$E \cdot T \cdot S \cdot D$

Ηλεκτρονική διαβίβαση ευαισθητης πληροφορίας

Η εφαρμογή χρησιμοποιείται για τη διαβίβαση ευαίσθητης πληροφορίας

Εγχειρίδιο βασικών λειτουργιών Εφαρμογής Ηλεκτρονικής Διαβίβασης Ευαίσθητης Πληροφορίας

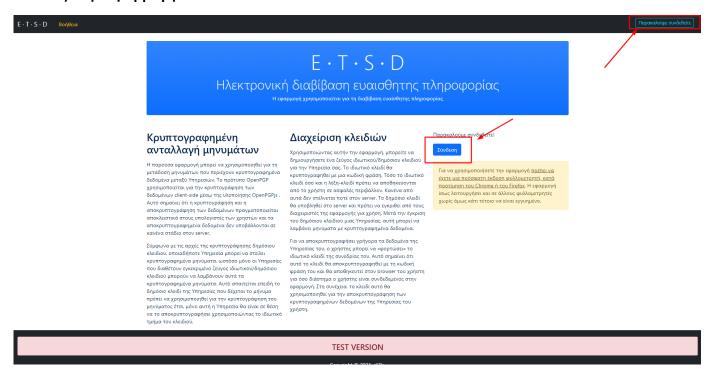
Η εφαρμογή Ηλεκτρονικής Διαβίβασης Ευαίσθητης Πληροφορίας μπορεί να χρησιμοποιηθεί για τη μετάδοση μηνυμάτων που περιέχουν κρυπτογραφημένα δεδομένα μεταξύ Υπηρεσιών. Το πρότυπο OpenPGP χρησιμοποιείται για την κρυπτογράφηση των δεδομένων client-side μέσω της υλοποίησης OpenPGPjs . Αυτό σημαίνει ότι η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων πραγματοποιείται αποκλειστικά στους υπολογιστές των χρηστών και τα αποκρυπτογραφημένα δεδομένα δεν υποβάλλονται σε κανένα στάδιο στον server.

Σύμφωνα με τις αρχές της κρυπτογράφησης δημόσιου κλειδιού, οποιαδήποτε Υπηρεσία μπορεί να στείλει κρυπτογραφημένα μηνύματα, ωστόσο μόνο οι Υπηρεσίες που διαθέτουν εγκεκριμένο ζεύγος ιδιωτικού/δημόσιου κλειδιού μπορούν να λαμβάνουν αυτά τα κρυπτογραφημένα μηνύματα. Αυτό απαιτείται επειδή το δημόσιο κλειδί της Υπηρεσίες που δέχεται το μήνυμα πρέπει να χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος έτσι, μόνο αυτή η Υπηρεσία θα είναι σε θέση να το αποκρυπτογραφήσει χρησιμοποιώντας το ιδιωτικό τμήμα του κλειδιού.

Χρησιμοποιώντας αυτήν την εφαρμογή, μπορείτε να δημιουργήσετε ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού για την Υπηρεσία σας. Το ιδιωτικό κλειδί θα κρυπτογραφηθεί με μια κωδική φράση. Τόσο το ιδιωτικό κλειδί όσο και η λέξη-κλειδί πρέπει να αποθηκεύονται από το χρήστη σε ασφαλές περιβάλλον. Κανένα από αυτά δεν στέλνεται ποτέ στον server. Το δημόσιο κλειδί θα υποβληθεί στο server και πρέπει να εγκριθεί από τους διαχειριστές της εφαρμογής για χρήση. Μετά την έγκριση του δημόσιου κλειδιού μιας Υπηρεσίας, αυτή μπορεί να λαμβάνει μηνύματα με κρυπτογραφημένα δεδομένα.

Για να αποκρυπτογραφήσει γρήγορα τα δεδομένα της Υπηρεσίας του, ο χρήστης μπορεί να «φορτώσει» το ιδιωτικό κλειδί της συνεδρίας του. Αυτό σημαίνει ότι αυτό το κλειδί θα αποκρυπτογραφηθεί με τη κωδική φράση του και θα αποθηκευτεί στον browser του χρήστη για όσο διάστημα ο χρήστης είναι συνδεδεμένος στην εφαρμογή. Στη συνέχεια, το κλειδί αυτό θα χρησιμοποιηθεί για την αποκρυπτογράφηση των κρυπτογραφημένων δεδομένων της Υπηρεσίας του χρήστη.

Είσοδος στην εφαρμογή



Η δοκιμαστική έκδοση της εφαρμογής βρίσκεται στην ηλεκτρονική διεύθυνση http://etsduat.hcg.gr. Για να εισέλθετε στην εφαρμογή επιλέξτε **Σύνδεση** από έναν από τους 2 συνδέσμους όπως φαίνονται στην εικόνα και εισάγετε τα στοιχεία του υπηρεσιακού λογαριασμού σας.



Κρυπτογραφημένη ανταλλαγή μηνυμάτων

Η παρούσα εφαρμογή μπορεί να χρησιμοποιηθεί για τη μετάδοση μηνυμάτων που περιέχουν κρυπτογραφημένα δεδομένα μεταξύ Υπηρεσιών. Το πρότυπο OpenPGP χρησιμοποιείται για την κρυπτογράφηση των δεδομένων client-side μέσω της υλοποίησης OpenPGPjs. Αυτό σημαίνει ότι η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων πραγματοποιείται αποκλειστικά στους υπολογιστές των χρηστών και τα αποκρυπτογραφημένα δεδομένα δεν υποβάλλονται σε κανένα στάδιο στον server.

Διαχείριση κλειδιών

Χρησιμοποιώντας αυτήν την εφαρμογή, μπορείτε να δημιουργήσετε ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού για την Υπηρεσία σας. Το ιδιωτικό κλειδί θα κρυπτογραφηθεί με μια κωδική φράση. Τόσο το ιδιωτικό κλειδί σο και η λέξη-κλειδί πρέπει να αποθηκεύονται από το χρήστη σε ασφαλές περιβάλλον. Κανένα από αυτά δεν στέλνεται ποτέ στον server. Το δημόσιο κλειδί θα υποβληθεί στο server και πρέπει να εγκριθεί από τους διαχειριστές της εφαρμογής για χρήση. Μετά την έγκριση του δημόσιου κλειδιού μιας Υπηρεσίας, αυτή μπορεί να λαμβάνει μηνύματα με κρυπτογραφημένα δεδομένα.

Για να αποκουπτουραφήσει νρήνορα τα δεδομένα της

Καλώς ήρθατε, ΝΙΚΟΛΑΟΣ ΛΑΓΚΑΣ (nlagkas)

Δεν έχετε Υπηρεσία
Χωρίς πρόσβαση!
Για να χρησιμοποιήσετε την εφαρμογή <u>πρέπει να</u>

τια να χρησιμοποιησετε την εφαρμογη <u>πρεπει να</u> έχε<u>τε μια πρόσφατη έκδοση φυλλομετρητή, κατά</u> <u>προτίμηση του Chrome ή του Firefox</u>. Η εφαρμογή ίσως λειτουργήσει και σε άλλους φυλλομετρητές χωρίς όμως κάτι τέτοιο να είναι εγγυημένο.

