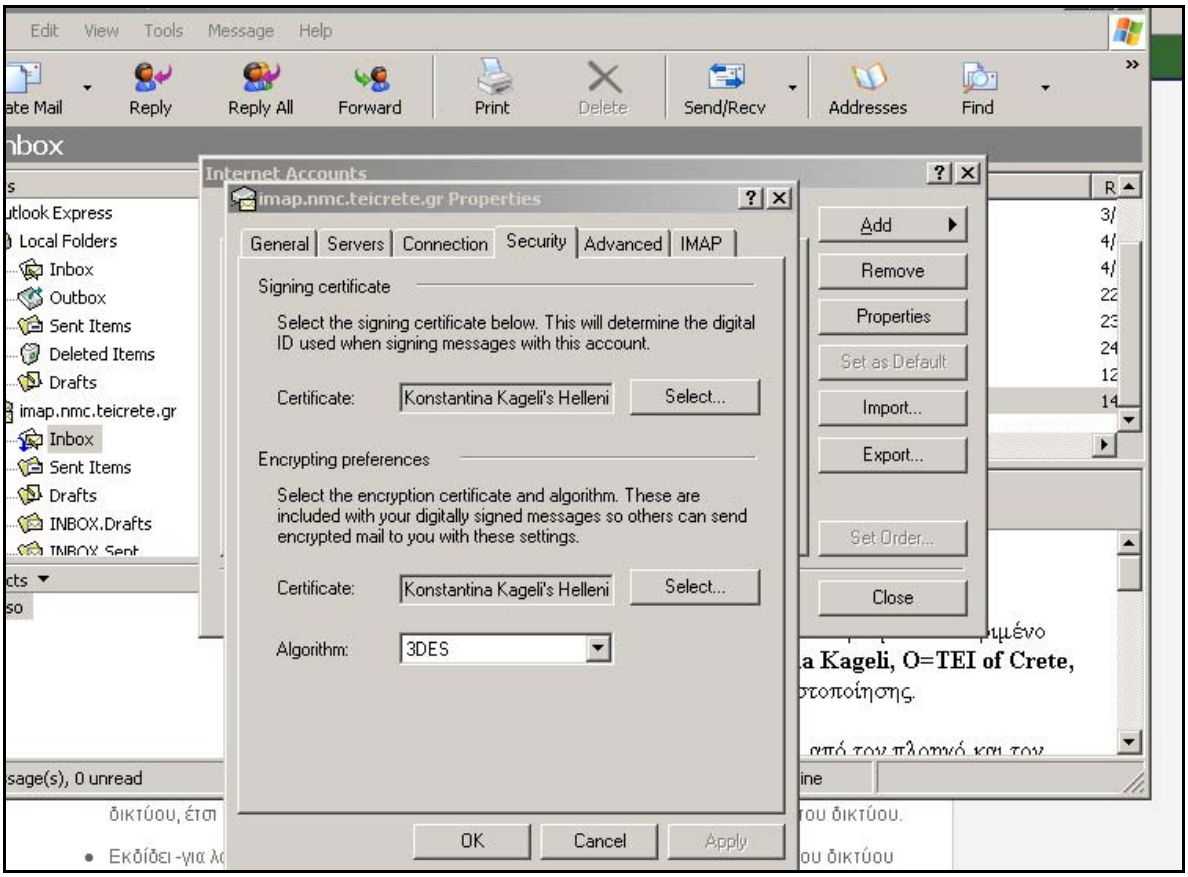
Σχήμα 2. Εμφάνιση πιστοποιητικών του Outlook Express.

Από το μενού πηγαίνουμε **Tools / Accounts**, επιλέγω το Mail Account και πατάω το κουμπί **Properties**, ώστε να δούμε ποια πιστοποιητικά χρησιμοποιούνται για ψηφιακή υπογραφή και κρυπτογράφηση.



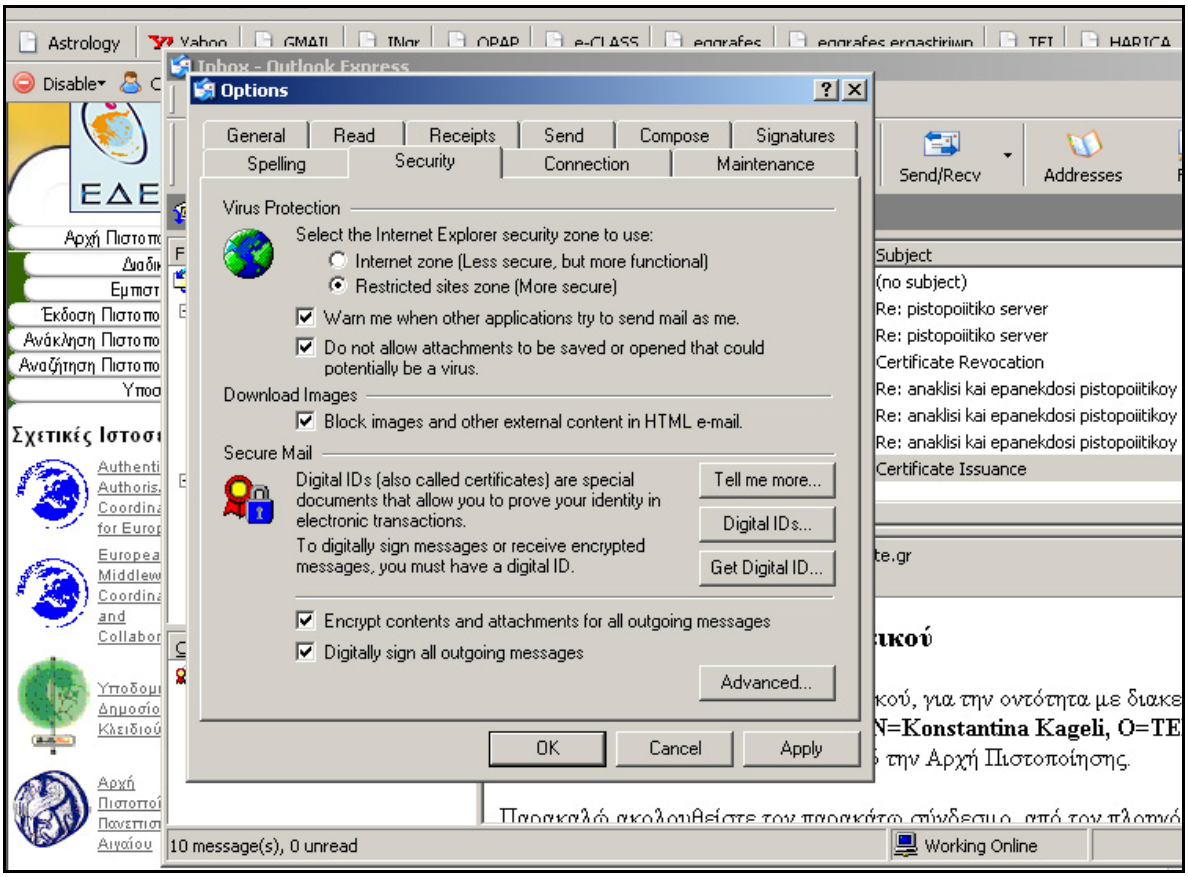
Σχήμα 3. Ιδιότητες του Mail Account.

Στην καρτέλα **Security** μπορούμε να δούμε ποιο πιστοποιητικό χρησιμοποιείται για ψηφιακή υπογραφή των emails και από ποιο πιστοποιητικό αντλείται το δημόσιο κλειδί για την κρυπτογράφηση μηνυμάτων που στέλνονται σε αυτό το λογαριασμό. Συνήθως μπαίνουν αυτόματα με βάση το προσωπικό πιστοποιητικό που είναι εγκατεστημένο στο browser. Σε περίπτωση που δεν έχουν εισαχθεί αυτόματα πατώντας το κουμπί **Select** επιλέγουμε εμείς το πιστοποιητικό.



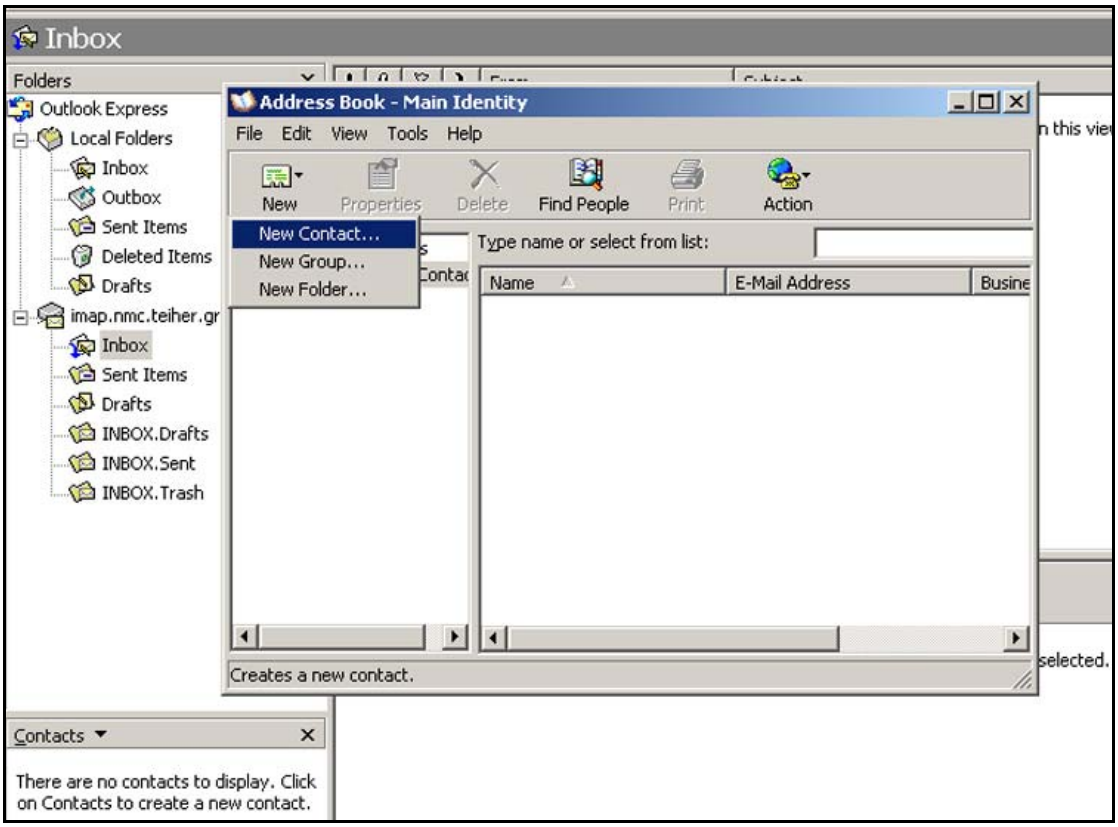
Σχήμα 4. Χρήση πιστοποιητικού από το Mail Account.

Στο Outlook Express μπορούμε να ρυθμίσουμε να υπογράφονται ψηφιακά, με το επιλεγμένο ψηφιακό πιστοποιητικό, όλα τα εξερχόμενα μηνύματα. Επίσης μπορούμε να επιλέξουμε να κρυπτογραφούνται τα μηνύματα με την προϋπόθεση ότι έχουμε το ψηφιακό πιστοποιητικό του παραλήπτη. Για την ενεργοποίηση τους τσεκάρουμε τις αντίστοιχες επιλογές στο μενού **Tools / Options** στην καρτέλα **Security.** Είναι προτιμότερο να επιλέξουμε την υπογραφή όλων των εξερχόμενων μηνυμάτων μόνο και όχι την κρυπτογράφηση γιατί δεν θα μπορεί να σταλεί το email σε πρόσωπα για τα οποία δεν έχουν ψηφιακό πιστοποιητικό.



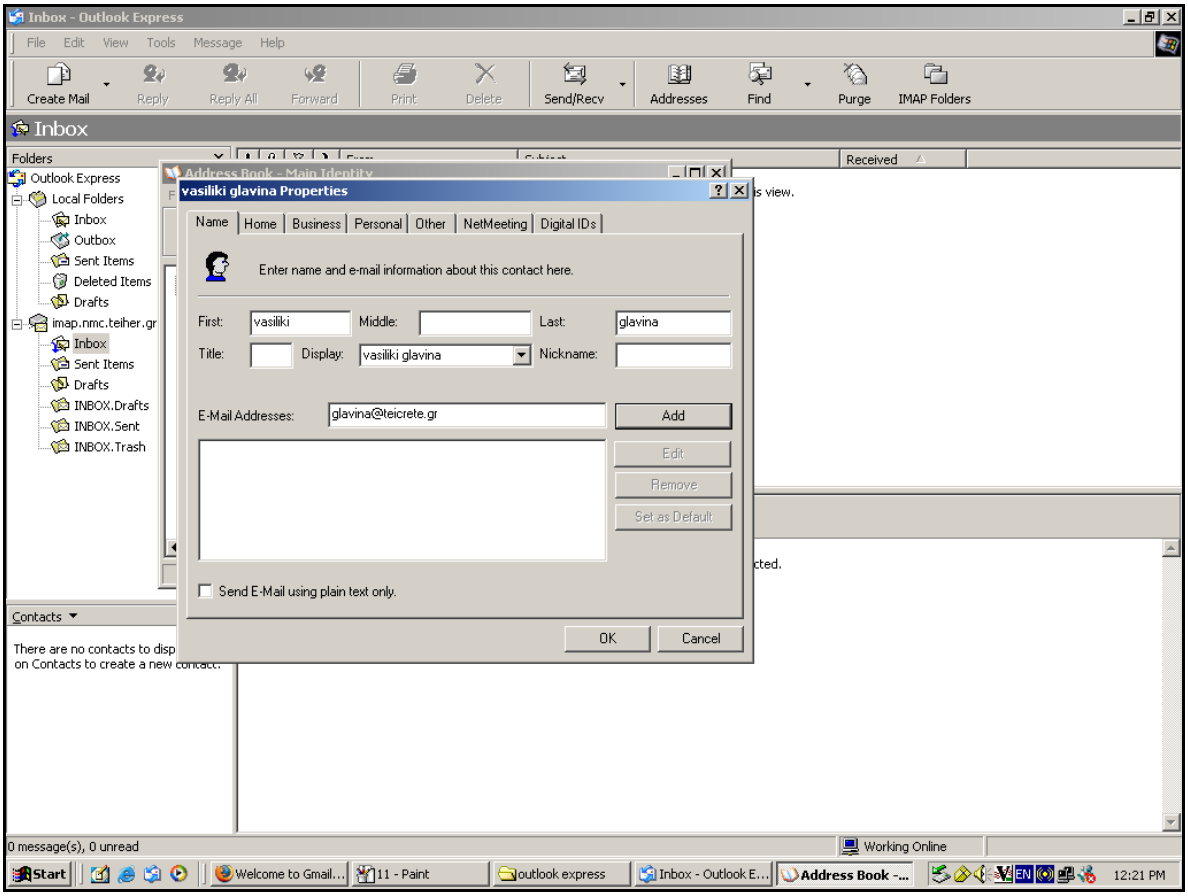
Σχήμα 5. Ρύθμιση επιλογών του Outlook Express.

Για να καταχωρήσουμε διευθύνσεις email άλλων προσώπων και τα ψηφιακά πιστοποιητικά τους, στις επαφές του λογαριασμού, από το μενού **Tools / Address Book**, πατάμε **New** και επιλέγουμε **New Contact**. Δημιουργούμε νέα επαφή.



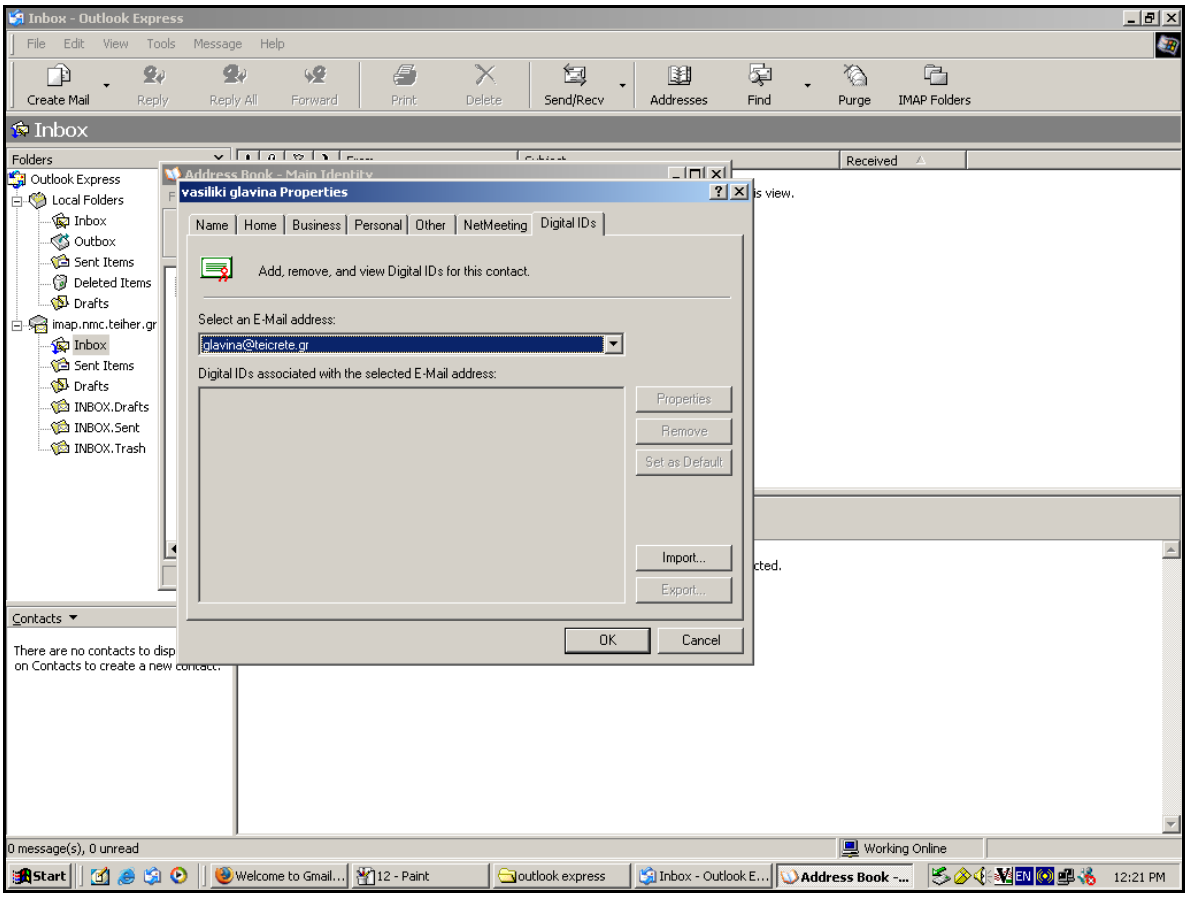
Σχήμα 6. Δημιουργία νέας επαφής.

Καταχωρούμε τα στοιχεία του προσώπου στην καρτέλα Name.



