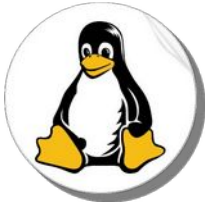
GreekLUG

Ελεύθερο Λογισμικό &



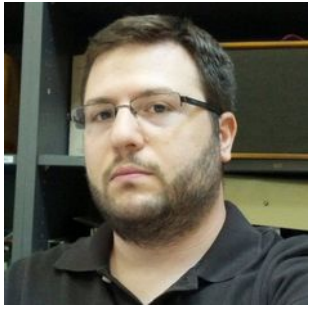
Λογισμικό Ανοικτού Κώδικα

OpenPGP σε Thunderbird για κρυπτογραφημένα ή/και υπογεγραμμένα μηνύματα

Ζήσης Μιχάλης, GreekLUG

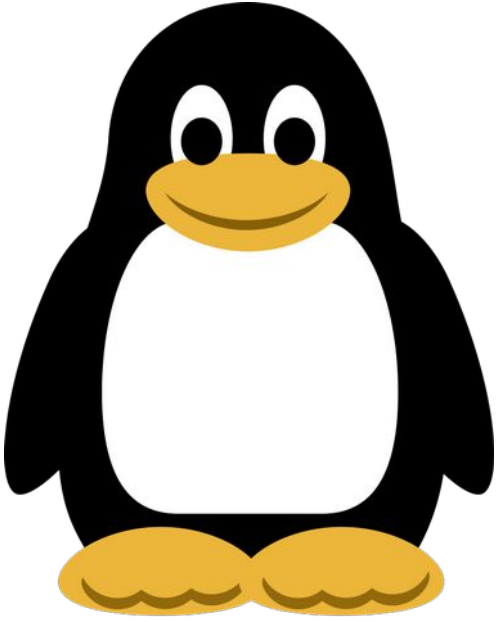
OpenPGP σε Thunderbird

whoami



~/Ζήσης Μιχάλης | System Administrator

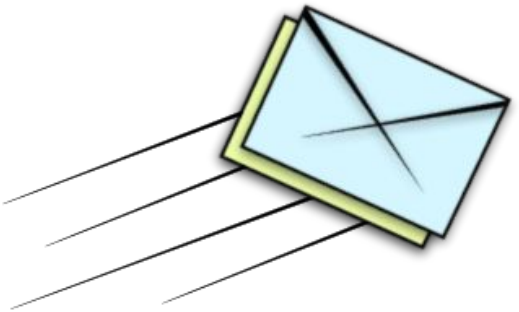
- Μέλος της κοινότητας ΕΛ/ΛΑΚ από περίπου το 2010
- Μέλος του GreekLUG (ΔΣ)



OpenPGP σε Thunderbird

Περιεχόμενα

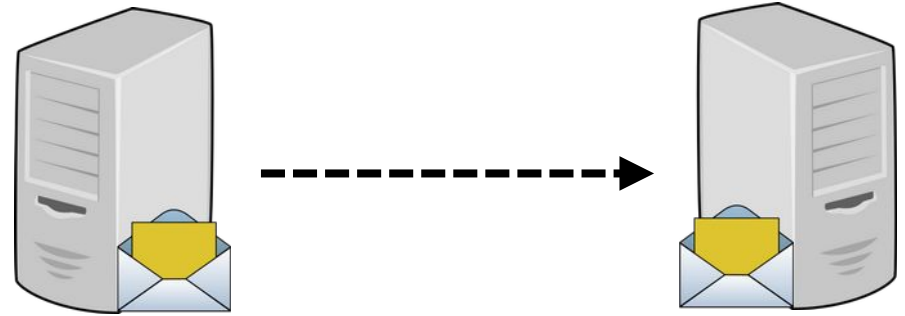
1) Λίγα λόγια για την κρυπτογράφηση & ασφαλή επικοινωνία
2) Mozilla Thunderbird και OpenPGP
3) Πως το χρησιμοποιώ, παράδειγμα χρήσης



Κρυπτογράφηση επικοινωνίας

Η τυπική διαδρομή… ενός email

[2]
- **Έλεγχοι**
- **Αποθήκευση στα “Απεσταλμένα”**
- **Εξερχόμενη αποστολή SMTP**



[3]
- **Παραλαβή μηνύματος**
- **έλεγχοι (πχ φίλτρο spam)**
- **Αποθήκευση στα “Εισερχόμενα”**

[1]
- **Σύνταξη**
- **Αποστολή μέσω SMTP**

[4]
- **Λήψη μηνύματος μέσω POP3/IMAP**
- **Ανάγνωση**

Κρυπτογράφηση επικοινωνίας

Η **κρυπτογράφηση επικοινωνίας** διασφαλίζει ότι τα δεδομένα που ανταλλάσουμε με τρίτους μεταφέρονται μέσω **ασφαλών καναλιών επικοινωνίας** (κρυπτογράφηση σύνδεσης) ή και σε **κρυπτογραφημένη μορφή** (κρυπτογράφηση μηνυμάτων).

Στο παρελθόν η επικοινωνία μέσω διαδικτύου γίνονταν συνήθως χωρίς κρυπτογράφηση, ωστόσο με τις νεότερες τεχνολογίες παρακολούθησης/δυνατοτήτων παραβίασης, υπήρξαν πολλαπλές υποθέσεις παραβίασης.

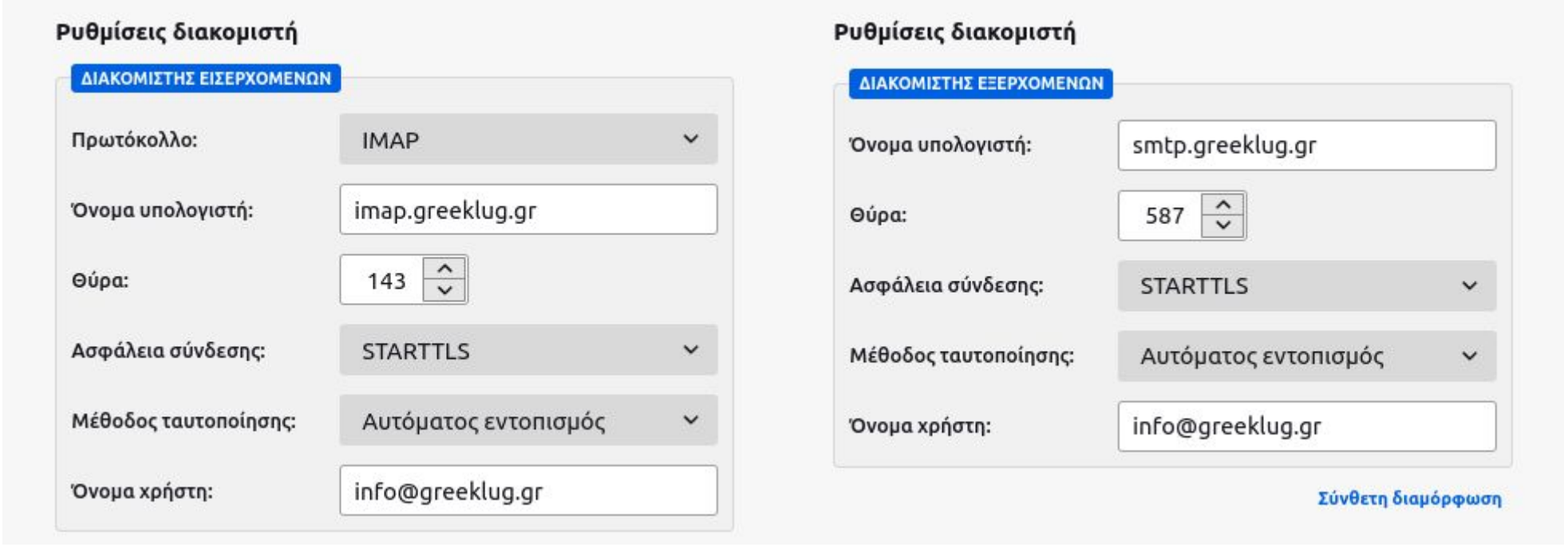
Ενδεικτικό παράδειγμα ήταν η πλοήγηση στο διαδίκτυο, η οποία πραγματοποιούνταν μέσω του πρωτοκόλλου HTTP (πόρτα 80). Η πρόσβαση σε ιστοσελίδες, ειδικά σε αυτές που υπήρχε σύνδεση χρηστών με όνομα χρήστη και κωδικό, μπορούσε να αναγνωστεί με διάφορες τεχνικές, με αποτέλεσμα κακόβουλοι χρήστες να μπορούν να πάρουν πρόσβαση σε λογαριασμούς ή και να καταγράψουν ευαίσθητα δεδομένα, όπως στοιχεία πιστωτικών καρτών.