Αρχικά, δεν εμφανίζεται κάποια επιλογή ή λειτουργικότητα καθώς δεν έχετε αντιστοιχηθεί με κάποια Υπηρεσία. Θα πρέπει κάποιος διαχειριστής να σας προσθέσει στους χρήστες κάποιας Υπηρεσίας, ή ένας ήδη υπάρχων χρήστης να σας προσθέσει στην Υπηρεσία του.

Ε·Τ·S·D Ηλεκτρονική διαβίβαση ευαισθητης πληροφορίας Η εφαρμογή χρησιμοποιείται για τη διαβίβαση ευαίσθητης πληροφορίας

Κρυπτογραφημένη ανταλλαγή μηνυμάτων

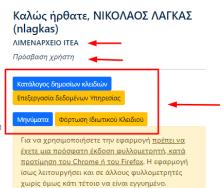
Η παρούσα εφαρμογή μπορεί να χρησιμοποιηθεί για τη μετάδοση μηνυμάτων που περιέχουν κρυπτογραφημένα δεδομένα μεταξύ Υπηρεσιών. Το πρότυπο OpenPGP χρησιμοποιείται για την κρυπτογράφηση των δεδομένων client-side μέσω της υλοποίησης OpenPGPjs . Αυτό σημαίνει ότι η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων πραγματοποιείται αποκλειστικά στους υπολογιστές των χρηστών και τα αποκρυπτογραφημένα δεδομένα δεν υποβάλλονται σε κανένα στάδιο στον server.

Σύμφωνα με τις αρχές της κρυπτογράφησης δημόσιου κλειδιού, οποιαδήποτε Υπηρεσία μπορεί να στείλει κρυπτογραφημένα μηνύματα, ωστόσο μόνο οι Υπηρεσίες που διαθέτουν εγκεκριμένο ζεύγος ιδιωτικού/δημόσιου κλειδιού μπορούν να λαμβάνουν αυτά τα κρυπτογραφημένα μηνύματα. Αυτό απαιτείται επειδή το δημόσιο κλειδί της Υπηρεσίες που δέχεται το μήνυμα

Διαχείριση κλειδιών

Χρησιμοποιώντας αυτήν την εφαρμογή, μπορείτε να δημιουργήσετε ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού για την Υπηρεσία σας. Το ιδιωτικό κλειδί θα κρυπτογραφηθεί με μια κωδική φράση. Τόσο το ιδιωτικό κλειδί όσο τοι διωτικό κλειδί όσο και η λέξη-κλειδί πρέπει να αποθηκεύονται από το χρήστη σε ασφαλές περιβάλλον. Κανένα από αυτά δεν στέλνεται ποτέ στον server. Το δημόσιο κλειδί θα υποβληθεί στο server και πρέπει να εγκριθεί από τους οιαχειριστές της εφαρμογής για χρήση. Μετά την έγκριστου δημόσιου κλειδιού μιας Υπηρεσίας, αυτή μπορεί να λαμβάνει μηνύματα με κρυπτογραφημένα δεδομένα.

Για να αποκρυπτογραφήσει γρήγορα τα δεδομένα της Υπηρεσίας του, ο χρήστης μπορεί να «φορτώσει» το ιδιωτικό κλειδί της συνεδρίας του. Αυτό σημαίνει ότι αυτό το κλειδί θα αποκρυπτογραφηθεί με τη κωδική φράση του και θα αποθηκευτεί στον browser του χρήστη για όσο διάστημα ο χρήστης είναι συνδεδεμένος στην εφαρμογή. Στη συνέχεια, το κλειδί αυτό θα χρησιμοποιηθεί για την αποκρυπτογράφηση των

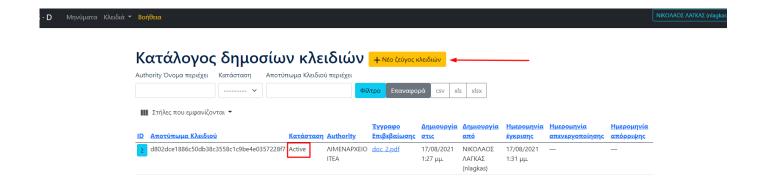


Αφού αντιστοιχηθείτε με κάποια Υπηρεσία, θα εμφανιστεί το μενού με τις λειτουργικότητες της εφαρμογής. Αν θέλετε η Υπηρεσία σας να λαμβάνει μηνύματα τότε θα πρέπει να δημιουργήσετε ένα νέο ζεύγος ιδιωτικού/δημόσιου κλειδιού και να το υποβάλλετε για έγκριση.

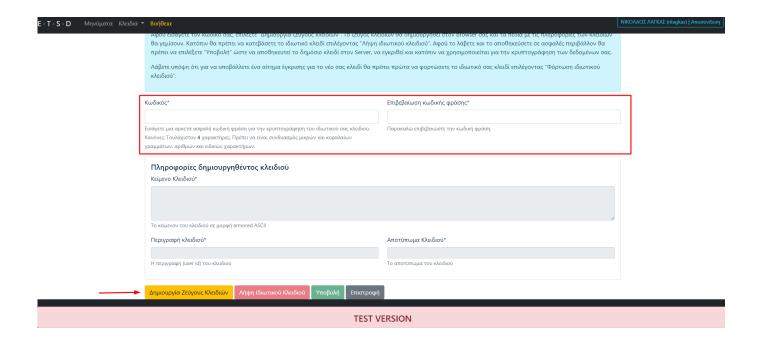
Δημιουργία ζεύγους κλειδιών



Για να δημιουργήσετε ένα ζεύγος κλειδιών, επιλέξτε **Κατάλογος Δημόσιων Κλειδιών** από έναν από τους 2 συνδέσμους όπως φαίνονται στην εικόνα.



Εδώ μπορείτε να δείτε όλα τα δημόσια κλειδιά που πιθανόν διαθέτει η Υπηρεσία σας. Μόνο ένα εξ αυτών θα είναι ενεργό. Για να δημιουργήσετε ένα **Νέο ζεύγος κλειδιών** επιλέξτε το αντίστοιχο κουμπί όπως φαίνεται στην εικόνα.

