OpenPGP

Το πρότυπο κρυπτογράφησης και οι εφαρμογές του

RFC 4880
(IETF)

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πρόγραμμα Μεταπτυχιακών Σπουδών στην Πληροφορική
Επικοινωνιακά Συστήματα και Τεχνολογίες
Προχωρημένα Θέματα Ασφάλειας

Δημήτριος Α. Ρούσης (ΑΜ: 532)

Περιεχόμενα

1. Εισαγωγή ... 3
1.1 Τι είναι το PGP ... 3
1.2 Πως χρησιμοποιήθηκε το OpenPGP ... 3
1.3 Σύνοψη ονοματολογίας (PGP, GnuPG, OpenPGP) ... 4
2. Η τεχνική υποστήριξη του OpenPGP ... 4
3. Γενικές λειτουργίες του OpenPGP ... 5
3.1 Εμπιστευτικότητα μέσω Κρυπτογράφησης ... 5
3.2 Ταυτοποίηση μέσω ψηφιακής υπογραφής ... 6
3.3 Συμπίεση ... 7
3.4 Συμμετρικοί και ασύμμετροι αλγόριθμοι κρυπτογράφησης ... 7
3.5 Συναρτήσεις κατακερματισμού ... 8
4. Σύνοψη λειτουργιών του OpenPGP ... 8
5. Τύποι δεδομένων ... 9
6. Δομή πακέτου ... 10
6.1 Ετικέτες πακέτων ... 10
6.2 Τύποι πακέτων ... 11
7. Ενισχυμένα κλειδιά ... 12
7.1 Αποτύπωμα και αναγνωριστικό κλειδιού ... 12
8. Μετατροπέας Radix-64 ... 13
9. ASCII armor ... 13
10. Ζητήματα κατά την υλοποίηση του OpenPGP ... 14
10.1 Παράμετροι ασφαλείας και επιθέσεις που πρέπει να ληφθούν υπόψιν ... 15
11. Νομοθεσία ... 15
12. Η εφαρμογή GnuPG ή GPG ... 16
12.1 Τα χαρακτηριστικά της εφαρμογής ... 16
13. Εγκατάσταση GnuPG στα Windows ... 17
13.1 Εγκατάσταση GnuPG μέσω της εφαρμογής Gpg4win ... 18
13.1.1 Επαλήθευση ακεραιότητας του αρχείου `gpg4win-2.2.4.exe` ... 19

14. Εγκατάσταση του Mozilla Thunderbird 20
14.1 Εγκατάσταση του προσθέτου Enigmail στον Mozilla Thunderbird..... 21
14.2 Δημιουργία νέου λογαριασμού email στον Mozilla Thunderbird 23
14.3 Ρύθμιση του Enigmail 24
15. Σενάριο χρήσης 27
15.1 Αποστολή κρυπτογραφημένου email και επισυναπτόμενου αρχείου.... 27
16. Παραρτήματα 31
16.1 Διαφορές OpenPGP από S/MIME X.509..... 31
16.2 Προτιμήσεις - ρυθμίσεις του Enigmail 32
16.3 Δημόσια κλειδιά 35
16.3.1 Δημόσιο κλειδί παραλήπτη 35
16.3.2 Δημόσιο κλειδί αποστολέα 36
17. Βιβλιογραφία 37

1. Εισαγωγή

Το παρόν έγγραφο αφορά την περιγραφή των βασικότερων χαρακτηριστικών του προτύπου OpenPGP και της παρουσίασης της λειτουργίας μιας εκ των υλοποιήσεών του (GnuPG).

1.1 Τι είναι το PGP

Το PGP[1] (Pretty Good Privacy), είναι λογισμικό κρυπτογράφησης το οποίο παρέχει ιδιωτικότητα και ταυτοποίηση κατά την επικοινωνία δεδομένων. Χρησιμοποιείται για την υπογραφή, κρυπτογράφηση, και αποκρυπτογράφηση κειμένων, emails, αρχείων, καταλόγων, αλλά και ολόκληρων κατατμήσεων δίσκων αποθήκευσης. Αναπτύχθηκε από τον Phil Zimmermann[2, 3] το 1991 (Bitcoin), και το 2010 εξαγοράστηκε[4, 5] από την εταιρία Symantec για 300 εκ. δολάρια, η οποία και το εμπορεύεται[6, 7] πλέον.

Το PGP έκανε εκτεταμένη χρήση των προστατευμένων με πατέντα, τεχνικών κρυπτογράφησης, RSA και IDEA[8]. Για το λόγο αυτό, όποιος ήθελε να το χρησιμοποιήσει έπρεπε να πληρώσει την αντίστοιχη άδεια χρήσης λογισμικού. Έτσι ο δημιουργός του το 1998 προσέφερε μια λύση. Η εταιρεία του, PGP Corporation, υπέβαλλε στην αρχή IETF (Internet Engineering Task Force) μια βελτιωμένη έκδοση του PGP με την ονομασία OpenPGP[9] (RFC 4880[10]).

1.2 Πως χρησιμοποιήθηκε το OpenPGP

Το OpenPGP καθόριζε πρότυπα με τα οποία τα διάφορα προγράμματα μπορούσαν να επικοινωνούν ελεύθερα αλλά με ασφάλεια, χρησιμοποιώντας μια βελτιωμένη έκδοση του πρωτοκόλλου PGP και μια ποικιλία διαφορετικών αλγορίθμων κρυπτογράφησης. Αυτό άνοιξε το δρόμο για τους ανθρώπους και τις εταιρείες να

[1] http://en.wikipedia.org/wiki/Pretty_Good_Privacy
[2] http://www.philzimmermann.com
[3] http://en.wikipedia.org/wiki/Phil_Zimmermann
[4] http://bcove.me/sf18vyck
[5] http://www.symantec.com/about/news/release/article.jsp?prid=20100607_01
[6] http://buy.symantec.com/estore/clp/category-encryption
[7] http://www.symantec.com/encryption/
[8] http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm
[9] http://www.openpgp.org
[10] http://tools.ietf.org/html/rfc4880

δημιουργήσουν τις δικές τους εφαρμογές του OpenPGP από το μηδέν, προσαρμόζοντάς τες ώστε να καλύπτουν τις δικές τους ανάγκες. Η εφαρμογή ανοικτού λογισμικού GnuPG[11] (ή GPG ή GNU Privacy Guard) αποτελεί ένα σημαντικό παράδειγμα και είναι αυτή που θα βοηθήσει στη συνέχεια της παρούσας εργασίας να παρουσιαστούν οι δυνατότητες του προτύπου OpenPGP.

1.3 Σύνοψη ονοματολογίας (PGP, GnuPG, OpenPGP)

Οι όροι PGP, GPG και OpenPGP αρκετές φορές δημιουργούν σύγχυση. Γι' αυτό παρακάτω συνοψίζεται η επεξήγηση της χρήσης τους:

- 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).

2. Η τεχνική υποστήριξη του OpenPGP

Στην εικόνα που ακολουθεί παρατίθεται το λογότυπό της συμμαχίας OpenPGP:

Η συμμαχία OpenPGP αποτελείται από ένα σύνολο εταιρειών[12] και οργανισμών που υλοποιούν το πρότυπο αυτό στις εφαρμογές τους. Συνεργάζονται προκειμένου να επιτυγχάνουν την συμβατότητα, την τεχνική διαλειτουργικότητα[13] και την εμπορική συνεργεία[14] μεταξύ των εφαρμογών OpenPGP.

Περισσότερες πληροφορίες, πηγές[15] και νέα[16] για το OpenPGP, μπορούν να βρεθούν και στην επίσημη ιστοσελίδα του προτύπου.

[11] https://www.gnupg.org
[12] http://www.openpgp.org/members
[13] http://www.openpgp.org/technical/interoperability
[14] http://www.openpgp.org/about_openpgp/services
[15] http://www.openpgp.org/resources
[16] http://www.openpgp.org/news_events

3. Γενικές λειτουργίες του OpenPGP

Το πρότυπο OpenPGP παρέχει υπηρεσίες ακεραιότητας δεδομένων, για μηνύματα και αρχεία δεδομένων, κάνοντας χρήση των παρακάτω τεχνολογιών:

- Ψηφιακές υπογραφές[17]
- Κρυπτογράφηση[18]
- Συμπίεση
- Μετατροπή Radix-64[19, 20]

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

3.1 Εμπιστευτικότητα μέσω Κρυπτογράφησης

Το OpenPGP συνδυάζει συμμετρική[21] και ασύμμετρη[22] κρυπτογράφηση προκειμένου να παρέχει εμπιστευτικότητα στην επικοινωνία. 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 που 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.

[17] http://en.wikipedia.org/wiki/Digital_signature
[18] http://en.wikipedia.org/wiki/Cryptography
[19] https://tools.ietf.org/html/rfc4880#section-2.4
[20] Πολλά συστήματα ηλεκτρονικού ταχυδρομείου μπορούν να μεταδώσουν μόνο μπλοκ κειμένου ASCII. Αυτό μπορεί να προκαλέσει προβλήματα κατά την αποστολή κρυπτογραφημένων δεδομένων αφού τα μπλοκ του κρυπτοκειμένου ενδέχεται να μην αντιστοιχούν στους χαρακτήρες ASCII που θα μεταδοθούν. Το OpenPGP ξεπερνά αυτό το πρόβλημα χρησιμοποιώντας μετατροπή ASCII σε radix-64.
[21] http://en.wikipedia.org/wiki/Symmetric-key_algorithm
[22] http://en.wikipedia.org/wiki/Public-key_cryptography

4) Το OpenPGP του αποστολέα κρυπτογραφεί το μήνυμα χρησιμοποιώντας το κλειδί συνόδου. Έτσι σε συνδυασμό με τα bit έναρξης προκύπτει ολόκληρο το πακέτο που θα μεταδοθεί. Πριν από την κρυπτογράφηση του μηνύματος προηγείται η συμπίεσή του με κάποιον από τους υποστηριζόμενους αλγόριθμους συμπίεσης.
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.

Με τη συμμετρική κρυπτογράφηση, ένα αντικείμενο μπορεί να κρυπτογραφηθεί με ένα συμμετρικό κλειδί που προκύπτει από κάποια κωδική φράση (passphrase), ή μέσω ενός μηχανισμού δύο σταδίων (two-stage) όπως αυτή που είδαμε πριν με τη μέθοδο δημοσίου κλειδιού.

Οι υπηρεσίες ψηφιακής υπογραφής και εμπιστευτικότητας θα πρέπει εφαρμοστούν και οι δύο στο ίδιο μήνυμα. Πρώτα δημιουργείται μια ψηφιακή υπογραφή για το μήνυμα και προσαρτάται σε αυτό. Στη συνέχεια, το μήνυμα μαζί με την υπογραφή, κρυπτογραφούνται χρησιμοποιώντας ένα συμμετρικό κλειδί συνόδου (σχηματίζοντας ένα μπλοκ). Τέλος, το κλειδί συνόδου κρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί και δέχεται ως πρόθεμα το κρυπτογραφημένο μπλοκ.

3.2 Ταυτοποίηση μέσω ψηφιακής υπογραφής

Ο μηχανισμός ψηφιακής υπογραφής χρησιμοποιεί έναν κωδικό κατακερματισμού (μέσω κάποιας hash function[23]) ή κάποιο αλγόριθμο message-digest[24], και έναν αλγόριθμο υπογραφής δημοσίου κλειδιού. Η ακολουθία των βημάτων είναι:

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.

[23] http://en.wikipedia.org/wiki/Hash_function
[24] http://en.wikipedia.org/wiki/Cryptographic_hash_function#Cryptographic_hash_algorithms

6) Το λογισμικό λήψης δημιουργεί ένα νέο hash κωδικό για το ληφθέν μήνυμα και το επαληθεύει χρησιμοποιώντας την υπογραφή του μηνύματος αυτού. Αν η ταυτοποίηση είναι επιτυχής, το μήνυμα γίνεται αποδεκτό ως αυθεντικό (γνήσιο).

