ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ

ΕΥΡΩΣΥΣΤΗΜΑ

ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΓΙΑ ΑΣΦΑΛΗ ΚΑΙ ΠΙΣΤΟΠΟΙΗΜΕΝΗ ΕΠΙΚΟΙΝΩΝΙΑ ΜΕ ΤΗΝ ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ

Οδηγίες προς τις Συνεργαζόμενες Τράπεζες

1. Εισαγωγή – Γνωριμία με τα Ψηφιακά Πιστοποιητικά

Η χρήση ηλεκτρονικών μέσων για το χειρισμό πληροφοριών μεγάλης κρισιμότητας θέτει υψηλές ανάγκες ασφαλείας. Οι πληροφορίες ανάλογα με τη διαβάθμιση τους πρέπει να προστατεύονται από τη μη εξουσιοδοτημένη πρόσβαση κατά τη μετάδοση τους.

Κατά την επικοινωνία με την Τράπεζα της Ελλάδος με ηλεκτρονικό ταχυδρομείο χρησιμοποιείται η τεχνολογία των *Ψηφιακών Πιστοποιητικών* (Digital Certificates). Τα ψηφιακά πιστοποιητικά δίνουν τις δυνατότητες:

- Ηλεκτρονικής *Κρυπτογράφησης* μηνυμάτων ηλεκτρονικού ταχυδρομείου ώστε να προστατεύονται από υποκλοπή

- *Ψηφιακής Υπογραφής* μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η ψηφιακή υπογραφή επιτρέπει **(α)** την επιβεβαίωση του αποστολέα επειδή συνδέει ένα χρήστη με τα ηλεκτρονικά μηνύματα που στέλνει κατά τρόπο που να μην επιδέχεται αμφισβήτηση, **(β)** την εξασφάλιση της πλήρους ακεραιότητας του μηνύματος και **(γ)** την εξασφάλιση ότι ο αποστολέας δε θα μπορεί να αρνηθεί την αποστολή του μηνύματος (non-repudiation).

Τι είναι τα Ψηφιακά Πιστοποιητικά;

Τα ψηφιακά πιστοποιητικά είναι μικρά αρχεία κωδικοποιημένης πληροφορίας τα οποία συνδέονται με μοναδικό τρόπο με έναν συγκεκριμένο χρήστη (πιο συγκεκριμένα με μια μοναδική διεύθυνση email). Αποτελούν ουσιαστικά τα κλειδιά κρυπτογράφησης του χρήστη. Περιέχουν πληροφορίες σχετικά με την ταυτότητα του ιδιοκτήτη τους, τον οργανισμό στον οποίο υπάγεται και τον σκοπό χρήσης τους.

Πως χρησιμοποιείται ένα ψηφιακό πιστοποιητικό (Τεχνική Εξήγηση);

Κάθε χρήστης στον οποίο εκδίδεται ένα Ψηφιακό Πιστοποιητικό αποκτά ένα ζευγάρι κλειδιών.

1. Ένα *Ιδιωτικό Κλειδί* το οποίο οφείλει να κρατά μόνον ο ίδιος και να το προστατεύει κατάλληλα. Συνήθως το Ιδιωτικό Κλειδί είναι ασφαλώς αποθηκευμένο στο σταθμό εργασίας και σε οποιεσδήποτε άλλες συσκευές χρησιμοποιεί ο χρήστης. Ανάλογα με την περίπτωση όμως μπορεί να του έχει παραδοθεί και σε εξωτερικό αποθηκευτικό μέσο (π.χ. CD, USB stick, smart card κ.λπ.)

2. Ένα *Δημόσιο Κλειδί* το οποίο διανέμεται ελεύθερα σε όλους όσους επιθυμούν να επικοινωνήσουν με το χρήστη.

Κρυπτογράφηση: Ο αποστολέας επιλέγοντας την κρυπτογράφηση χρησιμοποιεί το Δημόσιο Κλειδί του παραλήπτη. Αυτό θα πρέπει να το έχει αποκτήσει με μια αρχική διαδικασία (που περιγράφεται πιο κάτω) και να το έχει διαθέσιμο στην Address List του μαζί με τα υπόλοιπα στοιχεία του παραλήπτη. Με αυτό το Δημόσιο Κλειδί κρυπτογραφεί το μήνυμα. Στη συνέχεια το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνον από το αντίστοιχο Ιδιωτικό Κλειδί, δηλαδή μόνον από τον παραλήπτη που το έχει στη διάθεση του και από κανέναν τρίτο.