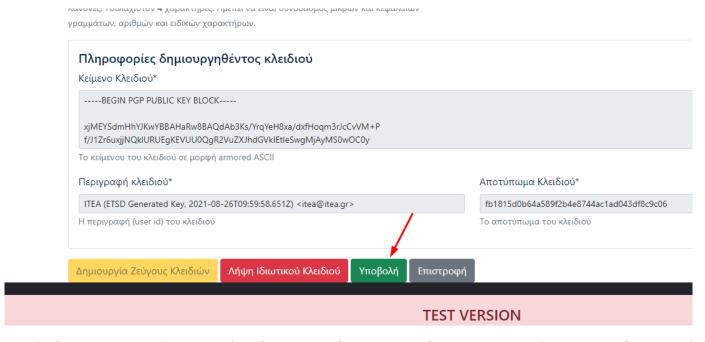


Σε αυτή τη φόρμα πρέπει να εισάγετε μια κατάλληλη κωδική φράση που θα χρησιμοποιηθεί για να κρυπτογραφήσει το ιδιωτικό σας κλειδί. Ακολουθήστε τις οδηγίες που σας παρέχονται και στη συνέχεια επιλέξτε **Δημιουργία ζεύγους κλειδιών** για να προχωρήσετε στη δημιουργία του ζεύγους κλειδιών στον browser σας.

ωδικός*	Επιβεβαίωση κωδικής φράσης*
	•••••
ισάγετε μια αρκετά ασφαλή κωδική φράση για την κρυπτογράφηση του ιδιωτικού σας κλειδιού. ανόνες: Τουλάχιστον 4 χαρακτήρες. Πρέπει να είναι συνδυασμός μικρών και κεφαλαίων ραμμάτων, αριθμών και ειδικών χαρακτήρων.	Παρακαλώ επιβεβαιώστε την κωδική φράση.
Πληροφορίες δημιουργηθέντος κλειδιού Κείμενο Κλειδιού*	
BEGIN PGP PUBLIC KEY BLOCK xjMEYSdmHhYJKwYBBAHaRw8BAQdAb3Ks/YrqYeH8xa/dxfHoqm3rJcCvVM+P f/J1Zr6uxjjNQkIURUEgKEVUUOQgR2VuZXJhdGVRIEtleSwgMjAyMS0wOCOy	•
Το κείμενου του κλειδιού σε μορφή armored ASCII	
Περιγραφή κλειδιού*	Αποτύπωμα Κλειδιού*
ITEA (ETSD Generated Key, 2021-08-26T09:59:58.651Z) <itea@itea.gr></itea@itea.gr>	fb1815d0b64a589f2b4e8744ac1ad043df8c9c06
Η περιγραφή (user id) του κλειδιού	Το αποτύπωμα του κλειδιού

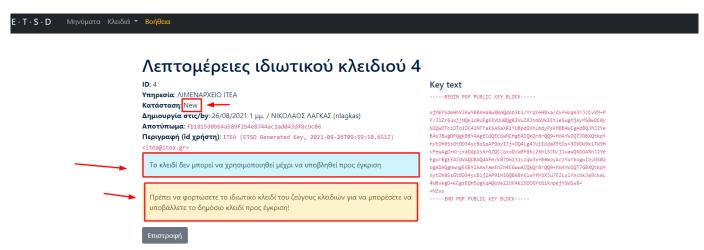
Στην συνέχεια το κουμπί **Λήψη Ιδιωτικού κλειδιού** θα ενεργοποιηθεί ώστε να μπορέσετε να αποθηκεύσετε το ιδιωτικό σας κλειδί. Το ιδιωτικό κλειδί που θα λάβετε, θα είναι κρυπτογραφημένο με τον κωδικό που εισήγατε και θα πρέπει να έχετε διαθέσιμα και τα δύο. Αν χάσετε ένα από αυτά, θα πρέπει να δημιουργήσετε νέο ζεύγος κλειδιών.

Να είστε ιδιαίτερα προσεκτικοί όταν λαμβάνετε το ιδιωτικό σας κλειδί. Είναι ένα αρχείο το οποίο πρέπει να χρησιμοποιείται μόνο για την αποκρυπτογράφηση των δεδομένων σας. Αν περιέλθει στην κατοχή τρίτου, σε συνδυασμό με την κωδική φράση σας, θα μπορεί να αποκρυπτογραφήσει τα δεδομένα σας. Συνιστάται να αποθηκεύσετε το ιδιωτικό σας κλειδί σε ασφαλές "περιβάλλον" και να καταγράψετε τον κωδικό σας σε διαφορετικό "περιβάλλον", ή ιδανικά να τον θυμάστε χωρίς να τον καταγράψετε κάπου.

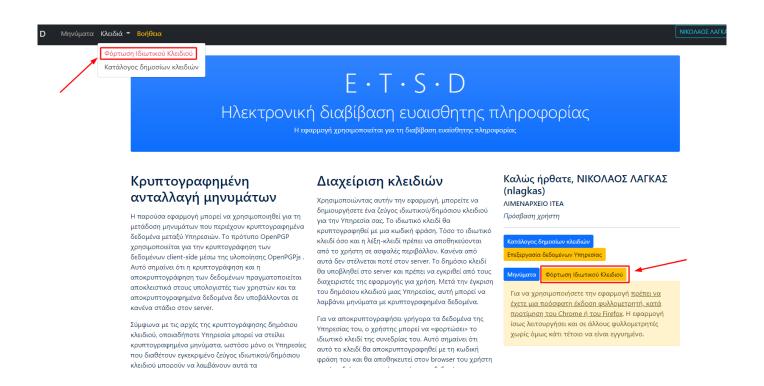


Αφού λάβετε το ιδιωτικό σας κλειδί, πρέπει να επιλέξετε **Υποβολή** για να αποθηκεύσετε το δημόσιο κλειδί που θα χρησιμοποιείται για να κρυπτογραφεί τα δεδομένα που αφορούν την Υπηρεσία σας στον server.

Έγκριση ζεύγους κλειδιών

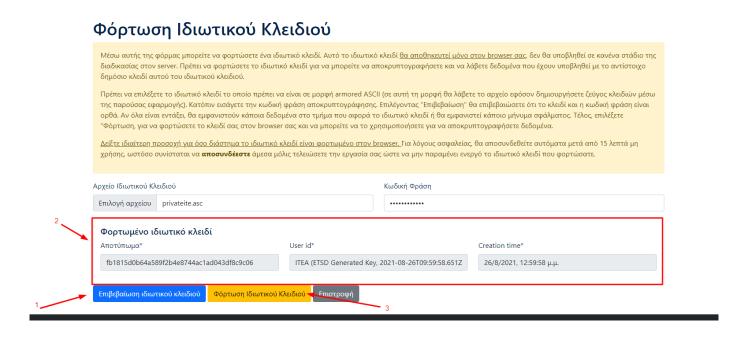


Το ζεύγος κλειδιών που μόλις δημιουργήσατε θα πρέπει να εγκριθεί προς χρήση. Για να εκκινήσετε την διαδικασία έγκρισης θα πρέπει πρώτα να φορτώσετε το ιδιωτικό κλειδί στον browser σας, επιλέγοντας **Φόρτωση Ιδιωτικού Κλειδιού** από έναν από τους 2 συνδέσμους όπως φαίνονται στην εικόνα.

