



OpenPGP

Το πρότυπο κρυπτογράφησης και οι εφαρμογές του.

RFC 4880

IETF

www.openpgp.org

Εισαγωγή στο πρότυπο OpenPGP



Η παρουσίαση αφορά την περιγραφή των βασικότερων χαρακτηριστικών του προτύπου και της υλοποίησής του, GnuPG.



Phil Zimmermann

Δημιουργός του OpenPGP

Σπούδασε Επιστήμη
Υπολογιστών στο
Πανεπιστήμιο
Florida Atlantic

Τι είναι το PGP (Pretty Good Privacy)

- Είναι λογισμικό κρυπτογράφησης που παρέχει ιδιωτικότητα και ταυτοποίηση
- Χρησιμοποιείται για την υπογραφή, κρυπτογράφηση, και αποκρυπτογράφηση κειμένων, emails, αρχείων, καταλόγων, αλλά και ολόκληρων κατατμήσεων δίσκων αποθήκευσης
- Αναπτύχθηκε από τον Phil Zimmermann (1991)
- Το 2010 εξαγοράστηκε από την εταιρία Symantec για 300 εκ. δολάρια
- Το PGP έκανε εκτεταμένη χρήση των προστατευμένων με πατέντα, τεχνικών κρυπτογράφησης, RSA και IDEA
- Όποιος ήθελε να το χρησιμοποιήσει έπρεπε να πληρώσει την αντίστοιχη άδεια χρήσης λογισμικού
- Ο δημιουργός του το 1998 προσέφερε μια δωρεάν λύση με την ονομασία OpenPGP

Πως χρησιμοποιήθηκε το OpenPGP

- Το OpenPGP καθόριζε δωρεάν και ελεύθερα πρότυπα με τα οποία τα διάφορα προγράμματα μπορούσαν να επικοινωνούν
- Έτσι οι εταιρείες άρχισαν να δημιουργούν εφαρμογές OpenPGP από το μηδέν, προσαρμόζοντάς τις στις ανάγκες τους

Ονοματολογία: PGP, GnuPG και OpenPGP

- PGP – Χρησιμοποιείται πλέον μόνο για τα προϊόντα της Symantec
- GnuPG ή GPG – Αφορά μόνο στην αντίστοιχη εφαρμογή που έχει υλοποιηθεί
- OpenPGP – Συνήθως χρησιμοποιείται από εφαρμογές όπως το GnuPG για να υποδηλωθεί η συμβατότητά τους με το πρότυπο αυτό (OpenPGP Compliant)

Η τεχνική υποστήριξη του OpenPGP

Η τεχνική υποστήριξη αποτελείται από ένα σύνολο εταιρειών και οργανισμών.



FLEXCRYPT



Συμμαχία OpenPGP

Η συμμαχία OpenPGP αποτελείται από ένα σύνολο εταιρειών και οργανισμών που υλοποιούν το πρότυπο αυτό στις εφαρμογές τους. Συνεργάζονται προκειμένου να επιτυγχάνουν την συμβατότητα, την τεχνική διαλειτουργικότητα και την εμπορική συνεργεία μεταξύ των εφαρμογών OpenPGP.

<http://www.openpgp.org/members>

1ο μέρος



Γενικές λειτουργίες του OpenPGP

Παρέχει υπηρεσίες ακεραιότητας δεδομένων, για μηνύματα και αρχεία δεδομένων.

Κάνει χρήση των παρακάτω τεχνολογιών

- Ψηφιακές υπογραφές
- Κρυπτογράφηση
- Συμπίεση
- Μετατροπή Radix-64

Επιπλέον, παρέχει διαχείριση κλειδιών και υπηρεσίες πιστοποίησης (πιστοποιητικά).

Σχετικοί σύνδεσμοι

http://en.wikipedia.org/wiki/Digital_signature

<http://en.wikipedia.org/wiki/Cryptography>

<https://tools.ietf.org/html/rfc4880#section-2.4>



Εμπιστευτικότητα μέσω Κρυπτογράφησης

Το OpenPGP συνδυάζει **συμμετρική** και **ασύμμετρη** κρυπτογράφηση προκειμένου να παρέχει εμπιστευτικότητα στην επικοινωνία.

Σύνοψη ενεργειών κρυπτογράφησης

- Αρχικά, το αντικείμενο της επικοινωνίας (ή σύνοδος) κρυπτογραφείται με ένα συμμετρικό αλγόριθμο.
- Κάθε συμμετρικό κλειδί χρησιμοποιείται μόνο μία φορά και για μια συγκεκριμένη σύνοδο επικοινωνίας.
- Ένα νέο κλειδί συνόδου (session key) δημιουργείται τυχαία για κάθε σύνοδο.
- Εφόσον το κλειδί συνόδου χρησιμοποιείται μόνο μία φορά, ενσωματώνεται με το κυρίως μήνυμα και μεταδίδεται μαζί με αυτό.

Για να προστατευτεί το κλειδί, κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη ως εξής:

- 1) Ο αποστολέας δημιουργεί ένα μήνυμα.
- 2) Το OpenPGP του αποστολέα δημιουργεί ένα τυχαίο αριθμό. Θα χρησιμοποιηθεί ως κλειδί συνόδου γι' αυτό το μήνυμα μόνο.
- 3) Το κλειδί συνόδου κρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί του κάθε παραλήπτη. Αυτά τα κρυπτογραφημένα κλειδιά συνόδου θα αποτελούν και τα bit έναρξης των τελικών πακέτων που θα μεταδοθούν.
- 4) Το OpenPGP του αποστολέα κρυπτογραφεί το μήνυμα χρησιμοποιώντας το κλειδί συνόδου.
- 5) Το OpenPGP του παραλήπτη αποκρυπτογραφεί το κλειδί συνόδου (bit έναρξης) χρησιμοποιώντας το του ιδιωτικό κλειδί.
- 6) Το OpenPGP του παραλήπτη αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το κλειδί συνόδου. Αν το μήνυμα είναι συμπιεσμένο, αποσυμπιέζεται πρώτα.

http://en.wikipedia.org/wiki/Symmetric-key_algorithm

http://en.wikipedia.org/wiki/Public-key_cryptography



Ταυτοποίηση μέσω ψηφιακής υπογραφής

Χρησιμοποιείται κωδικός κατακερματισμού (μέσω hash function) ή αλγόριθμος message-digest, και ένας αλγόριθμος υπογραφής δημοσίου κλειδιού.

Ακολουθία βημάτων ταυτοποίησης

- 1) Ο αποστολέας δημιουργεί ένα μήνυμα.
- 2) Το λογισμικό αποστολής δημιουργεί έναν hash κωδικό από το μήνυμα.
- 3) Το λογισμικό αποστολής δημιουργεί μια υπογραφή από τον hash κωδικό χρησιμοποιώντας το ιδιωτικό κλειδί του αποστολέα.
- 4) Η δυαδική υπογραφή προσαρτάται στο μήνυμα.
- 5) Το λογισμικό του παραλήπτη κρατά ένα αντίγραφο της υπογραφής του μηνύματος.
- 6) Το λογισμικό λήψης δημιουργεί ένα νέο hash κωδικό για το ληφθέν μήνυμα και το επαληθεύει χρησιμοποιώντας την υπογραφή του μηνύματος αυτού.
- 7) Αν η ταυτοποίηση είναι επιτυχής, το μήνυμα γίνεται αποδεκτό ως αυθεντικό (γνήσιο).

Οι υλοποιήσεις του προτύπου OpenPGP θα πρέπει να συμπιέζουν το μήνυμα μετά την προσάρτηση της ψηφιακής υπογραφής και πριν την κρυπτογράφηση. Οι **αλγόριθμοι συμπίεσης** που προτείνονται είναι:

- ✓ ZIP (RFC1951)
- ✓ ZLIB (RFC1950)
- ✓ BZip2

http://en.wikipedia.org/wiki/Hash_function

http://en.wikipedia.org/wiki/Cryptographic_hash_function#Cryptographic_hash_algorithms



Συμμετρικοί & ασύμμετροι αλγόριθμοι κρυπτογράφησης

Το OpenPGP συνδυάζει συμμετρικούς και ασύμμετρους αλγόριθμους κρυπτογράφησης.

Αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού (ασύμμετροι) που χρησιμοποιούνται συχνότερα σε υλοποιήσεις του OpenPGP:

Επίσης υπάρχει η δυνατότητα χρήσης των παρακάτω:

- ✓ ECC (Elliptic curve cryptography)
- ✓ ECDSA (Elliptic Curve Digital Signature Algorithm)
- ✓ Diffie-Hellman

	RSA	Elgamal	DSA
Κρυπτογράφηση	✓	✓	
Ψηφιακή Υπογραφή	✓		✓

Συμμετρικοί αλγόριθμοι που χρησιμοποιούνται συχνότερα σε υλοποιήσεις του OpenPGP:

- ✓ IDEA (International Data Encryption Algorithm)
- ✓ TripleDES ή 3DES (EDE mode)
- ✓ CAST-128 (RFC2144)
- ✓ Blowfish (128 bit key, 16 rounds)
- ✓ AES (Advanced Encryption Standard – 128, 192, 256-bit key)
- ✓ Twofish (256-bit key)

[https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

https://en.wikipedia.org/wiki/ElGamal_encryption

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

https://en.wikipedia.org/wiki/Digital_Signature_Algorithm

https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

Συναρτήσεις κατακερματισμού

Χρησιμοποιούνται στις ψηφιακές υπογραφές.



Οι κυριότερες που έχουν χρησιμοποιηθεί κατά καιρούς στο OpenPGP είναι:

- ✓ MD5 (**δεν προτείνεται**)
- ✓ SHA-1 (FIPS 180) (**προτείνεται**)
- ✓ RIPE-MD/160
- ✓ SHA256 (384, 512, 224)

Αν και μπορούν να χρησιμοποιηθούν όλες, στις νέες υλοποιήσεις οι εφαρμογές θα πρέπει να χρησιμοποιούν την SHA-1.0. Η MD5 δεν κρίνεται πλέον ασφαλής και δεν πρέπει να χρησιμοποιείται.

<http://csrc.nist.gov/publications/PubsFIPS.html>

<http://en.wikipedia.org/wiki/RIPEMD>

<http://en.wikipedia.org/wiki/SHA-2>

Οδηγός – σύνοψη ενεργειών στο OpenPGP



Το πρότυπο OpenPGP περιγράφει την υλοποίηση έξι λειτουργιών – ενεργειών.

Επιθυμητό αποτέλεσμα

Ενέργεια

Θέλω ο καθένας που διαβάζει αυτό το μήνυμα να γνωρίζει χωρίς καμία αμφιβολία ότι του το έστειλα εγώ. Να μην μπορώ να το απαρνηθώ.

Θέλω να εξακριβώσω την ταυτότητα του ατόμου που έστειλε ένα ψηφιακά υπογεγραμμένο μήνυμα προκειμένου να δω αν ο υποφαινόμενος αποστολέας είναι ο πραγματικός αποστολέας.

Θέλω να στείλω ένα μήνυμα το οποίο θα μπορεί να διαβάσει μόνο ο παραλήπτης που επιθυμώ.

Θέλω να αποκρυπτογραφήσω ένα μήνυμα που έλαβα.

Θέλω το μήνυμά μου να μπορεί να διαβαστεί μόνο από τον παραλήπτη που επιθυμώ, και εκείνος να είναι σε θέση να επιβεβαιώσει ότι το μήνυμα προέρχεται από εμένα.

Θέλω να αποκρυπτογραφήσω ένα μήνυμα το οποίο έχει ψηφιακή υπογραφή και να επιβεβαιώσω την ταυτότητα του αποστολέα του.

Ψηφιακή υπογραφή του μηνύματος με το ιδιωτικό μου κλειδί.

Επιβεβαίωση της ψηφιακής υπογραφής με το δημόσιο κλειδί του αποστολέα.

Κρυπτογράφηση του μηνύματος αυτού με το δημόσιο κλειδί του επιθυμητού παραλήπτη.

Αποκρυπτογράφηση του μηνύματος με το ιδιωτικό μου κλειδί.

Κρυπτογράφηση του μηνύματος με το δημόσιο κλειδί του παραλήπτη και ψηφιακή υπογραφή του μηνύματος με το ιδιωτικό μου κλειδί.

Αποκρυπτογράφηση του μηνύματος με το ιδιωτικό μου κλειδί και επαλήθευση της ψηφιακής υπογραφής με το δημόσιο κλειδί του αποστολέα.

Τύποι δεδομένων

Οι τύποι δεδομένων που περιγράφονται στο πρότυπο OpenPGP



Στο πρότυπο OpenPGP περιγράφονται οι εξής τύποι δεδομένων:

- ✓ Κλιμακούμενοι αριθμοί (Scalar Numbers)
- ✓ Ακέραιοι πολλαπλής ακρίβειας (Multiprecision Integers)
- ✓ Αναγνωριστικά κλειδιών (Key IDs)
- ✓ Κείμενο (Text)
- ✓ Πεδία χρόνου (Time Fields)
- ✓ Μπρελόκ κλειδιών (Keyrings)
- ✓ Προδιαγραφείς μετατροπής συμβολοσειράς σε κλειδί (String-to-Key (S2K) Specifiers)

Τι είναι Keyring

Ένα Keyring είναι μια συλλογή ενός ή περισσότερων κλειδιών κρυπτογράφησης που βρίσκονται αποθηκευμένα, είτε σε αρχείο, είτε σε κάποια βάση δεδομένων. Φυσικά, σε ασφαλή θέση και μορφή.

Δομή πακέτου OpenPGP



Ένα μήνυμα στο OpenPGP αποτελείται από έναν αριθμό εγγραφών που ονομάζονται και πακέτα.

Γενικά

- Κάθε πακέτο αποτελείται από την επικεφαλίδα (header) ακολουθούμενη από το κυρίως σώμα του.
- Η επικεφαλίδα δεν είναι σταθερού μήκους.
- Τα πρώτα 8 bit (first octet) της επικεφαλίδας αποτελούν την ετικέτα του πακέτου, η οποία καθορίζει τον τύπο του και το νόημά του.
- Το σημαντικότερο bit της ετικέτας είναι το αριστερότερο (bit 7).

Ετικέτες και τύποι πακέτων OpenPGP



Οι ετικέτες καθορίζουν τον τύπο του κάθε πακέτου και το νόημά του.

Ετικέτα	Τύπος πακέτου
1	Public-Key Encrypted Session Key
2	Signature
3	Symmetric-Key Encrypted Session Key
4	One-Pass Signature
5	Secret key
6	Public key
7	Secret subkey
8	Compressed data
9	Symmetrically encrypted data
10	Marker
11	Literal data
12	Trust ⁴²
13	User ID
14	Public subkey
17	User attribute
18	Symmetrically encrypted and integrity protected data
19	Modification detection code

Η σημασία του τύπου πακέτου

Ο τύπος του πακέτου αφορά την πληροφορία που φέρει στο εσωτερικό του. Με αυτό τον τρόπο η υλοποίηση του OpenPGP λαμβάνει και την απόφαση για τον τρόπο με τον οποίο θα χειριστεί το συγκεκριμένο πακέτο.

Τα πακέτα υπογραφής (ετικέτα 2), περιλαμβάνουν εκτός των άλλων, και δύο ειδικά πεδία:

- Key Server Preferences
- Preferred Keyserver

Και τα δύο αυτά πεδία, περιλαμβάνουν οδηγίες που αφορούν τον διακομιστή (ή τους διακομιστές) κλειδιών (Keyserver), που θα χρησιμοποιηθούν από το υλοποιημένο OpenPGP.

Διαφορά μεταξύ κλειδιών και υποκλειδιών (subkeys)

- Κλειδί – Παρέχει υπηρεσίες ψηφιακής υπογραφής
- Υποκλειδί – Παρέχει υπηρεσίες κρυπτογράφησης

[http://en.wikipedia.org/wiki/Key_server_\(cryptographic\)](http://en.wikipedia.org/wiki/Key_server_(cryptographic))



Ενισχυμένα κλειδιά στο OpenPGP

Οι δύο τύποι των ενισχυμένων κλειδιών είναι ο τύπος V3 και ο τύπος V4

Ένα ενισχυμένο κλειδί τύπου V3 (δεν προτείνεται σε νέες υλοποιήσεις) στο OpenPGP είναι της μορφής:

```
RSA Public Key
[Revocation Self Signature]
  User ID [Signature ...]
[User ID [Signature ...] ...]
```

Ένα ενισχυμένο κλειδί τύπου V4 (προτείνεται για νέες υλοποιήσεις) στο OpenPGP είναι της μορφής:

```
Primary-Key
[Revocation Self Signature]
[Direct Key Signature...]
  User ID [Signature ...]
[User ID [Signature ...] ...]
[User Attribute [Signature ...] ...]
[[Subkey [Binding-Signature-Revocation]
  Primary-Key-Binding-Signature] ...]
```

Οι τιμές που εμφανίζονται μέσα σε αγκύλες είναι προαιρετικές και τα αποσιωπητικά δηλώνουν επανάληψη.