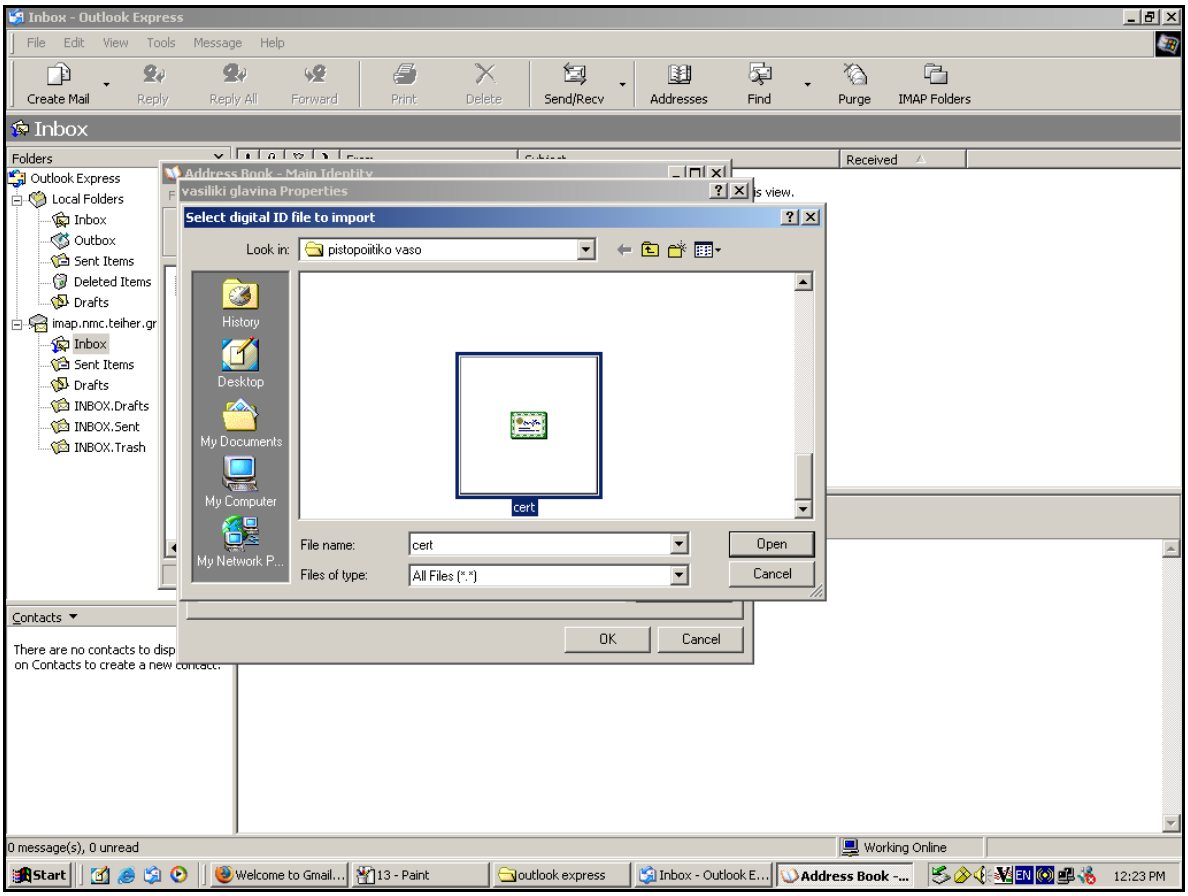
Σχήμα 7. Καταχώρηση στοιχείων της νέας επαφής.

Στην καρτέλα Digital IDs εισαγάγουμε το ψηφιακό πιστοποιητικό που αντιστοιχεί στην συγκεκριμένη επαφή πατώντας **Import**.



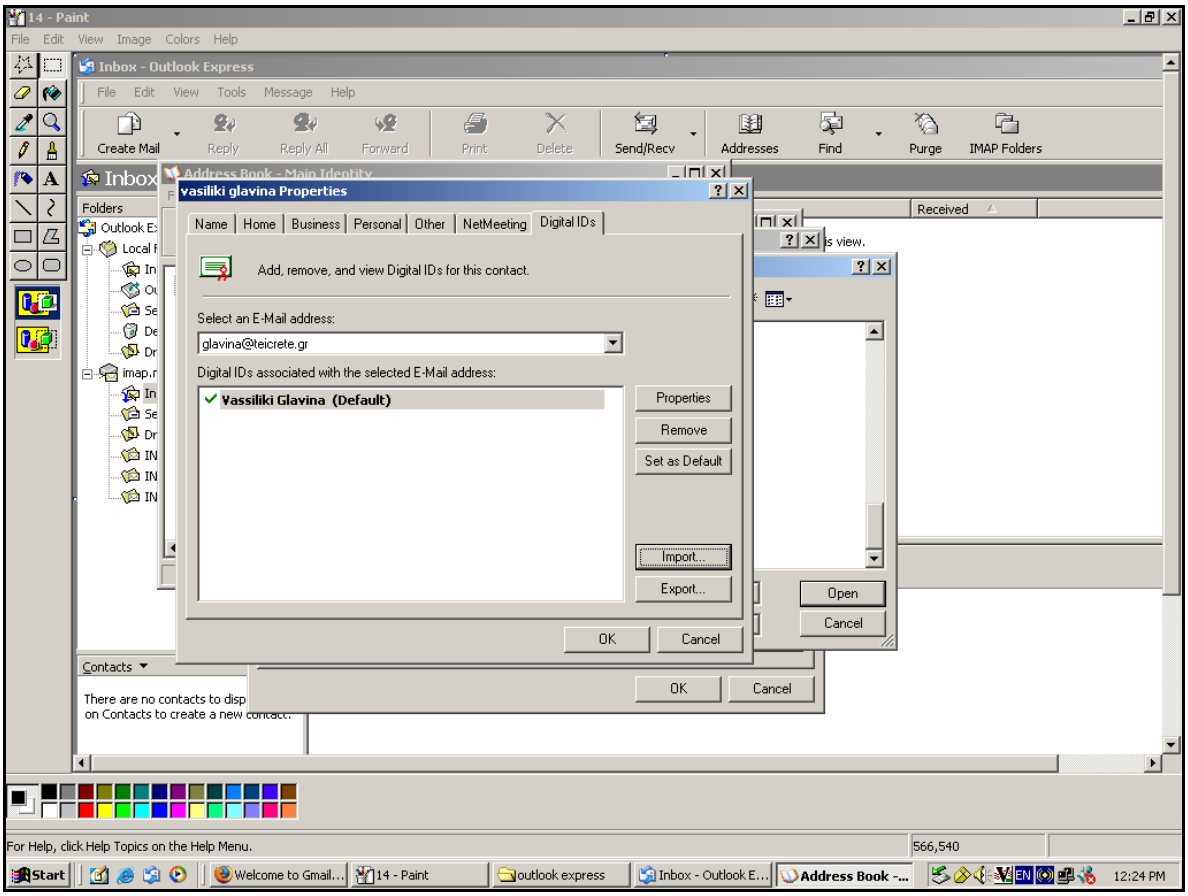
Σχήμα 8. Εισαγωγή πιστοποιητικού για την επαφή.

Εντοπίζουμε την τοποθεσία που είναι αποθηκευμένο το πιστοποιητικό και πατάμε **Open**.



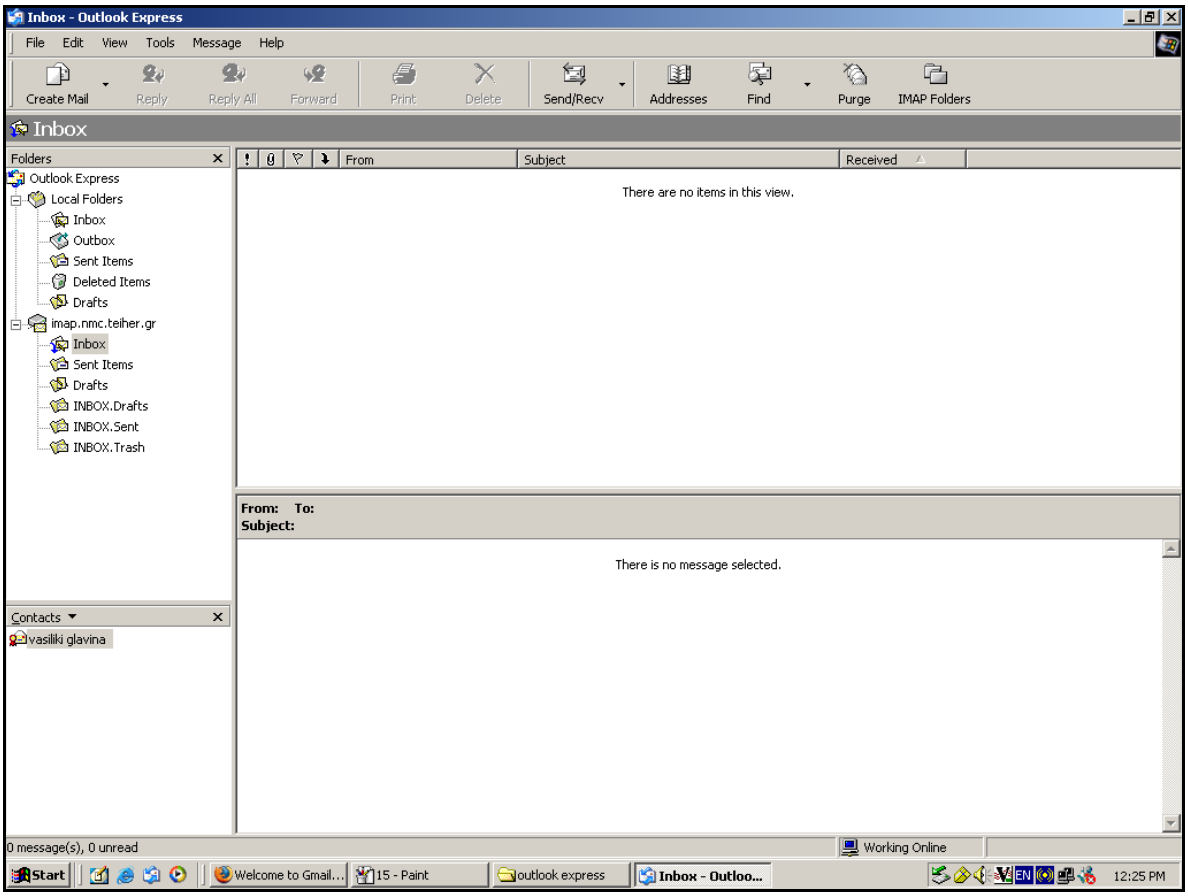
Σχήμα 9. Άνοιγμα πιστοποιητικού.

Βλέπουμε ότι η ψηφιακή υπογραφή της επαφής έχει καταχωρηθεί.



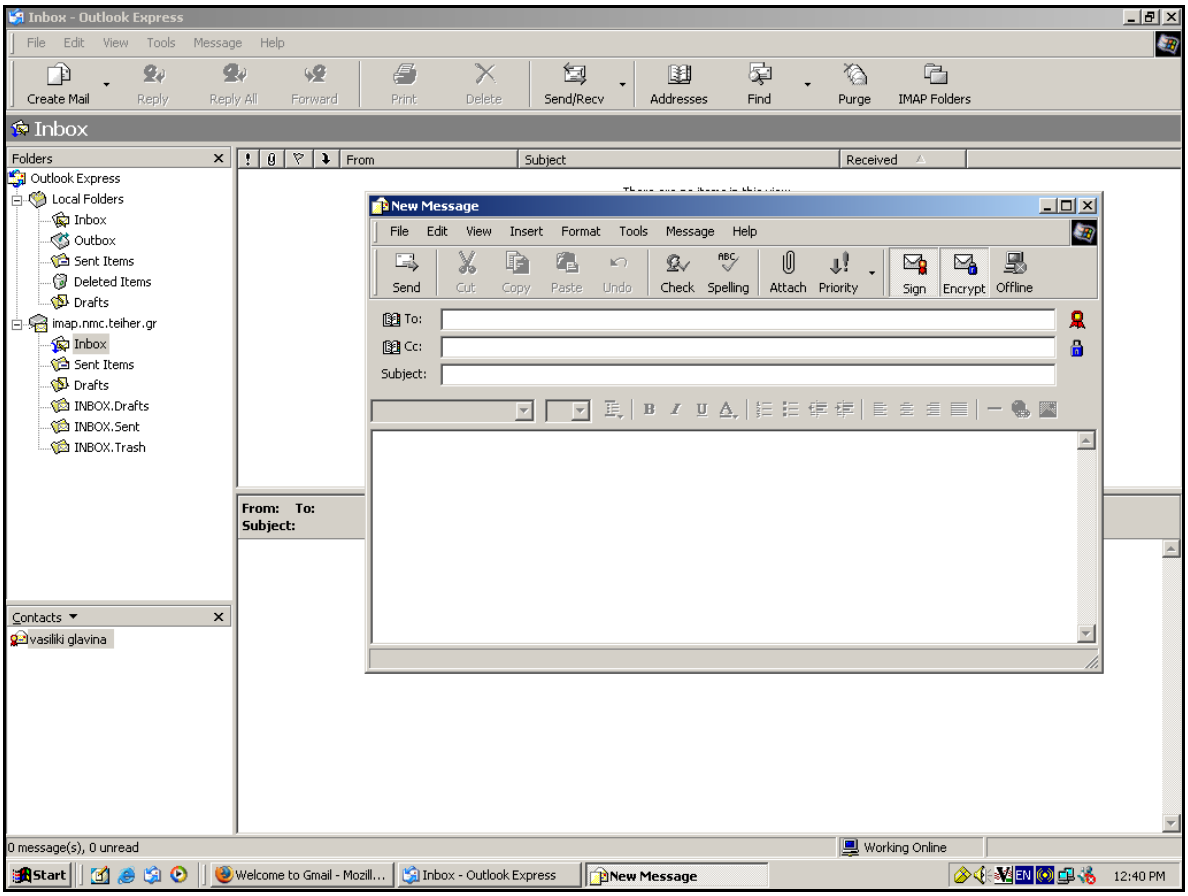
Σχήμα 10. Αποθήκευση ψηφιακής υπογραφής.

Παρατηρούμε ότι το όνομα της νέας επαφής που δημιουργήσαμε παρουσιάζεται κάτω αριστερά στα Contacts του Outlook Express, με το ενδεικτικό σήμα ότι η συγκεκριμένη επαφή φέρει και ψηφιακή υπογραφή.



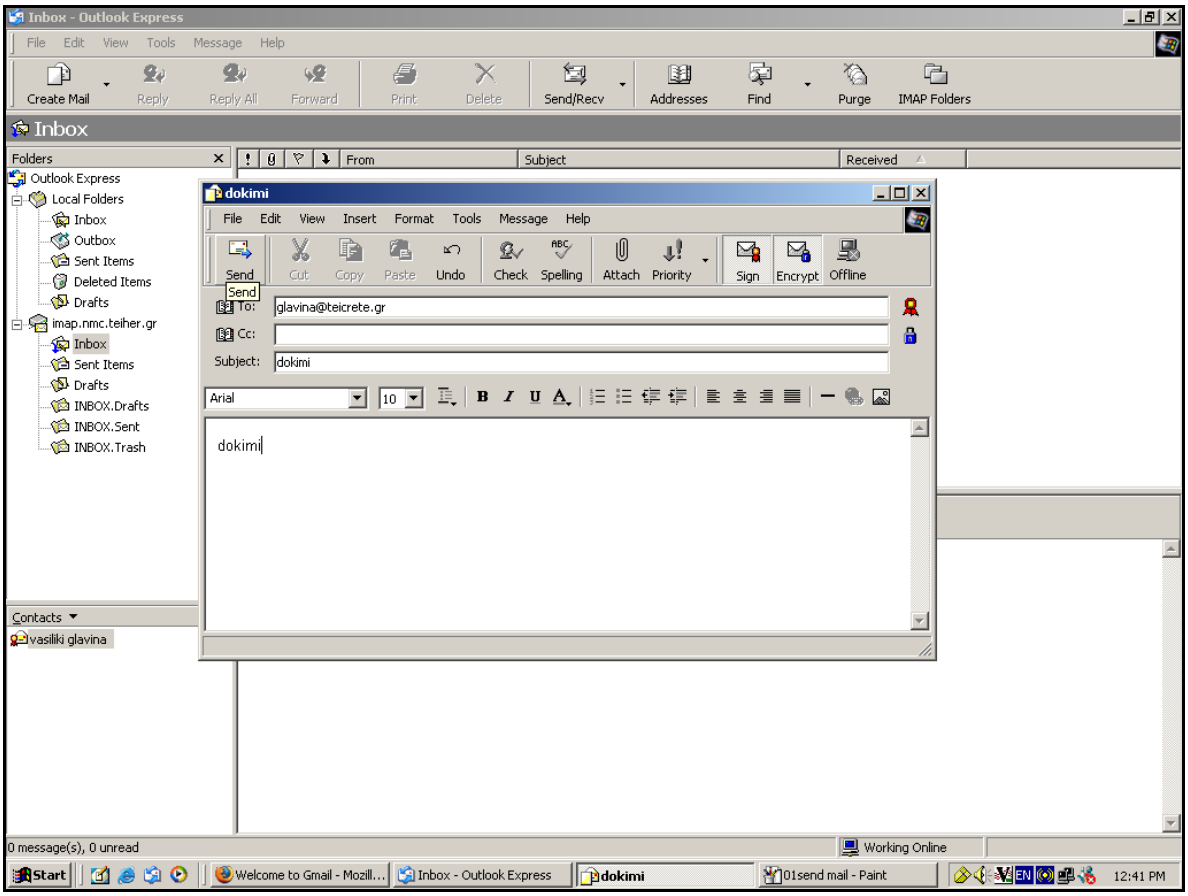
Σχήμα 11. Εμφάνιση επαφής.

Για να δούμε την εφαρμογή των ρυθμίσεων που κάναμε στέλνουμε ένα δοκιμαστικό email πατώντας **Create Mail**. Παρατηρούμε ότι είναι ενεργοποιημένη η επιλογή **Sign**, στην συγκεκριμένη περίπτωση ενεργοποιούμε και την επιλογή **Encrypt**.



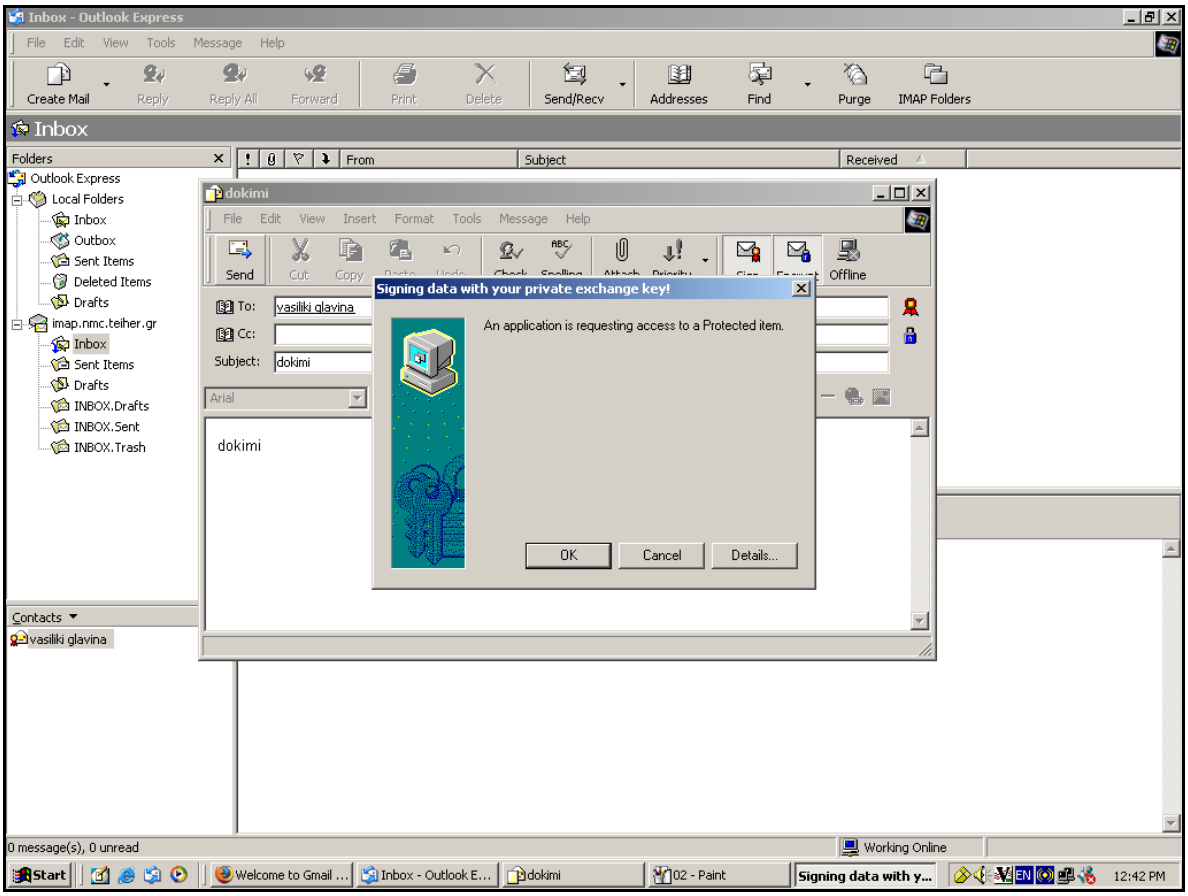
Σχήμα 12. Δημιουργία νέου μηνύματος.