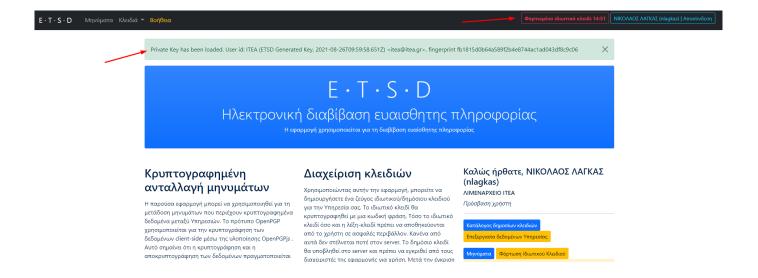


Φόρτωση Ιδιωτικού Κλειδιού Μέσω αυτής της φόρμας μπορείτε να φορτώσετε ένα ιδιωτικό κλειδί. Αυτό το ιδιωτικό κλειδί θα αποθηκευτεί μόνο στον browser σας, δεν θα υποβληθεί σε κανένα στάδιο της διαδικασίας στον server. Πρέπει να φορτώσετε το ιδιωτικό κλειδί για να μπορείτε να αποκρυπτογραφήσετε και να λάβετε δεδομένα που έχουν υποβληθεί με το αντίστοιχο δημόσιο κλειδί αυτού του ιδιωτικού κλειδιού. Πρέπει να επιλέξετε το ιδιωτικό κλειδί το οποίο πρέπει να είναι σε μορφή armored ASCII (σε αυτή τη μορφή θα λάβετε το αρχείο εφόσον δημιουργήσετε ζεύγος κλειδιών μέσω της παρούσας εφαρμογής). Κατόπιν εισάγετε την κωδική φράση αποκρυπτογράφησης. Επιλέγοντας "Επιβεβαίωση" θα επιβεβαιώσετε ότι το κλειδί και η κωδική φράση είναι ορθά. Αν όλα είναι εντάξει, θα εμφανιστούν κάποια δεδομένα στο τμήμα που αφορά το ιδιωτικό κλειδί ή θα εμφανιστεί κάποιο μήνυμα σφάλματος. Τέλος, επιλέξετε "Φόρτωση, για να φορτώσετε το κλειδί σας στον browser σας και να μπορείτε να το χρησιμοποιήσετε για να αποκρυπτογραφήσετε δεδομένα. Δείξτε ιδιαίτερη προσοχή για όσο διάστημα το ιδιωτικό κλειδί είναι φορτωμένο στον browser. Για λόγους ασφαλείας, θα αποσυνδεθείτε αυτόματα μετά από 15 λεπτά μη χρήσης, ωστόσο συνίσταται να **αποσυνδέεστε** άμεσα μόλις τελειώσετε την εργασία σας ώστε να μην παραμένει ενεργό το ιδιωτικό κλειδί που φορτώσατε. Αρχείο Ιδιωτικού Κλειδιού Κωδική Φράση Επιλογή αρχείου Δεν επιλέχθηκε κανένα αρχείο. Φορτωμένο ιδιωτικό κλειδί User id* Αποτύπωμα* Creation time* **Επιβεβαίωση ιδιωτικού κλειδιού** Φόρτωση Ιδιωτικού Κλειδιού **TEST VERSION**

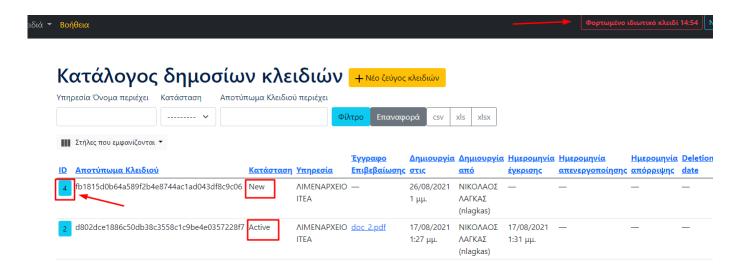
Για να φορτώσετε το κλειδί, επιλέξτε το αρχείο που περιέχει το ιδιωτικό σας κλειδί και εισάγετε την κωδική φράση στο αντίστοιχο πεδίο.



Στη συνέχεια επιλέξτε **Επιβεβαίωση ιδιωτικού κλειδιού** για να βεβαιωθείτε ότι το ιδιωτικό κλειδί αποκρυπτογραφήθηκε ορθά, βλέποντας τα στοιχεία του κλειδιού στο Φορτωμένο ιδιωτικό κλειδί όπως φαίνεται στην εικόνα. Τέλος επιλέξτε **Φόρτωση ιδιωτικού κλειδιού** για να μεταφορτωθεί το κλειδί στο session του browser σας.



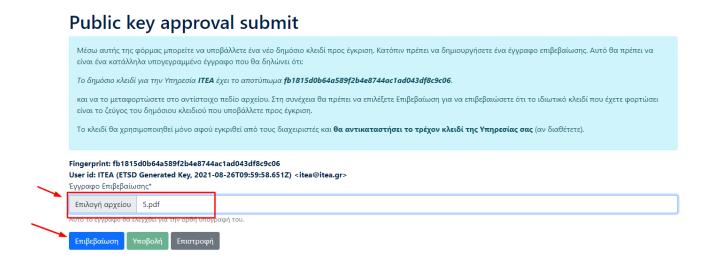
Ένα μήνυμα επιβεβαίωσης θα εμφανιστεί και πάνω δεξιά θα δείτε ένα κόκκινο πεδίο με ένα χρονόμετρο στη λήξη του οποίου το κλειδί θα αποδεσμευθεί από τον browser για λόγους ασφαλείας. Το χρονικό όριο των 15 λεπτών ανανεώνεται κάθε φορά που πραγματοποιείτε κάποια δραστηριότητα στην εφαρμογή.



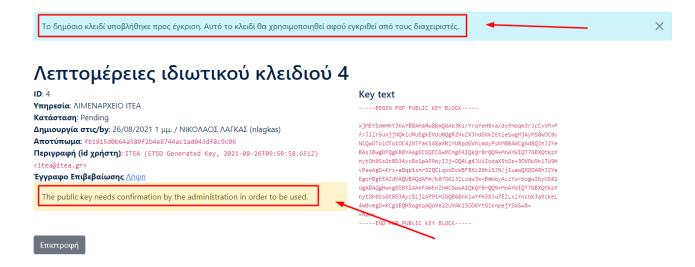
Αφού φορτώσετε το ιδιωτικό κλειδί, μπορείτε να υποβάλλετε το δημόσιο κλειδί στον server προς έγκριση. Για να το κάνετε επισκεφθείτε τον Κατάλογο δημοσίων κλειδιών και επιλέξτε το κλειδί που μόλις δημιουργήσατε επιλέγοντας το γαλάζιο πλαίσιο με το αντίστοιχο ID του κλειδιού.

