ΕΘΝΙΚΟ ΑΣΤΕΡΟΣΚΟΠΕΙΟ ΑΘΗΝΩΝ
Κέντρο Δικτύου NOAnet

Χρήση Προσωπικών Ψηφιακών Πιστοποιητικών.
Έκδοση 1.1 (3/3/2011)

Α. Γενικές οδηγίες χρήσεως προσωπικών ψηφιακών πιστοποιητικών

Με απλά λόγια, κάθε χρήστης Χ που αποκτά προσωπικό ψηφιακό πιστοποιητικό έχει πλέον στην διάθεσή του ένα ιδιωτικό κλειδί, μια ψηφιακή υπογραφή και ένα δημόσιο κλειδί. Το δημόσιο κλειδί του Χ διανέμεται ελεύθερα (αλλά με φερέγγυο τρόπο) και πρέπει υποχρεωτικά να χρησιμοποιηθεί από όσους θέλουν να στείλουν κρυπτογραφημένο μήνυμα στον Χ.

Με το ιδιωτικό κλειδί, ο Χ μπορεί:

1. Να υπογράφει ψηφιακά τα μηνύματα που αποστέλλει ώστε οι παραλήπτες να είναι βέβαιοι ότι ο αποστολέας είναι αυτός που ισχυρίζεται ότι είναι. Επιπλέον, εξασφαλίζεται ότι το μήνυμα (έστω και αν δεν είναι κρυπτογραφημένο) **δεν έχει αλλαχθεί κατά την μεταφορά του** και παραμένει ακριβώς όπως εστάλη. Επίσης, όσοι λαμβάνουν τα ψηφιακά υπογεγραμμένα μηνύματά του, αποκτούν αυτόματα και το δημόσιο κλειδί του (περιλαμβάνεται στην ψηφιακή υπογραφή), ώστε να μπορούν να κρυπτογραφούν μηνύματα προς αυτόν.
2. Να ανοίγει (αποκρυπτογραφεί) τα μηνύματα που του στέλνουν άλλοι (οι οποίοι πρέπει να έχουν κρυπτογραφήσει το μήνυμα προς τον Χ με το δημόσιο κλειδί του Χ).

Άρα, για να λάβουμε ένα κρυπτογραφημένο μήνυμα από κάποιον, πρέπει ο αποστολέας να το έχει κρυπτογραφήσει με χρήση του δημόσιου κλειδιού μας. (Η διαδικασία γίνεται αυτόματα, δείτε παρακάτω.)

Αντιστοίχως, όταν ο Χ επιθυμεί να στείλει κρυπτογραφημένο μήνυμα προς ένα παραλήπτη Υ, τότε πρέπει να διαθέτει το δημόσιο κλειδί του Υ (το οποίο πιθανώς να έχει λάβει μέσω μιας ψηφιακής υπογραφής σε ηλ. υπογεγραμμένο μήνυμα σταλέν από τον Υ στον Χ).

ΕΙΝΑΙ ΠΡΟΦΑΝΕΣ ΟΤΙ ΤΟ ΠΡΟΣΩΠΙΚΟ ΜΑΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΠΡΕΠΕΙ ΝΑ ΤΗΡΕΙΤΑΙ ΜΕ ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΟΛΥΤΩΣ ΕΜΠΙΣΤΕΥΤΙΚΟ.

Β. Οδηγίες δημιουργίας/εγκατάστασης προσωπικού ψηφιακού πιστοποιητικού

1. Δημιουργία προσωπικού ψηφιακού πιστοποιητικού

Οι οδηγίες δημιουργίας πιστοποιητικού αναφέρονται στο Mozilla Firefox (καθώς είναι λογισμικό που προσφέρεται δωρεάν και είναι διαθέσιμο για σχεδόν όλα τα λειτουργικά συστήματα). Για άλλους web browsers ισχύουν αντίστοιχα.

Προκειμένου να είναι εφικτή η εφαρμογή των οδηγιών, πρέπει να έχει προηγηθεί αίτηση στο helpdesk@noa.gr ώστε να δοθεί εξουσιοδότηση για την δημιουργία πιστοποιητικού.

- Με το Firefox επισκεπτόμαστε στην διεύθυνση http://pki.noa.gr, και επιλέγουμε (στην ελληνική έκδοση του site): "Έκδοση νέου Προσωπικού Ψηφιακού Πιστοποιητικού".

- Επιλέγουμε Login και δίνουμε το username / password που διαθέτουμε (όμοια με αυτά που χρησιμοποιούμε στον vmail.noa.gr).
- Επιλέγουμε "Δημιουργία CSR μέσω browser", επιλέγουμε τις ηλ. διευθύνσεις που θέλουμε να πιστοποιηθούν (συνήθως είναι ήδη επιλεγμένες), τσεκάρουμε την επιλογή "Αποδέχομαι τους όρους που αναγράφονται στην Πολιτική και Διαδικασίες Πιστοποίησης" και, τέλος, πατάμε το κουμπί "Δημιουργία".
- Μετά από λίγο χρόνο αναμονής, ενημερωνόμαστε ότι το πιστοποιητικό έχει εγκατασταθεί στο Firefox.