Εισάγουμε το όνομα, γράφουμε το μήνυμα και το στέλνουμε πατώντας **Send**.



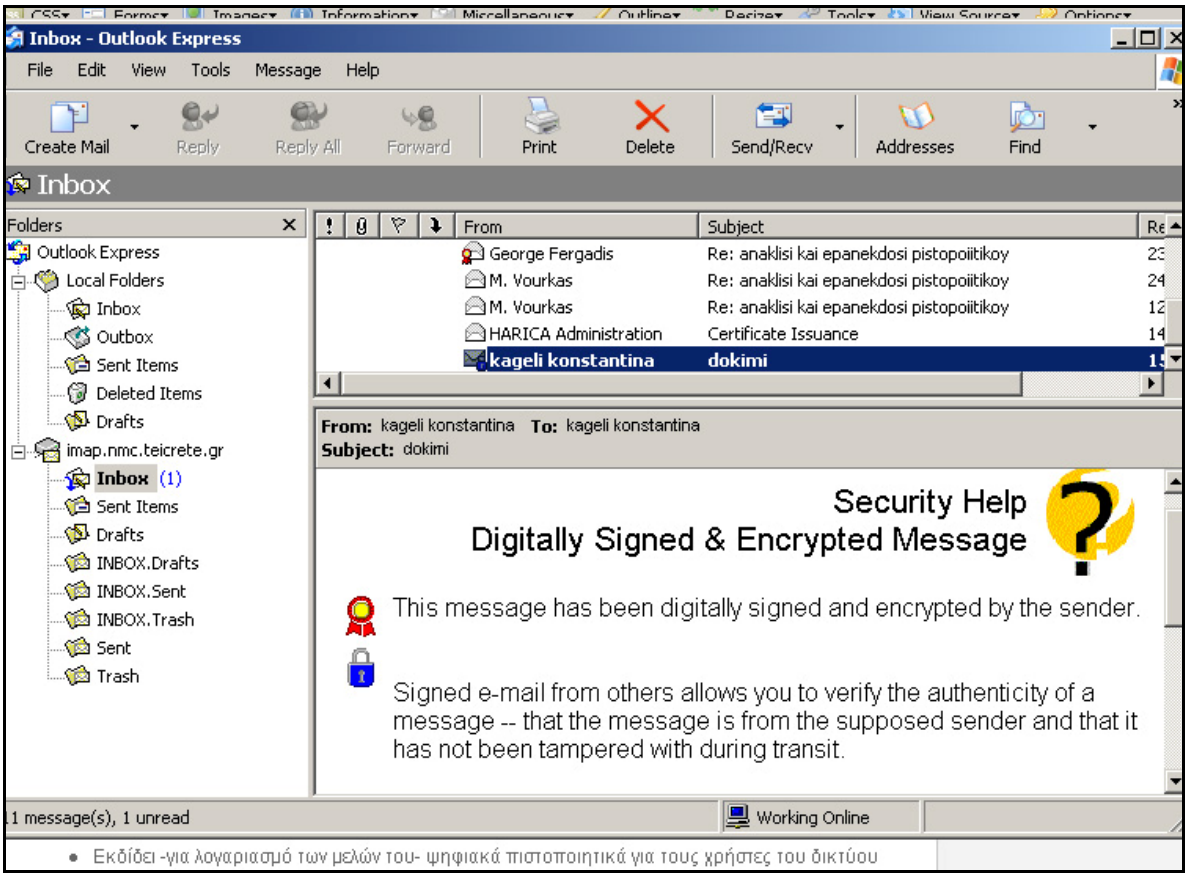
Σχήμα 13. Αποστολή μηνύματος.

Ένα προειδοποιητικό μήνυμα μας ενημερώνει ότι κάποια εφαρμογή πρόκειται να χρησιμοποιήσει το προσωπικό κλειδί μας. Πατάμε ok.



Σχήμα 14. Μήνυμα ασφαλείας.

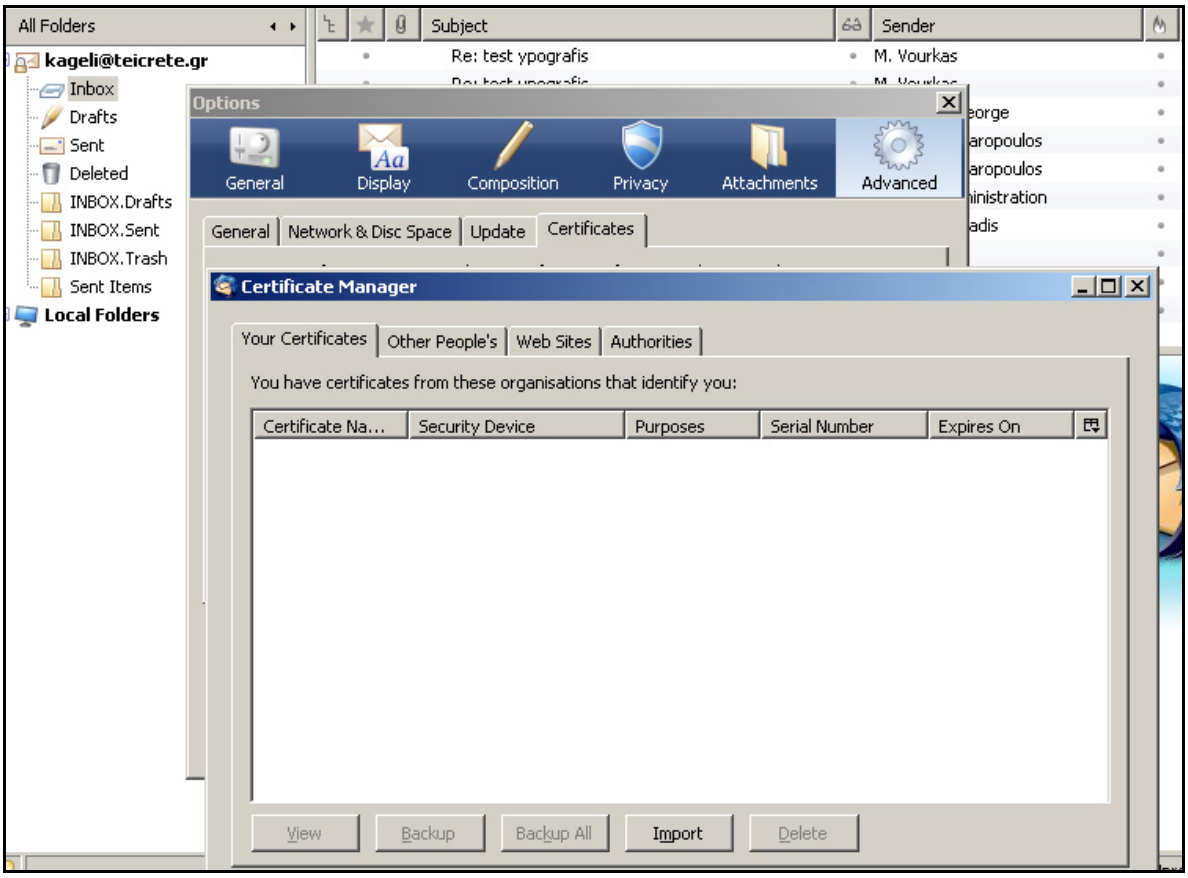
Το μήνυμα φτάνει στο λογαριασμό του παραλήπτη και εμφανίζεται μαρκαρισμένο ως υπογεγραμμένο και κρυπτογραφημένο. Επιλέγοντας να ανοίξουμε το μήνυμα αρχικά εμφανίζεται μια εισαγωγική σελίδα που μας λέει ότι το συγκεκριμένο μήνυμα είναι υπογεγραμμένο και κρυπτογραφημένο από τον αποστολέα. Για να μπορέσουμε να δούμε τα περιεχόμενα του μηνύματος πατάμε το κουμπί **Continue** που βρίσκεται στην εισαγωγική σελίδα.



Σχήμα 15. Εμφάνιση μηνύματος.

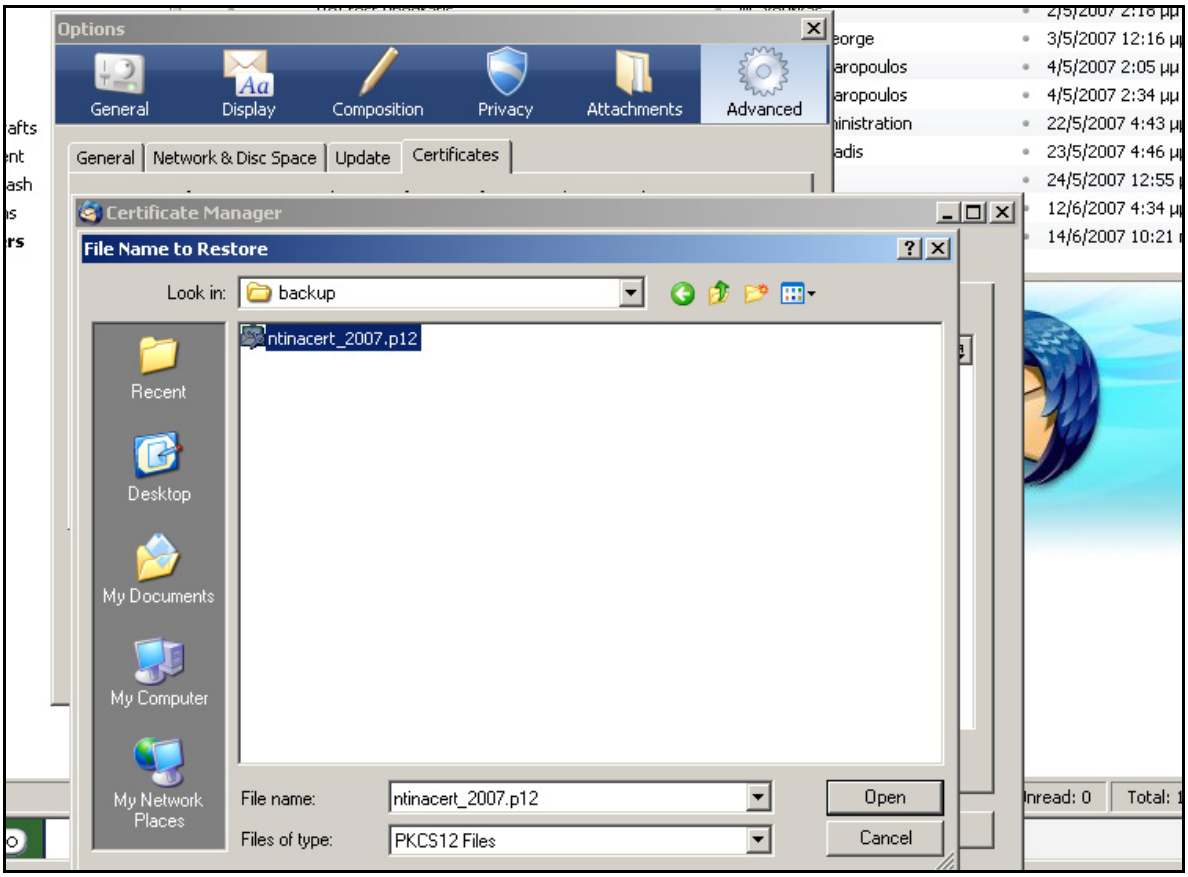
- Thunderbird

Σε αντίθεση με το Outlook Express που αντλεί τα εγκατεστημένα πιστοποιητικά από τον Internet Explorer, στο Thunderbird δεν συμβαίνει το ίδιο. Άσχετα με το αν υπάρχουν εγκατεστημένα πιστοποιητικά στο Mozilla Firefox, πρέπει να τα εγκαταστήσουμε εκ νέου. Από το μενού **Tools** / **Options**, επιλέγουμε **Advanced**, στην καρτέλα **Certificates** πατάμε το κουμπί **View Certificates** και στην καρτέλα **Your Certificates** πατάμε το κουμπί **Import** για να εγκαταστήσουμε το προσωπικό πιστοποιητικό του χρήστη.



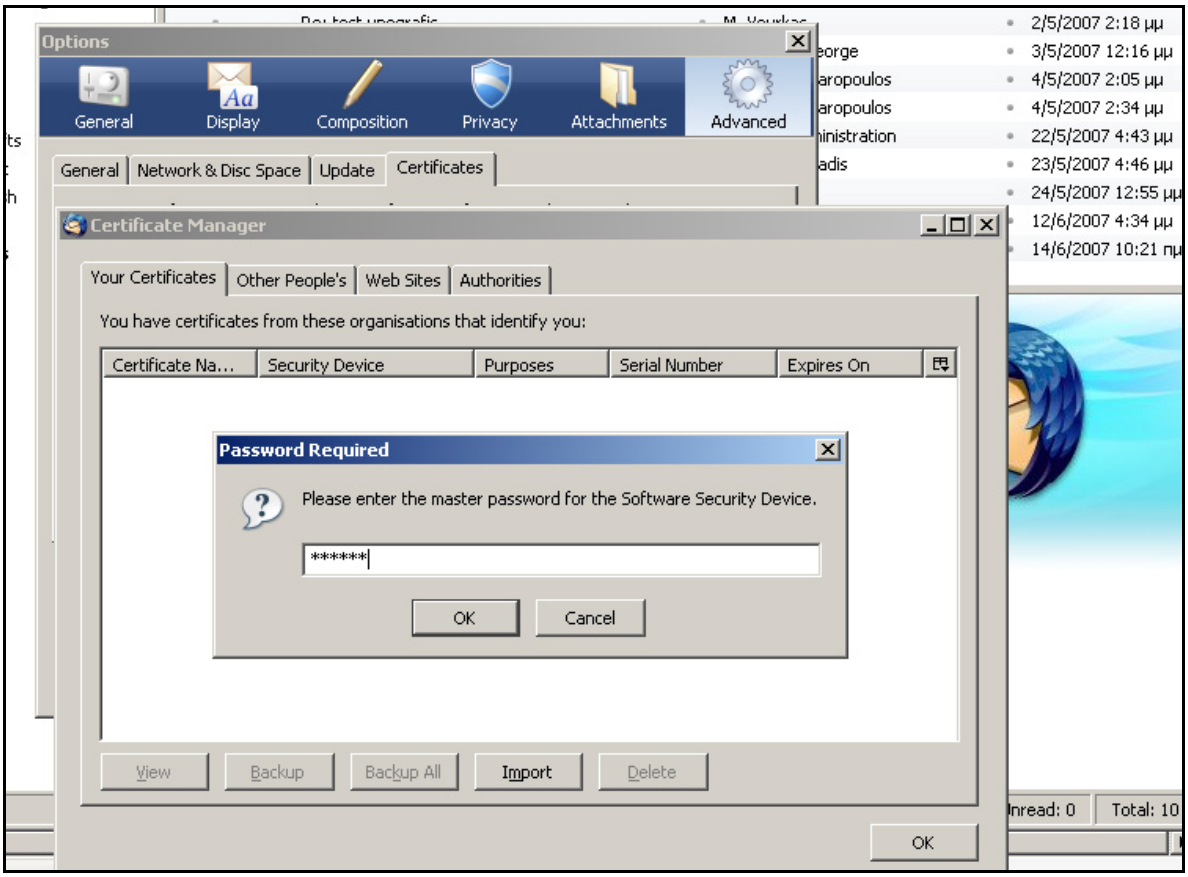
Σχήμα 16. Εισαγωγή προσωπικού πιστοποιητικού στο Thunderbird.

Εντοπίζουμε την τοποθεσία που έχουμε αποθηκεύσει το backup αρχείο του προσωπικού πιστοποιητικού και πατάμε **Open.**



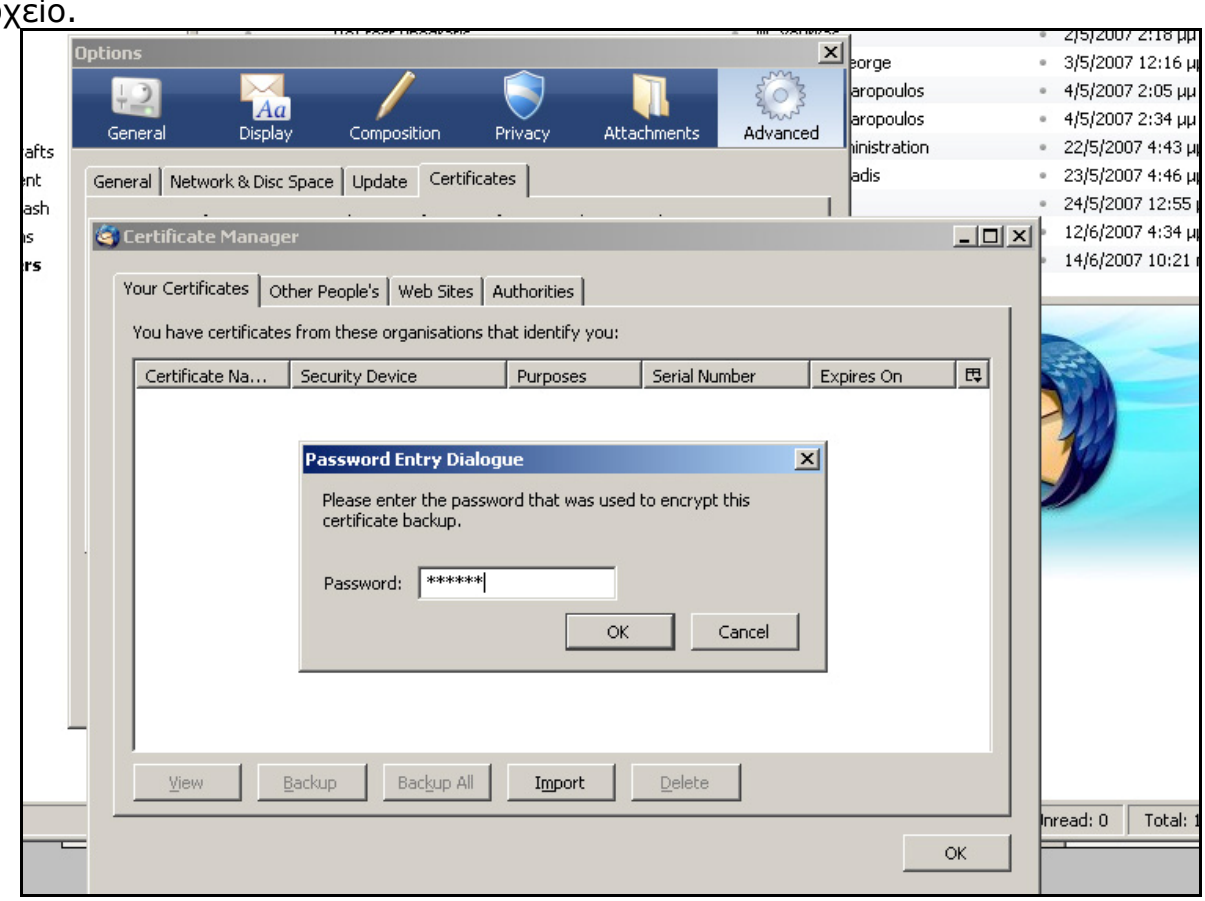
Σχήμα 17. Άνοιγμα πιστοποιητικού για εγκατάσταση.

