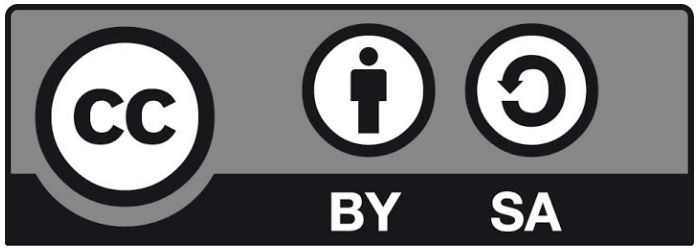
Υποδομή Δημόσιου Κλειδιού

Εισηγητής: Χρήστος Δαλαμάγκας
cdalamagkas@gmail.com

Άδεια χρήσης



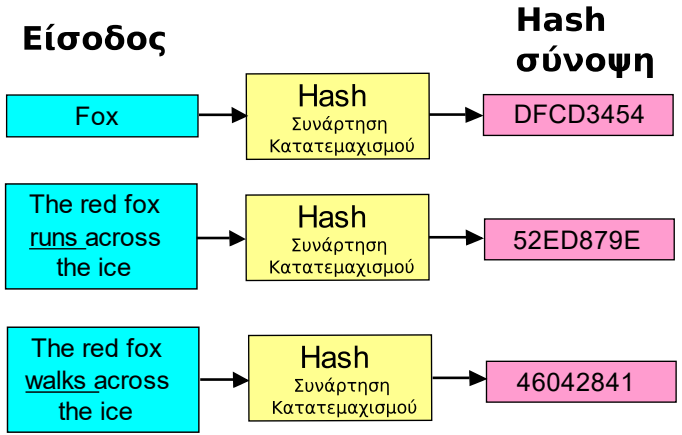
Ατζέντα

- Συναρτήσεις κατακερματισμού
- Ψηφιακή υπογραφή
- Ψηφιακό πιστοποιητικό
- Υποδομή Δημοσίου κλειδιού

Συναρτήσεις κατακερματισμού

Ορισμός συναρτήσεων κατακερματισμού

- Κατακερματισμός = hash
- Συνάρτηση Hash H(): μετασχηματισμός που εφαρμόζεται στα δεδομένα
- Είσοδος: ένα μήνυμα m **οποιουδήποτε** μήκους
- Έξοδος: μια ακολουθία (σύνοψη) χαρακτήρων h **συγκεκριμένου** μήκους
- h = H(m)