Ψηφιακή υπογραφή: Ο αποστολέας επιλέγοντας να υπογράψει ψηφιακά ένα εξερχόμενο μήνυμα χρησιμοποιεί το δικό του Ιδιωτικό Κλειδί. Κάθε ένας που θα λάβει αυτό το μήνυμα, θα μπορεί να το επιβεβαιώσει μέσω (του ελεύθερα διαθέσιμου) Δημόσιου Κλειδιού του αποστολέα. Ο μόνος που θα μπορούσε να το έχει υπογράψει είναι ο κάτοχος του (προστατευμένου) Ιδιωτικού Κλειδιού, άρα επιβεβαιώνεται η ταυτότητα του αποστολέα.

Πως μπορεί να αποκτηθεί ένα ψηφιακό πιστοποιητικό;

Στις επικοινωνίες με την Τράπεζα της Ελλάδος χρησιμοποιούνται αποκλειστικά Ψηφιακά Πιστοποιητικά τα οποία πρέπει να έχουν εκδοθεί από αναγνωρισμένους παρόχους υπηρεσιών πιστοποίησης (Certificate Authorities – CAs – Αρχές Πιστοποίησης). Υπάρχουν οι εξής περιπτώσεις για το ποιές θεωρούνται Αναγνωρισμένες Αρχές Πιστοποίησης:

(α) Η Εθνική επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) τηρεί στο δικτυακό της τόπο (http://www.eett.gr) λίστα με όλες τις επίσημα αναγνωρισμένες εντός Ελλάδος Αρχές Πιστοποίησης. Στη λίστα αυτή περιλαμβάνονται τόσο εμπορικοί πάροχοι όσο και η σχετική υπηρεσία του Ελληνικού Δημοσίου, ΕΡΜΗΣ.

(β) Γίνονται επίσης δεκτά από την Τράπεζα της Ελλάδος Ψηφιακά Πιστοποιητικά τα οποία έχουν εκδοθεί από εμπορικούς παρόχους του εξωτερικού, εφόσον αυτοί είναι «αναγνωρισμένοι» για τα λειτουργικά συστήματα Microsoft, δηλαδή τα κλειδιά τους είναι ήδη ενσωματωμένα στο Certificate Store του λειτουργικού.

(γ) Τέλος βάσει πρόσφατων κανονισμών της Ε.Ε. είναι δυνατόν να γίνουν αποδεκτά και Ψηφιακά Πιστοποιητικά τα οποία έχουν εκδοθεί από Αρχές Πιστοποίησης που είναι αναγνωρισμένες σε οποιαδήποτε άλλη χώρα της Ε.Ε.

Τι είδη Ψηφιακών Πιστοποιητικών υπάρχουν;

Για τους σκοπούς ανταλλαγής μηνυμάτων ηλεκτρονικού ταχυδρομείου υπάρχουν δύο περιπτώσεις ψηφιακών πιστοποιητικών που μπορούν να χρησιμοποιηθούν (ακολουθείται η γενικώς αποδεκτή ορολογία):

(α) Χαλαρής Αποθήκευσης (γνωστά και ως Class 1). Σε αυτά η επιβεβαίωση του κατόχου τους είναι πιο απλή και αρκεί να εξασφαλίζεται ότι είναι ο πραγματικός χρήστης της διεύθυνσης email που έχει δηλωθεί. Τα πιστοποιητικά αυτά συνήθως φυλάσσονται σαν απλά αρχεία στον υπολογιστή του χρήστη.

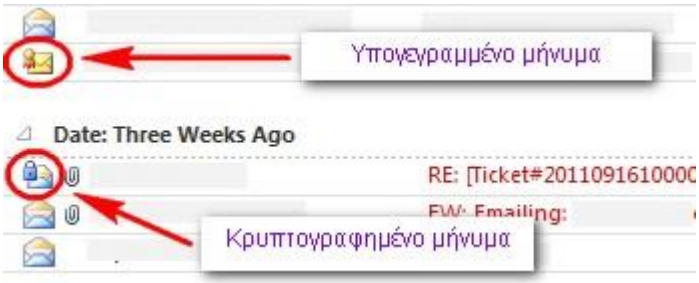
(β) Ισχυρής Αποθήκευσης (γνωστά και ως Σκληρής αποθήκευσης ή Class 2). Σε αυτά η επιβεβαίωση του κατόχου γίνεται με πλήρη ταυτοποίηση (έλεγχο ταυτότητας κατά την έκδοση κ.λπ.). Τα πιστοποιητικά αυτά συνήθως φυλάσσονται σε εξωτερική συσκευή ασφαλείας (token) που μπορεί να είναι USB key ή Smart Card.

