Ηλεκτρονική Διακυβέρνηση

Παπανικολάου Γεώργιος

Ψηφιακά Πιστοποιητικά

- Τα διαφορετικά πιστοποιητικά που μπορούν να αξιοποιηθούν από τους χρήστης για υπηρεσίες ηλεκτρονικής διακυβέρνησης είναι:
  - ψηφιακό πιστοποιητικό για ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων και εγγράφων.
  - ψηφιακό πιστοποιητικό για κρυπτογράφηση ηλεκτρονικών μηνυμάτων η εγγράφων.
  - Κάτοχοι ψηφιακών πιστοποιητικών έχουν οι χρήστες δημόσιοι λειτουργοί που κατέχουν συγκεκριμένη αρμοδιότητα στο πλαίσιο άσκησης των καθηκόντων τους και στην συγκεκριμένη οργανική μονάδα που υπηρετούν.

Ψηφιακά Πιστοποιητικά

- Τα ψηφιακά πιστοποιητικά που θα αξιοποιηθούν στις υπηρεσίες ηλεκτρονικής διακυβέρνησης περιλαμβάνουν τα βασικά πεδία που απαιτούνται από το Π.Δ. 150/2001 και είναι:
  - Έκδοση, Αριθμός σειράς, αλγόριθμος υπογραφής, διακριτικό όνομα εκδότη, ισχύει από, ισχύει μέχρι, διακριτικό όνομα υποκειμένου, δημόσιο κλειδί υποκειμένου, υπογραφή.

Ψηφιακά Πιστοποιητικά

- Έκδοση: Αναφέρεται στην έκδοση του προτύπου X.509 πιστοποιητικών και υποστηρίζει εκτεταμένα πεδία.
- Αριθμός σειράς: αποτελείται από το μοναδικό αριθμό του εκδιδόμενου πιστοποιητικού.
- Αλγόριθμος υπογραφής: αναφέρεται στον αλγόριθμο σύνοψης που θα αξιοποιείται από την υποδομή δημοσίου κλειδιού.
- Διακριτικό όνομα εκδότη: αναφέρεται στο όνομα του εκδότη του πιστοποιητικού και αποτελείται από τα υπο-πεδία Χώρα (Country), Οργανισμός (Organization), κοινό όνομα και ηλεκτρονική διεύθυνση. Τα παραπάνω πεδία πλην της Ηλεκτρονικής Διεύθυνσης είναι υποχρεωτικά.

Ψηφιακά Πιστοποιητικά

- Ισχύει από: περιλαμβάνει την ημερομηνία έκδοσης του πιστοποιητικού.
- Ισχύει έως: περιλαμβάνει την ημερομηνία λήξης του πιστοποιητικού.
- Διακριτικό όνομα υποκειμένου: αναφέρεται στον κάτοχο του πιστοποιητικού και αποτελείται από τα ύπο πεδία Χώρα, Οργανισμός, Κοινό όνομα και ηλεκτρονική διεύθυνση. Τα παραπάνω πεδία πλην της ηλεκτρονικής διεύθυνσης είναι υποχρεωτικά.

Ψηφιακά Πιστοποιητικά

- Μέθοδοι δημιουργίας κλειδιών κρυπτογράφησης
  - Τα ζεύγη κλειδιών κρυπτογράφησης θα δημιουργούνται κεντρικοποιημένα από την αρχή Πιστοποίησης.
  - Η δημιουργία γίνεται ακολουθώντας ασφαλείς διατάξεις σύμφωνα με το προεδρικό διάταγμα 150/2001.
  - Η δημόσιοι υπάλληλοι χρήστες του ΣΥΖΕΥΞΙΣ προβλέπεται να δημιουργήσουν και να αποθηκεύσουν τα ιδιωτικά κλειδιά αποκρυπτογράφησης.

Ψηφιακά Πιστοποιητικά

- Η Αρχή εγγραφής και Αρχή Πιστοποίησης διασφαλίζουν επικοινωνία με εμπιστευτικότητα και ακεραιότητα αξιοποιώντας πρωτόκολλα και μηχανισμούς.
- Κλειδιά: Το μήκος των κλειδιών για τους χρήστες πρέπει να είναι τουλάχιστον 1024 bits. Το μήκος

Ψηφιακά Πιστοποιητικά

- Το δημόσιο κλειδί, που αξιοποιείται στη διαδικασία της κρυπτογράφησης, βρίσκεται στη διάθεση της Αρχής Πιστοποίησης, καθώς τα κλειδιά αυτά δημιουργούνται κεντρικά, ενώ το δημόσιο κλειδί για την επαλήθευση της ψηφιακής υπογραφής αποθηκεύεται στην Αρχή Πιστοποίησης με την έκδοση του αντίστοιχου ψηφιακού πιστοποιητικού, το οποίο και συμπεριλαμβάνεται στην αντίστοιχη αίτηση έκδοσης πιστοποιητικού.

