ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Διαχείριση Ασφαλείας (ΙΙ)

Δημόσια & Ιδιωτικά Κλειδιά

Ψηφιακά Πιστοποιητικά – Ψηφιακή Υπογραφή

Έλεγχος Πρόσβασης Χρήστη, Single Sign-On (SSO)

Authentication & Authorization Infrastructures (AAI)

Πάροχοι Ταυτότητας (IdP)

SAML - Security Assertion Mark-up Language

Πρωτόκολλα & Αρχιτεκτονικές email

Συστήματα Προστασίας Firewall

Β. Μάγκλαρης

maglaris@netmode.ntua.gr

www.netmode.ntua.gr

20/11/2017

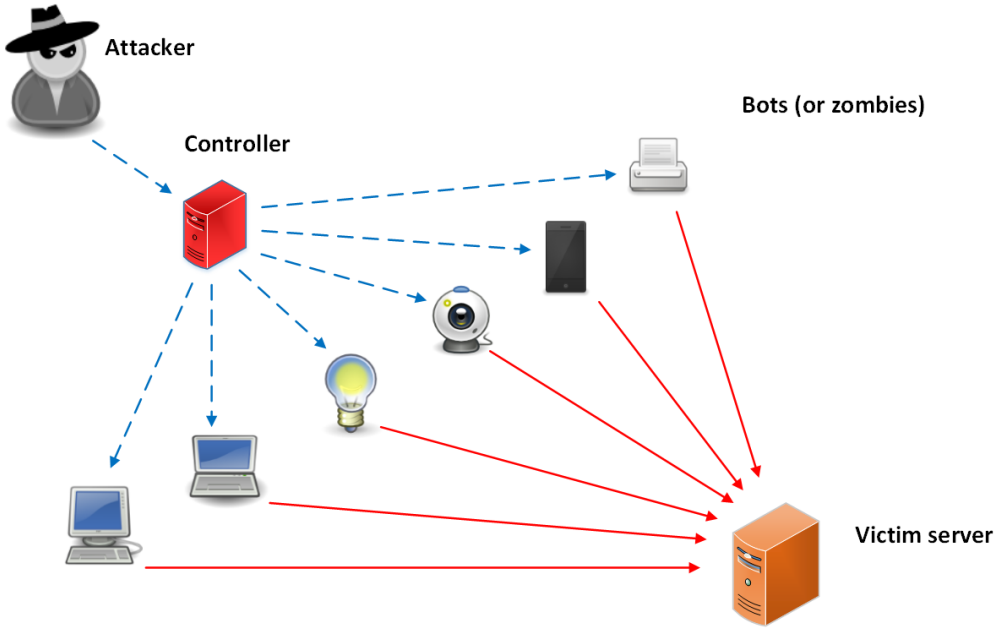
ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ (*Επανάληψη*)

- **Απόκτηση πληροφοριών για το σύστημα:**
  - Port Scanning
  - Fingerprinting
- **Μη εξουσιοδοτημένη πρόσβαση**
  - Υποκλοπή κωδικών
  - Λάθος διαμορφώσεις (ανοικτά συστήματα)
  - Από μη εξουσιοδοτημένα σημεία (π.χ. ανοιχτά σημεία ασύρματης πρόσβασης)
- **Επιθέσεις Άρνησης Υπηρεσίας** (Denial of Service Attacks - DoS)
- **Υποκλοπή και παραποίηση επικοινωνιών**
  - Packet sniffing
  - "Man-in-the-Middle" attacks
- **Κακόβουλο λογισμικό** (malware)
  - Ιοί, Δούρειοι ίπποι (trojans)
  - Αυτόματα διαδιδόμενοι ιοί (worms)