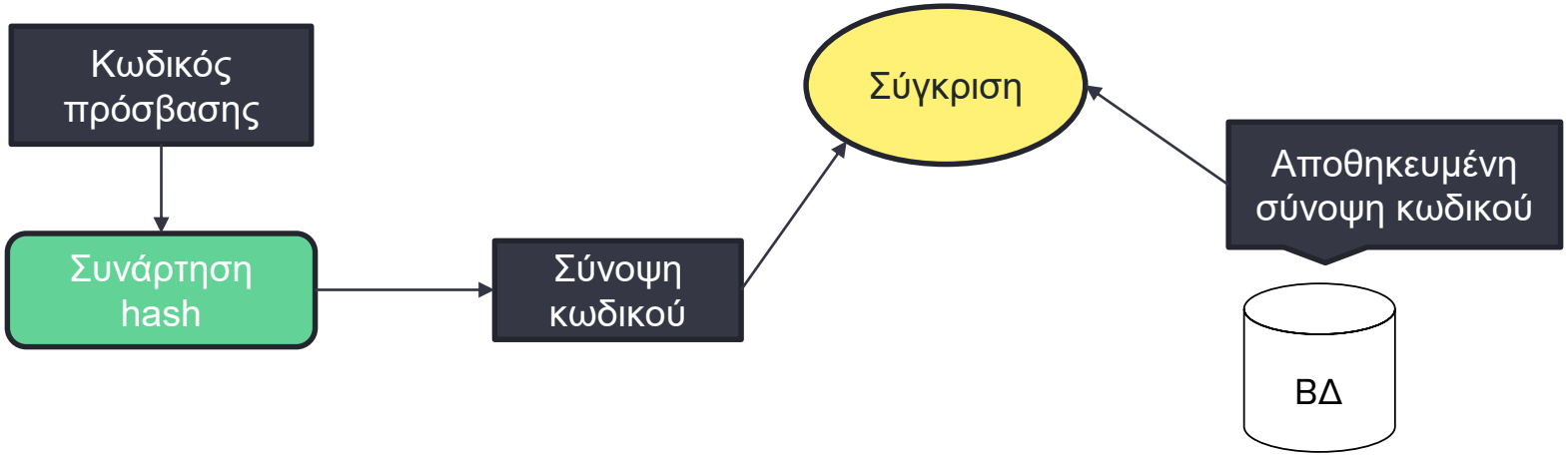
Ιδιότητες συναρτήσεων κατακερματισμού

- Η είσοδος έχει οποιοδήποτε μήκος
- Η έξοδος έχει συγκεκριμένο μήκος
- Με δεδομένο το m, ο υπολογισμός του h είναι εφικτός
- Με δεδομένο το h, ο υπολογισμός του m είναι αδύνατος
- Η συνάρτηση hash είναι μη αντιστρέψιμη και αμφιμονοσήμαντη (1:1)
- Έστω και ένα bit αν αλλάξει στο m, το h θα είναι εντελώς διαφορετικό

Για μας, οι συναρτήσεις H() είναι «μαύρο κουτί»: Δεν μας ενδιαφέρει πώς λειτουργούν.

Χρήσεις

- Κρυπτογράφηση
- Ταυτοποίηση δεδομένων
- Επιβεβαίωση αν ένα αρχείο έχει τροποποιηθεί ή αλλοιωθεί
- Απόκρυψη της πραγματικής μορφής των δεδομένων από τρίτους



Γνωστές συναρτήσεις κατακερματισμού

- MD5
  - Επιστρέφει έξοδο μήκους 128 bit
  - Έχει παραβιαστεί από το 2012 με τη μέθοδο επίθεσης συγκρούσεων (collision attacks)
  - Η χρήση του δε συνίσταται για λόγους ασφαλείας!
- SHA – Οικογένεια προτύπων για ασφαλείς συναρτήσεις hash
  - SHA-1: Επιστρέφει έξοδο μήκους 128 bit – Μη ασφαλής!
  - SHA-2: Σύνολο νεότερων συναρτήσεων με μεγαλύτερη έξοδο (SHA-224, SHA-256, SHA-384, SHA-512)
  - SHA-3: Η νεότερη ομάδα συναρτήσεων (SHA3-224, SHA3-256, SHA3-384, SHA3-512)