Για τις ανάγκες επικοινωνίας με τις υπηρεσίες της Τράπεζας της Ελλάδος είναι αρκετά τα πιστοποιητικά Χαλαρής Αποθήκευσης.

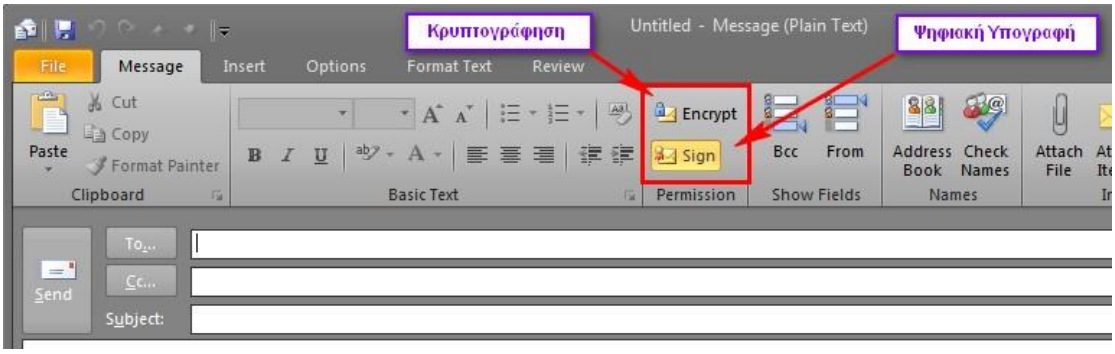
2. Χρήση Ψηφιακής Υπογραφής και Κρυπτογράφησης

Γενική Εικόνα

Στα εισερχόμενα μηνύματα του προγράμματος ηλεκτρονικού ταχυδρομείου τα μηνύματα με ψηφιακή υπογραφή ή κρυπτογράφηση έχουν συγκεκριμένη σήμανση (παράδειγμα από το Microsoft Outlook):

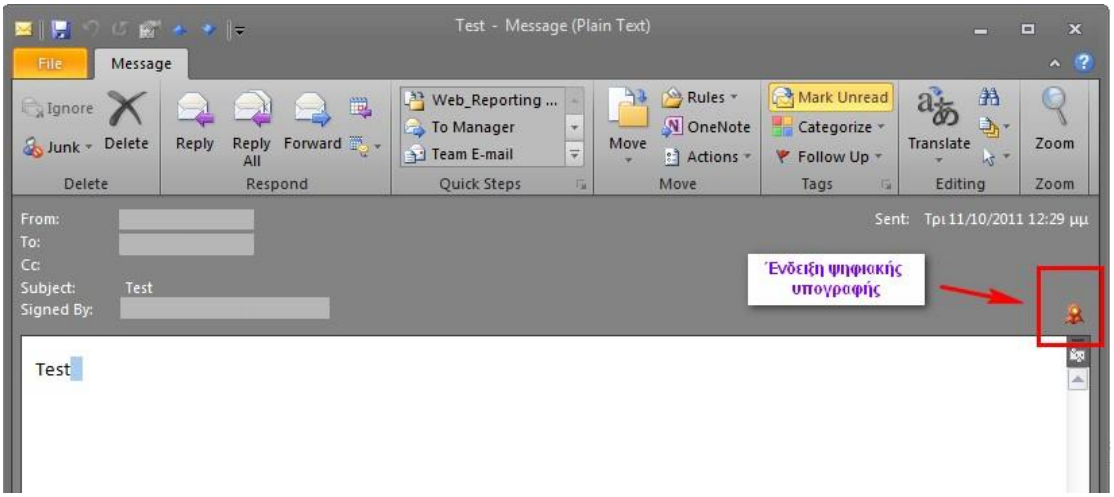


Στα εργαλεία του προγράμματος ηλεκτρονικού ταχυδρομείου, στη δημιουργία νέου μηνύματος, υπάρχουν διαθέσιμα τα σχετικά "κουμπιά" για κρυπτογράφηση του μηνύματος ή την προσθήκη ψηφιακής υπογραφής.



Ψηφιακή Υπογραφή και Έλεγχος Αποστολέα (παράδειγμα Microsoft Outlook)

Για να διαπιστωθεί η προέλευση ενός μηνύματος που λαμβάνουμε, το επιλέγουμε και αφού το ανοίξουμε, πηγαίνουμε στη δεξιά μεριά του μηνύματος. Με διπλό κλικ ανοίγουμε (εφόσον υπάρχει) το εικονίδιο της ψηφιακής υπογραφής.



