ΚΡΥΠΤΟΓΡΑΦΙΑ & GPG

Σταύρος Μεκέσης

Ευχαριστώ τον κ. Κωνσταντίνο Δραζιώτη για τις εύστοχες παρατηρήσεις και τις συμβουλές του

Τι θα δούμε;

- Έννοιες στην Κρυπτογραφία
  - Απλό κείμενο, κρυπτοκείμενο, κλειδί
  - Κρυπτογράφηση συμμετρικού κλειδιού
  - Κρυπτογράφηση δημοσίου κλειδιού
  - Συναρτήσεις κατακερματισμού
  - Ψηφιακές υπογραφές
- GPG
  - Στόχοι
  - Δημιουργία κλειδιού και πιστοποιητικού ανάκλησης
  - Κρυπτογράφηση και αποκρυπτογράφηση email
  - Ψηφιακές υπογραφές
  - Υπογραφή κλειδιών, κύκλος εμπιστευτικότητας
  - Thunderbird και Enigmail

Μια ιστορία για να χαλαρώσουμε...

- Η **Alice** και ο **Bob** είναι μέλη της διάσημης οργάνωσης **«Πυρήνες της Δραχμής»**
- Η Alice μένει στην Φρανκφούρτη (Wurrrst) και ο Bob στην Θεσσαλονίκη (χαλλλαρά)
- Επικοινωνούν μόνο μέσω **email**
- Η Alice σχεδιάζει ένα χτύπημα με **κομφετί** (!) στην ΕΚΤ
- Θέλει να ενημερώσει τον Bob χωρίς να το μάθει ο Mario
- Ο **Mario** είναι ο αρχηγός της ΕΚΤ και παρακολουθεί **τα ΠΑΝΤΑ**

Πρωταγωνιστές

Alice

Mario

Bob

Αν όλα πάνε καλά...

Απλό κείμενο και κρυπτοκείμενο

- Απλό κείμενο

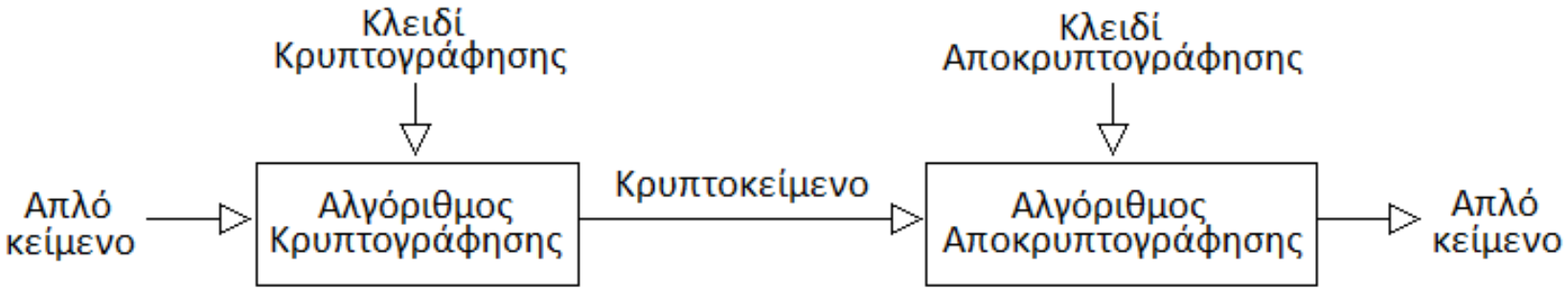
```
Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015
```

