Συχνές Ερωτήσεις

Σε αυτή την περιοχή συγκεντρώνονται όλες οι συχνές ερωτήσεις και απαντήσεις σχετικά με τα **γενικά θέματα** χρήσης Ψηφιακών Πιστοποιητικών και Ηλεκτρονικής Υπογραφής στην Ηλεκτρονική Συνταγογράφηση.

Τι είναι Ζεύγος Κλειδιών (Key Pair);

Στην ορολογία των τεχνολογιών PKI, είναι ο μοναδικός συνδυασμός δημοσίου και ιδιωτικού κλειδιού που συνδέονται μαθηματικά και προσφέρουν μεταξύ τους μεταξύ άλλων ασυμμετρική κρυπτογράφηση.

Τι είναι Ιδιωτικό κλειδί (Private Key);

Ιδιωτικό κλειδί είναι δεδομένα, όπως κώδικες ή ιδιωτικά κλειδιά κρυπτογραφίας, που στο PKI χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής. Το Ιδιωτικό Κλειδί του ζεύγους παραμένει μυστικό και υπό τον αποκλειστικό έλεγχο του κατόχου τους.

Τι είναι Δημόσιο κλειδί (Public Key);

Το δημόσιο κλειδί είναι δεδομένα επαλήθευσης υπογραφής, όπως κώδικες, ή δημόσια κλειδιά κρυπτογραφίας, τα οποία στο PKI χρησιμοποιούνται για την επαλήθευση της ηλεκτρονικής υπογραφής. Για το Δημόσιο όσο και Ιδιωτικό κλειδί του ζεύγους υπάρχει συσχέτιση με κάποιο φυσικό ή νομικό πρόσωπο ή αντικείμενο (web server, software κ.λ.π.). Το δημόσιο κλειδί είναι «ελεύθερα» προσβάσιμο σε τρίτους για επαλήθευση π.χ. μιάς Ψηφιακής Υπογραφής.

Τι είναι ψηφιακό Πιστοποιητικό (Certificate);

Πιστοποιητικό είναι η ηλεκτρονική βεβαίωση που συνδέει δεδομένα επαλήθευσης υπογραφής (δημόσιο κλειδί) με ένα άτομο και επιβεβαιώνει την ταυτότητά του.

Τι είναι Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ);

Πάροχος υπηρεσιών πιστοποίησης είναι φυσικό ή νομικό πρόσωπο ή άλλος φορέας, που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές. Για να είναι Αναγνωρισμένα τα πιστοποιητικά του πρέπει να έχει πιστοποιηθεί με βάση τα διεθνή πρότυπα, και να έχει εγγραφή στην λίστα της ΕΕΤΤ.

Τι είναι αναγνωρισμένο Πιστοποιητικό στο περιβάλλον PKI (ΥΔΚ);

Αναγνωρισμένο πιστοποιητικό είναι πιστοποιητικό που πληροί τους όρους που έχουν τεθεί από την σχετική νομοθεσία και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης, ο οποίος πληροί τις από το νόμο οριζόμενες προυποθέσεις και έχει εγγραφεί σε λίστα παρόχων αναγνωρισμένων ψηφιακών πιστοποιητικών (όπως της ΕΕΤΤ) για αξιοποίηση τους σε προηγμένες ηλεκτρονικές υπογραφές.

Τι είναι Ηλεκτρονική υπογραφή (Electronic Signature);

Ηλεκτρονική υπογραφή είναι δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως απόδειξη της γνησιότητας της ηλεκτρονικής υπογραφής.

Τι είναι Προηγμένη (ή Αναγνωρισμένη) Ηλεκτρονική υπογραφή (Digital Quatified Signature);

Προηγμένη ηλεκτρονική υπογραφή ή «ψηφιακή υπογραφή» είναι ηλεκτρονική υπογραφή, που πληροί τους εξής όρους:

1. συνδέεται μονοσήμαντα με τον υπογράφοντα,
2. είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος,
3. δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και
4. συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

Για Προηγμένες ή Αναγνωρισμένες ψηφιακές υπογραφές αξιοποιούνται αναγνωρισμένα ψηφιακά πιστοποιητικά.

Τι είναι Διάταξη Δημιουργίας Υπογραφής;

Διάταξη δημιουργίας υπογραφής είναι εξειδικευμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των δεδομένων δημιουργίας της υπογραφής, δηλαδή Ιδιωτικό κλειδί.

Τι είναι ΑΔΔΥ (Ασφαλής Διάταξη Δημιουργίας Υπογραφής);

ΑΔΔΥ ή Ασφαλής Διάταξη Δημιουργίας Υπογραφής, είναι ένα USB token, διαφορετικό από τα γνωστά στικάκια μνήμης που αποθηκεύουμε αρχεία, φωτογραφίες κλπ. Το USB token (ή TOKEN) έχει ενσωματωμένο ένα «κρυπτογραφικό» τσιπ, που αποθηκεύει με ύψιστη ασφάλεια τα ιδιωτικά κλειδιά του κατόχου (αναγνωρισμένα ψηφιακά πιστοποιητικά). Για να χρησιμοποιηθεί πρέπει να εισαχθεί σε ένα USB αναγνώστη.

Μία ΑΔΔΥ μπορεί να έχει την εμφάνιση ενός USB token ώστε να συνδέεται εύκολα σε μία θύρα USB σε ένα προσωπικό υπολογιστή (PC, φορητό). Η ΑΔΔΥ μπορεί επίσης να είναι σε μορφή έξυπνης κάρτας (όπως π.χ. οι τραπεζικές πιστωτικές κάρτες με τσιπ), που απαιτεί ειδικό αναγνώστη συνδεδεμένο στο PC.