Το παραπάνω ισχύει και για όλα τα γνωστά πρωτόκολλα επικοινωνίας, όπως και τα IMAP/POP3 /SMTP για την αποστολή και παραλαβή αλληλογραφίας.

Για την εξασφάλιση της επικοινωνίας τα πρωτόκολλα υποστηρίζουν την χρήση κρυπτογράφησης. Αυτή αναφέρεται συνήθως ως Secure Sockets Layer (**SSL**) ή Transport Layer Security (**TLS**).

Κρυπτογράφηση επικοινωνίας

Ενδεικτικές ρυθμίσεις αλληλογραφίας στην εφαρμογή Thunderbird:



Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Σύνδεσης

Κρυπτογράφηση επικοινωνίας

Χρήστης Α

Μη κρυπτογραφημένη Επικοινωνία

Κείμενο

Χρήστης Β

Κρυπτογράφηση Σύνδεσης

Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Σύνδεσης

Χρήστης Α

Μη κρυπτογραφημένη Επικοινωνία

Κείμενο

Χρήστης Β

Χρήστης Α

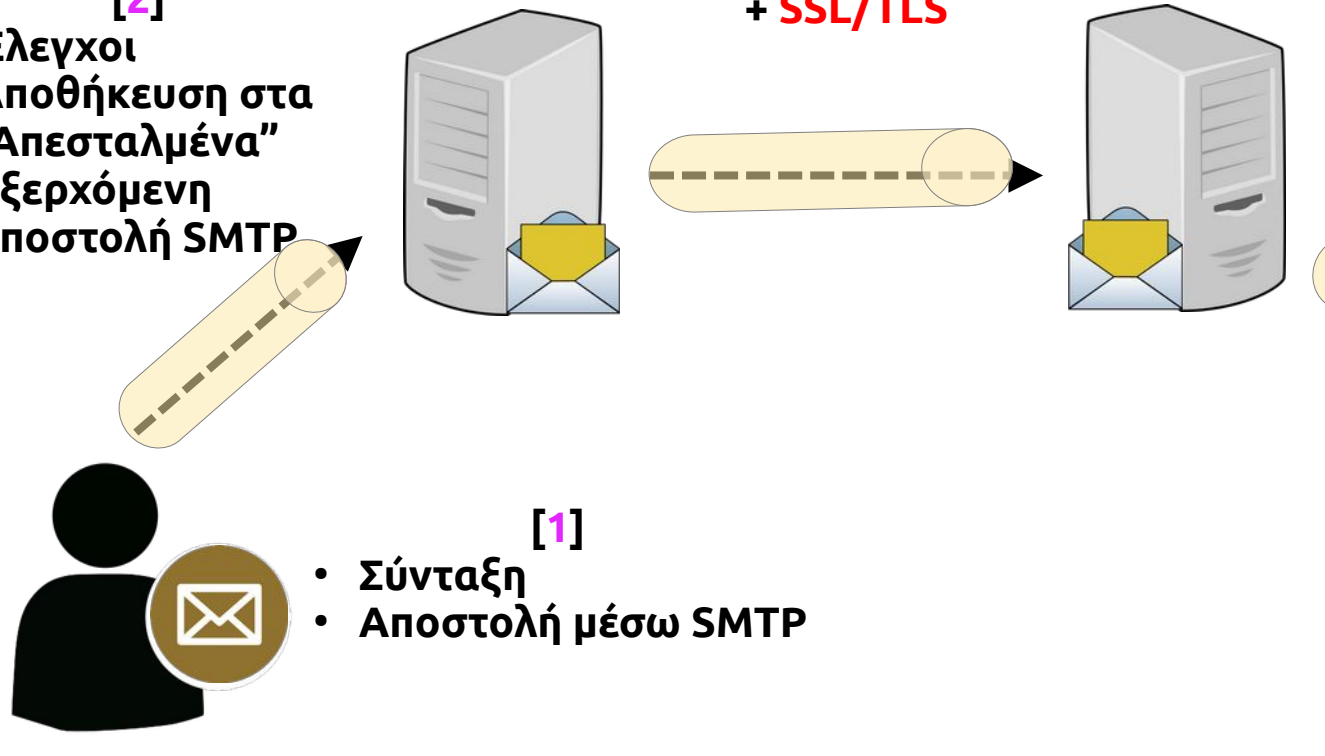
Κρυπτογραφημένη Επικοινωνία με SSL/TLS

Κείμενο

Χρήστης Β

Κρυπτογράφηση επικοινωνίας

Η τυπική διαδρομή… ενός email
+ SSL/TLS



[1]
- **Σύνταξη**
- **Αποστολή μέσω SMTP**

[2]
- **Έλεγχοι**
- **Αποθήκευση στα “Απεσταλμένα”**
- **Εξερχόμενη αποστολή SMTP**

[3]
- **Παραλαβή μηνύματος**
- **έλεγχοι (πχ φίλτρο spam)**
- **Αποθήκευση στα “Εισερχόμενα”**

[4]
- **Λήψη μηνύματος μέσω POP3/IMAP**
- **Ανάγνωση**

Κρυπτογράφηση επικοινωνίας

OpenPGP

Η κρυπτογράφησης **OpenPGP** αποτελεί ένα μη-ιδιοταγές πρότυπο,
το οποίο χρησιμοποιεί την μέθοδο δημοσίου κλειδιού ώστε να κρυπτογραφήσει

- δεδομένα ή
- την ταυτότητα

των χρηστών.

Βασίζεται στο παλαιότερο και ιδιοταγές λογισμικό PGP (Pretty Good Privacy).

Υπάρχουν υλοποιήσεις του σε διάφορα λογισμικά και λειτουργικά συστήματα, είτε ως εγγενείς υποστήριξη, είτε με την μορφή προσθέτων.

https://www.openpgp.org/software/

Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση μηνυμάτων με την μέθοδο δημοσίου κλειδιού
Κάθε χρήστης έχει το δικό του κλειδί, που αποτελείται από δύο τμήματα:
•ένα **ιδιωτικό**
•ένα **δημόσιο**

Σημεία κρυπτογράφησης:
•Κείμενο
•Υπογραφή

Κείμενο
I Love Free Software Day! - 14/02/2023

Κείμενο με κρυπτογράφηση
-----BEGIN PGP MESSAGE-----
wcFMA0JrV2MGhiq6AQ9G0hd4Af2nFDsUNuMhDQw2lstu3JZdSqk0lQ8NvwRuMYeYG9ZtF8dpSqLy
DePuP6OhguL6gK+vGmrCuC6FFTy1EYovEB4qPc1IntcrBInDvTu7vy7wXsE+wp8Hpy2YGsHp3...
-----END PGP MESSAGE-----