3.3 Συμπίεση

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[25])
- ✓ ZLIB (RFC1950[26])
- ✓ BZip2[27]

3.4 Συμμετρικοί και ασύμμετροι αλγόριθμοι κρυπτογράφησης

Οι αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού που χρησιμοποιούνται συχνότερα σε υλοποιήσεις του OpenPGP είναι:

	RSA [1]	**Elgamal** [2]	**DSA** [28]
Κρυπτογράφηση	✓	✓	
Ψηφιακή Υπογραφή	✓		✓

Επίσης υπάρχει η δυνατότητα χρήσης των παρακάτω:

- ✓ ECC (Elliptic curve cryptography[29])
- ✓ ECDSA (Elliptic Curve Digital Signature Algorithm[30])
- ✓ Diffie-Hellman[31]

[25] https://tools.ietf.org/html/rfc1951
[26] https://tools.ietf.org/html/rfc1950
[27] http://www.bzip.org
[28] http://dx.doi.org/10.6028/NIST.FIPS.186-4
[29] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography
[30] http://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
[31] http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

Οι συμμετρικοί αλγόριθμοι που χρησιμοποιούνται συχνότερα σε υλοποιήσεις του OpenPGP είναι:

- ✓ IDEA (International Data Encryption Algorithm)
- ✓ TripleDES[32] ή 3DES (EDE mode) [3]
- ✓ CAST-128[33] (RFC2144)
- ✓ Blowfish[34] (128 bit key, 16 rounds) [4]
- ✓ AES[35, 36] (Advanced Encryption Standard – 128, 192, 256-bit key)
- ✓ Twofish[37] (256-bit key) [5]

3.5 Συναρτήσεις κατακερματισμού

Οι κυριότερες συναρτήσεις κατακερματισμού που έχουν χρησιμοποιηθεί κατά καιρούς στο OpenPGP είναι:

- ✓ MD5 (δεν προτείνεται)
- ✓ SHA-1 (FIPS 180[38]) (προτείνεται)
- ✓ RIPE-MD/160[39]
- ✓ SHA256[40] (384, 512, 224)

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

4. Σύνοψη λειτουργιών του OpenPGP

Το πρότυπο OpenPGP περιγράφει την υλοποίηση έξι λειτουργιών – ενεργειών, που λείπουν από την τρέχουσα αρχιτεκτονική του ηλεκτρονικού ταχυδρομείου (web

[32] http://en.wikipedia.org/wiki/Triple_DES
[33] http://en.wikipedia.org/wiki/CAST-128
[34] http://en.wikipedia.org/wiki/Blowfish_(cipher)
[35] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[36] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[37] http://en.wikipedia.org/wiki/Twofish
[38] http://csrc.nist.gov/publications/PubsFIPS.html
[39] http://en.wikipedia.org/wiki/RIPEMD
[40] http://en.wikipedia.org/wiki/SHA-2

email αλλά και desktop email clients), και οι οποίες είναι εξαιρετικά πολύτιμες σε διάφορες περιστάσεις. Οι ενέργειες αυτές παρουσιάζονται στον παρακάτω πίνακα:

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.	Ψηφιακή υπογραφή του μηνύματος με το ιδιωτικό μου κλειδί.
Θέλω να εξακριβώσω την ταυτότητα του ατόμου που έστειλε ένα ψηφιακά υπογεγραμμένο μήνυμα προκειμένου να δω αν ο υποφαινόμενος αποστολέας είναι ο πραγματικός αποστολέας.	Επιβεβαίωση της ψηφιακής υπογραφής με το δημόσιο κλειδί του αποστολέα.
Θέλω να στείλω ένα μήνυμα το οποίο θα μπορεί να διαβάσει μόνο ο παραλήπτης που επιθυμώ.	Κρυπτογράφηση του μηνύματος αυτού με το δημόσιο κλειδί του επιθυμητού παραλήπτη.
Θέλω να αποκρυπτογραφήσω ένα μήνυμα που έλαβα.	Αποκρυπτογράφηση του μηνύματος με το ιδιωτικό μου κλειδί.
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.	Κρυπτογράφηση του μηνύματος με το δημόσιο κλειδί του παραλήπτη και ψηφιακή υπογραφή του μηνύματος με το ιδιωτικό μου κλειδί.
Θέλω να αποκρυπτογραφήσω ένα μήνυμα το οποίο έχει ψηφιακή υπογραφή και να επιβεβαιώσω την ταυτότητα του αποστολέα του.	Αποκρυπτογράφηση του μηνύματος με το ιδιωτικό μου κλειδί και επαλήθευση της ψηφιακής υπογραφής με το δημόσιο κλειδί του αποστολέα.

5. Τύποι δεδομένων

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)

Εδώ αξίζει να σημειωθεί ότι ένα Keyring είναι μια συλλογή ενός ή περισσοτέρων κλειδιών κρυπτογράφησης που βρίσκονται αποθηκευμένα, είτε σε αρχείο, είτε σε κάποια βάση δεδομένων. Φυσικά, σε ασφαλή θέση και μορφή.

6. Δομή πακέτου

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

6.1 Ετικέτες πακέτων

Οι προκαθορισμένες ετικέτες[41] πακέτων στο OpenPGP (στο δεκαδικό σύστημα αρίθμησης) είναι:

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

[41] Το κείμενο του πίνακα δεν μεταφράζεται σκοπίμως, καθώς πρόκειται για τμήμα του RFC4880.

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

Σε αυτό το σημείο είναι σημαντικό να ορίσουμε σύντομα τη **διαφορά μεταξύ κλειδιών και υποκλειδιών** στο OpenPGP:

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

6.2 Τύποι πακέτων

Όταν ένα πακέτο φέρει μία ετικέτα, τότε λέμε ότι αυτός είναι και ο τύπος του. Δηλαδή, 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.

Είναι χρήσιμο να αναφέρουμε, ότι 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[43]), που θα χρησιμοποιηθούν από το υλοποιημένο OpenPGP.

[42] Χρησιμοποιείται μόνο μέσα σε Keyrings
[43] http://en.wikipedia.org/wiki/Key_server_(cryptographic)

7. Ενισχυμένα κλειδιά

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.

7.1 Αποτύπωμα και αναγνωριστικό κλειδιού

Το αποτύπωμα (fingerprint[44]) του κάθε κλειδιού V4, προκύπτει με 160-bit SHA-1 hashing του πακέτου. Και το αναγνωριστικό (Key ID) προκύπτει από τα 60 χαμηλότερης τάξης bits του αποτυπώματος αυτού.

[44] http://en.wikipedia.org/wiki/Public_key_fingerprint

8. Μετατροπέας Radix-64

Όπως αναφέρθηκε, 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. Το σύστημα κωδικοποίησης Radix-64 του Open PGP παρέχει ακριβώς αυτή τη δυνατότητα.

Αποτελείται από δύο μέρη. Την κωδικοποίηση δυαδικών δεδομένων base64 (πανομοιότυπη με την κωδικοποίηση μεταφοράς περιεχομένου, MIME base64) και ένα checksum (CRC-24).

9. ASCII armor

Το σύστημα ASCII armor είναι ένας μετατροπέας δυαδικής κωδικοποίησης, σε γραμματική. Είναι χρήσιμο, καθώς το OpenPGP είναι πρότυπο που κυρίως υλοποιείται για την ασφαλή αποστολή και λήψη email. Επομένως σε κάποιο στάδιο θα πρέπει να προκύπτει κείμενο (plaintext) που θα είναι αναγνώσιμο από ανθρώπους.

Το OpenPGP ενημερώνει τον χρήστη για το είδος των δεδομένων που κωδικοποιούνται σε ASCII armor μέσω της χρήσης ειδικών κατατοπιστικών κεφαλίδων. 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.

Ένα παράδειγμα μηνύματος που έχει δημιουργηθεί με το σύστημα ASCII armor του OpenPGP είναι και το παρακάτω:


```
-----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[45]) 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[46])

10. Ζητήματα κατά την υλοποίηση του OpenPGP

Το πρότυπο OpenPGP είναι ένα τεχνικό έγγραφο που απλά περιλαμβάνει περιγραφές για τις τεχνικές λεπτομέρειες και τις μεθόδους που πρέπει να εφαρμοστούν προκειμένου μια εφαρμογή PGP να επικοινωνεί με ασφάλεια και αξιοπιστία.

Επομένως η μετατροπή του OpenPGP σε πραγματική εφαρμογή, θα πρέπει να γίνει από κάποιο προγραμματιστή (ή ομάδα προγραμματιστών), σε κάποια γλώσσα προγραμματισμού και με τη χρήση όποιων επιπλέον τεχνολογιών λογισμικού κριθούν απαραίτητες.

Κατά τη διαδικασία της ανάπτυξης μιας τέτοιας εφαρμογής, θα πρέπει στον κώδικα που αναπτύσσεται να εντάσσονται παράλληλα δικλείδες ασφαλείας, απαραίτητες για την ασφαλή επικοινωνία. Για να μπορεί να γίνει κάτι τέτοιο, ο προγραμματιστής θα πρέπει να είναι ενήμερος για όλες τις παραμέτρους ασφαλείας του OpenPGP, αλλά και για όλες τις επιθέσεις που μπορεί να δεχτεί.

[45] http://simple.wikipedia.org/wiki/Cleartext
[46] https://tools.ietf.org/html/rfc3156

10.1 Παράμετροι ασφαλείας και επιθέσεις που πρέπει να ληφθούν υπόψιν

Μερικά από τα σημαντικότερα θέματα ασφαλείας που θα πρέπει να ληφθούν υπόψιν κατά την υλοποίηση του OpenPGP, είναι τα εξής:

- ✓ 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 ασφαλίζεται 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[47].
- ✓ 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.

Φυσικά η λίστα δεν εξαντλείται εδώ. Στο αντίστοιχο RFC (σελίδα 81, παράγραφος 14, Security Considerations) που περιγράφει το OpenPGP γίνεται λεπτομερής αναφορά σε όλες τις πτυχές ασφαλείας που θα πρέπει να εξεταστούν.

11. Νομοθεσία

Το OpenPGP χρησιμοποιεί ορισμένους από τους ισχυρότερους κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού που είναι διαθέσιμοι στους κρυπτογράφους όλου του κόσμου.

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

[47] https://tools.ietf.org/html/rfc4086

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
```

12. Η εφαρμογή GnuPG ή GPG

Η εφαρμογή GnuPG, όπως αναφέρθηκε και στην αρχή, αποτελεί μια δωρεάν υλοποίηση του προτύπου OpenPGP.

Επίσης ο πηγαίος κώδικας είναι ανοικτός και ελεύθερος. Αυτό σημαίνει ότι ο καθένας μπορεί να τον κατεβάσει[48, 49, 50], να κάνει τις δικές του τροποποιήσεις και τις δικές του διανομές (σύμφωνα με τους όρους της άδειας χρήσης GNU General Public License[51]).

12.1 Τα χαρακτηριστικά της εφαρμογής

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).

[48] https://www.gnupg.org/download/index.html
[49] https://www.gnupg.org/download/cvs_access.html
[50] http://git.gnupg.org
[51] http://www.gnu.org/copyleft/gpl.html

Μερικά από τα βασικότερα χαρακτηριστικά της, είναι:

- ✓ 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 Keyservers

Επίσης:

- ✓ Διαθέτει τεχνική υποστήριξη[52, 53]
- ✓ Περιλαμβάνει εκτενή τεχνική τεκμηρίωση[54]
- ✓ Αποτελεί τη βάση (backend - API) για βοηθητικά λογισμικά[55]

13. Εγκατάσταση GnuPG στα Windows

Οι παραθυρικές εφαρμογές είναι φιλικότερες προς τον χρήστη και τον βοηθούν να καταλάβει σχεδόν άμεσα και χωρίς εγχειρίδιο, τη λειτουργία και τη χρήση τους. Επομένως, είναι χρήσιμο να εξασκηθούμε σε ένα απλό σενάριο χρήσης στα Windows.

Μέσα από αυτή τη διαδικασία θα γίνουν ευκολότερα αντιληπτές και οι έννοιες που αναφέρθηκαν κατά την ανάλυση του προτύπου OpenPGP. Θα δημιουργηθεί μια πιο πλήρης εικόνα για την πρακτική χρησιμότητα της κρυπτογραφημένης επικοινωνίας.