Πληροί όλες τις προυποποθέσεις (τεχνικές, νομικές), και η χρήση της είναι υποχρεωτική με βάση τα διεθνή πρότυπα και νομοθεσία για αναγνωρισμένες ψηφιακές υπογραφές που αναγνωρίζονται νομικά ως ισότιμες των ιδιόχειρων σε έγγραφα.

Πως Χρησιμοποιείται η ΑΔΔΥ στην Ηλεκτρονική Συνταγογράφηση;

Η χρήση της ΑΔΔΥ είναι απλή. Η ΑΔΔΥ εισάγεται σε μία USB θύρα που λειτουργεί ως αναγνώστης.

Για να «ξεκλειδώσει» και να χρησιμοποιηθούν τα αποθηκεμένα κλειδιά (ή πιστοποιητικά) στο τσιπ της ΑΔΔΥ πρέπει να δοθεί το PIN (Personal Indentification Number). Η λειτουργία δηλαδή είναι ανάλογη με την χρήση των τραπεζικών πιστωτικών καρτών με τσιπ.

Πότε ζητάτε το PIN στην Ηλεκτρονική Συνταγογράφηση;

Το PIN ζητάτε σε δύο περιπτώσεις :

- Όταν γίνεται αυθεντικοποίηση του χρήστη κατά την εισαγωγή του (sign on) στην εφαρμογή με χρήση του TOKEN. Αυτό αντικαθιστά τον τρόπο μέχρι σήμερα που απαιτεί τρία διακριτά πεδία : Όνομα Χρήστη (User name), Κωδικό (password) και το Κείμενο Εικόνας. Και τα τρία αντικαθίστανται με το PIN, αρκεί το TOKEN να είναι σε USB θύρα στο PC.
- Όταν ζητείται να υπογραφεί ψηφιακά μία συνταγή από Ιατρό ή να γίνει εκτέλεσή της από Φαρμακοποιό κα.

Γιατί ζητάτε το PIN τόσο στην είσοδο μίας εφαρμογής και μετά κατά την Ψηφιακή Υπογραφή;

Κάθε ΑΔΔΥ για την Ηλεκτρονική Συνταγογράφηση περιέχει δύο Ψηφιακά Πιστοποιητικά με βάση τα Διεθνή Πρότυπα. Το ένα πιστοποιητικό χρησιμοποιείται για την «αναγνώριση» ή αυθεντικοποίηση του χρήστη με το

TOKEN. Αυτό το πιστοποιητικό δεν μπορεί να χρησιμοποιηθεί για αναγνωρισμένες ψηφιακές υπογραφές, με βάση τα διεθνή πρότυπα.

Το δεύτερο πιστοποιητικό είναι για την αναγνωρισμένη ψηφιακή υπογραφή και πάλι με βάση τα διεθνή πρότυπα. Τα προγράμματα που χρησιμοποιούν αυτή την τεχνολογία ξέρουν ποιο από τα δύο πιστοποιητικά να χρησιμοποιήσουν ανάλογα με την εργασία που εκτελούν.

Η Τεχνολογία με τις ΑΔΔΥ και τα ψηφιακά πιστοποιητικά σε αυτές αναφέρεται ως ΥΔΚ (Υποδομή Δημόσιου Κλειδιού) ή PKI (Public Key Infrastructure).

Τι είναι ΥΔΚ ή PKI;

Η Υποδομή Δημόσιου Κλειδιού ή PKI (Public Key Infrastructure) είναι η πλέον ασφαλής τεχνολογία για την προστασία συναλλαγών μεταξύ διαφορετικών μερών αξιοποιώντας κάθε δημόσιο δίκτυο, ακόμα και το διαδίκτυο.

Η τεχνολογία είναι γνωστή για μερικές δεκαετίες (αναφέρεται και ως Ασύμμετρη Κρυπτογράφηση), και έχει καθιερωθεί τόσο στην Ευρωπαϊκή Ένωση, όσο και στην χώρα μας. Από το 2001 (στην Ελλάδα) υπάρχει σχετική νομοθεσία που καθιερώνει την τεχνολογία PKI ως αποδεκτή και νομικά ισότιμη όσο αφορά τις αναγνωρισμένες ψηφιακές υπογραφές με τις χειρόγραφες σε έντυπα.

Για τον λόγο αυτό και για την προφύλαξη των χρηστών έχουν δημιουργηθεί διεθνή πρότυπα, στα οποία αναφέρεται η νομολογία, ώστε μία «αναγνωρισμένη (ή προηγμένη)» ψηφιακή υπογραφή σε ένα ηλεκτρονικό μήνυμα, αρχείο κ.α. να είναι ισότιμη νομικά της ιδιόχειρης σε ένα τυπωμένο έγγραφο (έντυπο).

Η ΥΔΚ βασίζεται στα εξής μέρη:

- Τον Εκδότη των Ψηφιακών Πιστοποιητικών που βρίσκονται π.χ. στις ΑΔΔΥ. Αναφέρεται και ως Trust Center ή ΕΤΟ (Έμπιστη Τρίτη Οντότητα).
- Τον χρήστη (ή Συνδρομητή) που έχει στην κατοχή του ένα (ή περισσότερα) ψηφιακά πιστοποιητικά της ΕΤΟ π.χ. σε μία ΑΔΔΥ.
- Εφαρμογές που χρησιμοποιούν τα πιστοποιητικά για Αυθεντικοποίηση ή Ψηφιακή Υπογραφή.

