e:Presence.gov.gr

grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

Υπηρεσία Τηλεδιασκέψεων για τον ευρύτερο Δημόσιο Τομέα

e:Presence.gov.gr

Αναλυτικές πληροφορίες διασφάλισης επικοινωνιών και συμμόρφωσης με το θεσμικό πλαίσιο

Απρίλιος 2020

ΕΙΣΑΓΩΓΗ

Από τις 16 Μαρτίου 2020, η ΕΔΥΤΕ ΑΕ, ανταποκρινόμενη στις επείγουσες απαιτήσεις της Δημόσιας Διοίκησης για διεξαγωγή συνεδριάσεων και συναντήσεων μέσω τηλεδιασκέψεων, υλοποίησε και λειτουργεί σε 24ωρη βάση την υπηρεσία e:Presence.gov.gr (https://www.epresence.gov.gr), η οποία παρέχει τη δυνατότητα σε όλους τους φορείς του δημόσιου και ευρύτερου δημόσιου τομέα να προγραμματίσουν και να διενεργήσουν τις συνεδριάσεις των συλλογικών οργάνων τους μέσω τηλεδιάσκεψης.

Το παρόν κείμενο παραθέτει τα στοιχεία αρχιτεκτονικής της διαδικτυακής εφαρμογής που υλοποιεί η υπηρεσία e:Presence.gov.gr και τα μέτρα ασφάλειας που έχουν ληφθεί από την ΕΔΥΤΕ ΑΕ, με στόχο τη διασφάλιση:

- της εμπιστευτικότητας και της μυστικότητας των συνεδριάσεων
- της πιστοποίησης ταυτότητας των συμμετεχόντων σε μια τηλεδιάσκεψη
- της ασφάλειας ηλεκτρονικής διακίνησης δεδομένων φωνής και εικόνας κατά τη διάρκεια μιας τηλεδιάσκεψης
- της ακεραιότητας της μεταδιδόμενης πληροφορίας κατά τη διάρκεια μιας τηλεδιάσκεψης

βάσει όσων καθορίζονται στο σχετικό θεσμικό πλαίσιο (υπ΄αριθμ. ΔΙΑΔΠ/Α/7841/19.04.2005 κοινή υπουργική απόφαση (Β' 539), όπως τροποποιήθηκε και ισχύει)

Λόγω του γεγονότος ότι η ασφάλεια των επικοινωνιών μέσω της υπηρεσίας προϋποθέτει ότι και όλες οι συσκευές που χρησιμοποιούνται για τη σύνδεση σε τηλεδιασκέψεις (προσωπικοί υπολογιστές ή φορητές συσκευές) είναι διασφαλισμένες απέναντι σε κακόβουλες παρεμβάσεις οποιουδήποτε τύπου, το κείμενο περιλαμβάνει και μια σειρά από βέλτιστες πρακτικές για τους τελικούς χρήστες, οι οποίες μπορούν να μειώσουν κατά το δυνατόν τους κινδύνους υποκλοπής των επικοινωνιών που διεξάγονται μέσω της υπηρεσίας από τρίτους μη εξουσιοδοτημένους, κακόβουλους ή μη, χρήστες.

ΤΑΥΤΟΠΟΙΗΣΗ, ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΚΑΙ ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΧΡΗΣΤΩΝ

ΤΑΥΤΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ

Η ταυτοποίηση χρηστών γίνεται με βάση τον μοναδικό για τον καθένα Αριθμό Φορολογικού Μητρώου (ΑΦΜ), ο οποίος παρέχεται κατά τη διαδικασία της αυθεντικοποίησης.

ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ

Η πιστοποίηση της ταυτότητας των «χρηστών» γίνεται μέσω της αυθεντικοποίησης χρηστών (oAuth 2.0) που παρέχεται από το κέντρο διαλειτουργικότητας της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (ΓΓΠΣΔΔ), με τα διαπιστευτήρια που έχει ο χρήστης στο TaxisNet, κατά τα οριζόμενα στην υπ' αρ. 3981ΕΞ2020 απόφαση του Υπουργού Επικρατείας «Παροχή Υπηρεσίας Αυθεντικοποίησης Χρηστών oAuth2.0 σε Πληροφοριακά Συστήματα τρίτων Φορέων» (Β' 762) και στην Κοινή Υπουργική Απόφαση 429/2020 – ΦΕΚ 850/Β/13-03-2020. Μέσω της υπηρεσίας αυτής, χρησιμοποιούνται με ασφαλή τρόπο τα διαπιστευτήρια του TaxisNet για την αυθεντικοποίηση των χρηστών στη διαδικτυακή εφαρμογή της υπηρεσίας e:Presence.gov.gr. Πληροφορίες για την εν λόγω υπηρεσία αυθεντικοποίησης που παρέχει η ΓΓΠΣΔΔ παρέχονται στην ιστοσελίδα:

https://www.gsis.gr/dimosia-dioikisi/kentro-dialeitoyrgikotitas-ked-ypoyrgeioy-psifiakis-diakybernisis/diadiktyakes

Η εφαρμογή e:Presence.gov.gr δεν επιτρέπει στον χρήστη να αλλάξει τα στοιχεία ταυτότητάς του (ονοματεπώνυμο και ΑΦΜ). Αυτά παραμένουν πάντοτε όπως έχουν αποδοθεί αρχικά από την υπηρεσία αυθεντικοποίησης oAuth2.0 της ΓΓΠΣΔΔ, κατά την πρώτη φορά που ο χρήστης εισέρχεται στην υπηρεσία e:Presence.gov.gr και δημιουργεί τον προσωπικό του λογαριασμό.

Επιπλέον, μετά την πιστοποίηση της ταυτότητας των «χρηστών» μέσω της αυθεντικοποίησης χρηστών (oAuth 2.0) της ΓΓΠΣΔΔ, αντλείται από το Μητρώο Ανθρώπινου Δυναμικού του Ελληνικού Δημοσίου (http://apografi.gov.gr/) [εφεξής «Μητρώο»] με κριτήριο τον Α.Φ.Μ. του «χρήστη», η πληροφορία εάν ανήκει στο σχετικό «Μητρώο» καθώς και τα στοιχεία των «Φορέων» στους οποίους έχει απογραφεί. Στην περίπτωση ύπαρξης περισσότερων του ενός «Φορέων» στους οποίους έχει απογραφεί, ο «χρήστης» επιλέγει τον «Φορέα» που επιθυμεί να εμφανίζεται στον λογαριασμό του. Λογαριασμό «χρήστη», δύναται να δημιουργήσει κάποιος και ύστερα από εξατομικευμένη πρόσκληση, που τον καλεί να συμμετάσχει σε μια συγκεκριμένη τηλεδιάσκεψη. Απαραίτητη προϋπόθεση όμως πάντα είναι η αυθεντικοποίηση του μέσω TaxisNet.

ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΧΡΗΣΤΩΝ

Στην παρούσα παράγραφο χρησιμοποιούνται οι όροι "απλός χρήστης", "συντονιστής", "συντονιστής φορέα" και "συντονιστής οργανικής μονάδας", όπως αυτοί ορίζονται στους Όρους Χρήσης της υπηρεσίας e:Presence.gov.gr (https://www.epresence.gov.gr/terms).