- Κρυπτοκείμενο

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

jA0EAwMC70UAD2i1T7+3yUFqTEuEzTX6rVjf6V9Dqbc7OpUMOIPq+ca8Y
oVGxHIgvUiiLudhdfpX3FA1A2EbH9IXqn0TSGIoU2lFSV3WlKIchw...
-----END PGP MESSAGE-----
```

Κλειδί κρυπτογράφησης / αποκρυπτογράφησης

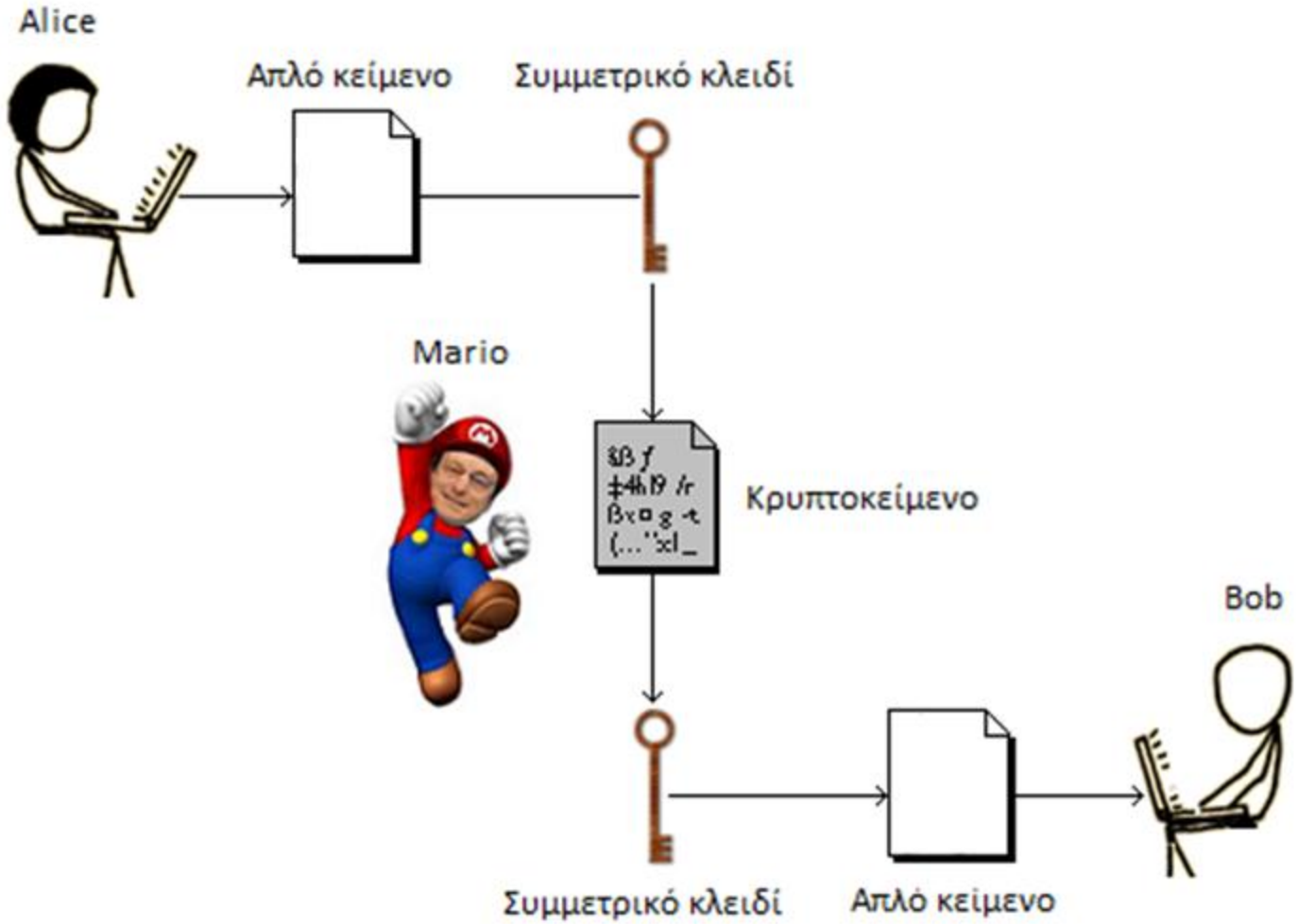
- Μια **ακολουθία bits**, π.χ. 01010111



Κρυπτογράφηση συμμετρικού κλειδιού

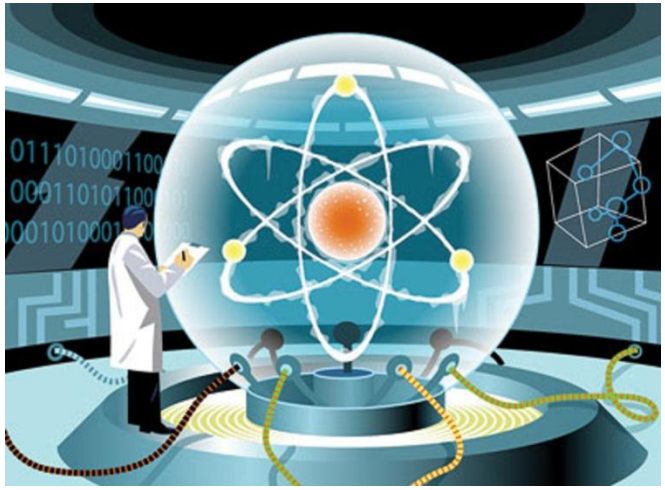
- Η Alice και ο Bob χρησιμοποιούν το **ίδιο μυστικό κλειδί**
- Η Alice θέλει να στείλει ένα email στον Bob
- Κρυπτογραφεί το απλό κείμενο με το κλειδί
- Στέλνει το κρυπτοκείμενο στον Bob
- Ο Bob αποκρυπτογραφεί το κρυπτοκείμενο με το κλειδί
- Διαβάζει το απλό κείμενο
- Ο Mario βλέπει μόνο το κρυπτοκείμενο
- Δημοφιλή συστήματα: **AES, CAST, Blowfish** κ.ά.

Κρυπτογράφηση συμμετρικού κλειδιού



Πλεονεκτήματα κρυπτογράφησης συμμετρικού κλειδιού

- Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης είναι **γρήγορη** (μικρά κλειδιά)
- Συστήματα όπως το **AES** θα μπορούσαν να αντισταθούν σε επιθέσεις **κβαντικών υπολογιστών**. Επιπλέον μελέτη: *Quantum Cryptography: As Awesome As It Is Pointless*, του Bruce Schneier



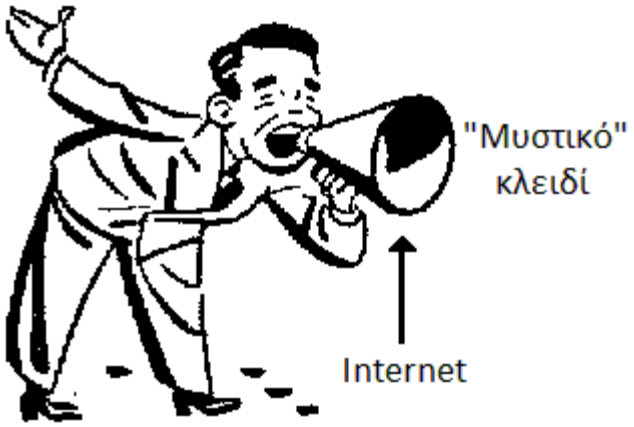
Μειονεκτήματα κρυπτογράφησης συμμετρικού κλειδιού

- 2 χρήστες → 1 κλειδί

  10 χρήστες → 45 κλειδιά

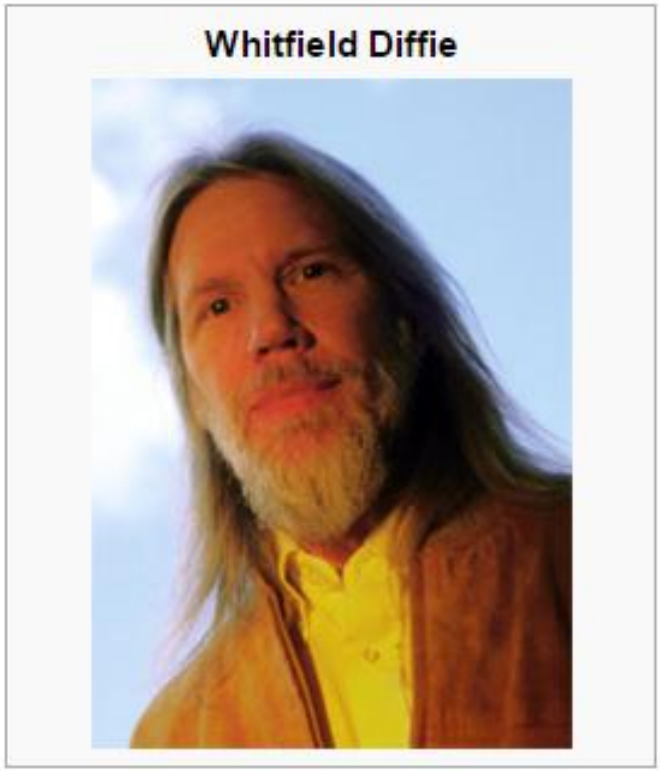
  100 χρήστες → **4.950 κλειδιά (!)**

  1.000 χρήστες → **499.500 κλειδιά (!!!)**
- Μπορούν η Alice και ο Bob να συνεννοηθούν με **ασφαλή τρόπο** για το ποιο κλειδί θα χρησιμοποιήσουν;



Κρυπτογράφηση δημοσίου κλειδιού

- Παρουσιάστηκε για πρώτη φορά το **1976** από τους **Whitfield Diffie** και **Martin Hellman**

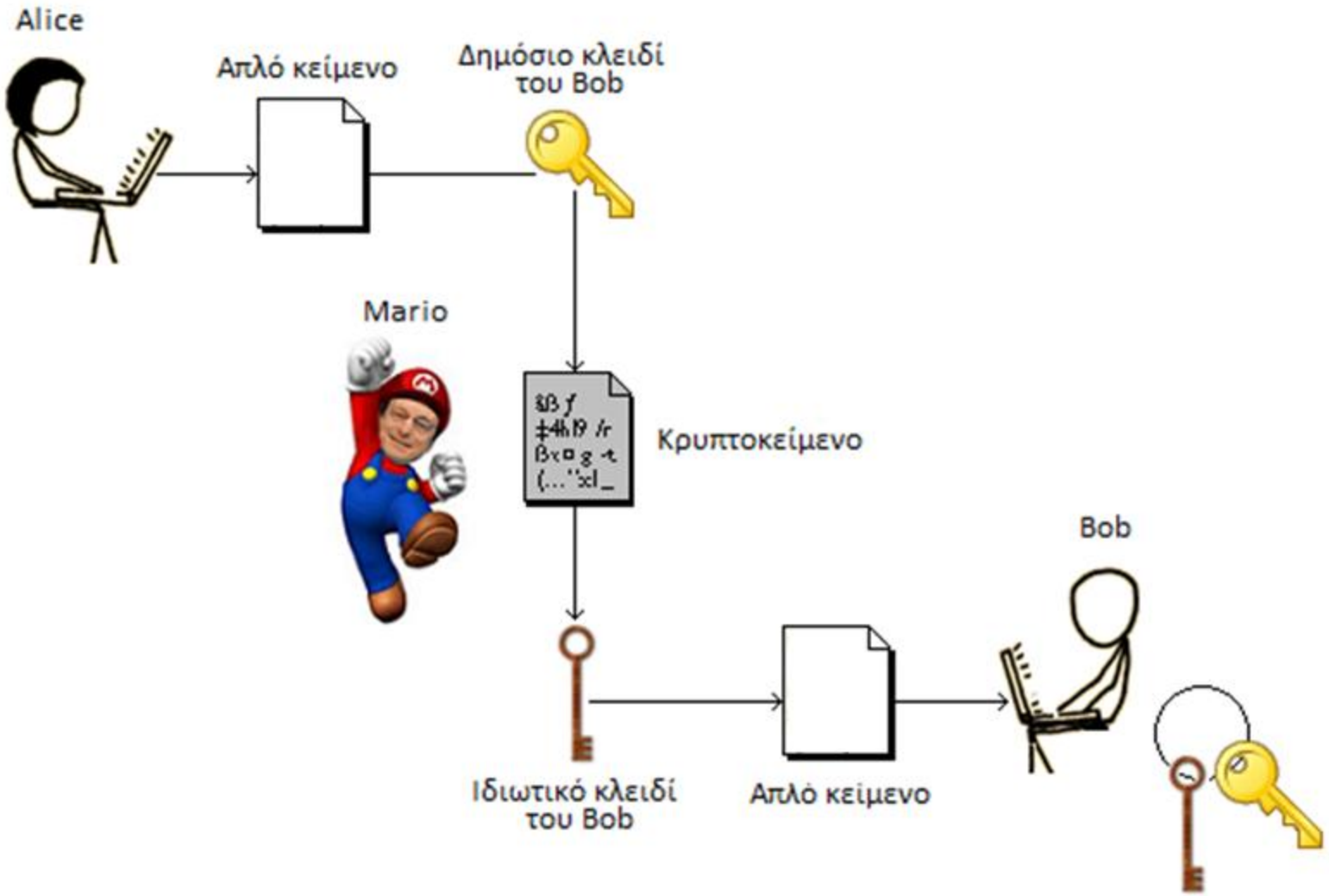


Κρυπτογράφηση δημοσίου κλειδιού

- Η Alice και ο Bob **δεν χρησιμοποιούν το ίδιο κλειδί**
- Κάθε χρήστης έχει **δύο κλειδιά**
  - **Ιδιωτικό κλειδί** (παραμένει κρυφό)
  - **Δημόσιο κλειδί** (κοινοποιείται)

- Η Alice θέλει να στείλει ένα email στον Bob
- **Κρυπτογραφεί** το απλό κείμενο με το **δημόσιο** κλειδί του Bob και στέλνει το κρυπτοκείμενο στον Bob
- Ο Bob **αποκρυπτογραφεί** το κρυπτοκείμενο με το **ιδιωτικό** κλειδί του και διαβάζει το απλό κείμενο
- Ο Mario βλέπει μόνο το κρυπτοκείμενο
- Δημοφιλή συστήματα: **RSA, ElGamal** κ.ά.

Κρυπτογράφηση δημοσίου κλειδιού



Πλεονεκτήματα κρυπτογράφησης δημοσίου κλειδιού

- Το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να μεταδοθεί ή να αποκαλυφθεί
- 2 χρήστες → 4 κλειδιά

  10 χρήστες → 20 κλειδιά

  100 χρήστες → 200 κλειδιά

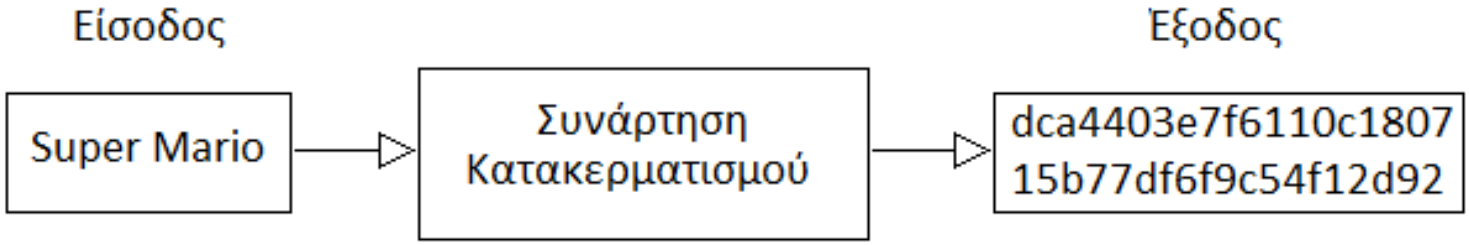
  1.000 χρήστες → **2.000 κλειδιά (≪ 499.500)**

Μειονεκτήματα κρυπτογράφησης δημοσίου κλειδιού

- Βασικό μειονέκτημα η **ταχύτητα** (μεγάλα κλειδιά)
- Υπάρχουν δημοφιλείς μέθοδοι κρυπτογράφησης συμμετρικού κλειδιού που είναι πολύ πιο γρήγορες

Συναρτήσεις κατακερματισμού

- Μαθηματικές συναρτήσεις
- Δέχονται στην είσοδο ένα μήνυμα και παράγουν στην έξοδο «αλαμπουρνέζικα»
- Η είσοδος έχει αυθαίρετο μέγεθος
- Η έξοδος έχει συγκεκριμένο μέγεθος (π.χ. 160 bits)



- Χρησιμοποιούνται και στις **ψηφιακές υπογραφές**
- Δημοφιλείς συναρτήσεις: **MD5, SHA-1, SHA-2** κ.ά.

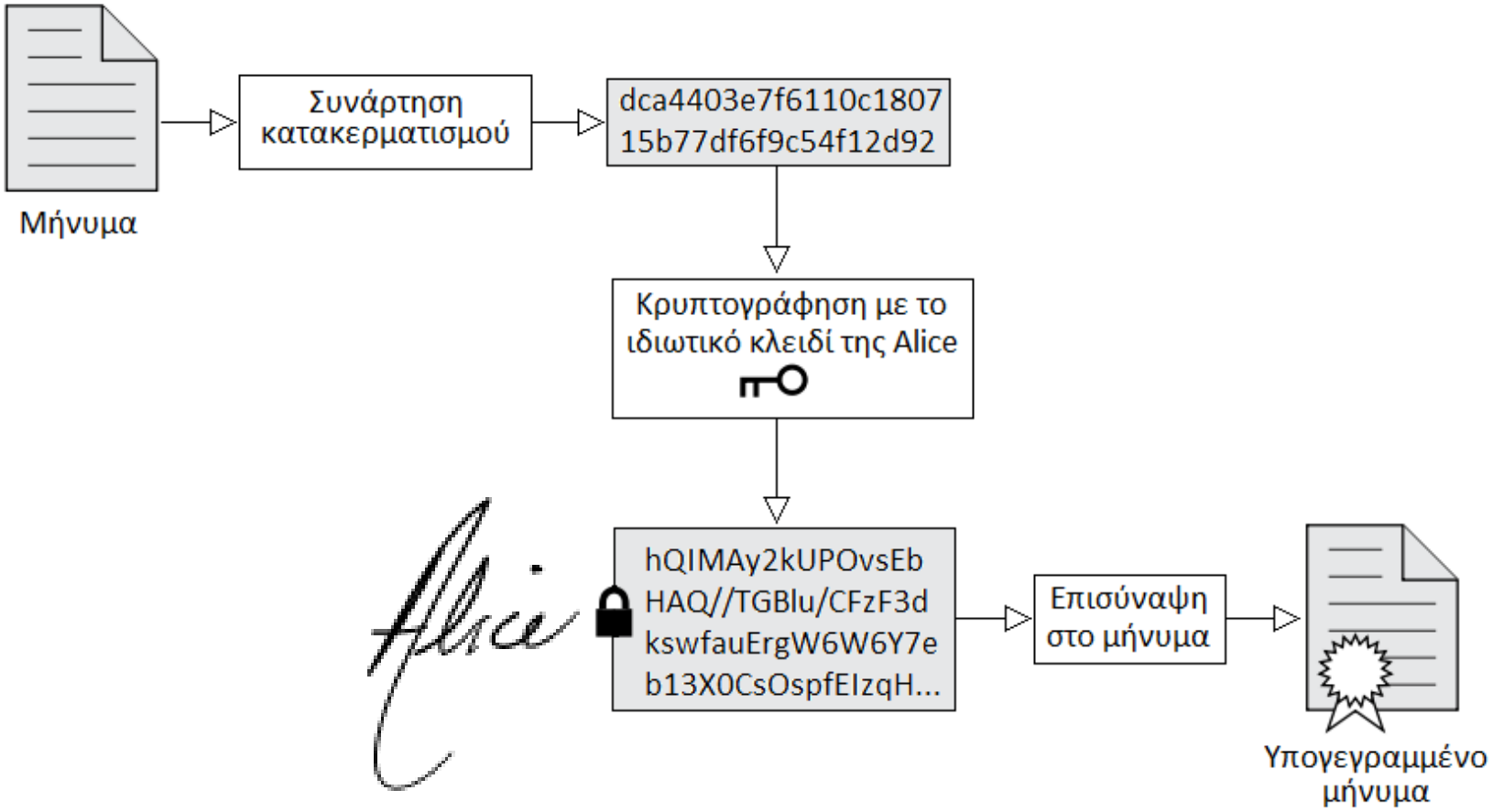
Ιδιότητες συναρτήσεων κατακερματισμού

- Μπορούμε να υπολογίσουμε **εύκολα** την έξοδο για οποιαδήποτε είσοδο
- Δεν μπορούμε να βρούμε **εύκολα** την είσοδο από την έξοδο
- Δεν μπορούμε να βρούμε **εύκολα** δύο διαφορετικές εισόδους που δίνουν το ίδιο αποτέλεσμα στην έξοδο
- **Αν αλλάξει η είσοδος, τότε αλλάζει και η έξοδος**

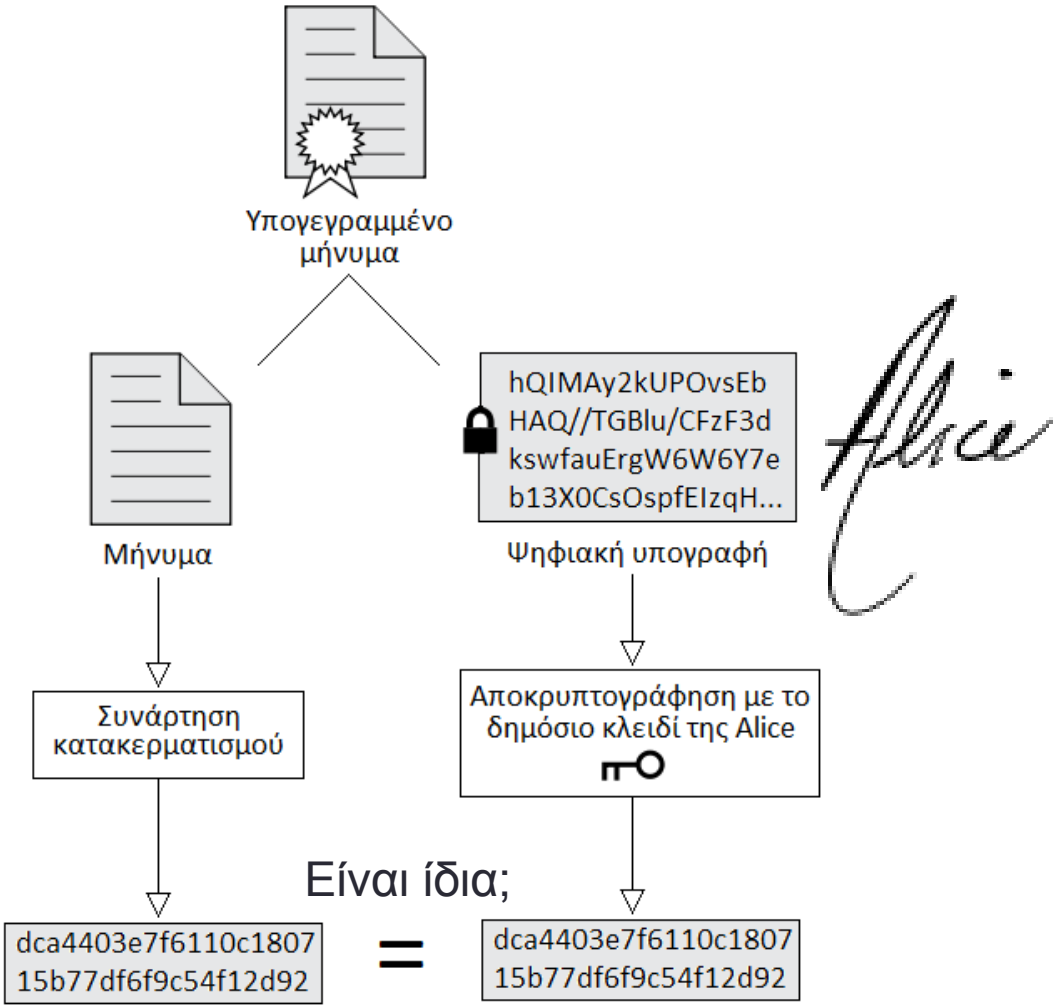
Ψηφιακές υπογραφές

- Κάθε χρήστης έχει **δύο κλειδιά**
  - **Ιδιωτικό κλειδί** (παραμένει κρυφό)
  - **Δημόσιο κλειδί** (κοινοποιείται)
- Η Alice θέλει να στείλει ένα email στον Bob
- Ο Bob θέλει να επιβεβαιώσει ότι το email ανήκει όντως στην Alice
- Η Alice **υπογράφει** το email με το **ιδιωτικό** κλειδί της και στέλνει το υπογεγραμμένο email στον Bob
- Ο Bob χρησιμοποιεί το **δημόσιο** κλειδί της Alice για να **επιβεβαιώσει** ότι το email ανήκει όντως στην Alice
- Η υπογραφή εξαρτάται από το περιεχόμενο του email
  - Αν αλλάξει το περιεχόμενο, τότε η υπογραφή παύει να είναι έγκυρη

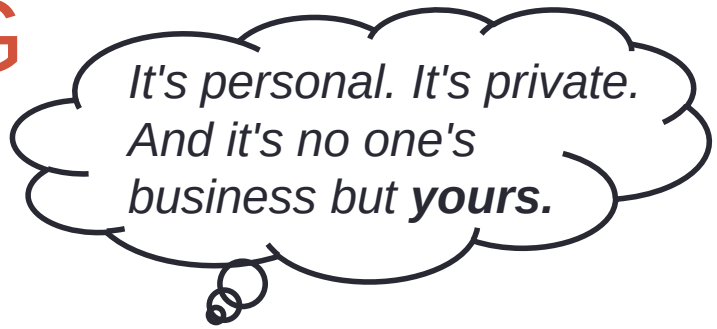
Πώς υπογράφει η Alice;



Πώς επιβεβαιώνει ο Bob;



Λίγη ιστορία του GPG



- **Pretty Good Privacy (PGP)**
  - **Phil Zimmerman, 1991**
  - Επιπλέον μελέτη: *Why I wrote PGP*, του Phil Zimmerman
- Προβλήματα με την Αμερικανική Δικαιοσύνη
- Προβλήματα με πατέντες (RSA)
- **OpenPGP**
  - **Ανοιχτό πρότυπο** για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων – **έχετε γεια πατεντούλες** ☺
- **GPG**
  - **Werner Koch, 1999**
  - Ελεύθερο λογισμικό, εναλλακτική στο PGP
  - Ακολουθεί το πρότυπο του OpenPGP

Στόχοι του GPG

- Μυστικότητα
- Έλεγχος ακεραιότητας
- Μη απάρνηση

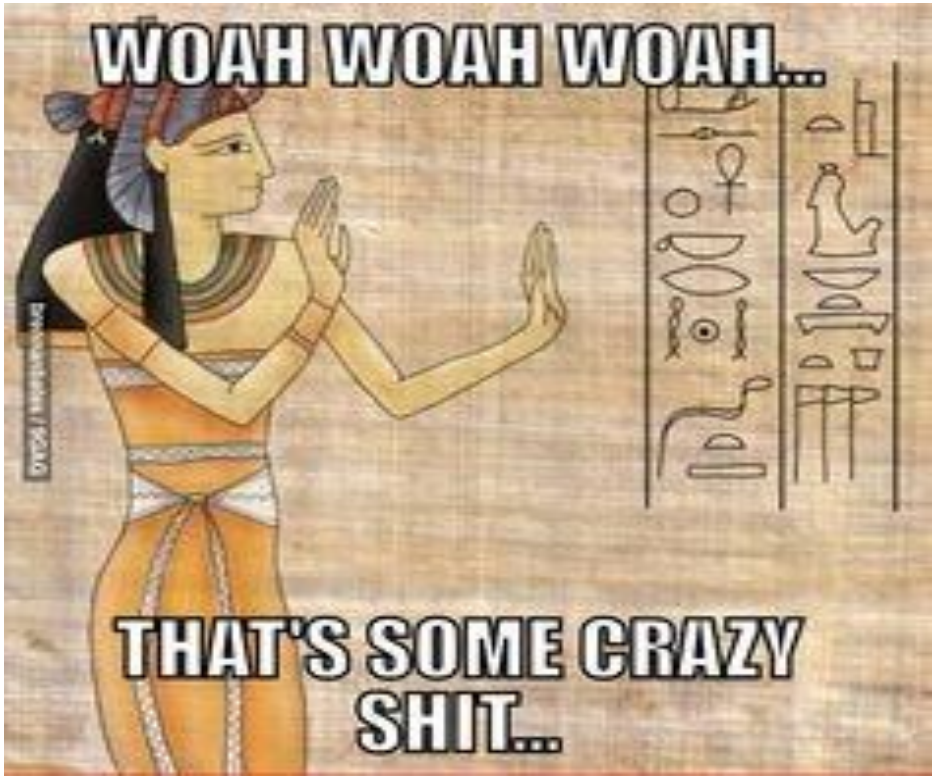
} Πιστοποίηση αυθεντικότητας

- Πώς τους πετυχαίνει;

Μυστικότητα	Έλεγχος ακεραιότητας	Μη απάρνηση
Κρυπτογράφηση δημοσίου κλειδιού	Ψηφιακές υπογραφές	Ψηφιακές υπογραφές

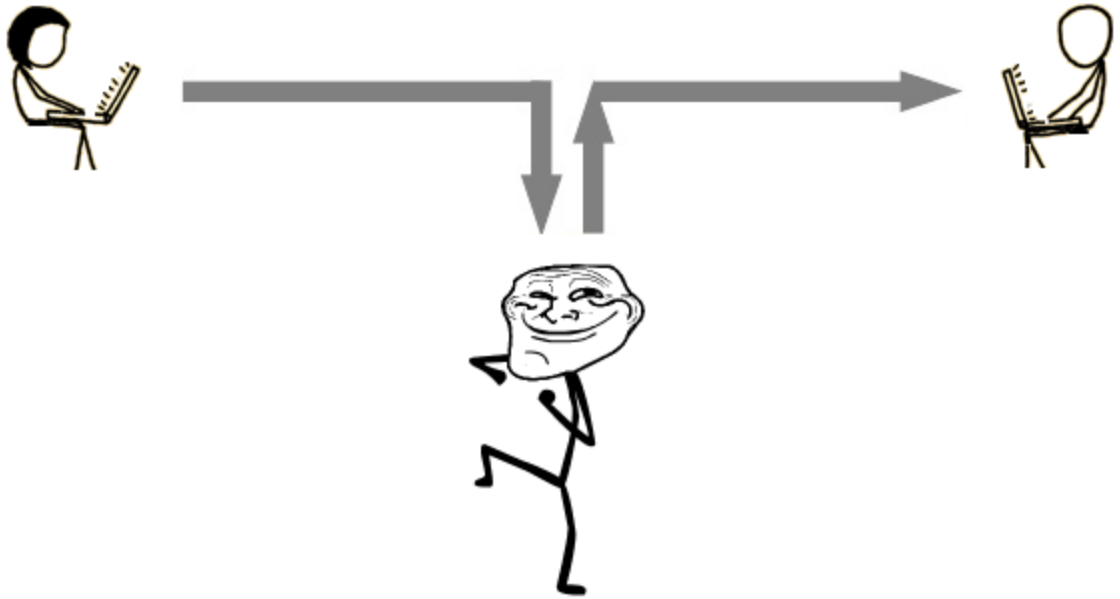
Μυστικότητα

- Το μήνυμα είναι **ακατανόητο** σε κάποιον τρίτο ($#%^@%)



Έλεγχος ακεραιότητας

- Μπορούμε να είμαστε βέβαιοι ότι το μήνυμα που λάβαμε ήταν όντως αυτό που στάλθηκε, και όχι κάτι που τροποποίησε στη διαδρομή κάποιος κακόβουλος χρήστης



Μη απάρνηση

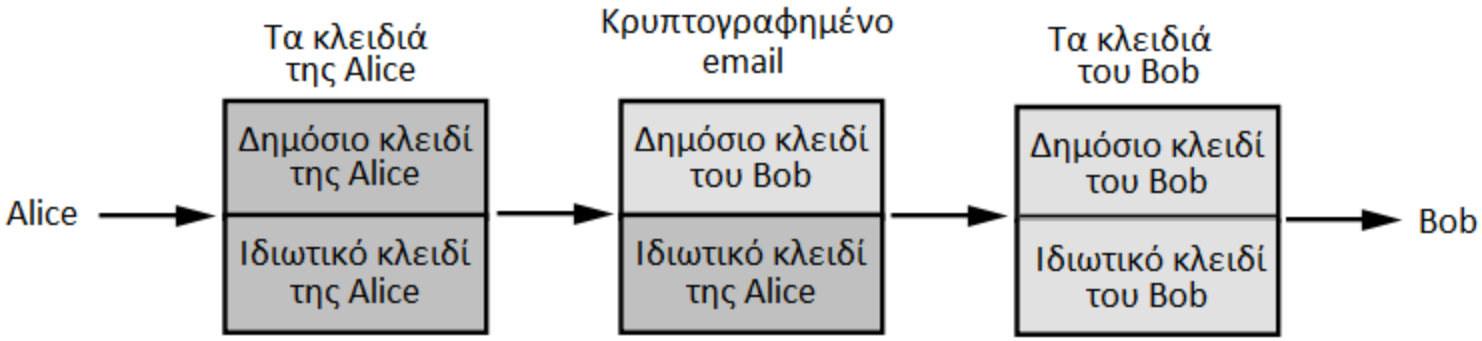
- Παράδειγμα: Πώς αποδεικνύεται ότι ο Χαρδούβελης όντως πρότεινε περικοπή συντάξεων στο περιβόητο email, όταν αργότερα αυτός ισχυρίζεται ότι δεν πρότεινε; Την κολοκυθιά θα παίξουμε τώρα;!

Πιστοποίηση αυθεντικότητας

- Γνωρίζουμε ότι
  - Το μήνυμα είναι ακατανόητο σε τρίτους
  - Το μήνυμα δεν έχει τροποποιηθεί
  - Ο αποστολέας του μηνύματος δεν μπορεί να ισχυριστεί ότι δεν το έστειλε ή ότι έστειλε κάτι άλλο
- Άρα το μήνυμα είναι **αυθεντικό**

GPG = Ψηφιακές Υπογραφές + Κρυπτ. Δημοσίου Κλειδιού

- Η Alice θέλει να στείλει ένα email στον Bob
- Υπογράφει το email με το ιδιωτικό κλειδί της
- Κρυπτογραφεί με το δημόσιο κλειδί του Bob
- Ο Bob αποκρυπτογραφεί με το ιδιωτικό κλειδί του
- Χρησιμοποιεί το δημόσιο κλειδί της Alice για να επιβεβαιώσει ότι το email ανήκει όντως στην Alice



Πού μπορούμε να βρούμε το GPG;

- Αν χρησιμοποιούμε Linux
  - Κατά πάσα πιθανότητα το έχουμε ήδη ☺
- Αν χρησιμοποιούμε Windows ή OS X
  - https://www.gnupg.org/download/index.html
  - Κάνουμε εγκατάσταση
- Έστω ότι χρησιμοποιούμε Linux

Πώς δημιουργούμε ένα GPG κλειδί;

- gpg --full-gen-key
- Επιλέγουμε τύπο κλειδιού
  - **RSA and RSA** (συστήνεται)
- Ορίζουμε μέγεθος κλειδιού
  - 4096 bits (συστήνεται)
- Ορίζουμε ημερομηνία λήξης κλειδιού
  - 1 χρόνος (συστήνεται)
  - Ανανεώνεται εύκολα
- Συμπληρώνουμε τα πραγματικά μας στοιχεία
  - Ονοματεπώνυμο
  - Email
- Ορίζουμε **passphrase**

Passphrase

- *"Think about a **common phrase that works for you**. It's **too long to brute force** and also make them **unlikely to be in the dictionary.**"*

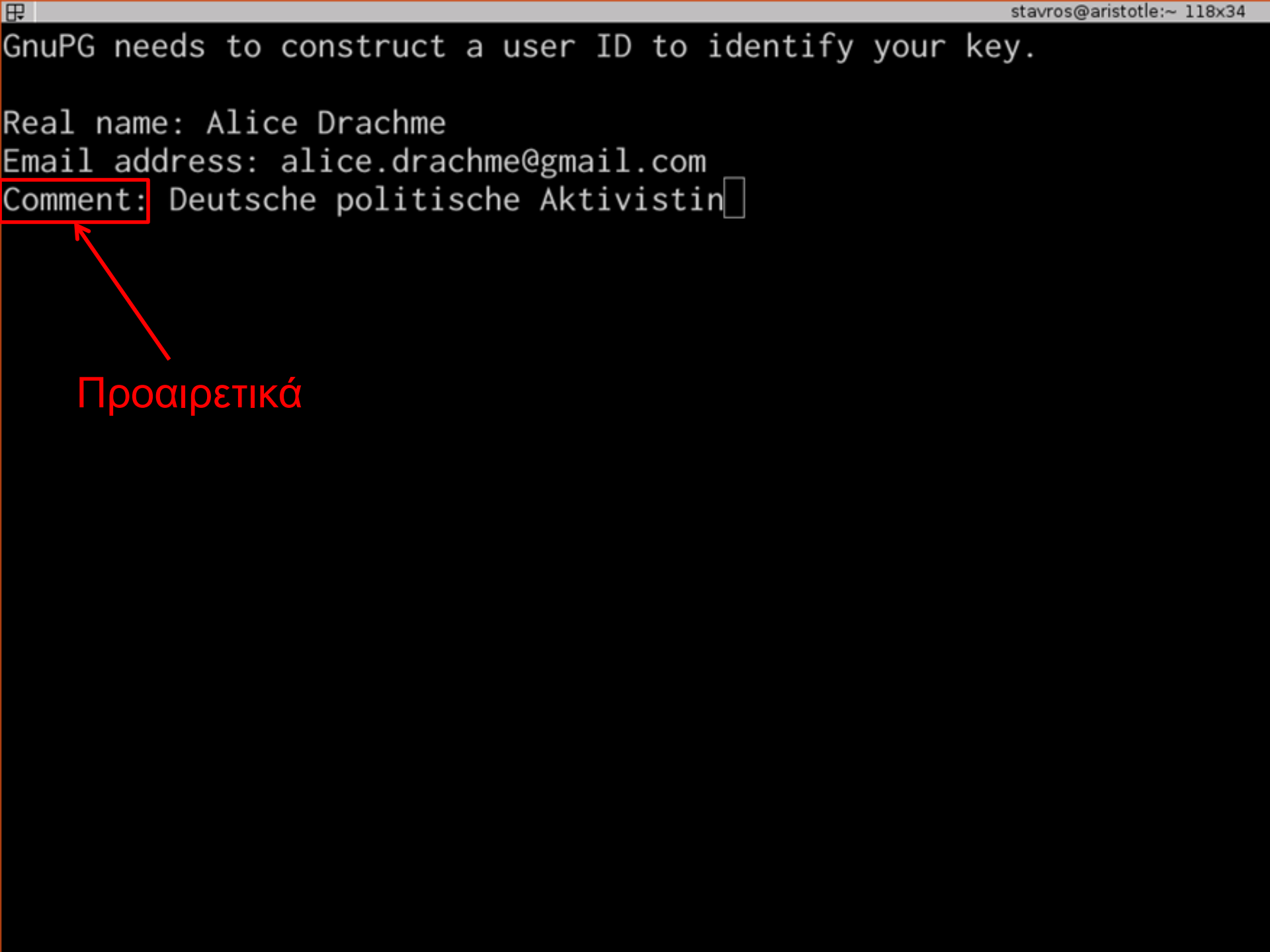
  – Edward Snowden
- Πρέπει να το θυμόμαστε εύκολα
- Πρέπει να είναι δύσκολο να το μαντέψει κάποιος
- Παράδειγμα: "d3n.yp@rxei.p3riptwsh.n4.to.vre1s!!"
- **Προστατεύει το ιδιωτικό κλειδί**
  - Το ιδιωτικό κλειδί κρυπτογραφείται με το passphrase και αποθηκεύεται στον δίσκο
- **Αν ξεχάσουμε το passphrase, δεν μπορούμε πια να υπογράφουμε ή να αποκρυπτογραφούμε**