Δίνουμε τον κωδικό με τον οποίο έχει κρυπτογραφηθεί το κλειδί (master password).



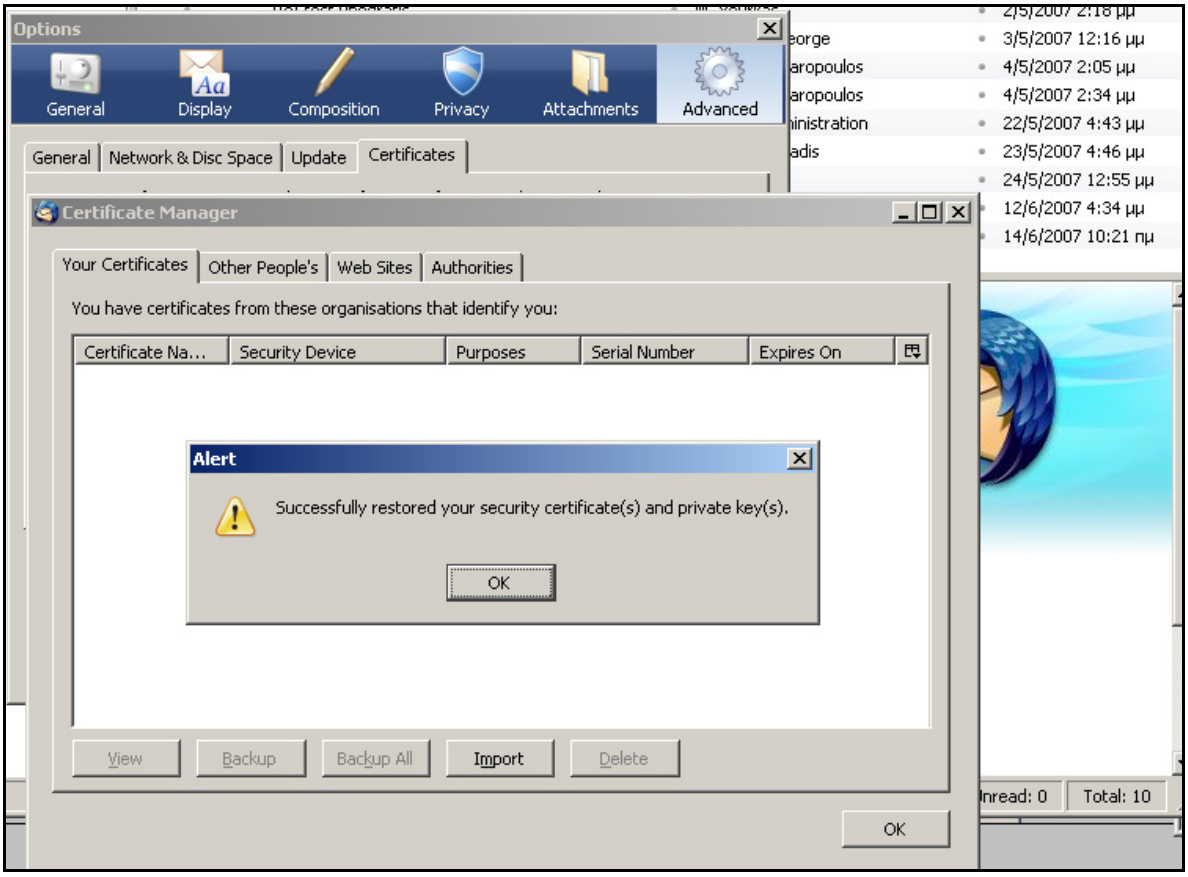
Σχημα 18. Εισαγωγή master password.

Έπειτα δίνουμε τον κωδικό με τον οποίο έχει κρυπτογραφηθεί το backup αρχείο.



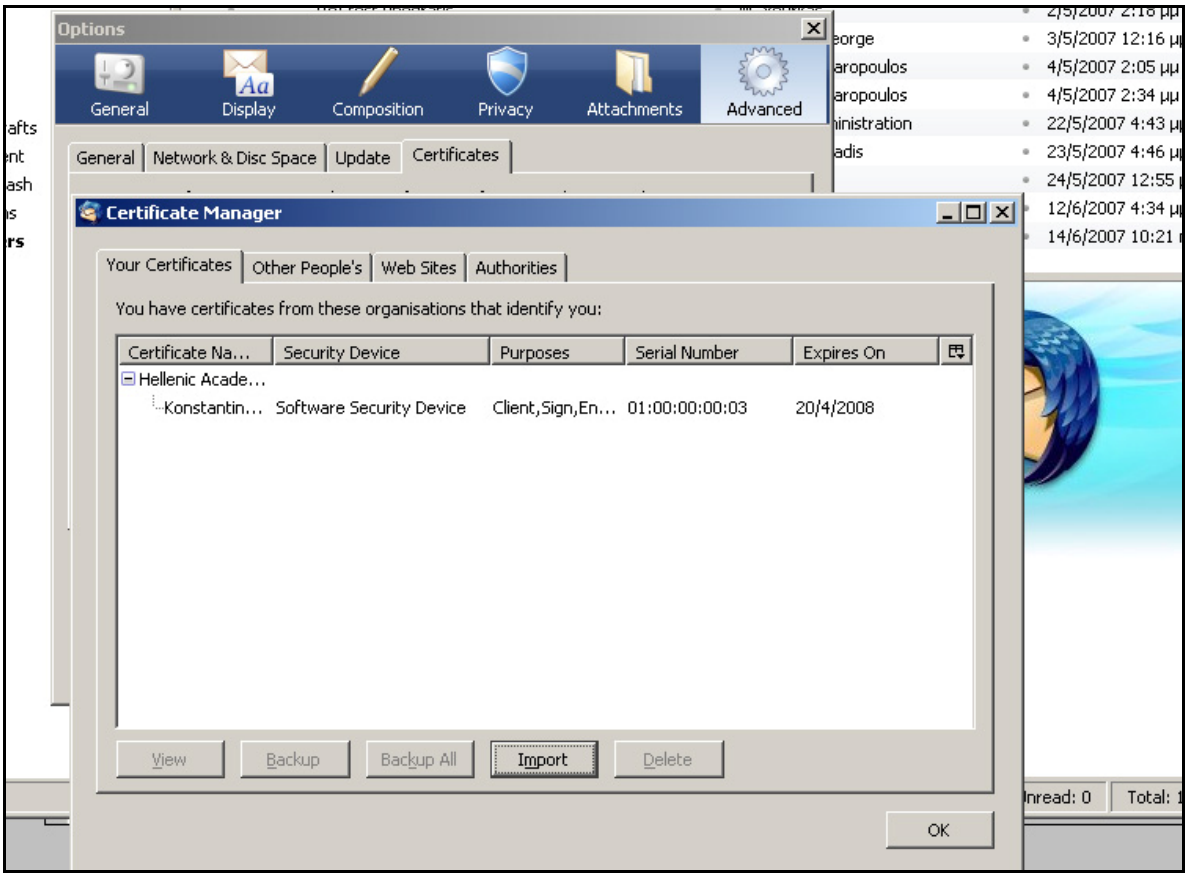
Σχήμα 19. Εισαγωγή κωδικού προστασίας για το backup αρχείο.

Το πρόγραμμα μας ενημερώνει ότι έγινε επιτυχώς η εγκατάσταση του πιστοποιητικού.



Σχήμα 20. Μήνυμα επιτυχούς εγκατάστασης πιστοποιητικού.

Εμφανίζεται το πιστοποιητικό στα εγκατεστημένα προσωπικά πιστοποιητικά.

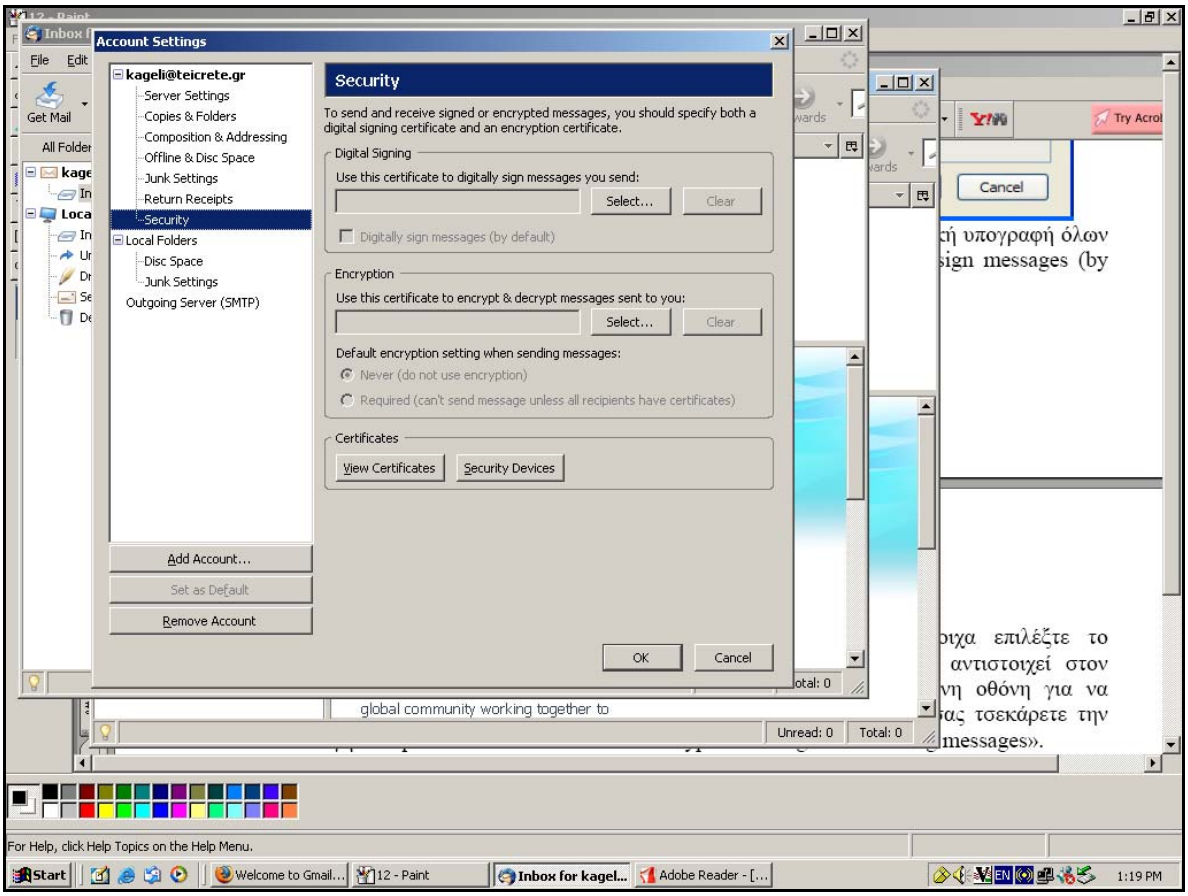


Σχήμα 21. Εμφάνιση πιστοποιητικού.

Σημείωση:

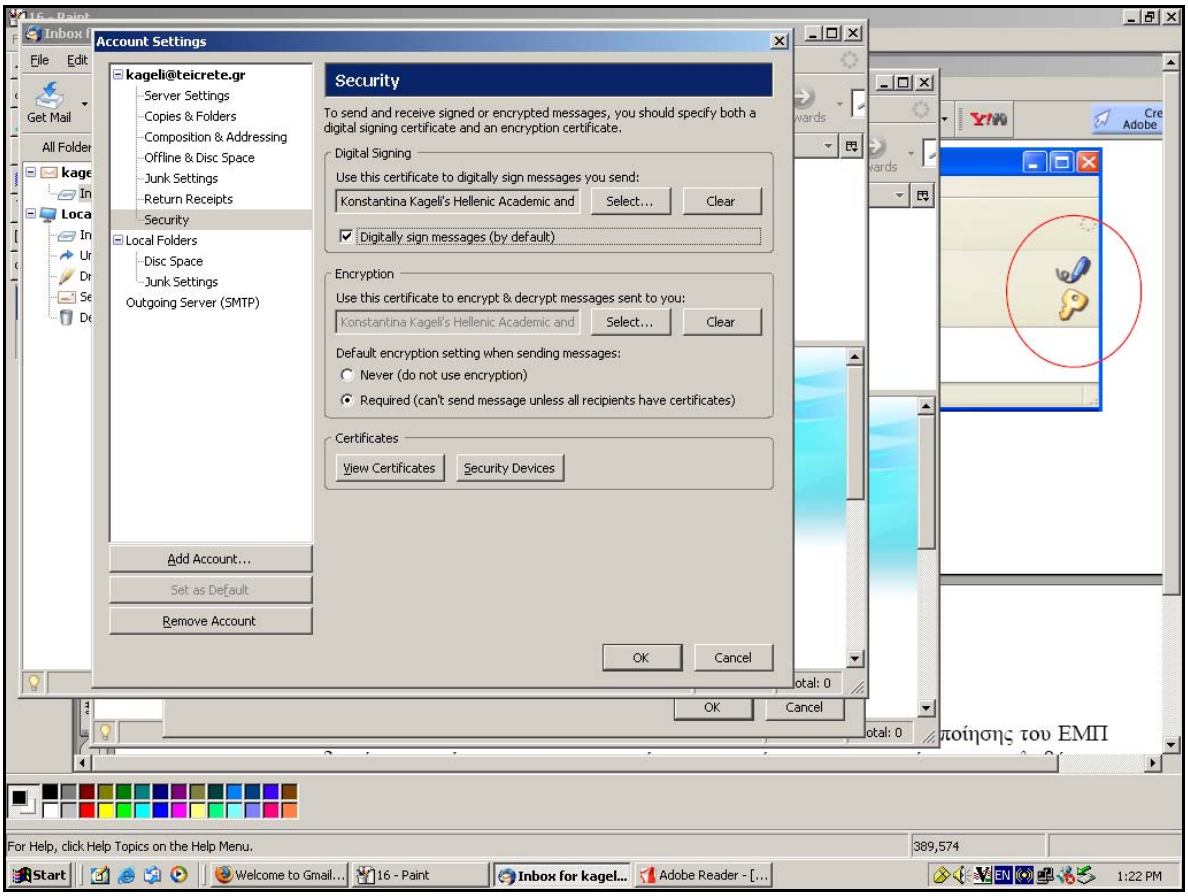
Σε περίπτωση που στο σκοπό χρήσης (Purposes) του πιστοποιητικού εμφανίζεται η ένδειξη «None» πηγαίνουμε στην καρτέλα **Authorities**, βρίσκουμε το πιστοποιητικό της HARICA, κάνουμε **Edit** και τσεκάρουμε και τις τρεις επιλογές που εμφανίζει.

Από το μενού **Tools/ Account Settings** επιλέγοντας **Security** μπορούμε να ορίσουμε ποιο πιστοποιητικό θα χρησιμοποιείται για ψηφιακή υπογραφή των emails και από ποιο πιστοποιητικό αντλείται το δημόσιο κλειδί για την κρυπτογράφηση μηνυμάτων που στέλνονται σε αυτό το λογαριασμό. Πατώντας το κουμπί **Select** επιλέγουμε εμείς τα πιστοποιητικά.



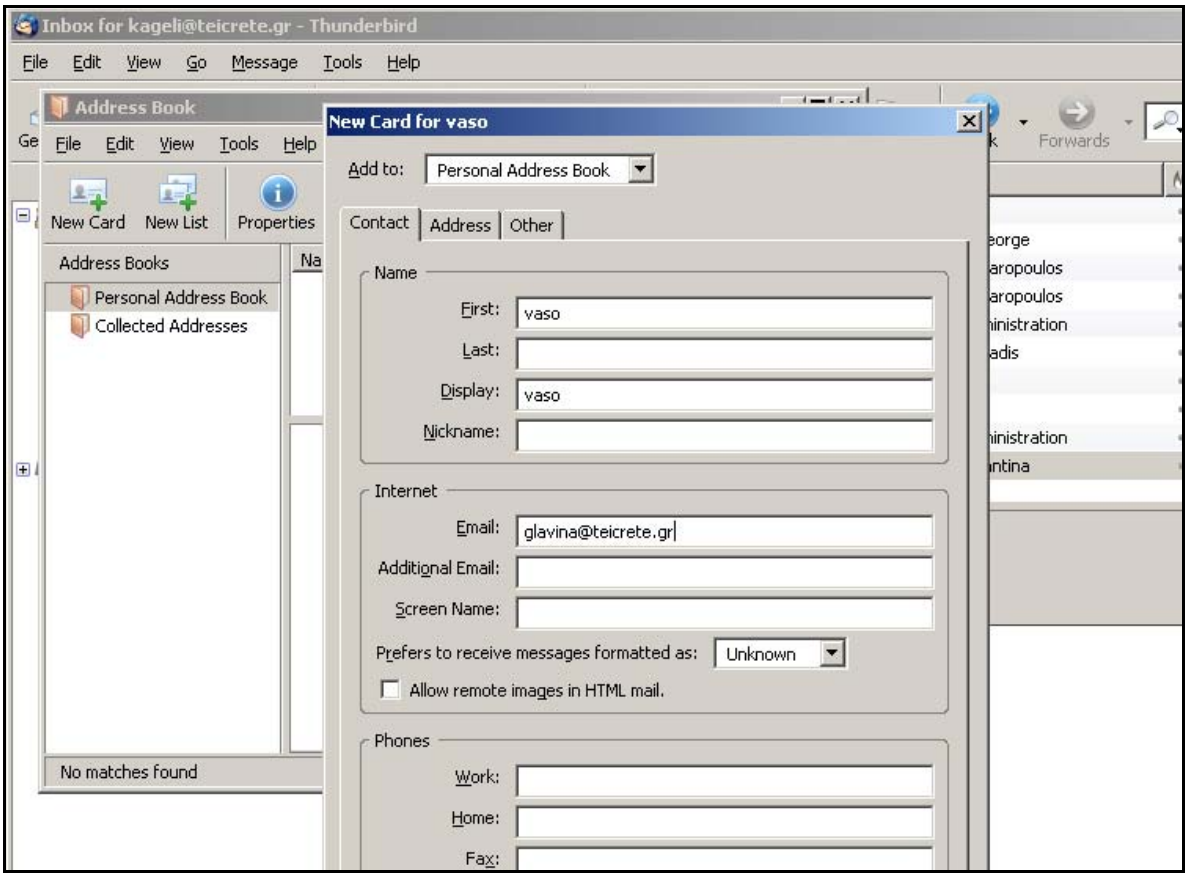
Σχήμα 22. Ορισμός πιστοποιητικών για χρήση από το Thunderbird.

