



# GreekLUG



Ελεύθερο Λογισμικό &



Λογισμικό Ανοικτού Κώδικα



# OpenPGP σε Thunderbird για κρυπτογραφημένα ή/και υπογεγραμμένα μηνύματα

Ζήσης Μιχάλης, GreekLUG



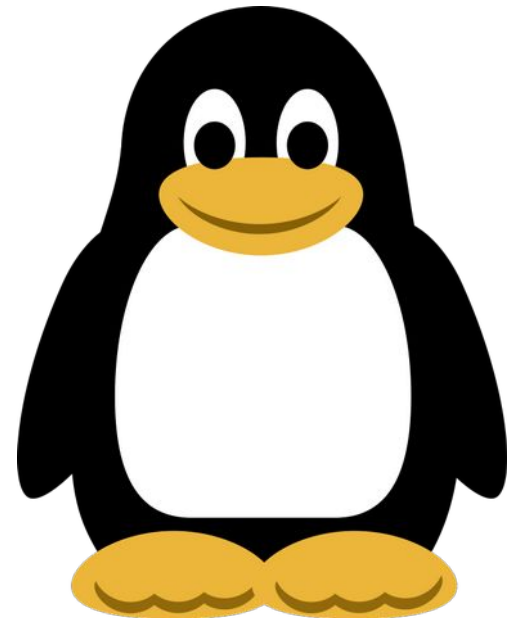
# OpenPGP σε Thunderbird

## whoami



~/Ζήσης Μιχάλης | System Administrator

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

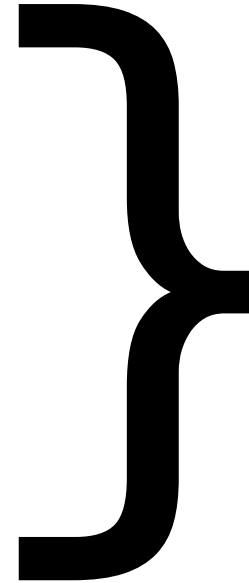
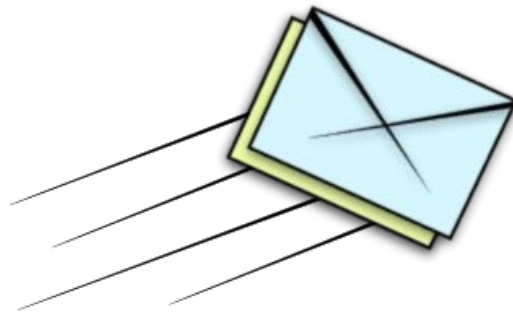




# OpenPGP σε Thunderbird

## Περιεχόμενα

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



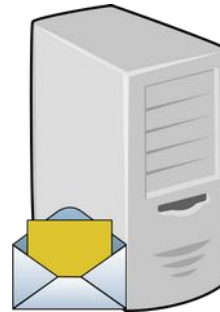
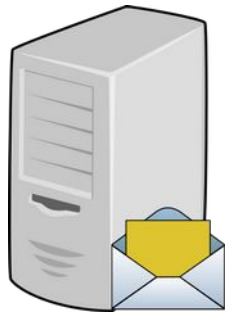


# Κρυπτογράφηση επικοινωνίας

## Η τυπική διαδρομή... ενός email

[2]

- Έλεγχοι
- Αποθήκευση στα "Απεσταλμένα"
- Εξερχόμενη αποστολή SMTP



[3]

- Παραλαβή μηνύματος
- έλεγχοι (πχ φίλτρο spam)
- Αποθήκευση στα "Εισερχόμενα"

[4]

- Λήψη μηνύματος μέσω POP3/IMAP
- Ανάγνωση

[1]

- Σύνταξη
- Αποστολή μέσω SMTP





# Κρυπτογράφηση επικοινωνίας

Η **κρυπτογράφηση επικοινωνίας** διασφαλίζει ότι τα δεδομένα που ανταλλάσσουμε 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:

## Ρυθμίσεις διακομιστή

### ΔΙΑΚΟΜΙΣΤΗΣ ΕΙΣΕΡΧΟΜΕΝΩΝ

Πρωτόκολλο:	IMAP
Όνομα υπολογιστή:	imap.greeklug.gr
Θύρα:	143
Ασφάλεια σύνδεσης:	STARTTLS
Μέθοδος ταυτοποίησης:	Αυτόματος εντοπισμός
Όνομα χρήστη:	info@greeklug.gr