```
[stavros@aristotle ~]$ gpg2 --full-gen-key
gpg (GnuPG) 2.1.6; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
```

```
[stavros@aristotle ~]$ gpg2 --full-gen-key
gpg (GnuPG) 2.1.6; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
```

```
[stavros@aristotle ~]$ gpg2 --full-gen-key
gpg (GnuPG) 2.1.6; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 1y
```

```
[stavros@aristotle ~]$ gpg2 --full-gen-key
gpg (GnuPG) 2.1.6; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 1y
Key expires at Tue 05 Jul 2016 03:27:29 PM EEST
Is this correct? (y/N) y
```

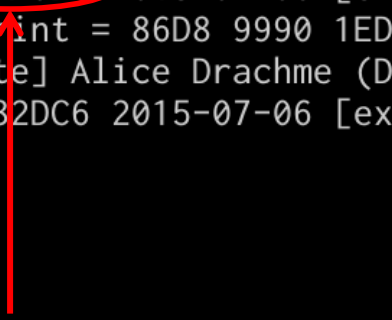

stavros@aristotle:~ 118x34
GnuPG needs to construct a user ID to identify your key.
Real name: Alice Drachme
Email address: alice.drachme@gmail.com
Comment: Deutsche politische Aktivistin
Προαιρετικά

```
GnuPG needs to construct a user ID to identify your key.

