ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟ

ΥΨηΔ 02/11/2020
Α. Π.: 30611 ΕΞ 2020

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

Γενική Γραμματεία
Ψηφιακής Διακυβέρνησης
& Απλούστευσης Διαδικασιών

ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΔΙΟΙΚΗΤΙΚΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΔΗΜΟΣΙΟΥ
ΔΙΕΥΘΥΝΣΗ ΥΠΗΡΕΣΙΩΝ ΜΙΑΣ ΣΤΑΣΗΣ
ΤΜΗΜΑ ΥΠΟΣΤΗΡΙΞΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΚΕΠ

ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΤΜΗΜΑ ΥΠΗΡΕΣΙΩΝ ΕΜΠΙΣΤΟΣΥΝΗΣ
e-mail: aped@mindigital.gr
Τηλ:210 909 8555, 8560, 8505, 8592, 8575

ΠΡΟΣ: Προϊσταμένους Κέντρων Εξυπηρέτησης Πολιτών της χώρας
Kep-all@kep.gov.gr

Θέμα: "Ενημέρωση Εντεταλμένων Γραφείων για τη λειτουργία νέας Εφαρμογής Διαχείρισης Ψηφιακών Πιστοποιητικών της ΑΠΕΔ"

Σχετικά:

- ✓ Κανονισμός (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (eIDAS) σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της Οδηγίας 1999/93/ΕΚ
- ✓ Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ
- ✓ Κανονισμός της ΕΕΤΤ 14/12/2017 (Β'4396) «Κανονισμός Παροχής Υπηρεσιών Εμπιστοσύνης» σκοπός του οποίου είναι η ρύθμιση ζητημάτων των υπηρεσιών εμπιστοσύνης και των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών εμπιστοσύνης σε συμπλήρωση του Κανονισμού (ΕΕ) αρ.910/2014 eIDAS
- ✓ Η υπ' αριθμ. ΥΑΠ/Φ.60/86/1435 Υπουργική Απόφαση με θέμα «Καθορισμός διαδικασιών υποβολής αιτήσεων έκδοσης, ανάκλησης, ανανέωσης ψηφιακών πιστοποιητικών καθώς και ανάκτησης του ψηφιακού πιστοποιητικού κρυπτογράφησης μέσω των Κέντρων Εξυπηρέτησης Πολιτών (ΚΕΠ), ως Εντεταλμένων Γραφείων»
- ✓ Ο υπ' αριθμ. ν.4727/2020 (Α'184/23-09-2020) «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της

Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις»

Σύμφωνα με το ν.4727/2020 (Α 184/23-9-2020) η ψηφιακή υπογραφή ενέχει θέση ιδιόχειρης υπογραφής και η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) αποτελεί τον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης του Ελληνικού Δημοσίου. Κατά τα οριζόμενα στον Κανονισμό (ΕΕ) eIDAS 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου προβλέπεται στο αρ. 24 ότι ο εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης οφείλει κατά την έκδοση εγκεκριμένου πιστοποιητικού με κατάλληλα μέσα, την εξακρίβωση της ταυτότητας άμεσα είτε μέσω τρίτου, σύμφωνα με το εθνικό δίκαιο. Η ταυτοποίηση του Συνδρομητή διενεργείται με μία από τις αναφερόμενες στην παρ. 1 του άρθρου 24 του Κανονισμού eIDAS μεθόδους.

Ειδικότερα ο εγκεκριμένος πάροχος υπηρεσιών Εμπιστοσύνης ΑΠΕΔ σύμφωνα με τον Κανονισμό του, (παρ.3.2.2) ορίζει ότι η εξακρίβωση της ταυτότητας του Συνδρομητή με φυσική παρουσία γίνεται με την προσωπική (φυσική) επαφή του με στέλεχος του Εντεταλμένου Γραφείου ή της Αρχής Εγγραφής όπου ελέγχεται η ταυτότητα του με έγγραφα ταυτοποίησης που εξειδικεύονται στην Αίτηση για έκδοση Πιστοποιητικού. Σύμφωνα με την υπ’ αριθμ. ΥΑΠ/Φ.60/86/1435 (Β 1876/13-06-2012) Υπουργική Απόφαση τα Κέντρα Εξυπηρέτησης Πολιτών (ΚΕΠ) ορίζονται ως Εντεταλμένα Γραφεία της ΑΠΕΔ.

Η Διεύθυνση Υπηρεσιών μίας Στάσης σε συνεργασία με τη Διεύθυνση Ηλεκτρονικής Διακυβέρνησης, στο εξής (ΔΗΔ), υφιστάμενες Διευθύνσεις της Γενικής Γραμματείας Ψηφιακής Διακυβέρνησης και Απλούστευσης Διαδικασιών (ΓΓΨΔΑΔ) του Υπουργείου Ψηφιακής Διακυβέρνησης στόχο έχουν την αποτελεσματική υποστήριξη των Εντεταλμένων Γραφείων, σε πάσης φύσεως ζητήματα που προκύπτουν και αφορούν τις διαδικασίες έκδοσης και διαχείρισης ψηφιακών πιστοποιητικών υπογραφής επιχειρησιακά και τεχνικά.

Σε συνέχεια των παραπάνω το Τμήμα Υπηρεσιών Εμπιστοσύνης της ΔΗΔ έχοντας την επιχειρησιακή διαχείριση της Αρχής Πιστοποίησης του Δημόσιου Τομέα ως Αρχή Εγγραφής προβαίνει σε αναβάθμιση της εφαρμογής της, καθώς υποχρεούται να συμμορφώνεται στις απαιτήσεις του Κανονισμού 910/2014 (eIDAS).

Από τα σημαντικότερα στοιχεία συμμόρφωσης στις διατάξεις του eIDAS είναι η ύπαρξη Πολιτικής Ασφάλειας των Πληροφοριακών Συστημάτων και των Πληροφοριών. Την Πολιτική Ασφάλειας οφείλει να τηρεί το σύνολο του προσωπικού που εμπλέκεται στη διαδικασία έκδοσης ψηφιακού πιστοποιητικού. Ως προσωπικό της ΑΠΕΔ θεωρείται το προσωπικό της Αρχής Εγγραφής και το προσωπικό των Εντεταλμένων Γραφείων. Οι μεν είναι υπάλληλοι του Τμήματος Υπηρεσιών Εμπιστοσύνης της Διεύθυνσης Ηλεκτρονικής Διακυβέρνησης της ΓΓΨΔΑΔ του ΥΨηΔ και είναι αρμόδιοι για την έγκριση της αίτησης έκδοσης των ψηφιακών πιστοποιητικών, οι δε είναι υπάλληλοι των ΚΕΠ ως προσωπικό

των Εντεταλμένων Γραφείων οι οποίοι είναι αρμόδιοι για τη φυσική ταυτοποίηση των φυσικών προσώπων που αιτούνται το ψηφιακό πιστοποιητικό και εποπτεύονται από τη Διεύθυνση Υπηρεσιών μίας Στάσης.

Για τον σκοπό αυτό όλοι οι Υπάλληλοι των ΚΕΠ που συμμετέχουν στην διαδικασία φυσικής ταυτοποίησης των φυσικών προσώπων που αιτούνται την έκδοση ψηφιακού πιστοποιητικού με ευθύνη των προϊσταμένων τους λαμβάνουν γνώση της Πολιτικής Ασφάλειας της ΑΠΕΔ (**ΠΑΡΑΡΤΗΜΑ Α**) στα σημεία που τους αφορούν και δεσμεύονται εγγράφως για την τήρησή της. (**ΠΑΡΑΡΤΗΜΑ Δ**)

Τονίζεται ότι η ΑΠΕΔ συμμορφώνεται πλήρως με το κανονιστικό πλαίσιο που διέπει τη συλλογή και επεξεργασία προσωπικών δεδομένων (Κανονισμός (ΕΕ) 2016/679). Η ΑΠΕΔ ως Πάροχος Υπηρεσιών Εμπιστοσύνης οφείλει να συλλέγει τις απαραίτητες πληροφορίες που απαιτούνται για την έκδοση Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής. Τα δεδομένα προσωπικού χαρακτήρα, τα οποία συλλέγονται κατά την εγγραφή και ταυτοποίηση για την έκδοση Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής, κατόπιν αιτήσεως του χρήστη, χρησιμοποιούνται αποκλειστικά για την έκδοση, ανάκληση και επεξεργασία των πιστοποιητικών ηλεκτρονικής υπογραφής, όπως ορίζεται στον Κανονισμό Πιστοποίησης της ΑΠΕΔ, και κοινοποιούνται σε τρίτα μέρη, μόνο με τη ρητή συγκατάθεση του Συνδρομητή.

Η Εφαρμογή Διαχείρισης Ψηφιακών Πιστοποιητικών αναμένεται να τεθεί σε παραγωγική λειτουργία μετά την ολοκλήρωσή της αξιολόγησης συμμόρφωσης ως προς τον Κανονισμό eIDAS. Οι υπάλληλοι θα πρέπει να χρησιμοποιούν Η/Υ των ΚΕΠ για την πρόσβασή τους στην Εφαρμογή Διαχείρισης Ψηφιακών Πιστοποιητικών μέσω της οποίας θα προωθούν την αίτηση στην Αρχή Εγγραφής αφού προηγουμένως έχουν ελέγξει την ορθότητα των στοιχείων της αίτησης με το ταυτοποιητικό έγγραφο που τους επιδεικνύει ο Συνδρομητής.

Ο υπάλληλος του ΚΕΠ για να συνδεθεί στην εφαρμογή, θα πρέπει να πληκτρολογήσει την ηλεκτρονική διεύθυνση https://www.ermis.gov.gr/apedkep/login και στη συνέχεια να ακολουθήσει τα βήματα τα οποία περιγράφονται στο εγχειρίδιο χρήσης (**ΠΑΡΑΡΤΗΜΑ Β**).

Το **ΠΑΡΑΡΤΗΜΑ Γ** αναφέρει τη διαδικασία που ακολουθεί ο Συνδρομητής (πολίτης) για να αιτηθεί και εν τέλει να εκδώσει Ψηφιακό πιστοποιητικό.

Επιπλέον η αξιολόγηση της συμμόρφωσης προς τον κανονισμό eIDAS προβλέπει και την αξιολόγηση των υπαλλήλων που συμμετέχουν στην διαδικασία έκδοσης Ψηφιακού Πιστοποιητικού.

