Του Κώστα Μπουκουβάλα <boukouvalas@greeklug.gr>

Ο Κώστας είναι ιδρυτικό μέλος του GREEKLUG.

Ψηφιακή πιστοποίηση με CAcert

Η ασφάλεια στην επικοινωνία μας με άλλους χρήστες ή με διαδικτυακούς servers προϋποθέτει την ύπαρξη και αποδοχή ψηφιακών πιστοποιητικών από κάποια ανεξάρτητη αρχή, όπως η CACert. Τι είναι όμως τα πιστοποιητικά και γιατί τα χρειαζόμαστε;

Περισσότερα HOW-TOs

Εργαλεία: Τερματικό
Δυσκολία: ★★☆☆☆
URL: http://cacert.org

Ξεκινώντας από τα βασικά για να γίνει κατανοητό το άρθρο, θα πρέπει πρώτα να καταλάβουμε τι είναι η ψηφιακή πιστοποίηση. Αυτή δεν είναι τίποτε άλλο από μία ηλεκτρονική διαδικασία που πιστοποιεί την ταυτότητα του χρήστη που χρησιμοποιεί κάποια υπηρεσία, που επικοινωνεί με κάποιο άλλο χρήστη ή γενικά κάποιου που αλληλεπιδρά απομακρυσμένα με υπολογιστή και η πρόσβαση σ' αυτόν απευθύνεται σε όσους αποδέχονται και χρησιμοποιούν μια συγκεκριμένη αρχή πιστοποίησης. Υπάρχουν πολλές αρχές πιστοποίησης, δηλαδή, οργανισμοί οι οποίοι εκδίδουν ψηφιακά πιστοποιητικά. Το ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο που χρησιμοποιεί μία ψηφιακή υπογραφή για να συνδέσει ένα δημόσιο κλειδί με μία ηλεκτρονική ταυτότητα. Με αυτόν τον τρόπο πιστοποιείται πως ο συγκεκριμένος χρήστης έχει στην κατοχή του το δημόσιο κλειδί που εκδίδεται από την αρχή πιστοποίησης.

> **Για τη δημιουργία εμπιστοσύνης και αυξημένου κύρους κάποιου ψηφιακού πιστοποιητικού, μεγάλο ρόλο παίζει και το πόσοι άνθρωποι το χρησιμοποιούν.**

CAcert.org

Η CAcert.org αποτελεί ένα μη κερδοσκοπικό οργανισμό και είναι μια αρχή πιστοποίησης, καθοδηγούμενη στην ουσία από την κοινότητά της. Εκδίδει ελεύθερα – και δεν πουλάει, όπως άλλες εμπορικές αρχές πιστοποίησης – πιστοποιητικά δημόσιου κλειδιού (public key certificates) τα οποία μπορούν να χρησιμοποιηθούν για διάφορους λόγους: Είτε για την κρυπτογράφηση των email, είτε για την πιστοποίηση και παροχή πρόσβασης ασφαλούς σύνδεσης σε websites.

Στην πράξη, οποιοσδήποτε κερδοσκοπικός ή μη οργανισμός μπορεί να αποτελέσει αρχή πιστοποίησης χρησιμοποιώντας την κατάλληλη υποδομή και το κατάλληλο software. Όμως ποιον από όλους αυτούς τους οργανισμούς ή εταιρείες μπορούμε να εμπιστευτούμε; Όταν χρησιμοποιούμε κάποιον δημοφιλή browser όπως ο Firefox, συνήθως θέλοντας και μη εμπιστευόμαστε αυτόματα περίπου 36 εμπορικές αρχές πιστοποίησης καθώς τις έχει εμπιστευτεί πριν από μας το Mozilla Foundation. Στην περίπτωση όμως του CAcert θα πρέπει να εισάγουμε ορισμένες φορές μόνοι μας το CAcert root certificate που εκδίδεται από την αρχή πιστοποίησης CAcert.org. Αυτό επιτυγχάνεται με τους παρακάτω τρόπους:

Debian/Ubuntu:

```
sudo apt-get install ca-certificates
```

Redhat 5+:

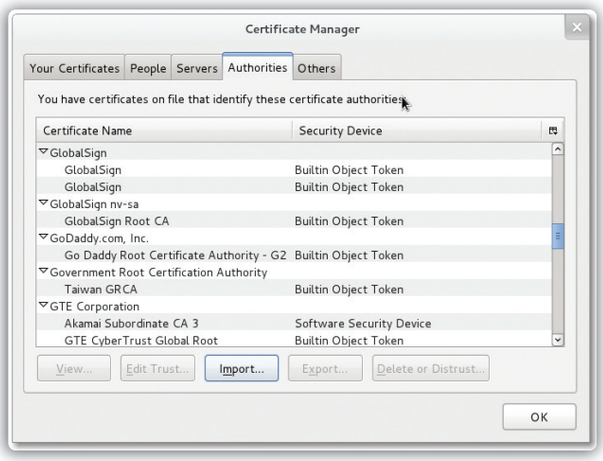
```
wget -O
 http://www.cacert.org/certs/root.txt >>
/etc/pki/tls/certs/ca-bundle.crt
```