[52] https://www.gnupg.org/service.html
[53] https://www.gnupg.org/people/index.html
[54] https://www.gnupg.org/documentation/index.html
[55] https://www.gnupg.org/related_software/index.html

13.1 Εγκατάσταση GnuPG μέσω της εφαρμογής Gpg4win

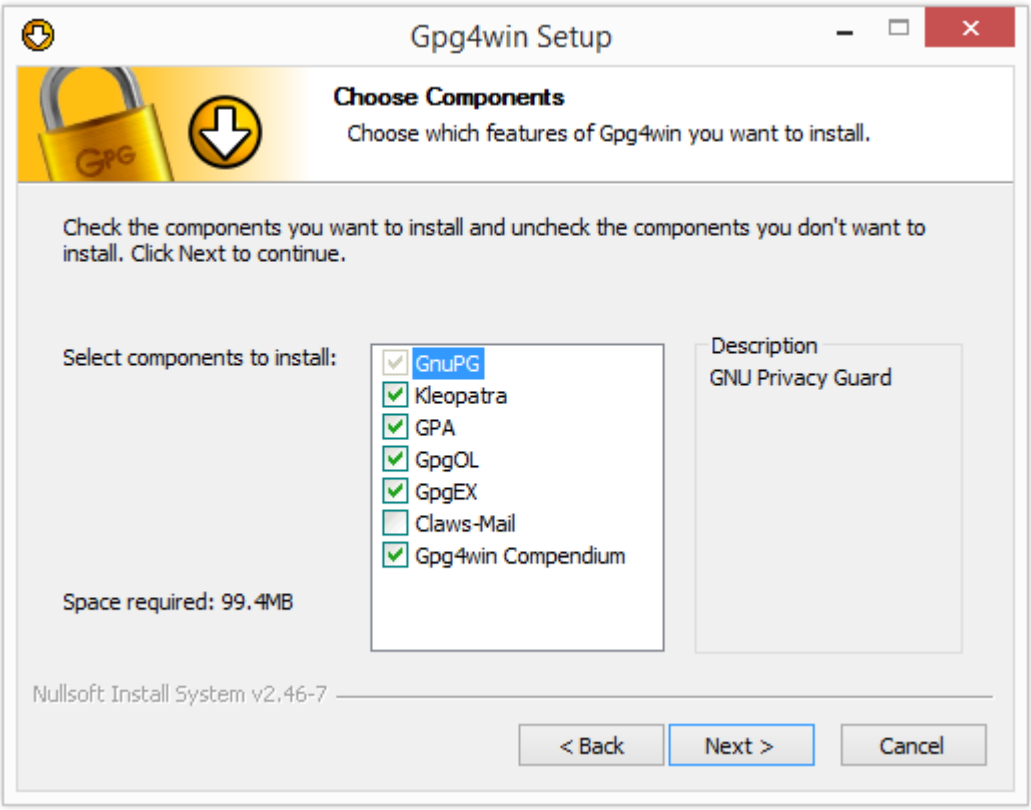
Η υλοποίηση GnuPG για το λειτουργικό σύστημα των Windows ονομάζεται Gpg4win[56] (GnuPG for Windows):

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

- ✓ **GnuPG** (2.0.27) – Η GNU υλοποίηση του OpenPGP
- ✓ **Kleopatra**[57] (2.2.0-git945878c) – Διαχειρίζεται κλειδιά OpenPGP και X.509
- ✓ **GPA**[58] (0.9.7) – GNU Privacy Assistant
- ✓ **GpgOL**[59] (1.2.1) – GnuPG για το Outlook
- ✓ **GpgEX**[60] (1.0.1) – Επέκταση του GnuPG για το Shell των Windows
- ✓ **Claws Mail**[61] (3.9.1) – Email client (δεν προτείνεται)
- ✓ **Kompendium**[62] (3.0.0) – Τεκμηρίωση (σε μορφή PDF)

Κατά την παρούσα εγκατάσταση επιλέχθηκαν τα εξής:

[56] http://gpg4win.org/download.html
[57] https://www.kde.org/applications/utilities/kleopatra
[58] https://www.gnupg.org/related_software/gpa/index.html
[59] http://git.gnupg.org/cgi-bin/gitweb.cgi?p=gpgol.git
[60] http://git.gnupg.org/cgi-bin/gitweb.cgi?p=gpgex.git
[61] http://www.claws-mail.org
[62] http://gpg4win.org/doc/en/gpg4win-compendium.html



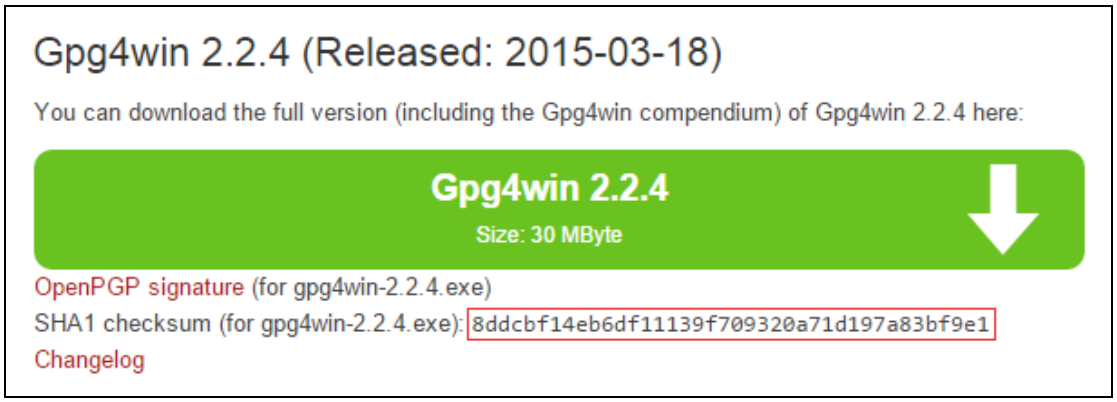
Η υπόλοιπη εγκατάσταση έγινε με τις προεπιλεγμένες ρυθμίσεις του εγκαταστάτη. Προηγήθηκε η επαλήθευση της ακεραιότητάς του.

13.1.1 Επαλήθευση ακεραιότητας του αρχείου `gpg4win-2.2.4.exe`

Εφόσον το κίνητρο χρήσης της εφαρμογής Gpg4win είναι η ασφάλεια της επικοινωνίας, αυτή θα πρέπει να ισχύει σε κάθε επίπεδο. Αν το εκτελέσιμο αρχείο που λάβαμε από τον server της εφαρμογής αυτής έχει παραποιηθεί από hackers, τότε θα λειτουργεί κατασκοπικά ή σαν ένας «δούρειος ίππος» προς όφελός τους φυσικά.

Ένα παράδειγμα κακόβουλης τροποποίησης θα μπορούσε να είναι η εν αγνοία μας αποστολή, σε κάποιο τρίτο μη-εξουσιοδοτημένο πρόσωπο, ενός μη-κρυπτογραφημένου αντίγραφου από κάθε email που θέλουμε να στείλουμε εμπιστευτικά. Ενώ εμείς θα αισθανόμαστε ασφαλείς, κάθε φορά που θα χρησιμοποιούμε την εφαρμογή Gpg4win, κάποιος άλλος θα έχει επίσης πρόσβαση στην επικοινωνία μας, και ίσως ακόμα και στο υπολογιστικό μας σύστημα.

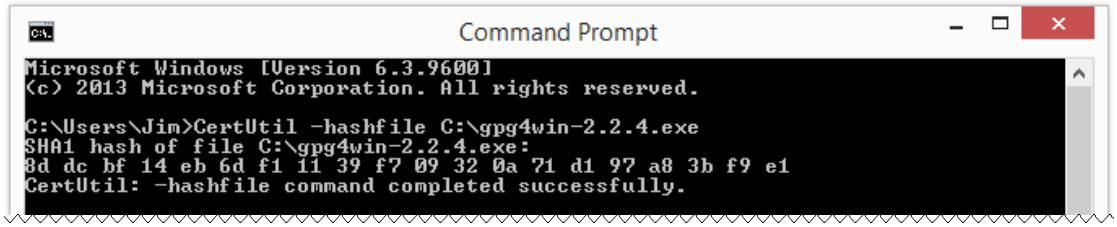
Για να αποφευχθεί κάτι τέτοιο, μετά τη λήψη, απαιτείται ο έλεγχος ακεραιότητας (integrity check[63]) του εκτελέσιμου αρχείου εγκατάστασης (gpg4win-2.2.4.exe). Αυτό μπορεί να γίνει με τον έλεγχο του αριθμού checksum[64][65] του εν λόγω αρχείου ο οποίος απεικονίζεται και παρακάτω (κόκκινο πλαίσιο):



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:

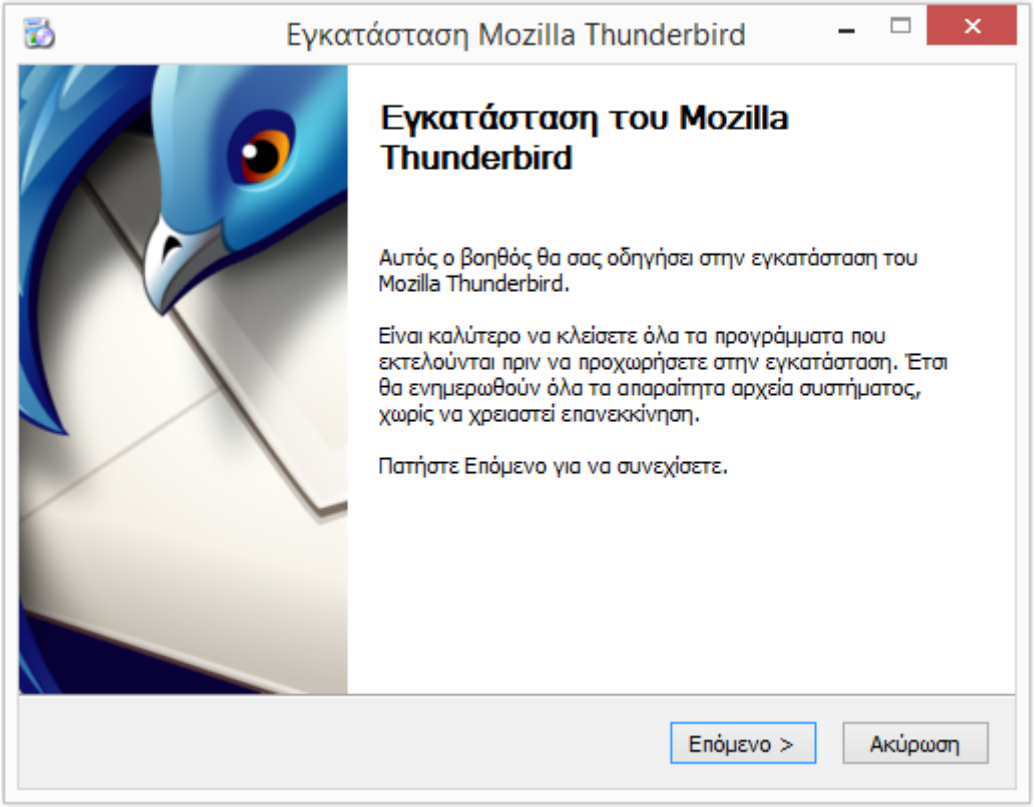


14. Εγκατάσταση του Mozilla Thunderbird

Για να είμαστε σε θέση να στείλουμε ένα κρυπτογραφημένο email μέσω της εφαρμογής GnuPG, θα πρέπει πρώτα να εγκαταστήσουμε κάποιον email client. Ο Mozilla Thunderbird[66] είναι μία δωρεάν και γενικότερα, πολύ δημοφιλής λύση.

[63] https://www.gnupg.org/download/integrity_check.html
[64] https://en.wikipedia.org/wiki/Checksum
[65] Checksum: 8ddcbf14eb6df11139f709320a71d197a83bf9e1
[66] https://www.mozilla.org/el/thunderbird

Η ελληνική έκδοση είναι προτιμότερη καθώς εξασφαλίζει ότι δεν θα υπάρχουν προβλήματα κωδικοποίησης κειμένου:



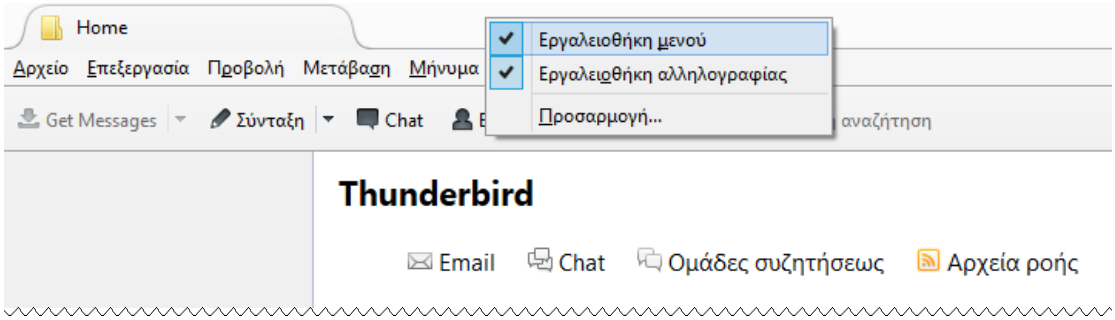
Η εγκατάσταση είναι απλή και μπορεί να γίνει με τις προεπιλεγμένες ρυθμίσεις του εγκαταστάτη.