Αποτύπωμα και αναγνωριστικό κλειδιού

- Το αποτύπωμα (fingerprint) του κάθε κλειδιού V4, προκύπτει με 160-bit SHA-1 hashing του πακέτου.
- Το αναγνωριστικό (Key ID) προκύπτει από τα 60 χαμηλότερης τάξης bits του αποτυπώματος αυτού.

http://en.wikipedia.org/wiki/Public_key_fingerprint

Μετατροπέας Radix-64

Είναι ένα σύστημα κωδικοποίησης.



Το σύστημα κωδικοποίησης Radix-64 του OpenPGP παρέχει αυτή τη δυνατότητα:

Η αναπαράσταση του κάθε αντικειμένου στο OpenPGP, είναι μια ακολουθία οκτάδων (αποτελούμενων από bits). Για το λόγο αυτό, θα πρέπει η μετατροπή τους σε μορφή ASCII να επιτυγχάνεται χωρίς να συμβαίνουν αλλοιώσεις.

Αποτελείται από δύο μέρη:

1. Την κωδικοποίηση δυαδικών δεδομένων base64 (πανομοιότυπη με την κωδικοποίηση μεταφοράς περιεχομένου, MIME base64)
2. Ένα checksum (CRC-24).

ASCII armor

Μετατροπέας δυαδικής κωδικοποίησης, σε γραμματική.



Ο ρόλος των κεφαλίδων του OpenPGP

Ενημερώνουν τον χρήστη για το είδος των δεδομένων που κωδικοποιούνται σε ASCII armor. Οι κεφαλίδες αυτές είναι οι ακόλουθες:

- BEGIN PGP MESSAGE
- BEGIN PGP PUBLIC KEY BLOCK
- BEGIN PGP PRIVATE KEY BLOCK
- BEGIN PGP MESSAGE, PART X/Y
- BEGIN PGP MESSAGE, PART X
- BEGIN PGP SIGNATURE

Οι επικεφαλίδες αυτές:

- Είναι μέρος του συστήματος ASCII armor και όχι του μηνύματος.
- Παρέχουν πληροφορίες για το πώς θα αποκωδικοποιηθεί ή πως θα χρησιμοποιηθεί το μήνυμα, από το OpenPGP του παραλήπτη, ή από τον χρήστη (παραλήπτη), αντίστοιχα.
- Για το λόγο αυτό δεν προστατεύονται με τυχόν υπογραφές που έχουν εφαρμοστεί σε αυτό.

Παράδειγμα κεφαλίδας που δημιουργήθηκε με ASCII armor

```
-----BEGIN PGP MESSAGE-----  
Version: OpenPrivacy 0.99  
  
yDgBO22WxBHv7O8X7O/jygAEzol  
56iUKiXmV+XmpCtmpqQUKiQrFqc  
lFqUDBoVzSvBSFjNSiVHsuAA===  
njUN  
-----END PGP MESSAGE-----
```

Κάποιες φορές είναι επιθυμητό να μπορούμε να υπογράψουμε μια ακολουθία οκτάδων κειμένου (cleartext) χωρίς να εφαρμόσουμε μετατροπή ASCII armor σε αυτή, ώστε το κείμενο που υπογράφηκε να εξακολουθεί να είναι αναγνώσιμο χωρίς ειδικό λογισμικό. Προκειμένου λοιπόν να είναι δυνατή η προσάρτηση μιας υπογραφής σε αυτό το κείμενο, το OpenPGP ενσωματώνει το CSF (Cleartext Signature Framework - RFC3156)

<http://simple.wikipedia.org/wiki/Cleartext>
<https://tools.ietf.org/html/rfc3156>



Πρόληψη κενών ασφαλείας και επιθέσεων

Ο προγραμματιστής πρέπει να γνωρίζει όλες τις παραμέτρους ασφαλείας του OpenPGP και τις επιθέσεις που μπορεί να δεχτεί.

Θέματα ασφαλείας που θα πρέπει να ληφθούν υπόψιν κατά την υλοποίηση του OpenPGP

- ❖ Γνωστές ευπάθειες των αλγορίθμων που υλοποιούνται για την κρυπτογράφηση (πχ: ευπάθειες RSA), την παραγωγή κλειδιών, και ψηφιακών υπογραφών (πχ: SHA-1).
- ❖ Έλεγχος για νέες ευπάθειες και κενών ασφαλείας που έχουν βρεθεί πρόσφατα στους αλγόριθμους κρυπτογράφησης που θα ενσωματωθούν.
- ❖ Το ζεύγος δημοσίου και ιδιωτικού κλειδιού θα πρέπει να ελέγχεται και να α-σφαλίζεται από μια κεντρική υπηρεσία που θα είναι αξιόπιστη.
- ❖ Οι γεννήτριες τυχαίων αριθμών θα πρέπει να έχουν μια αποδεκτή εντροπία η οποία περιγράφεται στο τεχνικό έγγραφο RFC4086 .
- ❖ Ο αλγόριθμος MD5 δεν είναι πλέον ασφαλής και δε θα πρέπει να χρησιμοποιείται. Αντ' αυτού υπάρχει ο SHA-1.
- ❖ Τα σφάλματα που προκύπτουν κατά την αποσυμπίεση θα πρέπει να αντιμετωπίζονται ως προβλήματα ασφαλείας και όχι δεδομένων.

Στο αντίστοιχο RFC (σελίδα 81, παράγραφος 14, Security Considerations) γίνεται λεπτομερής αναφορά σε όλες τις πτυχές ασφαλείας που θα πρέπει να εξεταστούν.

<https://tools.ietf.org/html/rfc4086>

Νομοθεσία κρυπτογράφησης επικοινωνιών



Κάποιες χώρες θέτουν νομικούς περιορισμούς στην κρυπτογράφηση της επικοινωνίας των πολιτών τους.

Τι ισχύει σήμερα:

- ☐ Ορισμένες χώρες επιτρέπουν στους πολίτες τους να χρησιμοποιούν ισχυρούς αλγόριθμους κρυπτογράφησης αλλά υπό περιορισμούς και με τη δυνατότητα η πολιτεία να μπορεί να τους παρακάμψει.
- ☐ Άλλες, απαιτούν όλα τα κλειδιά κρυπτογράφησης να δίνονται σε κάποιο οργανισμό που θα λειτουργεί ως εγγυητής και θα τα παρέχει σε περίπτωση που προκύψει κάποια εγκληματική ενέργεια εκ μέρους του ατόμου που κρυπτογραφεί (ακόμα και αν είναι απλά ύποπτος), ώστε να είναι δυνατό να ελεγχθεί νομικά.

Οι νόμοι που διέπουν την κρυπτογράφηση επικοινωνιών, μεταβάλλονται συνεχώς και απρόβλεπτα. Αυτό δημιουργεί ιδιαίτερη σύγχυση και για το λόγο αυτό θα πρέπει κανείς να ενημερώνεται συχνά για την τρέχουσα ισχύουσα νομοθεσία.

Στον σύνδεσμο που ακολουθεί μπορούν να βρεθούν οι αντίστοιχες πληροφορίες για την Ελλάδα αλλά και για τις υπόλοιπες χώρες του κόσμου:

<http://www.cryptolaw.org/cls2.htm#gr>

2ο μέρος



Τα χαρακτηριστικά της εφαρμογής GnuPG

Η εφαρμογή GnuPG αποτελεί μια δωρεάν υλοποίηση του προτύπου OpenPGP.

Γενικά στοιχεία

- ✓ Ο πηγαίος κώδικας είναι ανοικτός και ελεύθερος
- ✓ Η καθαυτού διεπαφή χρήστη της εφαρμογής GnuPG, είναι η γραμμή εντολών χωρίς κάποιο γραφικό περιβάλλον. Αποτελεί την καθαρή υλοποίηση της μηχανής κρυπτογράφησης του OpenPGP και μπορεί να χρησιμοποιηθεί απευθείας από τη γραμμή εντολών, από σενάρια εντολών κελύφους (shell scripts), ή από άλλα προγράμματα (πχ: email clients).