## Ρυθμίσεις διακομιστή

### ΔΙΑΚΟΜΙΣΤΗΣ ΕΞΕΡΧΟΜΕΝΩΝ

Όνομα υπολογιστή:	smtp.greeklug.gr
Θύρα:	587
Ασφάλεια σύνδεσης:	STARTTLS
Μέθοδος ταυτοποίησης:	Αυτόματος εντοπισμός
Όνομα χρήστη:	info@greeklug.gr

Σύνθετη διαμόρφωση



# Κρυπτογράφηση επικοινωνίας

## Κρυπτογράφηση Σύνδεσης







# Κρυπτογράφηση επικοινωνίας

## Κρυπτογράφηση Σύνδεσης

Χρήστης Α

Μη κρυπτογραφημένη  
Επικοινωνία

Κείμενο

Χρήστης Β





# Κρυπτογράφηση επικοινωνίας

## Κρυπτογράφηση Σύνδεσης

Χρήστης Α

Μη κρυπτογραφημένη  
Επικοινωνία

Κείμενο

Χρήστης Β



Χρήστης Α

Κρυπτογραφημένη  
Επικοινωνία με SSL/TLS

Κείμενο

Χρήστης Β

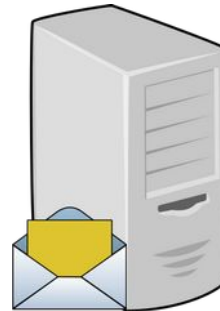
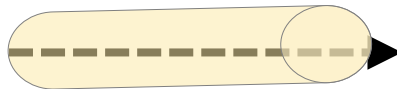
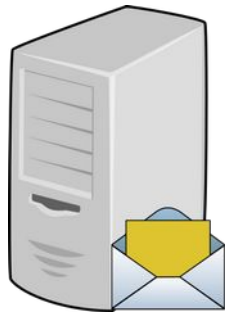


# Κρυπτογράφηση επικοινωνίας

Η τυπική διαδρομή... ενός email  
+ **SSL/TLS**

[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

[1]

- Σύνταξη
- Αποστολή μέσω SMTP





# 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+vGmrCuC6FFTy1EYovEB4qPc1IntcrBlndvTu7vy7wXsE+wp8Hpy2YGsHp3...

-----END PGP MESSAGE-----



# Κρυπτογράφηση επικοινωνίας

## Βήματα κρυπτογράφησης δημοσίου κλειδιού

- Ο **Χρήστης A** θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον **Χρήστη B**
- Ο **Χρήστης A** κρυπτογραφεί το απλό κείμενο με το δημόσιο κλειδί του **Χρήστη B** και στέλνει το μήνυμα
- Ο **Χρήστης B** 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 A** θα πρέπει να γνωρίζει το δημόσιο κλειδί του **Χρήστη B** για να μπορέσει να επικοινωνήσει μαζί του



# Κρυπτογράφηση επικοινωνίας

## Βήματα ψηφιακής υπογραφής δημοσίου κλειδιού

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

### Σημαντικό

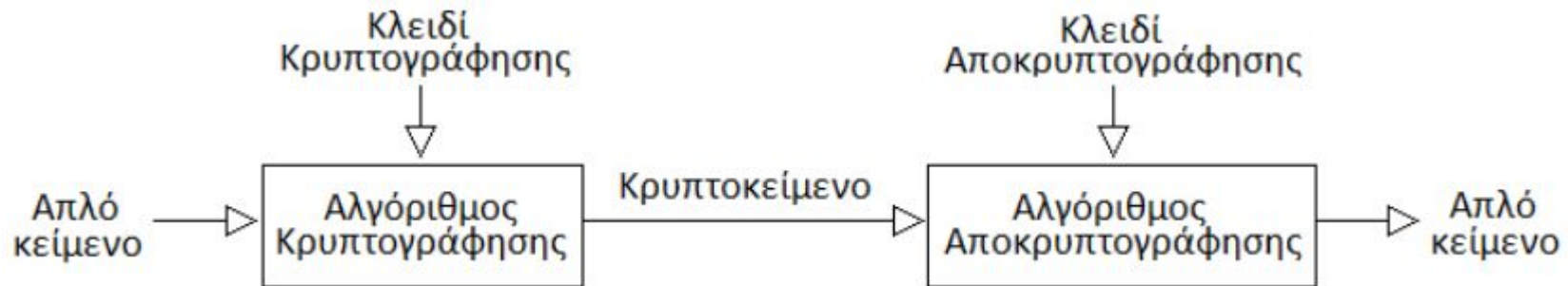
Η υπογραφή εξαρτάται από το περιεχόμενο του μηνύματος. Εάν αυτό τροποποιηθεί τότε η εγκυρότητα της υπογραφής δεν ισχύει