Τι είναι Αρχή Πιστοποίησης (ΑΠ) ή CA (Certification Authority);

Είναι ο συνδυασμός Λογισμικού και Εξοπλισμού που περιλαμβάνει κρυπτομηχανές και δημιουργούν τα Πιστοποιητικά με βάση τα διεθνή πρότυπα στις τεχνολογίες PKI. Πιστοποιητικά έχουν δυνατότητα να παράγουν εσωτερικά και οι ΑΔΔΥ, δηλαδή το κρυπτογραφικό τσιπ που είναι ενσωματωμένο στο TOKEN.

Τα πιστοποιητικά στο PKI παράγονται σε ζεύγη, δηλαδή το Ιδιωτικό (Private) και το Δημόσιο (Public). Το ιδιωτικό προστατεύεται και αξιοποιείται σε λειτουργίες όπως η ψηφιακή υπογραφή. Το Δημόσιο κλειδί αντίθετα είναι γνωστό και χρησιμοποιείται από όποιον επιθυμεί (απαραίτητο) για εργασίες που έχει χρησιμοποιηθεί το ιδιωτικό του ιδίου χρήστη π.χ. για αναγνώριση της γνησιότητας της ψηφιακής υπογραφής.

Ενδεικτικά αν ένα ηλεκτρονικό μήνυμα ή έγγραφο έχει υπογραφεί με το ιδιωτικό κλειδί ενός χρήστη, απαιτείται και χρησιμοποιείται το αντίστοιχο δημόσιο κλειδί του χρήστη ώστε να διαπιστωθεί η γνησιότητα της υπογραφής.

Πόσο ασφαλής είναι η Τεχνολογία PKI;

Είναι η πλέον ασφαλής τεχνολογία με την προϋπόθεση ότι τηρούνται τα διεθνή πρότυπα και κανόνες ασφαλείας.

Η ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων) έχει ορισθεί από την πολιτεία να ελέγχει εάν οι πάροχοι αναγνωρισμένων ψηφιακών πιστοποιητικών συμμορφώνονται με την Ευρωπαική και Ελληνική νομοθεσία και ακολουθούν τα διεθνή πρότυπα και τις οδηγίες και αποφάσεις που εκδίδει η ΕΕΤΤ .

Επιπλέον η ΕΕΤΤ διατηρεί λίστα Παρόχων που εκδίδουν Πιστοποιητικά και την κατηγορία τους, ανάλογα με την πιστοποίησή τους. Το πλέον γνωστό και αυστηρό διεθνές πρότυπο για να πιστοποιηθεί ένας Πάροχος που εκδίδει «αναγνωρισμένα» ψηφιακά πιστοποιητικά για «αναγνωρισμένες» ψηφιακές υπογραφές είναι το «Web Trust».

Το BYTE Trust Center που εκδίδει τα αναγνωρισμένα ψηφιακά πιστοποιητικά για λογαριασμό της ΗΔΙΚΑ για χρήση στην Ηλεκτρονική Συνταγογράφηση, είναι πιστοποιημένο κατά Web Trust και είναι στη λίστα της ΕΕΤΤ στην υψηλότερη δυνατή κατηγορία, δηλαδή να εκδίδει «αναγνωρισμένα» ψηφιακά πιστοποιητικά, που όταν χρησιμοποιούνται αναγνωρίζονται νομικά ως ισότιμα της ιδιόχειρης υπογραφής.

Τι είναι Υπογράφων ή Συνδρομητής στο περιβάλλον ΥΔΚ της Ηλεκτρονικής Συνταγογράφησης;

Υπογράφων ή Συνδρομητής (ή «πιστοποιούμενος") είναι το φυσικό πρόσωπο, που κατέχει διάταξη δημιουργίας υπογραφής (ΑΔΔΥ)και ενεργεί στο δικό του όνομα. Είναι η οντότητα που υπέβαλε αίτηση για έκδοση πιστοποιητικών και μετά από την απαιτούμενη διαδικασία επαλήθευσης της ταυτότητάς του, απέκτησε τα πιστοποιητικό από τον Πάροχο Υπηρεσιών Πιστοποίησης, που για την Ηλεκτρονική Συνταγογράφηση αποθηκεύονται σε ΑΔΔΥ τύπου USB token.

Πως λειτουργεί η ΥΔΚ (PKI- Public Key Infrastructure) στην Ηλεκτρονική Συνταγογράφηση;

Η Υπηρεσία Δημοσίου Κλειδιού (ΥΔΚ), είναι ευρέως αναγνωρισμένη ως η ασφαλέστερη και σήμερα η πλέον λειτουργική τεχνολογία για ηλεκτρονικές ανταλλαγές. Τα ψηφιακά πιστοποιητικά εστιάζουν σε θέματα ασφάλειας εμπιστευτικότητας , ακεραιότητας, επικύρωσης, προκειμένου οι τελικοί χρήστες να μπορούν να επικοινωνούν και να ανταλλάσσουν πληροφορίες σε ένα ασφαλές και αξιόπιστο περιβάλλον.