Πλέον, θα έχουμε ασφαλή πρόσβαση σε όσα Web sites απαιτούν την αποδοχή του πιστοποιητικού CAcert root certificate. Για να βεβαιωθούμε πως το πιστοποιητικό που λάβαμε με τη διανομή είναι γνήσιο, η αρχή πιστοποίησης CAcert.org συνεργάζεται με αρκετούς διαδικτυακούς τόπους που μπορούν να σας δώσουν το κατάλληλο fingerprint. Προσοχή! Ακόμα και αν έχουμε εγκατεστημένα τα πιστοποιητικά στον browser δε θα μπορούμε να έχουμε πρόσβαση αν δεν εκδώσουμε το προσωπικό μας client certificate μέσω του cacert.org. Γι' αυτό το λόγο θα πρέπει να συμπληρώσουμε τη φόρμα εγγραφής στο cacert.org, κάτι που θα χρειαστεί εξ' άλλου εάν θέλουμε να συμμετάσχουμε σε ο,τι αφορά τα ψηφιακά πιστοποιητικά που εκδίδει η CAcert. Είναι η ταυτότητα η οποία αναφέρθηκε προηγουμένως με την οποία θα συνδεθεί το ψηφιακό πιστοποιητικό.

Web of Trust

Πέρα όμως από τη χρήση του ψηφιακού πιστοποιητικού για τη χρήση του browser, ένας άλλος λόγος που χρησιμοποιούμε ένα πιστοποιητικό μπορεί να είναι η κρυπτογράφηση της επικοινωνίας μας μέσω e-mail με κάποιους φίλους ή συνεργάτες. Για τη δημιουργία υψηλού επιπέδου εμπιστοσύνης και στην ουσία ύπαρξη αυξημένου κύρους κάποιου ψηφιακού πιστοποιητικού μεγάλο ρόλο παίζει και το πόσοι άνθρωποι το χρησιμοποιούν. Με λίγα λόγια η δημιουργία ενός δικτύου εμπιστοσύνης (Web of trust). Η δημιουργία ενός Web of trust βασίζεται στην πολύ απλή αρχή της ανθρώπινης επικοινωνίας μέσω των key signing parties και των assuring events. Στα key signing parties συγκεντρώνονται φίλοι και γνωστοί οι οποίοι ανταλλάσσουν δημόσια κλειδιά (PGP ή GPG) και αφού είναι σίγουροι πως το κλειδί ανήκει στον άνθρωπο που το δίνει μέσω της προφορικής ή άλλης επιβεβαίωσης του fingerprint, υπογράφουν το κλειδί. Ο υποφαινόμενος, π.χ., είχε την ευτυχία η πρώτη υπογραφή που έλαβε στο δημόσιο κλειδί του να προέρχεται από τον ιδρυτή του Ιδρύματος Ελεύθερου Λογισμικού, Richard Stallman.

Αντίστοιχα, στην περίπτωση που εξετάζουμε, για τα μέλη της κοινότητας CAcert υπάρχει ο θεσμός της επιβεβαίωσης (assure) που λαμβάνει χώρα στο πλαίσιο άλλων events – αρκετές φορές είναι εκδηλώσεις της παγκόσμιας κοινότητας ελεύθερου λογισμικού. Αφού έχετε φτιάξει ένα λογαριασμό στο cacert.org και έχετε δώσει τα σχετικά στοιχεία μπορείτε να επιβεβαιωθείτε (get assured) από έναν επιβεβαιωτή



1 Στις Προτιμήσεις>Advanced>Encryption μπορείτε να δείτε το Διαχειριστή Πιστοποιητικών του Firefox.

2 Τα keysigning parties που γίνονται κατά καιρούς είναι ευκαιρία και για assuring!

(assurer) σε κάποιο meeting ή να βρείτε κάποιον επιβεβαιωτή μόνοι σας. Αυτή είναι μία τυπική διαδικασία φυσικής αναγνώρισης και επιβεβαίωσης με τη βοήθεια κάποιου κυβερνητικού εγγράφου (ταυτότητα, δίπλωμα οδήγησης κ.ά.). Αφού καταφέρετε να επιβεβαιωθείτε από κάποιον assurer τότε σταδιακά αποκτάτε ορισμένους πόντους ώστε να αποκτήσετε υψηλότερη θέση στο Web of trust και να αποκτήσετε ορισμένα προνόμια σε αυτό.