Στο Thunderbird μπορούμε να ρυθμίσουμε να υπογράφονται ψηφιακά, με το επιλεγμένο ψηφιακό πιστοποιητικό, όλα τα εξερχόμενα μηνύματα. Επίσης μπορούμε να επιλέξουμε να κρυπτογραφούνται τα μηνύματα με την προϋπόθεση ότι έχουμε το ψηφιακό πιστοποιητικό του παραλήπτη. Για την ενεργοποίηση τους τσεκάρουμε τις αντίστοιχες επιλογές στο μενού **Tools/ Account Settings**, **Security.** Είναι προτιμότερο να επιλέξουμε την υπογραφή όλων των εξερχόμενων μηνυμάτων μόνο και όχι την κρυπτογράφηση γιατί δεν θα μπορεί να σταλεί το email σε πρόσωπα για τα οποία δεν έχουν ψηφιακό πιστοποιητικό.



Σχήμα 23. Ρύθμιση επιλογών υπογραφής και κρυπτογράφησης μηνυμάτων.

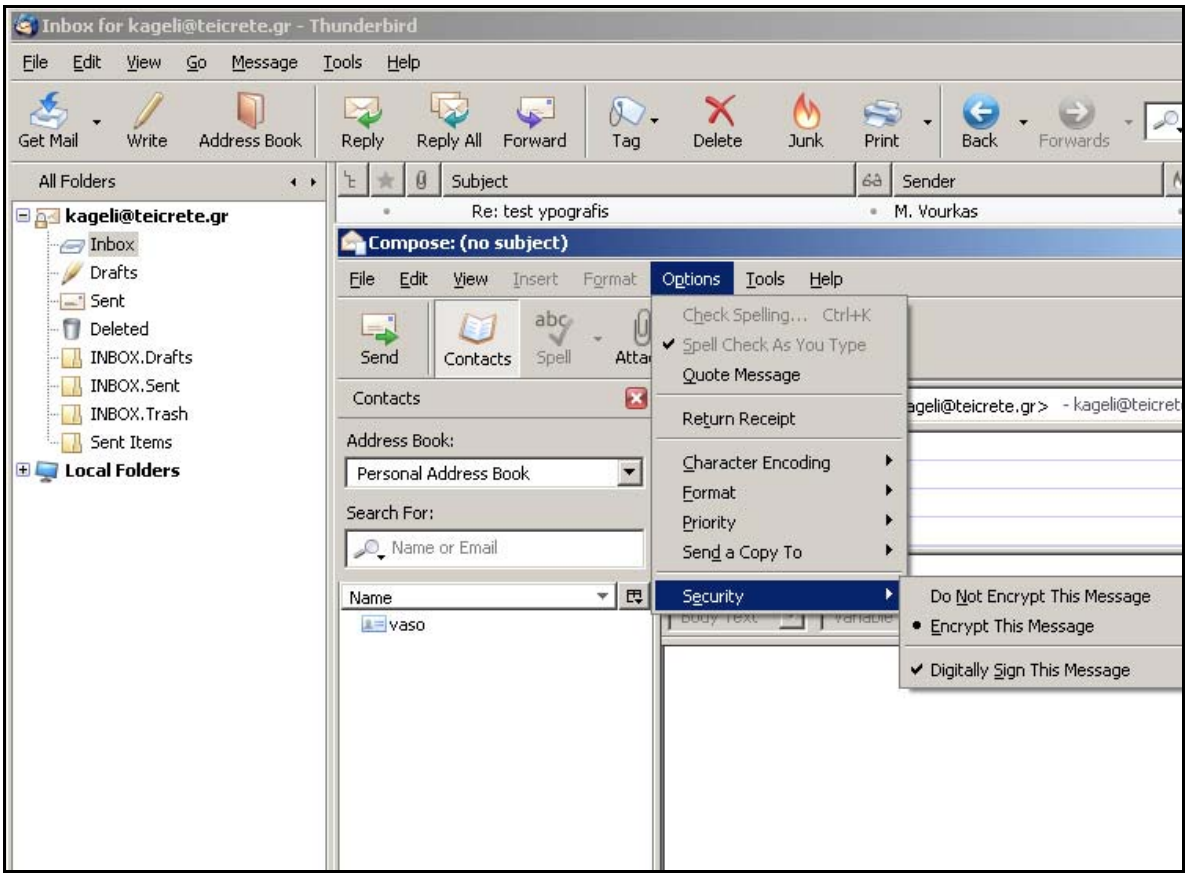
Για να καταχωρήσουμε διευθύνσεις email άλλων προσώπων και τα ψηφιακά πιστοποιητικά τους, στις επαφές του λογαριασμού, από το μενού **Tools / Address Book**, πατάμε **New** και επιλέγουμε **New Card**. Δημιουργούμε νέα επαφή. Καταχωρούμε τα στοιχεία του προσώπου στην καρτέλα.



Σχήμα 24. Εισαγωγή στοιχείων νέας επαφής.

Τα ψηφιακά πιστοποιητικά των προσώπων που είναι αποθηκευμένα στις επαφές τα αποθηκεύουμε στη καρτέλα Certificates και με βάση το email τα συσχετίζει με τα αντίστοιχα Contacts.

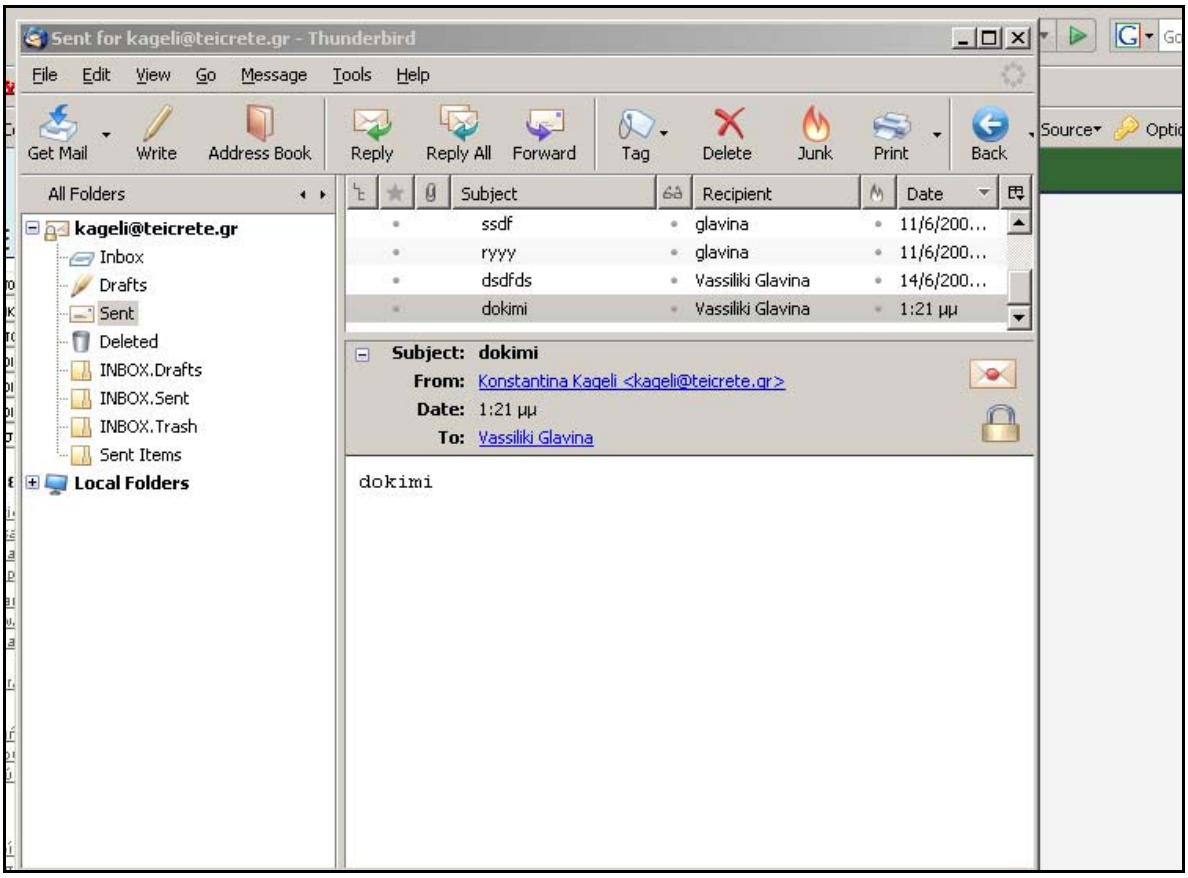
Για να δούμε την εφαρμογή των ρυθμίσεων που κάναμε θα στείλουμε ένα δοκιμαστικό email. Πατάμε το κουμπί **Write** από το μενού, εισάγουμε τον παραλήπτη, γράφουμε το μήνυμα και επιλέγουμε **Options / Security**. Παρατηρούμε ότι είναι ενεργοποιημένη η υπογραφή του μηνύματος, στη συγκεκριμένη περίπτωση θα επιλέξουμε και κρυπτογράφηση.



Σχήμα 24. Δημιουργία μηνύματος.

Στη συνέχεια στέλνουμε το μήνυμα πατώντας **Send**.

Ανοίγοντας το μήνυμα βλέπουμε ότι είναι μαρκαρισμένο ως υπογεγραμμένο και κρυπτογραφημένο. Πατώντας το σχετικό εικονίδιο μπορούμε να δούμε το ψηφιακό πιστοποιητικό του αποστολέα.

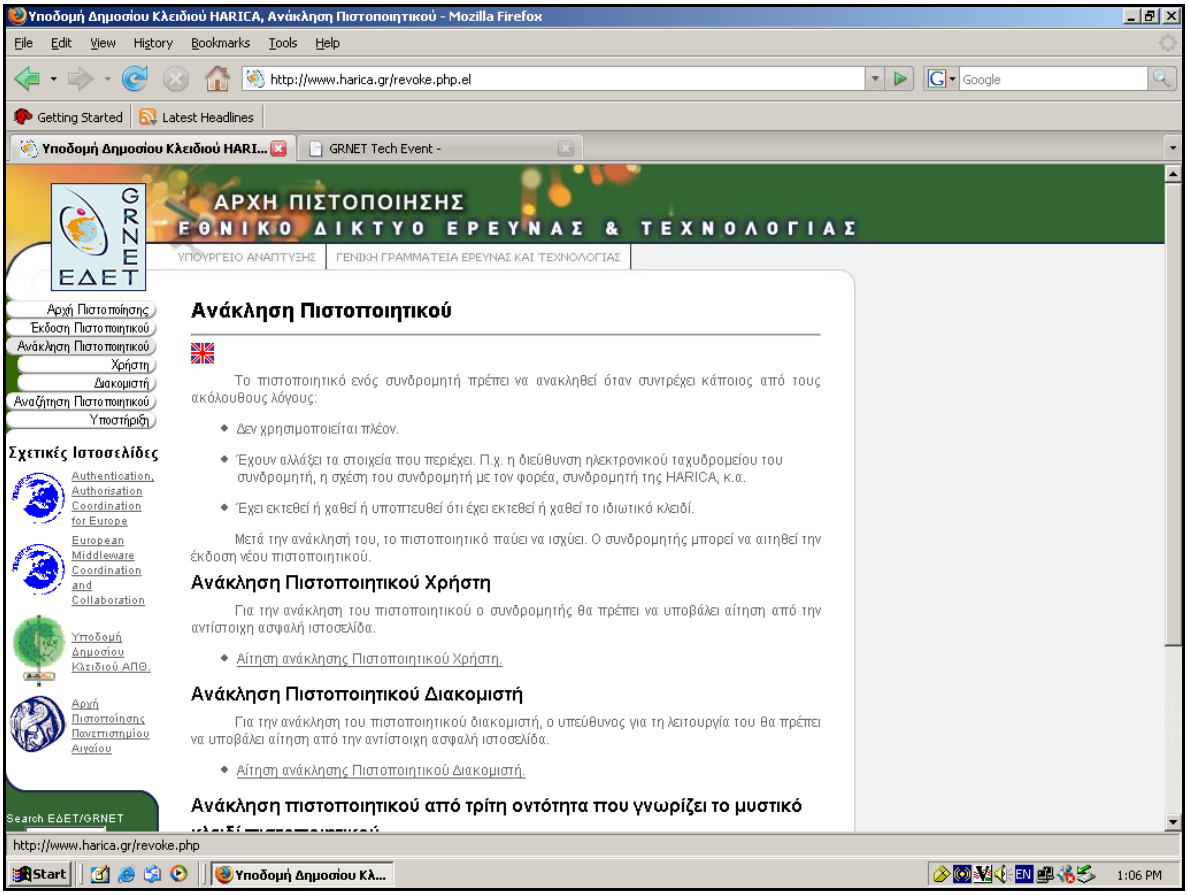


Σχήμα 25. Εμφάνιση μηνύματος.

Παράρτημα Ι

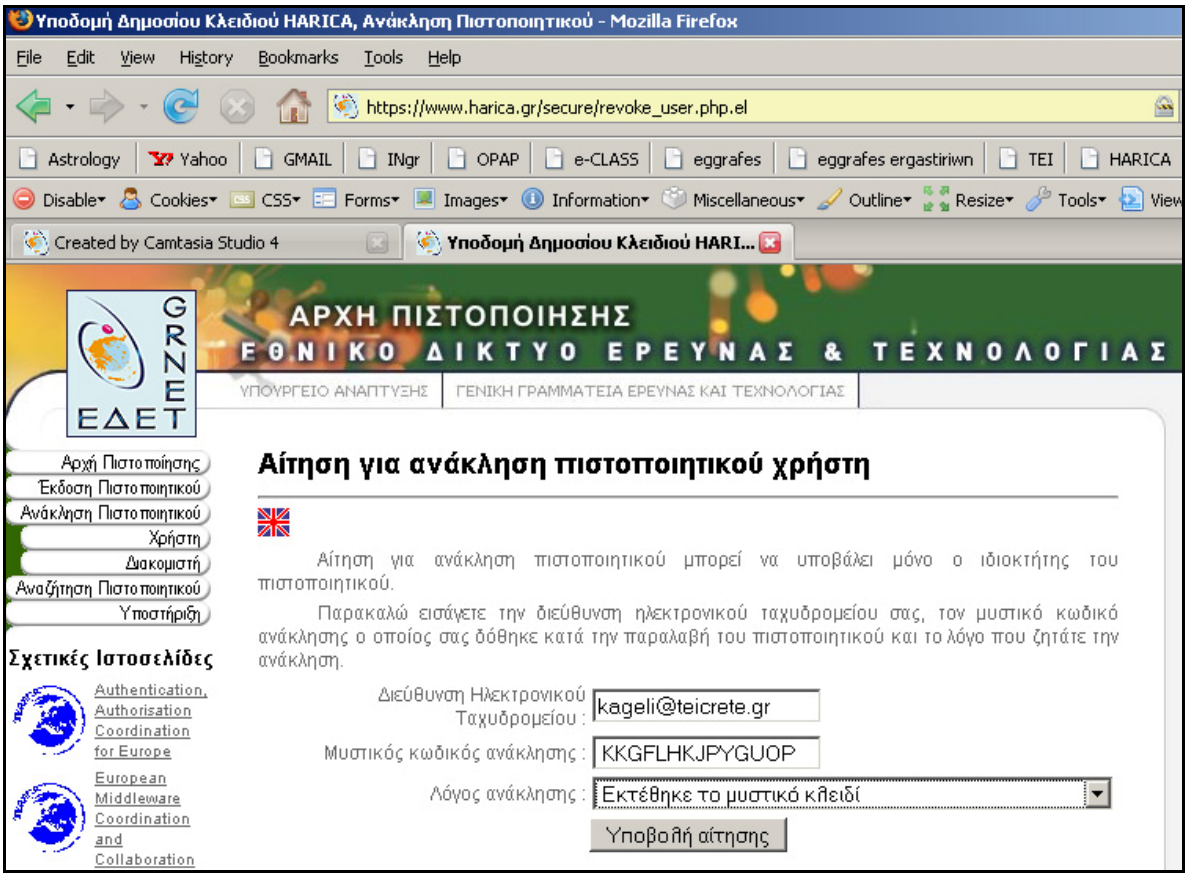
Οδηγίες για ανάκληση πιστοποιητικού χρήστη

Επισκεπτόμαστε τη σελίδα της HARICA και επιλέγουμε ανάκληση πιστοποιητικού. Μεταφερόμαστε στην επόμενη σελίδα όπου και επιλέγουμε ανάκληση για πιστοποιητικό χρήστη.



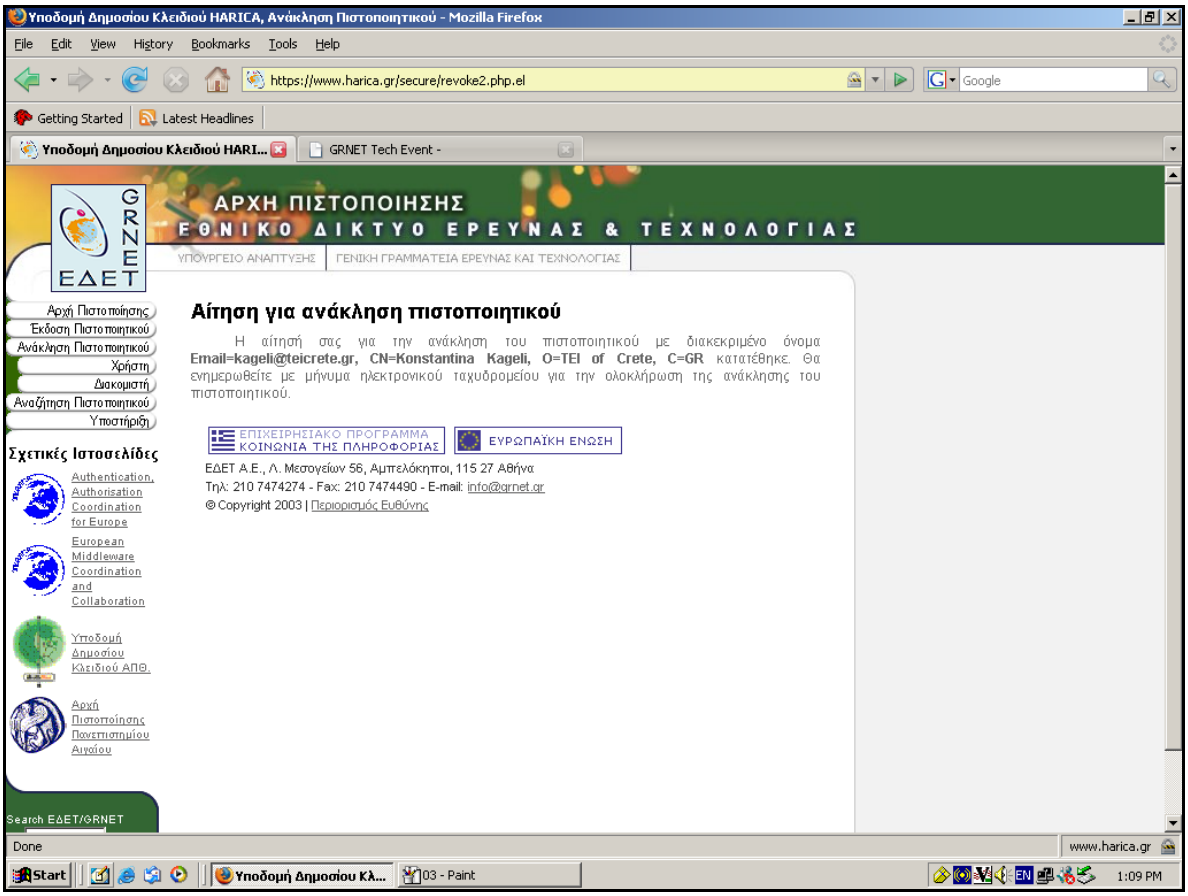
Σχήμα 1. Επιλογή ανάκλησης πιστοποιητικού χρήστη.