Η ΥΔΚ για την Ηλεκτρονική Συνταγογράφηση, υλοποιείται και λειτουργεί σε βήματα (ή συνιστώσες), ακολουθώντας τα παρακάτω βήματα:

- Βήμα 1ο: Ο χρήστης αποκτά από την υποδομή ΥΔΚ ένα ζεύγος κλειδιών, κατόπιν σχετικού αιτήματος του σε Αρχή Πιστοποίησης ενός Παρόχου Ψηφιακών Πιστοποιητικών.
- Βήμα 2ο: Η Αρχή Εγγραφής (Registration Authority-RA) συλλέγει τις απαιτούμενες πληροφορίες για να γίνει η εξακρίβωση της ταυτότητας του τελικού χρήστη και εγκρίνει την αίτηση – έκδοσης των προσωπικών ψηφιακών πιστοποιητικών.
- Βήμα 3ο: Η Αρχή Εγγραφής αποδέχεται ή απορρίπτει την αίτηση εφόσον δεν πληρούνται όλες οι απαιτούμενες προϋποθέσεις, π.χ. δεν διαθέτει (ή δεν καταθέτει όπως απαιτεί ο νόμος) αντίγραφο ισχυρού εγγράφου ταυτοποίησής του (π.χ. Αστυνομική Ταυτότητα, Διαβατήριο).
- Βήμα 4ο: Η Αρχή Πιστοποίησης (Certification Authority) ενός Παρόχου Αναγνωρισμένων Ψηφιακών Πιστοποιητικών παράγει τα ψηφιακά πιστοποιητικά του τελικού χρήστη και τον ενημερώνει πότε και πως μπορεί να τα αξιοποιήσει (π.χ. PIN).

Πως μπορώ να αποκτήσω ΑΔΔΥ με αναγνωρισμένα ψηφιακά πιστοποιητικά για την Ηλεκτρονική Συνταγογράφηση;

1. Η αίτηση για την ΑΔΔΥ και τα Ψηφιακά Πιστοποιητικά υποβάλλεται συμπληρώνοντας σχετική ηλεκτρονική φόρμα στην εφαρμογή της ΗΔΙΚΑ για την Ηλεκτρονική Συνταγογράφηση .
   Προσοχή.
   Η διεύθυνση στην αίτηση πρέπει να είναι αυτή που θα βρίσκεται ο χρήστης –αιτών για να παραλάβει αυτοπροσώπως την ΑΔΔΥ (υπογράφει την παραλαβή). Είναι υποχρεωτικό να δοθεί κινητό στο οποίο θα ειδοποιηθεί για την έκδοση των πιστοποιητικών και θα λάβει το PIN για να χρησιμοποιεί την ΑΔΔΥ. Χωρίς κινητό τηλέφωνο δεν θα εκδοθούν ψηφιακά πιστοποιητικά στην παρούσα φάση.
2. Η Αίτηση εξετάζεται και εγκρίνεται/απορρίπτεται από την ΗΔΙΚΑ που ενεργεί ως Αρχή Εγγραφής, αξιοποιώντας και υπηρεσίες του παρόχου. Ενδεικτικά αιτήσεις χωρίς Διεύθυνση παραλαβής της ΑΔΔΥ ή χωρίς κινητό δεν εγκρίνονται. Αιτήσεις ατόμων που δεν είναι χρήστες της Ηλεκτρονικής Συνταγογράφησης ώστε να υποβάλουν ηλεκτρονικά Αίτηση απόκτησης ΑΔΔΥ δεν γίνονται δεκτές. Οι νέοι χρήστες ακολουθούν την υπάρχουσα διαδικασία της ΗΔΙΚΑ να γίνουν πρώτα χρήστες της Ηλεκτρονικής Συνταγογράφησης με απόκτηση username, password. Στην συνέχεια μπορούν να υποβάλλουν ηλεκτρονικά αίτηση απόκτησης ΑΔΔΥ.
3. Μετά την έγκριση της Αίτησης από την Αρχή Εγγραφής αυτή μεταβιβάζεται στην Αρχή Πιστοποίησης, δηλαδή στο Trust Center της BYTE.

4. Τα πιστοποιητικά εκδίδονται με ασφαλή τρόπο στην ΑΔΔΥ που αποστέλλεται με συστημένη επιστολή (ΕΛΤΑ Courier) στον αιτούντα.
5. Ξεχωριστά ο αιτών λαμβάνει ειδοποίηση (SMS) ότι θα πρέπει να αναμένει να παραλάβει την ΑΔΔΥ με συστημένη. Επίσης του γνωστοποιείται στο SMS το PIN, που μπορεί όταν παραλάβει την ΑΔΔΥ να το αλλάξει.
6. Κατά την παραλαβή της ΑΔΔΥ, που γίνεται μόνο αυτοπροσώπως, ο αιτών παραδίδει φωτοτυπία της Αστυνομικής Ταυτότητας (μπρος, πίσω) που αντιπαραβάλλεται με την πρωτότυπη (ταυτοποίηση). Επίσης υπογράφει την σχετική Αίτηση και αναγράφεται η ημερομηνία παραλαβής.

Εάν δεν παραδοθεί φωτοτυπία της ταυτότητας ή δεν υπογραφεί η Αίτηση, η ΑΔΔΥ δεν παραδίδεται, διότι τότε δεν πληρούνται οι απαιτήσεις του νόμου και οι αποφάσεις της ΕΕΤΤ, για Ταυτοποίηση κατά την παραλαβή της ΑΔΔΥ.