Κρυπτογράφηση επικοινωνίας

Βήματα κρυπτογράφησης δημοσίου κλειδιού

•Ο **Χρήστης Α** θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον **Χρήστη Β**
•Ο **Χρήστης Α** κρυπτογραφεί το απλό κείμενο με το δημόσιο κλειδί του **Χρήστη Β** και στέλνει το μήνυμα
•Ο **Χρήστης Β** λαμβάνει το μήνυμα και αποκρυπτογραφεί το κωδικοποιημένο κείμενο με το ιδιωτικό κλειδί του
•Τρίτοι χρήστες βλέπουν μόνο το **κωδικοποιημένο** κείμενο

Σημαντικό
Το ιδιωτικό κλειδί παραμένει στον εκάστοτε χρήστη και δεν διαμοιράζεται

* Ο **Χρήστης Α** θα πρέπει να γνωρίζει το δημόσιο κλειδί του **Χρήστη Β** για να μπορέσει να επικοινωνήσει μαζί του

Κρυπτογράφηση επικοινωνίας

Βήματα ψηφιακής υπογραφής δημοσίου κλειδιού

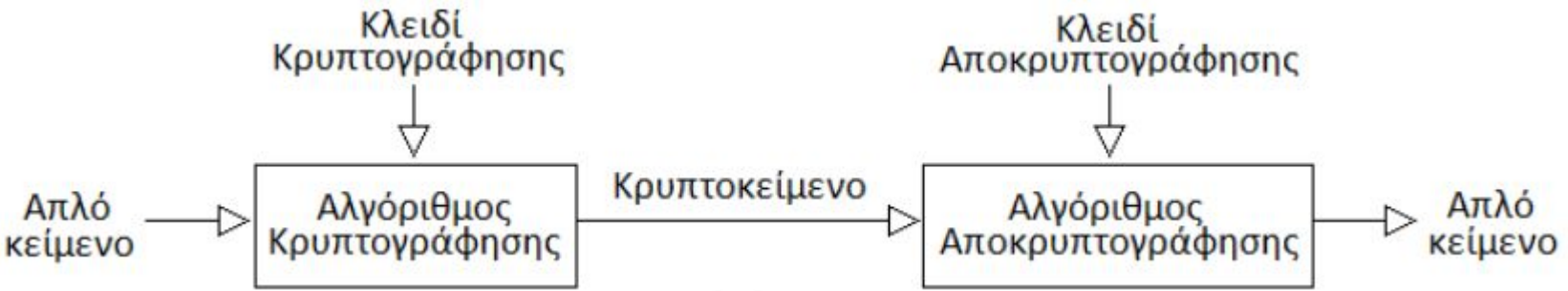
•Ο **Χρήστης Α** θέλει να στείλει ένα μήνυμα, ψηφιακά υπογεγραμμένο, στον **Χρήστη Β**
•Ο **Χρήστης Α** υπογράφει το μήνυμα με το ιδιωτικό κλειδί του και στέλνει το μήνυμα
•Ο **Χρήστης Β** λαμβάνει το μήνυμα και χρησιμοποιεί το δημόσιο κλειδί του **Χρήστη Α** για να επιβεβαιώσει ότι το μήνυμα στάλθηκε από αυτόν

Σημαντικό
Η υπογραφή εξαρτάται από το περιεχόμενο του μηνύματος. Εάν αυτό τροποποιηθεί τότε η εγκυρότητα της υπογραφής δεν ισχύει

* Ο **Χρήστης Β** θα πρέπει να γνωρίζει το δημόσιο κλειδί του **Χρήστη Α** για να μπορέσει να επιβεβαιώσει την εγκυρότητα του μηνύματος

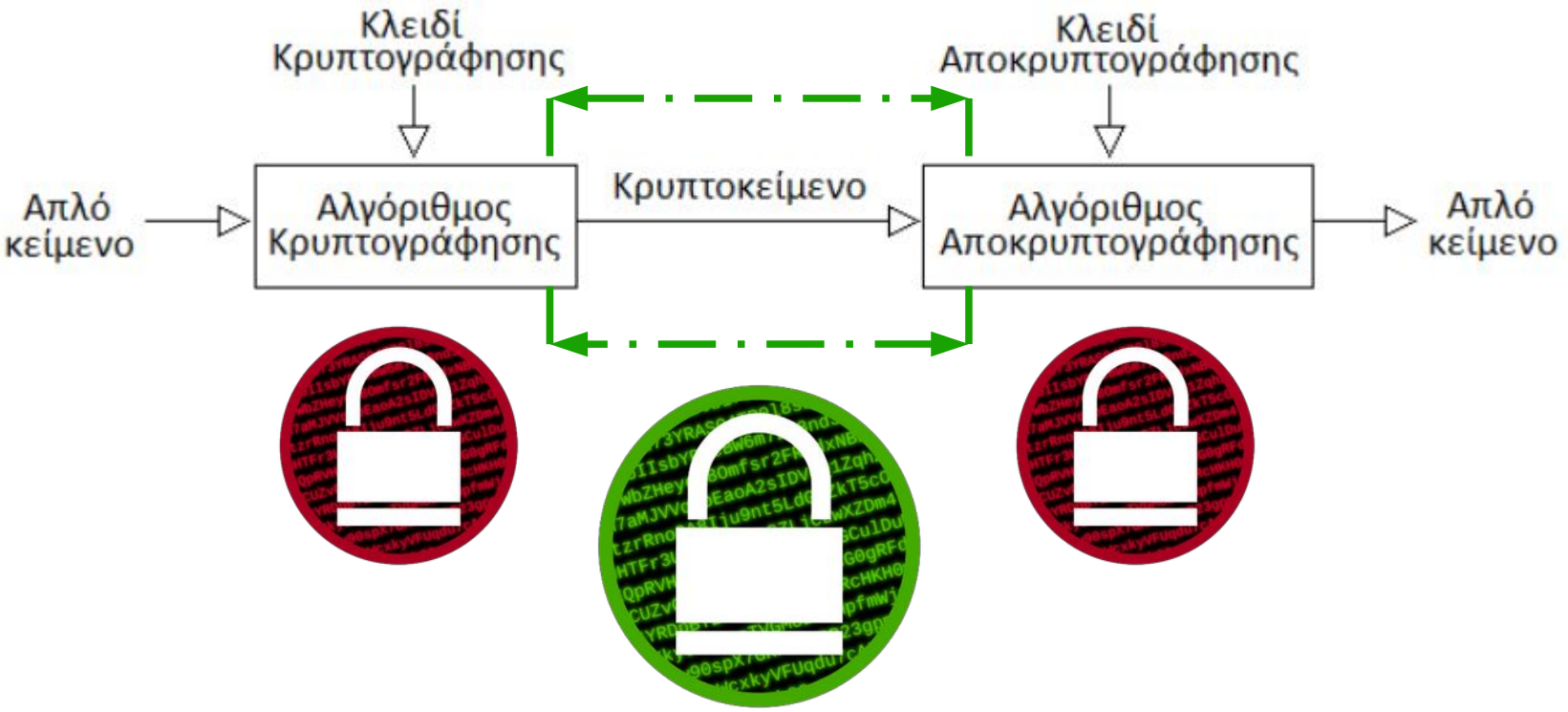
Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Μηνυμάτων