Μας ζητείται από την υπηρεσία να δώσουμε το email του χρήστη, τον κωδικό ανάκλησης και να προσδιορίσουμε το λόγο για τον οποίο ζητείται η ανάκληση.



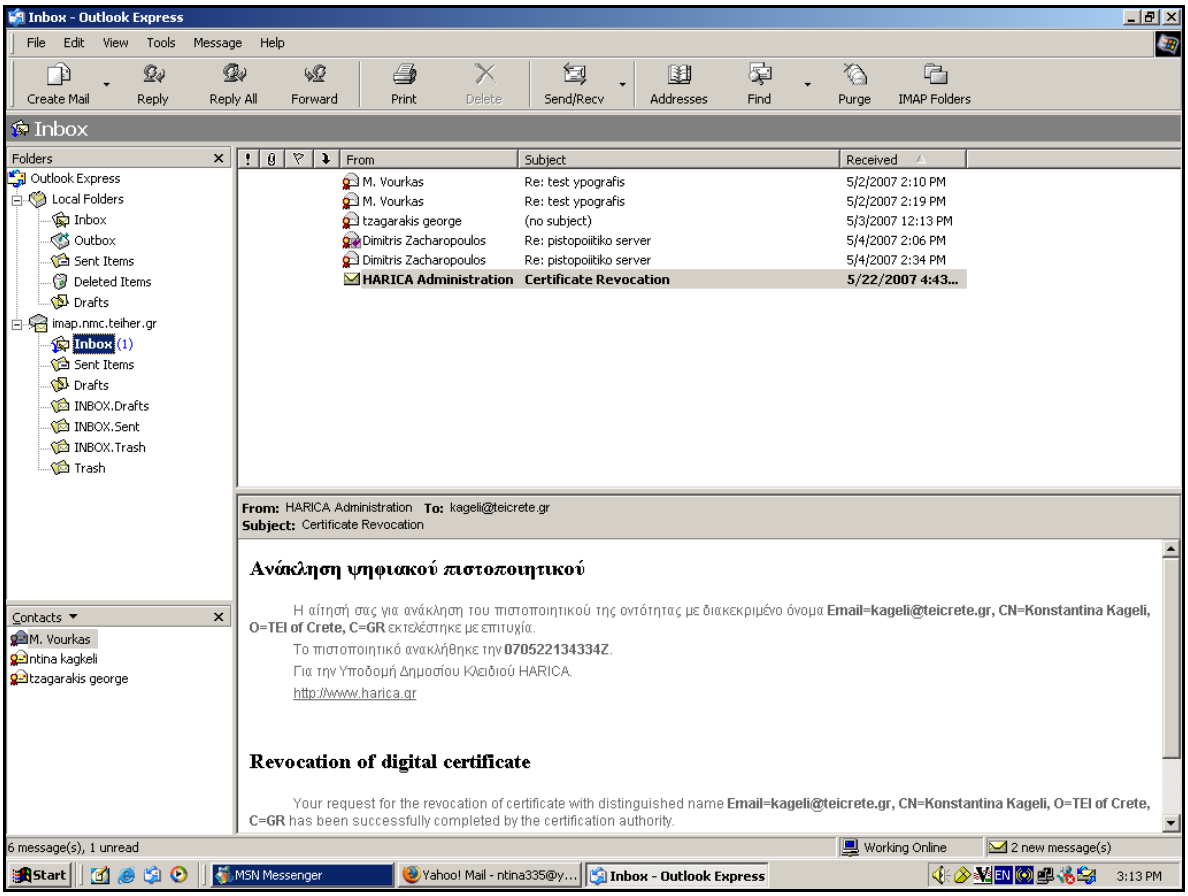
Σχήμα 2. Αίτηση για ανάκληση πιστοποιητικού χρήστη.

Η υπηρεσία μας ενημερώνει οτι η αίτηση ανάκλησης κατατέθηκε και θα ειδοποιηθούμε για την οριστικοποίηση της με email.



Σχήμα 3. Κατάθεση αίτησης για ανάκληση.

Αφού η Αρχή Πιστοποίησης πραγματοποιήσει την ανάκληση, αποστέλλεται το email για επιβεβαίωση της ανάκλησης.

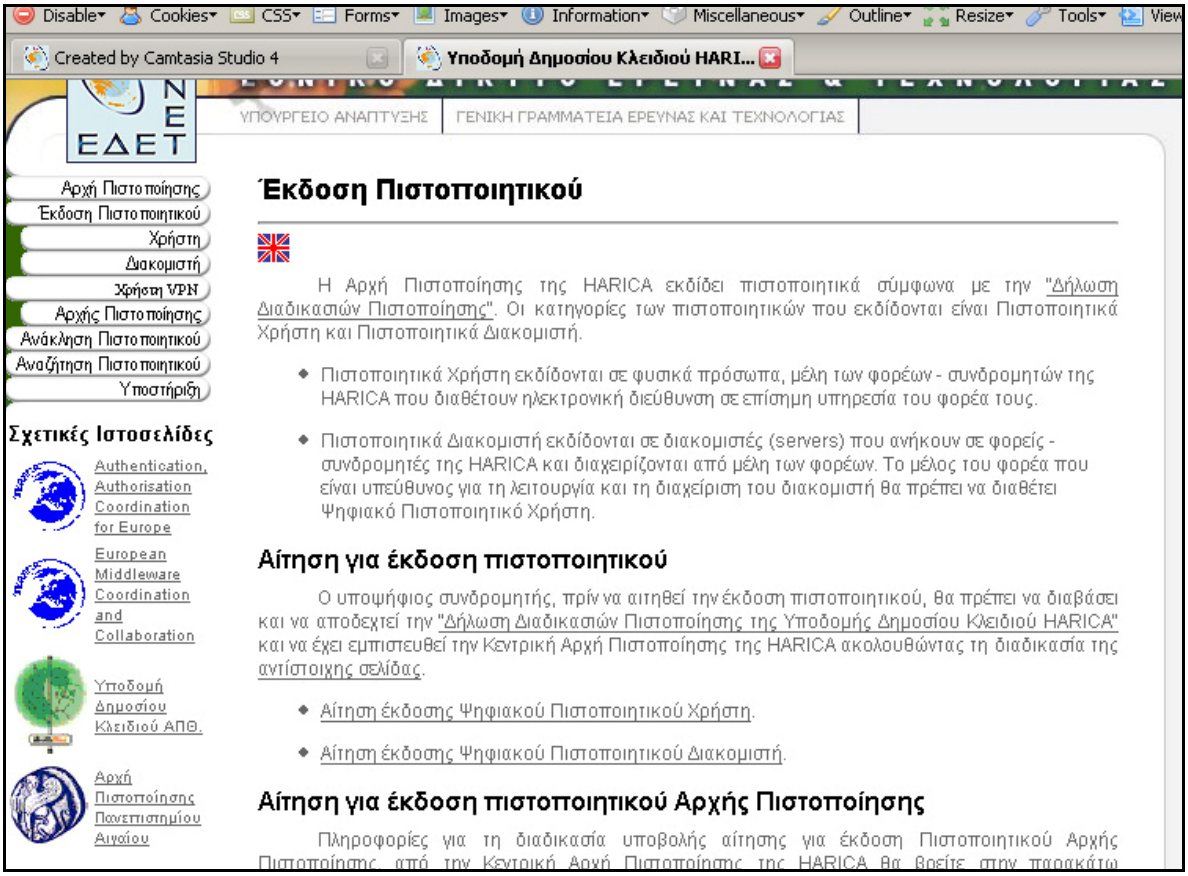


Σχήμα 4. Email για επιβεβαίωση ανάκλησης.

Παράρτημα Κ

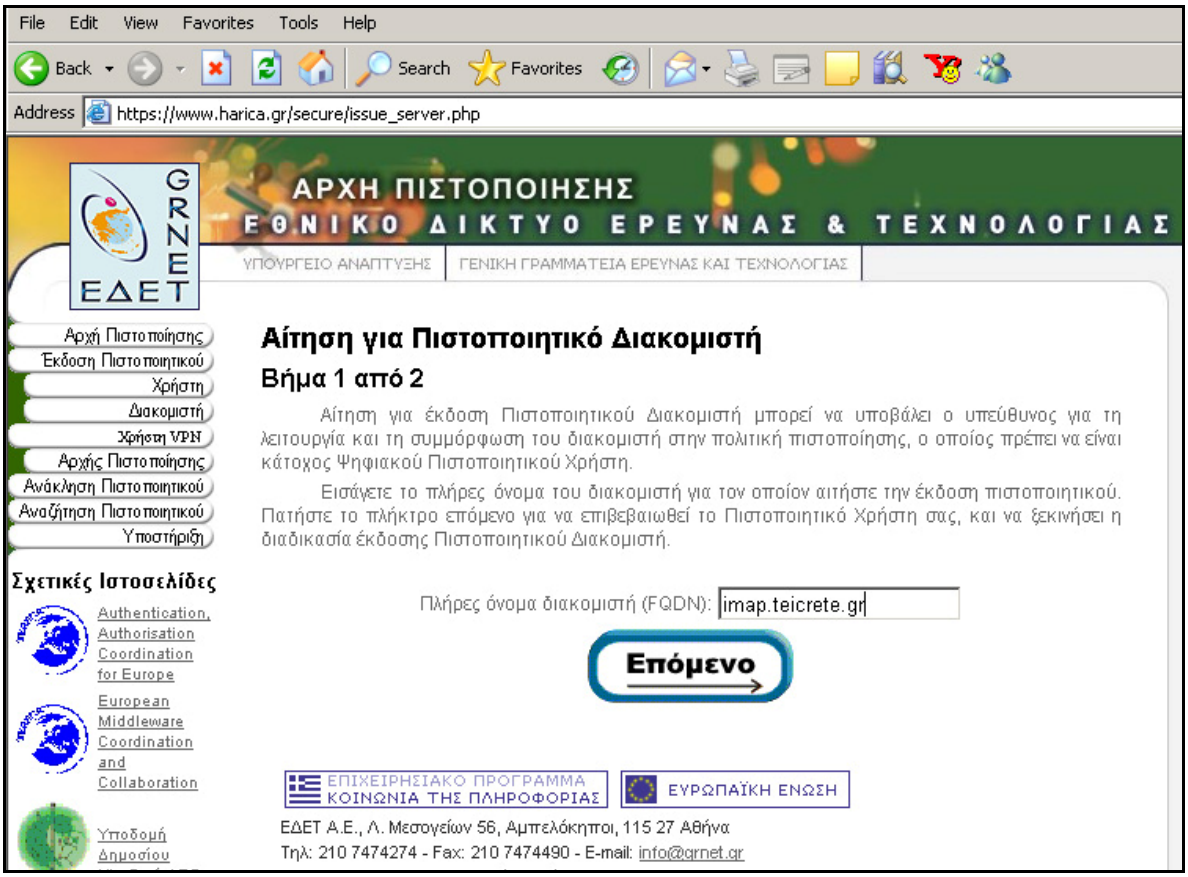
Οδηγίες για υποβολή αίτησης για πιστοποιητικό διακομιστή

Για να κάνουμε αίτηση για πιστοποιητικό διακομιστή, επισκεπτόμαστε τη σελίδα έκδοσης πιστοποιητικών της HARICA και επιλέγουμε το σχετικό σύνδεσμο.



Σχήμα 1. Επιλογή έκδοσης πιστοποιητικού για διακομιστή.

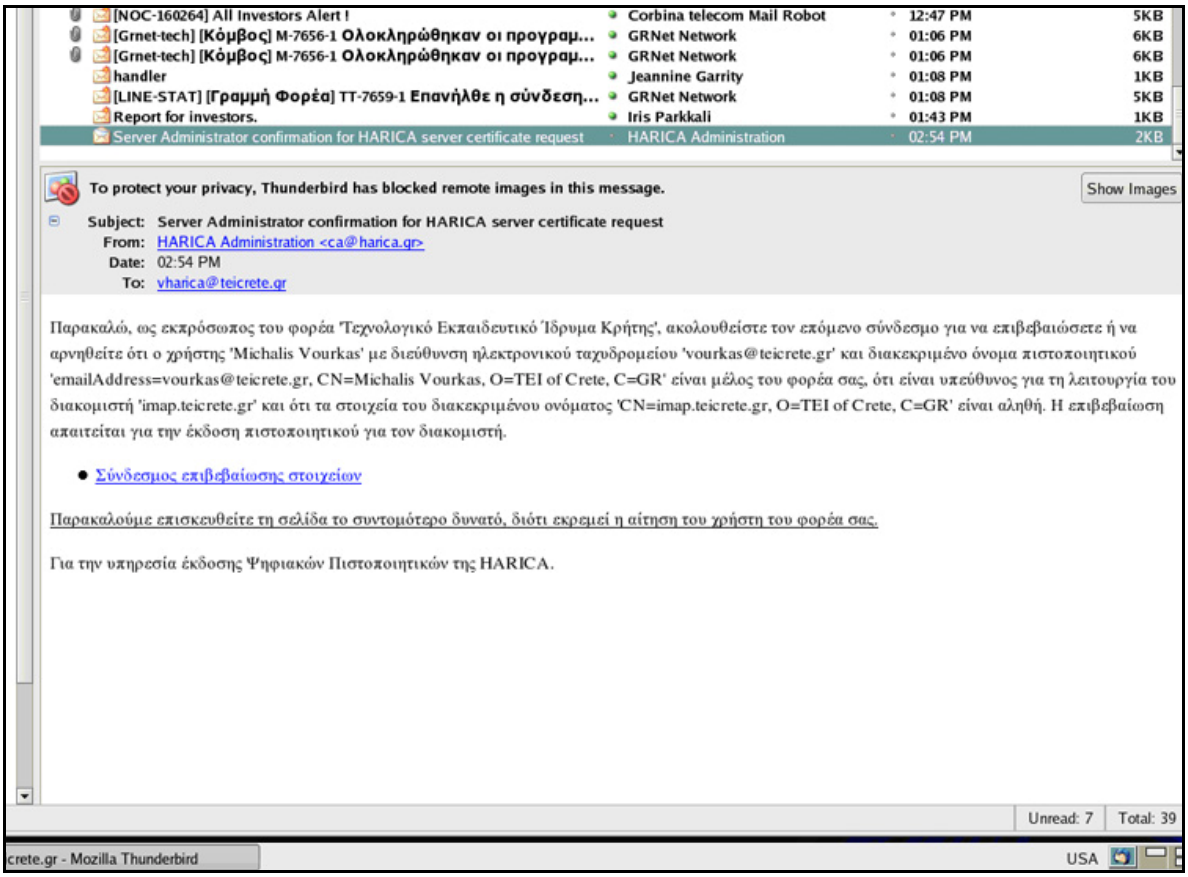
Αρχικά δίνουμε το όνομα του διακομιστή και πατάμε **next**.



Σχήμα 2. Εισαγωγή ονόματος διακομιστή.

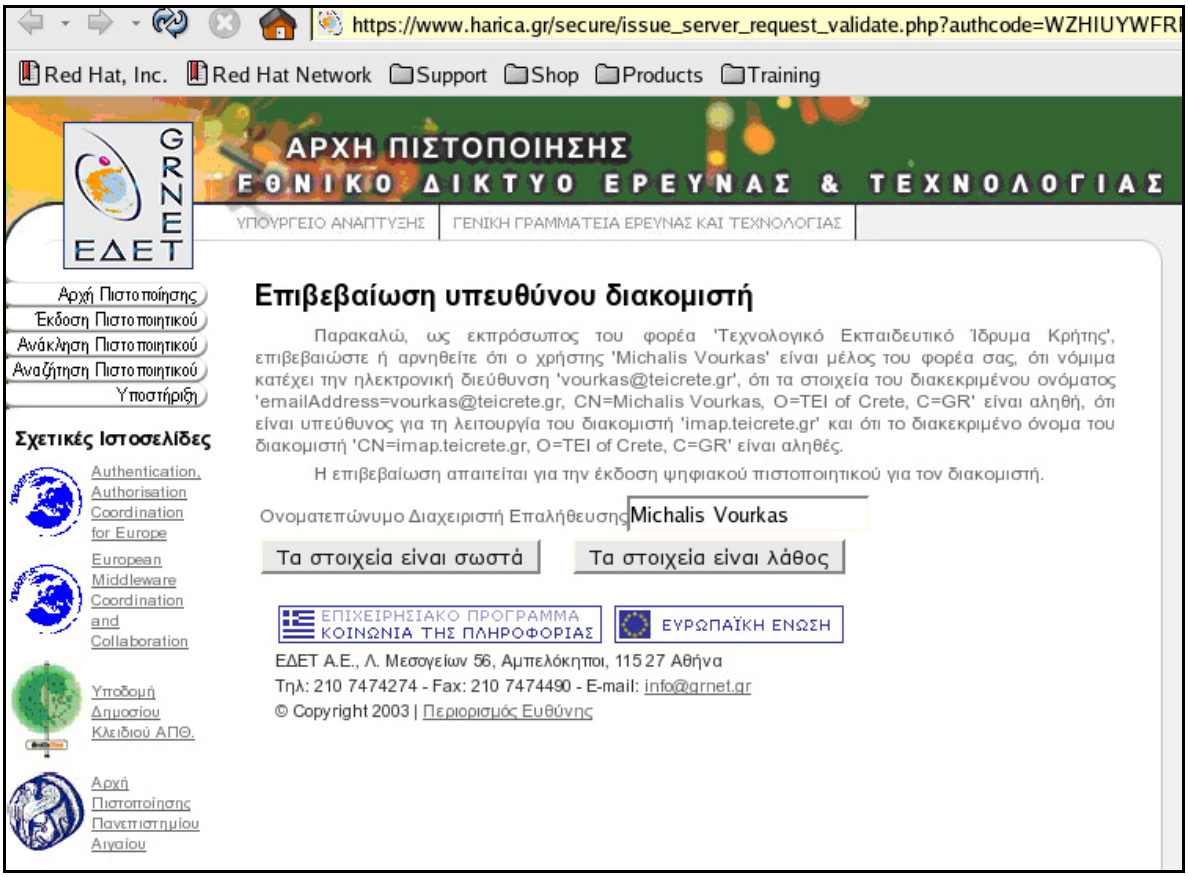
Χρειάζεται τη διαδικασία να την κάνει ο διαχειριστής του διακομιστή ώστε να έχει πρόσβαση στους μυστικούς κωδικούς ασφαλείας του διακομιστή.

Η υπηρεσία στέλνει μήνυμα στο διαχειριστή για να επιβεβαιώσει ότι πρόκειται να γίνει αίτηση πιστοποιητικού για το server imap.teicrete.gr, πατώντας το σχετικό σύνδεσμο που υπάρχει στο email.