Στο παράθυρο που εμφανίζεται θα πρέπει η υπογραφή να είναι «έγκυρη» (valid) και «αξιόπιστη» (trusted).

Εάν η υπογραφή είναι έγκυρη και αξιόπιστη, θα αναφέρεται όπως στην πιο πάνω οθόνη:

"The digital signature on this message is Valid and Trusted".

Ανταλλαγή δημοσίων κλειδιών

Για να είναι δυνατή η ανταλλαγή κρυπτογραφημένων και ψηφιακά υπογεγραμμένων μηνυμάτων πρέπει τα επικοινωνούντα μέρη να έχουν προηγουμένως ανταλλάξει τα Δημόσια Κλειδιά τους.

Η διαδικασία ανταλλαγής κλειδιών έχει ως εξής:

Βήμα 1: Στέλνετε ένα ψηφιακά υπογεγραμμένο μήνυμα (με οποιοδήποτε περιεχόμενο) στο χρήστη με τον οποίο επιθυμείτε να επικοινωνήσετε.

Βήμα 2: Ο χρήστης στην άλλη πλευρά εισάγει το ψηφιακό πιστοποιητικό σας στις επαφές του (π.χ. Outlook Contacts) και σας αποστέλλει με τη σειρά του ένα ψηφιακά υπογεγραμμένο μήνυμα με οποιοδήποτε περιεχόμενο.

Βήμα 3: Εισάγετε το ψηφιακό πιστοποιητικό του χρήστη στις επαφές σας

Εισαγωγή ψηφιακού πιστοποιητικού στις επαφές (παράδειγμα Microsoft Outlook)

Ανοίγετε το υπογεγραμμένο μήνυμα και κάνοντας δεξί κλικ στα στοιχεία του αποστολέα επιλέγετε Add to Contacts. Στην καρτέλα της επαφής εισάγονται αυτόματα ο λογαριασμός του e-mail και το ψηφιακό πιστοποιητικό του αποστολέα (Δημόσιο Κλειδί αποστολέα). Επιλέγετε το εικονίδιο Save and Close στο Toolbar. Πλέον, για την αποστολή κρυπτογραφημένων μηνυμάτων πρέπει να χρησιμοποιείται η ηλεκτρονική διεύθυνση από τις επαφές.

Αποστολή κρυπτογραφημένων και ψηφιακά υπογεγραμμένων μηνυμάτων

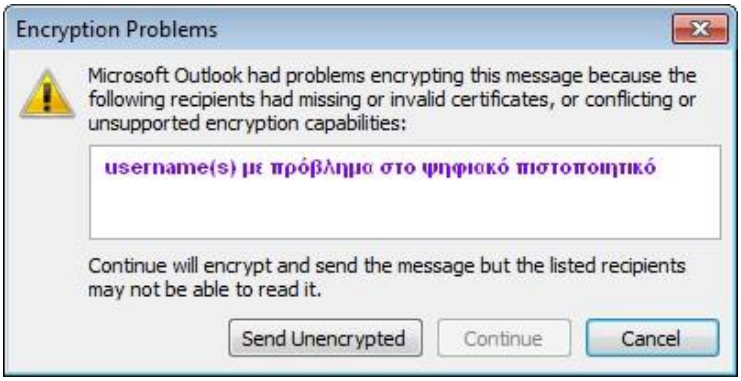
Ψηφιακή υπογραφή μηνύματος

Δημιουργείτε ένα νέο μήνυμα με το περιεχόμενο και (πιθανά και) τα συνημμένα αρχεία που επιθυμείτε και προτού το στείλετε επιλέγετε το εικονίδιο Sign στο Toolbar (εικονίδιο από το Microsoft Outlook).

Κρυπτογράφηση μηνύματος

Θα πρέπει να έχει προηγηθεί η ανταλλαγή των ψηφιακών πιστοποιητικών με τον τρόπο που περιγράφεται πάρα πάνω (εικονίδιο από το Microsoft Outlook).

Στην περίπτωση που για έναν ή περισσότερους από τους παραλήπτες του μηνύματος σας δε έχετε διαθέσιμο ψηφιακό πιστοποιητικό θα σας βγει σχετικό μήνυμα ότι δεν είναι δυνατή η κρυπτογράφηση.



Προσοχή: Αν επιλέξουμε "Send Unencrypted" το μήνυμα θα σταλεί χωρίς κρυπτογραφική προστασία.