Η εξουσιοδότηση απλού χρήστη για την είσοδο στην εφαρμογή και τη δημιουργία του προσωπικού του λογαριασμού χρήστη, γίνεται με βάση τα στοιχεία τα οποία αντλούνται αυτόματα από το Μητρώο Ανθρώπινου Δυναμικού του Ελληνικού Δημοσίου (https://hr.apografi.gov.gr), χρησιμοποιώντας τον ΑΦΜ του χρήστη:

- Σε περίπτωση που ο χρήστης (φυσικό πρόσωπο) έχει ενεργή σχέση εργασίας οποιουδήποτε τύπου με φορέα του δημόσιου ή ευρύτερου δημόσιου τομέα, η οποία είναι καταχωρημένη στο Μητρώο, επιτρέπεται η είσοδος στην εφαρμογή και δημιουργείται ο προσωπικός λογαριασμός του στην υπηρεσία.
- Σε περίπτωση που δεν υπάρχει συσχέτιση του φυσικού προσώπου με κανέναν φορέα στο Μητρώο, ο χρήστης ενημερώνεται ότι δεν εξουσιοδοτείται να χρησιμοποιήσει την υπηρεσία και δεν μπορεί να δημιουργήσει προσωπικό λογαριασμό.
- Σε περίπτωση που το ΑΦΜ που παρέχεται από την διαδικασία αυθεντικοποίησης αφορά σε νομικό πρόσωπο, ο χρήστης επίσης ενημερώνεται ότι δεν εξουσιοδοτείται να χρησιμοποιήσει την υπηρεσία και δεν μπορεί να δημιουργήσει προσωπικό λογαριασμό.

Η εφαρμογή e:Presence.gov.gr επιτρέπει παρόλα αυτά τη δημιουργία λογαριασμού απλού χρήστη και τη συμμετοχή σε τηλεδιασκέψεις για φυσικά πρόσωπα που δεν έχουν καταγεγραμμένη σχέση εργασίας στο Μητρώο, μόνο στην περίπτωση που αυτά έχουν προσκληθεί για να συμμετάσχουν σε τηλεδιασκέψεις. Η πρόσκληση αυτή γίνεται από άτομο που έχει ρόλο συντονιστή τηλεδιάσκεψης και αποστέλλεται μέσω ηλεκτρονικού ταχυδρομείου (email). Ο χρήστης που έχει προσκληθεί με αυτήν τη διαδικασία, πάντοτε ταυτοποιείται μέσω της υπηρεσίας oAuth2.0 με τη διαδικασία που περιγράφηκε παραπάνω.

Η εξουσιοδότηση διοργάνωσης τηλεδιασκέψεων (ρόλος συντονιστή), αποδίδεται μόνο σε φυσικά πρόσωπα που έχουν ενεργή σχέση εργασίας με φορέα του δημόσιου ή ευρύτερου δημόσιου τομέα, σύμφωνα με τα στοιχεία του Μητρώου. Η απόδοση αυτού του δικαιώματος γίνεται μετά από σχετικό αίτημα του χρήστη, στο οποίο υποχρεωτικά δηλώνει μεταξύ άλλων ένα τηλέφωνο επικοινωνίας και μια σύντομη αιτιολόγηση του αιτήματός του.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΠΟ ΑΚΡΗ ΣΕ ΑΚΡΗ (END-TO-END ENCRYPTION)

Η υπηρεσία e:Presence.gov.gr χρησιμοποιεί την υποδομή τηλεδιασκέψεων της εταιρείας Zoom (https://zoom.us), η οποία επιλέχθηκε για την αντίστοιχη υπηρεσία τηλεδιασκέψεων του ακαδημαϊκού και ερευνητικού τομέα (https://www.epresence.gr) το 2018 μετά από σχετική διερεύνηση των εμπορικά διαθέσιμων υπηρεσιών τηλεδιάσκεψης, γιατί ήταν η μόνη λύση που ανταποκρίθηκε στις απαιτήσεις προγραμματιστικής διαχείρισης τηλεδιασκέψεων μέσω REST API.