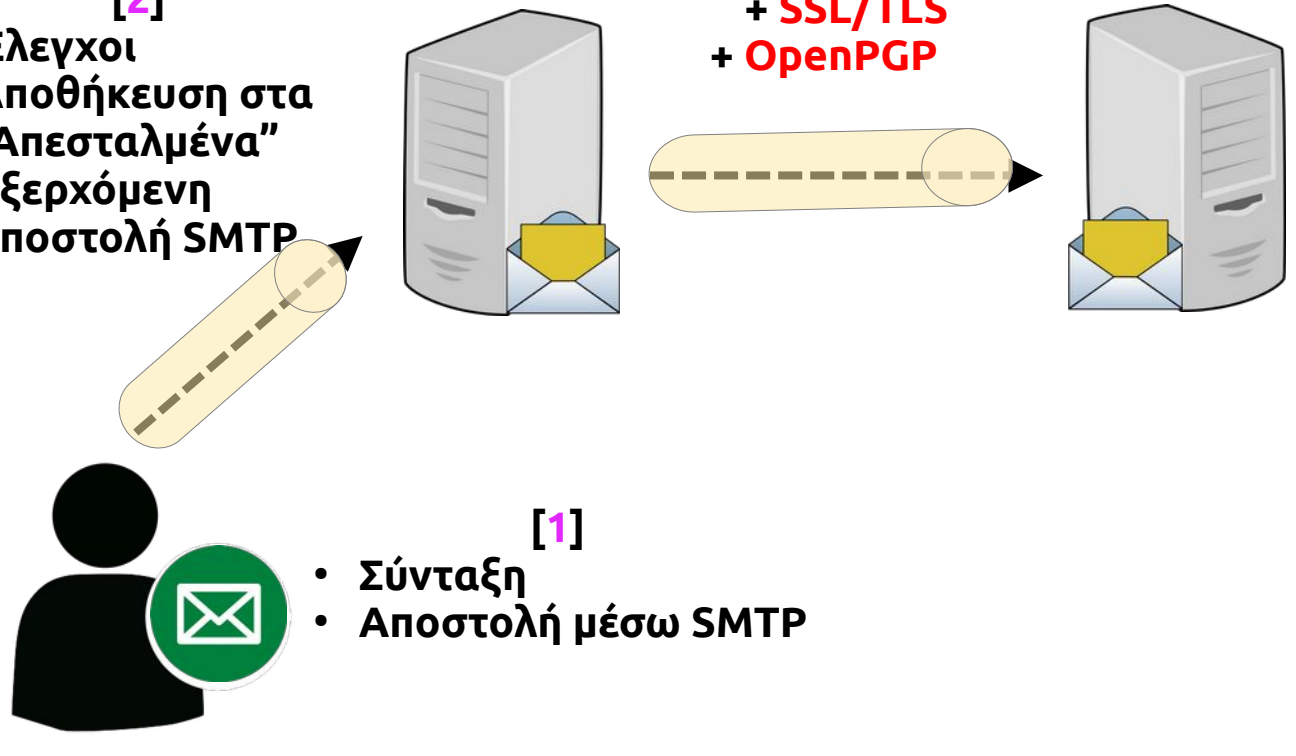
Κρυπτογράφηση επικοινωνίας

Κρυπτογράφηση Σύνδεσης
Κρυπτογράφηση Μηνυμάτων



Κρυπτογράφηση επικοινωνίας

Η τυπική διαδρομή… ενός email
+ SSL/TLS
+ OpenPGP



[1]
- **Σύνταξη**
- **Αποστολή μέσω SMTP**

[2]
- **Έλεγχοι**
- **Αποθήκευση στα “Απεσταλμένα”**
- **Εξερχόμενη αποστολή SMTP**

[3]
- **Παραλαβή μηνύματος**
- **έλεγχοι (πχ φίλτρο spam)**
- **Αποθήκευση στα “Εισερχόμενα”**

[4]
- **Λήψη μηνύματος μέσω POP3/IMAP**
- **Ανάγνωση**

Κρυπτογράφηση επικοινωνίας

Η εφαρμογή αλληλογραφίας **Mozilla Thunderbird** έχει την δυνατότητα χρήσης της κρυπτογράφησης **OpenPGP**.

Μέσω αυτής το Thunderbird μπορεί να κρυπτογραφεί, αποκρυπτογραφεί και να υπογράφει ψηφιακά μηνύματα.

Δημιουργεί επίσης και διαχειρίζεται τα δημόσια και ιδιωτικά κλειδιά που απαιτούνται για το σκοπό αυτό.

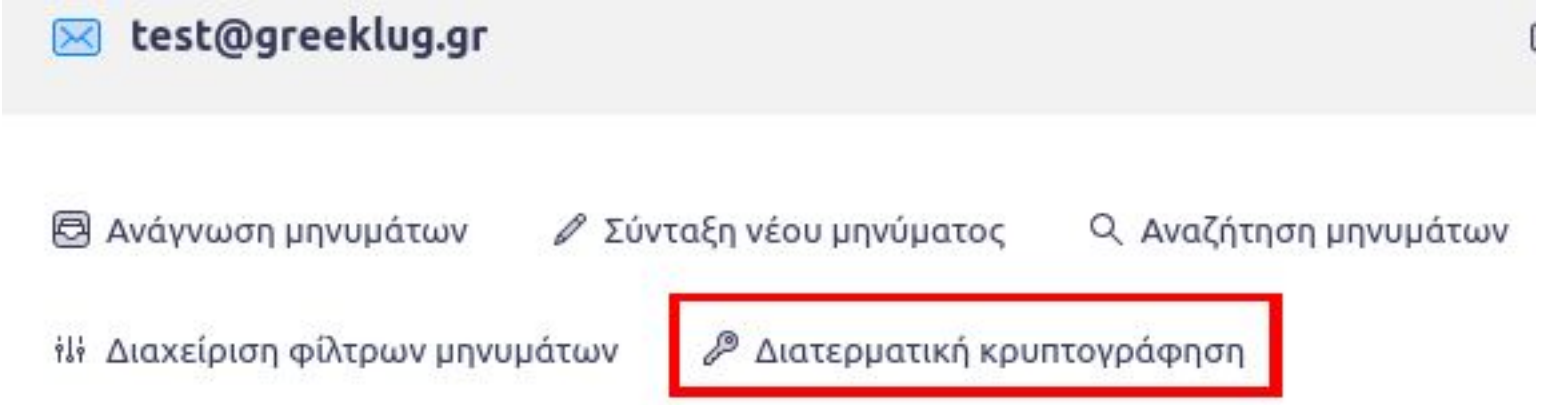
Η λειτουργία και σχετικές ρυθμίσεις παρέχονται από την επιλογή “Κρυπτογράφηση από άκρο σε άκρο”.

https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq

Thunderbird & OpenPGP

Κρυπτογράφηση επικοινωνίας

Αρχικά δημιουργούμε το δικό μας κλειδί OpenPGP που στηρίζεται στο μοντέλο δημόσιου κλειδιού (περιλαμβάνει δύο μέρη, το ιδιωτικό και το δημόσιο κλειδί).



Κρυπτογράφηση επικοινωνίας

Αρχικά δημιουργούμε το δικό μας κλειδί OpenPGP που στηρίζεται στο μοντέλο δημόσιου κλειδιού (περιλαμβάνει δύο μέρη, το ιδιωτικό και το δημόσιο κλειδί).

