Όροι και Ορθή χρήση ψηφιακής υπογραφής

Οι Τελικοί Χρήστες (φυσικό πρόσωπο για το οποίο εκδίδεται ένα ψηφιακό πιστοποιητικό κατόπιν αίτησης του) των εμπλεκόμενων φορέων διαθέτουν από δύο ψηφιακά πιστοποιητικά, ένα για ψηφιακή υπογραφή και ένα για κρυπτογράφηση. Τα ψηφιακά πιστοποιητικά (και τα σχετικά ζεύγη κλειδιών) δημιουργούνται από Ασφαλείς Διατάξεις, εκδίδονται ηλεκτρονικά από την ΥπΑΠ και αποθηκεύονται με ασφάλεια στις Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής, όπως έξυπνες κάρτες, Usb token, οι οποίες διατίθενται στους τελικούς χρήστες. Στο πρώτο στάδιο εφαρμογής της υπηρεσίας PKI χορηγούνται επίσης και οι απαραίτητοι αναγνώστες καρτών (card readers).

Τα ψηφιακά πιστοποιητικά είναι αυστηρώς προσωπικά και χρησιμοποιούνται αποκλειστικά στο πλαίσιο άσκησης των καθηκόντων των κατόχων τους για την εξυπηρέτηση υπηρεσιακών αναγκών του φορέα τους. Ενδεικτικές χρήσεις για τα ψηφιακά πιστοποιητικά είναι:

- Η ασφαλής επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου / ανταλλαγής μηνυμάτων (υπογραφή και κρυπτογράφηση)
- Η υπογραφή και κρυπτογράφηση ηλεκτρονικών αρχείων (π.χ. αρχεία Adobe Reader., αρχεία word)
- Ο ασφαλής προσδιορισμός ηλεκτρονικής ταυτότητας
- Ο έλεγχος πρόσβασης σε κατάλληλες εφαρμογές.

Οι όροι χορήγησης ψηφιακού πιστοποιητικού στο τελικό χρήστη, που αποτελούν παράλληλα και υποχρεώσεις του, σύμφωνα με τον Κανονισμό Πιστοποίησης περιλαμβάνουν τα ακόλουθα:

- Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται αποκλειστικά για εγκεκριμένους και σύννομους σκοπούς σύμφωνα με τον Κανονισμό Πιστοποίησης.
- Ο τελικός χρήστης θα πρέπει να λάβει υπόψη τους περιορισμούς στη διαχείριση και χρήση των πιστοποιητικών όπως αναφέρονται στον Κανονισμό Πιστοποίησης.
- Η έξυπνη κάρτα (ή usb token) και οι αντίστοιχοι κωδικοί αριθμοί PIN-PUK είναι
- αυστηρώς προσωπικοί και ο τελικός χρήστης είναι ο μόνος αρμόδιος για τη

- χρήση τους καθώς και για την ασφαλή φύλαξη τους. Ο τελικός χρήστης δεν πρέπει να αφήνει εκτεθειμένη την έξυπνη κάρτα ή το usb token του σε οποιοδήποτε μέρος, ακόμα και στο χώρο εργασίας του.
- Ο τελικός χρήστης θα πρέπει να υπογράψει την έξυπνη κάρτα στο ειδικό πλαίσιο στην πίσω πλευρά.
- Ο τελικός χρήστης δεν πρέπει να δανείζει την έξυπνη κάρτα ή να γνωστοποιεί τους κωδικούς αριθμούς PIN-PUK σε οποιονδήποτε.
- Εάν αντιμετωπίσει κάποιο πρόβλημα ή υποπέσει στην αντίληψη του κάποια παραβίαση των παραπάνω, ή απωλεσθεί, κλαπεί ή

καταστραφεί η έξυπνη κάρτα, ο τελικός χρήστης οφείλει να ενημερώσει άμεσα την Αρχή Εγγραφής στην οποία υπάγεται.

- Σε περίπτωση λήξης της εργασιακής του σχέσης με το φορέα που εργάζεται ο τελικός χρήστης οφείλει να ενημερώσει την αρχή εγγραφής που υπάγεται για την ανάκληση και επιστροφή της έξυπνης κάρτας.
- Ο τελικός χρήστης με την υποβολή αίτησης απόκτησης, ψηφιακού πιστοποιητικού αποδέχεται όλα τα δικαιώματα και τις υποχρεώσεις που απορρέουν από τον Κανονισμό Πιστοποίησης της ΑΠΕΔ.

Το φυσικό πρόσωπο που βασίζεται στα στοιχεία τα οποία περιέχονται σε ένα ψηφιακό πιστοποιητικό, το οποίο εκδίδεται σύμφωνα με τα προβλεπόμενα στον ΚΠ, ονομάζεται Τρίτος Συμμετέχων (ΤΣ).

- Ο Τρίτος Συμμετέχων πρέπει να έχει πρόσβαση, μέσω διαδικτύου, σε επαρκείς πληροφορίες που του παρέχονται από την Υποδομή Δημόσιου Κλειδιού της ΑΠΕΔ, στους δικτυακούς τόπους- που αναφέρονται στην παρούσα εγκύκλιο, οι οποίες του επιτρέπουν να ελέγξει κατά πόσον θα βασιστεί σε ένα ψηφιακό πιστοποιητικό.
- ο Τρίτος Συμμετέχων θα πρέπει να διαθέτει, σύγχρονες - κατάλληλες εφαρμογές (π.χ. Internet browses, κειμενογράφους κλπ) προκειμένου να προβεί «αυτόματα» σε όλες τις απαραίτητες ενέργειες για τον έλεγχο της εγκυρότητας ενός Πιστοποιητικού όπως προβλέπεται στον Κανονισμό Πιστοποίησης.
- Ο Τρίτος Συμμετέχων θα πρέπει να λάβει υπόψη τους περιορισμούς στη χρήση του πιστοποιητικού (υπογραφή ή κρυπτογράφηση) οι οποίοι αναφέρονται στον Κανονισμό Πιστοποίησης της ΑΠΕΔ.