Ψηφιακή Υπογραφή

Ψηφιακή Υπογραφή

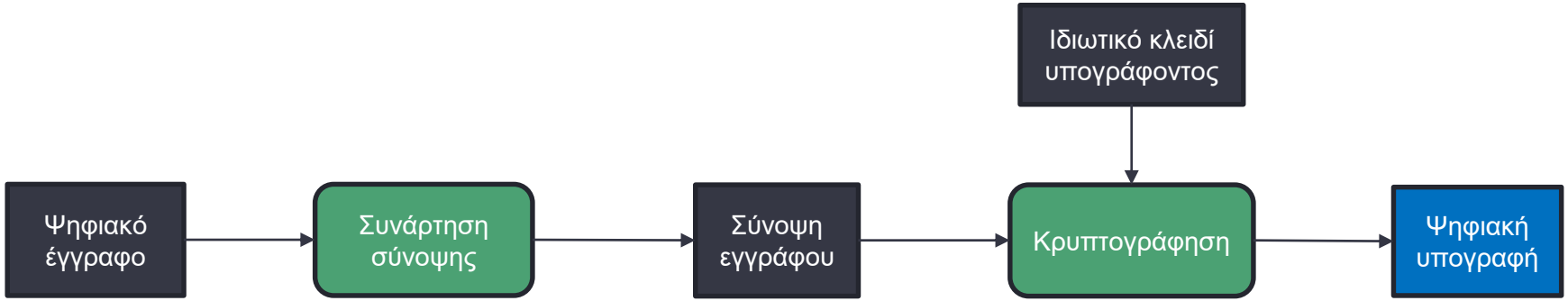
- Πρόκειται για μια εφαρμογή της ασύμμετρης κρυπτογράφησης
- Είναι ένα κομμάτι δεδομένων που πιστοποιεί τη γνησιότητα ενός ψηφιακού εγγράφου
- Γενικά, η ψηφιακή υπογραφή επιβεβαιώνει τα εξής:
  - Την ταυτότητα του συγγραφέα του ψηφιακού εγγράφου
  - Το πότε μπήκε η υπογραφή
  - Τα περιεχόμενα του εγγράφου τη στιγμή της υπογραφής
- Τρίτα πρόσωπα θα πρέπει να επιβεβαιώνουν τη γνησιότητα της υπογραφής

Ψηφιακή Υπογραφή

- Το δημόσιο κλειδί του RSA αποτελεί ένα ψηφιακό έγγραφο που χρειάζεται επιβεβαίωση.
  - Οι πελάτες που θέλουν να εγκαθιδρύσουν μια ασφαλή σύνδεση με έναν εξυπηρετητή, κρυπτογραφούν με το δημόσιο κλειδί του εξυπηρετητή.
  - Αν το δημόσιο κλειδί είναι πλαστό, τότε η ασφάλεια της σύνδεσης τίθεται σε αμφιβολία.
- Άλλες εφαρμογές:
  - Υπογραφή αρχείων PDF