<https://www.gnupg.org>

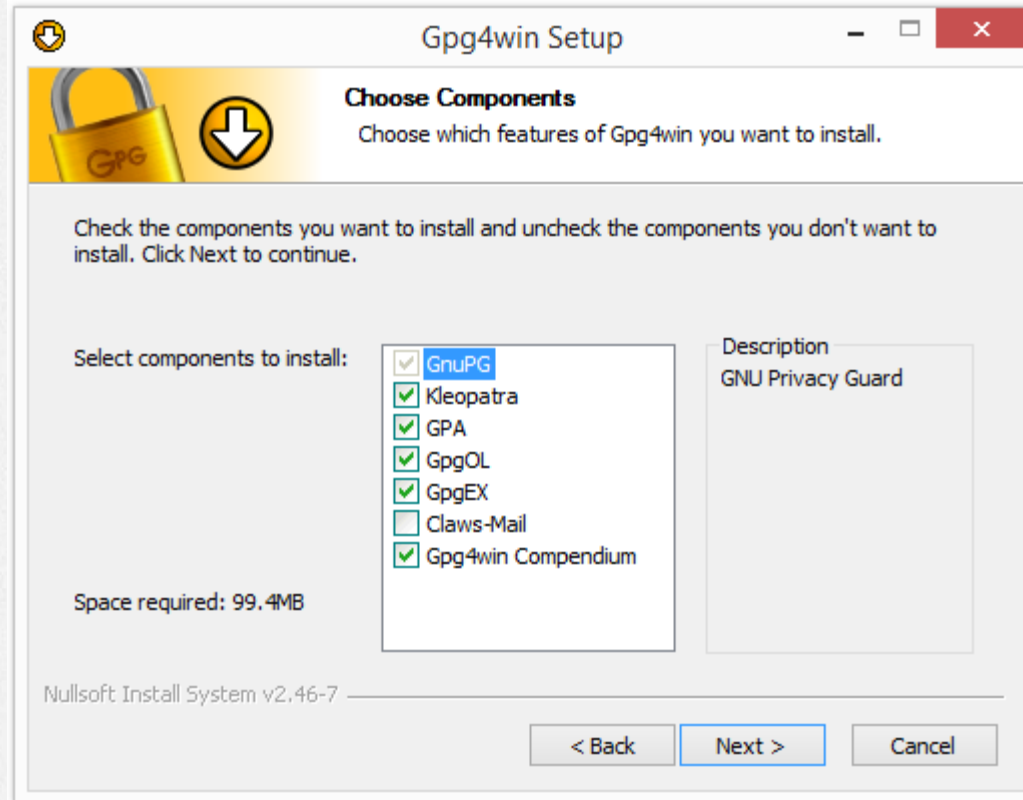
Τα βασικότερα χαρακτηριστικά της

- ✓ Αντικαθιστά πλήρως το PGP
- ✓ Δεν χρησιμοποιεί αλγόριθμους που προστατεύονται από πατέντες
- ✓ Αποτελεί την πλήρη υλοποίηση του προτύπου OpenPGP
- ✓ Αποκρυπτογραφεί και επαληθεύει μηνύματα PGP
- ✓ Υποστηρίζει τους αλγόριθμους ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 και TIGER.
- ✓ Η λειτουργικότητά της μπορεί να επεκταθεί με υλοποιήσεις νέων αλγορίθμων, μέσω του μηχανισμού των modules.
- ✓ Η μορφή του User ID είναι η standard
- ✓ Υποστηρίζει ημερομηνίες λήξης κλειδιών και υπογραφών
- ✓ Είναι πολύγλωσση
- ✓ Ενσωματώνει υποστήριξη για Keyserver
- ✓ Διαθέτει τεχνική υποστήριξη
- ✓ Περιλαμβάνει εκτενή τεχνική τεκμηρίωση
- ✓ Αποτελεί τη βάση (backend - API) για βοηθητικά λογισμικά

Εγκατάσταση GnuPG μέσω Gpg4win στα Windows



Η υλοποίηση GnuPG για το λειτουργικό σύστημα των Windows ονομάζεται Gpg4win.



Λεπτομέρειες εγκατάστασης

Η πιο πρόσφατη έκδοσή της (κατά την 11/06/2015) είναι η 2.2.4 (Released: 18/03/2015). Το μέγεθός του εκτελέσιμου που περιλαμβάνει το πλήρες πακέτο εγκατάστασης είναι περίπου 30MB.

Εφαρμογές πακέτου Gpg4win

- ✓ GnuPG (2.0.27) – Η GNU υλοποίηση του OpenPGP
- ✓ Kleopatra (2.2.0-git945878c) – Διαχειρίζεται κλειδιά OpenPGP και X.509
- ✓ GPA (0.9.7) – GNU Privacy Assistant
- ✓ GpgOL (1.2.1) – GnuPG για το Outlook
- ✓ GpgEX (1.0.1) – Επέκταση του GnuPG για το Shell των Windows
- ✓ Claws Mail (3.9.1) – Email client (**δεν εγκαταστάθηκε**)
- ✓ Kompendium (3.0.0) – Τεκμηρίωση (σε μορφή PDF)

<http://www.gpg4win.org>



Επαλήθευση ακεραιότητας του εγκαταστάτη

Έλεγχος του εκτελέσιμου αρχείου εγκατάστασης gpg4win-2.2.4.exe για κακόβουλη αλλοίωση.

Δυνατότητα επαλήθευσης

Μπορεί να γίνει με τον έλεγχο του αριθμού checksum του εν λόγω αρχείου ο οποίος απεικονίζεται και παρακάτω (κόκκινο πλαίσιο):

Gpg4win 2.2.4 (Released: 2015-03-18)

You can download the full version (including the Gpg4win compendium) of Gpg4win 2.2.4 here:

Gpg4win 2.2.4

Size: 30 MByte



OpenPGP signature (for gpg4win-2.2.4.exe)

SHA1 checksum (for gpg4win-2.2.4.exe): 8ddcbf14eb6df11139f709320a71d197a83bf9e1

Changelog

Μέθοδος πραγματοποίησης επαλήθευσης

Η επαλήθευση μπορεί να γίνει από το command prompt των Windows μέσω της εντολής:

```
CertUtil -hashfile C:\gpg4win-2.2.4.exe
```

Το αποτέλεσμα θα πρέπει να είναι το checksum:

8ddcbf14eb6df11139f709320a71d197a83bf9e1

```
Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

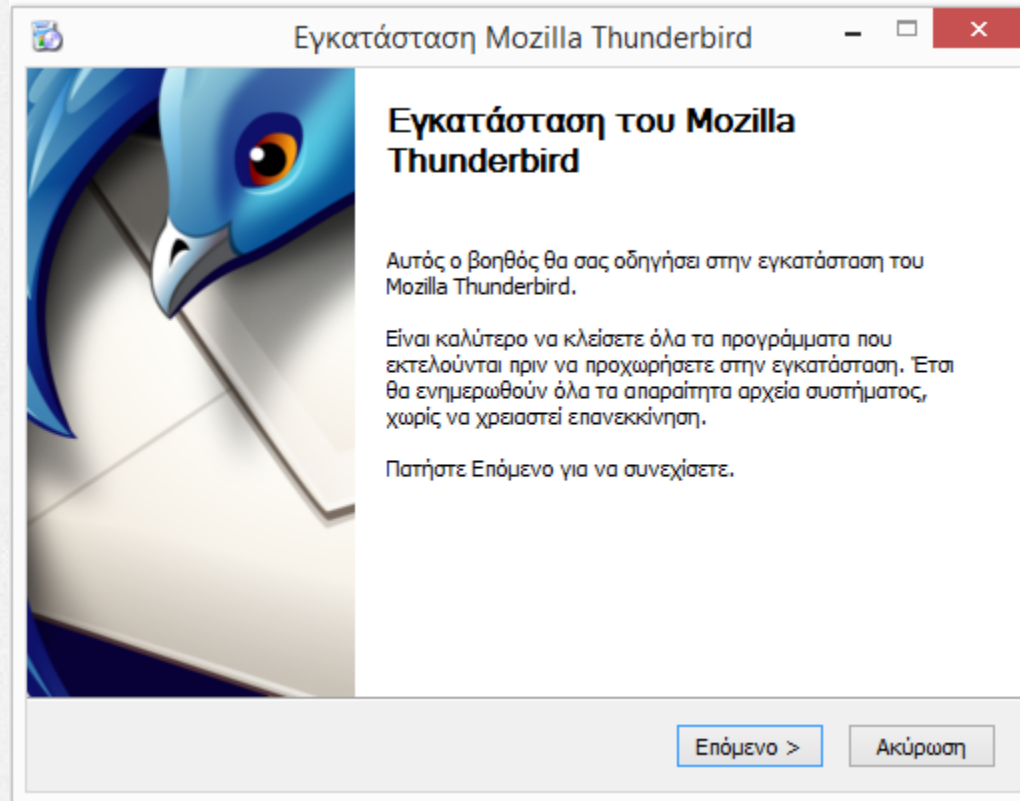
C:\Users\Jim>CertUtil -hashfile C:\gpg4win-2.2.4.exe
SHA1 hash of file C:\gpg4win-2.2.4.exe:
8d dc bf 14 eb 6d f1 11 39 f7 09 32 0a 71 d1 97 a8 3b f9 e1
CertUtil: -hashfile command completed successfully.
```

https://www.gnupg.org/download/integrity_check.html
<https://en.wikipedia.org/wiki/Checksum>

Εγκατάσταση του Mozilla Thunderbird



Πρόκειται για έναν δημοφιλή και δωρεάν, ανοικτού λογισμικού, email client, που μπορεί να συνεργαστεί με το Gpg4win.