Κρυπτογράφηση επικοινωνίας

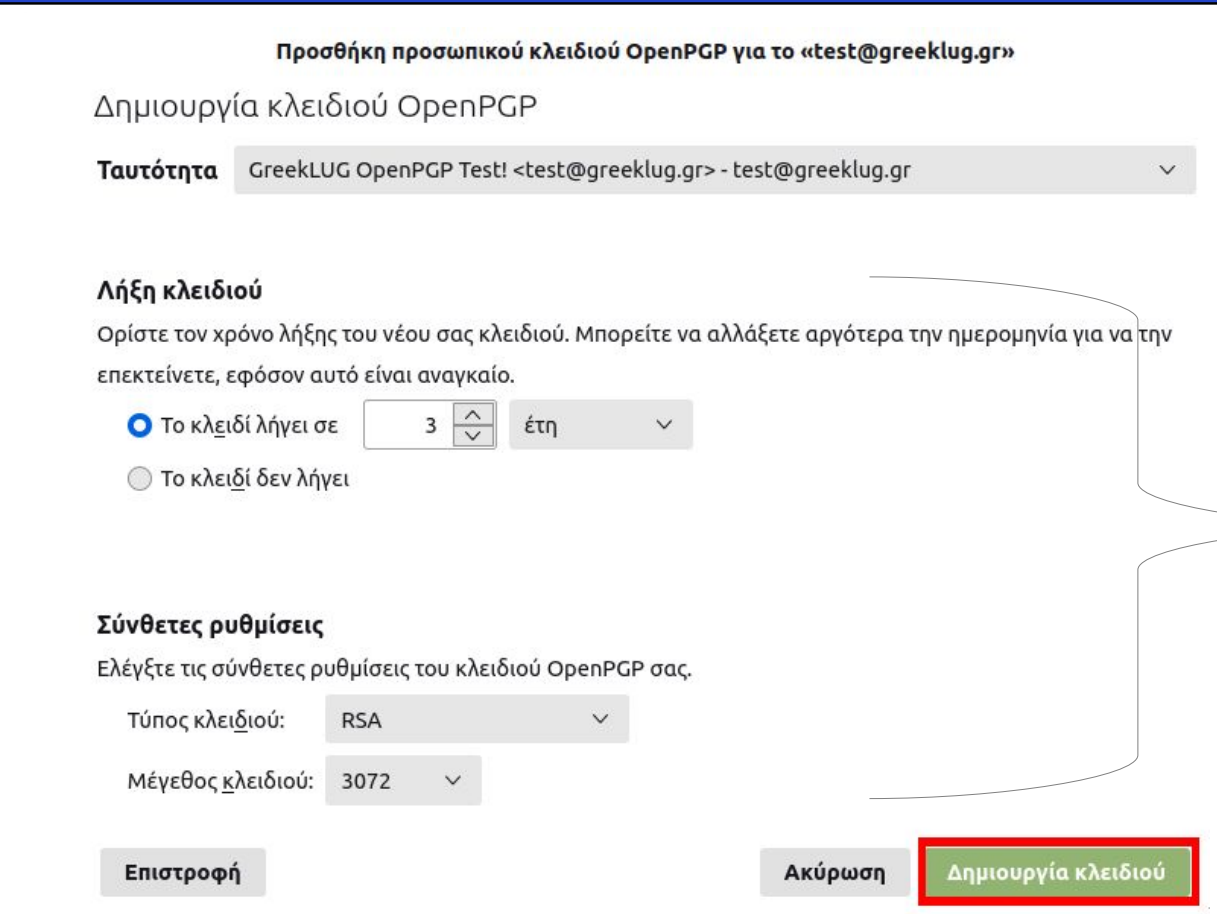
Προσθήκη προσωπικού κλειδιού OpenPGP για το «test@greeklug.gr»

ⓘ **Αν διαθέτετε ήδη ένα προσωπικό κλειδί** για αυτή τη διεύθυνση email, θα πρέπει να το εισαγάγετε. Διαφορετικά, δεν θα έχετε πρόσβαση στα αρχεία κρυπτογραφημένων email σας, ούτε θα μπορείτε να διαβάζετε εισερχόμενα κρυπτογραφημένα email από άτομα που χρησιμοποιούν το υπάρχον κλειδί σας. Μάθετε περισσότερα

- (●) Δημιουργία νέου κλειδιού OpenPGP
- ( ) Εισαγωγή υπάρχοντος κλειδιού OpenPGP

Ακύρωση | Συνέχεια

Κρυπτογράφηση επικοινωνίας



Δυνατότητα επιλογής διάρκειας & τύπου κρυπτογράφησης

Κρυπτογράφηση επικοινωνίας

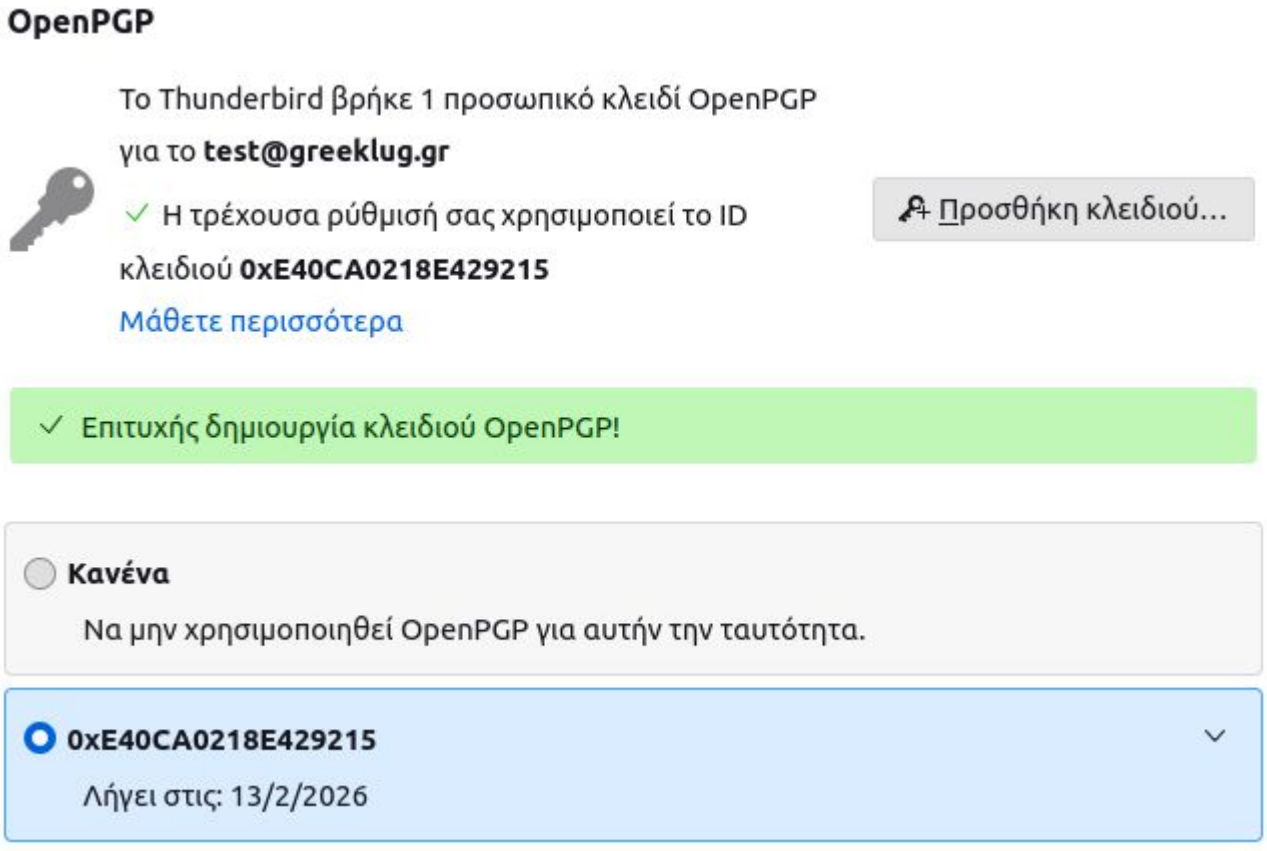
Προσθήκη προσωπικού κλειδιού OpenPGP για το «test@greeklug.gr»

ⓘ **Η ολοκλήρωση της δημιουργίας κλειδιού ενδέχεται να χρειαστεί αρκετά λεπτά.** Μην κλείσετε την εφαρμογή όσο είναι σε εξέλιξη η δημιουργία του κλειδιού. Η ενεργή περιήγηση ή η εκτέλεση εκτενών διαδικασιών που απασχολούν τον δίσκο κατά τη διάρκεια της δημιουργίας του κλειδιού θα γεμίσουν τη «δεξαμενή τυχαιότητας», επιταχύνοντας τη διαδικασία. Θα ενημερωθείτε όταν ολοκληρωθεί η δημιουργία του κλειδιού.