Οι υπάλληλοι των ΚΕΠ που θα εμπλακούν παρακαλούνται να διαβάσουν την πολιτική Ασφαλείας , το εγχειρίδιο χρήσης και στη συνέχεια να απαντήσουν στις ερωτήσεις που θα βρουν πληκτρολογώντας την ηλεκτρονική διεύθυνση:
http://www.aped.gov.gr/index.php?option=com_rsform&view=rsform&formId=9

Οι απαντήσεις στις ερωτήσεις προκύπτουν από το περιεχόμενο της παρούσης εγκυκλίου, την **Πολιτική Ασφάλειας**, τις οδηγίες χρήσης της **Εφαρμογής Διαχείρισης Ψηφιακού Πιστοποιητικού** και τη **Διαδικασία Αίτησης- Ταυτοποίησης- Έκδοσης- Ανάκλησης Ψηφιακού Πιστοποιητικού** (Παραρτήματα Α, Β, Γ).

Με εντολή Υπουργού
ο Γενικός Γραμματέας Ψηφιακής
Διακυβέρνησης και Απλούστευσης
Διαδικασιών

Λεωνίδας Χριστόπουλος

Παράρτημα Α

Απόσπασμα Πολιτικής Ασφαλείας ΑΠΕΔ

1. Εισαγωγή

Όλο το προσωπικό της ΑΠΕΔ, καθώς και όποιος έχει πρόσβαση στις εφαρμογές και τα πληροφοριακά συστήματα της ΑΠΕΔ, υποχρεούται να συμμορφώνεται στις απαιτήσεις της Πολιτικής Ασφάλειας Πληροφοριών και Πληροφοριακών Συστημάτων της ΑΠΕΔ και να συμβάλει στην ενίσχυση των πρακτικών ασφάλειας, συνειδητοποιώντας τις υποχρεώσεις που έχει στα πλαίσια της ισχύουσας νομοθεσίας για ασφάλεια προσωπικών δεδομένων και πληροφοριακών συστημάτων.

Οι πληροφορίες (υπηρεσιακά έγγραφα, δεδομένα πολιτών κτλ) δεν είναι δημόσιες, επομένως αποκάλυψή τους σε μη εξουσιοδοτημένα άτομα απαγορεύεται. Με βάση το νομικό πλαίσιο ορίζονται εξαιρέσεις στις οποίες τέτοιες πληροφορίες μπορούν να αποκαλύπτονται σε τρίτους (π.χ. διαβίβαση σε δικαστικές Αρχές, παραχώρηση σε πολίτες έχοντες έννομο συμφέρον μετά από έγγραφη αίτησή τους). Οι δημόσιες πληροφορίες ορίζονται ρητά από τις αρμόδιες Υπηρεσίες και αφορούν πληροφορίες, η αποκάλυψη των οποίων, δεν μπορεί να βλάψει την ΑΠΕΔ, το ΥΨηΔ και το Κράτος γενικότερα.

2. Εξουσιοδοτήσεις και Έλεγχος προσωπικού

Οι βασικές αρχές παροχής δικαιωμάτων πρόσβασης στα Δεδομένα της ΑΠΕΔ, είναι η αρχή των ελάχιστων δικαιωμάτων (least privilege) και της ανάγκης γνώσης (need to know basis), ήτοι ο κάθε χρήστης αποκτά πρόσβαση μόνο σε πληροφοριακούς πόρους, οι οποίοι θεωρούνται απαραίτητοι για την ομαλή διεκπεραίωση των καθημερινών εργασιών του.

Τα δικαιώματα πρόσβασης του κάθε χρήστη σε εφαρμογές και πληροφοριακά συστήματα απορρέουν από το αντικείμενο εργασίας του καθώς και από τη θέση την οποία κατέχει στα πλαίσια της οργάνωσης της Υπηρεσίας και πρέπει να ορίζονται λεπτομερώς ανάλογα με τον εργασιακό ρόλο του κάθε εργαζόμενου.

Το προσωπικό που χρησιμοποιεί τα Πληροφοριακά Συστήματα της ΑΠΕΔ, συγκροτείται από το προσωπικό της Αρχής Εγγραφής και το προσωπικό των Εντεταλμένων Γραφείων.

Προσωπικό Εντεταλμένων Γραφείων

Α. Υπάλληλοι των ΚΕΠ

Είναι αρμόδιοι για την φυσική ταυτοποίηση των φυσικών προσώπων που αιτούνται το ψηφιακό πιστοποιητικό.

Χρησιμοποιούν Η/Υ των ΚΕΠ για την πρόσβασή τους στην Εφαρμογή Διαχείρισης Ψηφιακών Πιστοποιητικών μέσω της οποίας προωθούν την αίτηση στην Αρχή Εγγραφής αφού προηγουμένως έχουν ελέγξει την ορθότητα των στοιχείων της αίτησης με το ταυτοποιητικό έγγραφο που τους επιδεικνύει ο πολίτης.

Με ευθύνη του Προϊσταμένου του ΚΕΠ ο υπάλληλος:

- Λαμβάνει γνώση της Πολιτικής Ασφάλειας και δεσμεύεται εγγράφως για την αποδοχή των όρων της.

- Αποκτά πρόσβαση στην ΕΔΨΠ σύμφωνα με την παρακάτω διαδικασία:

  Ο προϊστάμενος του ΚΕΠ στέλνει σχετικό αίτημα έκδοσης κωδικών που περιλαμβάνει τα στοιχεία του υπαλλήλου (Όνομα, Επώνυμο, email, υπηρεσιακό τηλέφωνο), την δέσμευση και την απόφαση διορισμού ή την απόφαση τοποθέτησης του υπαλλήλου στο ΚΕΠ μαζί με αντίγραφο της έγγραφης αποδοχής των όρων της πολιτικής ασφαλείας στην αρμόδια οργανική μονάδα του Υπουργείου Ψηφιακής Διακυβέρνησης η οποία έχει την εποπτεία των ΚΕΠ. Η αρμόδια οργανική μονάδα, εφόσον συμφωνεί, προωθεί το αίτημα στη Αρχή Εγγραφής. Η Αρχή Εγγραφής εκδίδει τους κωδικούς πρόσβασης τους οποίους στέλνει στο email του υπαλλήλου που θα χειρίζεται την ΕΔΨΠ. Το συνθηματικό αλλάζει υποχρεωτικά μετά την πρώτη είσοδο και έχει διάρκεια ζωής ένα(1) μήνα.

Οι προϊστάμενοι των ΚΕΠ πρέπει να :

- ενημερώνουν επαρκώς τους υπαλλήλους τους για το ρόλο και τις ευθύνες τους, καθώς και για τις απαιτήσεις ασφάλειας.
- Ενημερώνουν την Αρχή Εγγραφής στο aped@mindigital.gr σε κάθε περίπτωση μεταβολής της θέσης ή της σχέσης εργασίας του προσωπικού τους (απόσπαση, συνταξιοδότηση, μετάθεση, απόλυση) προκειμένου να επανεξεταστούν όλα τα δικαιώματα εισόδου και πρόσβασης ή και να ανακληθούν όλα τα δικαιώματα εισόδου και πρόσβασης που κατείχε το προσωπικό που αποχωρεί, κατά τη στιγμή ειδοποίησης σχετικά με την (επικείμενη) αποχώρηση/τερματισμό σχέσης εργασίας.

3. Πολιτική Πρόσβασης και Κωδικοί Ασφάλειας

Κάθε χρήστης έχει προσωπικό «Αναγνωριστικό Χρήστη» (username, user ID) ώστε να αναγνωρίζεται μοναδικά κατά την είσοδό του στο Π.Σ. και την εφαρμογή της ΑΠΕΔ. Ο χρήστης είναι υπεύθυνος για την επιλογή και διαφύλαξη ασφαλούς συνθηματικού/κωδικού (password) για την πρόσβαση στο λογαριασμό του.

Απαγορεύεται η χρήση λογαριασμών πρόσβασης άλλων χρηστών για οποιοδήποτε λόγο. Σε περιπτώσεις όπου απαιτείται η χρήση λογαριασμών πρόσβασης άλλων χρηστών για λόγους επίλυσης προβλημάτων, τότε απαιτείται η παρουσία του χρήστη, καθώς και η αλλαγή του συνθηματικού πρόσβασης μετά την ολοκλήρωση των ελέγχων.

Απαγορεύεται η αποκάλυψη του συνθηματικού πρόσβασης καθώς και κάθε είδους κωδικών που συνοδεύουν συστήματα πιστοποίησης ταυτότητας (smart card/ Usb tokens & PIN αυτών) σε τρίτα πρόσωπα. Σε περίπτωση υποψίας ότι οι μυστικοί κωδικοί πρόσβασης έπαυσαν να είναι μυστικοί, τότε πρέπει να τροποποιούνται άμεσα.

Οι κωδικοί πρόσβασης χρήστη πρέπει να είναι ισχυροί (τουλάχιστον οκτώ (8) χαρακτήρων και να περιλαμβάνουν γράμματα, αριθμούς και σύμβολα). Επιπλέον, πρέπει να αλλάζουν κάθε τρεις (3) μήνες. Όσοι κωδικοί τροποποιούνται, πρέπει να διαφέρουν από τους παλαιότερους.

Ο χρήστης υποχρεούται να αλλάζει σε τακτά χρονικά διαστήματα και τους κωδικούς που συνοδεύουν συστήματα πιστοποίησης ταυτότητας .
Οι κωδικοί πρόσβασης στην εφαρμογή της ΑΠΕΔ αλλάζουν κάθε ένα (1) μήνα.

Απαγορεύεται η αναγραφή κωδικών πρόσβασης σε οποιοδήποτε μέσο ηλεκτρονικό ή/και συμβατικό (πχ χαρτί)

Απαγορεύεται η αποθήκευση κωδικών πρόσβασης σε περιηγητές διαδικτύου (browsers).

Πριν τη χορήγηση ή την επαναφορά κωδικού πρόσβασης, πρέπει να εξακριβώνεται η ταυτότητα του χρήστη. Οι μυστικοί κωδικοί πρόσβασης πρέπει να τροποποιούνται από τους χρήστες μετά τη χορήγηση τους ή την επαναφορά τους από τον αρμόδιο διαχειριστή.

Απαγορεύεται η ταυτόχρονη χρήση του ίδιου λογαριασμού χρήστη σε παραπάνω από έναν σταθμό εργασίας.

Για την πρόσβαση σε κοινόχρηστα αρχεία απαιτείται ο καθορισμός δικαιωμάτων πρόσβασης και η χρήση κωδικού πρόσβασης.