\* Ο **Χρήστης B** θα πρέπει να γνωρίζει το δημόσιο κλειδί του **Χρήστη A** για να μπορέσει να επιβεβαιώσει την εγκυρότητα του μηνύματος



# Κρυπτογράφηση επικοινωνίας

## Κρυπτογράφηση Μηνυμάτων

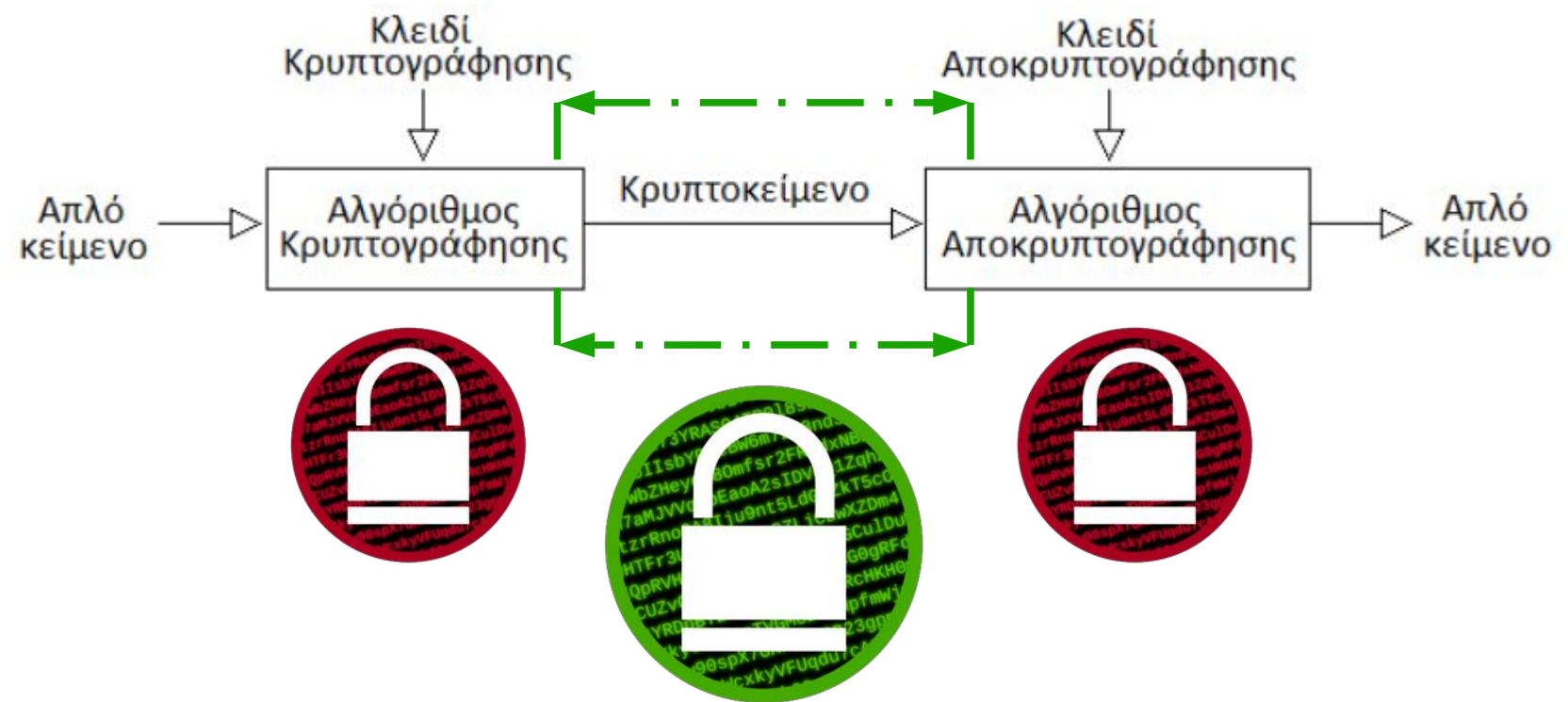






# Κρυπτογράφηση επικοινωνίας

**Κρυπτογράφηση Σύνδεσης**  
**Κρυπτογράφηση Μηνυμάτων**

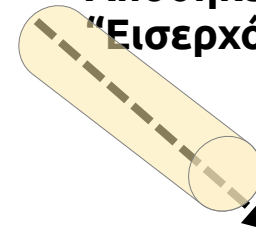
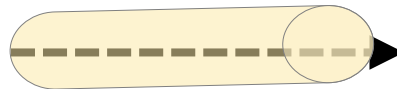
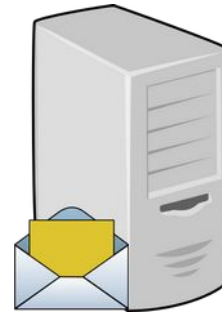
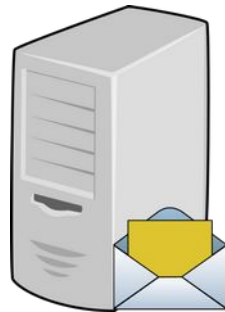




# Κρυπτογράφηση επικοινωνίας

Η τυπική διαδρομή... ενός email

+ **SSL/TLS**  
+ **OpenPGP**



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

Μέσω αυτής το Thunderbird μπορεί να κρυπτογραφεί, αποκρυπτογραφεί και να υπογράψει 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).

 test@greeklug.gr

 Ανάγνωση μηνυμάτων

 Σύνταξη νέου μηνύματος

 Αναζήτηση μηνυμάτων

 Διαχείριση φίλτρων μηνυμάτων

 Διατεματική κρυπτογράφηση



# Κρυπτογράφηση επικοινωνίας

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

✉ [test@greeklug.gr](mailto:test@greeklug.gr)

Ρυθμίσεις διακομιστή

Αντίγραφα & φάκελοι

Σύνθεση & διευθυνσιοδότηση

Ρυθμίσεις ανεπιθύμητων

Συγχρονισμός & αποθήκευση

Διατελεσματική κρυπτογράφηση

Αποδεικτικά προβολής

✉ Τοπικοί φάκελοι

Ρυθμίσεις ανεπιθύμητων