Η εταιρεία Zoom, για τη διασφάλιση της εμπιστευτικότητας και της μυστικότητας των επικοινωνιών, έχει υλοποιήσει τα ακόλουθα τεχνικά χαρακτηριστικά:

1. Κρυπτογράφηση της επικοινωνίας από άκρη σε άκρη (end-to-end encryption) στην περίπτωση που όλα τα συνδεδεμένα σημεία σε μια τηλεδιάσκεψη είναι κάποιος τύπος Zoom Client Application (για Windows, Mac, Linux, iOS και Android). Αυτή η περίπτωση εφαρμόζεται σε όλες τις τηλεδιασκέψεις της υπηρεσίας e:Presence.gov.gr. Βλέπε σχετικό άρθρο: https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/
2. Κρυπτογράφηση των επικοινωνιών με αλγόριθμο συμμετρικού κλειδιού AES-256 ECB, ο οποίος αναμένεται εντός του 2020 να αντικατασταθεί από αλγόριθμο AES-256 GCM. Βλέπε σχετικό άρθρο: https://blog.zoom.us/wordpress/2020/04/08/zoom-ask-eric-anything-webinar-addresses-user-security-privacy-concerns/
3. Διανομή κλειδιών κρυπτογράφησης μέσω κρυπτογραφημένου καναλιού TLS με κλειδί 256-bit.

Σχετικά με την κρυπτογράφηση από άκρη σε άκρη, οι εξαιρέσεις που αναφέρονται στο πρώτο από τα ως άνω άρθρα, δεν εφαρμόζονται ποτέ στην υπηρεσία e:Presence.gov.gr, άρα όλες οι τηλεδιασκέψεις είναι πάντα κρυπτογραφημένες από άκρη σε άκρη. Συγκεκριμένα:

- Σύνδεση σε τηλεδιάσκεψη Zoom μέσω τηλεφώνου: Η δυνατότητα αυτή δεν είναι ενεργοποιημένη στην υπηρεσία e:Presence.gov.gr.
- Σύνδεση σε τηλεδιάσκεψη Zoom μέσω συστήματος τηλεδιάσκεψης H.323/SIP: Η δυνατότητα αυτή δεν είναι ενεργοποιημένη στην υπηρεσία e:Presence.gov.gr.
- Σύνδεση σε τηλεδιάσκεψη Zoom μέσω Skype: Η δυνατότητα αυτή δεν είναι ενεργοποιημένη στην υπηρεσία e:Presence.gov.gr.
- Καταγραφή τηλεδιασκέψεων (recording): Επιτρέπεται μόνο η καταγραφή σε τοπικό αποθηκευτικό μέσο εξουσιοδοτημένου χρήστη, όπως αναφέρεται στο άρθρο 5 των όρων χρήσης της υπηρεσίας e:Presence.gov.gr (https://www.epresence.gov.gr/terms). Η αποκρυπτογράφηση των δεδομένων ήχου και εικόνας συμβαίνει μόνο στον υπολογιστή του συνδεδεμένου χρήστη, ο οποίος έχει αναλάβει να κάνει την καταγραφή. Η καταγραφή σε αποθηκευτικό χώρο της Zoom (Cloud recording) είναι απενεργοποιημένη στις ρυθμίσεις της υπηρεσίας.
- Μετάδοση τηλεδιασκέψεων μέσω Youtube, Facebook, κλπ.: Η δυνατότητα αυτή δεν είναι ενεργοποιημένη στην υπηρεσία e:Presence.gov.gr.

ΠΕΡΙΟΡΙΣΜΟΣ ΣΥΜΜΕΤΟΧΗΣ ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΩΝ ΧΡΗΣΤΩΝ ΣΕ ΤΗΛΕΔΙΑΣΚΕΨΕΙΣ

Η υλοποίηση της εφαρμογής e:Presence.gov.gr διασφαλίζει ότι κανείς μη εξουσιοδοτημένος χρήστης δεν θα μπορέσει να συνδεθεί σε μία τηλεδιάσκεψη της υπηρεσίας. Ως εξουσιοδοτημένος χρήστης νοείται ο χρήστης της υπηρεσίας, ο οποίος έχει ενεργό λογαριασμό στην εφαρμογή, έχοντας περάσει τη διαδικασία αυθεντικοποίησης oAuth2.0 της ΓΓΠΣΔΔ και έχει προσκληθεί να συμμετάσχει στην τηλεδιάσκεψη από τον διοργανωτή αυτής (συντονιστή).