Τα συστήματα της ΑΠΕΔ παρέχουν δυνατότητα αναγνώρισης της ταυτότητας του σταθμού εργασίας από τον οποίο ο χρήστης αποκτά πρόσβαση στο σύστημα ή στην εφαρμογή.

Κάθε σταθμός εργασίας που λειτουργεί εφαρμογές της ΑΠΕΔ κλειδώνει αυτόματα μετά από περίοδο αδράνειας 15 λεπτών..

Οι φορητές συσκευές που συνδέονται μέσω κλειστού VPN πρέπει να είναι ρυθμισμένες σύμφωνα με πρότυπες ρυθμίσεις, οι οποίες εγκρίνονται από το αρμόδιο τμήμα του ΥΨηΔ.

5. Προστασία του χώρου εργασίας

Όλο το προσωπικό υποχρεούται να τηρεί το γραφείο τους σε τακτική κατάσταση, προκειμένου να τηρείται η εμπιστευτικότητα των πληροφοριών.

- Οι χρήστες πρέπει να φροντίζουν έτσι ώστε να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση τρίτων σε μέσα αποθήκευσης δεδομένων, όπως usb flash drive ή εκτυπώσεις από τις εφαρμογές, τα οποία βρίσκονται στο γραφείο τους και κυρίως, σε εμπιστευτικά έγγραφα, είτε αυτά είναι σε ηλεκτρονική μορφή, είτε σε έντυπη μορφή.
- Οι εκτυπώσεις στοιχείων που δεν φέρουν μορφή υπογεγραμμένου εγγράφου πρέπει μετά τη χρήση τους να καταστρέφονται.
- Το προσωπικό πρέπει να παίρνει άμεσα τις εκτυπώσεις από τις συσκευές εκτύπωσης, προς αποφυγή κλοπής/υπεξαίρεσής τους και διαρροής ευαίσθητων πληροφοριών.
- Οι χρήστες πρέπει να απενεργοποιούν τον Η/Υ που χειρίζονται όσο απουσιάζουν ή να αποσυνδέονται ως χρήστες από το λειτουργικό σύστημα το οποίο χρησιμοποιούν, αν η απουσία τους είναι ολιγόλεπτη.
- Κατά την απουσία τους από το χώρο εργασίας τους, είναι απαραίτητο να κλειδώνουν είτε οι χώροι στους οποίους αποθηκεύονται

έγγραφα/εξοπλισμός/μέσα αποθήκευσης (συρτάρια, ντουλάπες κ.λπ.), είτε τον ίδιο το χώρο (γραφείο).

- Η πρόσβαση πολιτών και προσωπικού τρίτων φορέων σε χώρους με πληροφοριακό εξοπλισμό (πχ ηλεκτρονικούς υπολογιστές, δικτυακό εξοπλισμό) ή αρχεία σε έντυπη μορφή, επιτρέπεται μόνο κατόπιν έγκρισης και συνοδείας προσωπικού της ΑΠΕΔ, ή αντίστοιχης διαπίστευσης

8. Προστασία από Κακόβουλο Λογισμικό

Εγκεκριμένο πρόγραμμα προστασίας από κακόβουλο λογισμικό (antivirus) ενημερώνεται από εγκεκριμένους χρήστες ανά τακτά χρονικά διαστήματα.

Οι τελικοί χρήστες πρέπει να μην αποδέχονται και να μην εκτελούν λογισμικό από μη αξιόπιστες πηγές και γενικότερα λογισμικό του οποίου η χρήση δεν έχει εγκριθεί από την αρμόδια υπηρεσία.

Απαγορεύεται η εκτέλεση ενεργειών με πρόθεση τη δημιουργία ή διανομή κακόβουλου λογισμικού στο δίκτυο της ΑΠΕΔ.

Οι τελικοί χρήστες πρέπει να ενημερώνουν άμεσα τους εγκεκριμένους χρήστες και να υποβάλλουν αίτημα στο αρμόδιο τμήμα, σε περίπτωση που διαπιστώσουν προβλήματα κατά τη λειτουργία του antivirus ή ότι βρέθηκε υπολογιστικός ιός στον ηλεκτρονικό υπολογιστή τον οποίο χειρίζονται και δεν αντιμετωπίστηκε επιτυχώς αυτόματα από το antivirus του Η/Υ.

Κάθε υπολογιστικό σύστημα το οποίο δεν είναι επαρκώς προστατευμένο σύμφωνα με την παρούσα πολιτική δεν θα έχει πρόσβαση στο δίκτυο μέχρι να συμμορφωθεί με την παρούσα πολιτική.

Σε περίπτωση μόλυνσης με κακόβουλο λογισμικό, το μολυσμένο σύστημα αποσυνδέεται άμεσα από το δίκτυο και η λειτουργία του αποκαθίσταται με την ολική διαγραφή του και εν συνεχεία με την επανεγκατάσταση του λειτουργικού συστήματος και των λοιπών λογισμικών.

11. Ασφαλής Καταστροφή Πληροφοριών

Οι πόροι στους οποίους εμπεριέχονται υπηρεσιακά δεδομένα (χαρτί, δισκέτες, σκληροί δίσκοι, οπτικοί δίσκοι, ταινίες αποθήκευσης δεδομένων, κ.λπ.), οι οποίοι είτε δεν είναι πλέον χρήσιμοι είτε απορρίπτονται λόγω βλάβης, πρέπει να καταστρέφονται με τρόπο ώστε να μην είναι δυνατή η εξαγωγή συμπεράσματος σχετικά με τα δεδομένα που ήταν αποθηκευμένα σε αυτούς.

Σε περίπτωση μέσων αποθήκευσης που δεν πρόκειται να καταστραφούν, πρέπει να πραγματοποιείται “ασφαλής διαγραφή” των δεδομένων, ώστε να καθίσταται όσο το δυνατόν δυσχερέστερη η ανάκτησή τους.

Η μέθοδος καταστροφής επιλέγεται ανάλογα με το αν εμπεριέχονται ευαίσθητα ή προσωπικά δεδομένα.

12. Πολιτική Ορθής Χρήσης Πληροφοριακών Συστημάτων

Η χρήση των υπολογιστικών συστημάτων προβλέπεται για υπηρεσιακούς λόγους.

Κάθε χρήστης υποχρεούνται να μην καταναλώνει άσκοπα πόρους των πληροφοριακών συστημάτων, να τερματίζει/αποδεσμεύει τις άδειες λογισμικού καθώς και τη θέση εργασίας του μετά το πέρας της χρήσης του, πραγματοποιώντας πλήρη έξοδο (logoff), ανάλογα με το λειτουργικό του Η/Υ.

Απαγορεύεται σε οποιοδήποτε χρήστη να διακινεί παράνομο υλικό ή λογισμικό ή να εκμεταλλεύεται με οποιοδήποτε τρόπο και να καταχράται τους υπολογιστικούς πόρους της αρμόδιας υπηρεσίας.

13. Πολιτική ορθής χρήσης διαδικτύου

Η πρόσβαση στο διαδίκτυο πραγματοποιείται μόνο για υπηρεσιακούς λόγους.

Οι χρήστες υποχρεούνται να αναφέρουν στη αρμόδια υπηρεσίας, οποιαδήποτε δραστηριότητα – διαδικτυακή υπηρεσία της ΑΠΕΔ και ενδεχομένως μπορεί να θέσει σε κίνδυνο την ασφάλεια των υπηρεσιακών δεδομένων ή είναι καθ’ οιονδήποτε τρόπο αντίθετη με την παρούσα πολιτική.

Απαγορεύεται η πρόσβαση σε δικτυακούς τόπους που φιλοξενούν περιεχόμενο, είτε παράνομο, είτε άσχετο με τα υπηρεσιακά καθήκοντα, καθώς και περιεχομένου που καταναλώνει υπερβολικού πόρους δικτύου.

Απαγορεύεται η χρήση εφαρμογών ανταλλαγής αρχείων μεταξύ ανώνυμων χρηστών (peer to peer).

Απαγορεύεται η ανάρτηση υλικού στο διαδίκτυο (π.χ. φωτογραφίες από το χώρο εργασίας ή εκπαίδευσης) που μπορεί να αποκαλύψει προσωπικά και υπηρεσιακά δεδομένα.

Απαγορεύεται η δημοσίευση υπηρεσιακών εγγράφων και δεδομένων στο Διαδίκτυο αν δεν προβλέπεται ρητά από την νομοθεσία και τους κανονισμούς που διέπει την ΑΠΕΔ.

Απαγορεύεται η αποθήκευση ή ανάρτηση υλικού από/στο διαδίκτυο, που παραβιάζει τα δικαιώματα πνευματικής ιδιοκτησίας οποιουδήποτε φορέα.

Απαγορεύεται η αποθήκευση/ανταλλαγή υπηρεσιακών αρχείων στο υπολογιστικό νέφος (Cloud Computing), όπως σε εφαρμογές drop box, Google drive, viber για την αποφυγή διαρροής πληροφοριών.

Οποιαδήποτε πλοήγηση κατά την οποία υποβάλλονται πληροφορίες (λέξεις αναζήτησης, τυπικά δεδομένα εγγραφής, κ.λπ.) από το χρήστη να γίνονται μόνο από σελίδες που λειτουργούν με χρήση πρωτοκόλλου https.

Κατά την περιήγηση στο διαδίκτυο να γίνεται προσεκτική ανάγνωση των όρων αποδοχής υπηρεσιών και να μην επιλέγεται η χρήση κάθε διαδικτυακής υπηρεσίας που μπορεί να

θέσει σε κίνδυνο τα υπηρεσιακά δεδομένα που βρίσκονται αποθηκευμένα στον υπολογιστή.

Να προτιμάται η «Ανώνυμη Περιήγηση» που διαθέτουν οι browsers, αποφεύγοντας έτσι την αποθήκευση των cookies και του ιστορικού περιήγησης κάθε χρήστη.

Η αρμόδια υπηρεσία καθορίζει τη διαδικασία πρόσβασης στο διαδίκτυο και της απόδοσης δικαιωμάτων στους τελικούς χρήστες και τους τερματικούς Η/Υ.

Να καλύπτεται ή να αφαιρείται η χρήση της βιντεοκάμερας (webcam) από τον ηλεκτρονικό υπολογιστή, όταν δεν συντρέχει υπηρεσιακός λόγος (απομακρυσμένη παρουσίαση, σεμινάριο κ.λπ.)

Εξαιρέσεις επιτρέπονται μόνο κατόπιν έγκρισης, λόγω αιτιολογημένων υπηρεσιακών αναγκών.