## Διατελεσματική κρυπτογράφηση

Για να στείλετε κρυπτογραφημένα ή ψηφιακά υπογεγραμμένα μηνύματα, πρέπει να ρυθμίσετε μια τεχνολογία κρυπτογράφησης, είτε OpenPGP είτε S/MIME.

Επιλέξτε το προσωπικό σας κλειδί για να ενεργοποιήσετε τη χρήση του OpenPGP ή το προσωπικό σας πιστοποιητικό για να ενεργοποιήσετε τη χρήση του S/MIME. Για ένα προσωπικό κλειδί ή πιστοποιητικό έχετε και το αντίστοιχο μυστικό κλειδί.

[Μάθετε περισσότερα](#)

## OpenPGP



Το Thunderbird δεν έχει προσωπικό κλειδί OpenPGP για **test@greeklug.gr**

 Προσθήκη κλειδιού...



# 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

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

Δημιουργία κλειδιού OpenPGP

Ταυτότητα

## Λήξη κλειδιού

Ορίστε τον χρόνο λήξης του νέου σας κλειδιού. Μπορείτε να αλλάξετε αργότερα την ημερομηνία για να την επεκτείνετε, εφόσον αυτό είναι αναγκαίο.

Το κλειδί λήγει σε

Το κλειδί δεν λήγει

## Σύνθετες ρυθμίσεις

Ελέγξτε τις σύνθετες ρυθμίσεις του κλειδιού OpenPGP σας.

Τύπος κλειδιού:

Μέγεθος κλειδιού:

Επιστροφή

Ακύρωση

Δημιουργία κλειδιού

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


## OpenPGP

Το Thunderbird βρήκε 1 προσωπικό κλειδί OpenPGP  
για το **test@greeklug.gr**



✓ Η τρέχουσα ρύθμισή σας χρησιμοποιεί το ID  
κλειδιού **0xE40CA0218E429215**

[Μάθετε περισσότερα](#)

 Προσθήκη κλειδιού...