Real name: Alice Drachme
Email address: alice.drachme@gmail.com
Comment: Deutsche politische Aktivistin
You selected this USER-ID:
    "Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gm

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

```
GnuPG needs to construct a user ID to identify your key.

Real name: Alice Drachme
Email address: alice.drachme@gmail.com
Comment: Deutsche politische Aktivistin
You selected this USER-ID:
    "Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/stavros/.gnupg/trustdb.gpg: trustdb created
gpg: key BA8FA0D6 marked as ultimately trusted
gpg: directory '/home/stavros/.gnupg/openpgp-revocs.d' created
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-07-05
pub   rsa4096/BA8FA0D6 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 86D8 9990 1EDD 7E95 83AA  D04C 004E CF54 BA8F A0D6
uid       [ultimate] Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>
sub   rsa4096/7AA82DC6 2015-07-06 [expires: 2016-07-05]
```

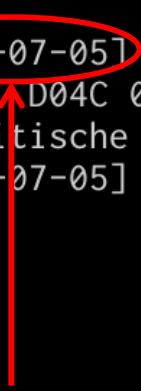
```
gpg: /home/stavros/.gnupg/trustdb.gpg: trustdb created
gpg: key BA8FA0D6 marked as ultimately trusted
gpg: directory '/home/stavros/.gnupg/openpgp-revocs.d' created
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-07-05
pub   rsa4096/BA8FA0D6 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 86D8 9990 1EDD 7E95 83AA  D04C 004E CF54 BA8F A0D6
uid       [ultimate] Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>
sub   rsa4096/7AA82DC6 2015-07-06 [expires: 2016-07-05]
```

```
gpg: /home/stavros/.gnupg/trustdb.gpg: trustdb created
gpg: key BA8FA0D6 marked as ultimately trusted
gpg: directory '/home/stavros/.gnupg/openpgp-revocs.d' created
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-07-05
pub   rsa4096/BA8FA0D6 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 86D8 9990 1EDD 7E95 83AA  D04C 004E CF54 BA8F A0D6
uid       [ultimate] Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>
sub   rsa4096/7AA82DC6 2015-07-06 [expires: 2016-07-05]
```



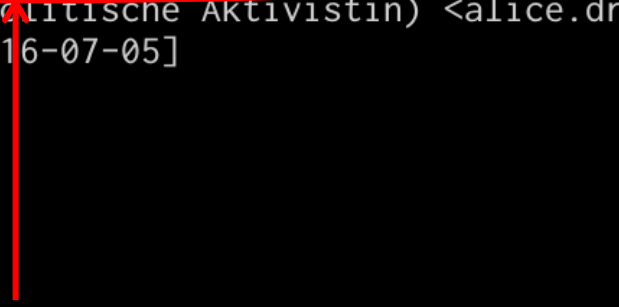
Αναγνωριστικό κλειδιού

```
gpg: /home/stavros/.gnupg/trustdb.gpg: trustdb created
gpg: key BA8FA0D6 marked as ultimately trusted
gpg: directory '/home/stavros/.gnupg/openpgp-revocs.d' created
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-07-05
pub   rsa4096/BA8FA0D6 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 86D8 9990 1EDD 7E95 83AA  D04C 004E CF54 BA8F A0D6
uid       [ultimate] Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>
sub   rsa4096/7AA82DC6 2015-07-06 [expires: 2016-07-05]
```



Ημερομηνία λήξης

```
gpg: /home/stavros/.gnupg/trustdb.gpg: trustdb created
gpg: key BA8FA0D6 marked as ultimately trusted
gpg: directory '/home/stavros/.gnupg/openpgp-revocs.d' created
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-07-05
pub   rsa4096/BA8FA0D6 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 86D8 9990 1EDD 7E95 83AA  D04C 004E CF54 BA8F A0D6
uid       [ultimate] Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>
sub   rsa4096/7AA82DC6 2015-07-06 [expires: 2016-07-05]
```



Αποτύπωμα κλειδιού

```
gpg: /home/stavros/.gnupg/trustdb.gpg: trustdb created
gpg: key BA8FA0D6 marked as ultimately trusted
gpg: directory '/home/stavros/.gnupg/openpgp-revocs.d' created
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2016-07-05
pub   rsa4096/BA8FA0D6 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 86D8 9990 1EDD 7E95 83AA  D04C 004F CF54 BA8F A0D6
uid       [ultimate] Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>
sub   rsa4096/7AA82DC6 2015-07-06 [expires: 2016-07-05]
```


Ονοματεπώνυμο, σχόλια και email

Φύλαγε τα ρούχα σου να έχεις τα μισά

- Χάνουμε το ιδιωτικό κλειδί
- Ή μας το κλέβουν
- Ή ξεχνάμε το passphrase
- Δεν υπάρχει «ό,τι βρέξει ας κατεβάσει» ☺
- Μετά την δημιουργία του GPG κλειδιού, δημιουργούμε αμέσως ένα **πιστοποιητικό ανάκλησης**
- Αν συμβεί το κακό, δημοσιεύουμε το πιστοποιητικό ανάκλησης
- Έτσι προειδοποιούμε τους άλλους χρήστες να μην χρησιμοποιούν πλέον το συγκεκριμένο κλειδί για να επικοινωνούν μαζί μας

Πώς δημιουργούμε ένα πιστοποιητικό ανάκλησης;

Αναγνωριστικό

- gpg -a --output bob.asc.revoke --gen-revoke F3E27C0D

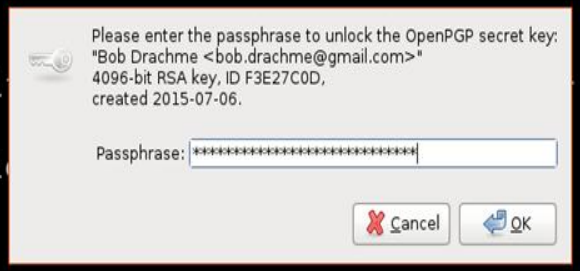
- Αποθηκεύουμε το πιστοποιητικό σε ένα ασφαλές μέσο
- Το εκτυπώνουμε (ακόμα καλύτερα)

```
[stavros@aristotle ~]$ gpg -a --output bob.drachma@gmail.com.asc.revoke --gen-revoke F3E27C0D

sec  rsa4096/F3E27C0D 2015-07-06 Bob Drachme <bob.drachme@gmail.com>

Create a revocation certificate for this key? (y/N) y
```

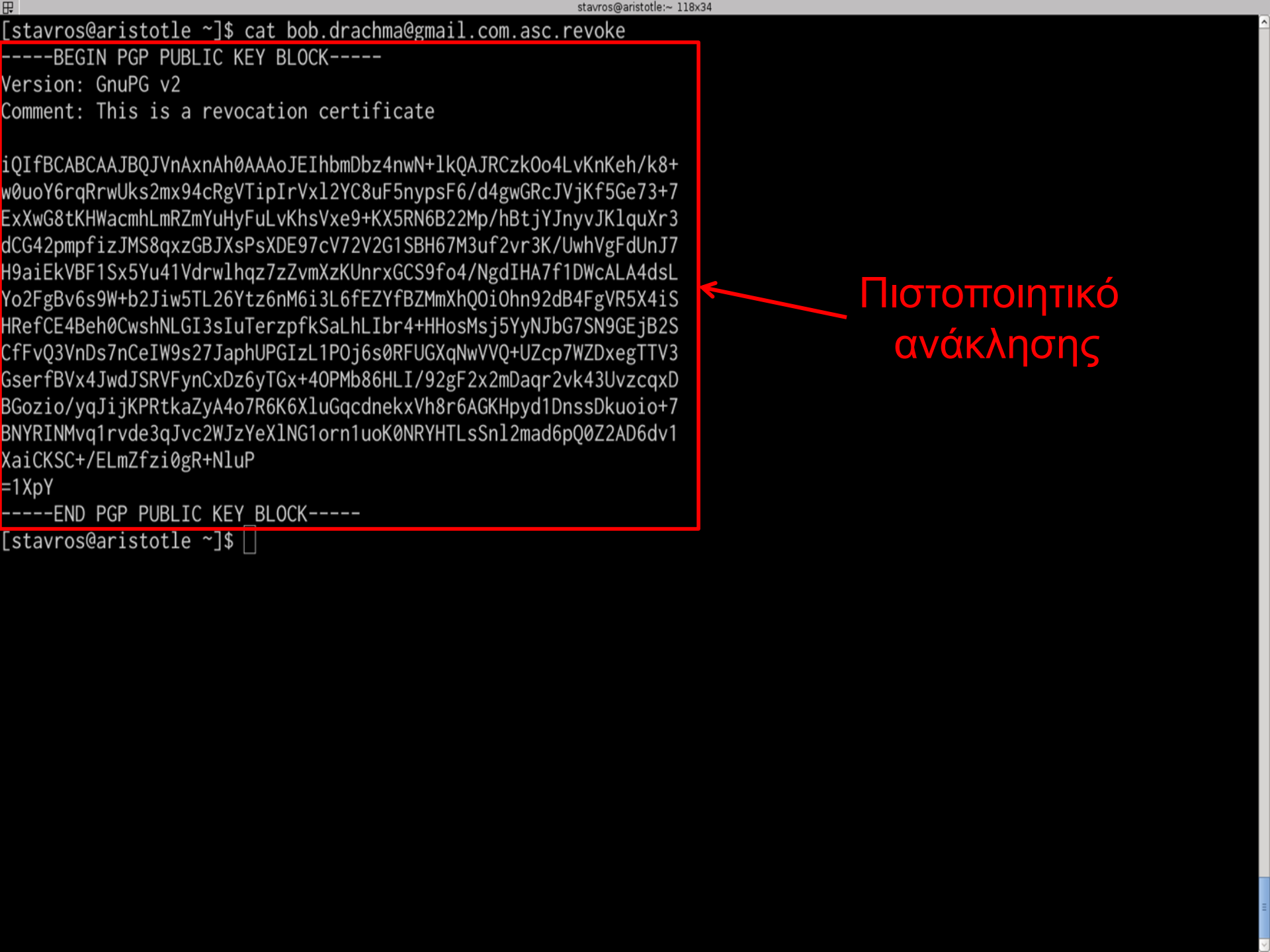
```
[stavros@aristotle ~]$ gpg -a --output bob.drachma@gmail.com.asc.revoke --gen-revoke F3E27C0D

sec  rsa4096/F3E27C0D 2015-07-06 Bob Drachme <bob.drachme@gmail.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 0
```

```
[stavros@aristotle ~]$ gpg -a --output bob.drachma@gmail.com.asc.revoke --gen-revoke F3E27C0D

sec  rsa4096/F3E27C0D 2015-07-06 Bob Drachme <bob.drachme@gmail.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 0
Enter an optional description; end it with an empty line:
>
Reason for revocation: No reason specified
(No description given)
Is this okay? (y/N) y
```

```
[stavros@aristotle ~]$ gpg -a --output bob.drachma@gmail.com.asc.revoke --gen-revoke F3E27C0D

sec  rsa4096/F3E27C0D 2015-07-06 Bob Drachme <bob.drachme@gmail.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 0
Enter an optional description; end it wi
>
Reason for revocation: No reason specifi
(No description given)
Is this okay? (y/N) y
```



```
[stavros@aristotle ~]$ gpg -a --output bob.drachma@gmail.com.asc.revoke --gen-revoke F3E27C0D

sec  rsa4096/F3E27C0D 2015-07-06 Bob Drachme <bob.drachme@gmail.com>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 0
Enter an optional description; end it with an empty line:
>
Reason for revocation: No reason specified
(No description given)
Is this okay? (y/N) y
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!
```


stavros@aristotle:~ 118x34
[stavros@aristotle ~]$ cat bob.drachma@gmail.com.asc.revoke
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2
Comment: This is a revocation certificate
iQIfBCABCAAJBQJVnAxnAh0AAAoJEIhbmDbz4nwN+lkQAJRCzkOo4LvKnKeh/k8+
w0uoY6rqRrwUks2mx94cRgVTipIrVxl2YC8uF5nypsF6/d4gwGRcJVjKf5Ge73+7
ExXwG8tKHWacmhLmRZmYuHyFuLvKhsVxe9+KX5RN6B22Mp/hBtjYJnyvJKlquXr3
dCG42pmpfizJMS8qxzGBJXsPsXDE97cV72V2G1SBH67M3uf2vr3K/UwhVgFdUnJ7
H9aiEkVBF1Sx5Yu41Vdrwlhqz7zZvmXzKUnrxGCS9fo4/NgdIHA7f1DWcALA4dsL
Yo2FgBv6s9W+b2Jiw5TL26Ytz6nM6i3L6fEZYfBZMmXhQOiOhn92dB4FgVR5X4iS
HRefCE4Beh0CwshNLGI3sIuTerzpfkSaLhLIbr4+HHosMsj5YyNJbG7SN9GEjB2S
CfFvQ3VnDs7nCeIW9s27JaphUPGIzL1POj6s0RFUGXqNwVVQ+UZcp7WZDxegTTV3
GserfBVx4JwdJSRVFynCxDz6yTGx+4OPMb86HLI/92gF2x2mDaqr2vk43UvzcqxD
BGozio/yqJijKPRtkaZyA4o7R6K6XluGqcdnekxVh8r6AGKHpyd1DnssDkuoio+7
BNYRINMvq1rvde3qJvc2WJzYeXlNG1orn1uoK0NRYHTLsSnl2mad6pQ0Z2AD6dv1
XaiCKSC+/ELmZfzi0gR+NluP
=1XpY
-----END PGP PUBLIC KEY BLOCK-----
[stavros@aristotle ~]$
Πιστοποιητικό ανάκλησης

Πώς εξάγουμε το δημόσιο κλειδί μας;

- gpg --armor --export alice.drachme@gmail.com
  - Εμφανίζεται στην οθόνη
  - Σε μορφή κατανοητή από τον άνθρωπο