15. Εκπαίδευση Χρηστών

Η ενημέρωση όλων των τελικών χρηστών, αλλά και των διαχειριστών και της διοίκησης είναι απαραίτητη για την προστασία από πληθώρα επιθέσεων όπως:
κακόβουλο λογισμικό, Social engineering, Phishing/ Spearphishing μέσω email, τηλεφώνου κ.λ.π.

Το προσωπικό λαμβάνει εκπαιδεύσεις, καθώς και ενημερωτικό υλικό από τη αρμόδια υπηρεσία (π.χ. μέσω αποστολής εγγράφων ενημερωτικού χαρακτήρα, αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου) όποτε κρίνεται απαραίτητο (π.χ. στις περιπτώσεις ανάπτυξης νέων πληροφοριακών συστημάτων, σημαντικής μεταβολής σε υπάρχον πληροφοριακό σύστημα ή εφαρμογή, σημαντικές εξελίξεις στον τομέα της Πληροφορικής ή στο Νομοθετικό Πλαίσιο).

17. Προστασία Προσωπικών Δεδομένων

Ως προσωπικό δεδομένο θεωρείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο (έμμεσα ή άμεσα) φυσικό πρόσωπο (υποκείμενο των δεδομένων), συμπεριλαμβανομένων των κατηγοριών που χρήζουν μεγαλύτερης προστασίας, όπως τα γενετικά και βιομετρικά δεδομένα.

Κάθε χρήστης των πληροφοριακών συστημάτων της ΑΠΕΔ οφείλει να επεξεργάζεται τα απολύτως απαραίτητα προσωπικά δεδομένα για το σκοπό που έχει οριστεί στο πλαίσιο των υπηρεσιακών του καθηκόντων. Οποιαδήποτε άλλη αποθήκευση η πρόσβαση σε προσωπικά δεδομένα απαγορεύεται.

Όταν ο χρήστης πρόκειται να αποθηκεύσει ή να επεξεργαστεί προσωπικά δεδομένα πολιτών, και εάν δεν υπάρχει άλλη νομιμοποιητική βάση για την επεξεργασία των δεδομένων οφείλει να λάβει ρητή συγκατάθεση τους, πριν την έναρξη της επεξεργασίας.

Το υποκείμενο των δεδομένων έχει δικαίωμα στη διαφανή ενημέρωση για την επεξεργασία των δεδομένων του, στην πρόσβαση, διόρθωση, διαγραφή, περιορισμό της επεξεργασίας, στην εναντίωση στην επεξεργασία και στην ανθρώπινη παρέμβαση σχετικά με την αυτοματοποιημένη λήψη αποφάσεων, κατάρτιση προφίλ κτλ. Προς τούτο

μπορεί να υποβάλει γραπτό αίτημα προς την ΑΠΕΔ. Το αίτημα, αξιολογείται και ικανοποιείται κατάλληλα με απάντηση εντός 30 ημερολογιακών ημερών.

Ως περιστατικό παραβίασης προσωπικών δεδομένων νοείται κάθε συμβάν στο οποίο πραγματοποιείται τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Σε περίπτωση υποψίας τέτοιου περιστατικού κάθε υπάλληλος υποχρεούνται να ενημερώσει την αρμόδια υπηρεσία.

Σημειώνεται ότι υφίσταται νομική υποχρέωση της ΑΠΕΔ να ενημερώσει την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και το υποκείμενο των δεδομένων (μέσω του Υπεύθυνου Προστασίας Δεδομένων), σε περιστατικά παραβίασης προσωπικών δεδομένων.

18. Πειθαρχικές Κυρώσεις

Όλοι οι χρήστες έχουν την υποχρέωση και την ευθύνη να είναι ενήμεροι για τις νομικές ή κανονιστικές απαιτήσεις που αφορούν στα καθημερινά τους καθήκοντα σε θέματα ασφάλειας πληροφοριών και προστασίας προσωπικών δεδομένων. Σε περιπτώσεις παράνομων ενεργειών οι χρήστες είναι αποκλειστικά υπεύθυνοι, π.χ. για τη χρήση παράνομου λογισμικού που θα βρεθεί στους υπολογιστές τους ή στην κατοχή τους και θα ελέγχονται πειθαρχικά, εκτός της ενδεχόμενης ποινικής δίωξης.

Η μη εφαρμογή της παρούσας πολιτικής, αλλά και κάθε μη εξουσιοδοτημένη χρήση/κοινοποίηση δεδομένων προσωπικού χαρακτήρα υπόκειται σε πειθαρχικές και ενδεχομένως ποινικές κυρώσεις.

19. Ελεγκτικό Πλάνο (Εσωτερικός Ελεγκτής - Internal Auditor, Υπεύθυνος Ασφαλείας - Security Officer, Υπεύθυνος Συμμόρφωσης - Compliance Officer)

Ο Εσωτερικός Ελεγκτής (Internal Auditor) είναι υπεύθυνος για την παρακολούθηση ανά τακτά διαστήματα της ορθής λειτουργίας της υπηρεσίας. Τρόπος παρακολούθησης:

- Έλεγχος επί τόπου στα γραφεία της Αρχή Εγγραφής και Εντεταλμένα Γραφεία
- Επεξεργασία ερωτηματολογίων – εισήγηση για εγκυκλίους στα Εντεταλμένα Γραφεία

Ο Υπεύθυνος Ασφάλειας (Security Officer) φροντίζει για την εφαρμογή της Πολιτικής Ασφάλειας με τους παρακάτω τρόπους:

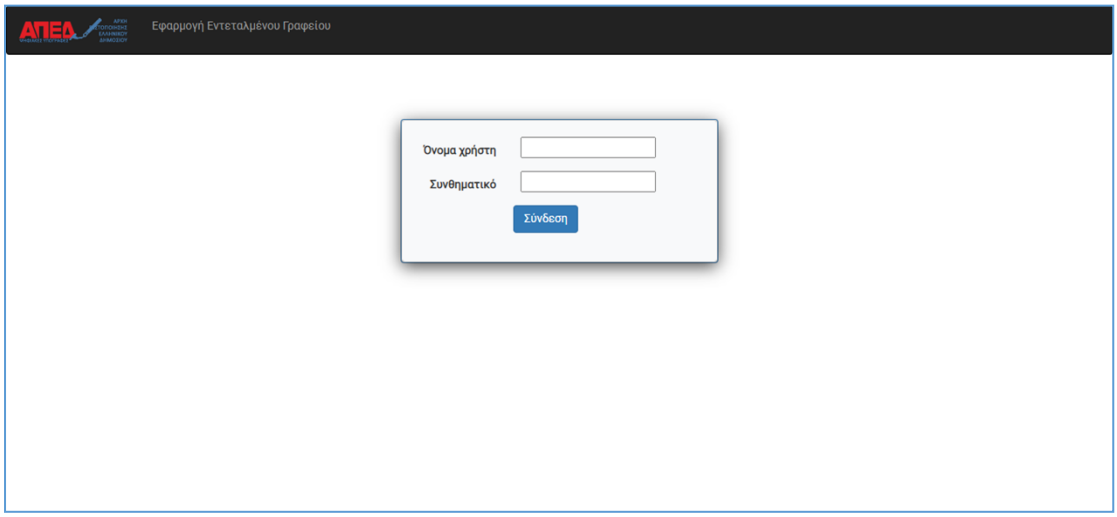
- Έλεγχος σε χώρους της ΑΠΕΔ- Αρχή Εγγραφής - Εντεταλμένα Γραφεία (φυσικούς χώρους, Υπολογιστικά Συστήματα σε συνεργασία με τα τμήματα Πληροφορικής)
- Αποστολή ερωτηματολογίων - εισήγηση για εγκύκλιους στα Εντεταλμένα Γραφεία.
- Εποπτεύει και ελέγχει την τήρησης της Πολιτικής Ασφάλειας και την εφαρμογή των προβλεπόμενων μέτρων.
- Υποδέχεται, καταγράφει και ερευνά Περιστατικά Ασφαλείας.

Παράρτημα Β

Εγχειρίδιο Χρήσης Εφαρμογής Διαχείρισης Ψηφιακού Πιστοποιητικού

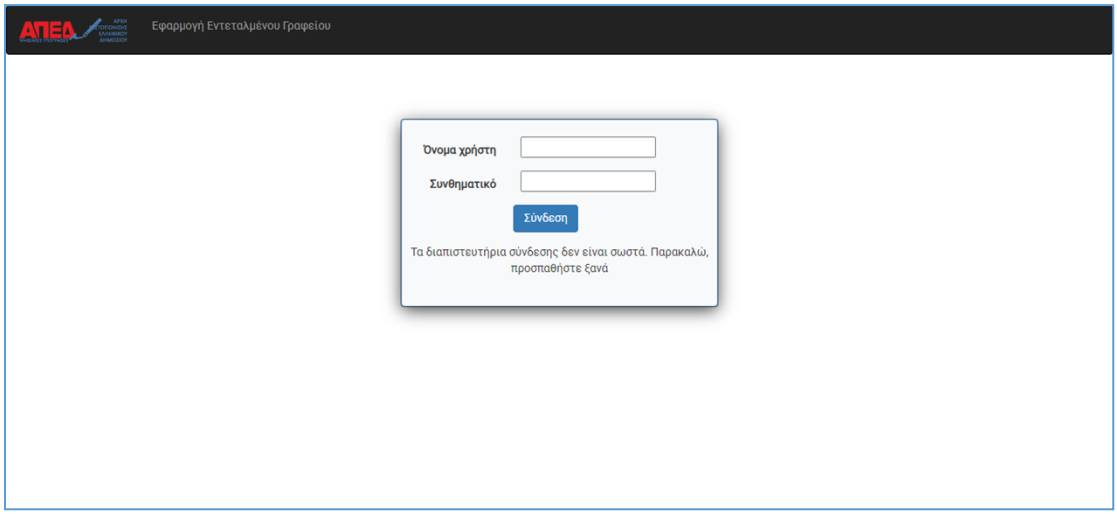
Σύνδεση στην εφαρμογή

Για να συνδεθεί ο χρήστης στην εφαρμογή, θα πρέπει να πληκτρολογήσει την ηλεκτρονική διεύθυνση **https://www.ermis.gov.gr/apedkep/**. Ακολούθως, θα πρέπει να συμπληρώσει τα διαπιστευτήρια σύνδεσης (όνομα χρήστη, συνθηματικό) που έχει για την εφαρμογή ekep-ermis ώστε να συνδεθεί επιτυχώς (Εικόνα 1).