Έχω Παραλάβει την ΑΔΔΥ τι Απαιτείται για να την Χρησιμοποιήσω;

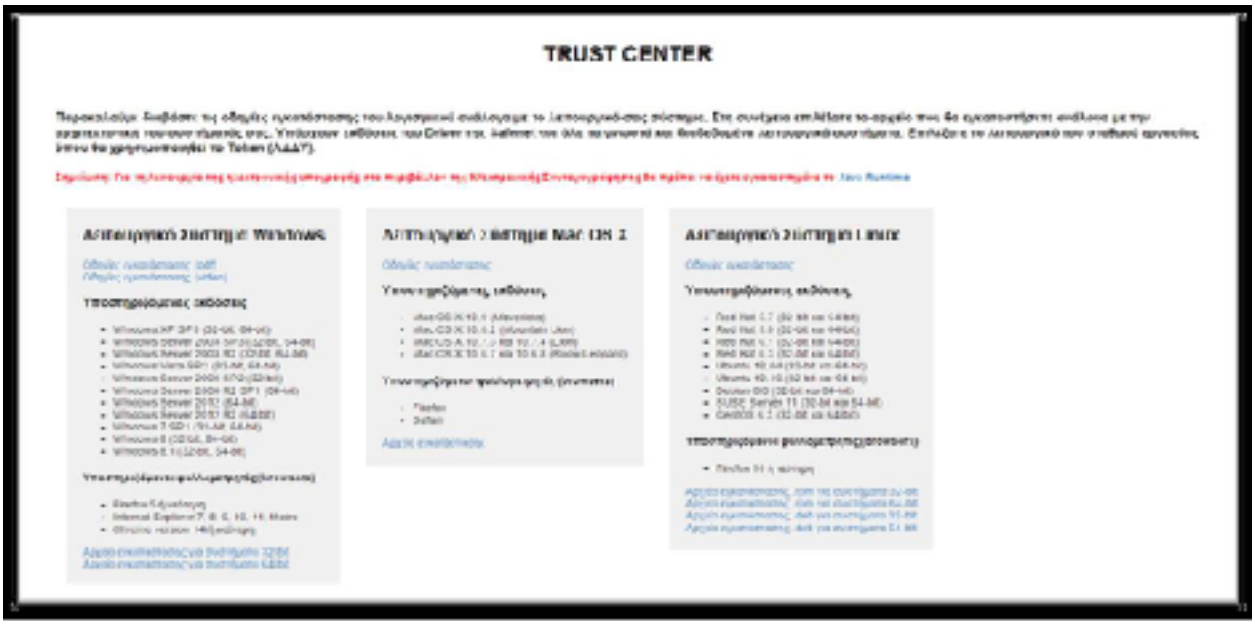
Το μόνον επιπλέον που απαιτείται είναι να εγκατασταθεί στο PC το λογισμικό που επικοινωνεί με την ΑΔΔΥ (drivers).

Ανάλογα με το λειτουργικό στο PC απαιτείται διαφορετικό λογισμικό. Στον ιστότοπο www.e-prescription.gr/tokenSoftware υπάρχουν οι drivers για όλα τα διαδεδομένα λειτουργικά (Microsoft Windows, Linux, Apple Mac), που μπορείτε να κατεβάσετε και να χρησιμοποιήσετε με βάση τις αντίστοιχες οδηγίες εγκατάστασης Βλέπε αμέσως παρακάτω.

Μετά την εγκατάσταση του λογισμικού επικοινωνίας PC με ΑΔΔΥ, για να γίνει χρήση ενός πιστοποιητικού (Αυθεντικοποίηση, Ψηφιακή Υπογραφή) το μόνο που απαιτείται είναι η ΑΔΔΥ να βρίσκεται σε μία USB θύρα και επιπλέον να δοθεί όταν του ζητηθεί το PIN που «ξεκλειδώνει» το κρυπτογραφικό τσιπ και επιτρέπεται η επικοινωνία μεταξύ PC και ΑΔΔΥ.

Ποια Λειτουργικά Συστήματα στο PC υποστηρίζονται;

Όλα τα TOKEN για την Ηλεκτρονική Συνταγογράφηση είναι του κατασκευαστή SafeNet και συγκεκριμένα το USB eToken-5100. Τα υποστηριζόμενα λειτουργικά είναι τα παρακάτω στο www.e-prescription.gr/tokenSoftware



Σε περίπτωση απώλειας του TOKEN, ποια είναι η σχετική διαδικασία για την ακύρωση των ψηφιακών πιστοποιητικών και την απόκτηση νέου TOKEN;

Αρχικά θα πρέπει να ανακληθούν τα ψηφιακά πιστοποιητικά. Η ανάκληση των ψηφιακών πιστοποιητικών γίνεται από το Trust Center με εντολή της ΗΔΙΚΑ που είναι ο κάτοχος των TOKEN και Πιστοποιητικών για χρήση στην Ηλεκτρονική Συνταγογράφηση. Για περιπτώσεις έκτακτης ανάγκης πχ απώλεια ΑΔΔΥ και PIN μαζύ (κάτι που δεν πρέπει να συμβεί, δηλαδή να είναι μαζύ πχ να έχει γραφτεί το PIN πάνω στην ΑΔΔΥ) υπάρχουν σχετικές οδηγίες καθώς και για την επιβάρυνση για νέο USB Token με νέα πιστοποιητικά.