14.1 Εγκατάσταση του προσθέτου Enigmail στον Mozilla Thunderbird

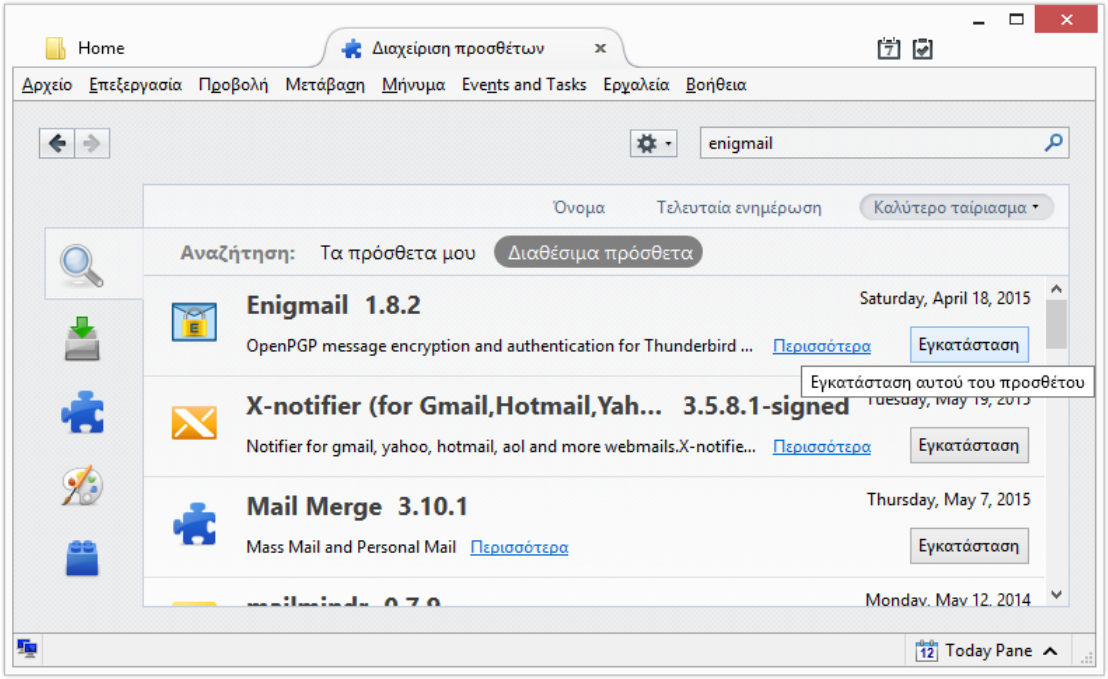
Ο Thunderbird email client για να είναι δυνατόν να συνεργάζεται με την εφαρμογή Gpg4win, ώστε να μπορούν να αποστέλλονται και να λαμβάνονται μηνύματα τα οποία ο χρήστης θα είναι σε θέση να κρυπτογραφεί και αποκρυπτογραφεί, προαπαιτεί την ύπαρξη του προσθέτου Enigmail[67].

Αρχικά θα πρέπει να εμφανίσουμε (αν δεν εμφανίζεται ήδη) την εργαλειοθήκη μενού με δεξί κλικ στο ανώτερο τμήμα του παραθύρου και στη συνέχεια επιλέγοντάς την:

[67] https://www.enigmail.net

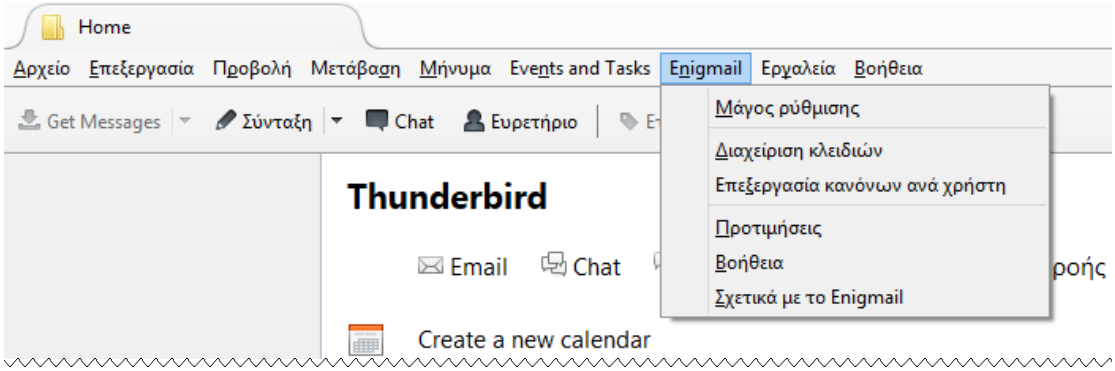


Στη συνέχεια επιλέγοντας από το κυρίως μενού `Εργαλεία > Πρόσθετα` και εισάγοντας ως κριτήριο αναζήτησης τη λέξη `enigmail`, εντοπίζουμε το πρόσθετο και το εγκαθιστούμε:



Αμέσως μετά θα πρέπει να γίνει επανεκκίνηση του Thunderbird προκειμένου να ολοκληρωθεί η εγκατάσταση του προσθέτου.

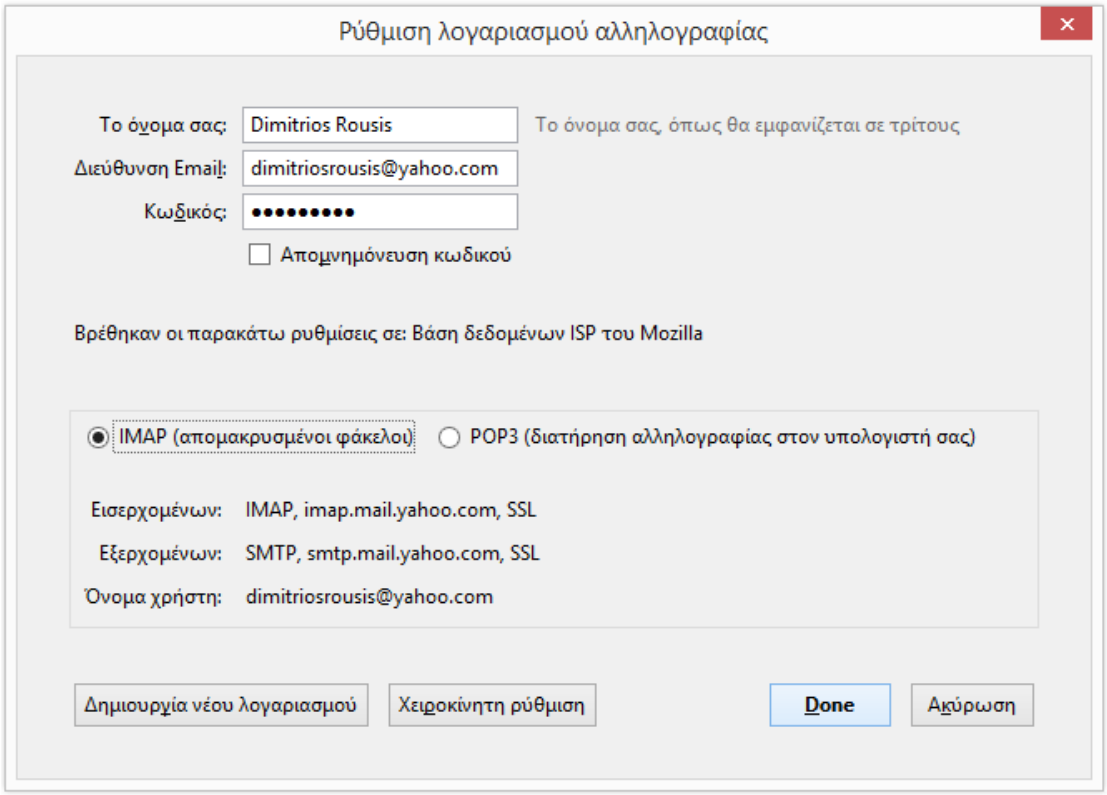
Αν όλα έχουν ολοκληρωθεί επιτυχώς, θα πρέπει να έχει εμφανιστεί ένα νέο μενού με το όνομα Enigmail:



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

14.2 Δημιουργία νέου λογαριασμού email στον Mozilla Thunderbird

Επιλέγουμε `Αρχείο > Νέο > Δημιουργία νέου λογαριασμού αλληλογραφίας` για να εισάγουμε τη διεύθυνση email που ήδη διαθέτουμε:

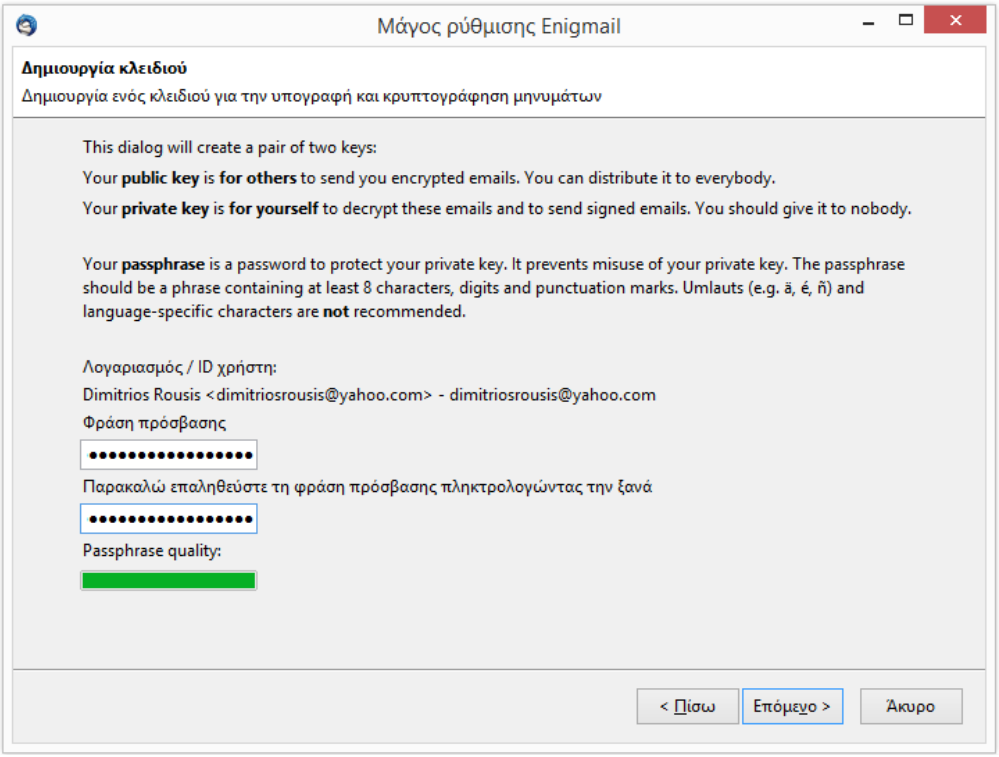


14.3 Ρύθμιση του Enigmail

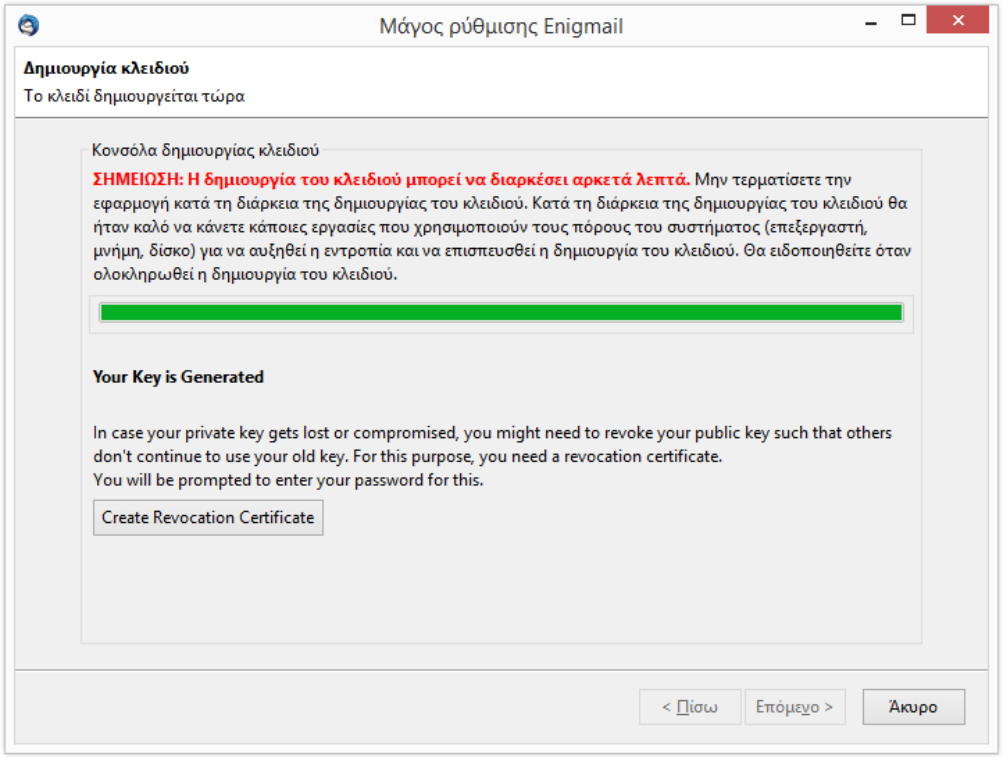
Επιλέγουμε `Enigmail > Μάγος ρύθμισης` (Setup wizard) και στα επόμενα παράθυρα διαλόγου που θα προκύψουν επιλέγουμε με τη σειρά:

1) `I prefer an extended configuration (recommended for beginners advanced users)`. Οι ρυθμίσεις για experts μπορούν να γίνουν και εκ των υστέρων.

2) `Θέλω να δημιουργήσω ένα νέο ζεύγος κλειδιών για την υπογραφή και κρυπτογράφηση της αλληλογραφίας μου:`



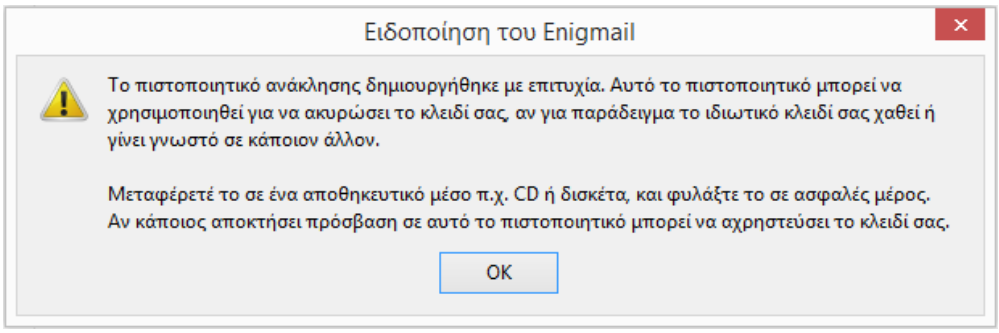
3) Αφού έχουμε επιλέξει `Επόμενο` στο προηγούμενο παράθυρο:



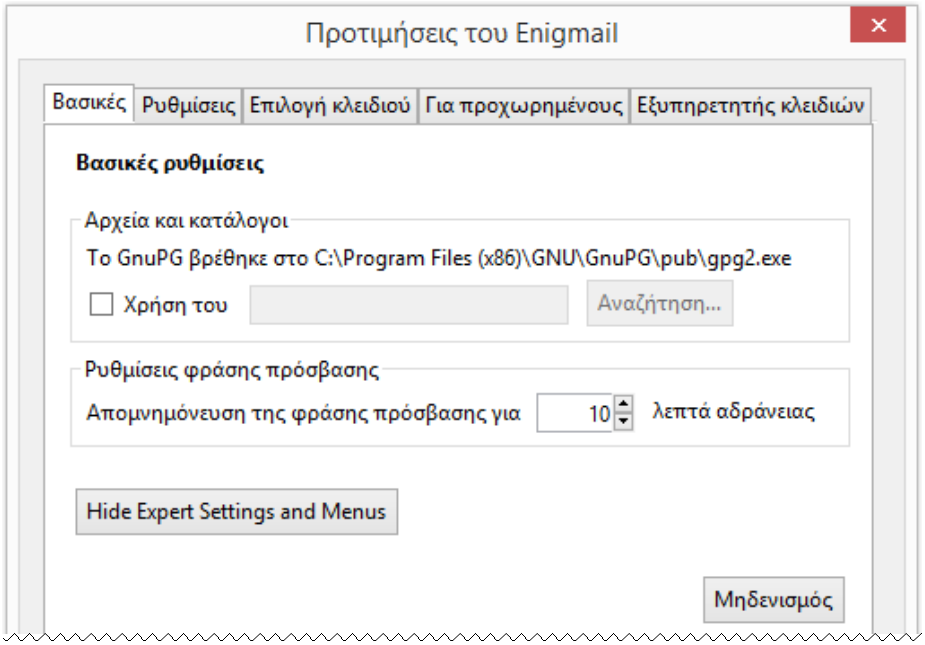
4) `Create Revocation Certificate` (δημιουργία πιστοποιητικού ανάκλησης)

5) Αποθήκευση πιστοποιητικού ανάκλησης σε ασφαλές σημείο (σε μορφή .asc). Ζητείται επίσης η passphrase που δώσαμε νωρίτερα.

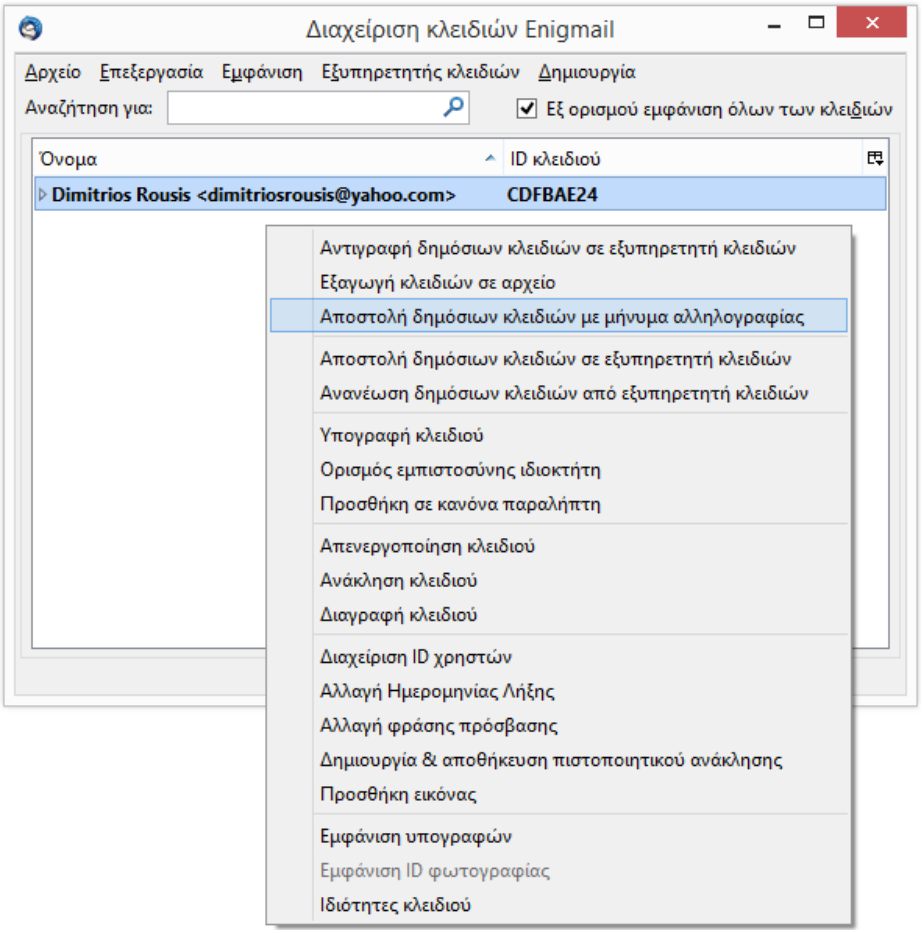
6) Αφού έχουμε ολοκληρώσει την αποθήκευση του πιστοποιητικού:



Σε αυτό το σημείο η τυπική παραμετροποίηση του προσθέτου Enigmail έχει ολοκληρωθεί και μπορεί να πραγματοποιηθεί η παραμετροποίηση για experts, είτε και πάλι μέσω του wizard, είτε επιλέγοντας `Enigmail > Προτιμήσεις`:



Για να δούμε το κλειδί που δημιουργήθηκε επιλέγουμε `Enigmail > Διαχείριση κλειδιών`:



Στην εικόνα φαίνονται και οι επιλογές που υπάρχουν αν γίνει δεξί κλικ επάνω στο κλειδί.

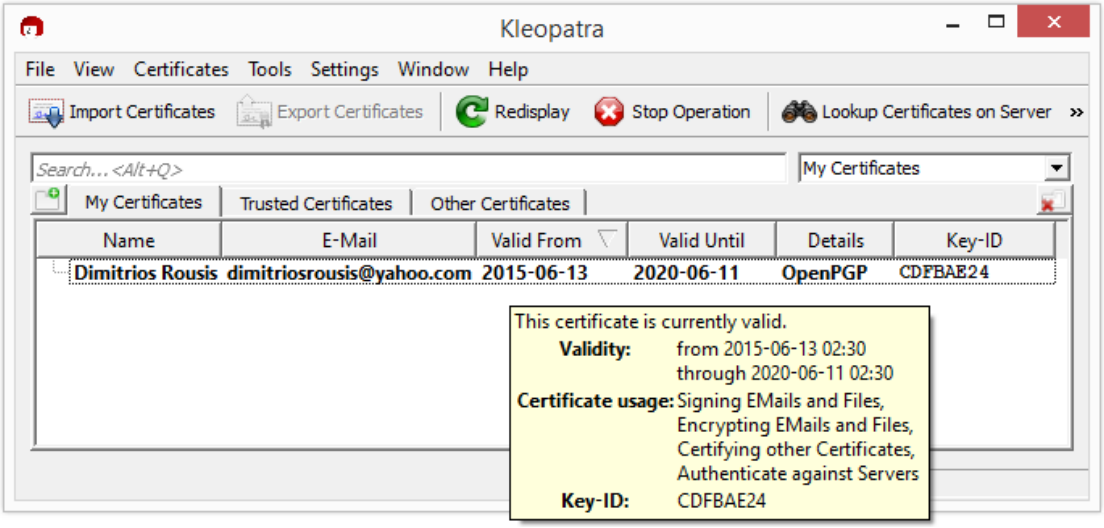
Σε αυτό το σημείο έχουμε δημιουργήσει ένα πλήρες περιβάλλον μέσω του οποίου μπορούμε να επικοινωνούμε με ασφάλεια αλλά και να πραγματοποιούμε μια σειρά άλλων ενεργειών, όπως είναι για παράδειγμα η κρυπτογράφηση αρχείων.