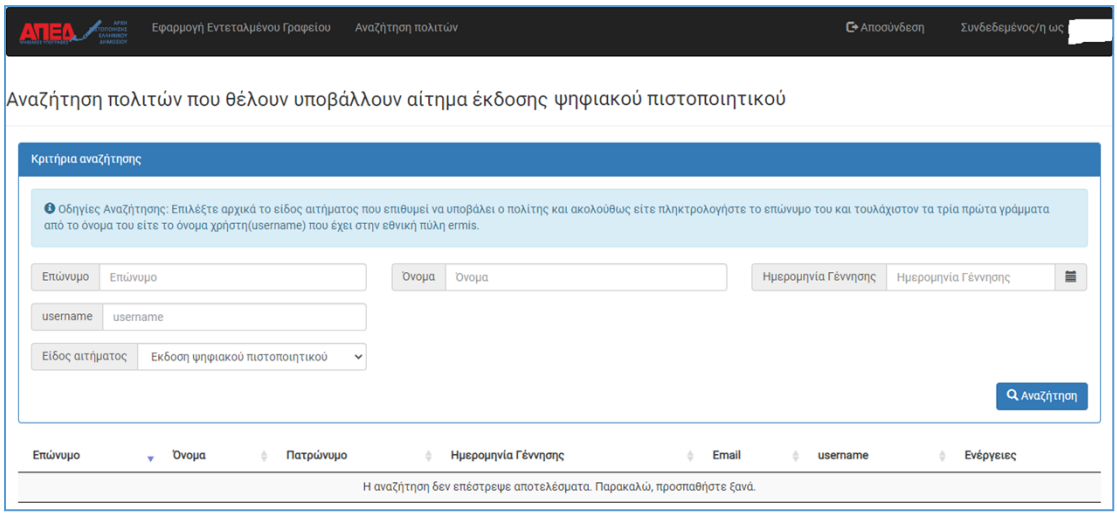
Εικόνα 1 - Οθόνη σύνδεσης στην εφαρμογή Εντεταλμένου Γραφείου

Σε περίπτωση αποτυχημένης σύνδεσης, στην οθόνη του χρήστη εμφανίζεται σχετικό μήνυμα (Εικόνα 2).



Εικόνα 2 – Ανεπιτυχής προσπάθεια σύνδεσης

Σε περίπτωση επιτυχημένης σύνδεσης στην εφαρμογή, στην οθόνη του χρήστη εμφανίζεται η αρχική οθόνη της εφαρμογής η οποία είναι η οθόνη αναζήτησης πολιτών.



Εικόνα 3 – Επιτυχής προσπάθεια σύνδεσης στην εφαρμογή

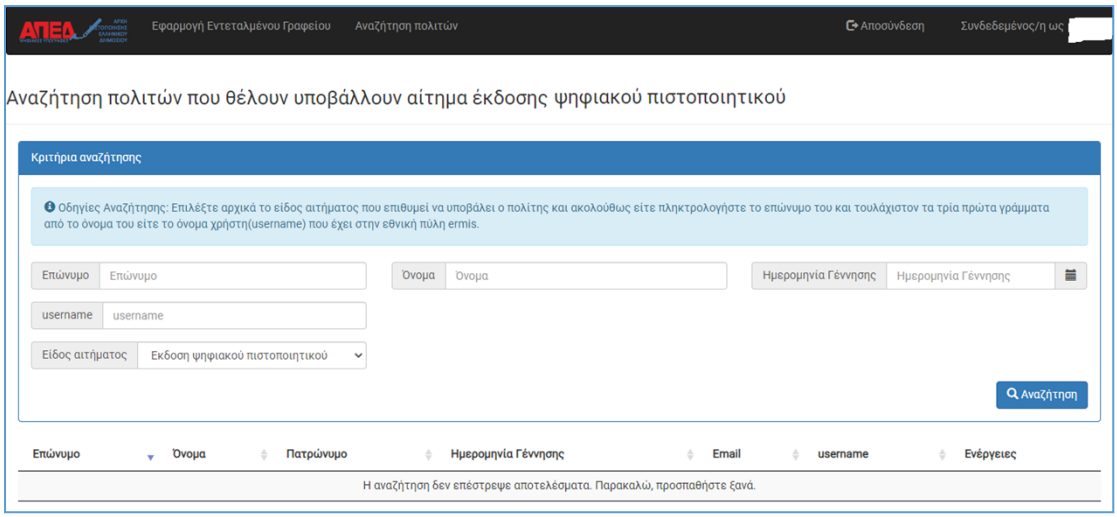
Αναζήτηση αιτήματος έκδοσης ψηφιακού πιστοποιητικού

Με την βοήθεια της οθόνης αναζήτησης αιτήματος έκδοσης ψηφιακού πιστοποιητικού, ο χρήστης της εφαρμογής έχει την δυνατότητα να εντοπίσει το αίτημα που έχει υποβάλει ο πολίτης που έχει προσέλθει στο ΚΕΠ και να εκκινήσει την διαδικασία φυσικής ταυτοποίησης του (εικόνα 4). Πιο συγκεκριμένα, ο χρήστης έχει την δυνατότητα να αναζητήσει το αίτημα του πολίτη με έναν από του ακόλουθους δύο τρόπους :

- **Αναζήτηση βάσει Επωνύμου, Ονόματος, Ημερομηνίας Γέννησης:** Σε αυτή την περίπτωση, ο χρήστης θα πρέπει κατ' ελάχιστον να συμπληρώσει ολόκληρο το επώνυμο του πολίτη και τα τρία πρώτα γράμματα του ονόματος.

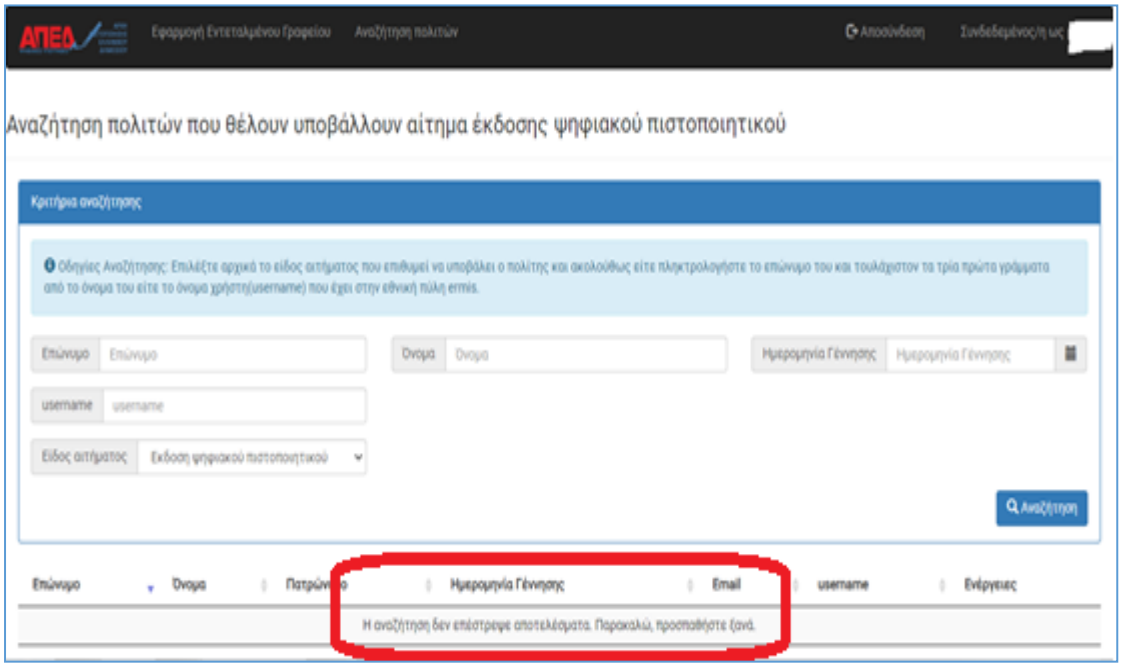
- **Αναζήτηση βάσει του username που έχει ο πολίτης στην Εθνική Πύλη Ermis**: Σε αυτή την περίπτωση, ο χρήστης θα πρέπει να συμπληρώσει ολόκληρο το username του πολίτη.

Μόλις ο χρήστης συμπληρώσει το επιθυμητό κριτήριο αναζήτησης, πρέπει να πατήσει το κουμπί «Αναζήτηση» για να εκτελεσθεί η αναζήτηση.



Εικόνα 4 – Οθόνη αναζήτησης αιτήματος έκδοσης ψηφιακού πιστοποιητικού

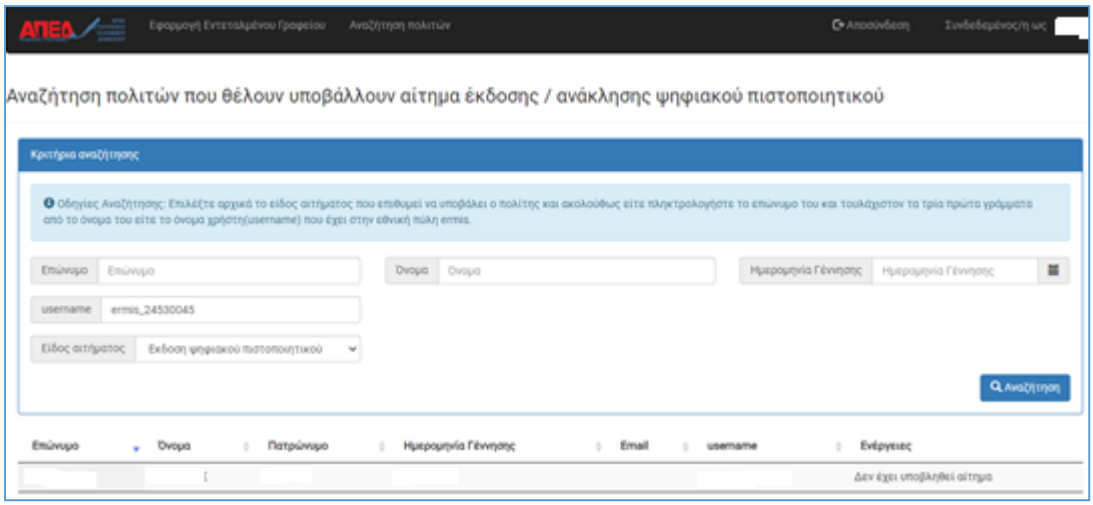
Σε περίπτωση που η αναζήτηση δεν επιστρέψει κάποιο αποτέλεσμα, στον πίνακα των αποτελεσμάτων εμφανίζεται το ακόλουθο μήνυμα (εικόνα 5) : «Η αναζήτηση δεν επέστρεψε αποτέλεσμα. Παρακαλώ, προσπαθήστε ξανά».