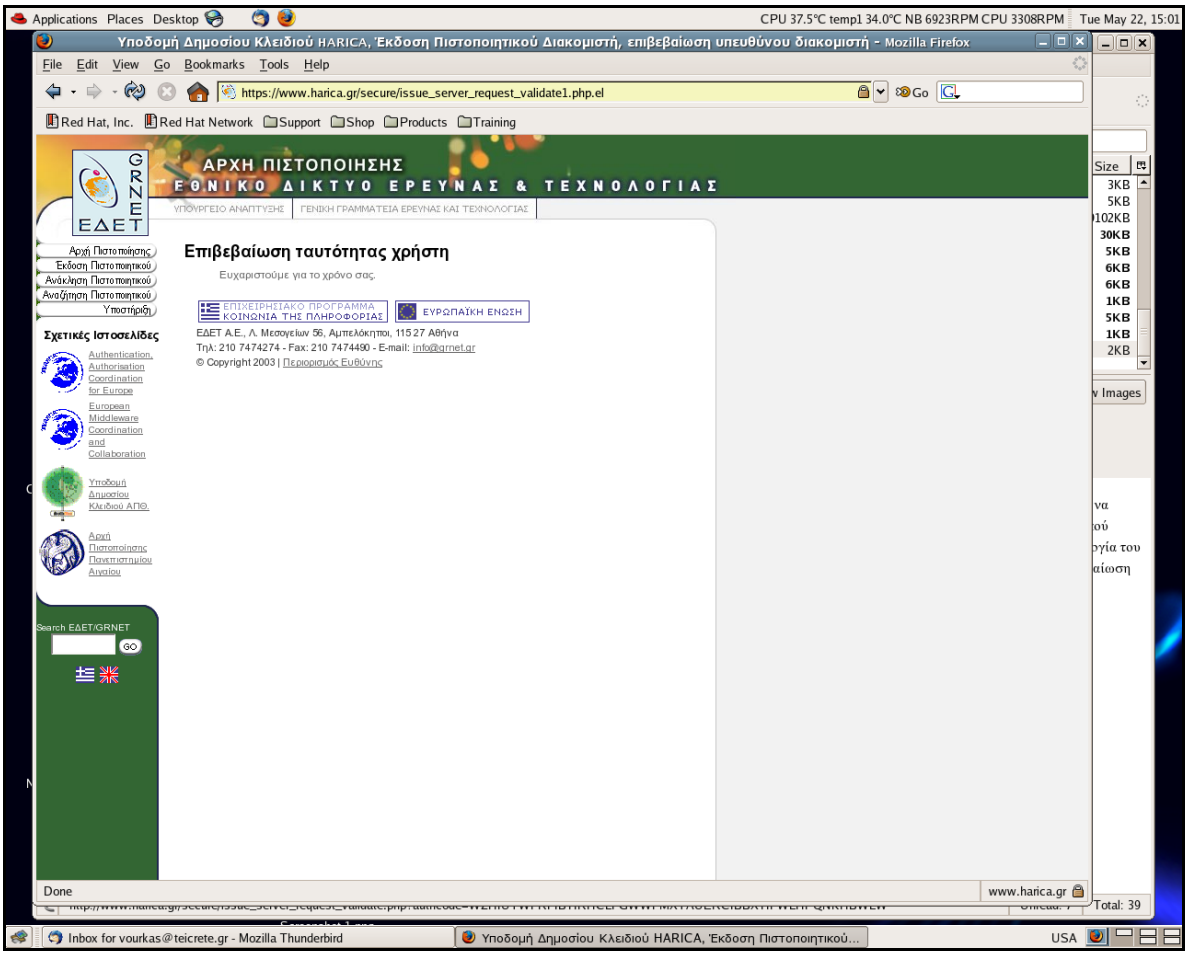
Σχήμα 3. Μήνυμα για επιβεβαίωση στοιχείων διαχειριστή και διακομιστή.

Στη συνέχεια ο διαχειριστής δίνει το όνομα του και δηλώνει ότι τα στοιχεία του πιστοποιητικού που εμφανίζονται είναι σωστά.



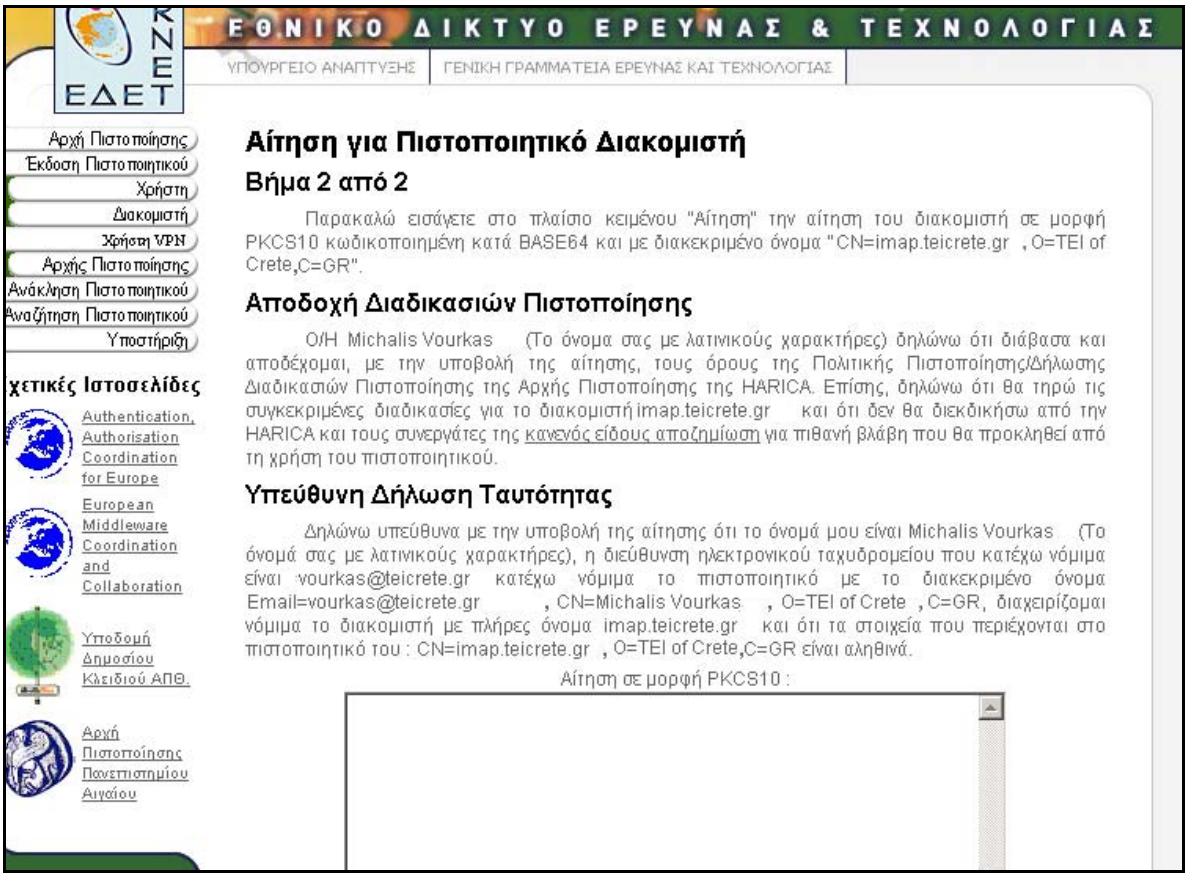
Σχήμα 4. Επιβεβαίωση στοιχείων από το διαχειριστή

Η υπηρεσία μας ειδοποιεί οτι επιβεβαιώθηκαν τα στοιχεία του διαχειριστή.



Σχήμα 5. Μήνυμα ολοκλήρωσης διαδικασίας επιβεβαίωσης στοιχείων.

Στη συνέχεια, προχωρώντας στο επόμενο βήμα, εμφανίζονται τα στοιχεία του server και του διαχειριστή και ζητείται να επικολλήσουμε την αίτηση σε μορφή PKCS10.



Σχήμα 6. Αίτηση πιστοποιητικού διακομιστή.

Ανοίγουμε ένα command prompt ή command shell και εκτελούμε τα ακόλουθα βήματα με το πρόγραμμα openssl σε Linux:

- Δημιουργούμε ένα αρχείο ρύθμισης με όνομα **servercert.cnf** με τα στοιχεία του πιστοποιητικού που θα ζητήσουμε.

```
##### BEGIN CONFIGURATION FILE #####
[ req ]
default_bits = 1024
distinguished_name = usr
prompt = no
[ usr ]
C = GR
O = TEI of Crete
CN = imap.teicrete.gr
##### END CONFIGURATION FILE #####
```

- Δημιουργούμε το ιδιωτικό κλειδί (προστατευμένο με κωδικό) το οποίο θα χρησιμοποιηθεί για το αίτημα ψηφιακού πιστοποιητικού και στη συνέχεια για τη χρήση του τελικού πιστοποιητικού. Το κλειδί θα δημιουργηθεί στο αρχείο με όνομα **server.key**, δίνοντας την παρακατω εντολή.

```
Openssl genrsa -des3 -out server.key 1024
```

- Δημιουργούμε το αίτημα ψηφιακού πιστοποιητικού (Certificate Server Request) εκτελώντας την παρακάτω εντολή. Το αίτημα θα δημιουργηθεί στο αρχείο **server.csr**

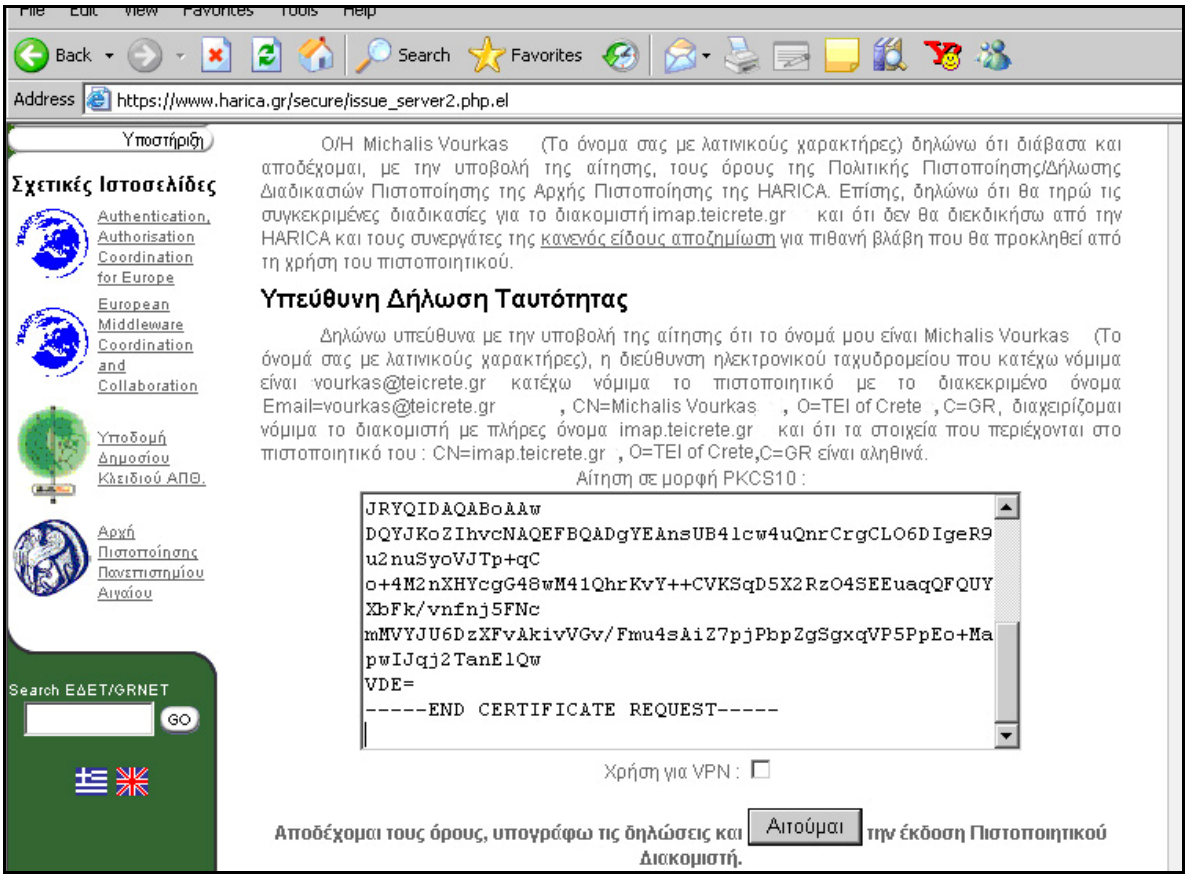
`Openssl req -new -key server.key -config my.cnf -out server.req`

Ανοίγουμε το αρχείο "server.req" και βλέπουμε το περιεχόμενό του με την εντολή
`Cat server.req`