✓ Επιτυχής δημιουργία κλειδιού OpenPGP!

**Κανένα**

Να μην χρησιμοποιηθεί OpenPGP για αυτήν την ταυτότητα.

**0xE40CA0218E429215**

Λήγει στις: 13/2/2026



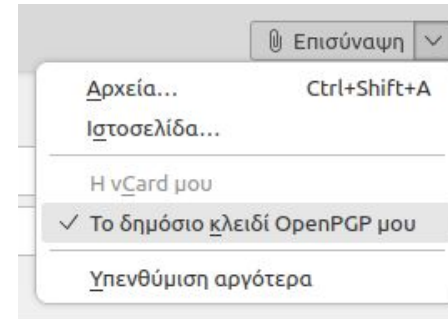
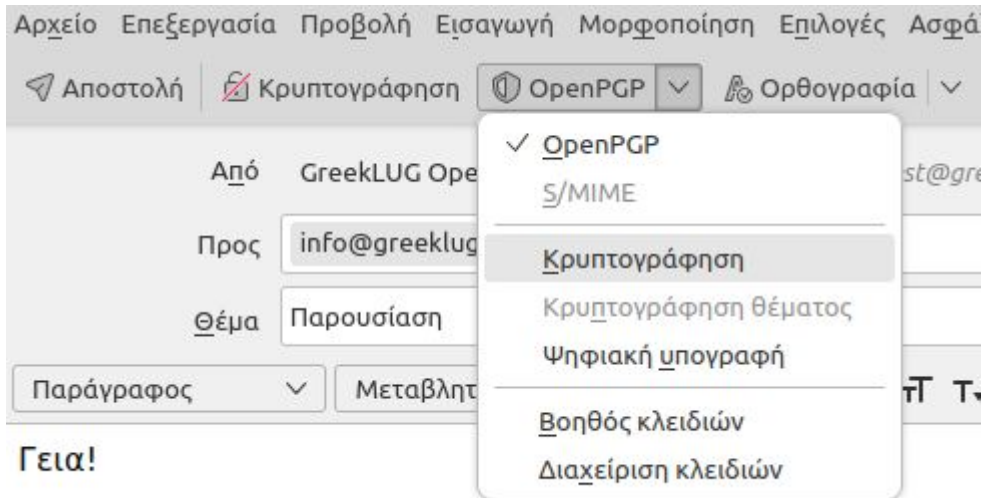


# Κρυπτογράφηση επικοινωνίας

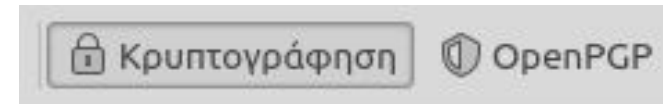
Κατά την σύνταξη ενός μηνύματος, μπορούμε να επιλέξουμε:

- **“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.



Η διατεματική κρυπτογράφηση απαιτεί την επίλυση ζητημάτων κλειδιών για το mixasgr@greeklug.gr

Χωρίς κρυπτογράφηση

Επίλυση...





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

## Ασφάλεια μηνύματος - OpenPGP

 Το μήνυμα ισχυρίζεται ότι περιέχει το δημόσιο κλειδί OpenPGP του αποστολέα.

 Εισαγωγή...

### Αβέβαιη ψηφιακή υπογραφή


Αυτό το μήνυμα περιέχει ψηφιακή υπογραφή, αλλά είναι αβέβαιο αν είναι σωστό. Για να επαληθεύσετε την υπογραφή, θα χρειαστεί να αποκτήσετε ένα αντίγραφο του δημόσιου κλειδιού του αποστολέα.

ID κλειδιού υπογράφοντος: 0xE40CA0218E429215

### Το μήνυμα είναι κρυπτογραφημένο

Αυτό το μήνυμα κρυπτογραφήθηκε πριν να σας σταλεί. Η κρυπτογράφηση διασφαλίζει ότι το μήνυμα μπορεί να διαβαστεί μόνο από τους παραλήπτες για τους οποίους προορίζεται.