Εικόνα 5 – Αποτελέσματα αναζήτησης αιτήματος έκδοσης ψηφ. πιστοποιητικού (Δεν βρέθηκαν αποτελέσματα)

Σε περίπτωση που η αναζήτηση επιστρέψει αποτελέσματα, στον πίνακα των αποτελεσμάτων εμφανίζεται μία εγγραφή για κάθε πολίτη που ικανοποιεί τα κριτήρια αναζήτησης (εικόνα 6). Πιο συγκεκριμένα, για κάθε πολίτη εμφανίζεται η ακόλουθη πληροφορία :

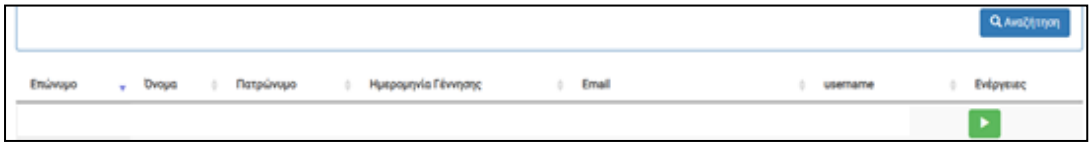
- Επώνυμο
- Όνομα
- Πατρώνυμο
- Ημερομηνία Γέννησης
- E-mail
- Username
- Ενέργειες



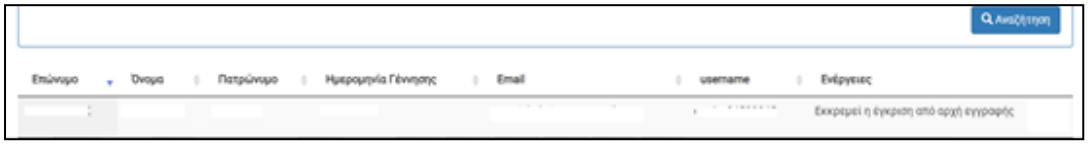
Εικόνα 6 – Αποτελέσματα αναζήτησης αιτήματος έκδοσης ψηφ. πιστοποιητικού (Βρέθηκαν αποτελέσματα)

Το πεδίο «Ενέργειες» είναι αυτό που υποδεικνύει στο χρήστη της εφαρμογής σε ποιο στάδιο είναι το αίτημα έκδοσης ψηφιακού πιστοποιητικού του πολίτη. Οι τιμές που μπορεί να λάβει το πεδίο αυτό είναι οι ακόλουθες :

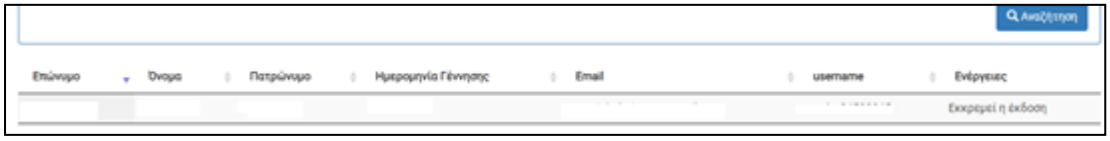
- **Δεν έχει υποβληθεί αίτημα** (εικόνα 6) : Ο πολίτης δεν έχει υποβάλει αίτημα έκδοσης ψηφιακού πιστοποιητικού μέσω της διαδικτυακής εφαρμογής.
- **Εκκίνηση της διαδικασία υποβολής αιτήματος** (εικόνα 7) : Ο πολίτης έχει υποβάλει αίτημα έκδοσης ψηφιακού πιστοποιητικού μέσω της διαδικτυακής εφαρμογής. Ο χρήστης της εφαρμογής εκκινεί την διαδικασία φυσικής ταυτοποίησης του πολίτη πατώντας το «πράσινο κουμπί».
- **Εκκρεμεί έγκριση από Αρχή Εγγραφής** (εικόνα 8): Ο πολίτης έχει ολοκληρώσει τη διαδικασία φυσικής ταυτοποίησης. Το αίτημα του βρίσκεται προς εξέταση από την Αρχή Εγγραφής.
- **Εκκρεμεί η έκδοση** (εικόνα 9) : Το αίτημα του πολίτη έχει εγκριθεί από την αρχή εγγραφής και μπορεί να προχωρήσει στην έκδοση του ψηφιακού πιστοποιητικού.
- **Έγκυρο** (εικόνα 10) : Ο πολίτης έχει ολοκληρώσει επιτυχώς την έκδοση του ψηφιακού πιστοποιητικού.
- **Έγκυρο, εκκρεμεί αίτημα ανάκλησης** (εικόνα 11) : Ο πολίτης έχει υποβάλει αίτημα ανάκλησης του εν ισχύ ψηφιακού πιστοποιητικού του.



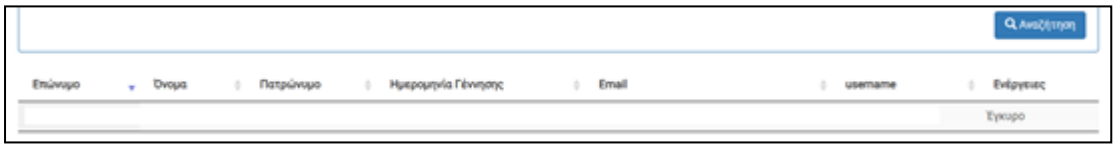
Εικόνα 7 – Αποτελέσματα αναζήτησης (Εκκίνηση της διαδικασία υποβολής αιτήματος)



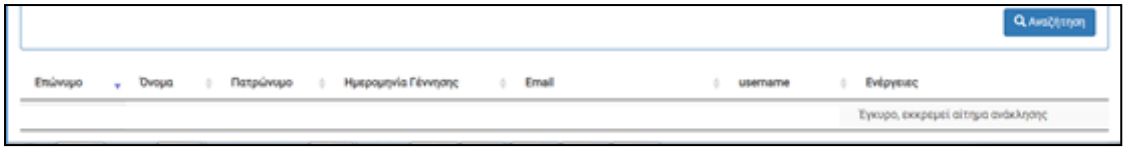
Εικόνα 8 – Αποτελέσματα αναζήτησης (Εκκρεμεί έγκριση από Αρχή Εγγραφής)



Εικόνα 9 – Αποτελέσματα αναζήτησης (Εκκρεμεί η έκδοση)



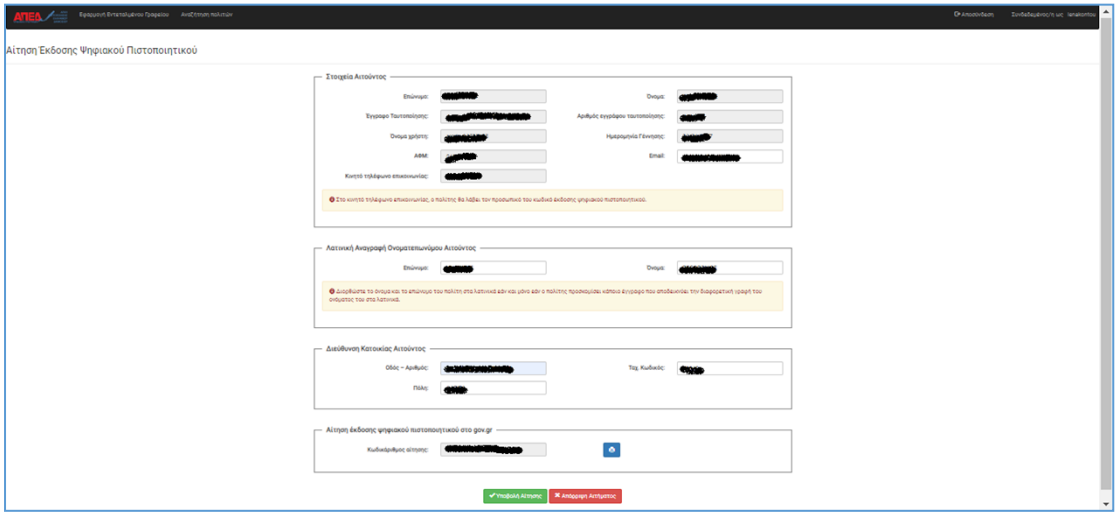
Εικόνα 10 – Αποτελέσματα αναζήτησης (Έγκυρο)



Εικόνα 11 – Αποτελέσματα αναζήτησης (Έγκυρο, εκκρεμεί αίτημα ανάκλησης)

Υποβολή Αιτήματος Έκδοσης Ψηφιακού Πιστοποιητικού

Μόλις ο χρήστης εκκινήσει την υποβολή αιτήματος έκδοσης ψηφιακού πιστοποιητικού, θα εμφανιστεί στην οθόνη του η ηλεκτρονική φόρμα υποβολής αιτήματος (εικόνα 12).



Εικόνα 12 – Ηλεκτρονική φόρμα υποβολής αιτήματος

Η ηλεκτρονική φόρμα υποβολής αιτήματος έκδοσης ψηφιακού πιστοποιητικού αποτελείται από τα ακόλουθα μέρη :

- **Στοιχεία Αιτούντος**

    - **Επώνυμο** : Το πεδίο αυτό είναι προ συμπληρωμένο βάσει των στοιχείων που περιέχονται στο μητρώο της ΑΑΔΕ για τον συγκεκριμένο πολίτη. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

    - **Όνομα**: Το πεδίο αυτό είναι προ συμπληρωμένο βάσει των στοιχείων που περιέχονται στο μητρώο της ΑΑΔΕ για τον συγκεκριμένο πολίτη. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

    - **Έγγραφο Ταυτοποίησης:** Το πεδίο αυτό είναι προ συμπληρωμένο βάσει των στοιχείων που περιέχονται στην υπεύθυνη δήλωση που υπέβαλλε ο πολίτης στο gov.gr. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Αριθμός εγγράφου ταυτοποίησης:** Το πεδίο αυτό είναι προ συμπληρωμένο βάσει των στοιχείων που περιέχονται στην υπεύθυνη δήλωση που υπέβαλλε ο πολίτης στο gov.gr. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Όνομα χρήστη**: Το πεδίο αυτό είναι προ συμπληρωμένο και περιέχει το username του χρήστη στην εθνική πύλη ermis. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Ημερομηνία Γέννησης:** Το πεδίο αυτό είναι προ συμπληρωμένο βάσει των στοιχείων που περιέχονται στο μητρώο της ΑΑΔΕ για τον συγκεκριμένο πολίτη. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **ΑΦΜ:** Το πεδίο αυτό είναι προ συμπληρωμένο βάσει των στοιχείων που περιέχονται στο μητρώο της ΑΑΔΕ για τον συγκεκριμένο πολίτη. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Email:** Το πεδίο αυτό είναι προ συμπληρωμένο και περιέχει το email του χρήστη στην εθνική πύλη ermis. Το πεδίο **μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Κινητό τηλέφωνο επικοινωνίας :** Το πεδίο αυτό είναι προ συμπληρωμένο βάσει των στοιχείων που περιέχονται στην υπεύθυνη δήλωση που υπέβαλλε ο πολίτης στο gov.gr. Το πεδίο **δεν μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Λατινική Αναγραφή Ονοματεπωνύμου Αιτούντος :**

  - **Επώνυμο :** Το πεδίο αυτό είναι προ συμπληρωμένο με την λατινική αναγραφή του επώνυμου του πολίτη όπως προκύπτει από την χρήση του προτύπου ΕΛΟΤ-743. Το πεδίο **μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής εάν και μόνο εάν ο πολίτης προσκομίσει σχετικό έγγραφο που αποδεικνύει την διαφορετική γραφή του επωνύμου του στα λατινικά.