Λεπτομέρειες εγκατάστασης

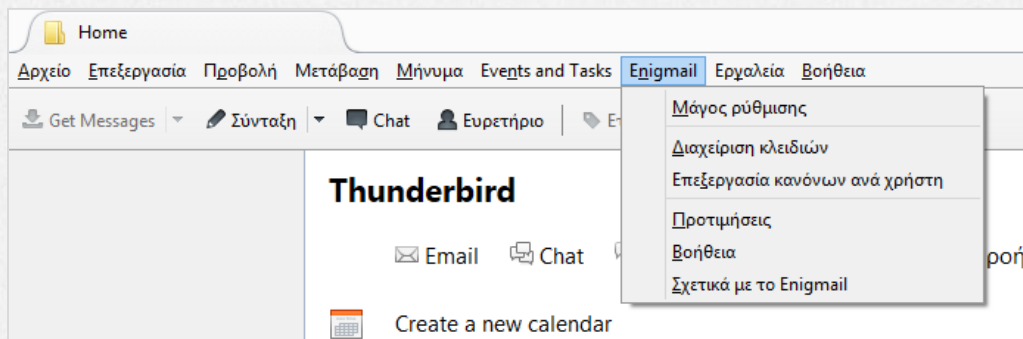
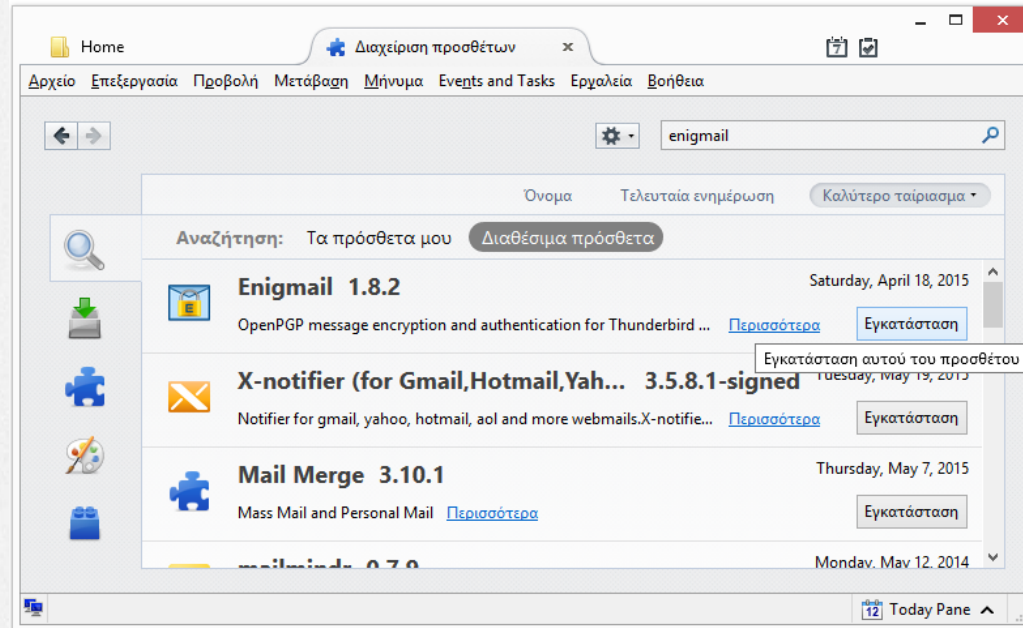
- ✓ Η ελληνική έκδοση είναι προτιμότερη καθώς εξασφαλίζει ότι δεν θα υπάρχουν προβλήματα κωδικοποίησης κειμένου
- ✓ Η εγκατάσταση είναι απλή και μπορεί να γίνει με τις προεπιλεγμένες ρυθμίσεις του εγκαταστάτη.

<https://www.mozilla.org/el/thunderbird>

Εγκατάσταση Enigmail στον Mozilla Thunderbird



Πρόκειται για ένα πρόσθετο που λειτουργεί ως γέφυρα ανάμεσα στον Thunderbird και στις εφαρμογές του Gpg4win.



Λεπτομέρειες εγκατάστασης Enigmail

- ✓ Επιλέγοντας από το κυρίως μενού του Mozilla Thunderbird, Εργαλεία > Πρόσθετα και εισάγοντας ως κριτήριο αναζήτησης τη λέξη enigmail, εντοπίζουμε το πρόσθετο και το εγκαθιστούμε
- ✓ Αν όλα έχουν ολοκληρωθεί επιτυχώς, θα πρέπει να έχει εμφανιστεί ένα νέο μενού με το όνομα Enigmail.

Λειτουργικότητα Enigmail

Το πρόσθετο Enigmail λειτουργεί συμπληρωματικά με τα προγράμματα Kleopatra και GPA (GNU Privacy Assistant) που εγκαταστάθηκαν από το Gpg4win.

<https://addons.mozilla.org/el/thunderbird/addon/enigmail>
<https://www.enigmail.net>

Δημιουργία λογαριασμού email στον Thunderbird



Απαιτείται ένα έγκυρο προσωπικό email για να υπάρχει η δυνατότητα ανταλλαγής μηνυμάτων με άλλους χρήστες.

Ρύθμιση λογαριασμού αλληλογραφίας

Το όνομα σας: Το όνομα σας, όπως θα εμφανίζεται σε τρίτους

Διεύθυνση Email:

Κωδικός:

☐ Απομνημόνευση κωδικού

Βρέθηκαν οι παρακάτω ρυθμίσεις σε: Βάση δεδομένων ISP του Mozilla

☒ IMAP (απομακρυσμένοι φάκελοι) ☐ POP3 (διατήρηση αλληλογραφίας στον υπολογιστή σας)

Εισερχομένων: IMAP, imap.mail.yahoo.com, SSL

Εξερχομένων: SMTP, smtp.mail.yahoo.com, SSL

Όνομα χρήστη: dimitriosrousis@yahoo.com

Λεπτομέρειες

1) Επιλέγουμε Αρχείο > Νέο > Δημιουργία νέου λογαριασμού αλληλογραφίας για να εισάγουμε τη διεύθυνση email που ήδη διαθέτουμε. Στην περίπτωση μας:

dimitriosrousis@yahoo.com

2) Επιλέγουμε κωδικό, και το πρωτόκολλο IMAP για να μην αποθηκεύονται τα μηνύματα στον υπολογιστή αλλά μόνο η δομή των καταλόγων.

Ρύθμιση του προσθέτου Enigmail (1/3)



Απαιτείται για μπορεί να λειτουργεί ως γέφυρα ανάμεσα στον Thunderbird και στις εφαρμογές του Gpg4win.

Μάγος ρύθμισης Enigmail

Δημιουργία κλειδιού
Δημιουργία ενός κλειδιού για την υπογραφή και κρυπτογράφηση μηνυμάτων

This dialog will create a pair of two keys:
Your **public key** is for **others** to send you encrypted emails. You can distribute it to everybody.
Your **private key** is for **yourself** to decrypt these emails and to send signed emails. You should give it to nobody.

Your **passphrase** is a password to protect your private key. It prevents misuse of your private key. The passphrase should be a phrase containing at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, é, ñ) and language-specific characters are **not** recommended.

Λογαριασμός / ID χρήστη:
Dimitrios Rousis <dimitriosrousis@yahoo.com> - dimitriosrousis@yahoo.com

Φράση πρόσβασης
.....
Παρακαλώ επαληθεύστε τη φράση πρόσβασης πληκτρολογώντας την ξανά
.....
Passphrase quality:
.....