- gpg --armor --export alice.drachme@gmail.com **>** key.gpg
  - Αποθηκεύεται σε αρχείο

```
[stavros@aristotle ~]$ gpg --armor --export alice.drachme@gmail.com
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQINBFWa7TgBEACi/KYVQ04fcgnX9Kk//und+PwmcU211ae9JZ26YxNxUAp9MGm6
lcWOpqhZuKFHAxbxWlsDUk6x2JySVorWubcbA0j2qIpLwvwObcwRD2iaZWAdfMqP
DIU01N0JLrWnT8F3GLc58jfETIPWoAC2d2EKLrrDpUWpyrfL5rSydWfawkxxiReN
wKVe3GY0BS6mjh3UvzKtSEAJ2ZClhfizdysMKj+F/9eQf5XiS/P2qM62u1j1vu7B
hLsFVwf1wB6cJcExuApqWm2qcHAC6NoWKDDnIulG4Xyw1ZJjtlYbn1KXrqKdtYet
1v5TDfHx0cgxYjLleChMHKWnm1/Sl1Zkq4f1dO2k7xj9LdGDhpqxV0up2+QPUPwR
CeIloxyUvDBR/XWnogdiw5WGOxdjtoqrf6Nylgnc4+celSoKmhk5ODpHBh5+ApAf
tMrzwB1pdgxWPU1abnlzpWUmgus7wVafHMAhuFJxaUnUHOPiFc5zSXyuwF0YK0HI
NQIzLa0dE5EsJ9q4Gy2fBYxKvt8RowPvqoCqiwU6kVxXMzYDOM/yYxzSRNRH0qey
zWRL5qDktOw4FApgV/OFHqEyAMmeCbdpOAbvvlUFxNg395E/eD1ublagfQX7VAk8
MSsBgIwO3JlN8ZfZR+saQbSnThhPFLg8etjY70+3E3ZL80tBea+pN/OpwwARAQAB
tCNCb2IgRHJhY2htZSA8Ym9iLmRyYWNobWVAZ21haWwuY29tPokCPQQTAQgAJwUC
VZrtOAIbAwUJAeEzgAULCQgHAgYVCAkKCwIEFgIDAQIeAQIXgAAKCRCIW5g28+J8
DXmBD/9E97KktTZyflS45UPqT74QILG2wqLDl5lp/bFcej7i3ZkxwkgLeHBCw4ek
ORS7Hya4ZFenhHHj+YWEXLdCc2m5RKV8sOHrFJATVLPmP5Tx2MDh/mjZOKSw3RMn
rcshaqGndV0RieWkSeeF0gq3boKJgmHhZeBeLS5EEPhGJCwIhrEpFQ6AFcJZtxlj
fPWXBd10hY3i4sO9qnhC8n8DL6P0reiCO4XyJVIUtLW38K8GcTULHejdArRJowb4
aBqrmqgdejcHHP5QvGJ/rQuMCM/ViRcLQeXZgMoPHe93cMGMLJc7UgxVcJbJf1VT
dUwBB25ZBZDQJrL++ltNf9Z90HKLN9Q/tQ3V8jUu25koficUzj9xCSJ/VCX+IUX6
J6WXTO/4u9HGwxiV45OKfeNWrobkF7xGbhy9ibs+IL1UBOv0zRgFs40+TlrGKFqg
PZe0SJHJdQJJmoPOWZ5X4aWs9ZNaHTy9uaVVCg64kzQh3yIkTYje6u3xti9KcZAZ
zwEJpk5KVzRK882gllHuIj+OrOmlUfKMchrQiu3Ro7tv1mR2Eq1WarKt6TurULIE
lWN1qfb6F4MMHZL9yrIJsdh/UQmTwVWFJ2S9Y8ezP5doxHvoviVzX9sf4mGxiKeG
TOetaQuPOSXg7YUG+FQuNEmE93UmFkrzazWAggiOozZ8VeNFU7kCDQRVmu04ARAA
mFpXiLTigZGUFr4omVm/LXljsj4Xw6g5byCLne/lBFdLxYw2192NUrzxZXd+thsG
VC6QSJKGfEI9tXwd2ERwqoZJ43LwCNJt9LYphnRRYzTrM26Od9B4aJjoHRZ13Mkv
oPkbInBSWOmufCFL7kYRo9B1EJDHgQO03iL/MZc9T5+0EfFEhQVmsE7IU6nmTTvh
sa+SvEXcbB/2RX0FZTRljw2rtrn1hTGa3Hib9n8XLcCQedSkjhILB51SEBFo3uOx
an9ndKuyvd0UZsxxD7r3J2mLuYz1QZ7Q+7buHHGKgpK7RCFa6z4Bx/6qfveaxr8h
ZasRawDvwzxsWNTh7SqrVNEbWD+r0hpNiNBzknuSk4PvwhJygJffRgl4mJ+zJ02j
k++CAisxRSGn6kpYk0dE8xrmzxFP2aN2DoRN44ngs2kv1Z5NisPi2gac+OIWHm+A
8x82VJ/vPWDHKDWXUjNg46DPCcdIJmHCHZc9CTetJhJENIDWHmYUbFsT4q7JMvrz
2Z0i4iyj39dvBH3rmXnjq5BrvUZYSsOBTNXP2TXFH9T2seiB9eC5OKleXwoSi28H
4m9rtgJIm8cAUkH1QRqzz0PE+0E4Z9AeaXagObKTraw0Z6/GGIQyVAJExZ53HaMR
7igVMW66uXQIUwW2DKVJrOwRrLU4xm/ItQ+HbIVDRf8AEQEAAYkCJQQYAQgADwUC
VZrtOAIbDAUJAeEzgAAKCRCIW5g28+J8DbxmD/9Ew8t0XhnIk3BEy6MTlwBSniyI
9UeKsM/GMmk4dwrvwJ4xneiUYhB4XWaDvev8j1Tk/hqHqiIq4VL2h2cJwFGMeMrt
AX9Q4Ads2BGi37aFR4ASFLRFChZQE6HfCvW+OZ5ty5bd2tKYrGSBQlNvRDuzsDkI
9/8R6zwUFP3A/Q4r5LpAv5C/4I0l2JPsG5otmwOw51qEKqS/1sSZVkvoCQi31Xq1
LhKNH0IKDTrdHtByKe2dixaRuXzcpTbo4dIAB/z/DIFiR+OQ846Ii65qzCEQ0s42
L/cK9eS+JBNI4K17CrveHGYLoy4gfQbOKgCXR859INQyIEnEpkzaJrtjrJ6SXpc5
IyHSFXXhtjTCkgm4tbmcCTW1dJfmzLfWGncOSM8f6iVvHop/US+EKnNxwORFiSlK
OJhFIFo8EDwYQpp2g/Fh4rXPy/E8yg88I7G4/wOgomnChXKYmla+0ZX8diJpczy6
LV4qDHbZ8X5eEB52ikPDuLPo+7zjq7DwvdVP9cgMtM5mglfVN6UwkTgOvLbXqzlU
b/BNN/uZUCXvir/oSZRp7IQU2GATb26xKqRf/1Nc9WWxXTSWX1omO1zRMBynGaqf
wRW12yFZbcfpzOKfRevahGlA2bWVWNwLtuZvEZuVT6pnnx/ql20Q2eb1rEO3DXGt
7rBED5b+9E2PB7uUCg==
=WGUe
-----END PGP PUBLIC KEY BLOCK-----
```

Δημόσιο κλειδί

Πώς εισάγουμε ένα δημόσιο κλειδί;

- gpg --import
- Κάνουμε επικόλληση το δημόσιο κλειδί
- Πατάμε Enter και μετά Ctrl + D

- gpg --import key.gpg
  - Εισαγωγή από αρχείο

Πώς βλέπουμε τα κλειδιά;

- gpg --list-keys
  - Όλα τα δημόσια κλειδιά
- gpg --list-keys bob.drachme@gmail.com
  - Δημόσια κλειδιά με το συγκεκριμένο email
- gpg --list-keys Bob Drachme
  - Δημόσια κλειδιά με το συγκεκριμένο όνομα
- gpg --list-secret-keys
  - Δημόσια κλειδιά για τα οποία έχουμε τα αντίστοιχα ιδιωτικά

```
[stavros@aristotle ~]$ gpg --list-keys
/home/stavros/.gnupg/pubring.kbx
--------------------------------
pub   rsa4096/BA8FA0D6 2015-07-06 [expires: 2016-07-05]
uid       [ultimate] Alice Drachme (Deutsche politische Aktivistin) <alice.drachme@gmail.com>
sub   rsa4096/7AA82DC6 2015-07-06 [expires: 2016-07-05]

pub   rsa4096/F3E27C0D 2015-07-06 [expires: 2016-07-05]
uid       [ unknown] Bob Drachme <bob.drachme@gmail.com>
sub   rsa4096/5567D432 2015-07-06 [expires: 2016-07-05]

pub   rsa4096/EDACEA67 2013-09-06
uid       [ unknown] schneier <schneier@schneier.com>
sub   rsa4096/D7B630DF 2013-09-06

pub   rsa4096/B8DE0B54 2015-07-07 [expires: 2016-07-06]
uid       [ unknown] Stavros Mekesis <smekesis@csd.auth.gr>
sub   rsa4096/42D863F7 2015-07-07 [expires: 2016-07-06]
```

Πού δημοσιεύουμε το δημόσιο κλειδί μας;

- Στην προσωπική μας ιστοσελίδα
- Στο **Facebook**

- Σε έναν **key server**
- Οπουδήποτε

Key server

- Φιλοξενεί δημόσια κλειδιά
- Μπορούμε να ανεβάσουμε το κλειδί μας σε αυτόν
- Μπορούμε να αναζητήσουμε κλειδιά
  - Με βάση τα προσωπικά στοιχεία (ονοματεπώνυμο, email)
  - Με βάση το αναγνωριστικό του κλειδιού (π.χ. 0x**BA8FA0D6**)
- Μπορούμε να κατεβάσουμε κλειδιά
- Δημοφιλείς key servers
  - **MIT PGP Key Server** – https://pgp.mit.edu
  - PGP Global Directory – https://keyserver.pgp.com
  - SKS Key Server Pool – https://sks-keyservers.net

https://pgp.mit.edu

MIT PGP Public Key Server

Help: Extracting keys / Submitting keys / Email interface / About this server / FAQ
Related Info: Information about PGP /

Extract a key

Search String: Do the search!

Index: Verbose Index:

Show PGP fingerprints for keys

Only return exact matches

Submit a key

Enter ASCII-armored PGP key here:

Clear Submit this key to the keyserver!

Remove a key

Search String: Remove the key!

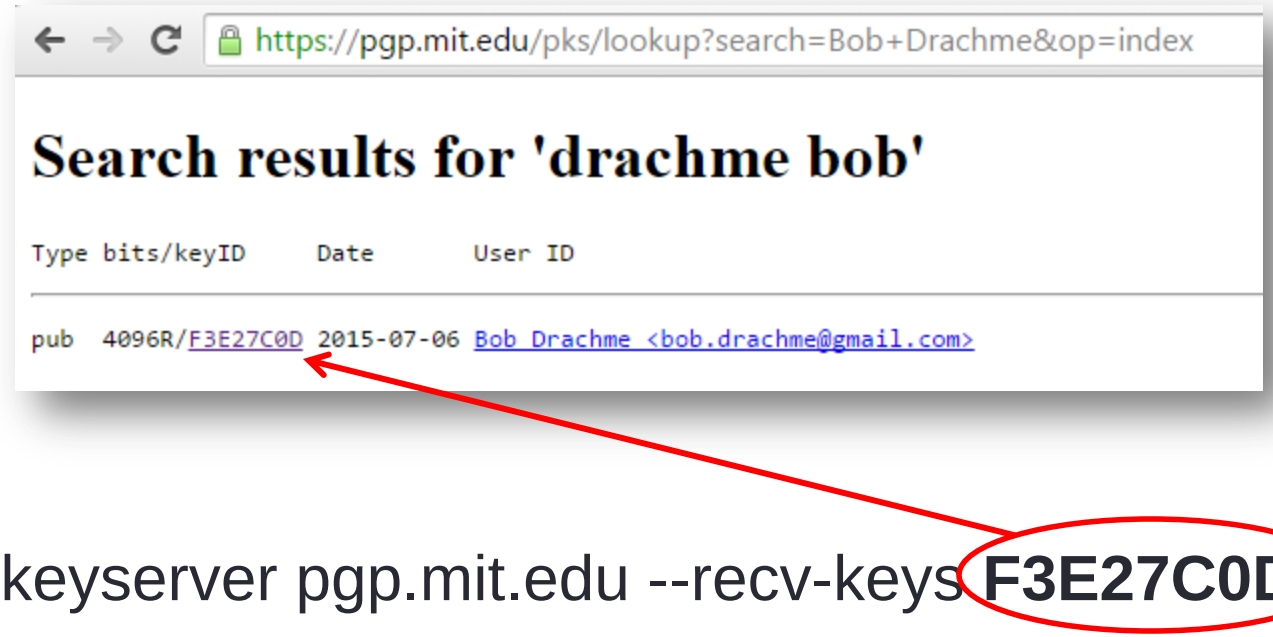
Please send bug reports or problem reports to <bug-pks@mit.edu> only after reading our FAQ.

Πώς ανεβάζουμε το δημόσιο κλειδί μας στον key server;

Αναγνωριστικό

- gpg --keyserver pgp.mit.edu --send-keys **BA8FA0D6**

Πώς κατεβάζουμε ένα δημόσιο κλειδί από τον key server;



- gpg --keyserver pgp.mit.edu --recv-keys **F3E27C0D**

Πώς κρυπτογραφούμε ένα μήνυμα;

- Κατεβάζουμε / εισάγουμε πρώτα το δημόσιο κλειδί του παραλήπτη, αν δεν το έχουμε

- gpg -a --encrypt --recipient bob.drachme@gmail.com
- Γράφουμε το μήνυμα
  - «Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015»
- Πατάμε Enter και μετά Ctrl + D
- Εμφανίζεται το κρυπτογραφημένο μήνυμα

```
[stavros@aristotle ~]$ gpg -a --encrypt --recipient bob.drachme@gmail.com
Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQIMA+xawZxVZ9QyAQ//dYPciPgME1ymJ39fp3zCUm5i4nyo2k1LRRCLHgWV9NxK
qrB/M72nvw1nrPYmr0ZAaN72B05LXDti8B7Jus83B2mHx0i98D7pkmmdE97hVuaZ
YJLOocvpIuzWF6B8zJfN4KHQmcdV2YW/P2uVnzxUC8p6hFC29mxpKWxZQTfIQIzD
tXfGeaKO2tgF9apmb0tx9Ko1niheLb/qELWE107ZFJsTHWKr8/JFDnVovIspsw1S
PDjXW/jch5lGDIhINxGU4z0b3jilY81U3GYSSVYbE/VUmLchcPnnqJ1CdIxzPtIu
B69zDf2LOe4r/yf5CDy2Nr08wCH6irjCpxQ/1Sgu2D+KWea2NBWwSLSjJ5gPAIZu
Vn3H3RGpy4Nf/VSqxW5c5MOKvq87zE7VZfpGzXp7Panb9R/oAWo81cS423KjYjZa
tU68Jaic2hno6qmj8nwrs2eqcFwUzQyrkZN/IMxChA6nGtiNKVHw6M60LU3jyl/v
GKChzv1rtMCvbPO8glEeltwp6o8sAhPsLyVkQZ0IUX20wMl9fCOHORyU+aoWsnim
e5lBMlwxMApQXad7Gm2Rr92X+sCZfUuymOEz+yGw5/B50IJa1pAxBnIRV2OsmL4J
pxvGTL7fckKeMtLUoGHZz5FWeHbPm5zpP1l1ZGUb3TtRZeh04P211WIyRrIVMl3S
hAEluwJt8vKf9fYbrD/7niiFd1cmqIfTZxF02DldQoOAo1gw4H9HiJIbRLZGRnXg
d1tne7r7yVC83KHFjh5FnUDA+RD7ZCND7MZ8bKepMJ274hKQUVeASZtKo/jPzHpi
IWuhaD9bVNTNkHc+2P9GtTgshoCZ5gICVk6CPyyxuCxBlH8rCA==
=C6Ho
-----END PGP MESSAGE-----
```

Πώς αποκρυπτογραφούμε ένα μήνυμα;

- gpg --decrypt
- Κάνουμε επικόλληση το κρυπτογραφημένο μήνυμα
- Πατάμε Enter και μετά Ctrl + D
- Εμφανίζεται το αποκρυπτογραφημένο μήνυμα

Πώς υπογράφουμε ένα μήνυμα;