  - **Όνομα :** Το πεδίο αυτό είναι προ συμπληρωμένο με την λατινική αναγραφή του ονόματος του πολίτη όπως προκύπτει από την χρήση του προτύπου ΕΛΟΤ-743. Το πεδίο **μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής εάν και μόνο εάν ο πολίτης προσκομίσει σχετικό έγγραφο που αποδεικνύει την διαφορετική γραφή του ονόματός του στα λατινικά.

- **Διεύθυνση Κατοικίας Αιτούντος** :

  - **Οδός – Αριθμός :** Το πεδίο αυτό είναι προ συμπληρωμένο και περιέχει την διεύθυνση κατοικίας του χρήστη στην εθνική πύλη ermis. Το πεδίο **μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Ταχ. Κωδικός :** Το πεδίο αυτό είναι προ συμπληρωμένο και περιέχει τον ταχυδρομικό κωδικό κατοικίας του χρήστη στην εθνική πύλη ermis. Το πεδίο **μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

- **Πόλη :** Το πεδίο αυτό είναι προ συμπληρωμένο και περιέχει την πόλη κατοικίας του χρήστη στην εθνική πύλη ermis. Το πεδίο **μπορεί** να τροποποιηθεί από τον χρήστη της εφαρμογής.

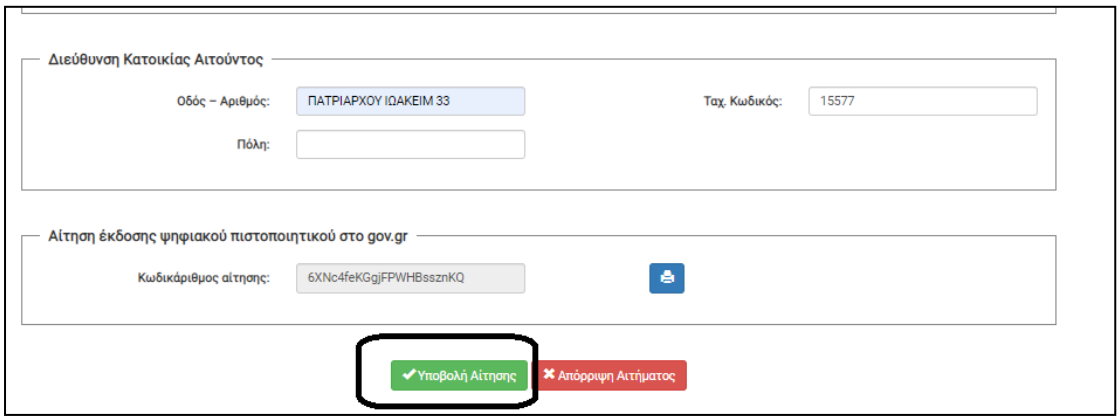
- **Αίτηση έκδοσης ψηφιακού πιστοποιητικού στο gov.gr :**

  - **Κωδικάριθμος αίτησης:** Το πεδίο αυτό είναι προ συμπληρωμένο και περιέχει τον κωδικάριθμο της υπεύθυνης δήλωσης που υπέβαλε ο πολίτης. Το πεδίο δε **μπορεί** να τροποποιηθεί από το χρήστη της εφαρμογής.

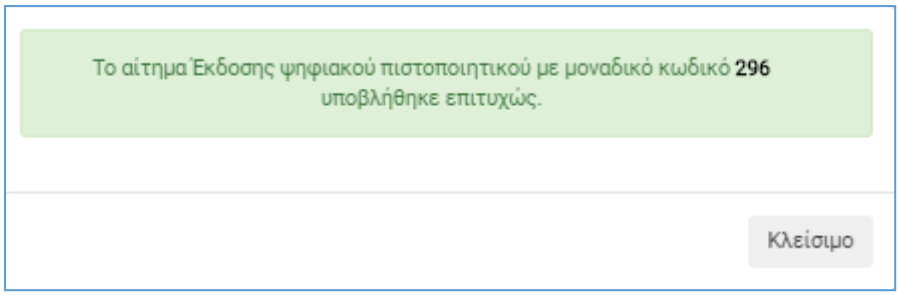
Ο χρήστης της εφαρμογής πρέπει να συμπληρώσει όλα τα πεδία και πριν υποβάλει την αίτηση θα πρέπει να κάνει τους ακόλουθους ελέγχους.

- Πατάει το κουμπί δίπλα στον κωδικάριθμο στην «Αίτηση έκδοσης πιστοποιητικού στο gov.gr»
- Επιβεβαιώνει την ορθότητα των στοιχείων της αίτησης του gov.gr, συγκρίνοντάς τα με το ταυτοποιητικό έγγραφο που επιδεικνύει ο πολίτης. Το ταυτοποιητικό έγγραφο πρέπει να είναι το ίδιο με αυτό που εμφανίζεται στην αίτηση gov.gr. Αν δεν είναι, η αίτηση ακυρώνεται
- Κάνει αντιπαραβολή ανάμεσα στα στοιχεία της αίτησης στην ΑΠΕΔ, εικ 12 (Επώνυμο, Όνομα, Πατρώνυμο, Μητρώνυμο, ΑΦΜ) και τα αντίστοιχα στην αίτηση gov.gr

Σε περίπτωση που ο χρήστης της εφαρμογής ολοκληρώσει επιτυχώς τους ανωτέρω ελέγχους θα πρέπει να πατήσει το κουμπί «Υποβολή Αίτησης» (εικόνα 13). Στην οθόνη του θα εμφανιστεί μήνυμα το οποίο τον βεβαιώνει ότι το αίτημα υποβλήθηκε επιτυχώς (εικόνα 14). Ο πολίτης λαμβάνει sms που τον ενημερώνει για την επιτυχή ολοκλήρωση της φυσικής ταυτοποίησης.

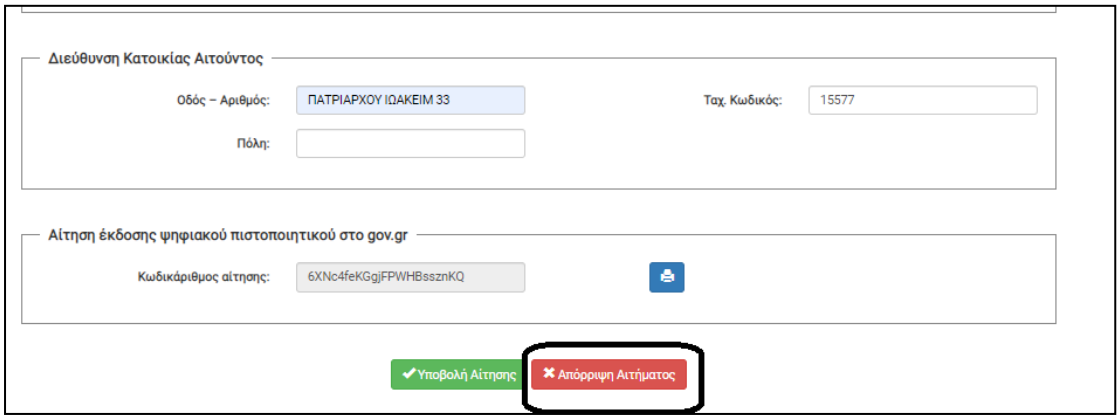


Εικόνα 13 – Κουμπί «Υποβολή Αίτησης»



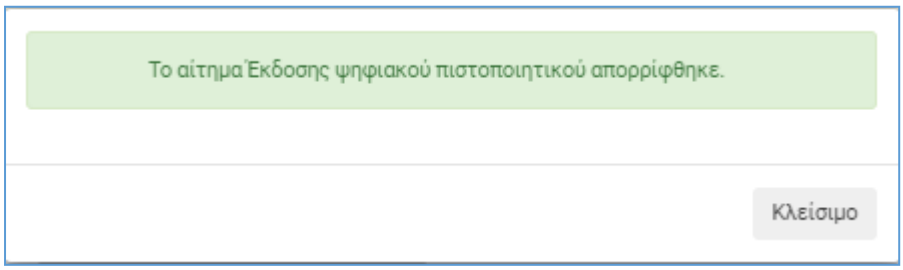
Εικόνα 14 – Επιτυχής υποβολή αιτήματος έκδοσης ψηφιακού πιστοποιητικού

Σε περίπτωση που ο χρήστης της εφαρμογής δεν ολοκληρώσει επιτυχώς τους ανωτέρω ελέγχους θα πρέπει να πατήσει το κουμπί «Απόρριψη Αιτήματος» (εικόνα 15). Ακολούθως, θα του ζητηθεί να καταχωρήσει τον λόγο απόρριψης του αιτήματος (εικόνα 16). Μόλις συμπληρώσει τον λόγο απόρριψης της αίτησης θα πρέπει να πατήσει το κουμπί «Απόρριψη» (εικόνα 16) και θα δει στην οθόνη του (εικάνα17) επιβεβαιωτικό μήνυμα αναφορικά με την οριστική απόρριψη του αιτήματος.