Λεπτομέρειες ιδιωτικού κλειδιού 4 Υπηρεσία: ΛΙΜΕΝΑΡΧΕΙΟ ΙΤΕΑ -----BEGIN PGP PUBLIC KEY BLOCK-----Κατάσταση: New xjMEYSdmHhYJKwYBBAHaRw8BAQdAb3Ks/YrqYeH8xa/dxfHoqm3rJcCvVM+P Δημιουργία στις/by: 26/08/2021 1 μμ. / ΝΙΚΟΛΑΟΣ ΛΑΓΚΑΣ (nlagkas) f/J1Zr6uxjjNQk1URUEgKEVUU0QgR2VuZXJhdGVkIEtleSwgMjAyMS0w0C0y **Αποτύπωμα**: fb1815d0b64a589f2b4e8744ac1ad043df8c9c06 N1QwOTo1OTo1OC42NTFaKSA8aXR1YUBpdGVhLmdyPsKMBBAWCgAdBQJhJ2Ye BAsJBwgDFQgKBBYAAgECGQECGwMCHgEAIQkQrBrQQ9+MnAYWIQT7GBXQtkpY Περιγραφή (id χρήστη): ITEA (ETSD Generated Key, 2021-08-26T09:59:58.651Z) nytOh0SsGtBD34ycBoSpAP9oyIJj+OQ4Lg4JUiIodaX5tOs+3OVOW9k1TW9H <itea@itea.gr> PewAgD+Krz+aDqp1shrGZQCLqxoDcW8F8Xc26hiSJN/jIuawQXOOARhJ2Ye EgorBgEEAZdVAQUBAQdAFm/k0706131Lzqw3x+BmWoyAczYorbogwIbyUS02 Το κλειδί δεν μπορεί να χρησιμοποιηθεί μέχρι να υποβληθεί προς έγκριση ogADAQgHwngEGBYIAAkFAmEnZh4CGwwAIQkQrBrQQ9+MnAYWIQT7GBXQtkpY nytOhOSsGtBD34ycBlj2AP91HiGQB68nKlwYfH3XJu7EZLx1YncbkJa9ckeL 4W0vegD+KCgsEQH5ogKqAQoVe22UVAKi5006YtGiKnpejYSWSw8= Submit for approval ----END PGP PUBLIC KEY BLOCK-----Επιστροφή

Στη συνέχεια επιλέξτε **Υποβολή προς έγκριση** (Το αντίστοιχο κουμπί θα ενεργοποιηθεί μόνο αφού φορτωθεί το ιδιωτικό κλειδί).



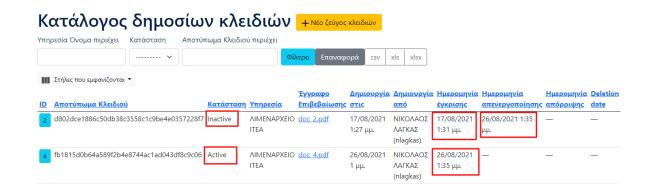
Στο επόμενο μενού, θα πρέπει να φορτώσετε ένα κατάλληλα και ηλεκτρονικά υπογεγραμμένο έγγραφο με το οποίο θα δηλώνετε ότι αυτό είναι το κλειδί που επιθυμείτε να χρησιμοποιηθεί για την Υπηρεσία σας. Αφού το επιλέξετε, πατήστε **Επιβεβαίωση** και εν συνεχεία **Υποβολή**.



Το αίτημα έγκρισής σας θα υποβληθεί στους διαχειριστές της εφαρμογής.



Εφόσον το εγκρίνουν, η Υπηρεσία σας θα μπορεί να λαμβάνει κρυπτογραφημένα δεδομένα,

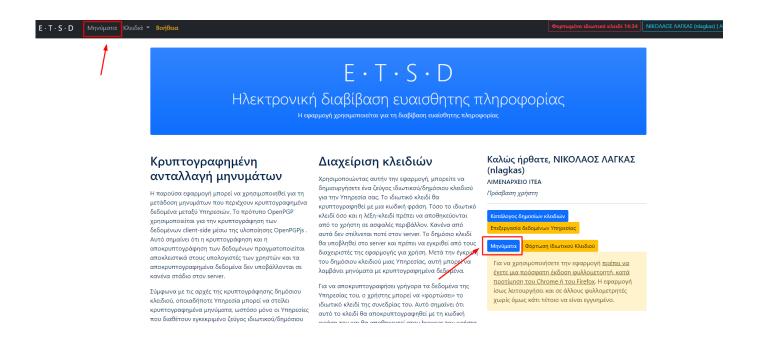


ενώ αν η Υπηρεσία σας διέθετε ήδη κάποιο κλειδί, αυτό θα καταστεί ανενεργό και εφεξής θα χρησιμοποιείται το νέο. **Ιδιαίτερη προσοχή πρέπει να δείξετε στο γεγονός ότι όσα μηνύματα έχετε λάβει με το παλιό κλειδί, αποκρυπτογραφούνται με το αντίστοιχο παλιό ιδιωτικό κλειδί και κωδικό.** Οπότε αν θέλετε να έχετε πρόσβασή στα παλιά σας δεδομένα θα πρέπει να διαθέτετε όλα τα παλιά κλειδιά σας καθώς και τους αντίστοιχους κωδικούς.

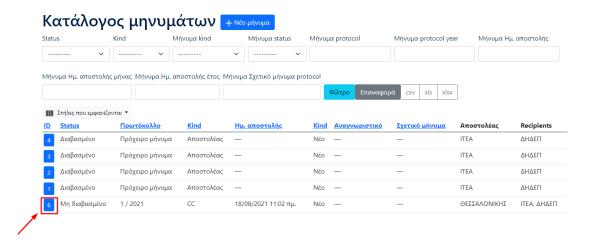
Κρυπτογραφημένη ανταλλαγή μηνυμάτων

Χρησιμοποιώντας αυτή την εφαρμογή μπορείτε να ανταλλάξετε μηνύματα μεταξύ Υπηρεσιών Όλα τα δεδομένα των μηνυμάτων είναι κρυπτογραφημένα χρησιμοποιώντας κρυπτογράφηση δημόσιου κλειδιού: Το δημόσιο κλειδί της Υπηρεσίας που θα λάβει το μήνυμα χρησιμοποιείται για την κρυπτογράφηση. Στη συνέχεια, αυτή η Υπηρεσία θα χρησιμοποιήσει το ιδιωτικό της κλειδί για την αποκρυπτογράφηση. Όλες οι διαδικασίες κρυπτογράφησης/αποκρυπτογράφησης γίνονται browser-side που σημαίνει ότι τα ιδιωτικά κλειδιά των Υπηρεσιών και τα μη κρυπτογραφημένα δεδομένα δεν φθάνουν ποτέ στον server.