DISTRIBUTED DENIAL OF SERVICE ATTACKS

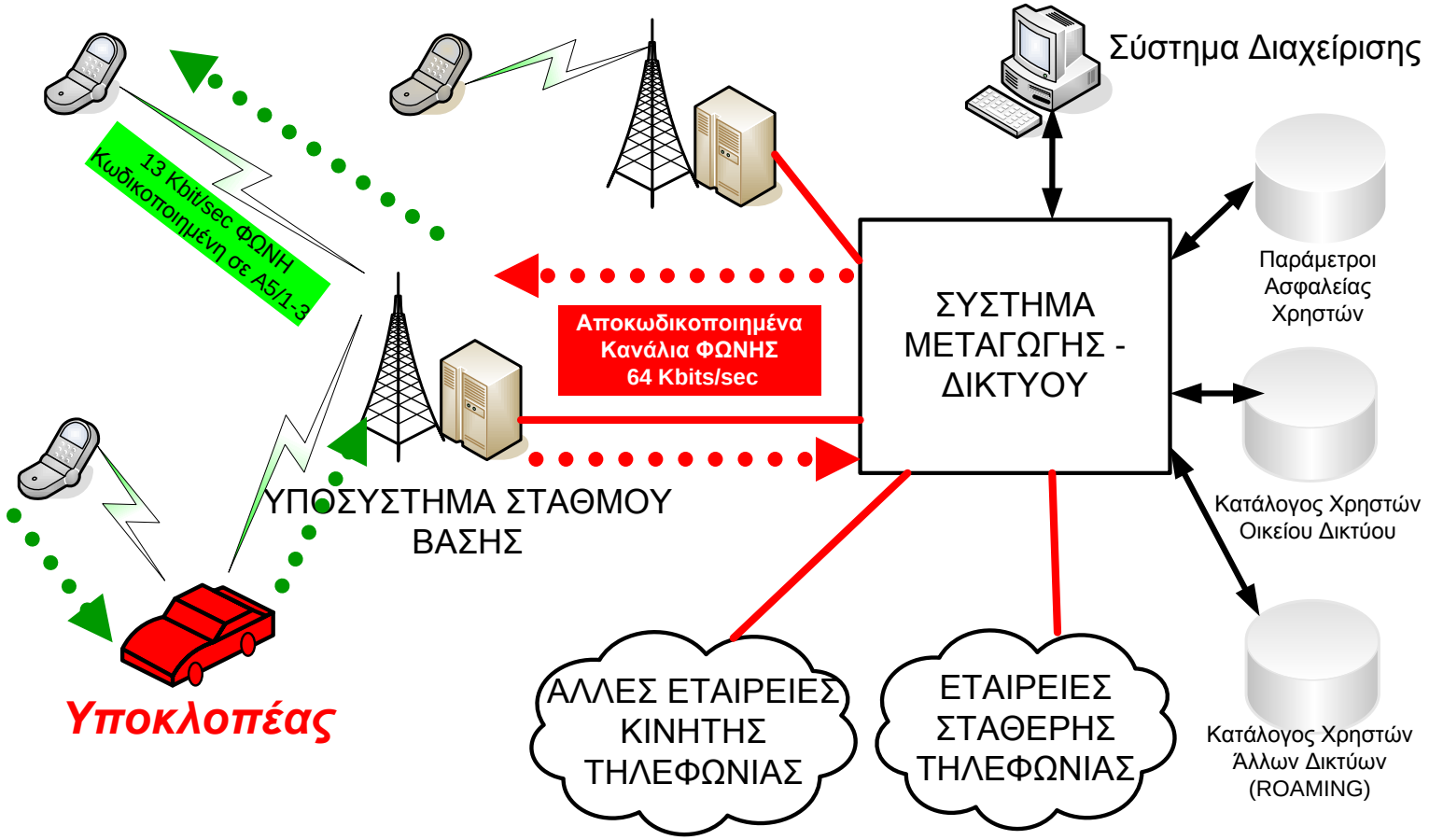
DDoS Attacks (*Επανάληψη*)

- **Bots ή Zombies**: *Μολυσμένοι* (π.χ. μέσω **worms** ή **Trojans**) *κόμβοι στο* **Internet** *(υπολογιστές - smart phones - sensors…) που ενεργοποιούνται σε ορισμένη χρονική στιγμή σαν* **bots** *ή* **zombie** *μαζικών Επιθέσεων Άρνησης Υπηρεσίας* (**Distributed Denial of Service Attacks, DDoS**)
- *Δρομολογείται μεγάλος όγκος κίνησης προς ένα θύμα με στόχο την κατασπατάληση του εύρους ζώνης της σύνδεσης του θύματος ή των πόρων του (επεξεργαστική ισχύς, μνήμη) ώστε να παρεμποδίζεται η όποια παρεχόμενη υπηρεσία*