Εικόνα 15 – Κουμπί «Απόρριψη Αιτήματος»

Εικόνα 16 – Αιτιολόγηση απόρριψης αιτήματος



Εικόνα 17 – Επιβεβαίωση απόρριψης αιτήματος έκδοσης ψηφιακού πιστοποιητικού

Παράρτημα Γ

Διαδικασία Αίτησης- Ταυτοποίησης- Έκδοσης- Ανάκλησης Ψηφιακού Πιστοποιητικού

Αίτηση Έκδοσης Ψηφιακού Πιστοποιητικού

- Ο πολίτης μεταβαίνει στο gov.gr στην αίτηση – υπεύθυνη δήλωση για έκδοση ΨΠ και τη δημιουργεί.
    - Η αίτηση στο gov.gr έχει τυποποιημένο κείμενο. Ο χρήστης την επιλέγει, αυθεντικοποιείται, συμπληρώνει τα πεδία ταυτοποίησης και την δημιουργεί. Στην αίτηση περιλαμβάνονται επιπλέον ενότητες (κείμενο μόνο): ενημέρωση για επεξεργασία δεδομένων προσωπικού χαρακτήρα, και ορισμένοι βασικοί όροι χρήσης και παραπομπή στο κείμενο των όρων χρήσης.
- Ο πολίτης υποβάλλει το αίτημα στο portal της ΑΠΕΔ.
    - Συνδέεται στο portal https://www.ermis.gov.gr/apedcitizen/login με τα διαπιστευτήρια του Taxis net.
    - Υποβάλλει αίτημα έκδοσης ΨΠ.
        - Τα βασικά πεδία είναι προσυμπληρωμένα (ανάκτηση από το web service της ΑΑΔΕ).
        - Συμπληρώνει προαιρετικά στοιχεία επικοινωνίας: email, διεύθυνση κατοικίας.
        - Συμπληρώνει τον κωδικάριθμο της αίτησης.
        - Επιλέγει υποβολή του αιτήματος.
        - Γίνεται αυτόματα έλεγχος στα βασικά πεδία (όνομα, επώνυμο, ΑΦΜ) ανάμεσα σε ανακτηθέντα στοιχεία ΑΑΔΕ και αίτηση gov.gr.
        - Τα στοιχεία εμφανίζονται στον πολίτη και καλείται να επιβεβαιώσει (τσεκάρει) ότι έχει διαβάσει τους όρους χρήσης.
        - Υποβάλλει την ηλεκτρονική αίτηση («αίτημα στο portal της ΑΠΕΔ»). Η αίτηση gov.gr αποθηκεύεται στη βάση δεδομένων.
- Ο πολίτης μεταβαίνει σε οποιοδήποτε ΚΕΠ (Εντεταλμένο Γραφείο) για να γίνει η φυσική ταυτοποίηση.
    - Ο υπάλληλος ΚΕΠ συνδέεται στο portal της ΑΠΕΔ, αναζητά και εντοπίζει τον πολίτη. Μεταφέρεται στη σελίδα με τα στοιχεία της αίτησης. Από εκεί θα μπορεί να δει την αίτηση gov.gr.
    - Ο υπάλληλος ΚΕΠ ταυτοποιεί τον πολίτη και επιβεβαιώνει την ορθότητα των στοιχείων της αίτησης του gov.gr.
    - Ο υπάλληλος ΚΕΠ κάνει και αντιπαραβολή ανάμεσα στα ανακτηθέντα στοιχεία από το μητρώο του Taxis (όνομα, επώνυμο, ΑΦΜ) και στα αντίστοιχα στην αίτηση του gov.gr. Αν δεν υπάρχει ταύτιση ακυρώνεται το αίτημα.
    - Ο υπάλληλος διορθώνει, αν απαιτείται, τα πεδία που μπορεί να επεξεργαστεί (ονοματεπώνυμο (λατινικά), διεύθυνση, email).
    - Το αναγνωριστικό του ταυτοποιητικού εγγράφου (ταυτότητα ή διαβατήριο) εισάγεται αυτόματα από την αίτηση gov.gr. Το ταυτοποιητικό έγγραφο

πρέπει να είναι το ίδιο με αυτό που έχει εισάγει στην αίτηση gov.gr ο πολίτης και είναι είτε ταυτότητα (αστυνομική ή στρατιωτική), είτε διαβατήριο.
    - Η αίτηση για ΨΠ έχει ένα μοναδικό αναγνωριστικό (αντίστοιχο του αριθμού πρωτοκόλλου) το οποίο και εμφανίζεται στον υπάλληλο ΚΕΠ. Δεν τυπώνεται η αίτηση για ΨΠ και αποδεικτικό παραλαβής.
    - Ο υπάλληλος του ΚΕΠ ολοκληρώνει την ταυτοποίηση και καταχώρηση του αιτήματος («Ολοκλήρωση ενεργειών»). Αυτόματα αποστέλλεται sms στο κινητό του πολίτη που ενημερώνει ότι ολοκληρώθηκε επιτυχώς η φυσική ταυτοποίηση.
    - Στο portal, στην οθόνη διαχείρισης ΨΠ του πολίτη, αναγράφεται ότι έχει γίνει η ταυτοποίηση από Εντεταλμένο Γραφείο καθώς και ο μοναδικός αναγνωριστικός αριθμός.
- Το αίτημα εγκρίνεται από την Αρχή Εγγραφής.
    - Το στέλεχος της ΑΕ πλοηγείται στην οθόνη «Αιτήματα Έκδοσης ΨΠ» και επιλέγει το αίτημα.
    - Ελέγχει τα στοιχεία της αίτησης του portal καθώς και την αίτηση gov.gr. Εφόσον διαπιστώσει ότι όλα είναι σωστά, εγκρίνει το αίτημα.
      Αν διαπιστώσει παρατυπία απορρίπτει το αίτημα και ο πολίτης ενημερώνεται με sms. Στο portal ο πολίτης βλέπει την αιτιολογία απόρριψης, και ενημερώνεται για τις διορθωτικές ενέργειες που πρέπει να κάνει προκειμένου να υποβάλλει εκ νέου το αίτημα.
    - Ο πολίτης ενημερώνεται με sms στο κινητό του ότι εγκρίθηκε το αίτημα. Το μήνυμα περιέχει τον οκταψήφιο κωδικό έκδοσης/ανάκλησης.
- Ο πολίτης ακολουθώντας τις οδηγίες προχωρά σε έκδοση του ψηφιακού πιστοποιητικού.

<u>Ανάκληση Ψηφιακού Πιστοποιητικού</u>

- Ανάκληση με οκταψήφιο κωδικό
    - Στην περίπτωση αυτή ο ίδιος ο πολίτης κάνει την ανάκληση του πιστοποιητικού του χωρίς παρέμβαση / εμπλοκή της Αρχής Εγγραφής.
    - Ο πολίτης συνδέεται στο portal της ΑΠΕΔ και επιλέγει την ανάκληση του πιστοποιητικού του. Πρέπει να εισάγει τον μοναδικό οκταψήφιο κωδικό που δημιουργήθηκε όταν εγκρίθηκε το αίτημα έκδοσης και του είχε αποσταλεί με sms στο κινητό του. Με την εισαγωγή του κωδικού και την υποβολή αιτήματος το πιστοποιητικό ακυρώνεται αυτόματα.
    - Αν ο πολίτης δεν έχει αποθηκεύσει τον οκταψήφιο κωδικό, μπορεί να γίνει υπενθύμιση. Στην περίπτωση αυτή εισάγει τον ΑΦΜ και την ημερομηνία γέννησης του και εφόσον αυτά τα στοιχεία επαληθευτούν, αποστέλλεται sms με τον κωδικό στο κινητό τηλέφωνο που καταχωρήθηκε στην έκδοση του πιστοποιητικού. Αν έχει αλλάξει αριθμό κινητού, δεν μπορεί να γίνει τροποποίηση του καταχωρημένου κινητού και δεν μπορεί να λάβει τον κωδικό υπενθύμισης.

- Ανάκληση με αίτηση στο gov.gr

- Η επιλογή αυτή χρησιμοποιείται αν ο πολίτης δεν έχει τον οκταψήφιο κωδικό και δεν μπορεί να γίνει υπενθύμιση επειδή έχει αλλάξει αριθμό κινητού.
- Ο πολίτης πλοηγείται στο gov.gr, εντοπίζει την αίτηση ανάκλησης και την δημιουργεί.
- Ο πολίτης συνδέεται στο portal της ΑΠΕΔ και επιλέγει να προχωρήσει στην ανάκληση εισάγοντας τον κωδικάριθμο της αίτησης – υπεύθυνης δήλωσης που δημιούργησε στο gov.gr.
- Με την υποβολή του αιτήματος γίνεται αυτόματα έλεγχος στα βασικά πεδία (ΑΦΜ, όνομα, επώνυμο) και το αίτημα δρομολογείται στην Αρχή Εγγραφής. Η αίτηση του gov.gr καταχωρείται στη βάση δεδομένων.
- Η Αρχή Εγγραφής ελέγχει το αίτημα και προχωρά στην ανάκληση του ψηφιακού πιστοποιητικού.
- Ο πολίτης ενημερώνεται με sms για την ανάκληση.

Παράρτημα Δ

Δήλωση Αποδοχής Πολιτικής Ασφάλειας

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

(άρθρο 8 Ν.1599/1986)

Η ακρίβεια των στοιχείων που υποβάλλονται με αυτή τη δήλωση μπορεί να ελεγχθεί με βάση το αρχείο άλλων υπηρεσιών (άρθρο 8 παρ. 4 Ν. 1599/1986)

ΠΡΟΣ(1):	**ΑΠΕΔ**		
Ο – Η Όνομα:		Επώνυμο:	
Όνομα και Επώνυμο Πατέρα:			
Όνομα και Επώνυμο Μητέρας:			
Ημερομηνία Γέννησης(2):			
Αριθμός Δελτίου Ταυτότητας:		Τηλ:	
Αρ. Τηλεομοιοτύπου (Fax):		Δ/νση Ηλεκτρ. Ταχυδρομείου (Email):	

Ο παρακάτω υπογεγραμμένος υπάλληλος του ΚΕΠ….. δηλώνω ότι διάβασα τους όρους της Πολιτικής Ασφάλειας της ΑΠΕΔ τους οποίους αποδέχομαι και δηλώνω ότι θα τους τηρώ.

Ημερομηνία: / /202

Ο/Η Δηλών /ούσα

(Υπογραφή)

(1) Αναγράφεται από τον ενδιαφερόμενο πολίτη ή Αρχή ή η Υπηρεσία του δημόσιου τομέα, που απευθύνεται η αίτηση.
(2) Αναγράφεται ολογράφως.