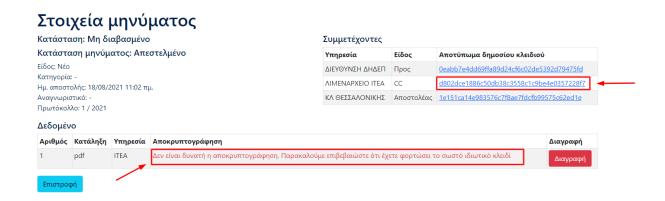
Προβολή μηνυμάτων



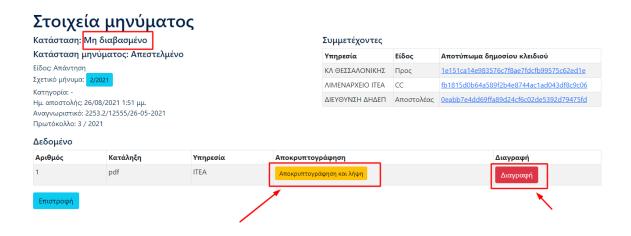
Επιλέξτε **Μηνύματα** από έναν από τους 2 συνδέσμους όπως φαίνονται στην εικόνα για να μεταφερθείτε στον Κατάλογο Μηνυμάτων όπου μπορείτε να δείτε όλα τα μηνύματα που αφορούν την Υπηρεσία σας (είτε ως αποστολέας είτε ως παραλήπτης). Τα μηνύματα εξ' ορισμού κατηγοριοποιούνται ανά κατάσταση: Πρώτα τα Μη Αναγνωσμένα (ή Μη Απεσταλμένα), μετά τα Αναγνωσμένα και μετά τα αρχειοθετημένα. Μπορείτε να φιλτράρετε/αναζητήσετε μηνύματα από τα εργαλεία φιλτραρίσματος της σελίδας. Μηνύματα με όμοια κατάσταση θα κατηγοριοποιούνται ανά ημερομηνία αποστολής.



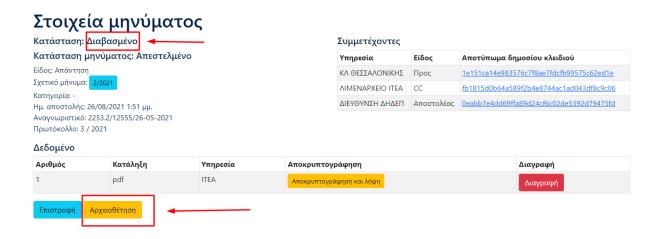
Επιλέγοντας το μπλε κουμπί με το id κάθε μηνύματος, μπορείτε να δείτε περαιτέρω λεπτομέρειες για αυτό.



Υπόψιν ότι δεν μπορείτε να δείτε τα δεδομένα του μηνύματος πάρα μόνο εφόσον πραγματοποιήσετε Φόρτωση Ιδιωτικού κλειδιού για την Υπηρεσία σας και για το χρησιμοποιηθέν δημόσιο κλειδί.

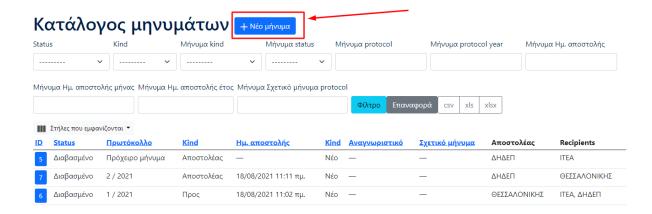


Αφού φορτώσετε το σωστό ιδιωτικό κλειδί θα μπορείτε να **λάβετε και να αποκρυπτογραφήσετε** τα δεδομένα του μηνύματος, ενώ αν το επιθυμείτε μπορείτε να τα διαγράψετε.

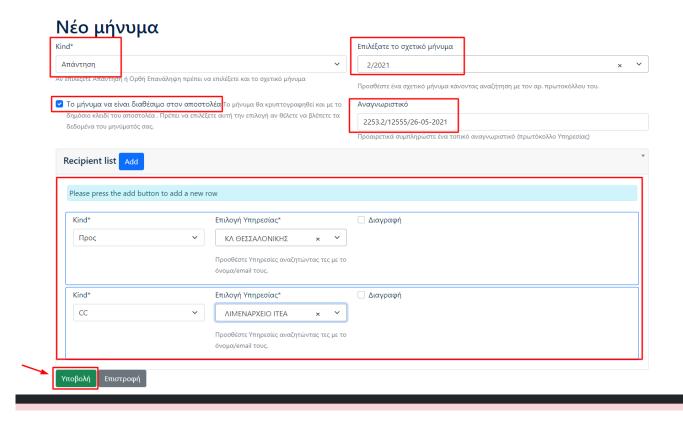


Όταν όλα τα δεδομένα του μηνύματος έχουν ληφθεί και αποκρυπτογραφηθεί, η κατάσταση του μηνύματος θα αλλάξει σε "Διαβασμένο". Ένα "Διαβασμένο" μήνυμα μπορεί να αρχειοθετηθεί επιλέγοντας **Αρχειοθέτηση**. Ένα "Αρχειοθετημένο" μήνυμα απλώς θα μετακινηθεί στο τέλος της λίστας μηνυμάτων. Μπορείτε να σημάνετε ένα "Αρχειοθετημένο" μήνυμα ξανά ως "Αναγνωσμένο".

Αποστολή μηνυμάτων



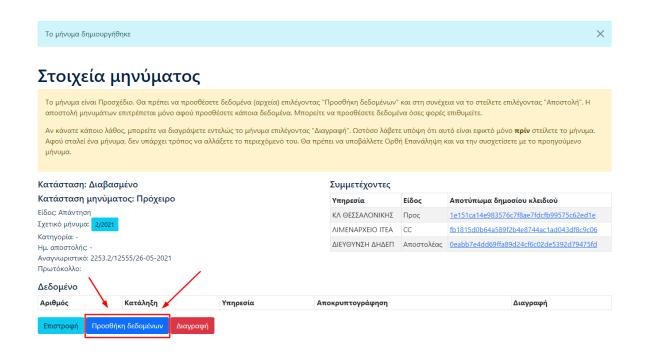
Για την αποστολή ενός κρυπτογραφημένου μηνύματος, πρέπει να επισκεφθείτε τον Κατάλογο μηνυμάτων και να επιλέξετε **Νέο μήνυμα**.