Τα μέτρα που έχουν ληφθεί για αυτόν τον σκοπό είναι τα εξής:

1. Κάθε τηλεδιάσκεψη στην υπηρεσία που παρέχει η Zoom έχει ένα 11ψήφιο αναγνωριστικό αριθμό (Meeting ID). Ο αριθμός αυτός, υπό συγκεκριμένες συνθήκες, θα μπορούσε να αξιοποιηθεί από κάποιον τρίτο για να προσπαθήσει να συνδεθεί σε μία συγκεκριμένη τηλεδιάσκεψη. Στην υπηρεσία e:Presence.gov.gr, ο αριθμός αυτός υπάρχει μόνο στη βάση δεδομένων του εξυπηρετητή, ώστε να μπορεί η εφαρμογή να διαχειριστεί προγραμματιστικά την τηλεδιάσκεψη και δεν εμφανίζεται σε καμία ιστοσελίδα.
2. Ακόμη κι αν κάποιος δει το Meeting ID στη διάρκεια μιας τηλεδιάσκεψης (διαθέσιμο στον Zoom Client), οι ρυθμίσεις όλων των τηλεδιασκέψεων του e:Presence.gov.gr δεν επιτρέπουν τη σύνδεση οποιουδήποτε σε μια τηλεδιάσκεψη, γνωρίζοντας μόνο το Meeting ID. Βλέπε και το επόμενο σημείο.
3. Κάθε συμμετέχων (προσκληθείς) στην τηλεδιάσκεψη, έχει ένα μοναδικό προσωποποιημένο URL σύνδεσης με το οποίο μόνο αυτός μπορεί να συνδεθεί και η κάθε τηλεδιάσκεψη δέχεται συνδέσεις μόνο από χρήστες που έχουν χρησιμοποιήσει αυτό το μοναδικό URL σύνδεσης. Τα URL αυτά παράγονται από την υπηρεσία της Zoom, μετά από προγραμματιστικό αυτόματο αίτημα που κάνει για κάθε συμμετέχοντα η εφαρμογή e:Presence.gov.gr κατά την έναρξη μιας τηλεδιάσκεψης. Στη συνέχεια αποθηκεύονται στην τοπική βάση δεδομένων και παρέχονται στον εξουσιοδοτημένο (με την έννοια που αναφέρεται στην πρώτη παράγραφο παραπάνω) χρήστη με διαφανή ανακατεύθυνση, μόλις πατήσει το κουμπί “Σύνδεση” σε μία τηλεδιάσκεψη στην οποία έχει προσκληθεί. Τέλος, τα URL σύνδεσης παύουν να είναι ενεργά, μόλις η τηλεδιάσκεψη ολοκληρωθεί, βάσει του προγραμματισμού της.
4. Η δυνατότητα πρόσκλησης τρίτων σε μία τηλεδιάσκεψη, που υπάρχει εγγενώς ως διαθέσιμο χαρακτηριστικό σε κάθε εφαρμογή της εταιρείας Zoom, είναι μεν ενεργή, αλλά δεν μπορεί να χρησιμοποιηθεί (δεν έχει κανένα αποτέλεσμα) διότι, όπως προαναφέρθηκε, μόνο με προσωποποιημένα, μοναδικά URL μπορεί κάποιος να συνδεθεί σε μία τηλεδιάσκεψη του e:Presence.gov.gr και αυτά τα URL δεν μπορούν να παραχθούν από κάποιον τρίτο.
5. Η δυνατότητα σύνδεσης σε μία τηλεδιάσκεψη ενεργοποιείται μόνο την προγραμματισμένη ώρα έναρξής της και απενεργοποιείται όταν φτάσει η προγραμματισμένη ώρα λήξης αυτής. Η σύνδεση σε μία τηλεδιάσκεψη εκτός των προγραμματισμένων ωρών της είναι αδύνατη.
6. Για να αποκλειστεί η περίπτωση κάποιος κακόβουλα να αποκτήσει τον έλεγχο μιας τηλεδιάσκεψης εκμεταλλευόμενος τη δυνατότητα αυξημένης διαχείρισης (Host Key) μιας τηλεδιάσκεψης, όπως αυτή αναφέρεται στο άρθρο 5 των Όρων Χρήσης (https://www.epresence.gov.gr/terms), το Host Key ανανεώνεται προγραμματιστικά για κάθε νέα τηλεδιάσκεψη και μπορεί να χρησιμοποιηθεί μόνο για τη συγκεκριμένη τηλεδιάσκεψη στην οποία έχει ζητηθεί αυτή η δυνατότητα. Το Host Key μιας τηλεδιάσκεψης παρέχεται μόνο στον συντονιστή που την έχει διοργανώσει, και στους συντονιστές του φορέα στον οποίο αυτός ο συντονιστής υπάγεται.

ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ ΔΙΑΣΦΑΛΙΣΗΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΓΙΑ ΤΟΥΣ ΧΡΗΣΤΕΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Όπως γίνεται σαφές από τα παραπάνω, η ΕΔΥΤΕ ΑΕ, έχει λάβει όλα τα εφικτά μέτρα προστασίας της ασφάλειας των επικοινωνιών μέσω της υπηρεσίας e:Presence.gov.gr. Παρόλα αυτά, η ασφάλεια των επικοινωνιών μπορεί τυχόν να παραβιαστεί, αν οι συσκευές που χρησιμοποιούν οι χρήστες για να συνδεθούν στην υπηρεσία (προσωπικοί υπολογιστές, smartphones ή tablets) δεν είναι επίσης διασφαλισμένα από κακόβουλες παρεμβάσεις.

Προς αυτήν την κατεύθυνση, παρατίθενται παρακάτω μια σειρά από βέλτιστες πρακτικές που συνιστάται να ακολουθούν όλοι οι χρήστες της υπηρεσίας, για να μειωθούν οι κίνδυνοι μη εξουσιοδοτημένης παρέμβασης από τρίτους, παρακάμπτοντας τα μέτρα ασφαλείας που έχουν ληφθεί από την ΕΔΥΤΕ ΑΕ.

ΤΑΚΤΙΚΗ ΕΓΚΑΤΑΣΤΑΣΗ ΕΝΗΜΕΡΩΣΕΩΝ ΛΟΓΙΣΜΙΚΟΥ

Για το λειτουργικό σύστημα κάθε υποστηριζόμενης συσκευής (Windows, Mac OS, Linux, iOS, Android) πρέπει να λαμβάνονται και να εγκαθίστανται όλες οι ενημερώσεις λογισμικού που προτείνονται από τον εκάστοτε κατασκευαστή του. Η ενημέρωση αυτή πρέπει να γίνεται τακτικά (μια φορά την εβδομάδα).

Το ίδιο ισχύει και για τους υποστηριζόμενους περιηγητές (browsers) που χρησιμοποιούνται για την πρόσβαση στην υπηρεσία (Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge).

Ειδικά για το λογισμικό Zoom που χρησιμοποιείται για τη σύνδεση στις τηλεδιασκέψεις, τυχόν διαθέσιμες ενημερώσεις που εμφανίζονται όταν ο χρήστης ανοίγει την εφαρμογή, πρέπει να εγκαθίστανται άμεσα (μόλις γίνουν διαθέσιμες), πριν ο χρήστης προσπαθήσει να συνδεθεί σε οποιαδήποτε τηλεδιάσκεψη.