2. Εξαγωγή / backup / μεταφορά του προσωπικού πιστοποιητικού (από τον Firefox)

- Επιλέγουμε (στον Firefox): Tools / Options / Advanced / Καρτέλα Encryption: "View Certificates".
- Στην καρτέλα "Your Certificates" επιλέγουμε το προσωπικό μας πιστοποιητικό και πατάμε "Backup". Δίνουμε ένα password για την προστασία του πιστοποιητικού και το αποθηκεύουμε.

3. Εισαγωγή προσωπικού πιστοποιητικού:

1. Στο Mozilla Thunderbird:

   - Tools / Options / Advanced / Καρτέλα Certificates και πατάμε View Certificates.
   - Κατόπιν, στην καρτέλα "Your Certificates" κάνουμε Import και επιλέγουμε το αποθηκευμένο στον δίσκο μας αρχείο το οποίο εξήχθη από το Firefox. Δίνουμε το password και το πιστοποιητικό εισάγεται.

2. Στο Office (Internet Explorer / Outlook)
   [Δείτε και http://www.globalsign.com/support/personal-certificate/per_outlook07.html]

   - Στο Internet Explorer:
     Tools / Internet Options / Content / Certificates / Import / Browse (View all files) και επιλέγουμε το αρχείο που εξήχθη από το Thunderbird.
   - Στο Microsoft Outlook (2007/2010):
     (ΠΡΟΣΟΧΗ! Θα πρέπει να έχει προηγουμένως εγκατασταθεί το πιστοποιητικό στον Internet Explorer!)

     - Options / Trust Center / Κουμπί Trust Center Settings / E-Mail Security / Κουμπί Settings
     - Το Outlook θα εντοπίσει πιθανότατα αυτόματα το Certificate και θα δείξει τις ρυθμίσεις. Μπορούμε να αφήσουμε όλες τις ρυθμίσεις χωρίς αλλαγή.
     - Πατάμε OK / OK για να κλείσουμε τα παράθυρα ρυθμίσεων.

4. Ψηφιακή Υπογραφή / Κρυπτογράφηση:

4.1. Για να υπογράψουμε ηλεκτρονικά μηνύματα με την ψηφιακή μας υπογραφή:

- **Στο Mozilla Thunderbird:**

  Κατά την σύνθεση του μηνύματος επιλέγουμε Options / Digitally Sign This Message.
  Εάν θέλουμε τα ηλ. μηνύματα που στέλνουμε να υπογράφονται ψηφιακά πάντοτε, τότε επιλέγουμε: Options / Account Settings, και στον λογαριασμό που μας ενδιαφέρει πατάμε Security και τσεκάρουμε την επιλογή: "Digitally Sign Messages (by default)" (αφού

επιβεβαιώσουμε ότι στο προηγούμενο πεδίο "Use this certificate to digitally sign messages you send" είναι επιλεγμένο το σωστό πιστοποιητικό.

- **Στο Microsoft Outlook (2007/2010):**

  Κατά την σύνθεση του μηνύματος πατάμε το κουμπί Options / Sign.

  Εάν θέλουμε τα ηλ. μηνύματα που στέλνουμε να υπογράφονται ψηφιακά πάντοτε, τότε επιλέγουμε: Options / Trust Center / Κουμπί Trust Center Settings / E-Mail Security και τσεκάρουμε την επιλογή: "Add digital signature to outgoing messages".

4.2. Για να κρυπτογραφήσουμε μηνύματα:

- **Στο Mozilla Thunderbird:**

  Κατά την σύνθεση του μηνύματος επιλέγουμε Options / Encrypt This Message.

  [Προφανώς, η αποστολή θα αποτύχει αν το Thunderbird δεν διαθέτει δημόσιο κλειδί για τον παραλήπτη του μηνύματος. Μπορούμε να δούμε τα δημόσια κλειδιά που υπάρχουν ήδη διαθέσιμα στο Thunderbird εδώ: Tools / Options / Advanced / Καρτέλα Certificates, πατάμε View Certificates / Καρτέλα People. Μπορούμε να εισαγάγουμε νέα δημόσια κλειδιά πατώντας (στην ίδια καρτέλα) "Import".]

  Εάν θέλουμε τα ηλ. μηνύματα που στέλνουμε να κρυπτογραφούνται πάντοτε, τότε επιλέγουμε: Options / Account Settings, και στον λογαριασμό που μας ενδιαφέρει πατάμε Security και στην ρύθμιση "Default encryption setting when sending messages", επιλέγουμε: "Required".

- **Στο Microsoft Outlook (2007/2010):**

  Κατά την σύνθεση του μηνύματος επιλέγουμε Options / Encrypt.

  Εάν θέλουμε τα ηλ. μηνύματα που στέλνουμε να κρυπτογραφούνται πάντοτε, τότε επιλέγουμε: Options / Trust Center / Κουμπί Trust Center Settings / E-Mail Security και τσεκάρουμε την επιλογή: "Encrypt contents and attachments for outgoing messages".