Βλέπε ΗΔΙΚΑ «Αίτηση – Όροι Συνδρομητή – ePrescription» στον ιστότοπο www.e-prescription.gr

Με ποιον τρόπο μπορώ να αλλάξω τον προσωπικό κωδικό PIN στην ΑΔΔΥ;

Οδηγίες για αλλαγή PIN (Personal Identification Number) υπάρχουν για κάθε ένα από τα υποστηριζόμενα λειτουργικά στο ιστότοπο www.e-prescription.gr/tokenSoftware . Σημειώνεται ότι οι οδηγίες αυτές ισχύουν μόνο για το SafeNet USB Token (ΑΔΔΥ) που παραδόθηκε.

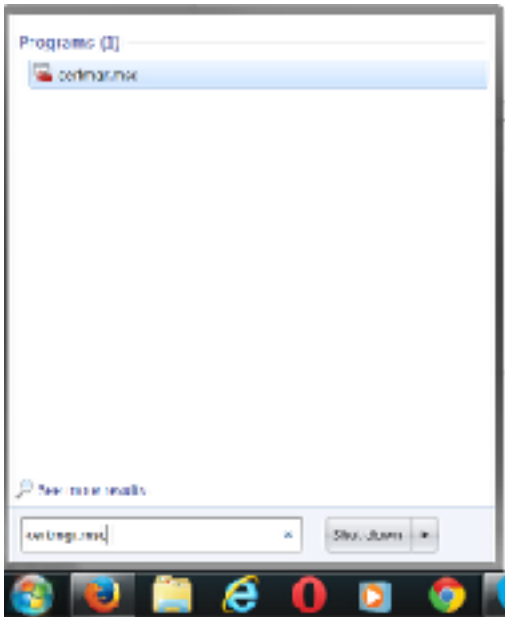
Σημείωση.
Το PIN είναι γνωστό μόνο στον χρήστη (συνδρομητή) που έχει παραλάβει την ΑΔΔΥ, που με την διαδικασία που περιγράφεται παραπάνω μπορεί να το αλλάξει όσες φορές το επιθυμεί. Το PIN για λόγους ασφάλειας είναι άγνωστο στο Trust Center και δεν μπορεί να επέμβει αν π.χ. ο χρήστης το ξεχάσει. Στις περιπτώσεις αυτές γίνεται επανέκδοση.

Πως μπορώ να ελέγξω την ημερομηνία έκδοσης των ψηφιακών μου πιστοποιητικών ώστε να γνωρίζω ότι είναι τα σωστά και πότε λήγουν;

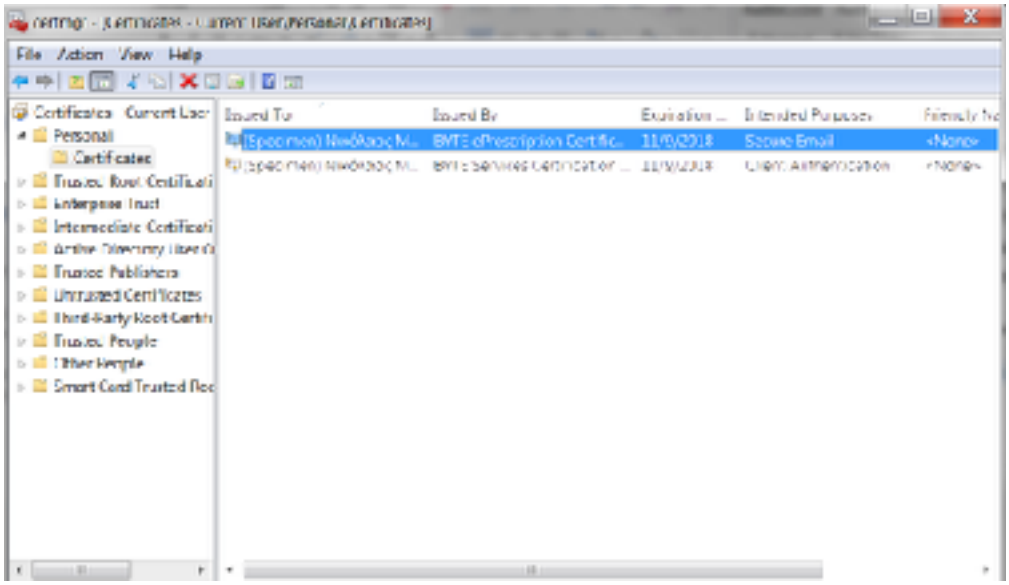
Τα πιστοποιητικά έχουν διάρκεια ζωής τέσσερα (4) έτη. Μπορείτε να δείτε την ημερομηνία που εκδόθηκαν τα πιστοποιητικά σας καθώς και πότε λήγουν.
Η διαδικασία είναι σχετικά απλή:

Το TOKEN εισάγεται σε μία θύρα USB.