Για παράδειγμα, για να υπογραφεί ένα PGP ή GPG κλειδί από την CAcert θα πρέπει ένα μέλος του CAcert να έχει 50 πόντους για να το κάνει αυτό. Εφόσον υπογραφεί αυτό το κλειδί σημαίνει πως τουλάχιστον δυο άνθρωποι επιβεβαιώνουν την ταυτότητά μας, καθώς για να έχουμε 50 πόντους θα πρέπει να έχουμε επιβεβαιωθεί από δύο άλλους ανθρώπους. Έτσι, το κλειδί σας αποκτά μεγαλύτερη αξιοπιστία όσον αφορά στη γνησιότητά του. Πέρα όμως από περιφερειακά οφέλη, όπως αυτό που μόλις περιγράψαμε, ο κύριος τρόπος λειτουργίας της κοινότητας CAcert είναι η απόκτηση πόντων επιβεβαίωσης (assurance points) για μεγαλύτερη συμμετοχή στην κοινότητα και χρήση των πιστοποιητικών της CAcert. Όσο περισσότερους πόντους έχει κάποιος, λοιπόν, τόσο μεγαλύτερη πρόσβαση στα (δωρεάν) εκδιδόμενα πιστοποιητικά της CAcert αποκτά. Οι βαθμίδες είναι:

- Client certificates τα οποία μάς επιτρέπουν να στέλνουμε και να δεχόμαστε κρυπτογραφημένα μηνύματα e-mails. Έχουν διάρκεια ζωής 6 μήνες και δεν χρειάζεται να είναι κάποιος assured μέλος.
- Assured client certificates τα οποία μάς δίνουν τις ίδιες δυνατότητες με τα client certificates, αλλά διαρκούν 24 μήνες και μπορούμε να προσθέσουμε το όνομά μας σ' αυτά. Πρέπει να έχουμε 50 πόντους.
- Code signing certificates με τα οποία μπορούμε να υπογράφουμε ψηφιακό κώδικα, Web applets, installers κ.λπ., τα οποία διαρκούν 12 μήνες και πρέπει να περιλάβουμε το όνομά μας σ' αυτά. Για την απόκτησή τους θα πρέπει να έχουμε λάβει τουλάχιστον 100 πόντους.
- Server certificates τα οποία μάς επιτρέπουν να ενεργοποιούμε την ασφαλή πρόσβαση για όποιον επιθυμεί να συνδεθεί σε κάποια δικτυακή υπηρεσία μας (Web, e-mail, SSL). Αυτά διαρκούν 6 μήνες και μόνο το domain name μπορεί να τοποθετηθεί στο πιστοποιητικό.
- Assured server certificates τα οποία μας δίνουν τις ίδιες δυνατότητες με τα server certificates αλλά διαρκούν 24 μήνες.

Για να τα λάβουμε χρειάζονται 50 πόντοι.

Εάν καταφέρει κάποιος να γίνει assurer στο δίκτυο εμπιστοσύνης της CAcert (100 πόντοι και μία μικρή διαδικασία εκπαίδευσης) τότε θα αποκτήσει τη δυνατότητα να επιβεβαιώνει άλλους χρήστες και να επεκτείνει το δίκτυο εμπιστοσύνης της CAcert. Τέλος, κάποιος με $10 μπορεί να γίνει μέλος στην Ένωση CAcert και να αποκτήσει το δικαίωμα του εκλέγεσθαι για το CAcert board.

Πού μπορώ να λάβω βαθμούς επιβεβαίωσης;

Στην Ελλάδα ένα από τα λίγα key signing parties που έλαβαν ποτέ χώρα είναι αυτό που πραγματοποιήθηκε στο 1ο Fosscomm, το 2008 (http://bit.ly/kmyRhX) και στο οποίο υπήρχε επίσης η δυνατότητα εγγραφής στο CAcert. Από τότε μέχρι σήμερα η κοινότητα των CAcert assurers στην Ελλάδα έχει μεγαλώσει αλλά δεν έχει λάβει την προβολή που της αξίζει. Εφόσον έχετε εγγραφεί στο cacert.org, έχετε διαθέσιμο το πιστοποιητικό στον browser που χρησιμοποιείτε και έχει γίνει το binding με το προσωπικό σας πιστοποιητικό, μπορείτε να βρείτε assurers ανάλογα με την απόσταση από τον τόπο κατοικία σας. Αυτή τη στιγμή υπάρχουν μερικοί φίλοι του CAcert στην Αθήνα οι οποίοι είναι κυρίως παλαιά μέλη της ελληνικής κοινότητας open source, μεταξύ των οποίων και αρκετοί assurers.

> Για να υπογραφεί ένα PGP ή GPG κλειδί από την CAcert θα πρέπει ένα μέλος του CAcert να έχει 50 πόντους για να το κάνει αυτό

Η τεχνολογία πίσω από την CAcert

Η αρχή πιστοποίησης CAcert είναι μία robot certification authority η οποία υπογράφει αυτόματα δημόσια κλειδιά τα οποία ικανοποιούν ορισμένες προϋποθέσεις. Η CAcert υπογράφει πιστοποιητικά για διευθύνσεις e-mail που ελέγχονται από τον αιτούμενο και για domains των οποίων συγκεκριμένες διευθύνσεις όπως (hostmaster@example.com) επίσης ελέγχονται από τον αιτούμενο. Αυτά τα πιστοποιητικά θεωρούνται γενικά αδύναμα εξαιτίας του γεγονότος ότι η CAcert δεν παρέχει πληροφορίες πέραν του domain name ή της διεύθυνσης e-mail (πεδίο CommonName στα πιστοποιητικά X.509).