Δημιουργία δημόσιου και ιδιωτικού κλειδιού για το «GreekLUG OpenPGP Test! **"test@greeklug.gr"**»;

Ακύρωση | Επιβεβαίωση

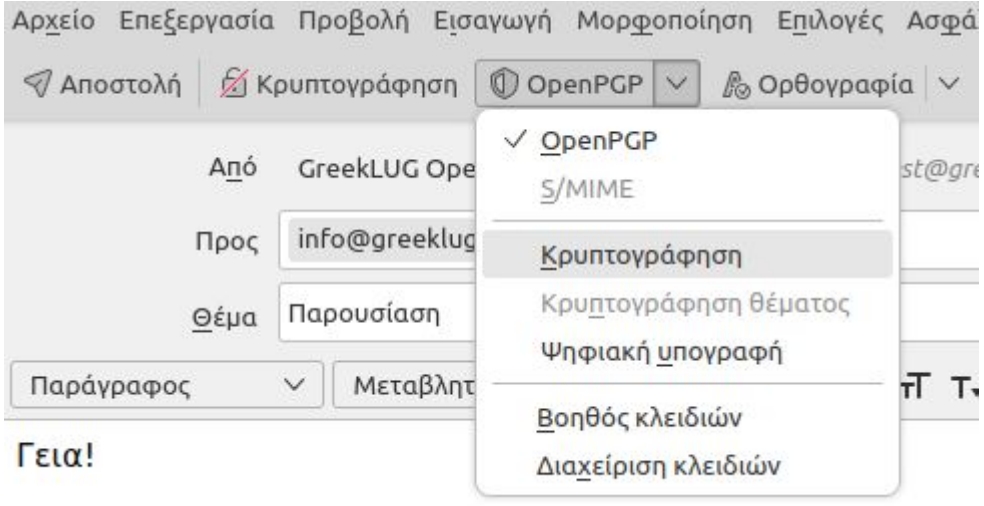
Κρυπτογράφηση επικοινωνίας

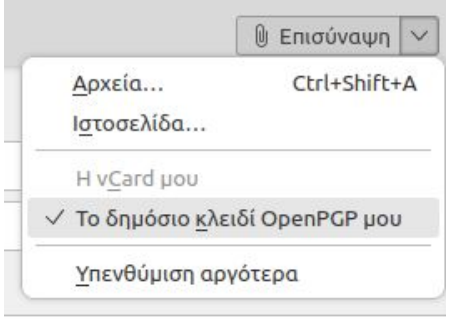


Κρυπτογράφηση επικοινωνίας

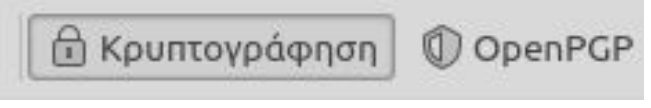
Κατά την σύνταξη ενός μηνύματος, μπορούμε να επιλέξουμε:
- "**Κρυπτογράφηση**", ώστε το μήνυμά μας να κρυπτογραφηθεί
  "**Κρυπτογράφηση θέματος**", εφόσον επιθυμούμε να κρυπτογραφηθεί και το Θέμα
- "**Ψηφιακή υπογραφή**", ώστε να υπογράψουμε το μήνυμα (το περιεχόμενο του μηνύματος δεν κρυπτογραφείται)

Επίσης έχουμε την δυνατότητα να επισυνάψουμε το δημόσιο κλειδί μας, εφόσον ο παραλήπτης δεν το διαθέτει, πχ είναι η πρώτη φορά επικοινωνίας μαζί του.



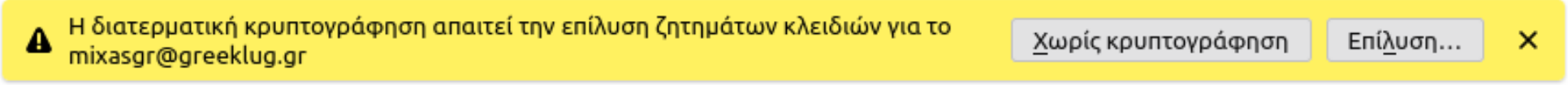


Εφόσον επιλέξουμε κάποια ασφάλεια αλλάζει η ένδειξης χρήσης κρυπτογράφησης:



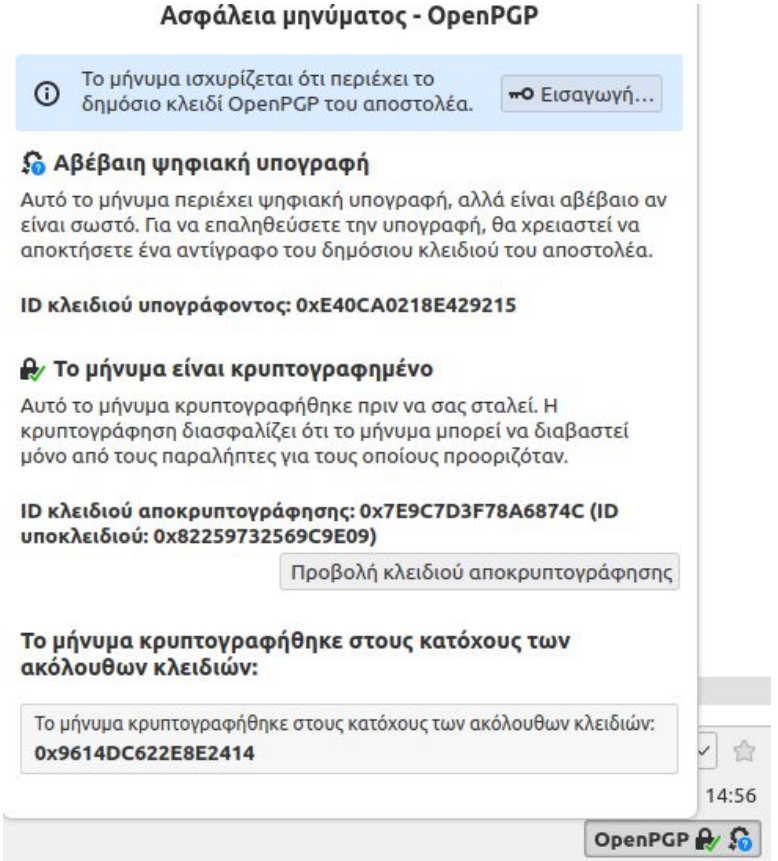
Κρυπτογράφηση επικοινωνίας

Για να είναι εφικτή η αποστολή ενός κρυπτογραφημένου μηνύματος σε κάποιον θα πρέπει να διαθέτουμε το δημόσιο κλειδί του στην κλειδοθήκη μας. Διαφορετικά η αποστολή αποτυγχάνει.



Θα πρέπει αντίστοιχα να εισάγουμε το δημόσιο κλειδί, είτε χειροκίνητα, είτε μέσω κάποιου μηνύματος που μας είχε προωθηθεί από τον παραλήπτη, που να έχει συνημμένο το κλειδί του.