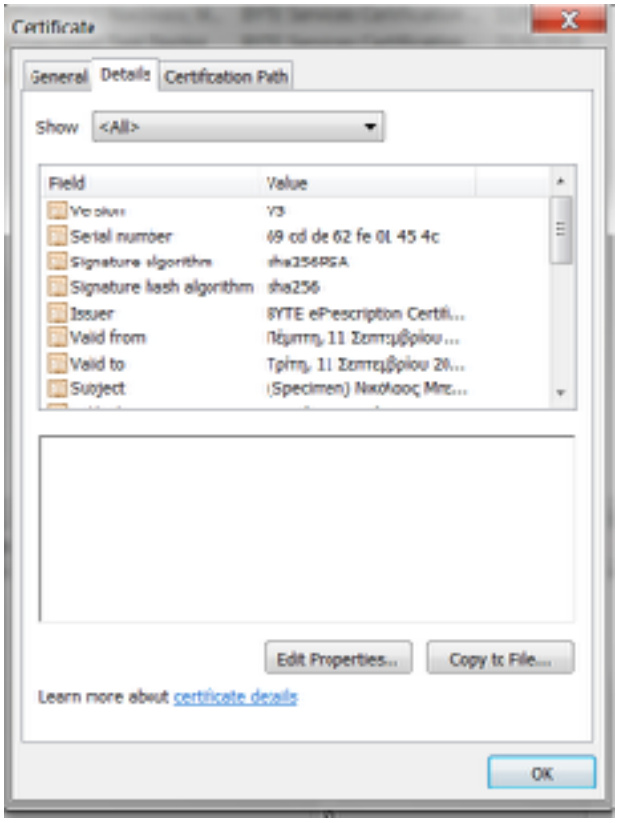
Ανοίγουμε τη Διαχείριση Πιστοποιητικών (Certificate Manager), πατώντα το Start button και γράφοντας certmgr.msc στο πεδίο αναζήτησης και πατάμε enter. (Μπορεί να σας ζητηθεί administrator password).

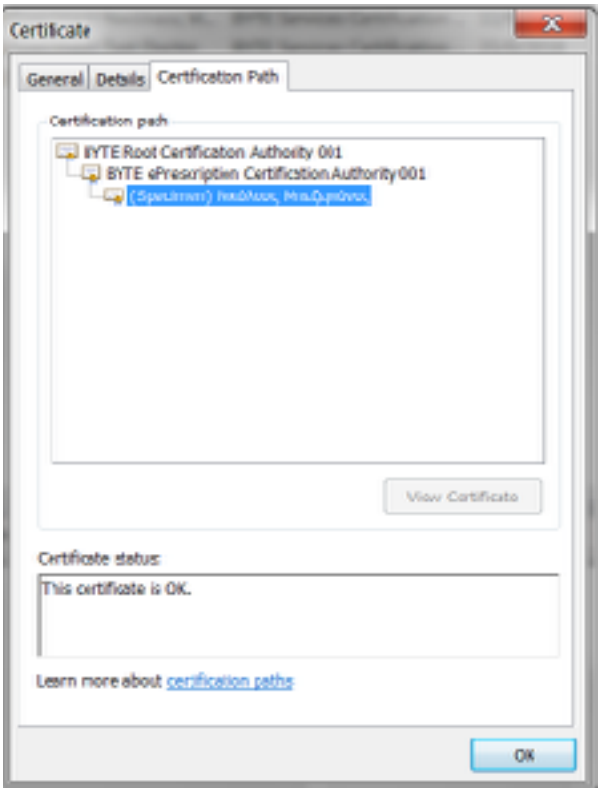


Επιλέγουμε το φάκελο Personal, Certificates και εμφανίζονται δεξιά τα προσωπικά μας πιστοποιητικά που είναι αποθηκευμένα στο USB Token μαζί με πληροφορίες για την ημερομηνία λήξης καθώς και το σκοπό για τον οποίο έχουν εκδοθεί. Να σημειωθεί ότι ο σκοπός Secure Email αφορά στη γενική υπογραφή εγγράφων.



Πατώντας διπλό κλικ σε όποιο πιστοποιητικό θέλουμε 2 πιστοποιητικά (για την Ηλεκτρονική Συνταγογράφηση) μπορούν να δούμε περισσότερες πληροφορίες. Εμφανίζεται δηλαδή το παρακάτω παράθυρο, το οποίο στη καρτέλα λεπτομέρειες (Details) περιέχει όλη τη πληροφορία για το συγκεκριμένο πιστοποιητικό. Παρατηρούμε ότι για κάθε Certificate εμφανίζονται πλήθος πληροφοριών μεταξύ των οποίων το όνομα του κατόχου, ποιός το έκδωσε, πότε εκδόθηκε, μέχρι πότε ισχύει, αν είναι σε ισχύ (valid) σε σχέση με την ημερομηνία λήξης που έχει καταγραφεί στο πιστοποιητικό(και όχι αν έχει ανακληθεί για άλλο λόγο), κα.





Στη καρτέλα Certification Path μπορούμε να δούμε την Αρχή Πιστοποίησης που εγγυάται και έχει πιστοποιήσει το συγκεκριμένο πιστοποιητικό.

Έχω παραλάβει την ΑΔΔΥ. Τί ακριβώς θα πρέπει να κάνω για να χρησιμοποιώ τα ψηφιακά πιστοποιητικά στον υπολογιστή μου;

Όπως και αλλού αναφέρεται πριν την χρήση απαιτείται να εγκαταστήσετε στον υπολογιστή σας το λογισμικό της SafeNet που κατασκευάζει τις ΑΔΔΥ. Η διαδικασία γίνεται μία φορά σε κάθε υπολογιστή από τον οποίο θέλετε να χρησιμοποιήσετε τα ψηφιακά σας πιστοποιητικά (Αυθεντικοποίηση, Ψηφιακή Υπογραφή). Το λογισμικό της SafeNet (client) μπορείτε να κατεβάσετε από τον ιστότοπο www.e-prescription.gr/tokenSoftware .

Για κάθε υποστηριζόμενο λειτουργικό υπάρχει αντίστοιχο λογισμικό και «οδηγίες εγκατάστασης» που πρέπει να συμβουλευτείτε πριν την εγκατάσταση.