15. Σενάριο χρήσης

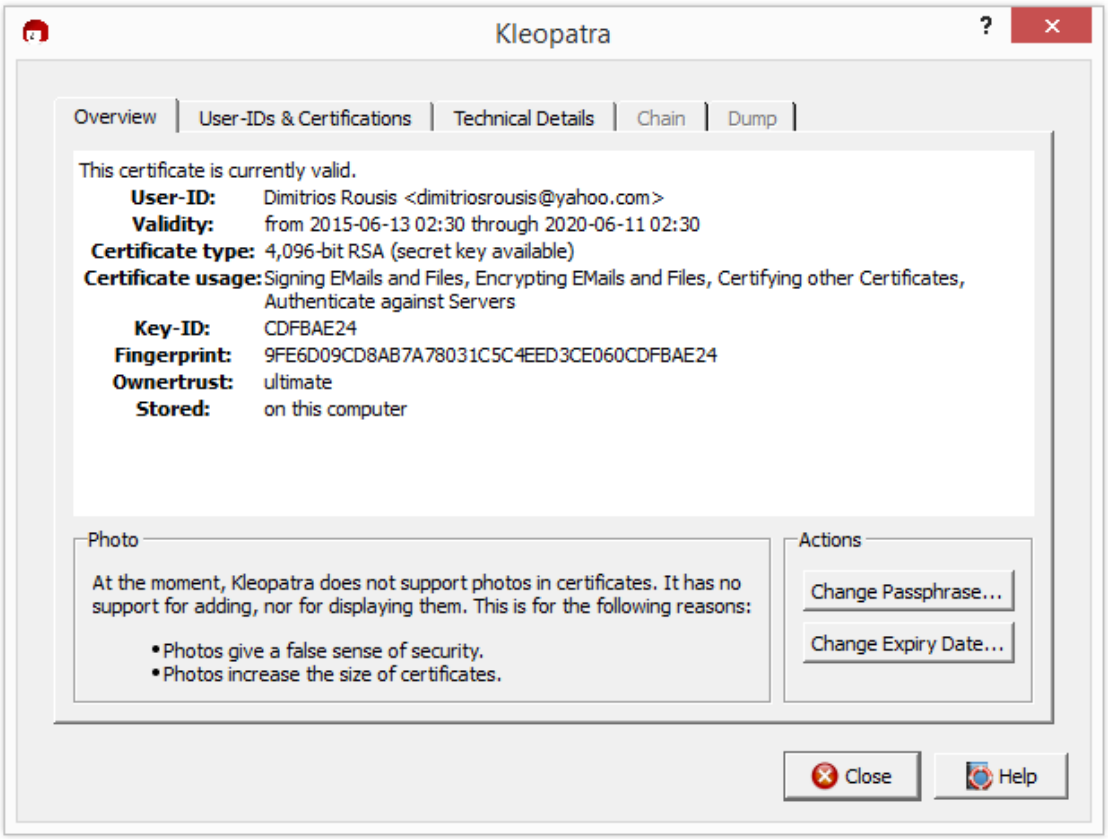
Ο φοιτητής Δημήτρης (αποστολέας), θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον καθηγητή του (παραλήπτης) μέσω ηλεκτρονικής αλληλογραφίας. Στο μήνυμα αυτό θα περιλαμβάνεται ως επισυναπτόμενο αρχείο, το δημόσιό του κλειδί (`0xCDFBAE24.asc`), και ως κρυπτογραφημένο κείμενο μηνύματος, ορισμένες συνοδευτικές πληροφορίες.

15.1 Αποστολή κρυπτογραφημένου email και επισυναπτόμενου αρχείου

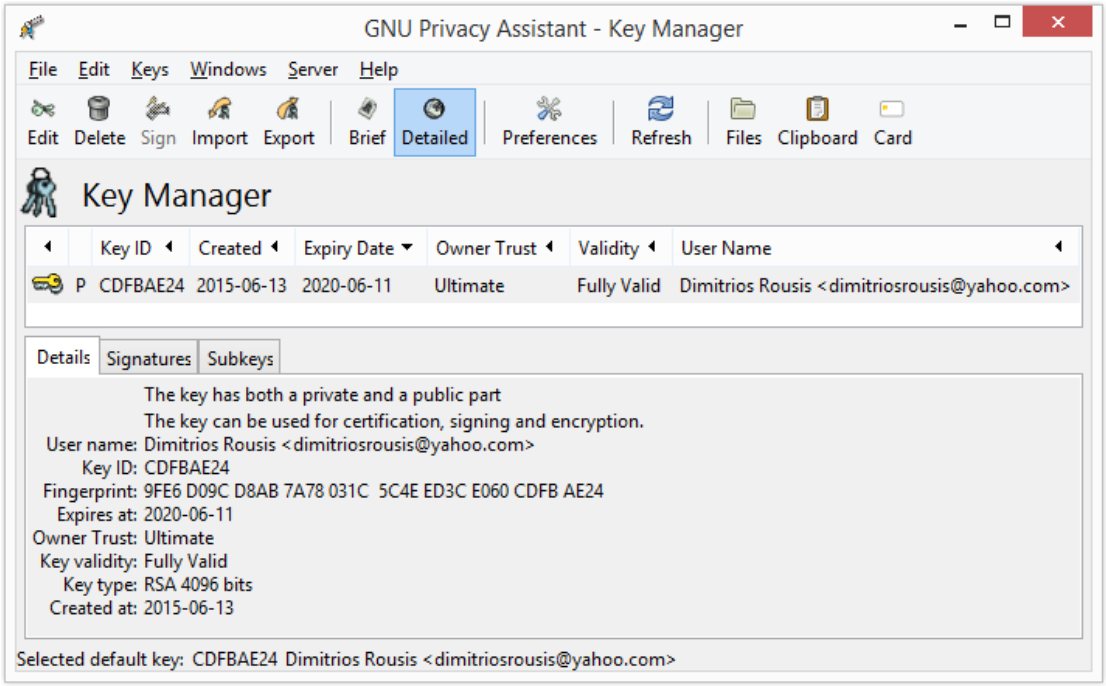
Σε προηγούμενη παράγραφο, κατά την εγκατάσταση του προσθέτου Enigmail δημιουργήθηκε ένα πιστοποιητικό ανάκλησης αλλά και το δημόσιο και ιδιωτικό κλειδί του αποστολέα. Αυτό μπορεί να επιβεβαιωθεί με τη χρήση της εφαρμογής Kleopatra:



Κάνοντας δεξί κλικ στο πιστοποιητικό και επιλέγοντας `Certificate details`:



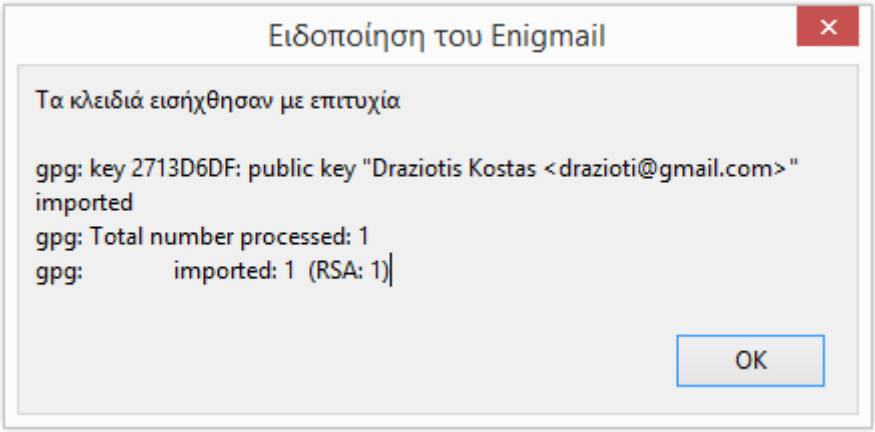
Αλλά, και μέσω της εφαρμογής GPA, αντίστοιχα:



Για να είναι εφικτή η επικοινωνία ανάμεσα σε αποστολέα και παραλήπτη, θα πρέπει αρχικά να είναι γνωστό το email του δεύτερου από τον πρώτο. Για να είναι και ασφαλής, το ίδιο θα πρέπει να ισχύει και για το δημόσιο κλειδί[68]:

Παραλήπτης
Email = `drazioti@gmail.com`
Δημόσιο κλειδί = `http://users.auth.gr/drazioti/pgp.htm`

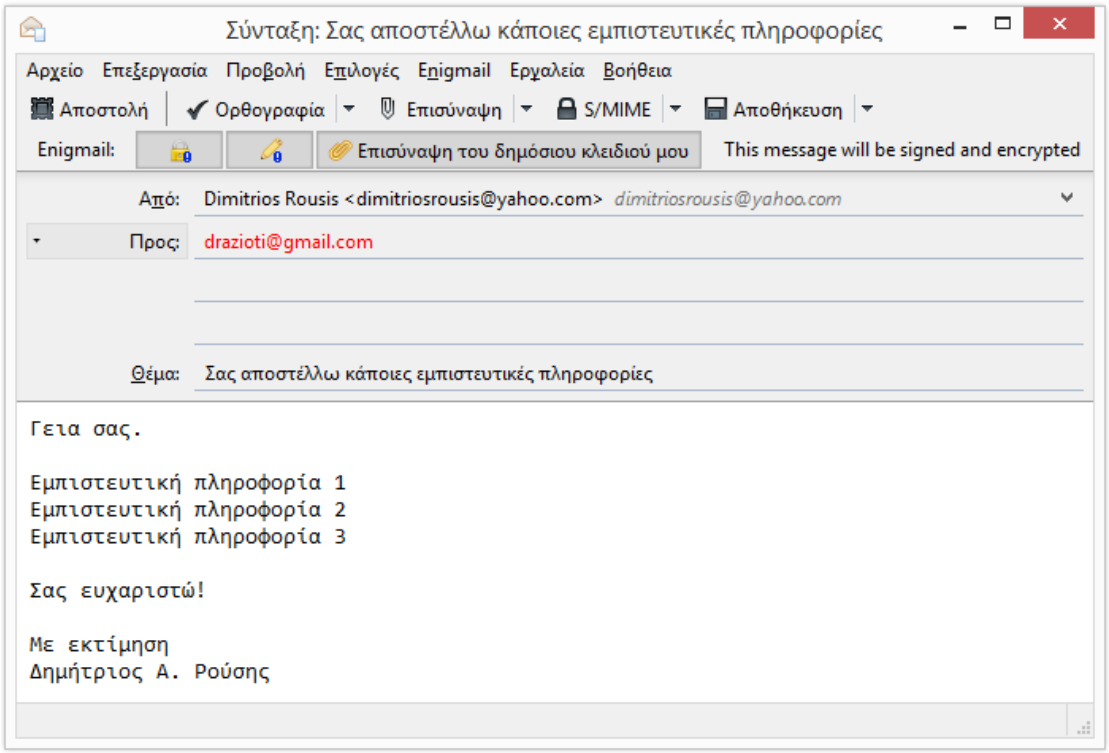
Αφού ο αποστολέας γνωρίζει το δημόσιο κλειδί του παραλήπτη, μπορεί να το εισάγει επιλέγοντας `Enigmail > Διαχείριση κλειδιών` και `Αρχείο > Εισαγωγή κλειδιών από αρχείο`, επιλέγοντας το αρχείο `.asc` που το περιλαμβάνει:



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.

[68] Παρατίθεται σε αντίστοιχο παράρτημα

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/WBB8CAcVn3Ne8EfkWeyw7nVilt7
JzN0jASQ5AW/0In/9hr+KZVln6r5D4xr3TtcURMhy4Lv0cXmDNewMtKjWqfOCy3H
. . . . .
1rfjZI1h6Hp4j7ECKNcFjXECLThqNbiRIClFCQ9bA4mAU63wl9mD+qjedMOG+HAL
UoqLNV/ICJ4wDux9oTFw4fOTenjcZrhEQ9rYmy+/R3LtJfm7DucLdEvldxfDipEW
PA==
=rP+n
-----END PGP MESSAGE-----

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

16. Παραρτήματα

16.1 Διαφορές OpenPGP από S/MIME X.509

Οι κυριότερες διαφορές μεταξύ των OpenPGP και X.509 PKIs[69] μπορούν να χωριστούν σε τρεις κατηγορίες [6]:

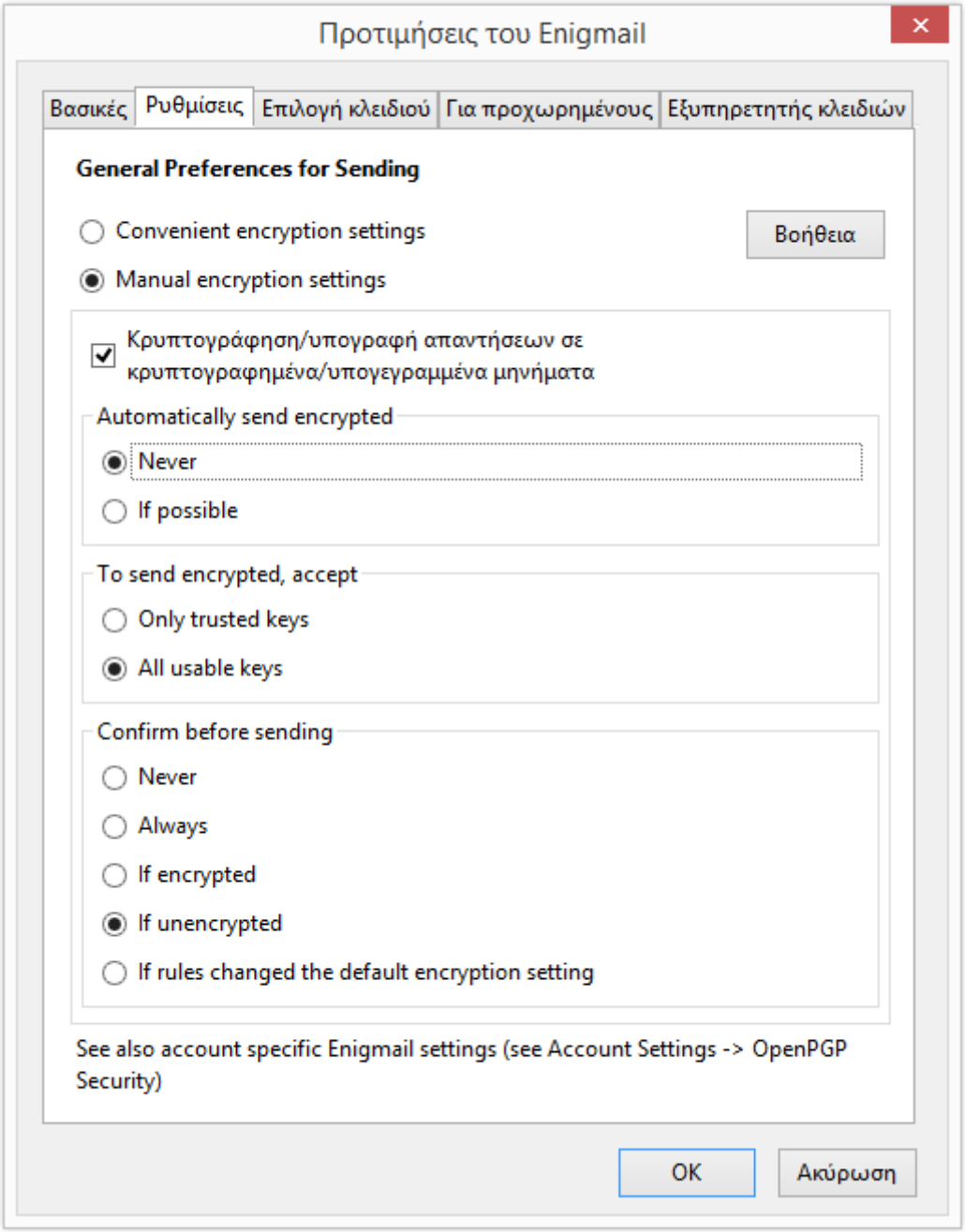
- **Διαφορές στο πιστοποιητικό** – Κάθε πιστοποιητικό OpenPGP περιέχει μια αυτοϋπογραφή και μπορεί να περιέχει πολλές υπογραφές, ενώ τα πιστοποιητικά X.509 υποστηρίζουν μόνο μία ψηφιακή υπογραφή για να πιστοποιούν την εγκυρότητα του κλειδιού. Τα πιστοποιητικά X.509 υποστηρίζουν εγγενώς μόνο ένα όνομα για τον ιδιοκτήτη του κλειδιού. Τα πιστοποιητικά OpenPGP έχουν δημόσιο κλειδί με διάφορες ετικέτες που προσδιορίζουν τον χρήστη με διαφορετικούς τρόπους.

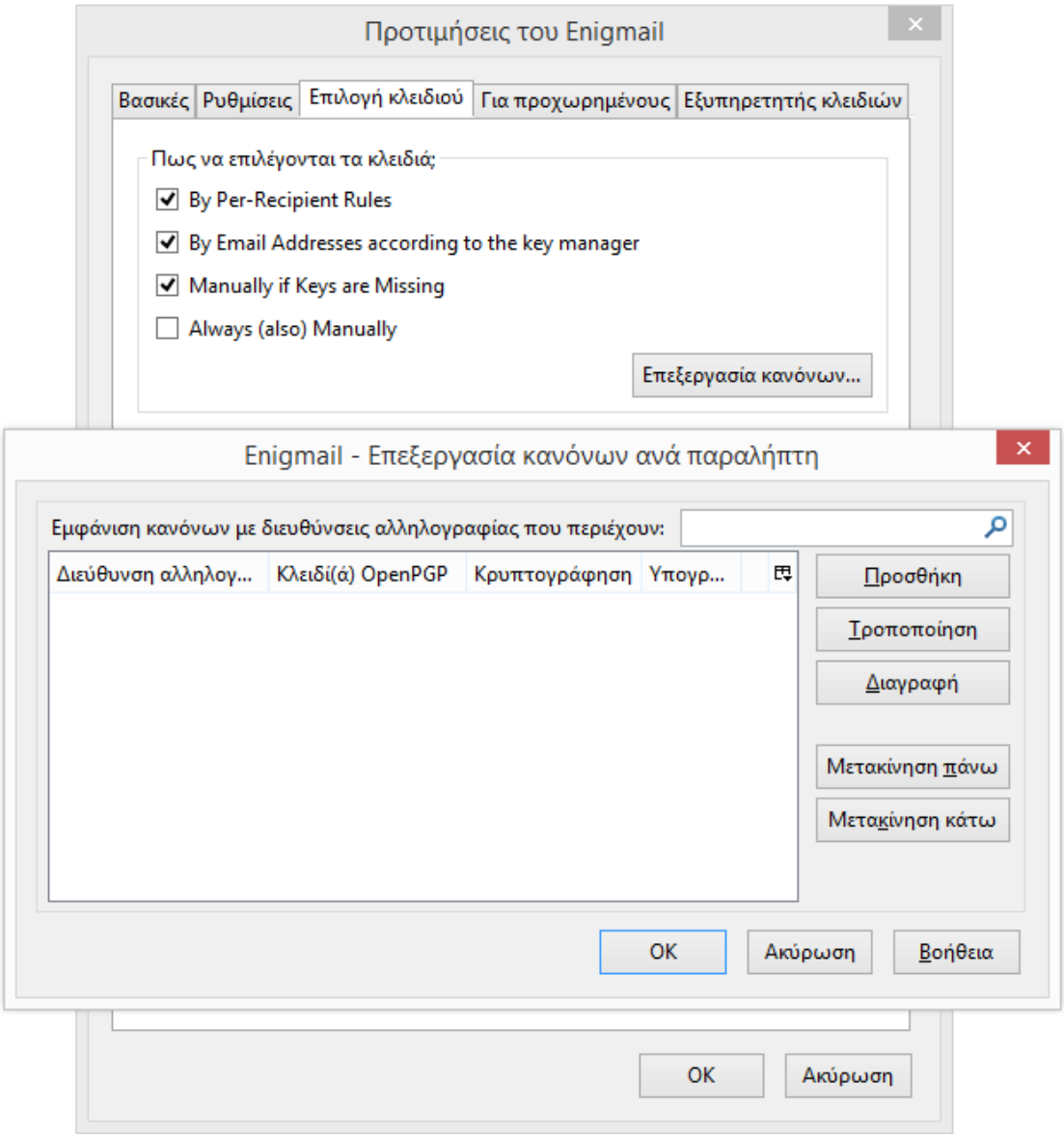
- **Διαφορές στο δίκτυο εμπιστοσύνης** (Network of Trust) – Ο χρήστης μπορεί να δημιουργήσει το δικό του πιστοποιητικό OpenPGP, αλλά στην περίπτωση του X.509 θα πρέπει να ζητήσει να εκδοθεί από μια Αρχή Πιστοποίησης. Με τα πιστοποιητικά X.509, μεσολαβεί πάντα μια Αρχή Πιστοποίησης. Επίσης το OpenPGP 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[70]), έτσι ώστε κάθε χρήστης να μπορεί να ενεργεί ως αρχή πιστοποίησης.

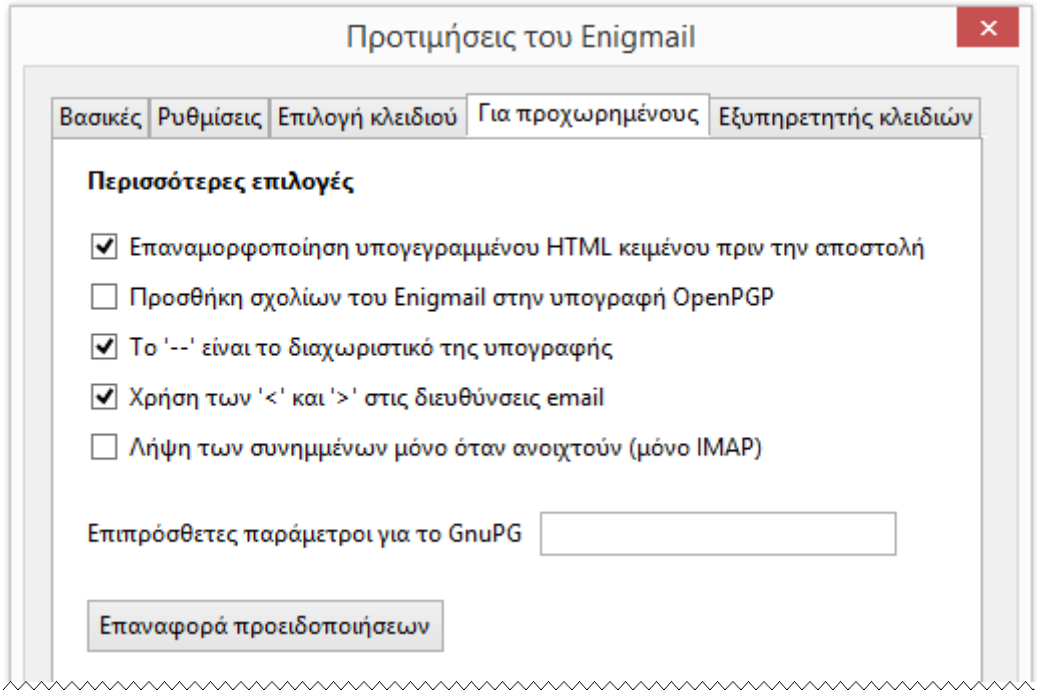
- **Διαφορές στη διαδικασία ανάκλησης** (revocation procedure) – Με τα πιστοποιητικά X.509, μια ανακληθείσα υπογραφή είναι σχεδόν το ίδιο με ένα πιστοποιητικό που έχει ανακληθεί, δεδομένου ότι η μόνη υπογραφή του πιστοποιητικού είναι αυτή που την έκανε έγκυρη εξ' αρχής. Δηλαδή η υπογραφή της Αρχής Πιστοποίησης. 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.

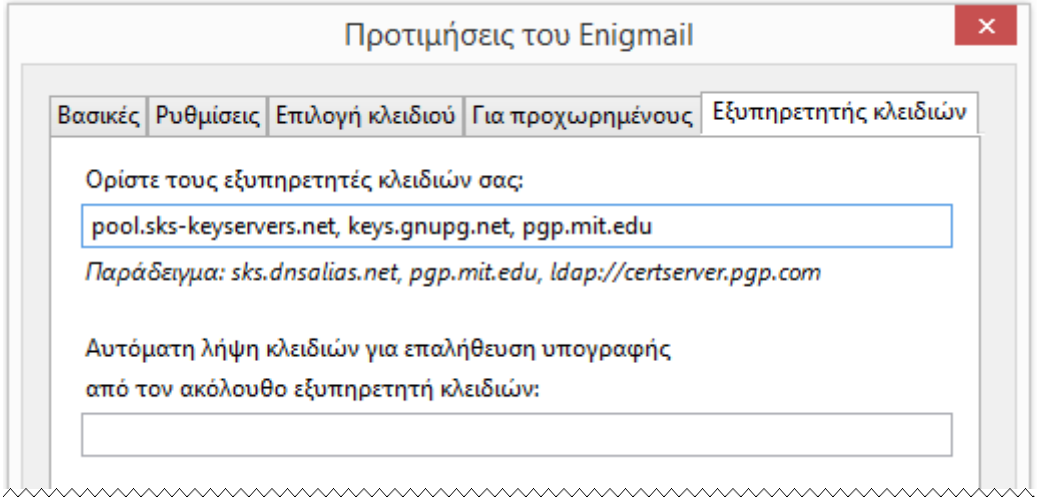
[69] https://en.wikipedia.org/wiki/Public_key_infrastructure
[70] https://en.wikipedia.org/wiki/Web_of_trust