- gpg --clearsign
- Γράφουμε το μήνυμα
  - «Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015»
- Πατάμε Enter και μετά Ctrl + D
- Εμφανίζεται το υπογεγραμμένο μήνυμα

```
[stavros@aristotle ~]$ gpg --clearsign
Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2

iQIcBAEBCAAGBQJVmxS7AAoJEIhbmDbz4nwNnP4P/0fSa/zGbsFkuzjm679ONc3z
1rIpzZ2b7QlQm89e1ntnSYMsTGKzHg3IyVBQmPxZwnhEtUgUgl6frmEhORiHPI3u
SMVwtK8TsMF3ueGd9UzlPqlG+0NNfqAu7RH8fnOjVp7pMhsYd617WgzWRpNXhkNf
yab73m5N+Mkl6AljvdDG5B+jRf6iKIMIvawEjJ8tXaN1iQLnHAWrzwTm9F7bNXue
HE1e8IfcUQQy8Fg9y6Rf5oqt6mYSmvxh9enQc7vCvEMTfqzofEjxch3G9R25ZTNk
vQ9zxcXqjNPdJT0PkO1pcSzVox+sqfrbGHHdl3xFXnXzfHO2OoH+l6/AqfBiJFpn
fefmyq0Sp9u+jpjsLe1h0khtHW4IOWTUB2ryHAdWlBZJh26xqmDQ5f/VqxdyvwyT
kMzZHoeU+y+Dqt7uwV8K+lcxL2YxhXYPaar1Pqg0ZApKYU4yhDOAGFc6cXJS3CHk
GOT7oN1gggLY7bEvm7z5+PQ5HPBDH+unvjI/IohtkObLwGVcODh1yilCDCjmE321
F04bOVziGpqrsBE2Sesmpf++BQ1bVorEgbJzJhi/xUN/5Y0r/0WKAMcxT/8+4YA1
gw4tTbSFdXKOvPBHfFOY+orRiy8DI+c/jd3s96vvFCiFJxvXjetTLpfFuzsWN5bl
xWOYkbV0ZgP2tm6fn13w
=EKDb
-----END PGP SIGNATURE-----
```

Πώς επιβεβαιώνουμε ότι η υπογραφή είναι έγκυρη;

- Κατεβάζουμε / εισάγουμε πρώτα το δημόσιο κλειδί του αποστολέα, αν δεν το έχουμε

- gpg --verify
- Κάνουμε επικόλληση το υπογεγραμμένο μήνυμα
- Πατάμε Enter και μετά Ctrl + D
- Αν εμφανιστεί το μήνυμα “**Good signature** from…”, τότε η υπογραφή είναι έγκυρη

Πρόβλημα

- *“Στο GPG είσαι ό,τι δηλώσεις”*

  – Ο Τσαρούχης του GPG

- Ο Mario ισχυρίζεται ότι είναι ο Bob
- Δημιουργεί ένα ψεύτικο GPG κλειδί με τα προσωπικά στοιχεία του Bob
- Ανεβάζει το δημόσιο κλειδί του στον key server του MIT
- Η Alice κατεβάζει αυτό το κλειδί
- Νομίζει ότι επικοινωνεί με τον Bob, ενώ στην πραγματικότητα επικοινωνεί με τον Mario

ΑΝ ΣΤΟ GPG Ο ΚΑΘΕΝΑΣ ΕΙΝΑΙ Ο,ΤΙ ΔΗΛΩΣΕΙ

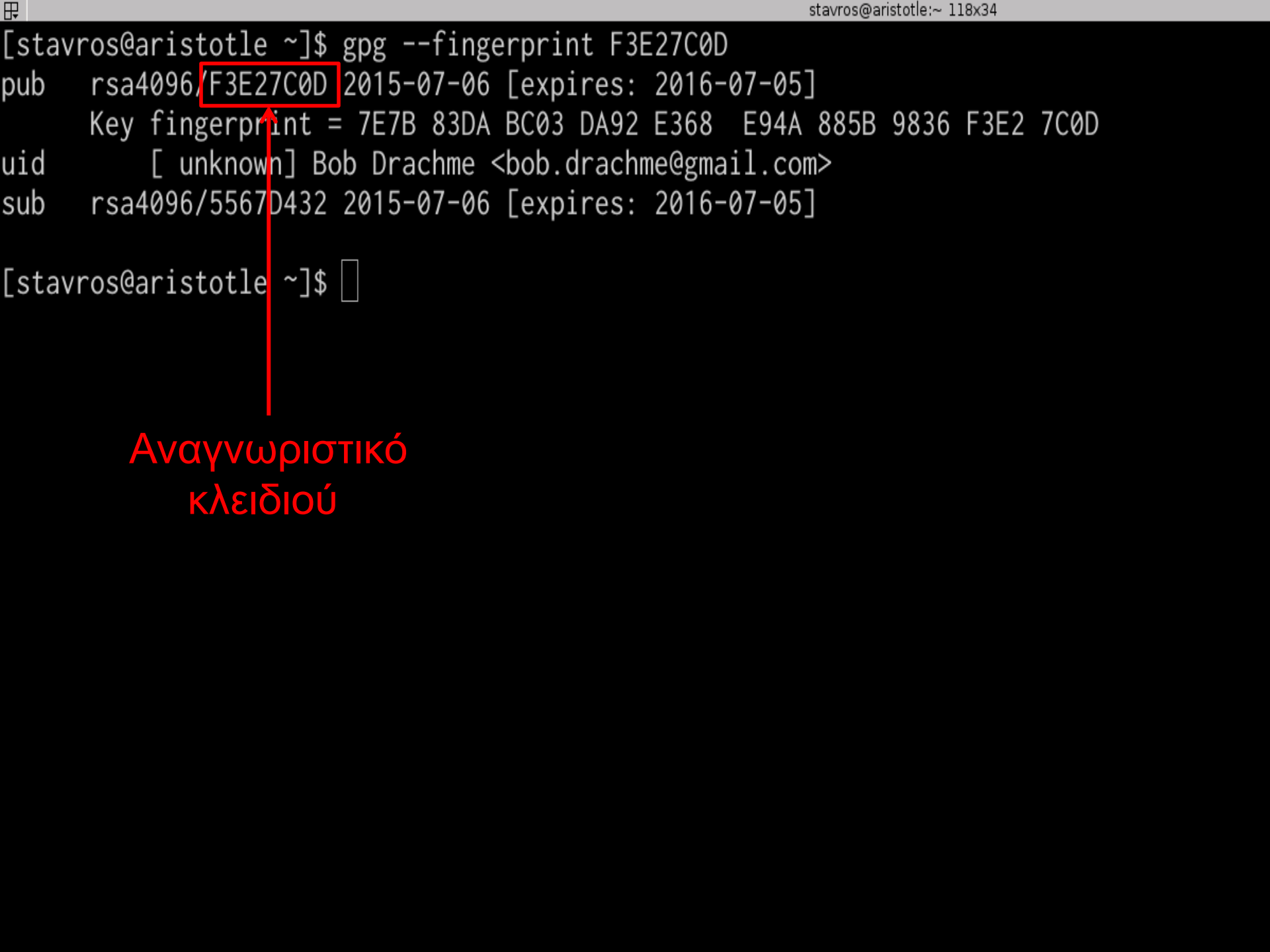
ΠΩΣ ΜΠΟΡΩ ΝΑ ΕΜΠΙΣΤΕΥΤΩ ΚΑΠΟΙΟΝ;

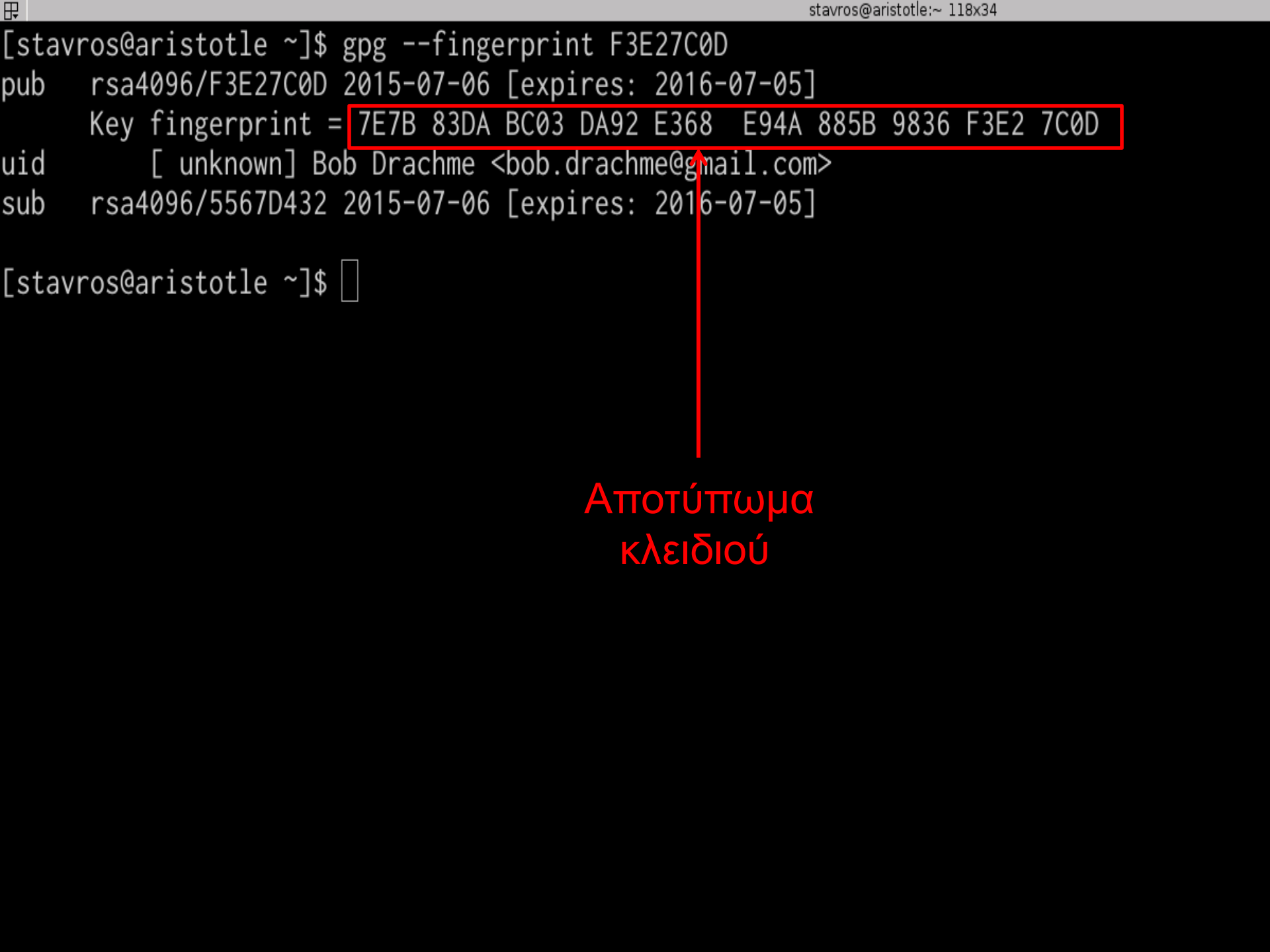
Μια λύση

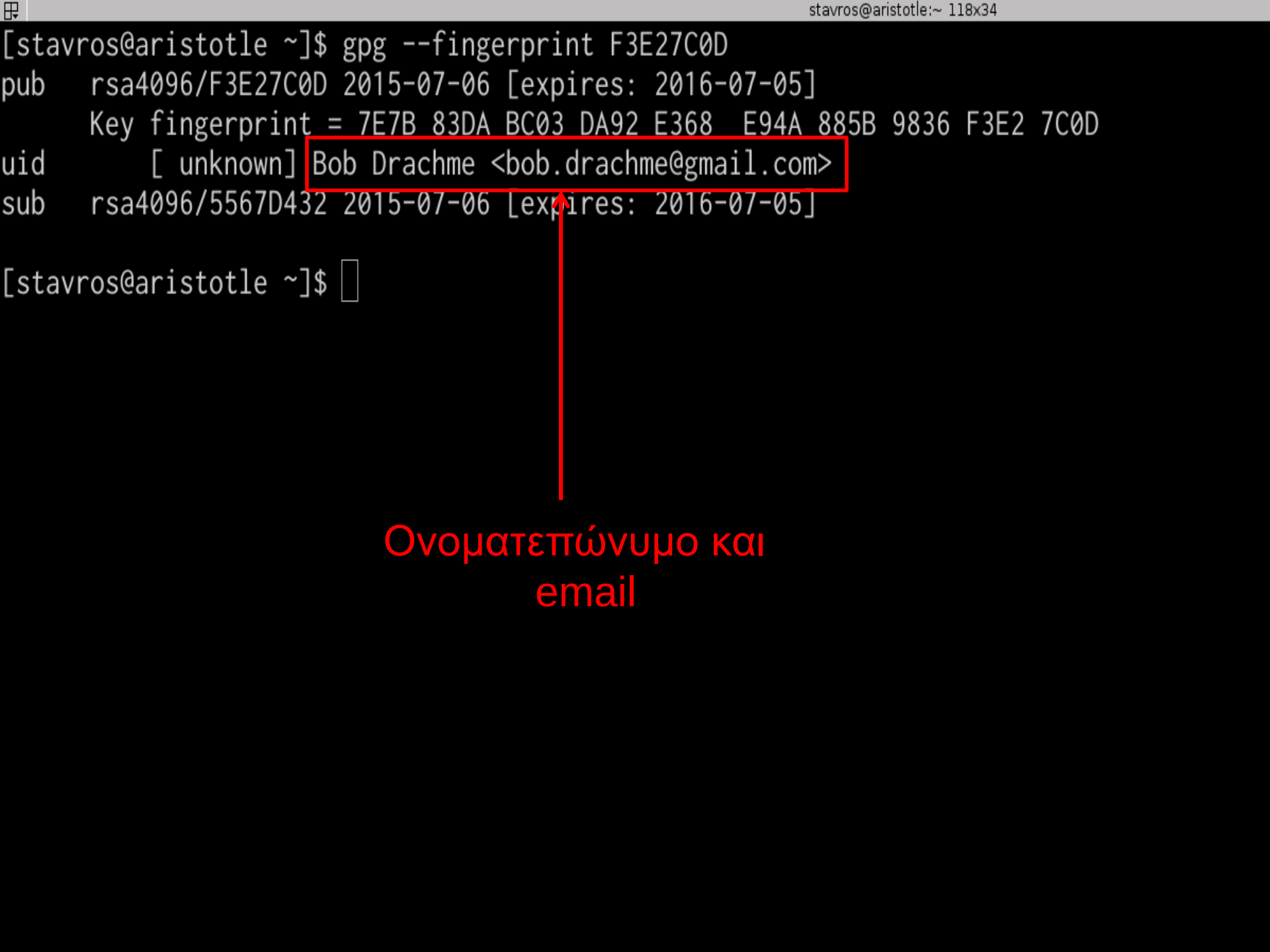
- Επιβεβαιώνουμε ότι το κλειδί ανήκει όντως στο άτομο στο οποίο αναφέρεται
- Με προσωπική συνάντηση
- Ελέγχουμε αν το ονοματεπώνυμό του στο κλειδί είναι πραγματικό
- Ελέγχουμε αν του ανήκει το email του κλειδιού
- Ελέγχουμε αν το αναγνωριστικό και το αποτύπωμα του κλειδιού είναι όντως αυτά που ισχυρίζεται
- Αν όλα είναι εντάξει, **υπογράφουμε το κλειδί**
- **Δημοσιεύουμε την υπογραφή**
- Η υπογραφή πιστοποιεί ότι το κλειδί ανήκει στον φερόμενο ως ιδιοκτήτη του (εμπιστοσύνη)

