Υπηρεσία Τηλεδιασκέψεων για τον Ακαδημαϊκό και Ερευνητικό Τομέα

e:Presence

Αναλυτικές πληροφορίες διασφάλισης επικοινωνιών και συμμόρφωσης με το θεσμικό πλαίσιο

Ιούνιος 2020

ΕΙΣΑΓΩΓΗ

Από το 2011, η ΕΔΥΤΕ ΑΕ, ανταποκρινόμενη στις απαιτήσεις του Ακαδημαϊκού και Ερευνητικού τομέα για διεξαγωγή συνεδριάσεων και συναντήσεων μέσω τηλεδιασκέψεων υψηλής ποιότητας, υλοποίησε και λειτουργεί σε 24ωρη βάση την υπηρεσία e:Presence (https://www.epresence.gr), η οποία παρέχει τη δυνατότητα σε όλους τους φορείς του ακαδημαϊκού και ερευνητικού 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 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 δύο διαφορετικούς τρόπους:

- Για τα μέλη της Ακαδημαϊκής και Ερευνητικής κοινότητας, που διαθέτουν λογαριασμό σε έναν από τους αναγνωρισμένους φορείς του τομέα αυτού, η ταυτοποίηση γίνεται με την ακολουθία χαρακτήρων persistent_id, η οποία χρησιμοποιείται από την υποδομή ταυτοποίησης και εξουσιοδότησης της Ομοσπονδίας ΔΗΛΟΣ του ΕΔΥΤΕ (https://aai.grnet.gr). Η ακολουθία χαρακτήρων αυτή είναι μοναδική για κάθε τριάδα παρόχου ταυτότητας, παρόχου υπηρεσίας, και ταυτοποιούμενου χρήστη.

- Για τρίτους που προσκαλούνται να συμμετέχουν σε τηλεδιασκέψεις (π.χ. συνεργαζόμενοι φορείς, πανεπιστήμια του εξωτερικού), η ταυτοποίηση γίνεται με όνομα χρήστη και μυστικό κωδικό, που αποδίδονται στον χρήστη κατά την εγγραφή του στην υπηρεσία.

ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ

Η αυθεντικοποίηση των χρηστών της Ακαδημαϊκής και Ερευνητικής κοινότητας που προσπελαύνουν την υπηρεσία μέσω του μηχανισμού ταυτοποίησης της Ομοσπονδίας ΔΗΛΟΣ γίνεται μέσω του μηχανισμού Shibboleth, με τρόπο ώστε να χρησιμοποιούνται με ασφάλεια τα διαπιστευτήρια του χρήστη στον οικείο πάροχο ταυτότητας (ακαδημαϊκός ή ερευνητικός φορέας) για την αυθεντικοποίηση των χρηστών στη διαδικτυακή εφαρμογή της υπηρεσίας e:Presence.

Για τους τρίτους χρήστες, εκτός της ακαδημαϊκής και ερευνητικής κοινότητας, η διαδικασία αυθεντικοποίησης αφορά μόνο στην ταυτοποίησή τους στην υπηρεσία και την επιβεβαίωση μιας email διεύθυνσης την οποία δηλώνουν οι ίδιοι.

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 (https://www.epresence.gr/terms).

Οι χρήστες που ανήκουν σε κάποιον ακαδημαϊκό ή ερευνητικό φορέα και εισέρχονται στην εφαρμογή χρησιμοποιώντας τον μηχανισμό ταυτοποίησης της Ομοσπονδίας ΔΗΛΟΣ, έχουν αυτοδικαίως την εξουσιοδότηση να χρησιμοποιήσουν την εφαρμογή για να συμμετέχουν σε τηλεδιασκέψεις που αφορούν στο αντικείμενο εργασίας του φορέα τους.

Οι τρίτοι χρήστες, εκτός της ακαδημαϊκής και ερευνητικής κοινότητας, μπορούν να αποκτήσουν λογαριασμό στην εφαρμογή e:Presence μόνο μετά από πρόσκληση ενός χρήστη που έχει αποκτήσει ρόλο “συντονιστή” και ανήκει σε κάποιον ακαδημαϊκό ή ερευνητικό φορέα

Η εξουσιοδότηση διοργάνωσης τηλεδιασκέψεων (ρόλος συντονιστή), αποδίδεται σε οποιονδήποτε χρήστη της υπηρεσίας, μετά από σχετικό αίτημα του χρήστη, στο οποίο υποχρεωτικά δηλώνει μεταξύ άλλων ένα τηλέφωνο επικοινωνίας και μια σύντομη αιτιολόγηση του αιτήματός του, το οποίο πρέπει να αφορά σε εξυπηρέτηση αναγκών επικοινωνίας ενός ή περισσότερων φορέων της ακαδημαϊκής και ερευνητικής κοινότητας.