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBfjCB6AIBADA/MQswCQYDVQQGEwJHUjEVMBMGA1UEChMMVEVJIG9mIENyZXRl
MRkwFwYDVQQDExBpbWFwLnRlaWNyZXRlLmdyMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCnsSszdInV8dyRkA1jgZjO5l9FeXnjJx3VYuJoxkviUelWnegrzGF7
N5mbgz8kwSwU8fKUBBkesIg5seI8YboeVSpHyKOJ1jO8bfNkihVp/57Xip7Aacso
v9+y5YHky7g1+v2Qs/5MvyEVqyKORQodAGp48RiT5qCKVnwiE9JRYQIDAQABoAAw
DQYJKoZIhvcNAQEFBQADgYEAnsUB4lcw4uQnrCrgCLO6DIgeR9u2nuSyoVJTp+qC
o+4M2nXHYcgG48wM41QhrKvY++CVKSqD5X2RzO4SEEuaqQFQUYXbFk/vnfnj5FNc
mMVYJU6DzXFvAkivVGv/Fmu4sAiZ7pjPbpZgSgxqVP5PpEo+MapwIJqj2TanE1Qw
VDE=
-----END CERTIFICATE REQUEST-----
```

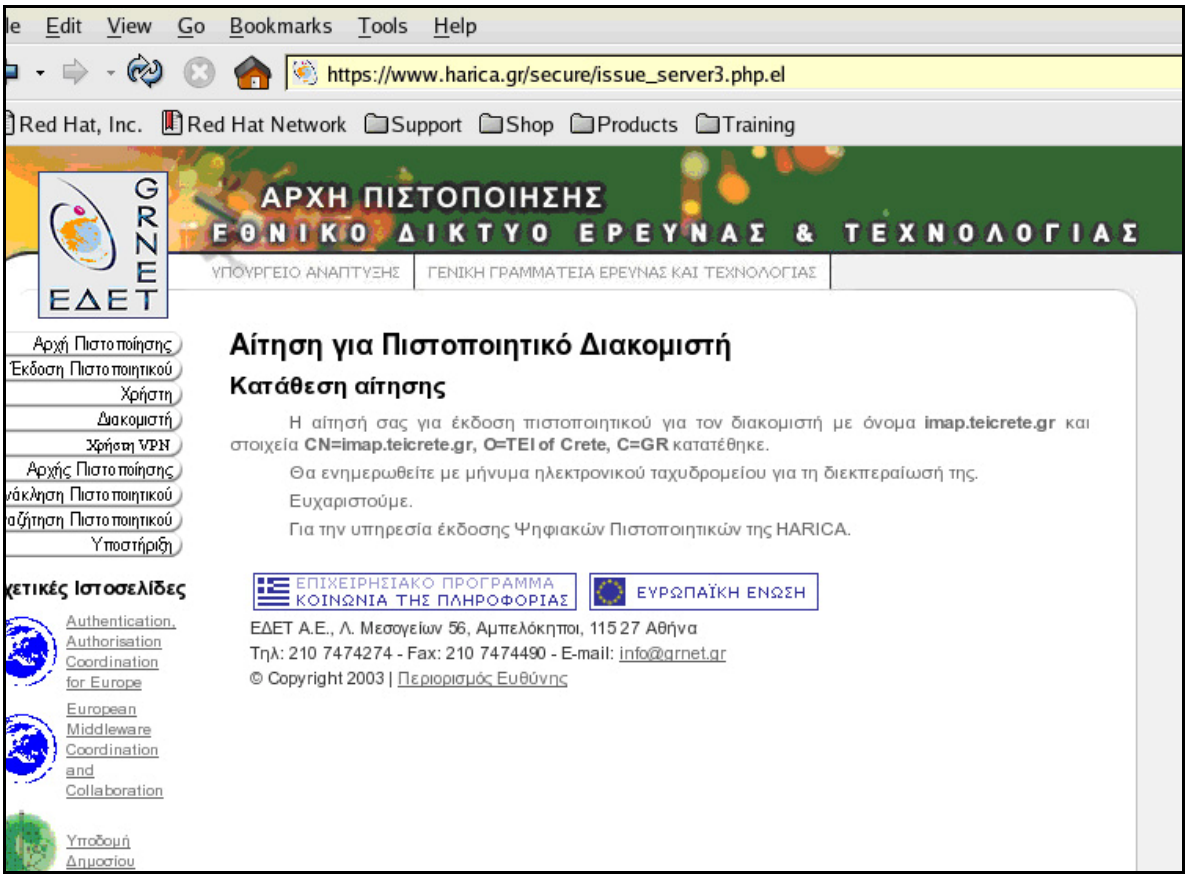
Σχήμα 7. Αίτημα του διακομιστή σε μορφή PKCS10.

Αντιγράφουμε τα περιεχόμενα του και τα επικολλούμε στο πεδίο "Αίτηση σε μορφή PKCS10" της σελίδας αίτησης για έκδοση πιστοποιητικού. Τέλος, υποβάλλουμε την αίτηση.



Σχήμα 8. Υποβολή αίτησης πιστοποιητικού.

Η αίτηση θα επεξεργαστεί και θα ενημερωθούμε με μήνυμα ηλεκτρονικού ταχυδρομείου για την έκδοση του πιστοποιητικού. Στο μήνυμα θα μας δοθεί σύνδεσμος για την αποδοχή και παραλαβή του πιστοποιητικού.

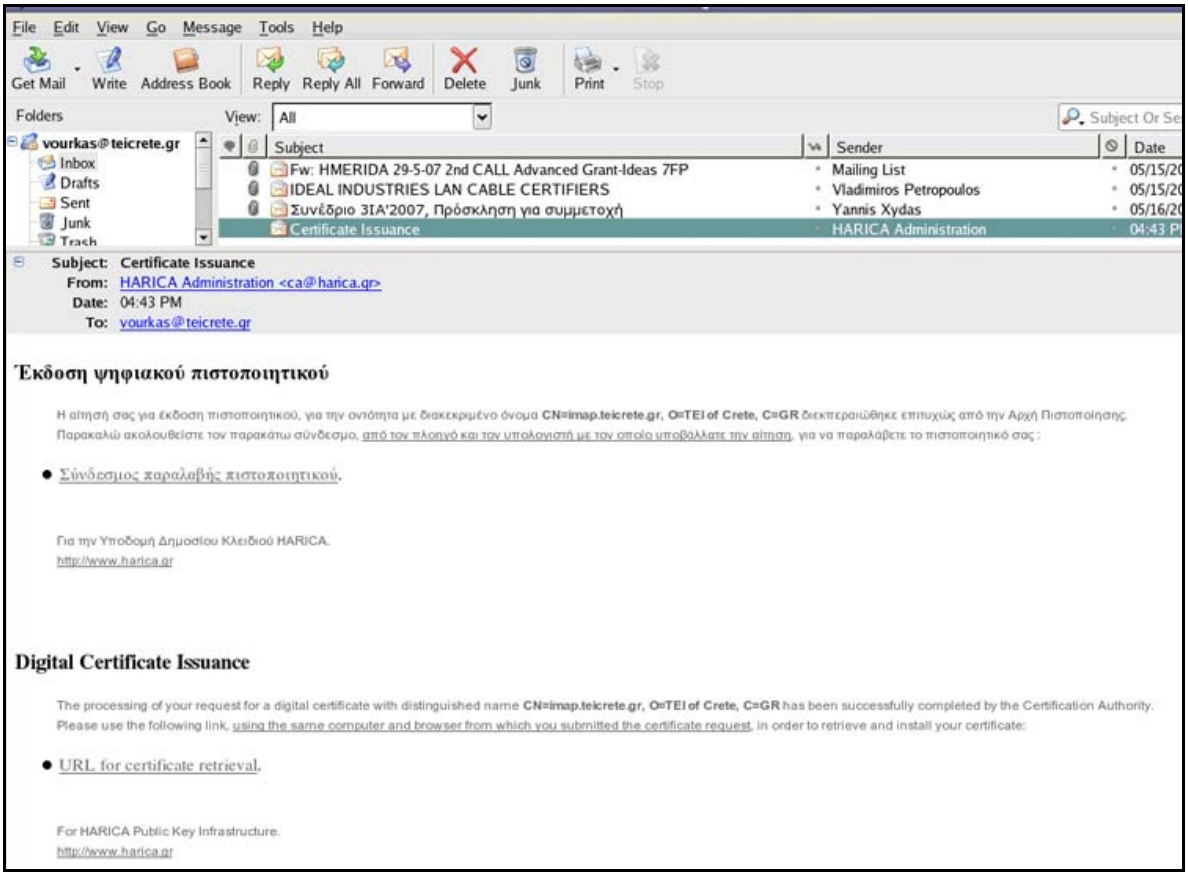


Σχήμα 9. Κατάθεση αίτησης για πιστοποιητικό.

Παράρτημα Λ

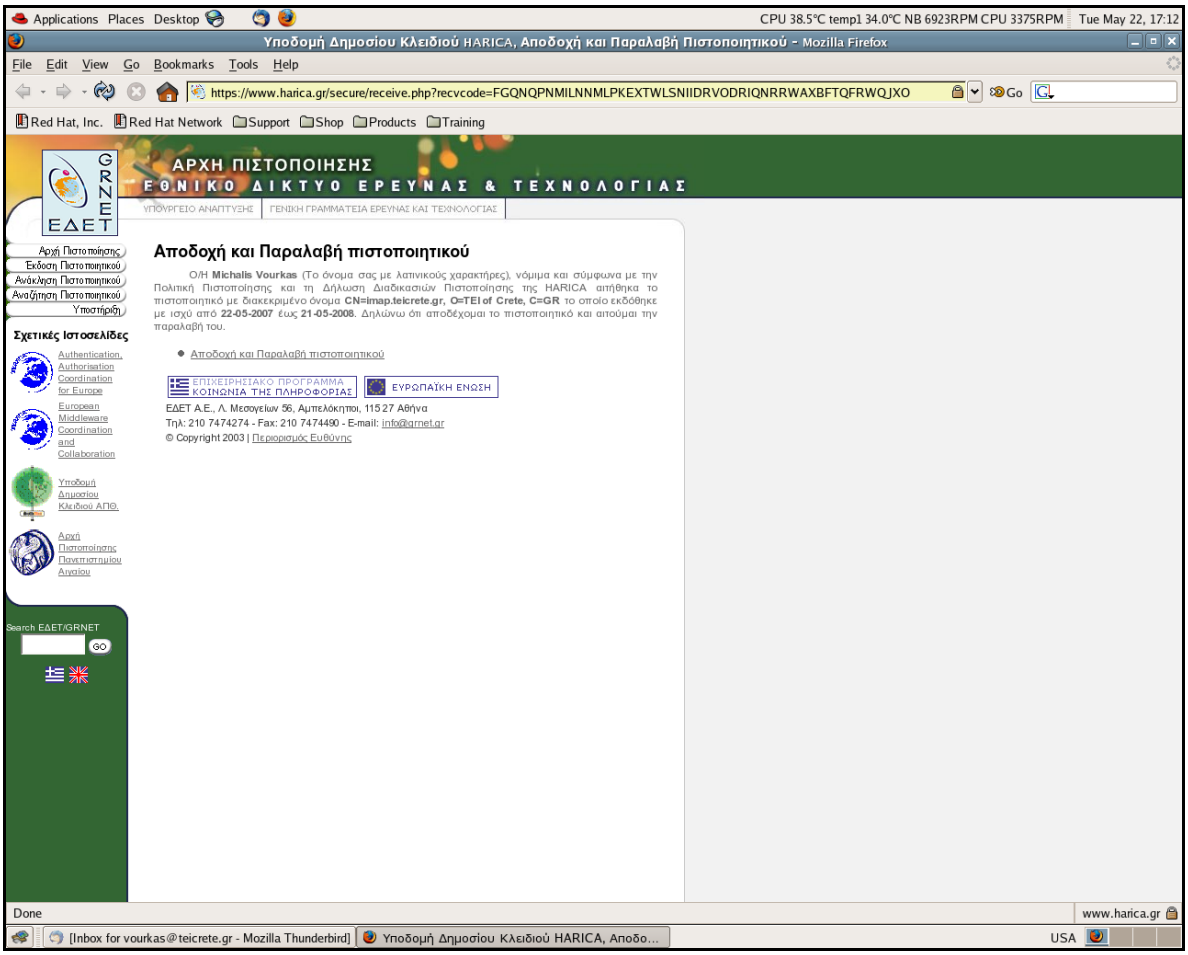
Οδηγίες για παραλαβή και αποθήκευση του πιστοποιητικού διακομιστή

Αφού εγκριθεί η αίτηση και εκδοθεί το πιστοποιητικό διακομιστή, ειδοποιείται ο διαχειριστής για την παραλαβή του πιστοποιητικού, μέσω email και παραλαμβάνει το πιστοποιητικό πατώντας στο σχετικό συνδεσμο.



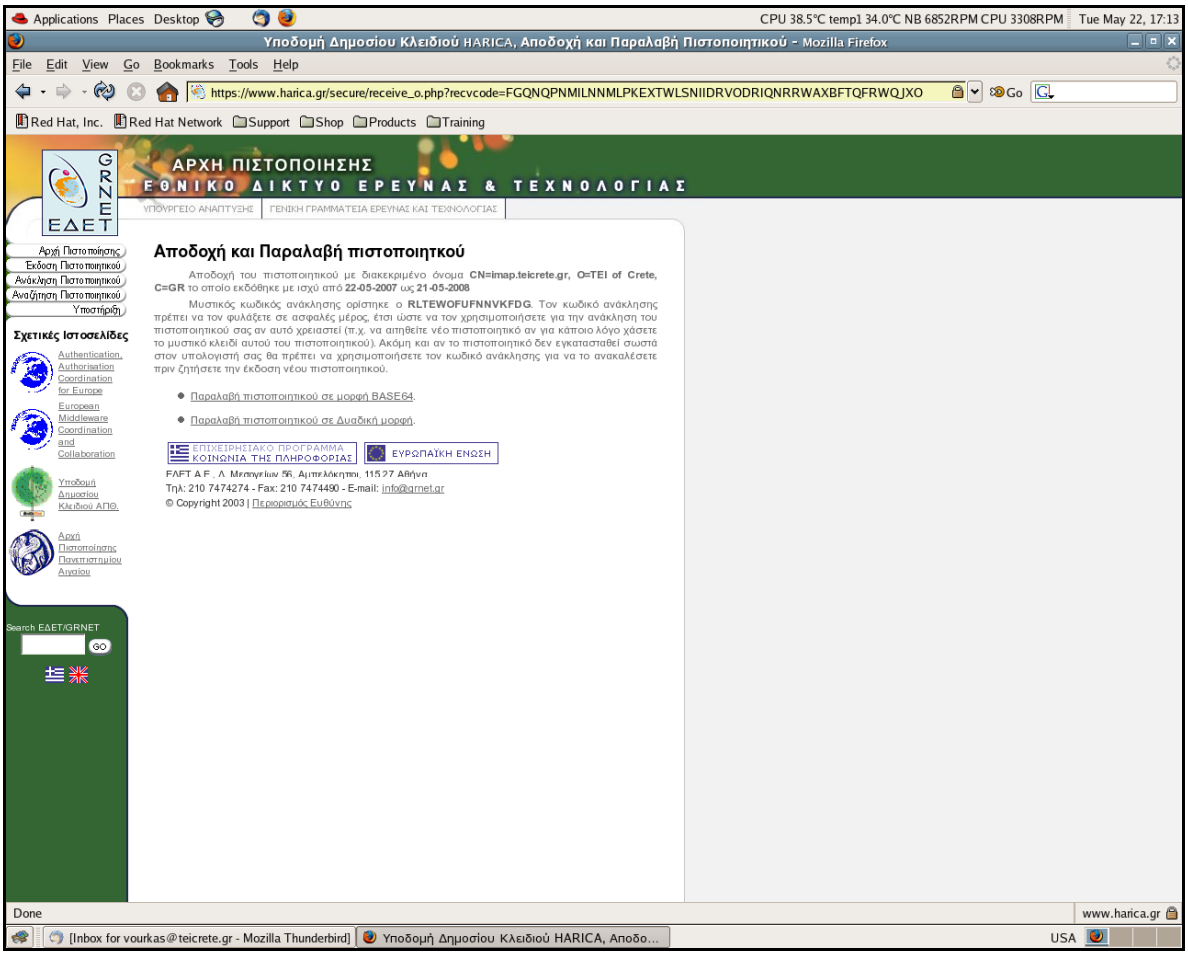
Σχήμα 1. Email παραλαβής πιστοποιητικού.

Στη συνέχεια μεταφέρεται στη σελίδα παραλαβής του πιστοποιητικού, όπου ο διαχειριστής επιβεβαιώνει ότι αιτήθηκε πιστοποιητικό διακομιστή και πατώντας το σύνδεσμο αποδέχεται το πιστοποιητικό.



Σχήμα 2. Αποδοχή και παραλαβή πιστοποιητικού.

Τέλος, μεταφερόμαστε στη σελίδα όπου μπορούμε να αποθηκεύσουμε το πιστοποιητικό σε μορφή BASE64.



Σχήμα 3. Αποθήκευση πιστοποιητικού.

Στη συνέχεια, ανοίγουμε το πιστοποιητικό με ένα Notepad το αντιγράφουμε και το βάζουμε σε ένα αρχείο μαζί με το ιδιωτικό κλειδί του πιστοποιητικού. Το αρχείο αυτό προστατεύεται από ένα κωδικό ασφαλείας(passphrase). Σε δημόσιους διακομιστές αν και είναι κακή πρακτική ασφαλείας, πρέπει να αφαιρούμε τον κωδικό ασφαλείας.

Για να βάλουμε το πιστοποιητικό και το ιδιωτικό κλειδί σε ένα αρχείο πληκτρολογούμε την εντολή

```
Cat server.key cert.pem > server.pem
```

Για να αφαιρέσουμε το passphrase πληκτρολογούμε τις εντολές

```
Openssl rsa –in server.pem –out newcert.pem
Openssl x509 –in server.pem >> newcert.pem
```

Τέλος, αποθηκεύουμε το αρχείο newcert.pem με το όνομα imapd.pem.

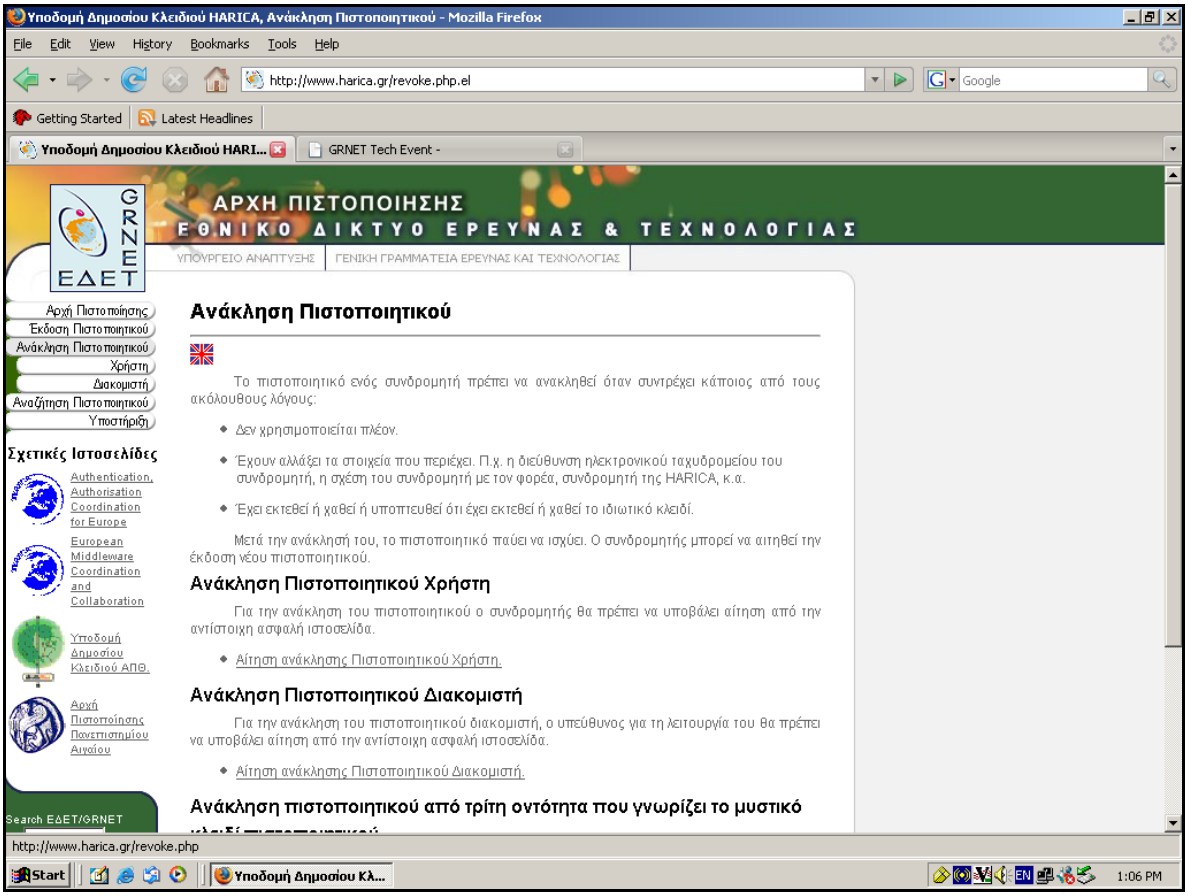
```
Cp newcert.pem imapd.pem
```

Το αρχείο imapd.pem βρίσκεται αποθηκευμένο στον κατάλογο etc/pki/tls/certs.

Παράρτημα Μ

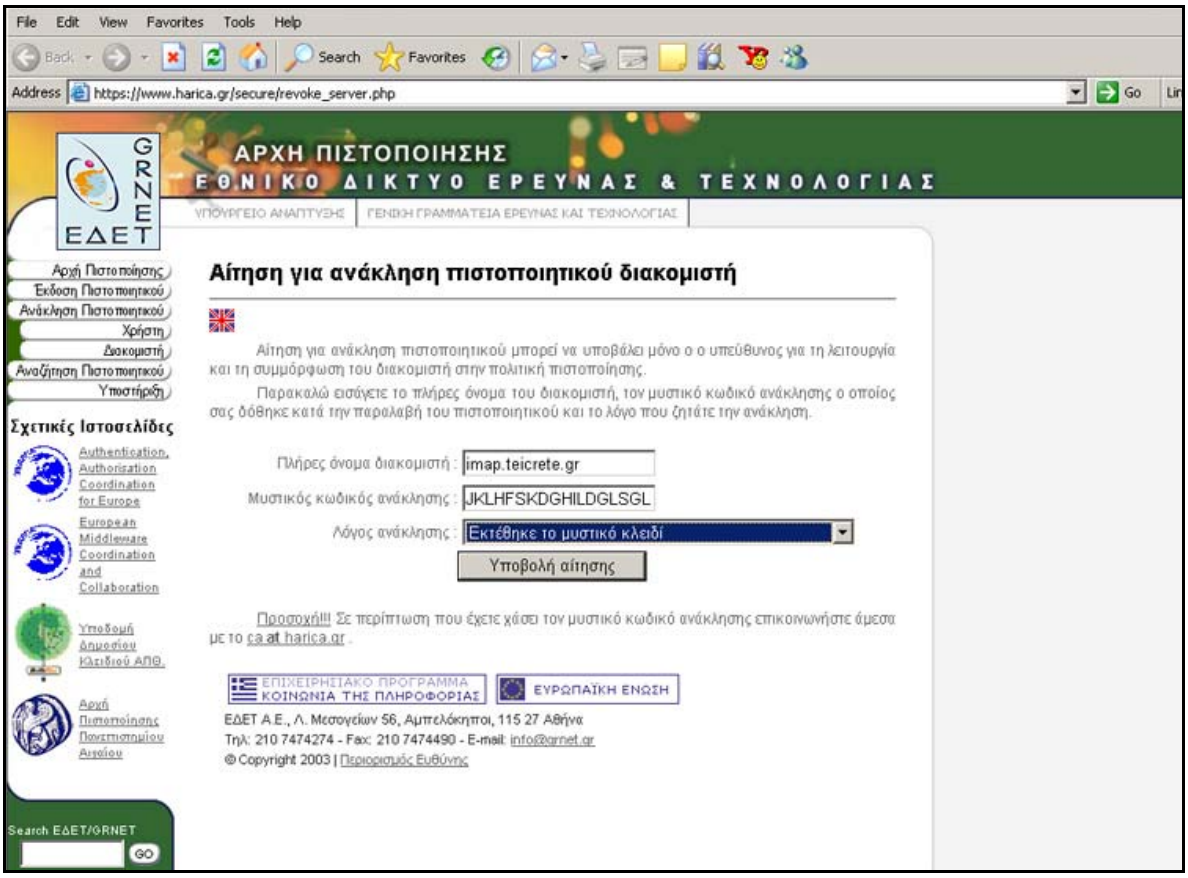
Οδηγίες για ανάκληση πιστοποιητικού διακομιστή.

Για την ανάκληση του πιστοποιητικού ο διαχειριστής θα πρέπει να υποβάλει αίτηση από την αντίστοιχη ασφαλή ιστοσελίδα δίνοντας το μυστικό κωδικό ανάκλησης, το όνομα του διακομιστή και το λόγο ανάκλησης, στην αντίστοιχη ιστοσελίδα της HARICA



Σχήμα 1. Επιλογή ανάκλησης πιστοποιητικού διακομιστή.

Στη συνέχεια εισάγουμε τα στοιχεία του διακομιστή.



Σχήμα 2. Εισαγωγή στοιχείων διακομιστή στη φόρμα ανάκλησης.

Η υπηρεσία μας ενημερώνει οτι η αίτηση ανάκλησης κατατέθηκε και θα ειδοποιηθεί ο διαχειριστής για την οριστικοποίησή της με email.

Παράρτημα Ν

Δήλωση Διαδικασιών Πιστοποίησης της HARICA

Παράρτημα Ξ

Πολιτική Πιστοποίησης της HARICA

ΒΙΒΛΙΟΓΡΑΦΙΑ & ΑΝΑΦΟΡΕΣ

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ασφάλεια Δικτύων, Chris Breton- Cameron Hunt
- Ασφάλεια Δικτύων Υπολογιστών, Στέφανου Γκριτζάλη-Σωκράτη Κ. Κάτσικο-Δημήτρη Γκριτζάλη.
- Understanding PKI 2nd Edition, Carlisli Adams-Steve Lloyd.
- Network Security, Fred Simods
- Computer Security, Matt Bishop.
- Fundamentals of Network Security, John E. Canavan.

ΑΝΑΦΟΡΕΣ

- http://www.grnet.gr
- http://vnoc.grnet.gr
- http://noc.auth.gr/services/rootca
- http://rootca.aegean.gr
- http://harica.gr
- http://www.grnet.gr/g-tech
- http://milliwaysconsulting.net/support/systems/courier-ssl.html
- http://gagravarr.org/writing/openssl-certs/personal.shtml
- http://www.thawte.com/ssl-digital-certificates/technical-support/keygen/apache_keygen.html
- http://www.ja.net/services/publications/factsheets/069-using-server-certificates.pdf
- http://slacksite.com/apache/certificate.html
- http://www.sitepoint.com/article/securing-apache-2-server-ssl