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Συνιστάται έντονα η χρήση οποιουδήποτε σύγχρονου λογισμικού anti-virus/anti-malware με τακτικό (μια φορά την εβδομάδα) έλεγχο της συσκευής που χρησιμοποιείται για τη σύνδεση στην υπηρεσία. Τυχούσα ύπαρξη κακόβουλου λογισμικού στη συσκευή, μπορεί να υποκλέψει τα στοιχεία σύνδεσης σε τηλεδιασκέψεις, είτε μέσω του λειτουργικού συστήματος, είτε μέσω του browser που χρησιμοποιείται. Γι’ αυτόν τον λόγο, οποιαδήποτε προειδοποίηση που παρέχεται από λογισμικά anti-virus/anti-malware θα πρέπει να εξετάζεται και να αντιμετωπίζεται με τον προτεινόμενο τρόπο.

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΜΗ ΑΣΦΑΛΗ ΔΙΚΤΥΑ

Αν οι χρήστες συνδέονται στην υπηρεσία από ασύρματα (WiFi) δίκτυα, θα πρέπει να βεβαιώνονται ότι η κρυπτογράφηση που χρησιμοποιείται στο συγκεκριμένο ασύρματο δίκτυο είναι τύπου WPA2. Επίσης να προτιμάται η κρυπτογράφηση WPA2 Enterprise αντί της WPA2 Personal.

Η χρήση της υπηρεσίας από δημόσια διαθέσιμα δίκτυα (ασύρματα δίκτυα Δήμων, Internet Café) δεν είναι ασφαλής και δεν προτείνεται.

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΕΞΥΠΗΡΕΤΗΤΗ PROXY

Στην περίπτωση που ο χρήστης της υπηρεσίας χρησιμοποιεί εξυπηρετητή HTTPS Proxy (είτε κάνοντας τις σχετικές ρυθμίσεις στη συσκευή του, είτε διαφανώς) για την πρόσβασή του στο διαδίκτυο, θα πρέπει να ακυρώνει οποιαδήποτε προσπάθεια σύνδεσης στην υπηρεσία e:Presence.gov.gr αν του εμφανιστεί προειδοποίηση για μη έμπιστο πιστοποιητικό εξυπηρετητή, διότι σε αυτήν την περίπτωση δεν υπάρχει καμία διασφάλιση των διακινούμενων δεδομένων. Στην περίπτωση αυτή, συνιστάται να ενημερωθεί σχετικά ο διαχειριστής του τοπικού δικτύου.

ΣΥΝΔΕΣΗ ΣΤΗΝ ΥΠΗΡΕΣΙΑ E:PRESENCE.GOV.GR

Κατά τη σύνδεση στην υπηρεσία, ο χρήστης θα πρέπει να βεβαιώνεται ότι η διεύθυνση που αναγράφεται στον browser ξεκινά με το https://www.epresence.gov.gr και ότι το πιστοποιητικό SSL είναι έγκυρο. Στους περισσότερους browsers η διασφάλιση του πιστοποιητικού εμφανίζεται με κάποιο εικονίδιο λουκέτου δίπλα στην διαδικτυακή διεύθυνση.

ΧΡΗΣΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

Ο χρήστης πρέπει να βεβαιώνεται ότι εισάγει πάντα τα διαπιστευτήρια σύνδεσής του στο TaxisNet όταν συνδέεται στην υπηρεσία e:Presence.gov.gr, και ότι αποσυνδέεται από την υπηρεσία (Logout - Έξοδος) όταν δε χρειάζεται να τη χρησιμοποιήσει πλέον. Αυτό διασφαλίζει ότι κανείς μη εξουσιοδοτημένος χρήστης δε θα μπορεί να κάνει χρήση του λογαριασμού του, αν αποκτήσει πρόσβαση στην συσκευή του (προσωπικό υπολογιστή ή φορητή συσκευή).