ID κλειδιού αποκρυπτογράφησης: 0x7E9C7D3F78A6874C (ID υποκλειδιού: 0x82259732569C9E09)

 Προβολή κλειδιού αποκρυπτογράφησης

Το μήνυμα κρυπτογραφήθηκε στους κατόχους των ακόλουθων κλειδιών:

Το μήνυμα κρυπτογραφήθηκε στους κατόχους των ακόλουθων κλειδιών:  
0x9614DC622E8E2414

14:56

OpenPGP  

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.

## Ασφάλεια μηνύματος - OpenPGP

### Έγκυρη ψηφιακή υπογραφή

Αυτό το μήνυμα περιλαμβάνει μια έγκυρη, ψηφιακή υπογραφή από ένα κλειδί που έχετε ήδη αποδεχτεί. Ωστόσο, δεν έχετε επαληθεύσει ακόμη ότι το κλειδί ανήκει πράγματι στον αποστολέα.

ID κλειδιού υπογράφοντος:  
0x7E9C7D3F78A6874C

 Προβολή κλειδιού υπογράφοντα



# Κρυπτογράφηση επικοινωνίας

Το αρχείο περιέχει ένα δημόσιο κλειδί, όπως φαίνεται παρακάτω:

**ID: 0x7E9C7D3F78A6874C** Αποτύπωμα: 7AEA002196BE961C2A9902A87E9C7D3F78A6874C  
mixasgr (mixasgr PGP) <mixasgr@greeklug.gr>

Αποδέχεστε αυτό το κλειδί για την επαλήθευση ψηφιακών υπογραφών και για την κρυπτογράφηση μηνυμάτων, για όλες τις εμφανιζόμενες διευθύνσεις email;

Μη αποδεκτό (χωρίς απόφαση)

Αποδεκτό (μη επαληθευμένο)

Ακύρωση

Εισαγωγή

Επιτυχία! Έγινε εισαγωγή κλειδιών

**mixasgr (mixasgr PGP) <mixasgr@greeklug.gr>**

Bits Δημιουργήθηκε

2048 29/9/2010

Αποτύπωμα

7AEA 0021 96BE 961C 2A99

02A8 7E9C 7D3F 78A6 874C


[Προβολή λεπτομερειών και διαχείριση αποδοχής κλειδιών](#)

OK




# Κρυπτογράφηση επικοινωνίας

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

OpenPGP 

### Ασφάλεια μηνύματος - OpenPGP

 Έγκυρη Ψηφιακή Υπογραφή

Αυτό το μήνυμα περιλαμβάνει μια έγκυρη, ψηφιακή υπογραφή από ένα κλειδί που έχετε ήδη αποδεχτεί. Ωστόσο, δεν έχετε επαληθεύσει ακόμη ότι το κλειδί ανήκει πράγματι στον αποστολέα.

**Αναγνωριστικό κλειδιού  
υπογράφοντος:**  
0x6003DA7E278AF6A9

[Προβολή κλειδιού υπογράφοντα](#)

**Το μήνυμα δεν είναι κρυπτογραφημένο**

Το μήνυμα δεν έχει κρυπτογραφηθεί πριν να σας σταλεί. Οι πληροφορίες που στέλνονται μέσω διαδικτύου χωρίς κρυπτογράφηση είναι απροστάτευτες στα αδιάκριτα μάτια τρίτων κατά τη μεταφορά.



# Κρυπτογράφηση επικοινωνίας

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

Ιδιότητες κλειδιού ✕

Υποτιθέμενος κάτοχος κλειδιού	mixasgr (mixasgr PGP) <mixasgr@greeklug.gr>
Τύπος	δημόσιο κλειδί
ID κλειδιού	0x7E9C7D3F78A6874C
Αποτύπωμα	7AEA 0021 96BE 961C 2A99 02A8 7E9C 7D3F 78A6 87
Δημιουργήθηκε	29/9/2010
Λήξη	Το κλειδί δεν λήγει

Ανανέωση από το [διαδίκτυο](#)

[Η αποδοχή σας](#)

Πιστοποιητικά

Δομή

Αποδέχεστε αυτό το κλειδί για την επαλήθευση ψηφιακών υπογραφών και για την κρυπτογράφηση μηνυμάτων;


- Όχι, απόρριψη κλειδιού.
- Όχι ακόμα, ίσως αργότερα.
- Ναι, αλλά δεν έχω επαληθεύσει ότι είναι το σωστό κλειδί.
- Ναι, έχω επαληθεύσει αυτοπροσώπως ότι αυτό το κλειδί έχει το σωστό αποτύπωμα.