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

Η υπηρεσία e:Presence χρησιμοποιεί την υποδομή τηλεδιασκέψεων της εταιρείας Zoom (https://zoom.us), η οποία επιλέχθηκε για την 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, με εξαίρεση τις τηλεδιασκέψεις στις οποίες συμμετέχει τουλάχιστον μία παραδοσιακή (legacy) τερματική συσκευή τηλεδιάσκεψης H.323/SIP. Βλέπε σχετικό άρθρο: https://github.com/zoom/zoom-e2e-whitepaper
2. Κρυπτογράφηση των επικοινωνιών με αλγόριθμο συμμετρικού κλειδιού AES-256 GCM. Βλέπε σχετικό άρθρο: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
3. Διανομή κλειδιών κρυπτογράφησης μέσω κρυπτογραφημένου καναλιού TLS με κλειδί 256-bit.

Επειδή η συμμετοχή μιας τερματικής συσκευής τηλεδιάσκεψης H.323/SIP σε μία τηλεδιάσκεψη του e:Presence παρακάμπτει την από άκρη σε άκρη κρυπτογράφηση, λόγω της ανάγκης για διακωδικοποίηση των σημάτων εικόνας και ήχου, η ΕΔΥΤΕ ΑΕ έχει εγκαταστήσει και συντηρεί διασφαλισμένη ιδιωτική υποδομή διασύνδεσης συσκευών H.323/SIP σε τηλεδιασκέψεις της υπηρεσίας e:Presence, η οποία παρέχει τα ακόλουθα πρόσθετα χαρακτηριστικά ασφαλείας:

- Επιτρέπει τη σύνδεση συσκευών H.323/SIP μόνο με εισερχόμενη κλήση προς μία τηλεδιάσκεψη (dial-in), και μόνο από διεύθυνση IP που έχει δηλωθεί μέσω της εφαρμογής e:Presence από ταυτοποιημένο χρήστη της υπηρεσίας, για ένα περιορισμένο χρονικό διάστημα λίγων λεπτών μετά τη δήλωση της διεύθυνσης. Οποιαδήποτε άλλη κλήση από μη δηλωμένη διεύθυνση IP ή εκτός του χρονικού διαστήματος ενεργοποίησης μιας δηλωμένης διεύθυνσης, απορρίπτεται από την υπηρεσία.

- Απαγορεύει τις εξερχόμενες κλήσεις προς συσκευές H.323/SIP μέσω της εφαρμογής τηλεδιάσκεψης Zoom.

- Περιορίζει την αποκρυπτογράφηση των μεταδιδόμενων σημάτων εικόνας και ήχου στους εξυπηρετητές διασύνδεσης της ΕΔΥΤΕ ΑΕ, με αποκλειστικό σκοπό να γίνεται η απαραίτητη διακωδικοποίηση ροών (transcoding). Τα σήματα εικόνας και ήχου κρυπτογραφούνται εκ νέου για να αναμεταδοθούν προς την υποδομή τηλεδιασκέψεων της εταιρείας Zoom, όπου συνεχίζει να τηρείται η κρυπτογράφηση από άκρη σε άκρη.

Σχετικά με τις υπόλοιπες εξαιρέσεις της κρυπτογράφησης από άκρη σε άκρη, που αναφέρονται στο πρώτο από τα ως άνω άρθρα, δεν εφαρμόζονται ποτέ στην υπηρεσία e:Presence, 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.
- Σύνδεση σε τηλεδιάσκεψη Zoom μέσω Skype: Η δυνατότητα αυτή δεν είναι ενεργοποιημένη στην υπηρεσία e:Presence.
- Καταγραφή τηλεδιασκέψεων (recording): Η δυνατότητα αυτή δεν είναι ενεργοποιημένη στην υπηρεσία e:Presence.
- Μετάδοση τηλεδιασκέψεων μέσω Youtube, Facebook, κλπ.: Η δυνατότητα αυτή δεν είναι ενεργοποιημένη στην υπηρεσία e:Presence.

ΠΕΡΙΟΡΙΣΜΟΣ ΣΥΜΜΕΤΟΧΗΣ ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΩΝ ΧΡΗΣΤΩΝ ΣΕ ΤΗΛΕΔΙΑΣΚΕΨΕΙΣ

Η υλοποίηση της εφαρμογής e:Presence 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 όπως αναφέρεται παραπάνω 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, 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 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 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 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.

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. 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

Κατά τη σύνδεση στην υπηρεσία, ο χρήστης θα πρέπει να βεβαιώνεται ότι η διεύθυνση που αναγράφεται στον browser ξεκινά με το https://www.epresence.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 όταν συνδέεται στην υπηρεσία e:Presence, 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).