16.2 Προτιμήσεις - ρυθμίσεις του Enigmail




Προτιμήσεις του Enigmail
Βασικές
Ρυθμίσεις
Επιλογή κλειδιού
Για προχωρημένους
Εξυπηρετητής κλειδιών
Πως να επιλέγονται τα κλειδιά;
By Per-Recipient Rules
By Email Addresses according to the key manager
Manually if Keys are Missing
Always (also) Manually
Επεξεργασία κανόνων...
Enigmail - Επεξεργασία κανόνων ανά παραλήπτη
Εμφάνιση κανόνων με διευθύνσεις αλληλογραφίας που περιέχουν:
Διεύθυνση αλληλογ...
Κλειδί(ά) OpenPGP
Κρυπτογράφηση
Υπογρ...
Προσθήκη
Τροποποίηση
Διαγραφή
Μετακίνηση πάνω
Μετακίνηση κάτω
OK
Ακύρωση
Βοήθεια
OK
Ακύρωση


Προτιμήσεις του Enigmail
Βασικές
Ρυθμίσεις
Επιλογή κλειδιού
Για προχωρημένους
Εξυπηρετητής κλειδιών
Περισσότερες επιλογές
Επαναμορφοποίηση υπογεγραμμένου HTML κειμένου πριν την αποστολή
Προσθήκη σχολίων του Enigmail στην υπογραφή OpenPGP
Το '--' είναι το διαχωριστικό της υπογραφής
Χρήση των '<' και '>' στις διευθύνσεις email
Λήψη των συνημμένων μόνο όταν ανοιχτούν (μόνο IMAP)
Επιπρόσθετες παράμετροι για το GnuPG
Επαναφορά προειδοποιήσεων


Προτιμήσεις του Enigmail
Βασικές
Ρυθμίσεις
Επιλογή κλειδιού
Για προχωρημένους
Εξυπηρετητής κλειδιών
Ορίστε τους εξυπηρετητές κλειδιών σας:
pool.sks-keyservers.net, keys.gnupg.net, pgp.mit.edu
Παράδειγμα: sks.dnsalias.net, pgp.mit.edu, ldap://certserver.pgp.com
Αυτόματη λήψη κλειδιών για επαλήθευση υπογραφής
από τον ακόλουθο εξυπηρετητή κλειδιών:

16.3 Δημόσια κλειδιά

16.3.1 Δημόσιο κλειδί παραλήπτη

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.17 (MingW32)

mQENBE3r5lQBCADzg7s867Wtq7GVkR2VYhwJcLsx9tTikdD3xtk7cmDCmCwmYlNs
eEw4vaEsNE4ZE2FkjVEUZk4tpnO4/T7AJ1UC9/0R1XNZmbA1twifrOsfR9w9kB0+
jJFp4jaumjuuJUTy5ttlF9ZlnXMRf2Eg4SJZifd9nFWxxyxlwW65CHoImlTEKUT3
Jz80zDmtzIwV/gNUcdIOkY7Rab2QROM3Fm2llVA9fLzh5YcHXEvn3I70aesntE45
tdznimwH4V176kqI40BqVnxhh4ySX7GK9pEFz1Ier3IaOEoaM/Fd54121RuCMC1s
gEFfQXxCw4WDpx1MkCkpkkgZeiZKaWhQ7kK7ABEBAAG0JERyYXppb3RpcyBLLiA8
ZHJhemlvdGlAbWF0aC5hdXRoLmdyPokBOAQTAQIAIgUCTevmVAIbDwYLCQgHAwIG
FQgCCQoLBBYCAwECHgECF4AACgkQ6xGF+CcT1t/awwf/a7V9XujS5KQ0Z5rAAe0t
SAs403f7ET0moNcWMP+JGztXrE1bYWVysMsrFbsfkoJr9KTR18izFtLlEMxTBndC
wfk2JOC7yIitK692CO2VZ705/uYAy1e0FeS91eaTrU1HzRjtL6mHwy+TSfyhJWYB
mE1y5WwkS53cezmamj1dynisrj5JEC4kiWeXfyHZBr5PsC88n1DcfTKpy6YRIFh7
TpQUUR8kyYa0wcOIVqNuIVOhcZmAgOPN2Y3XjyHqHFXCJewEVhhJU1463i7vXitv
ngaWVF+0k9ke2m1QpdKVCcLWlWA+z5HhziALabVHPqrRSDKnjZAQn2XFuEMCGQPY
JLQlRHJhemlvdGlzIEtvc3RhcyA8ZHJhemlvdGlAZ21haWwuY29tPokBOAQTAQIA
IgUCTevnmQIbDwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQ6xGF+CcT1t/B
fQgAwwPwoG82P89DoJPwk22omSAWfqIl//cOmir4Rtj5FQL7zEmZrVe+czvz6w2V
W7uSUrL7rZAjPUtnT/KAELJtQyeko0npKFf0tYJPbQnJeGUiL9uX2xd7Y7zxPh7f
EVIrd72rAbYtPvgm2X2bs5g+nEP8DCzBICVTyB6aHbEBdIF6tNYWVNqXbJq7+MmL
G2kXPpc0wpiySrg1x8beE/rhq/sL3f5ruSTLRfef0auKu1k/JiUT3Z5kAFUsuIUv
/t+5WGvuwsRAO3Zrzh63l7jlj2FGsNe1HPyT6+tN1tWyf8xrnkjWFUD0/NeN6Si4
8ajLCJr5CMNYNovgtUp/9F/qrg==
=0uam
-----END PGP PUBLIC KEY BLOCK-----

16.3.2 Δημόσιο κλειδί αποστολέα

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQINBFV7a4kBEACpGRL6srLk3llyMxo8nwlup8852EXwNUlzBWPSnFa0RcXKMNvv
5WLxMFNXgRI+reo/JYurIp83EatDoNAgbHX0fv6yN68nIv/CsMQ302x+I5sF0fM3
MUWcTAvGFIVH9K63251tUl1DRCZyOMb9ME+yFk8NINLAed33o/S8rZ8vh7VF+By3
P7ZXckfAu1Gx1SrjSpnfRs6O+4Qj+1z6/WgNpT4f620dE6RFoSD6yWaWmaconBrc
bTYFAnhyJR/ENUDrYrv/QAsVUfpdSjRrMVuvbxHlnoCxve3LZIDN0ZzbIxuuWe6i
3FIX4QxtCqDIv955rPtewUN+sH092qogVY+ksfGX1zK+9+3g+v+ZW3Xwzv2HDGdG
ZmmjEEFNIFkpza+e/S+LNZGN9t91tsLRNX7lKoWj4LuFxZ9te9sOrHLQLAXJ3pP+
tYDNZh6s3G7OruHqm5N5/puL4OGDTAOqLMYBuN6J9Y3pd5oDZ5TWNrfQFZMJnjvx
BWMPyMlYH24HPaBkTUfZRoxvSDrz+MfnFf2T8u96aoY6ojsrvDhxTTO8gPnH3n8O
FGGV8gbx2CFcAS7JDl6qVaaEq43ZpfsCLw52vqTx1XSSHvV+TDNF4t3FhUMwaknP
YlKCDy3RpMuBaJQKL4RG/RtnAuR3RwbDRQTqWtojay91K6br6dje/GbmHQARAQAB
tCxEaW1pdHJpb3MgUm91c2lzIDxkaW1pdHJpb3Nyb3VzaXNAeWFob28uY29tPokC
PwQTAQgAKQUCVXtriQIbIwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheA
AAoJEO084GDN+64kTUMP+gPeSfizt8gfLfsAXvXJpxooF3CqbB/udLc9S8gLOCd3
uH5kg97oFG4fdNqoo9nzf51xpcr/o3izdfqGBN6Time7OMFuhqsTZ/i6vcpEcwbn
LE78qZ2JAO20FvrJOr6u/yDi69k8lTML4v5PYe0jZstV8D75G/tlfmktqSr5x+IW
oA7mIEzAPRPyyE0TWYtCpIjCcfcHixY5MT9+jNECgeTMBIFHxweHi9cVVD2BFIQx
LRNZaZbrkros24xu/CxYToIXRz5NzoyEesXBRNvOrG4faiFg6MXMgJFZaCP8e1GV
xkB8SWbBb2HZE1UgBJGGi4ce0kyzuRER0eViDeRA31Qok5pUPXOLa3kdOmOljRIy
n8KvN1eOMFj1o9tT8QI4sGAmxjbxBhWC+tR3kJClJHbzctpLWN9mlppOf75PUtsL
B290l9OO0I3q6LL5dhNr9IZgCcc/zgYPo59YLS9OoW1y6wLH9yQPuEOKIr8Y/C3A
JzrlgWAH+iDF6mwP15GEG7iwkMKw7KoAa4I+6JYjhAaUvNqJNEq4dPKBKMUHwpzq
URIKrvXLcpCZpQ4f+X9LqRxdY0l2Wvtc2G9IAL2F45d0RxcsjFIIJjS1MiNDNvN3
8TPY9/tPas9n+xCVAvjKAsUT2/C33Hmc1hg26Ur+4zkMnR0fatPkXAObcw2uhL48
uQINBFV7a4kBEACydNlpCnUoGRPBnnX+eE8vJHzkx3iO37iVcPrG3QbGOKp6j8UG
sP5utKhSOKTO7zJUH5/U/8xdthqf87RI+5Xdw/iaet9Eo12E+ThLPgU9gjDaLkE3
t2rH5JxXP5VIidGp+7eB/WHc6gaAq1vS13iB+bNUzS1jIDup5cqQztGydYimObRP
1SwX0rj0j8kyO8HQWc2LqsMN/l8PMDa/M+DG7Wo4G3zk60BHChgkLy2mLoWyX0OI
I/QJmDdE0HEZ4XFh2VJ9sM2tTJnRMcqq7FRxm/yQbpTWCTo5bwv+yZJ7My5GMWAv
CIFK9CZPyb9FZ9kOSroxe+Lsh9zjeDqfQ1ztfjTJxKN5O7oLctYzDBwzWY49VhN8
epzsIpm0IXn9AuMKbI4U9ol4RKk3wrW/iL9Iqip6hvLLog7Y05SDUd/N1plq7h9/
fAQ45csDZp/rPhu7hEVHZ8iHoE4y/2q0J5LksXODJp5Q3tEvk0+kMx3Qd6ZoaLfO
1VoxVlz3y/F3edPp9345VD9Hrz4+02auJxISBj2QihUGKa8kKR1sdz0GCzN+HROK
TlHd0n67u9cCS1924gd/ILPsRzpaAX953nKYM/mCeN5A8VohvTDXCcFfvRLmitb2

bKtnlWMlsbOTpjeAK99v/XWU0kU34F4zjwmE6KvFAyJeAj992hDLKLIOYQARAQAB
iQIlBBgBCAAPBQJVe2uJAhsMBQkJZgGAAAoJEO084GDN+64k+zwP/0FAVR4WBxBw
W6t0JcdJgqz7qpm14EplH2B9PO4q3IDsQ+d23NxkgAY4/Uqj2x6EX8wLU6bRYuzy
pf4L3yz9CdQDUEeOdIuP1KEhVsN9a9zFzC5W619vUNKmA/iuOCwc3jEpAg2v8SRR
dBoycM/2FY2mtEckb8+hlL7r1IWuD5r8+lx5UiwOmUGRwdusaggAXnHwFz53yUne
n5NgEv16AR91ECI6QvkfRdbI9fNtMzTfGvgZb/cMal3kiSpCi0Vz+mNOZBVokuvn
22bM2kBg6ok6VIagQQPJEcv3NLpLMrPUDFkf1xBbpajmYtJNpehRQldKYBMy9dhy
FLq3uDHNBvmlMgg4ve+ciAVUTPJKgDxWgqw0TfVlqTqhwJ6dRkuiPirtCWiSqtBo
ifbQCdPPY78FE++oxi007UtA7SPzzabDO32fCxJOt001MKQl7cpF5OK2PrD3rRK2
WJU3/d6FhvGiFoJKY+zQjRh+1GysonwqV9TOlzTeFj4zettCPzVf5IBZNIKrOJL8
quAwLA82GEUwuT89ztKTh/LKThspQ9/MCb07zBX0I+FRe7uEep8piI5ERZzqkWFD
QlsnFSpJZvcDxiQ+TZeZ6sMcPy47PF7hbTqAbA4tqKUNpeiaeq/at76lVp0AerN3
OdoHolE0lHdEp0ybdvV0/Bo/KhJnTSNS
=5TeQ
-----END PGP PUBLIC KEY BLOCK-----

17. Βιβλιογραφία

[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.