Επαληθεύστε το αποτύπωμα του κλειδιού μέσω ενός ασφαλούς καναλιού επικοινωνίας, εκτός του ηλεκτρονικού ταχυδρομείου, ώστε να βεβαιωθείτε ότι πρόκειται πράγματι για το κλειδί του mixasgr@greeklug.gr.




# Κρυπτογράφηση επικοινωνίας

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

OpenPGP 

**Ασφάλεια μηνύματος - OpenPGP**

 Έγκυρη Ψηφιακή Υπογραφή

Αυτό το μήνυμα περιλαμβάνει μια έγκυρη, ψηφιακή υπογραφή από ένα επαληθευμένο κλειδί.

**Αναγνωριστικό κλειδιού υπογράφοντος:**  
0x6003DA7E278AF6A9

[Προβολή κλειδιού υπογράφοντα](#)

**Το μήνυμα δεν είναι κρυπτογραφημένο**

Το μήνυμα δεν έχει κρυπτογραφηθεί πριν να σας σταλεί. Οι πληροφορίες που στέλνονται μέσω διαδικτύου χωρίς κρυπτογράφηση είναι απροστάτευτες στα αδιάκριτα μάτια τρίτων κατά τη μεταφορά.





# Κρυπτογράφηση επικοινωνίας

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

OpenPGP

**Ασφάλεια μηνύματος - OpenPGP**

**Έγκυρη Ψηφιακή Υπογραφή**

Αυτό το μήνυμα περιλαμβάνει μια έγκυρη, ψηφιακή υπογραφή από ένα επαληθευμένο κλειδί.

**Αναγνωριστικό κλειδιού υπογράφοντος:** 0x6003DA7E278AF6A9 Προβολή κλειδιού υπογράφοντα

**Κρυπτογραφημένο μήνυμα**

Το μήνυμα έχει κρυπτογραφηθεί πριν να σας σταλεί. Η κρυπτογράφηση κάνει δύσκολη την ανάγνωση των πληροφοριών από αδιάκριτα μάτια τρίτων καθώς ταξιδεύουν στο διαδίκτυο.

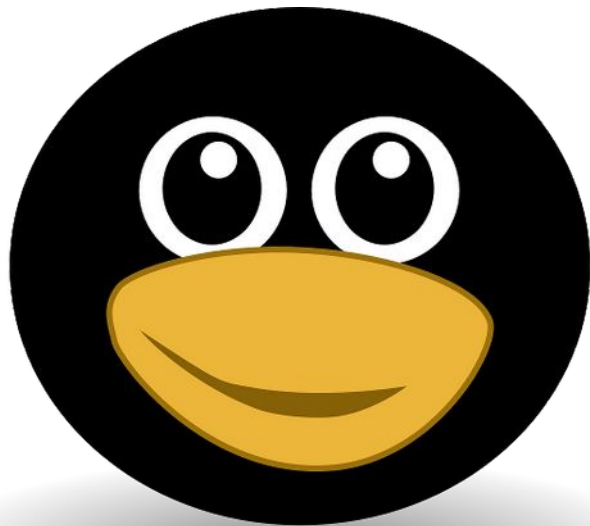
**ID κλειδιού αποκρυπτογράφησης:** 0xBE7DC0161CAE3A51 (ID υποκλειδιού: 0x9D64196787808B5A) Προβολή του κλειδιού σας αποκρυπτογράφησης

**Το μήνυμα κρυπτογραφήθηκε στους κατόχους των ακόλουθων κλειδιών:**

Michalis Zisis <mixasgr@greeklug.gr>  
0x6003DA7E278AF6A9 (0x426B576306862ABA)



GreekLUG



Ευχαριστούμε!



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

Creative Commons Αναφορά Δημιουργού - Μη Εμπορική Χρήση - Παρόμοια Διανομή 4.0 Διεθνές  
(CC BY-NC-SA 4.0)

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.el>

Ελληνική Ένωση Φίλων Ελεύθερου Λογισμικού | GreekLUG

<https://www.greeklug.gr/>