Πώς ελέγχουμε ένα κλειδί;

- gpg --fingerprint F3E27C0D


stavros@aristotle:~ 118x34
[stavros@aristotle ~]$ gpg --fingerprint F3E27C0D
pub   rsa4096/F3E27C0D 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 7E7B 83DA BC03 DA92 E368 E94A 885B 9836 F3E2 7C0D
uid   [unknown] Bob Drachme <bob.drachme@gmail.com>
sub   rsa4096/5567D432 2015-07-06 [expires: 2016-07-05]
[stavros@aristotle ~]$
Αναγνωριστικό κλειδιού


stavros@aristotle:~ 118x34
[stavros@aristotle ~]$ gpg --fingerprint F3E27C0D
pub   rsa4096/F3E27C0D 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 7E7B 83DA BC03 DA92 E368 E94A 885B 9836 F3E2 7C0D
uid   [unknown] Bob Drachme <bob.drachme@gmail.com>
sub   rsa4096/5567D432 2015-07-06 [expires: 2016-07-05]
[stavros@aristotle ~]$
Αποτύπωμα
κλειδιού

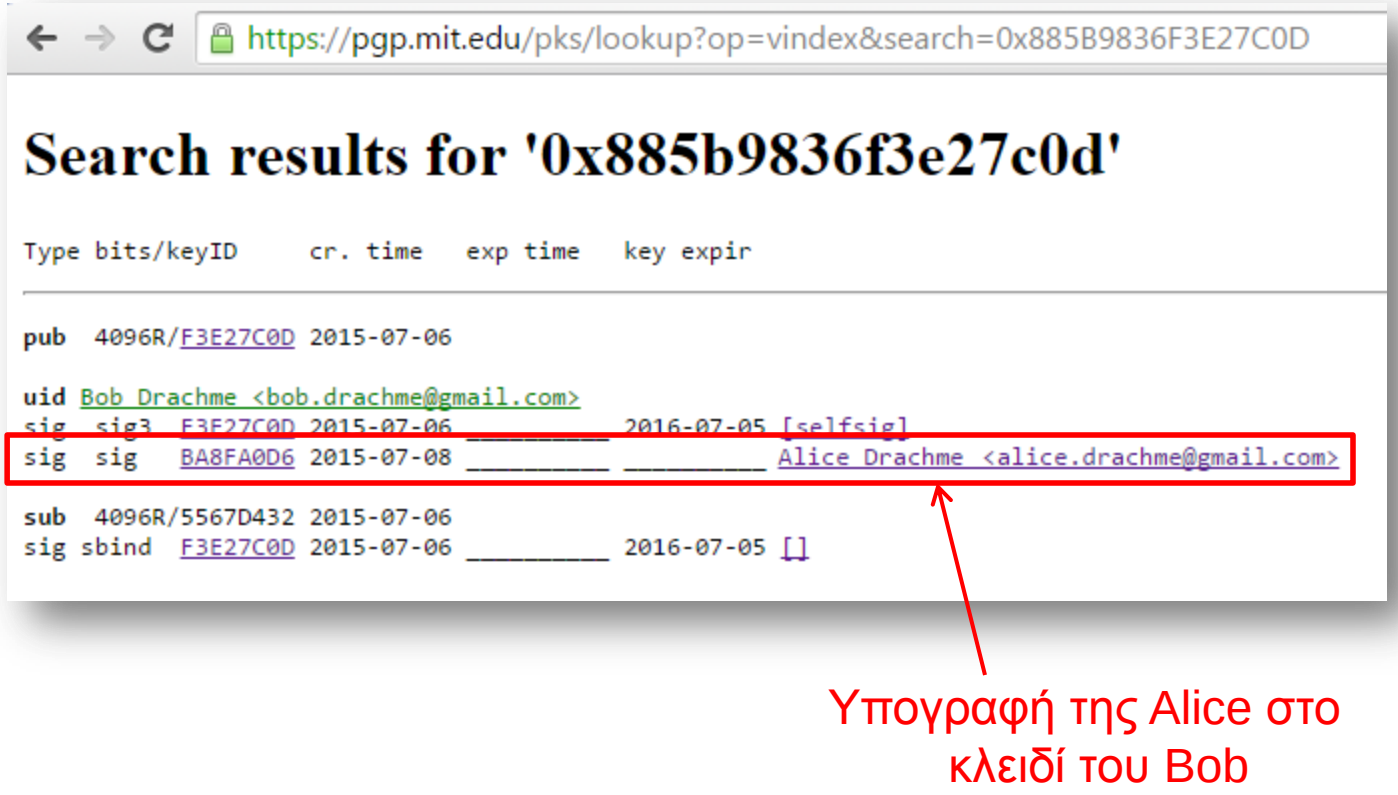

stavros@aristotle:~ 118x34
[stavros@aristotle ~]$ gpg --fingerprint F3E27C0D
pub   rsa4096/F3E27C0D 2015-07-06 [expires: 2016-07-05]
      Key fingerprint = 7E7B 83DA BC03 DA92 E368 E94A 885B 9836 F3E2 7C0D
uid   [unknown] Bob Drachme <bob.drachme@gmail.com>
sub   rsa4096/5567D432 2015-07-06 [expires: 2016-07-05]
[stavros@aristotle ~]$
Ονοματεπώνυμο και email

Πώς υπογράφουμε ένα κλειδί;

- gpg --sign-key F3E27C0D
- Θα μας ζητηθεί το passphrase

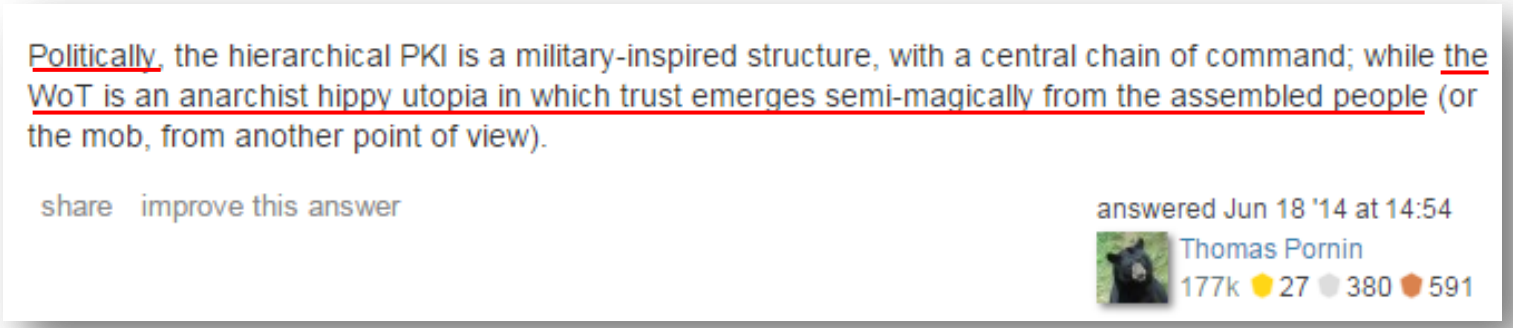
Πώς δημοσιεύουμε την υπογραφή;

- gpg --keyserver pgp.mit.edu --send-keys F3E27C0D



Άλλη λύση

- **Κύκλος Εμπιστευτικότητας (Web of Trust)**
- Ένας **κατανεμημένος ιστός ξεχωριστών οντοτήτων**
- Στηρίζεται στην **εμπιστοσύνη ανάμεσα στους χρήστες**
- Η αποκέντρωση στο μεγαλείο της



Politically, the hierarchical PKI is a military-inspired structure, with a central chain of command; while the WoT is an anarchist hippy utopia in which trust emerges semi-magically from the assembled people (or the mob, from another point of view).

share improve this answer

answered Jun 18 '14 at 14:54

Thomas Pornin

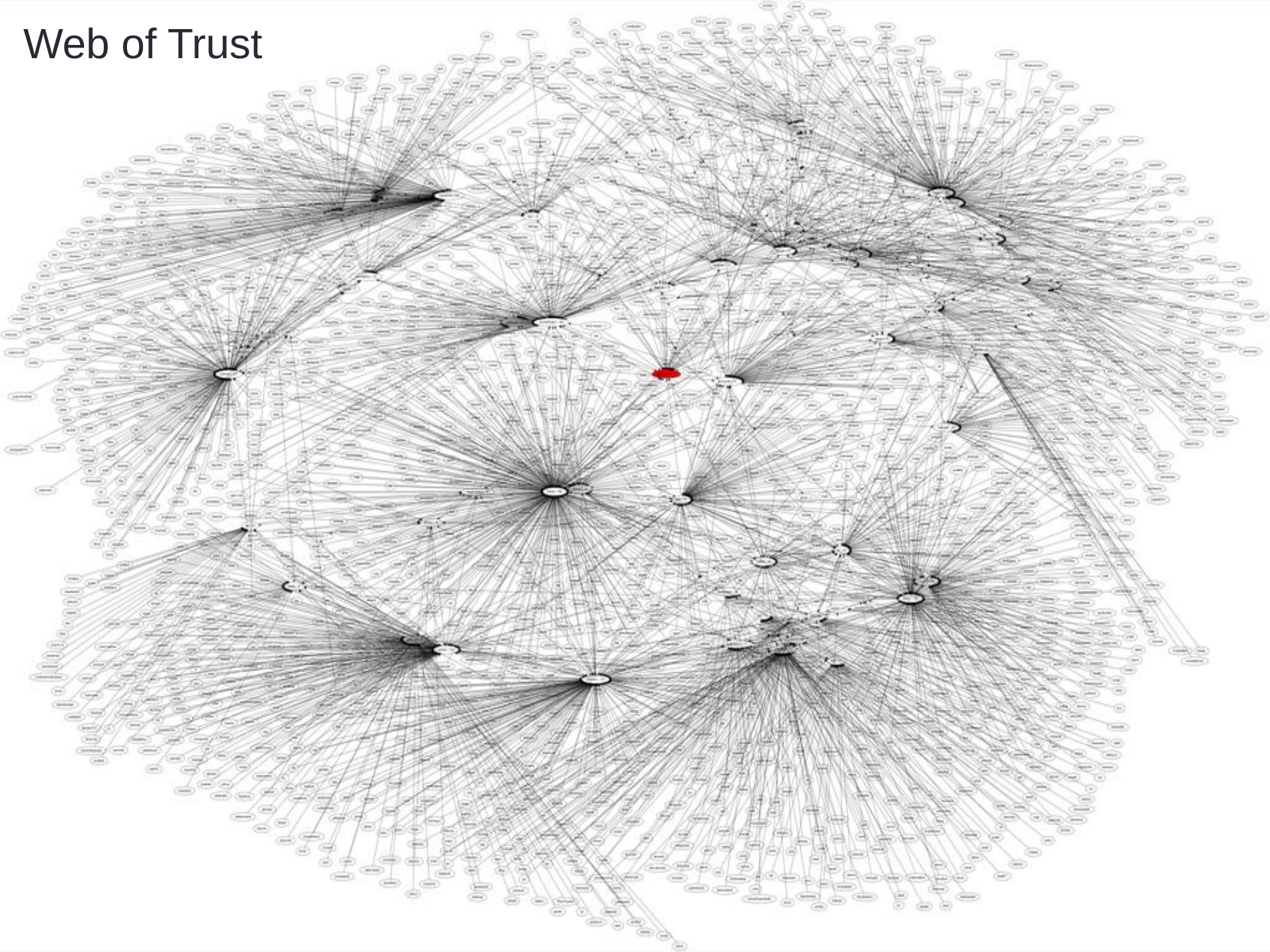
177k 27 380 591

http://security.stackexchange.com/questions/61360/what-is-the-web-of-trust

Κύκλος εμπιστευτικότητας

- Η Alice εμπιστεύεται τον Σταύρο
  - Γνωρίζει ότι το κλειδί του Σταύρου είναι αυθεντικό
  - Έχει υπογράψει το δημόσιο κλειδί του Σταύρου
- Ο Σταύρος εμπιστεύεται τον Bob
  - Γνωρίζει ότι το κλειδί του Bob είναι αυθεντικό
  - Έχει υπογράψει το δημόσιο κλειδί του Bob
- Η Alice εμπιστεύεται τον Σταύρο και ο Σταύρος εμπιστεύεται τον Bob
- Τελικά η Alice εμπιστεύεται τον Bob
- Όσες περισσότερες υπογραφές έχει ένα κλειδί, τόσο μεγαλύτερη είναι η πιθανότητα να είναι αυθεντικό (με την προϋπόθεση ότι οι υπογραφές είναι αυθεντικές)