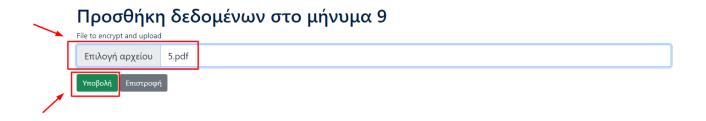
Το μήνυμα μπορεί να είναι "Νέο" (Μη σχετιζόμενο με κάποιο άλλο μήνυμα), "Απάντηση" σε ένα υπάρχον μήνυμα ή "Ορθή Επανάληψη" ενός υπάρχοντος μηνύματος. Αν επιλέξετε "Απάντηση" ή "Ορθή Επανάληψη" θα πρέπει να επιλέξετε και το σχετικό μήνυμα. Αν ενεργοποιηθεί η επιλογή "Το μήνυμα να είναι διαθέσιμο στον αποστολέα", τα δεδομένα του μηνύματος θα κρυπτογραφηθούν και για τον αποστολέα και θα αποθηκευτούν στον server ώστε να είναι διαθέσιμα για αποκρυπτογράφηση με το ιδιωτικό του κλειδί. Αν ο αποστολέας δεν διαθέτει εγκεκριμένο δημόσιο κλειδί, αυτή η επιλογή δεν είναι διαθέσιμη. Προαιρετικά μπορείτε να προσθέσετε ένα Αναγνωριστικό (πχ το υπηρεσιακό πρωτόκολλο του Εγγράφου) για να αναγνωρίζετε το μήνυμα καθώς για λόγους προστασίας δεδομένων δεν επιτρέπεται να

προσθέσετε κάποιον τίτλο στο μήνυμα. Το αναγνωριστικό δέχεται μόνο αριθμούς και τους χαρακτήρες / - .

Για να προσθέσετε κάποιον αποδέκτη, επιλέξτε Προσθήκη και συμπληρώστε την Υπηρεσία από τη λίστα αυτόματης συμπλήρωσης και αν είναι "Προς" ή "CC" (κοινοποίηση). Μόνο Υπηρεσίες που διαθέτουν Δημόσιο κλειδί είναι διαθέσιμες προς επιλογή. Μπορείτε να προσθέσετε όσους αποδέκτες επιθυμείτε. Όταν τελειώσετε επιλέξτε **Υποβολή**.

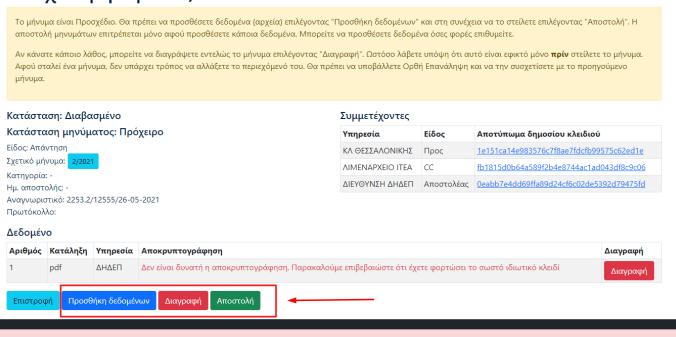


Κατόπιν θα πρέπει να προσθέσετε τα δεδομένα στο μήνυμα επιλέγοντας Προσθήκη Δεδομένων.



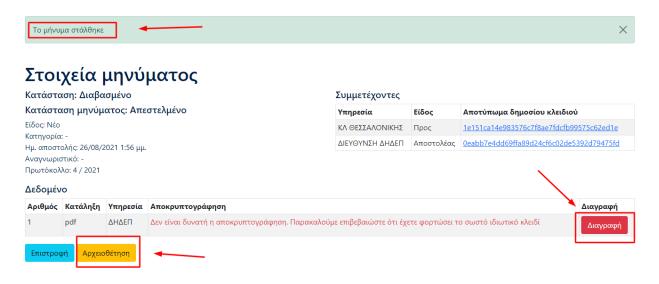
Σε αυτή τη φόρμα απλώς επιλέξτε (ή σύρετε) το αρχείο που θέλετε και στη συνέχεια επιλέξτε **Υποβολή**. Θα εμφανιστεί ένα αναδυόμενο μήνυμα το οποίο θα σας ενημερώσει ότι το αρχείο σας έχει μεταφορτωθεί.

Στοιχεία μηνύματος



Μπορείτε να προσθέσετε κι άλλα αρχεία ή να επιλέξετε Επιστροφή για να κλείσετε τη φόρμα και να επιστρέψετε στο κύριο μενού προβολής του μηνύματος. Αφού προσθέσετε τα δεδομένα στο μήνυμα, μπορείτε να το στείλετε επιλέγοντας Αποστολή. Η αποστολή είναι εφικτή μόνο αφού προσθέσετε δεδομένα στο αρχείο. Επιπρόσθετα, πριν αποστείλετε το μήνυμα, μπορείτε να το διαγράψετε εξολοκλήρου μαζί με όσα δεδομένα έχετε προσθέσει επιλέγοντας Διαγραφή. Δεν είναι δυνατή η διαγραφή κάποιου μηνύματος το οποίο έχει ήδη αποσταλεί.

TECT VEDGLONI



Αφού στείλετε το μήνυμα θα δείτε ένα μήνυμα επιβεβαίωσης. Κατόπιν μπορείτε να κάνετε όλες τις ενέργειες που μπορείτε να κάνετε και σε ένα 'Διαβασμένο' μήνυμα (Αρχειοθέτηση, Διαραφή δεδομένων κτλ).

Επεξεργασία δεδομένων Υπηρεσίας



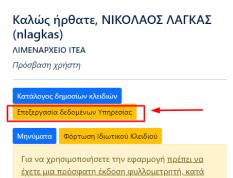
Κρυπτογραφημένη ανταλλαγή μηνυμάτων

Η παρούσα εφαρμογή μπορεί να χρησιμοποιηθεί για τη μετάδοση μηνυμάτων που περιέχουν κρυπτογραφημένα δεδομένα μεταξύ Υπηρεσιών. Το πρότυπο OpenPGP χρησιμοποιείται για την κρυπτογράφηση των δεδομένων client-side μέσω της υλοποίησης OpenPGPjs . Αυτό σημαίνει ότι η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων πραγματοποιείται αποκλειστικά στους υπολογιστές των χρηστών και τα αποκρυπτογραφημένα δεδομένα δεν υποβάλλονται σε κανένα στάδιο στον server.

Επεξεργασία δεδομένων Υπηρεσίας

Διαχείριση κλειδιών

Χρησιμοποιώντας αυτήν την εφαρμογή, μπορείτε να δημιουργήσετε ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού για την Υπηρεσία σας. Το ιδιωτικό κλειδί θα κρυπτογραφηθεί με μια κωδική φράση. Τόσο το ιδιωτικό κλειδί όσο και η λέξη-κλειδί πρέπει να αποθηκεύονται από το χρήστη σε ασφαλές περιβάλλον. Κανένα από αυτά δεν στέλνεται ποτέ στον server. Το δημόσιο κλειδί θα υποβληθεί στο server και πρέπει να εγκριθεί από τους διαχειριστές της εφαρμογής για χρήση. Μετά την έγκριση του δημόσιου κλειδιού μιας Υπηρεσίας, αυτή μπορεί να λαμβάνει μηνύματα με κρυπτογραφημένα δεδομένα.