Ψηφιακά Πιστοποιητικά

- Η αρχή πιστοποίησης έχει την δυνατότητα ανάκλησης των πιστοποιητικών στις ακόλουθες περιπτώσεις:
  - Λήξη του πιστοποιητικού του χρήστη.
  - Μη συμμόρφωση του χρήστη με την παρούσα πολιτική.
  - Διακύβευση του ιδιωτικού κλειδιού.
  - Απώλεια της ασφαλούς διάταξης αποθήκευσης των κλειδιών
  - Τερματισμός λειτουργίας της Αρχής Πιστοποίησης.

Ψηφιακά Πιστοποιητικά

- Χρήστες των ψηφιακών πιστοποιητικών είναι:
  - Κάθε φυσικό πρόσωπο.
  - Κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου ιδιωτικού δικαίου.
  - Κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου δημοσίου δικαίου.

Ψηφιακά Πιστοποιητικά

Μέθοδος ανάκλησης ζεύγους κλειδιών

- Τα ζεύγη κλειδιών θα διαγράφονται από το διακριτικό στο οποίο αποθηκεύονται, εφόσον γίνεται αποδεκτή η αίτηση ανάκλησης.
- Για να ανακαλέσουμε ένα ζεύγος κλειδιών θα πρέπει να χρησιμοποιήσουμε την κατάλληλη υπηρεσία ανάκλησης στα πλαίσια της οποίας θα συμπληρώσουμε αίτηση, θα την υπογράψουμε ψηφιακά και θα την υποβάλλουμε ηλεκτρονικά εφόσον βέβαια είναι ενεργό το διακριτικό αποθήκευσης. Σε διαφορετική περίπτωση ο χρήστης θα πρέπει να μεταβεί αυτοπροσώπως στην Αρχή Εγγραφής και να υποβάλει την αίτηση.

Ψηφιακό Πιστοποιητικό

- Αφού διαπιστωθεί η εγκυρότητα των στοιχείων από την Αρχή Εγγραφής, η αίτηση προωθείται στην Αρχή Πιστοποίησης για περαιτέρω επεξεργασία και την τελική ανάκληση των κλειδιών, με τη διαγραφή τους από το διακριτικό αποθήκευσης, την ανάκληση των αντίστοιχων πιστοποιητικών, καθώς και την ενημέρωση της λίστας ανακλημένων πιστοποιητικών.

Ψηφιακό Πιστοποιητικό

Επαναδημιουργία – Ανανέωση Κλειδιού

Η ανανέωση-επαναδημιουργία των κλειδιών κρυπτογράφησης μπορεί να πραγματοποιηθεί για μη ανακλημένα πιστοποιητικά στις ακόλουθες περιπτώσεις:

- Απώλεια του Διακριτικού Αποθήκευσης των κλειδιών
- Αστοχία υλικού στο διακριτικό αποθήκευσης των κλειδιών (μοναδική περίπτωση επαναδημιουργίας)
- Δημοσίευση επιθέσεων οι οποίες επηρεάζουν τα υπάρχοντα ζεύγη κλειδιών
- Καθιερωμένη ανανέωση κλειδιών πριν τη λήξη του πιστοποιητικού

Ψηφιακό Πιστοποιητικό

- Η ενεργοποίηση των κλειδιών θα πραγματοποιείται με την αξιοποίηση του αντίστοιχου PIN/PUK.
- Οι οντότητες που αιτούνται την έκδοση πιστοποιητικών θα πρέπει να εφαρμόζουν και να αποδέχονται, σε κάθε περίπτωση, την Πολιτική Πιστοποιητικών που εφαρμόζει η εκάστοτε ΥΔΚ. Για να είναι δυνατή η αίτηση έκδοσης πιστοποιητικών, ο χρήστης θα πρέπει να έχει παραλάβει το διακριτικό αποθήκευσης στο οποίο είναι αποθηκευμένα τα ζεύγη κλειδιών του, αφού βέβαια έχει πρώτα υποβάλει αίτηση εγγραφής σε υπηρεσίες ακολουθώντας τις διαδικασίες εγγραφής.

Ψηφιακά Πιστοποιητικά

- Εφόσον έχει παραλάβει το διακριτικό αποθήκευσης είναι σε θέση να αιτηθεί την έκδοση των πιστοποιητικών, αξιοποιώντας την ηλεκτρονική υπηρεσία έκδοσης ψηφιακών πιστοποιητικών.