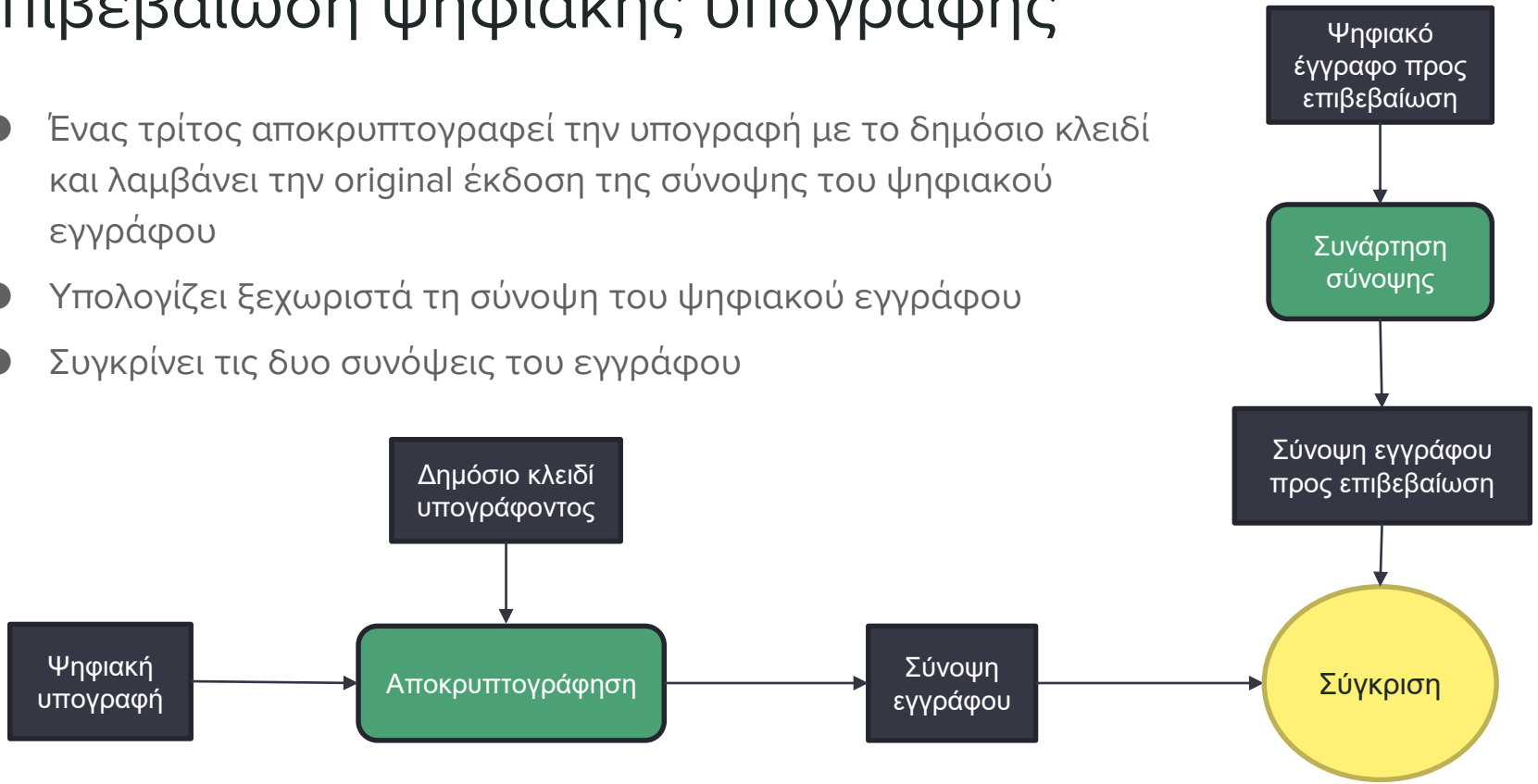
Δημιουργία ψηφιακής υπογραφή

- Υποβάλλεται το ψηφιακό έγγραφο σε αυτόν που υπογράφει
- Ο υπογράφων υπολογίζει τη σύνοψη του εγγράφου
- Ο υπογράφων **κρυπτογραφεί** τη σύνοψη με το **ιδιωτικό** του κλειδί
- Η υπογραφή είναι η κρυπτογραφημένη εκδοχή της σύνοψης του εγγράφου



Επιβεβαίωση ψηφιακής υπογραφής

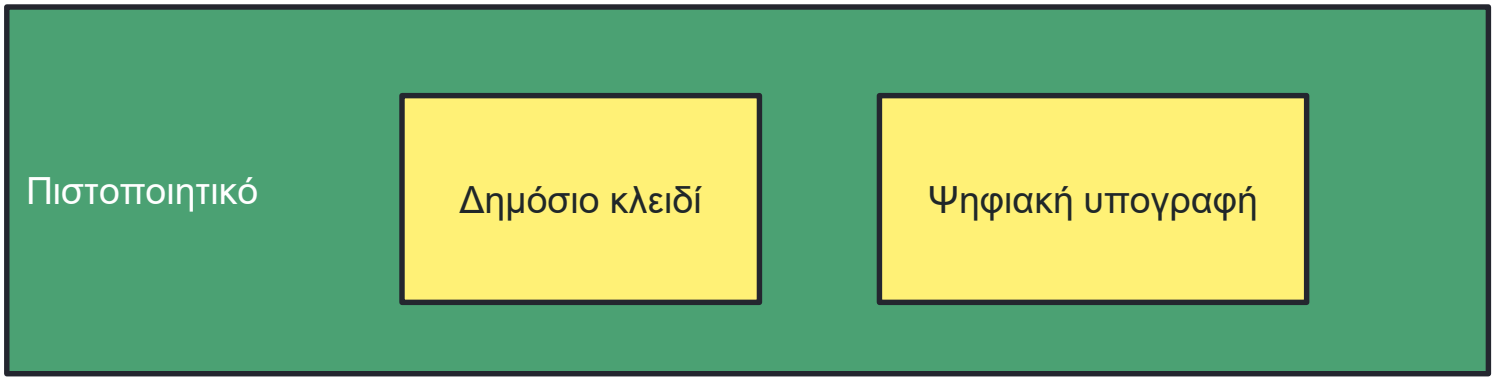
- Ένας τρίτος αποκρυπτογραφεί την υπογραφή με το δημόσιο κλειδί και λαμβάνει την original έκδοση της σύνοψης του ψηφιακού εγγράφου
- Υπολογίζει ξεχωριστά τη σύνοψη του ψηφιακού εγγράφου
- Συγκρίνει τις δυο συνόψεις του εγγράφου