Επιλέγοντας **Επεξεργασία δεδομένων Υπηρεσίας** μπορείτε να επεξεργαστείτε τους ενεργούς χρήστες και το email της Υπηρεσίας σας.

Επίλογή χρηστών | ΚΙΚΟΛΑΟΣ ΛΑΓΚΑΣ (nlagkas) | Χ Υ | | Μπορείτε να αφαιρέσετε χρήστες με το "χ" δίπλα στο όνομα τους ή να προσθέσετε περισσότερους αναζητώντας τους με το username/επιθέτο/email τους. | Email | | itea@itea.gr

Μπορείτε να αφαιρέσετε χρήστες με το "x" δίπλα στο όνομα τους ή να προσθέσετε περισσότερους αναζητώντας τους με το username/επίθετο/email τους. Όταν τελειώσετε επιλέξτε **Υποβολή**.

Πρόσβαση Διαχειριστών



Κρυπτογραφημένη ανταλλαγή μηνυμάτων

Η παρούσα εφαρμογή μπορεί να χρησιμοποιηθεί για τη μετάδοση μηνυμάτων που περιέχουν κρυπτογραφημένα δεδομένα μεταξύ Υπηρεσιών. Το πρότυπο OpenPGP χρησιμοποιείται για την κρυπτογράφηση των δεδομένων client-side μέσω της υλοποίησης OpenPGPjs. Αυτό σημαίνει ότι η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων πραγματοποιείται αποκλειστικά στους υπολογιστές των χρηστών και τα αποκρυπτογραφημένα δεδομένα δεν υποβάλλονται σε κανένα στάδιο στον server.

Σύμφωνα με τις αρχές της κρυπτογράφησης δημόσιου κλειδιού, οποιαδήποτε Υπηρεσία μπορεί να στείλει κρυπτογραφημένα μηνύματα, ωστόσο μόνο οι Υπηρεσίες που διαθέτουν εγκεκριμένο ζεύγος ιδιωτικού/δημόσιου κλειδιού μπορούν να λαμβάνουν αυτά τα

Διαχείριση κλειδιών

Χρησιμοποιώντας αυτήν την εφαρμογή, μπορείτε να δημιουργήσετε ένα ζεύγος ιδιωτικού/δημόσιου κλειδιού για την Υπηρεσία σας. Το ιδιωτικό κλειδί θα κρυπτογραφηθεί με μια κωδική φράση. Τόσο το ιδιωτικό κλειδί όσο και η λέξη-κλειδί πρέπει να αποθηκεύονται από το χρήστη σε ασφαλές περιβάλλον. Κανένα από αυτά δεν στέλνεται ποτέ στον server. Το δημόσιο κλειδί θα υποβληθεί στο server και πρέπει να εγκριθεί από τους διαχειριστές της εφαρμογής για χρήση. Μετά την έγκριτη του δημόσιου κλειδιού μιας Υπηρεσίας, αυτή μπορεί να λαμβάνει μηνύματα με κρυπτογραφημένα δεδομένα.

Για να αποκρυπτογραφήσει γρήγορα τα δεδομένα της Υπηρεσίας του, ο χρήστης μπορεί να «φορτώσει» το ιδιωτικό κλειδί της συνεδρίας του. Αυτό σημαίνει ότι αυτό το κλειδί θα αποκρυπτογραφηθεί με τη κωδική φράση του και θα αποθρυπτογραφηθεί με τη νωδική του βράση του και θα αποθρυπτογραφηθεί με το χρήστη



Πρόσβαση <u>διαχειριστή</u> και χρήστη

Κατάλογος δημοσίων κλειδιών
Επεξεργασία δεδομένων Υπηρεσίας
Μαγώνατα (Φάρτωση Ιδιωτικού Κλειδ

ατα Υπηρεσίες

Για να χρησιμοποιήσετε την εφαρμογή <u>πρέπει να</u> έχετε μια <u>πρόσφατη έκδοση φυλλομετρητή, κατά</u> <u>προτίμηση του Chrome ή του Firefox</u>. Η εφαρμογή ίσως λειτουργήσει και σε άλλους φυλλομετρητές χωρίς όμως κάτι τέτοιο να είναι εγγυημένο.

Οι διαχειριστές έχουν δύο επιπλέον λειτουργικότητες από τους απλούς χρήστες, στις οποίες έχουν πρόσβαση επιλέγοντας **Όλα τα μηνύματα** και **Υπηρεσίες**.

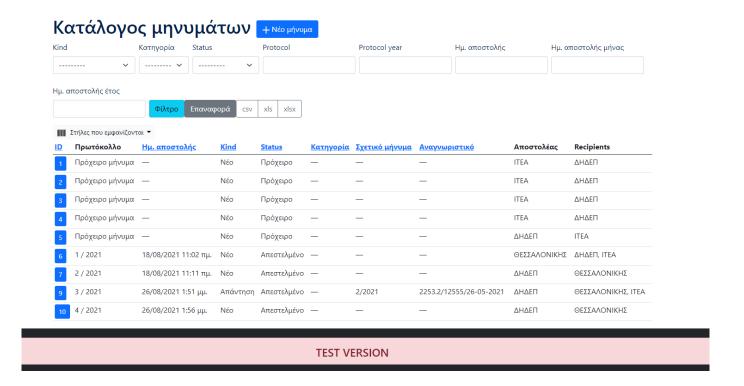
Ε·Τ·S·D Μηνύματα Κλειδιά ▼ Βοήθεια

Κατάλογος Υπηρεσίών

ΛΙΜΕΝΑΡΧΕΙΟ ΙΤΕΑ Εμφάνιση Επεξεργασία Επεξεργασία χρηστών
 ΔΙΕΥΘΥΝΣΗ ΔΗΔΕΠ Εμφάνιση Επεξεργασία Επεξεργασία χρηστών
 ΚΛ ΘΕΣΣΑΛΟΝΙΚΗΣ Εμφάνιση Επεξεργασία Επεξεργασία χρηστών

Δημιουργία

Επιλέγοντας **Υπηρεσίες** έχουν πρόσβαση σε όλες τις Υπηρεσίες τις εφαρμογής, ώστε να προσθαφαιρέσουν χρήστες, να τροποποιήσουν στοιχεία των Υπηρεσιών αλλά και να δημιουργήσουν νέες Υπηρεσίες που χρησιμοποιούν την εφαρμογή.



Επιλέγοντας **Όλα τα μηνύματα** έχουν πρόσβαση σε όλα τα μηνύματα όλων των Υπηρεσιών. Σημειώνεται ότι οι διαχειριστές μπορούν να ελέγξουν τα διακινούμενα μηνύματα άλλα δεν έχουν πρόσβαση στα κρυπτογραφημένα δεδομένα, παρά μόνο σε αυτά που αφορούν την δική τους Υπηρεσία.