Web of Trust

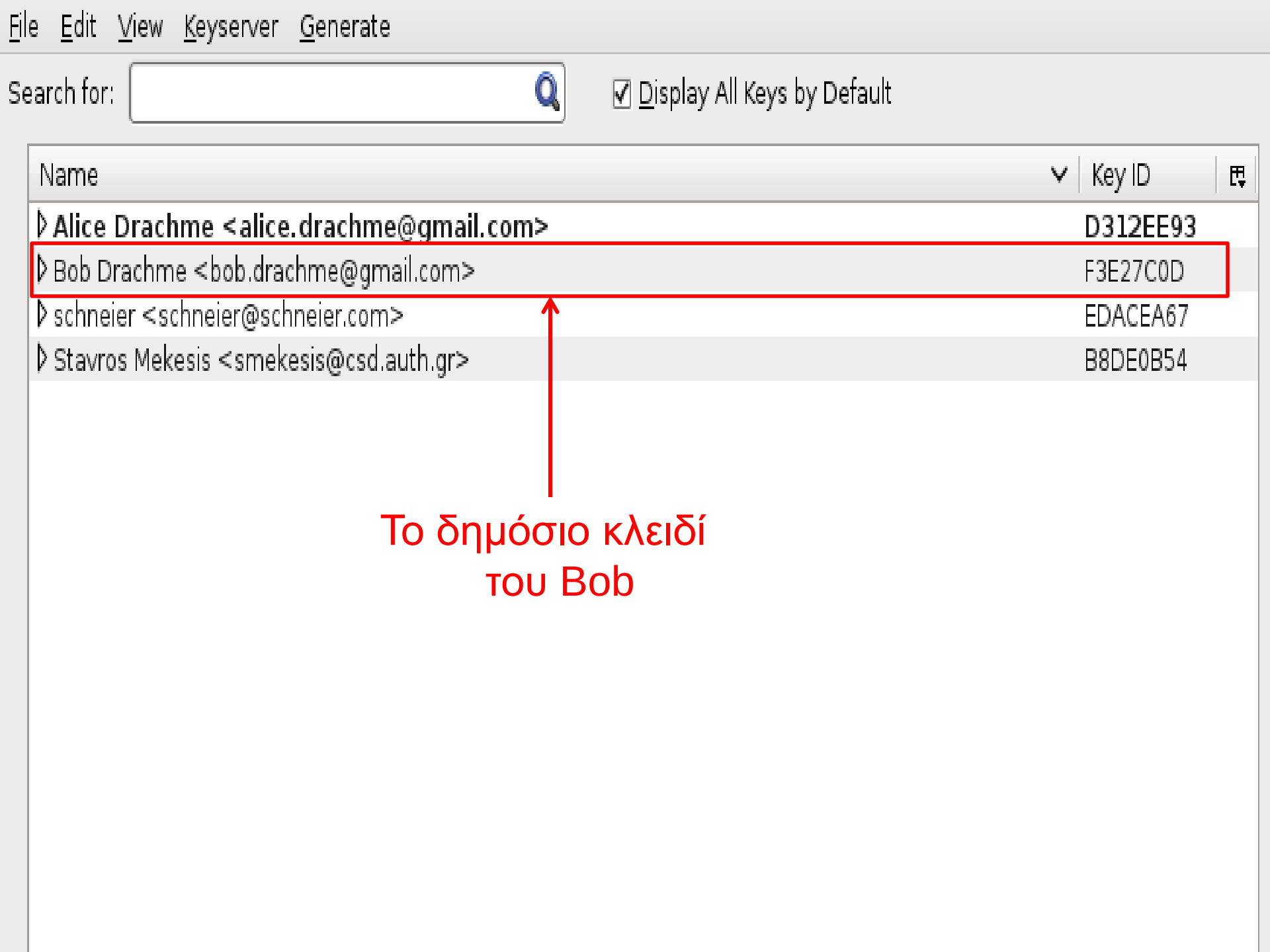


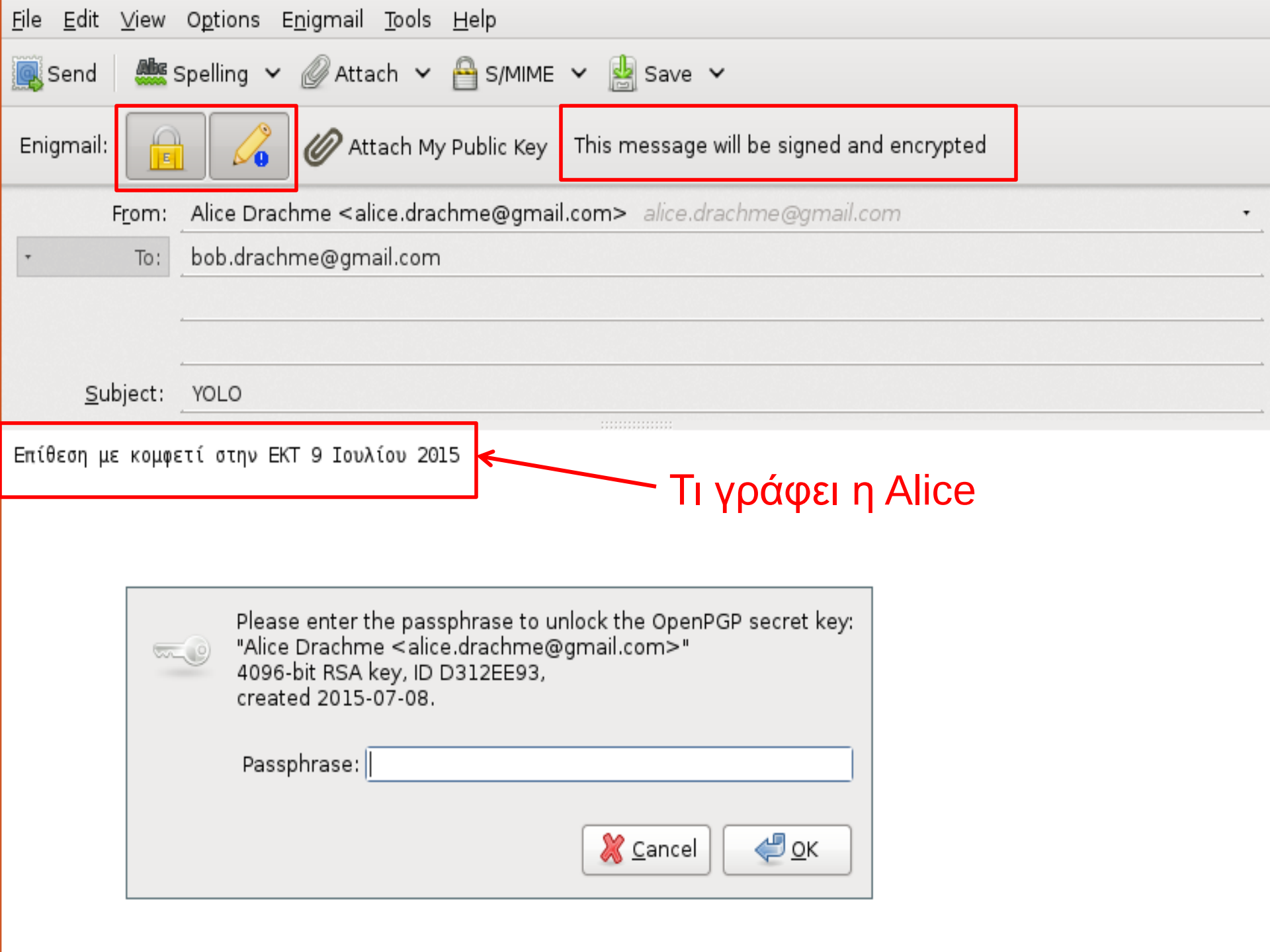
Key signing party

Thunderbird και Enigmail

- Καλό το τερματικό, αλλά και το GUI έχει την δική του χάρη ☺
- Κάνουμε εγκατάσταση το **Thunderbird**
  - https://www.mozilla.org/en-US/thunderbird/download
- Κάνουμε εγκατάσταση το add-on **Enigmail**
  - https://www.enigmail.net/home/index.php
- Ρυθμίζουμε το Enigmail
  - https://www.enigmail.net/documentation/quickstart.php

- Ας δούμε μερικές εικόνες από το πρόγραμμα...


File Edit View Keyserver Generate
Search for:
Display All Keys by Default
Name
Key ID
Alice Drachme <alice.drachme@gmail.com>
D312EE93
Bob Drachme <bob.drachme@gmail.com>
F3E27C0D
schneier <schneier@schneier.com>
EDACEA67
Stavros Mekesis <smekesis@csd.auth.gr>
B8DE0B54
Το δημόσιο κλειδί
του Bob


File Edit View Options Enigmail Tools Help
Send
Spelling
Attach
S/MIME
Save
Enigmail:
Attach My Public Key
This message will be signed and encrypted
From: Alice Drachme <alice.drachme@gmail.com> alice.drachme@gmail.com
To: bob.drachme@gmail.com
Subject: YOLO
Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015
Τι γράφει η Alice
Please enter the passphrase to unlock the OpenPGP secret key:
"Alice Drachme <alice.drachme@gmail.com>"
4096-bit RSA key, ID D312EE93,
created 2015-07-08.
Passphrase:
Cancel
OK

Gmail

More

COMPOSE

Inbox (3)

Starred

Sent Mail

Drafts

More

Bob

YOLO

Inbox x

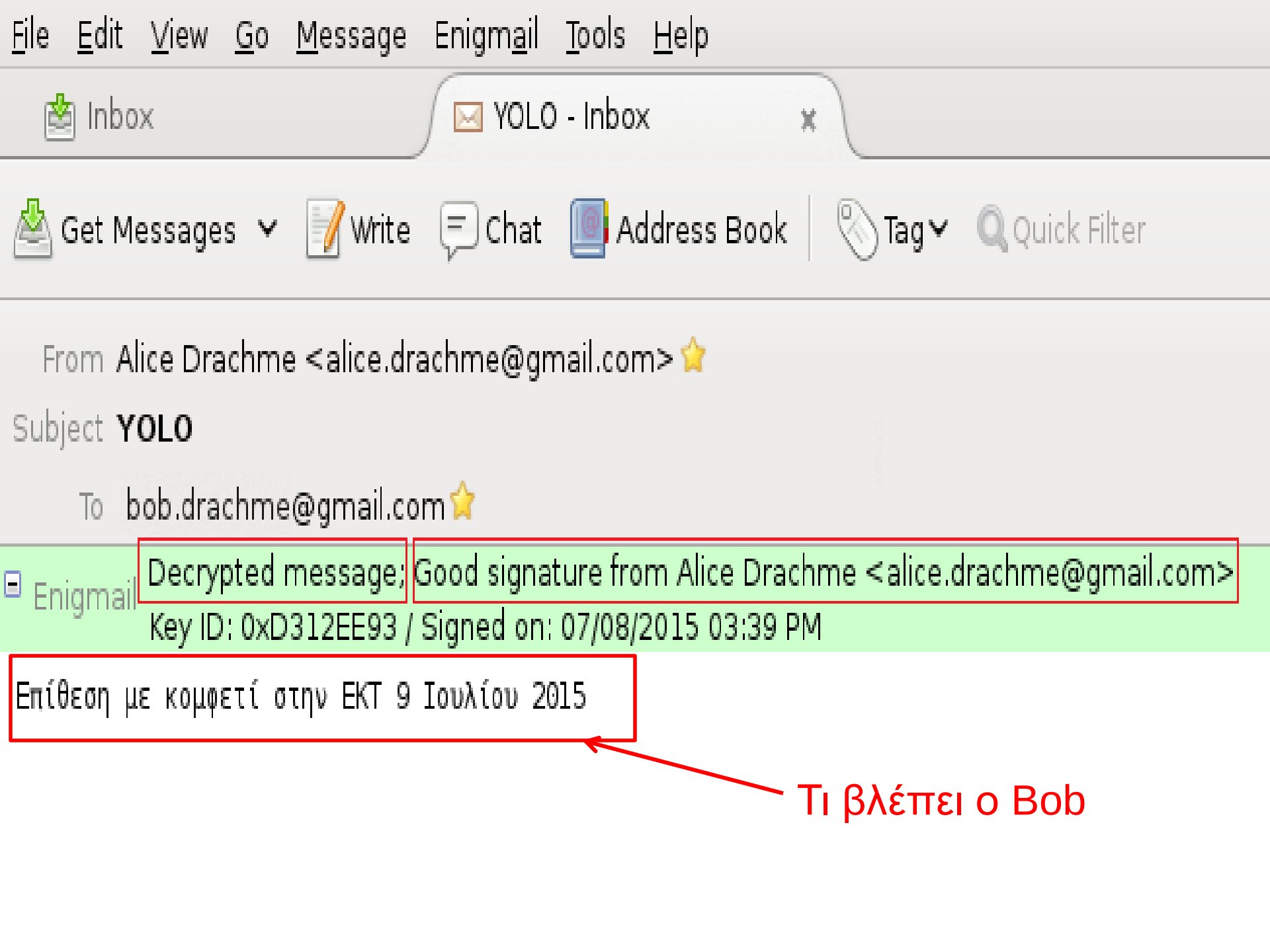
Alice Drachme <alice.drachme@gmail.com>

to me


```
-----BEGIN PGP MESSAGE-----
Charset: utf-8
Version: GnuPG v2

hQIMA+xawZxVZ9QyAQ//dD62YRHHPPDk+VrRzYEmC4k3FH2Gt68sY5XVL4wzaVq9
nXpMmAsio0FLONp6WbnJlaw6G4oqlGxid6Ri7G15dLJ2qK6KHjOM4w6hprkFXyEX
fXLVb1WTvajtslbao3hVU/6pLQfvXhP3bdFD3pgMRrPixBugom+sh+lPkdb27DBf
zJ6qsQERwy11a2/aCq0JHkaq6kRXTCuEYhLCZdiV87W6heUR0yByPoEmDJXsv7VM
7hCcDjDyRFPSXbsXqyl+68nNr50vNKiaSoPYgRXONhupaAxH9nP+98fM/NG69XSS
H/0tdY0RlbPVwYDOAPk5GsDCgjEHsEnBCTQSMiLUO3+rrRm7hZkH2j5NGimyuO55
+l/XPWtJKaR/tYzC5JspCrWSLY8ICIdMXFt1/68RaIR3A8LwNYvhyZ3hlWsVJv/Z
uTHVj75zors1l3NcbTY9Nmwe80KfcSLqw5MQffwQJzvgntzCpaGr6aAJj2DbwhR6
6i728vUJYf2OQQBKOomR6Wsx93gF5YJ8cVoStXoPb7P/MmYu5uDMN70NPeGgp4q5
kdmprSGhVoAgBgKRQPUXuxnlOHu3gOjlieEwvl+2x52mBm50hF5xvMfMhuzN1z2w
lifmrfyz4XBqRohxMwB5Fc2EZBG4j2WLyQQ7k5W3+5l7hDiyHtsP6lLzrkc5vH6F
AgwDW/jtlUlKfb0BD/0YxdHaXW7jpNcpOFvAhPhFCtwaVYITlU9pZOKXGbUqWg4Q
iYDkB3fjqbA4la3alhiicSjx9AqkrHQb0dnmKBsQQvkrQxSTpgt1QocYa1P7bKlP
jd1a9kBSKpNZswucqukGqu387xusb0r50GtHSU+gLCDnBWJbqNxDf1iszdfmYnef
kpxCWvqh/5efB2U+usl18/gOHAerCoz9ZpHCpNh7Ado/J1lKCd0AgQREDh/rR/Rl
GcLu37QCZm0JqrokrTX7LXVf7llNPQnf93nqw7UMRFQaC9Qr4ARa8Ras6DMzbvfo
bZX6TTgczvJ6fR+VCEXhQhlVOyucXkYJ8J2SPzlV3Nx9WGHkpASHcqA2qKiD5kmG
o555JzG83UdCsbE1//tQCrqv5v4dQeVQjyGiho5vf6aqLhqdDaqahOlcRsAN3HzD
Pk8rbjoOMTpXyPthfusm56E9H+pMqujV823mioRXYcvN3uhPbxBJ0vOFDyGr5rZT
mE7BUDNEi/ExlHWjsUYeu5fifLvF/2pW8jCa7SHEg3BzGsbNbhOk4b47bMqPcO9h
1NiovFkP/pOt2j/CW4rHU/TvVpeqNKkdzVkBpTN+YaBDihR3dL3Cs1XP7rkWeGO3
7feEMGoHx1YUp9bqp4Xy0c5BwwuZPQ6/ZGeFvVGzyzxj93ca/9ADSoA9d5UM99KF
AUBMxLRX6nlnUJwE2NUVNAhslSOyxhCZ8x9KYOUhjNSAm5kxh4Vs3gilWFhSe9RK
TOEmWRqEHM2C/Riy88Uv5s+xF7iNoka7jzFom27hFQktRcJfdleoWTs4uLgDmRsy
b1lYUruyca+olN/WduMiO/73Op1dWjzUOPc8LSt+k2fDaRwHrA==
=XP9g
-----END PGP MESSAGE-----
```


Τι βλέπει κάποιος τρίτος

YOU MAD?


File Edit View Go Message Enigmail Tools Help
Inbox
YOLO - Inbox
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
From Alice Drachme <alice.drachme@gmail.com>
Subject YOLO
To bob.drachme@gmail.com
Enigmail
Decrypted message; Good signature from Alice Drachme <alice.drachme@gmail.com>
Key ID: 0xD312EE93 / Signed on: 07/08/2015 03:39 PM
Επίθεση με κομφετί στην ΕΚΤ 9 Ιουλίου 2015
Τι βλέπει ο Bob

Επιπλέον μελέτη

- PGP & GPG: Email for the Practical Paranoid. Michael Lucas. No Starch Press.
- https://www.gnupg.org/gph/en/manual.html

Σας ευχαριστώ! ☺