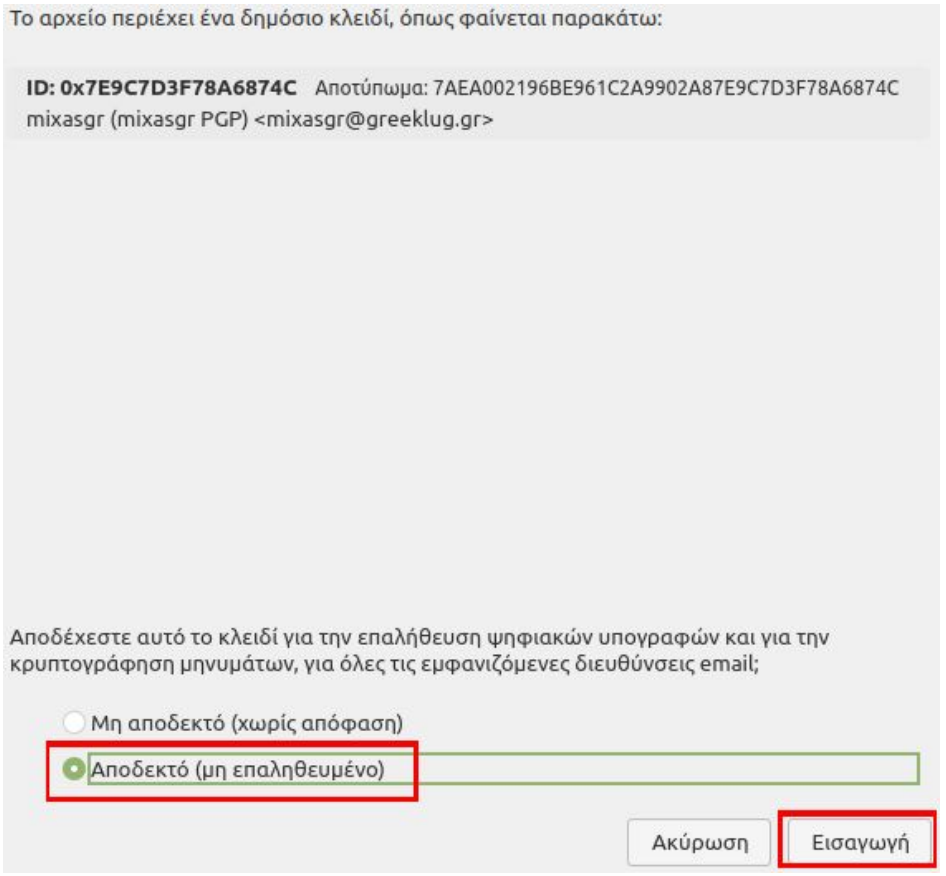
Κρυπτογράφηση επικοινωνίας

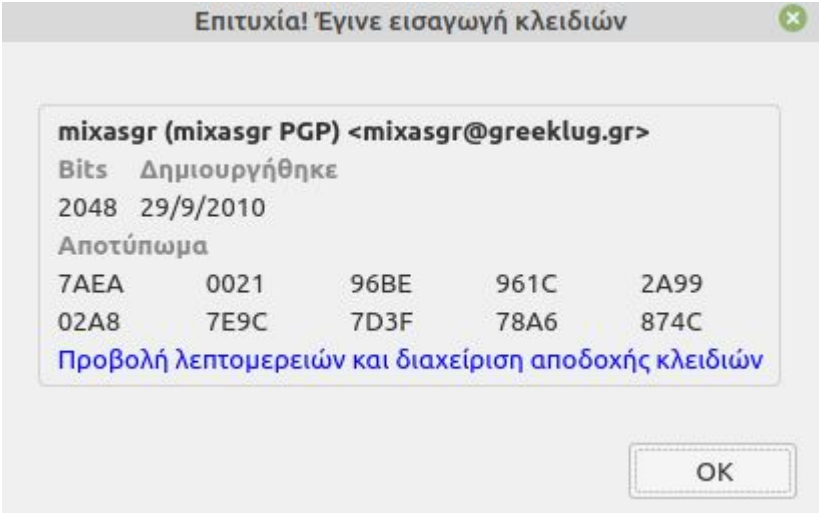


Εφόσον ένα μήνυμα περιέχει κάποιο κλειδί OpenPGP εμφανίζεται σχετική ένδειξη.

Επίσης μέσω αυτής μπορούμε να δούμε πληροφορίες για την υπογραφή και να το εισάγουμε στην κλειδοθήκη μας.