< Πίσω Επόμενο > Άκυρο

Λεπτομέρειες ρύθμισης Enigmail

Επιλέγουμε Enigmail > Μάγος ρύθμισης (Setup wizard) και στα επόμενα παράθυρα διαλόγου που θα προκύψουν επιλέγουμε με τη σειρά:

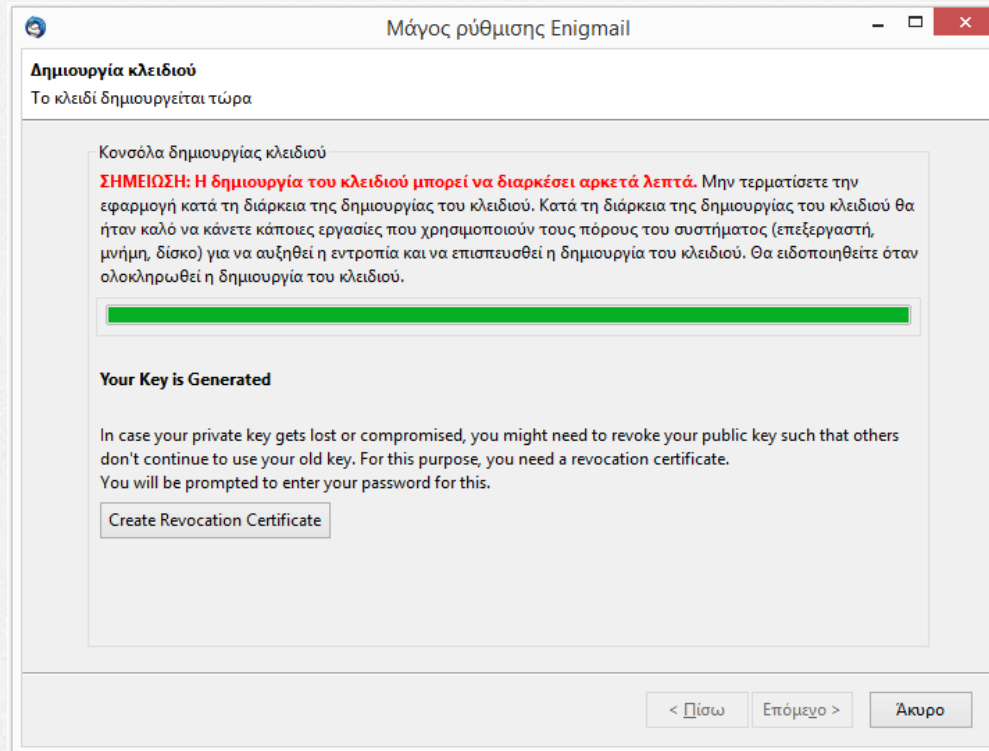
- 1) I prefer an extended configuration (recommended for beginners advanced users). Οι ρυθμίσεις για experts μπο-ρούν να γίνουν και εκ των υστέρων.
- 2) Θέλω να δημιουργήσω ένα νέο ζεύγος κλειδιών για την υπογραφή και κρυπτογράφηση της αλληλογραφίας μου



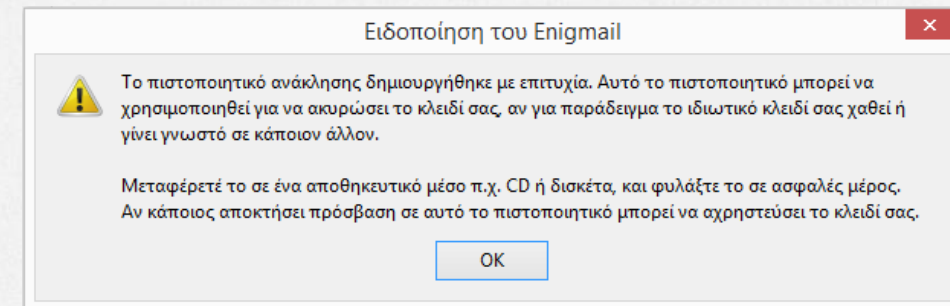
Ρύθμιση του προσθέτου Enigmail (2/3)



Απαιτείται για μπορεί να λειτουργεί ως γέφυρα ανάμεσα στον Thunderbird και στις εφαρμογές του Gpg4win.



- 3) Create Revocation Certificate (δημιουργία πιστοποιητικού ανάκλησης)
- 4) Αποθήκευση πιστοποιητικού ανάκλησης σε ασφαλές σημείο (σε μορφή .asc). Ζητείται επίσης η passphrase που δώσαμε νωρίτερα.
- 5) Αφού έχουμε ολοκληρώσει την αποθήκευση του πιστοποιητικού:



Σε αυτό το σημείο η τυπική παραμετροποίηση του προσθέτου Enigmail έχει ολοκληρωθεί και μπορεί να πραγματοποιηθεί η παραμετροποίηση για experts .

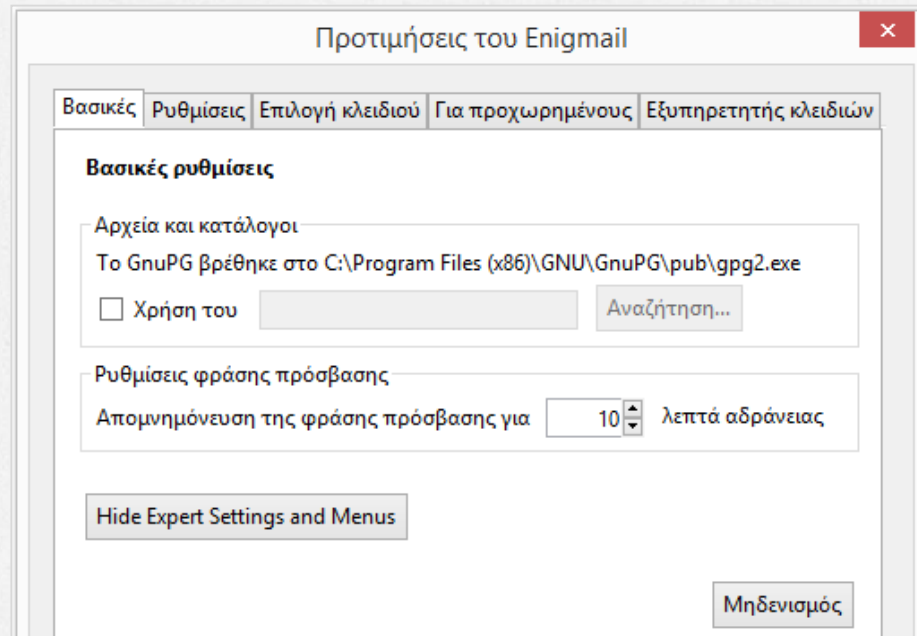


Ρύθμιση του προσθέτου Enigmail (3/3)

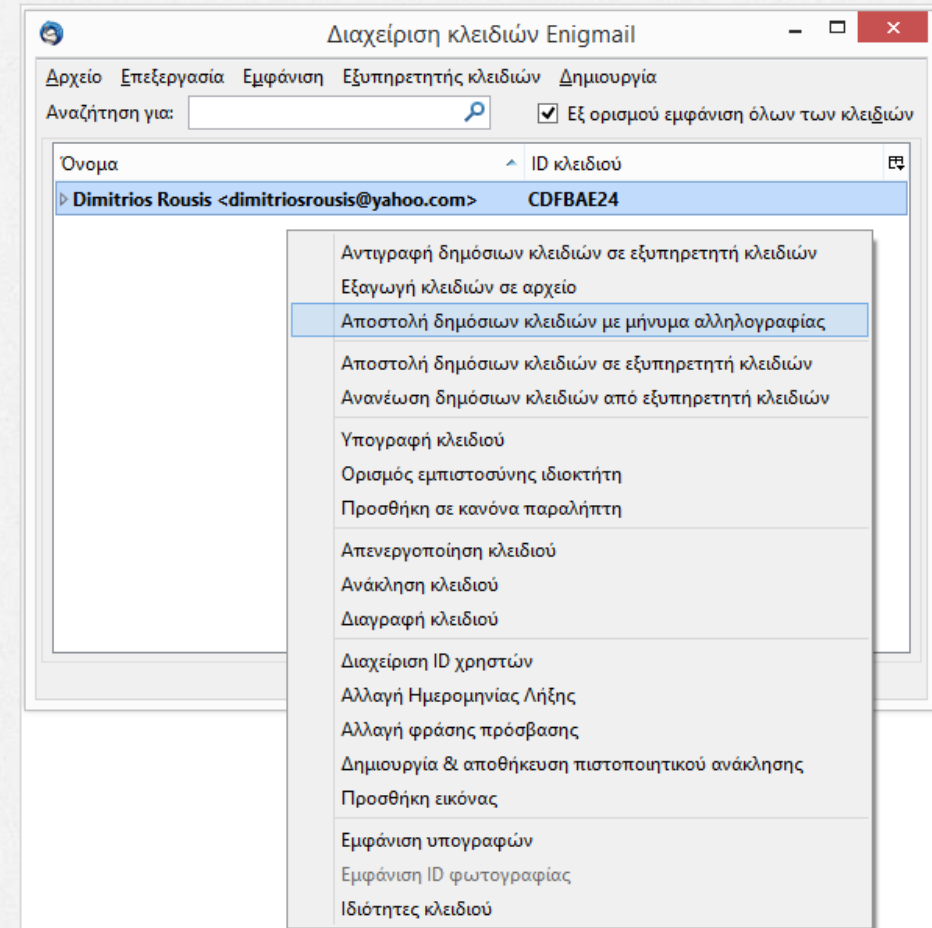


Απαιτείται για μπορεί να λειτουργεί ως γέφυρα ανάμεσα στον Thunderbird και στις εφαρμογές του Gpg4win.