Ψηφιακό Πιστοποιητικό

Ψηφιακό Πιστοποιητικό

- Ορισμός: Ένα δημόσιο κλειδί μαζί με τη ψηφιακή υπογραφή του στο τέλος
- Χρήση: Πιστοποιεί την αυθεντικότητα ενός δημοσίου κλειδιού
- Δημιουργείται από μια τρίτη έμπιστη οντότητα – Αρχή Πιστοποίησης (Certification Authority – CA)



Διαδικασία παραγωγής πιστοποιητικού

1. Ο πελάτης παράγει έναν συνδυασμό δημοσίου και ιδιωτικού κλειδιού
2. Ο πελάτης δημιουργεί μια αίτηση υπογραφής πιστοποιητικού (Certificate Signing Request – CSR). Η αίτηση περιέχει το δημόσιο κλειδί και διάφορες άλλες πληροφορίες.
3. Με κάποιον ασφαλή τρόπο, ο πελάτης υποβάλλει την αίτηση στην Αρχή Πιστοποίησης
4. Η αρχή πιστοποίησης διαβάζει την αίτηση υπογραφής και δημιουργεί το πιστοποιητικό ως εξής:
    I. Υπολογίζει τη σύνοψη του δημοσίου κλειδιού και την κρυπτογραφεί με το ιδιωτικό κλειδί
    II. Προσαρτεί την υπογραφή στο τέλος του δημοσίου κλειδιού και δημιουργεί το πιστοποιητικό
5. Η Αρχή Πιστοποίησης παραδίδει το πιστοποιητικό στον πελάτη

Επιβεβαίωση πιστοποιητικού

1. Ένας τρίτος λαμβάνει το πιστοποιητικό
2. Διαβάζοντας το πιστοποιητικό, βλέπει ποια είναι η Αρχή Πιστοποίησης
3. Λαμβάνει το δημόσιο κλειδί της Αρχής Πιστοποίησης
4. Αποκρυπτογραφεί την υπογραφή με το δημόσιο κλειδί της Αρχής Πιστοποίησης
5. Παράγει τη σύνοψη του δημοσίου κλειδιού που περιλαμβάνεται στο πιστοποιητικό
6. Συγκρίνει την πρωτότυπη σύνοψη της υπογραφής με τη σύνοψη που υπολόγισε
7. Αν είναι ίδια, τότε το πιστοποιητικό είναι αυθεντικό

Το πρότυπο X.509

- Ορίζει τη μορφή ενός πιστοποιητικού δημοσίου κλειδιού
- Αποτελείται από τα εξής πεδία:
  - **Πιστοποιητικό** με τα πεδία: έκδοση, σειριακός αριθμός, στοιχεία εκδότη (issuer), χρονική περίοδος ισχύος, στοιχεία υποκείμενου (Subject), αλγόριθμος δημοσίου κλειδιού (πχ RSA), δημόσιο κλειδί
    - Εκδότης: η αρχή πιστοποίησης που έκδωσε το πιστοποιητικό
    - Υποκείμενο: ο πελάτης που κατέχει το δημόσιο κλειδί
    - **Common Name**: Τα ονόματα των προαναφερθέντων οντοτήτων προσδιορίζονται από τα πεδία Common Name (CN)
  - **Αλγόριθμος υπογραφής πιστοποιητικού**: πχ SHA-256 με κρυπτογράφηση RSA
  - **Υπογραφή πιστοποιητικού**