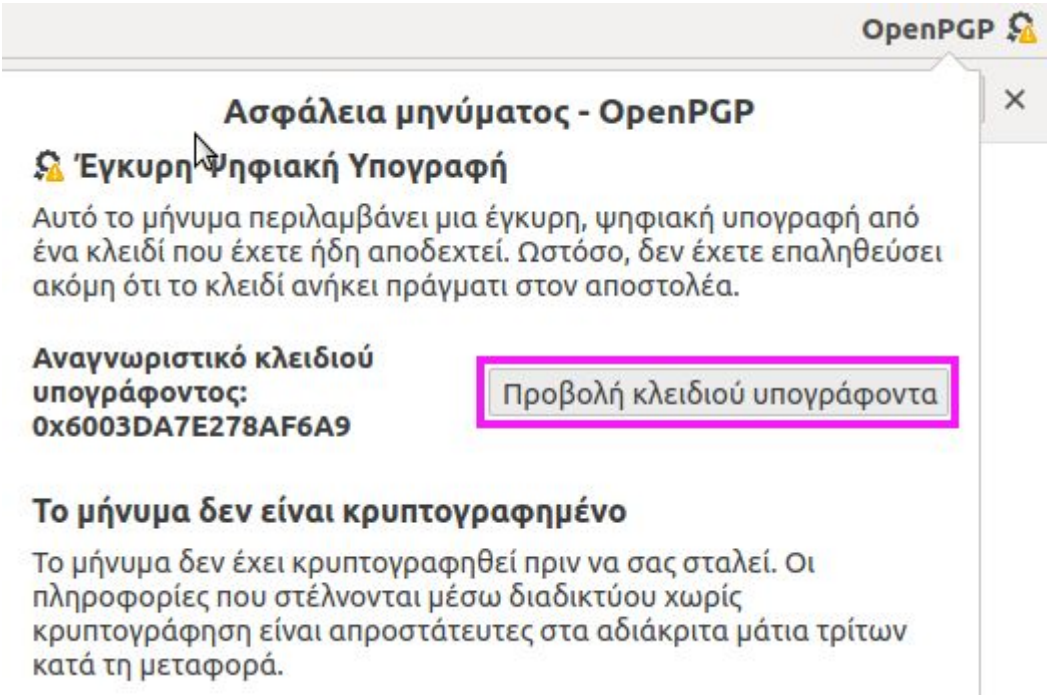
Κρυπτογράφηση επικοινωνίας





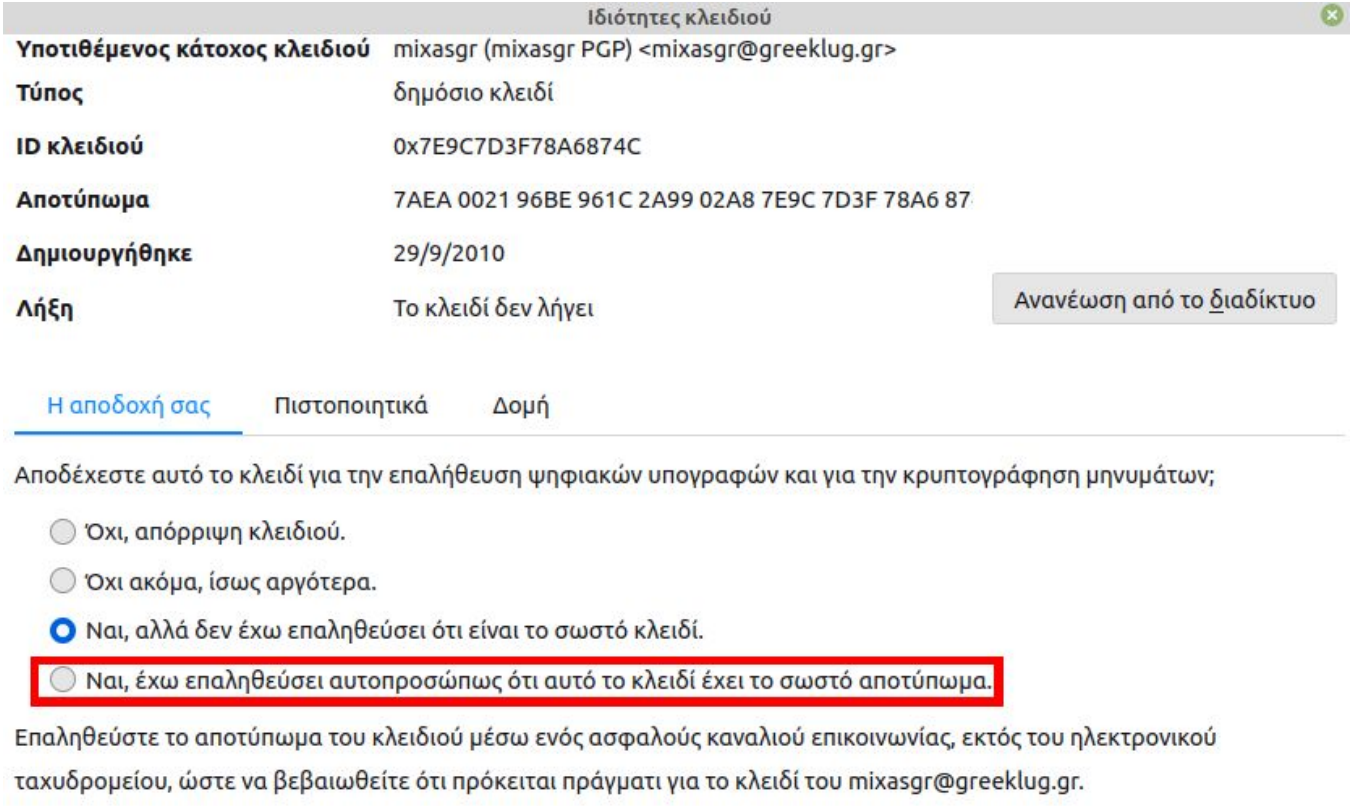
Κρυπτογράφηση επικοινωνίας

Από προκαθορισμένα το κλειδί εισάγεται στην κλειδοθήκη, ωστόσο δεν θεωρείται έγκυρο μέχρι να το ελέγξουμε και να το επαληθεύσουμε με τον κάτοχο.



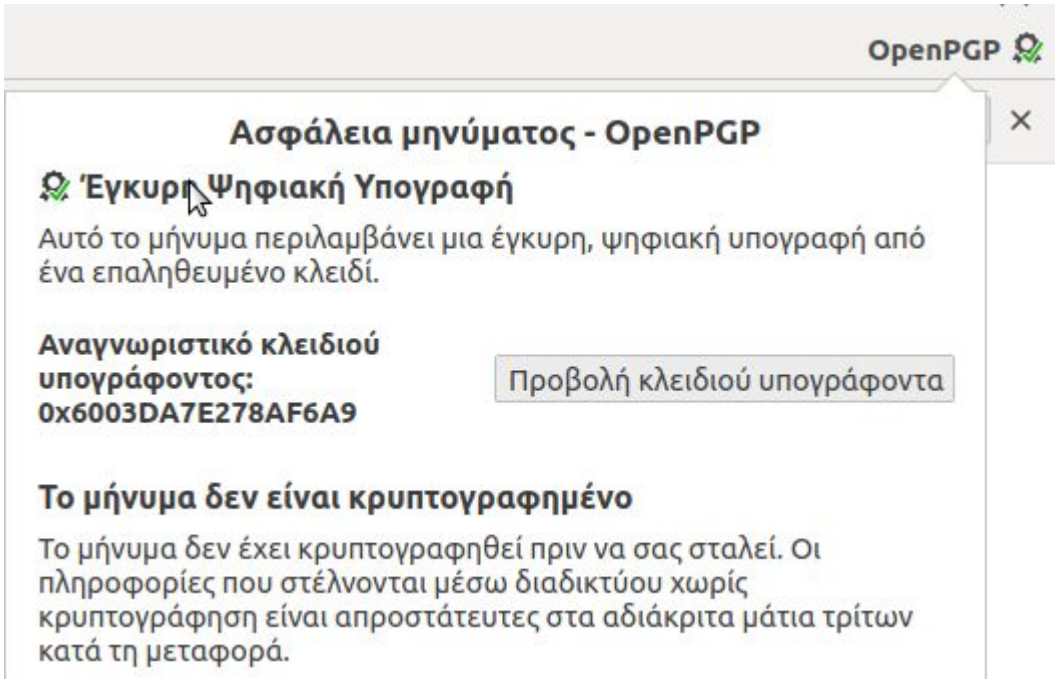
Κρυπτογράφηση επικοινωνίας

Εφόσον επαληθεύσουμε την ορθότητα του κλειδιού, μπορούμε να το αποδεχθούμε πλήρως.



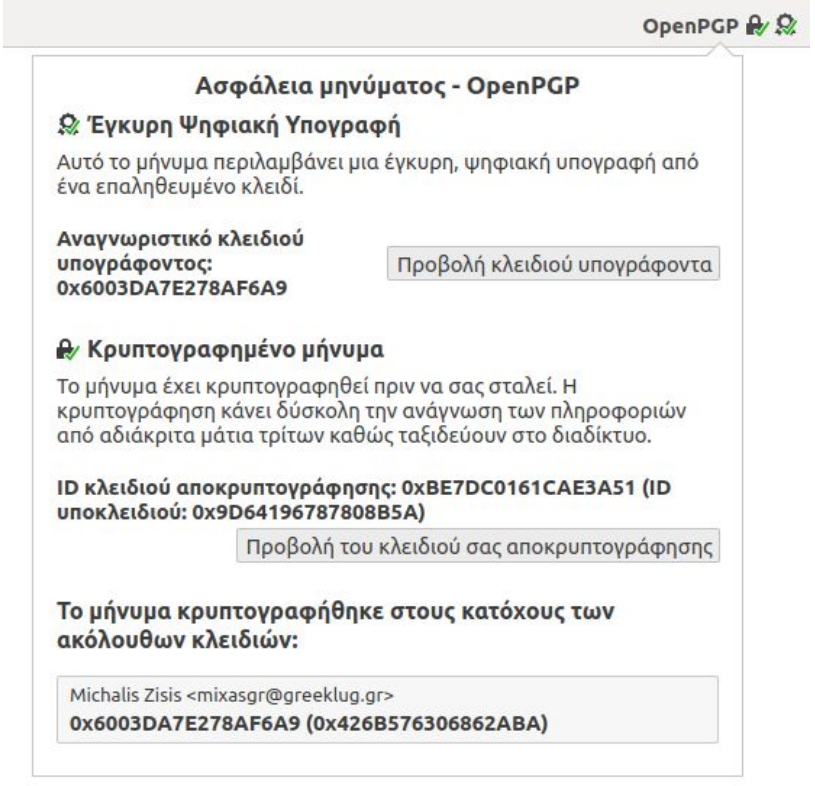
Κρυπτογράφηση επικοινωνίας

Ένδειξη ενός έγκυρου και επαληθευμένου κλειδιού σε μη κρυπτογραφημένο μήνυμα, που περιλαμβάνει ψηφιακή υπογραφή.



Κρυπτογράφηση επικοινωνίας

Ένδειξη ενός έγκυρου και επαληθευμένου κλειδιού σε κρυπτογραφημένο μήνυμα, που περιλαμβάνει επίσης ψηφιακή υπογραφή.



GreekLUG

Ευχαριστούμε!

Το αρχείο της παρουσίασης από την
Ελληνική Ένωση Φίλων ΕΛ/ΛΑΚ (GreekLUG) διέπεται από την άδεια

Ελληνική Ένωση Φίλων Ελεύθερου Λογισμικού | GreekLUG
https://www.greeklug.gr/