Μπορώ να κατεβάσω εκ νέου τα ψηφιακά μου πιστοποιητικά μου στην ΑΔΔΥ;

Όχι. Τα πιστοποιητικά εκδίδονται με αυστηρά ασφαλή τρόπο και μία μόνον φορά, και δεν επιτρέπεται να κάνουμε αντίγραφα ασφαλείας. Με βάση τα διεθνή πρότυπα τα πιστοποιητικά (Ιδιωτικά) είναι αποθηκευμένα με ασφαλή τρόπο μόνον στην ΑΔΔΥ.

Επιτρέπεται η κατοχή διαφορετικών ψηφιακών πιστοποιητικών από τον ίδιο χρήστη;

Η ψηφιακή υπογραφή του χρήστη για την Ηλεκτρονική Συνταγογράφηση είναι μία. Τα ψηφιακά πιστοποιητικά περιέχουν πληροφορίες που αφορούν τον τελικό χρήστη, όπως αυτά δόθηκαν στην Αίτησή του και σύμφωνα με το θεσμικό πλαίσιο ο τελικός χρήστης θα πρέπει υποχρεωτικά να ανακαλέσει τα πιστοποιητικά του άμεσα σε οποιαδήποτε μεταβολή των στοιχείων του. Επομένως, δεν δικαιολογείται η κατοχή διαφορετικών ψηφιακών

πιστοποιητικών από τον ίδιο χρήστη για ψηφιακή υπογραφή στην Ηλεκτρονική Συνταγογράφηση, δεδομένου ότι το ζευγάρι πιστοποιητικών είναι από μόνο του ικανό και αρκετό για να ταυτοποιήσει τον τελικό χρήστη.

Όπως και αλλού αναφέρουμε για κάθε χρήστη εκδίδεται 2 ζευγάρια πιστοποιητικών (Ιδιωτικό, Δημόσιο), το 1ο ζευγάρη για την Αυθεντικοποίηση, και το 2ο ζευγάρι για την αναγνωρισμένη ψηφιακή υπογραφή.

Στην Αίτηση και φυσική ταυτοποίηση θα πρέπει να χρησιμοποιήσω ελληνικά ή λατινικά γράμματα;

Οι οδηγίες ευρίσκονται στην φόρμα Αίτησης. Βλέπε www.e-prescription.gr .

1. Ακρωνύμια – Συντομογραφία – Ελληνικοί Όροι

ΑΕ (RA)	Αρχή Εγγραφής (RA)
Α.Δ.Α.	Αριθμός Διαδικτυακής Ανάρτησης
ΑΠ (CA)	Αρχή Πιστοποίησης (CA)
ΑΔΔΥ (SSCD)	Ασφαλής Διάταξη Δημιουργίας Υπογραφής (SSCD)
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΑΠΕΔ	Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΕΡΜΗΣ)
Δ.Π.(CPS)	Δήλωση Πρακτικής
ΔΔΤ	Δημόσιος Διαδικτυακός Τόπος
ΛΑΠ ή ΚΑΠ	Λίστα ή Κατάλογος Ανακληθέντων Πιστοποιητικών (CRL)
ΟΤΣ	Όροι Τρίτων Συμμετεχόντων
Ο.Χ.Π.	Όροι Χρήσης Πιστοποιητικών
ΠΑ (OID)	Προσδιοριστής Αντικειμένου
ΠΚΑ ή PIN	Προσωπικός Κωδικός Αναγνώρισης (του συνδρομητή - PIN)
ΠΠ (CP)	Πολιτική Πιστοποιητικών (CP)
ΠΠΔΔΤ	Πλαίσιο Πιστοποίησης Δημόσιων Διαδικτυακών Τόπων
ΠΥΠ (CSP)	Πάροχος Υπηρεσιών Πιστοποίησης (CSP)
Τ.Π.Ε.	Τεχνολογίες Πληροφορικής και Επικοινωνιών
ΥΠ.ΑΠ.	Υποκείμενες Αρχές Πιστοποίησης (subCAs)

ANSI	American National Standards Institute
C	Country
CA	Certification Authority
RA	Registration Authority
CP	Certificate Policy.
NCP	Normalized Certificate Policy
CPS	Certification Practices Statement
CE	Certifying Entity
CN	Common Name
CRL	Certificate Revocation List (or LRC)
CMS	Card Management System
CSR	Certificate Signing Request
DCE	Document Certifying Entity
DL	Decree-Law
DN	Distinguished Name

CPS	Certification Practices Statement
RD	Regulatory Decree
DCE	Document Certification Authority
GMT	Greenwich Mean Time
EAL	Evaluation assurance level (pursuant to the Common Criteria).
FIPS	United State Federal Information Processing Standards.
EEET	Hellenic Telecommunications and Post Commission
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
HSM	Hardware Security Module
MAC	Message Authentication Codes
ICANN	Internet Corporation for Assigned Names and Numbers
IdM	Identity Management System
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
ITU-T ITU	ITU Telecommunication Standardization Sector
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OVCP	Organizational Validation Certificate Policy
PIN	Personal identification Number.
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
RA	Registration Authority.
RFC	Request for comment.
SHA	Secure Hash Algorithm
SGCVC	System for Managing the Certificate Life Cycle
SSCD	Secure Signature-Creation Device
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
TSA	Time-Stamping Authority (the same as EVC)
TLS	Transport Layer Security
URL	Uniform Resource Locator

UTC	Coordinated Universal Time
X.509	The ITU−T standard for Certificates and their corresponding authentication framework