- 6) Η παραμετροποίηση για experts μπορεί να πραγματοποιηθεί, είτε και πάλι μέσω του wizard, είτε επιλέγοντας Enigmail > Προτιμήσεις:



- 7) Για να δούμε το κλειδί που δημιουργήθηκε επιλέγουμε Enigmail > Διαχείριση κλειδιών:



3ο μέρος

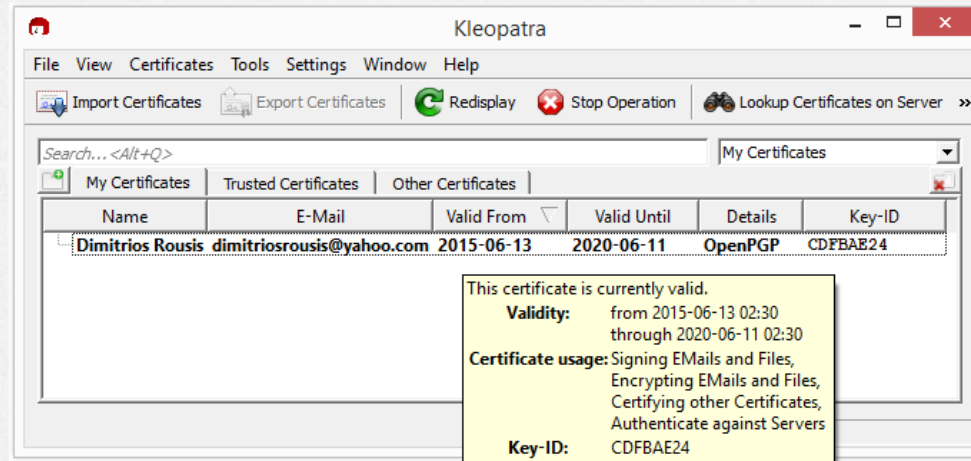


Αποστολή κρυπτογραφημένου email και επισυναπτόμενου αρχείου.

Το σενάριο

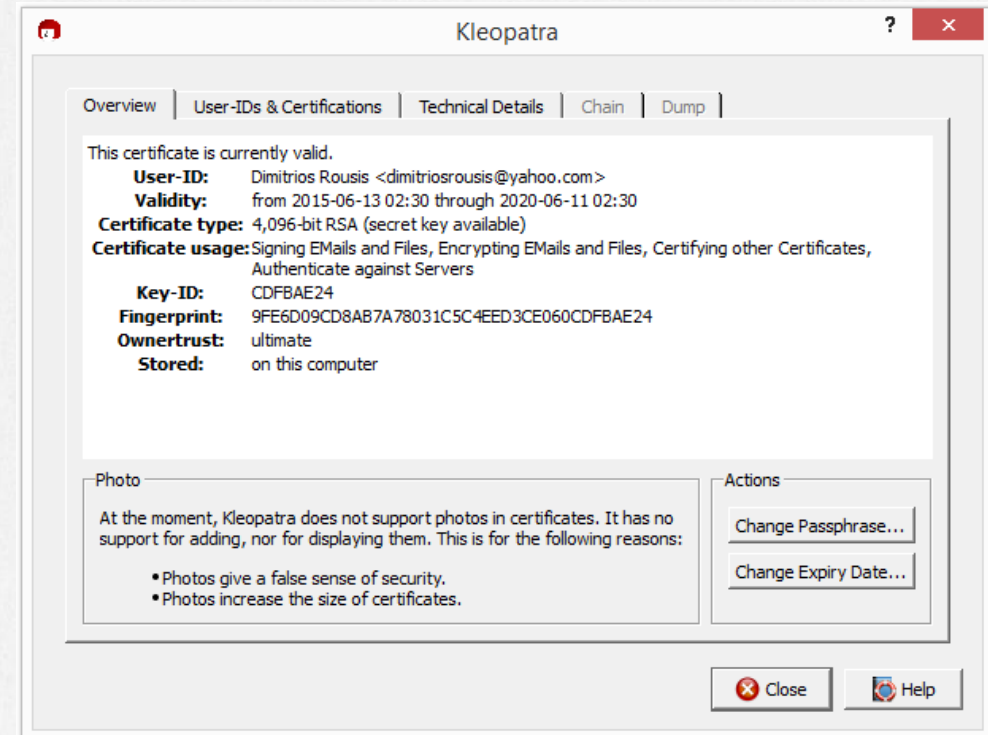
Ο φοιτητής Δημήτρης (αποστολέας), θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον καθηγητή του (παραλήπτης) μέσω ηλεκτρονικής αλληλογραφίας.

Στο μήνυμα αυτό θα περιλαμβάνεται ως επισυναπτόμενο αρχείο, το δημόσιό του κλειδί (0xCDFBAE24.asc), και ως κρυπτογραφημένο κείμενο μηνύματος, ορισμένες συνοδευτικές πληροφορίες.



Εμφάνιση πιστοποιητικού στην Kleopatra

Το πιστοποιητικό ανάκλησης και το δημόσιο και ιδιωτικό κλειδί του αποστολέα, δημιουργήθηκαν κατά την εγκατάσταση του προσθέτου Enigmail:



Σενάριο χρήσης Gpg4win και Thunderbird (2/3)



Αποστολή κρυπτογραφημένου email και επισυναπτόμενου αρχείου.

Εγκατάσταση επικοινωνίας

Για να είναι εφικτή η επικοινωνία ανάμεσα σε αποστολέα και παραλήπτη, θα πρέπει αρχικά να είναι γνωστό το email του δεύτερου στον πρώτο. Για να είναι και ασφαλής, το ίδιο θα πρέπει να ισχύει και για το δημόσιο κλειδί :

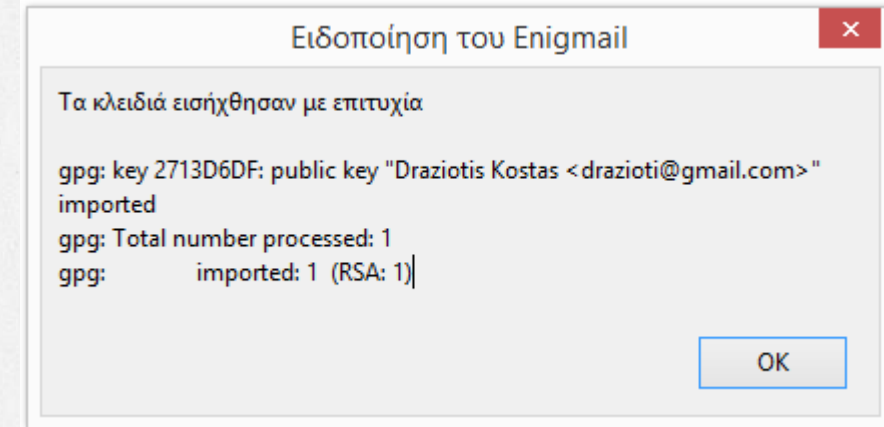
Παραλήπτης

Email = drazioti@gmail.com

Δημόσιο κλειδί

<http://users.auth.gr/drazioti/pgp.htm>

Αφού ο αποστολέας γνωρίζει το δημόσιο κλειδί του παραλήπτη, μπορεί να το εισάγει επιλέγοντας
Enigmail > Διαχείριση κλειδιών και Αρχείο > Εισαγωγή κλειδιών από αρχείο, επιλέγοντας το αρχείο .asc που το περιλαμβάνει.