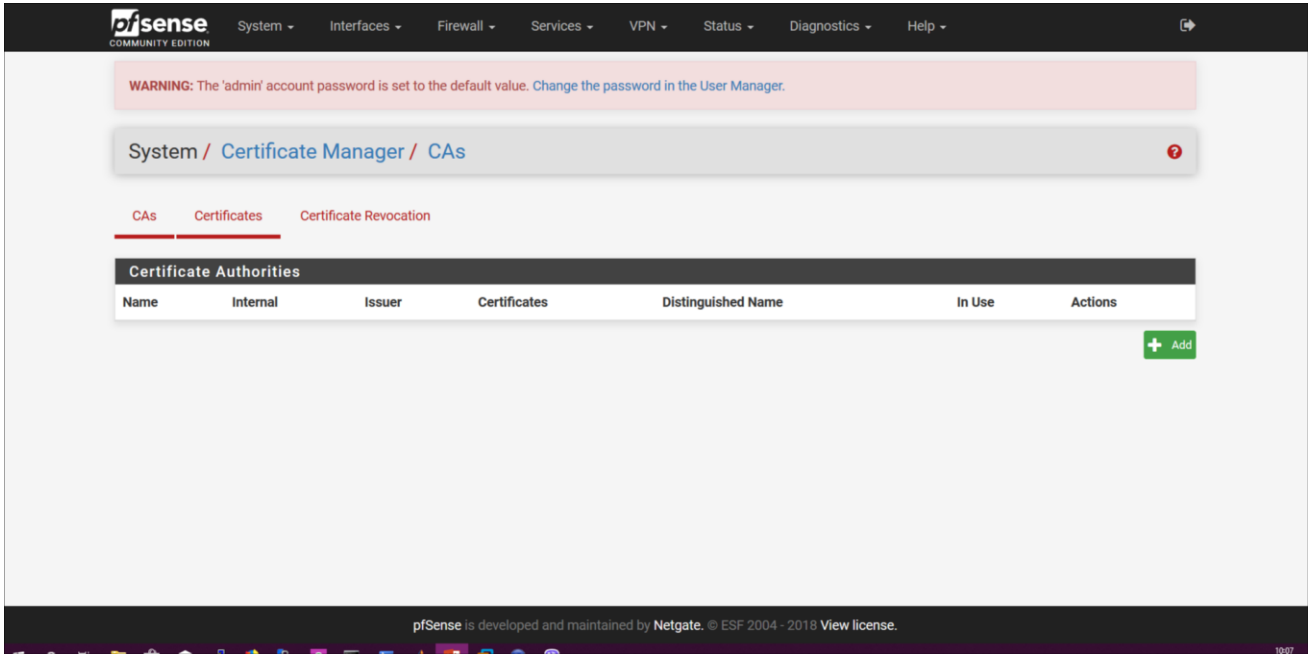
Υποδομή Δημοσίου Κλειδιού

Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure – PKI)

- Ένα σύστημα για τη δημιουργία, διαχείριση, διανομή, χρήση, αποθήκευση και ανάκληση ψηφιακών πιστοποιητικών δημοσίου κλειδιού
- Οντότητες:
  - **Αρχή Πιστοποίησης (CA)**: Η οντότητα που αποθηκεύει, εκδίδει και υπογράφει πιστοποιητικά. Η CA διαθέτει ένα ζεύγος δημόσιου και ιδιωτικού κλειδιού, καθώς και ένα δικό της πιστοποιητικό που αφορά την εγκυρότητα του δημοσίου κλειδιού της.
  - Υποκείμενα: Οι πελάτες/οντότητες που αποκτούν πιστοποιητικά
  - Κεντρικός κατάλογος: Εκεί όπου αποθηκεύονται τα πιστοποιητικά
  - Σύστημα διαχείρισης πιστοποιητικών: Ένα σύστημα που διαχειρίζεται την πρόσβαση στα πιστοποιητικά, καθώς και τη διανομή τους προς τους πελάτες
  - Πολιτική πιστοποιητικών: Κανόνες που αφορούν την έκδοση πιστοποιητικών
  - Λίστα ανακλήσεων (Revocation List): Λίστα με τα πιστοποιητικά που έχουν ετάκτως ανακληθεί και δεν θεωρούνται αξιόπιστα+