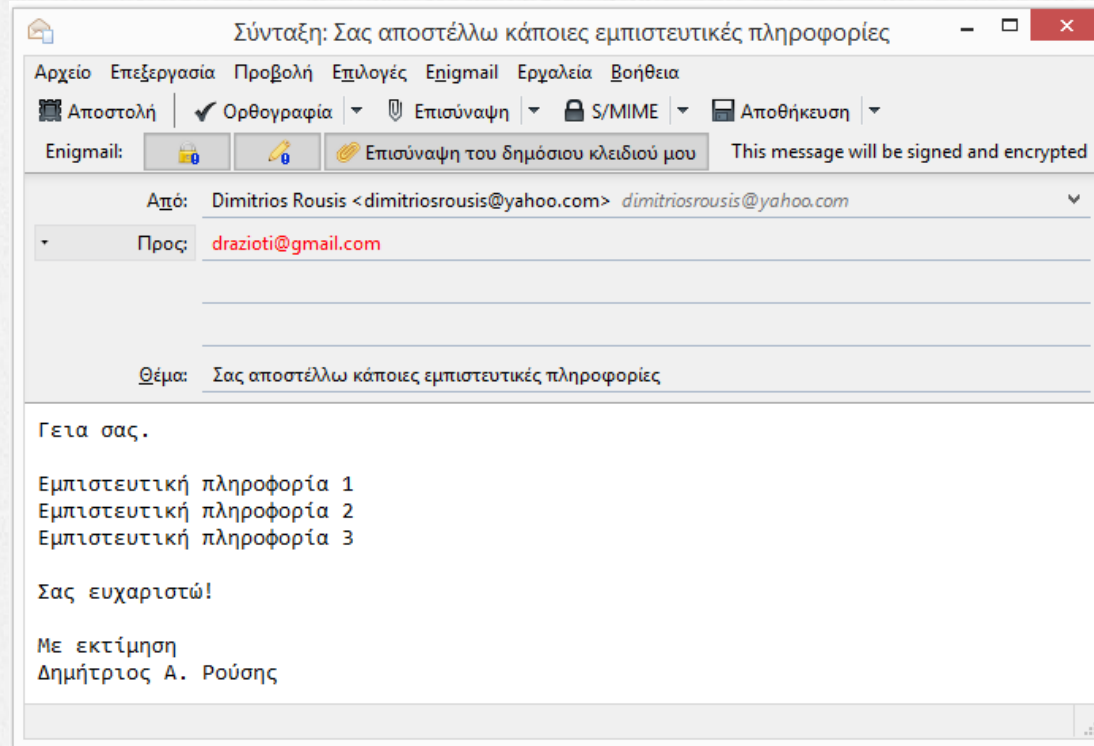
Με αυτό, ο αποστολέας θα μπορεί να κρυπτογραφήσει το μήνυμα που θα στείλει στον παραλήπτη, ώστε αυτός με το ιδιωτικό του κλειδί, στη συνέχεια να μπορεί να το αποκρυπτογραφήσει.

Σενάριο χρήσης Gpg4win και Thunderbird (3/3)



Αποστολή κρυπτογραφημένου email και επισυναπτόμενου αρχείου.

Το περιβάλλον αποστολής email του Thunderbird σε αυτή την περίπτωση είναι το παρακάτω:



Μετά την αποστολή το κρυπτογραφημένο μήνυμα (ένα τμήμα του) που λαμβάνει ο παραλήπτης είναι το ακόλουθο:

-----BEGIN PGP MESSAGE-----

Charset: utf-8

Version: GnuPG v2

hQEMA+sRhfgnE9bfAQgA60iKWktDNqTSMNRs/WBB8C
AcVn3Ne8EfkWeyw7nViIt7
JzN0jASQ5AW/0In/9hr+KZVln6r5D4xr3TtcURMhy4
Lv0cXmDNewMtKjWqfOCy3H

.

1rfjZI1h6Hp4j7ECKNcFjXECLThqNbIRIClFCQ9bA4
mAU63wl9mD+qjedMOG+HAL
UoqLNV/ICJ4wDux9oTFw4f0TenjcZrhEQ9rYmy+/R3
LtJfm7DucLdEvldxfDipEW
PA==

=rP+n

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

Για να μπορέσει να το διαβάσει το αποκρυπτογραφεί με το ιδιωτικό του κλειδί.

4ο μέρος



Οι κυριότερες διαφορές μεταξύ των OpenPGP και X.509 PKIs μπορούν να χωριστούν σε τρεις κατηγορίες:

- A.** Διαφορές στο πιστοποιητικό – Κάθε πιστοποιητικό OpenPGP περιέχει μια αυτοϋπογραφή και μπορεί να περιέχει πολλές υπογραφές, ενώ τα πιστοποιητικά X.509 υποστηρίζουν μόνο μία ψηφιακή υπογραφή για να πιστοποιούν την εγκυρότητα του κλειδιού. Τα πιστοποιητικά X.509 υποστηρίζουν εγγενώς μόνο ένα όνομα για τον ιδιοκτήτη του κλειδιού. Τα πιστοποιητικά Open-PGP έχουν δημόσιο κλειδί με διάφορες ετικέτες που προσδιορίζουν τον χρήστη με διαφορετικούς τρόπους.
- B.** Διαφορές στο δίκτυο εμπιστοσύνης (Network of Trust) – Ο χρήστης μπορεί να δημιουργήσει το δικό του πιστοποιητικό OpenPGP, αλλά στην περίπτωση του X.509 θα πρέπει να ζητήσει να εκδοθεί από μια Αρχή Πιστοποίησης. Με τα πιστοποιητικά X.509, μεσολαβεί πάντα μια Αρχή Πιστοποίησης. Επίσης το OpenPGP χρησιμοποιεί ψηφιακές υπογραφές για την σύσταση ενός ατόμου στους άλλους. Κάθε φορά που κάποιος χρήστης υπογράφει το δημόσιο κλειδί κάποιου άλλου, γίνεται ο διαμεσολαβητής που τον συστήνει στους υπόλοιπους ως ένα έμπιστο άτομο. Καθώς αυτή η διαδικασία συνεχίζεται, θεσπίζεται ένας ιστός εμπιστοσύνης (web of trust), έτσι ώστε κάθε χρήστης να μπορεί να ενεργεί ως αρχή πιστοποίησης.
- C.** Διαφορές στη διαδικασία ανάκλησης (revocation procedure) – Με τα πιστοποιητικά X.509, μια ανακληθείσα υπογραφή είναι σχεδόν το ίδιο με ένα πιστοποιητικό που έχει ανακληθεί, δεδομένου ότι η μόνη υπογραφή του πιστοποιητικού είναι αυτή που την έκανε έγκυρη εξ' αρχής. Δηλαδή η υπογραφή της Αρχής Πιστοποίησης. Τα πιστοποιητικά OpenPGP από την άλλη, παρέχουν το επιπλέον χαρακτηριστικό, ότι ο χρήστης μπορεί να ανακαλέσει ολόκληρο το πιστοποιητικό του, αν αισθάνεται ότι αυτό έχει παραβιαστεί.



- [1] A. Menezes, P. Oorschot και S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
- [2] T. Elgamal, «A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,» *IEEE Transactions on Information Theory*, pp. 469-472, 1985.
- [3] B. Schneier, Applied Cryptography [Second Edition]: protocols, algorithms, and source code in C, John Wiley & Sons , 1996.
- [4] B. Schneier, «Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption,» *Cambridge Security Workshop Proceedings, Springer-Verlag*, pp. 191-204, 1994.
- [5] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall και N. Ferguson, The Twofish Encryption Algorithm: A 128-Bit Block Cipher, John Wiley & Sons , 1996 .
- [6] N. Prohic, «Public Key Infrastructures – PGP vs. X.509,» *INFOTECH Seminar Advanced Communication Services (ACS)*, p. 9, 2005.

Μενού

1. [Εισαγωγή στο πρότυπο OpenPGP](#)
2. [Η τεχνική υποστήριξη του OpenPGP](#)
3. [Γενικές λειτουργίες του OpenPGP](#)
4. [Εμπιστευτικότητα μέσω Κρυπτογράφησης](#)
5. [Ταυτοποίηση μέσω ψηφιακής υπογραφής](#)
6. [Συμμετρικοί & ασύμμετροι αλγόριθμοι κρυπτογράφησης](#)
7. [Συναρτήσεις κατακερματισμού](#)
8. [Οδηγός – σύνοψη ενεργειών στο OpenPGP](#)
9. [Τύποι δεδομένων](#)
10. [Δομή πακέτου OpenPGP](#)
11. [Ετικέτες και τύποι πακέτων OpenPGP](#)
12. [Ενισχυμένα κλειδιά στο OpenPGP](#)
13. [Μετατροπές Radix-64](#)
14. [ASCII armor](#)
15. [Πρόληψη κενών ασφαλείας και επιθέσεων](#)
16. [Νομοθεσία κρυπτογράφησης επικοινωνιών](#)
17. [Τα χαρακτηριστικά της εφαρμογής GnuPG](#)
18. [Εγκατάσταση GnuPG μέσω Gpg4win στα Windows](#)
19. [Επαλήθευση ακεραιότητας του εγκαταστάτη](#)
20. [Εγκατάσταση του Mozilla Thunderbird](#)
21. [Εγκατάσταση Enigmail στον Mozilla Thunderbird](#)
22. [Δημιουργία λογαριασμού email στον Thunderbird](#)
23. [Ρύθμιση του προσθέτου Enigmail](#)
24. [Σενάριο χρήσης Gpg4win και Thunderbird](#)
25. [Διαφορές OpenPGP από S/MIME X.509](#)
26. [Βιβλιογραφία](#)