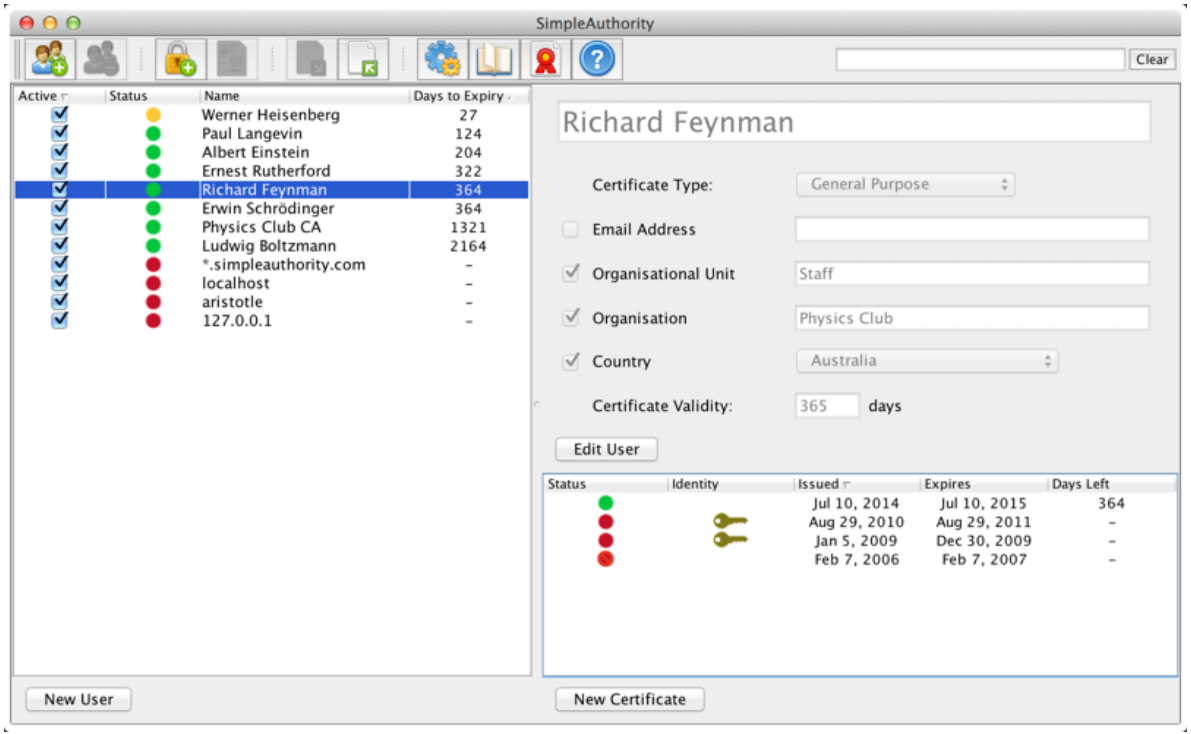
Λογισμικό PKI

- pfsense



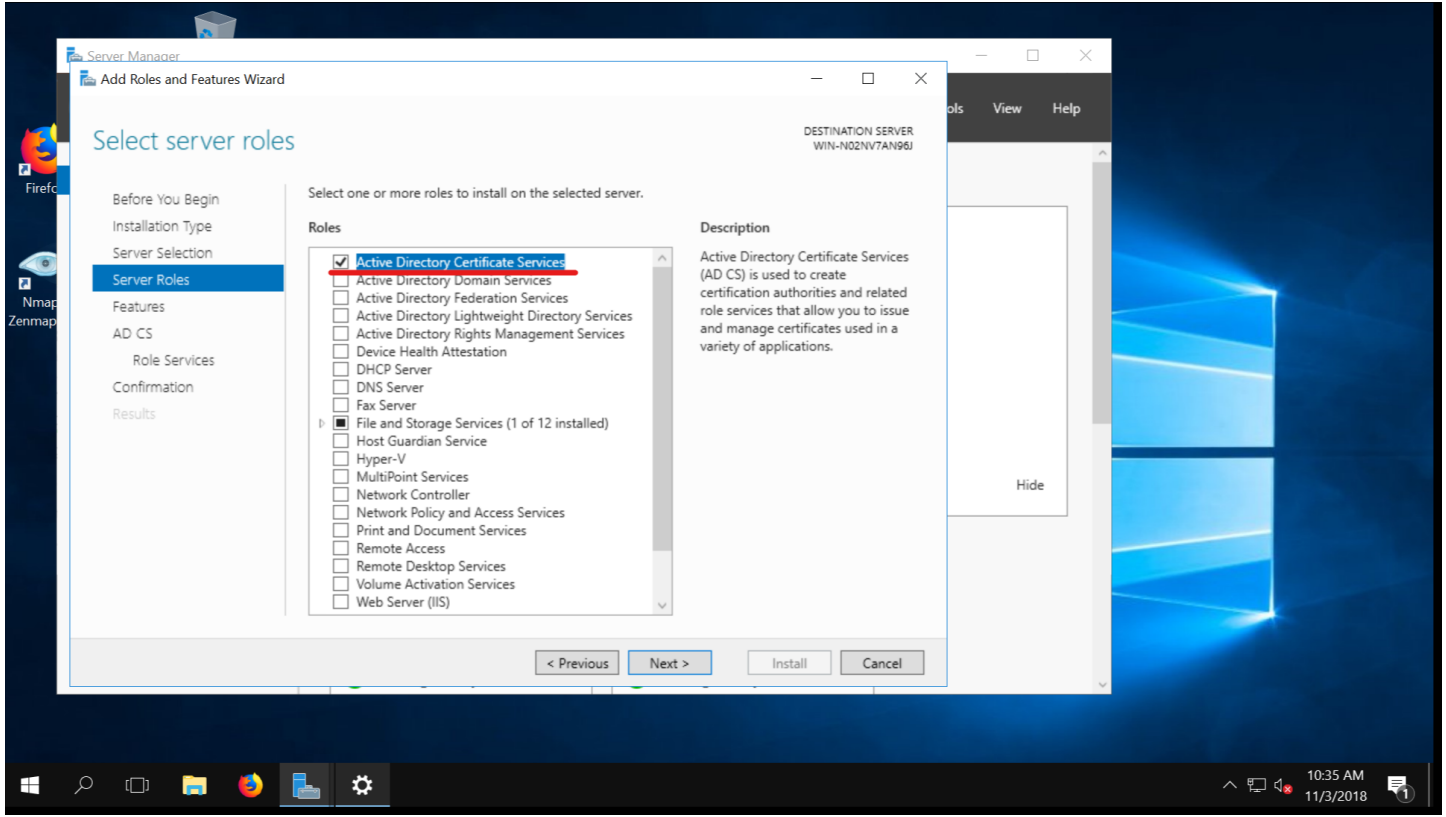
Λογισμικό PKI

- SimpleAuthority



Λογισμικό PKI

- Windows Server 2016



Εφαρμογές PKI

- Ασφαλής σύνδεση με έναν ιστότοπο
  - HTTPS
- Ασφαλής σύνδεση σε απομακρυσμένο δίκτυο μέσω VPN
  - OpenVPN
  - IPSec
- Χρήση δημοσίου κλειδιού για απομακρυσμένη σύνδεση σε τερματικό
  - SSH