ΥΠΟΚΛΟΠΗ ΚΛΗΣΕΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

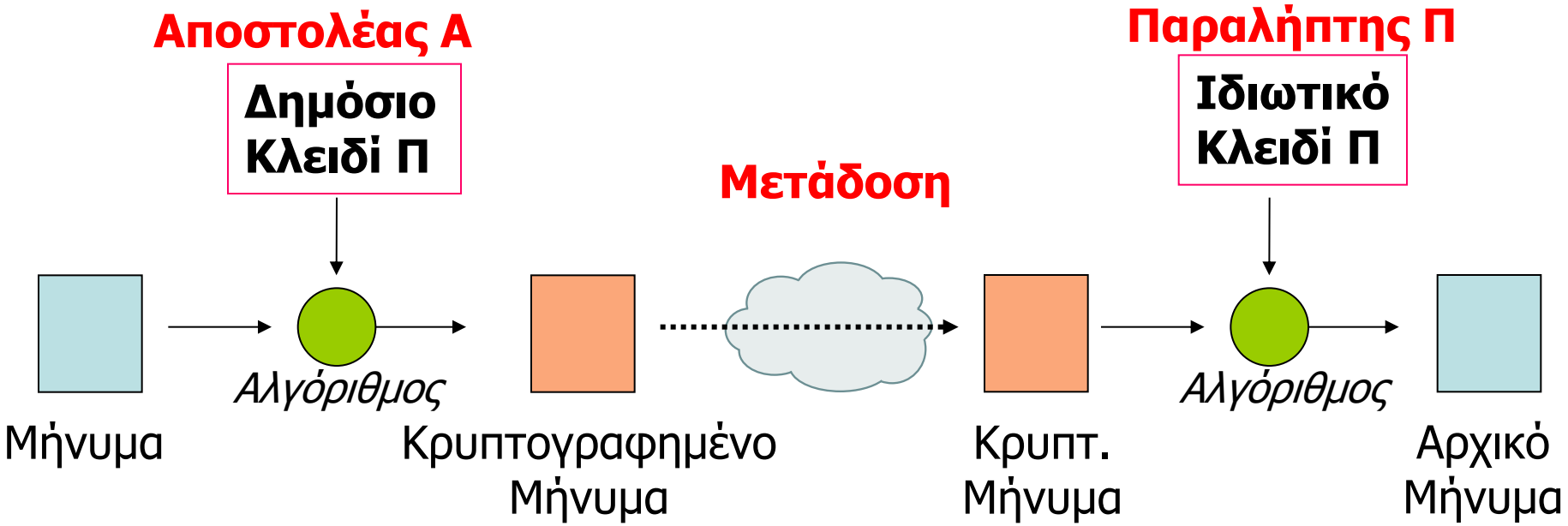
GSM Man-in-the Middle Attack (*Επανάληψη*)



A5/1-3: Αλγόριθμοι Κρυπτογράφησης Συνδιαλέξεων **GSM** – Σταθμός Βάσης ⇔ Κινητό Τηλέφωνο
Εξέλιξη **GSM** → **UMTS**, **LTE**: Αυθεντικοποίηση Σταθμού Βάσης σε συσκευή Κινητού Τηλέφωνου
(προβλήματα μετάβασης, downward compatibility με GSM;)

ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ:
Confidentiality

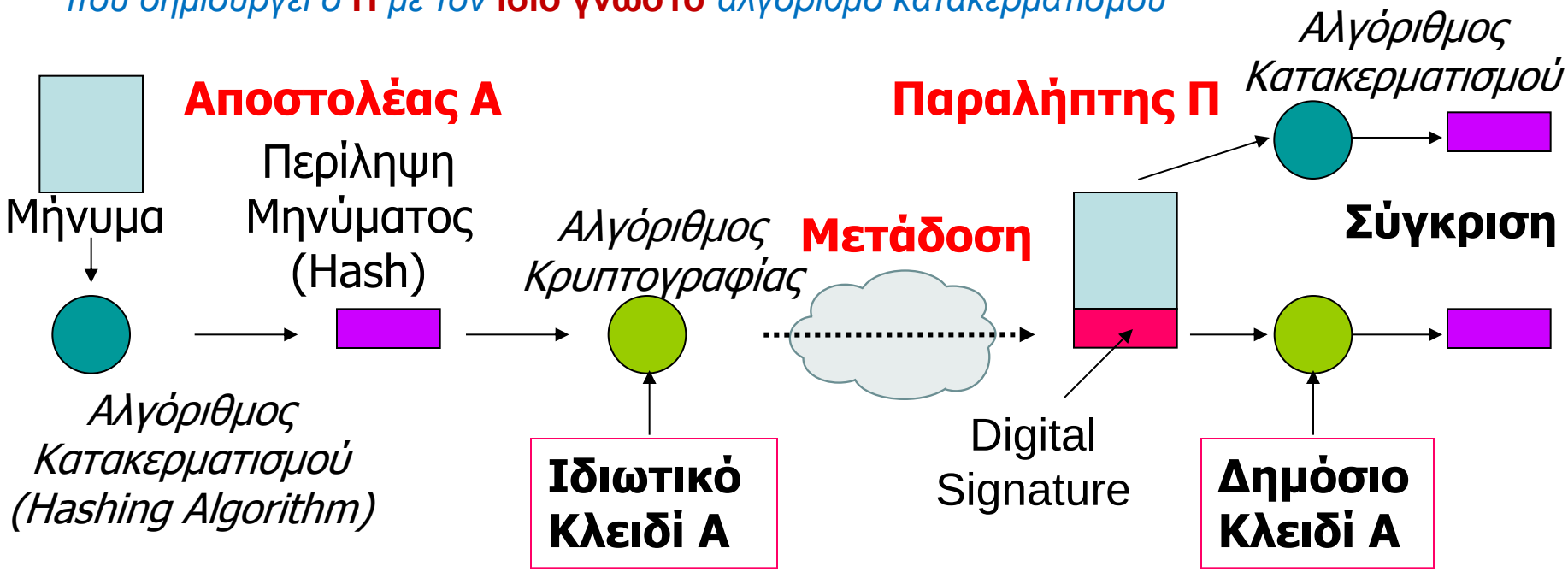
- Ο Αποστολέας **Α** γνωρίζει το **Δημόσιο Κλειδί** του Παραλήπτη **Π** (π.χ. με Ψηφιακό Πιστοποιητικό από Certification Authority **CA**, self-signed ή υπογραμμένο από 3ης έμπιστη οντότητα – Third Trusted Party **TTP**, στα πλαίσια Υποδομής Δημοσίου Κλειδιού - **Public Key Infrastructure PKI**)
  - *Κρυπτογράφηση στον* **Α:** *Με το* **Δημόσιο Κλειδί** *του* **Π**
  - *Αποκρυπτογράφηση στον* **Π:** *Με το* **Ιδιωτικό Κλειδί** *του* Π



ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ:

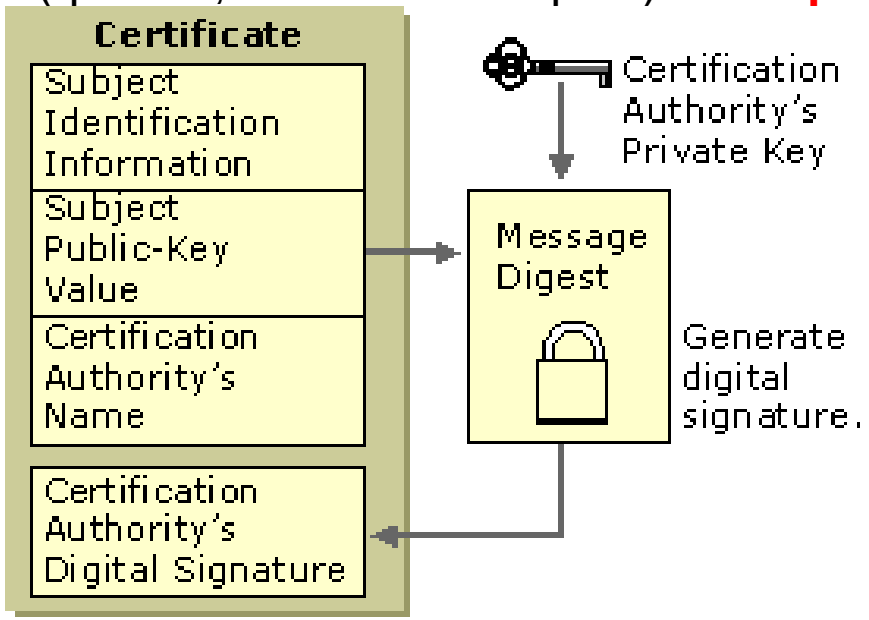
Sender Authentication / Non Repudiation – Message Integrity

- Οι Αποστολέας **Α** και Παραλήπτης **Π** κατέχουν ζεύγη Δημοσίου & Ιδιωτικού Κλειδιού και έχουν αμοιβαία γνώση των **Δημοσίων Κλειδιών** & αλγορίθμων κρυπτογράφησης - κατακερματισμού
- Ο Αποστολέας **Α** προσθέτει Ψηφιακή Υπογραφή (**Digital Signature**) στο μήνυμα με κρυπτογράφηση με το Ιδιωτικό του κλειδί περίληψης (**hash**) του μηνύματος που προκύπτει με αλγόριθμο κατακερματισμού (**hashing algorithm**)
- Ο Παραλήπτης **Π** επιβεβαιώνει (**authenticate**) την ταυτότητα του **Α**, χωρίς δυνατότητά του **Α** άρνησης της αποστολής (**non-repudiation**) & επιβεβαιώνει την μη αλλοίωση του μηνύματος (**message integrity**) με βάση την σύγκριση:
  - *Ψηφιακής Υπογραφής, αποκρυπτογραφημένης στον* **Π** *με το* **γνωστό** *Δημόσιο Κλειδί του* **Α**
  - *Νέας περίληψης του ληφθέντος* (**μη κρυπτογραφημένου, clear text**) *κυρίως μηνύματος που δημιουργεί ο* **Π** *με τον* **ίδιο γνωστό** *αλγόριθμο κατακερματισμού*



ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ X.509

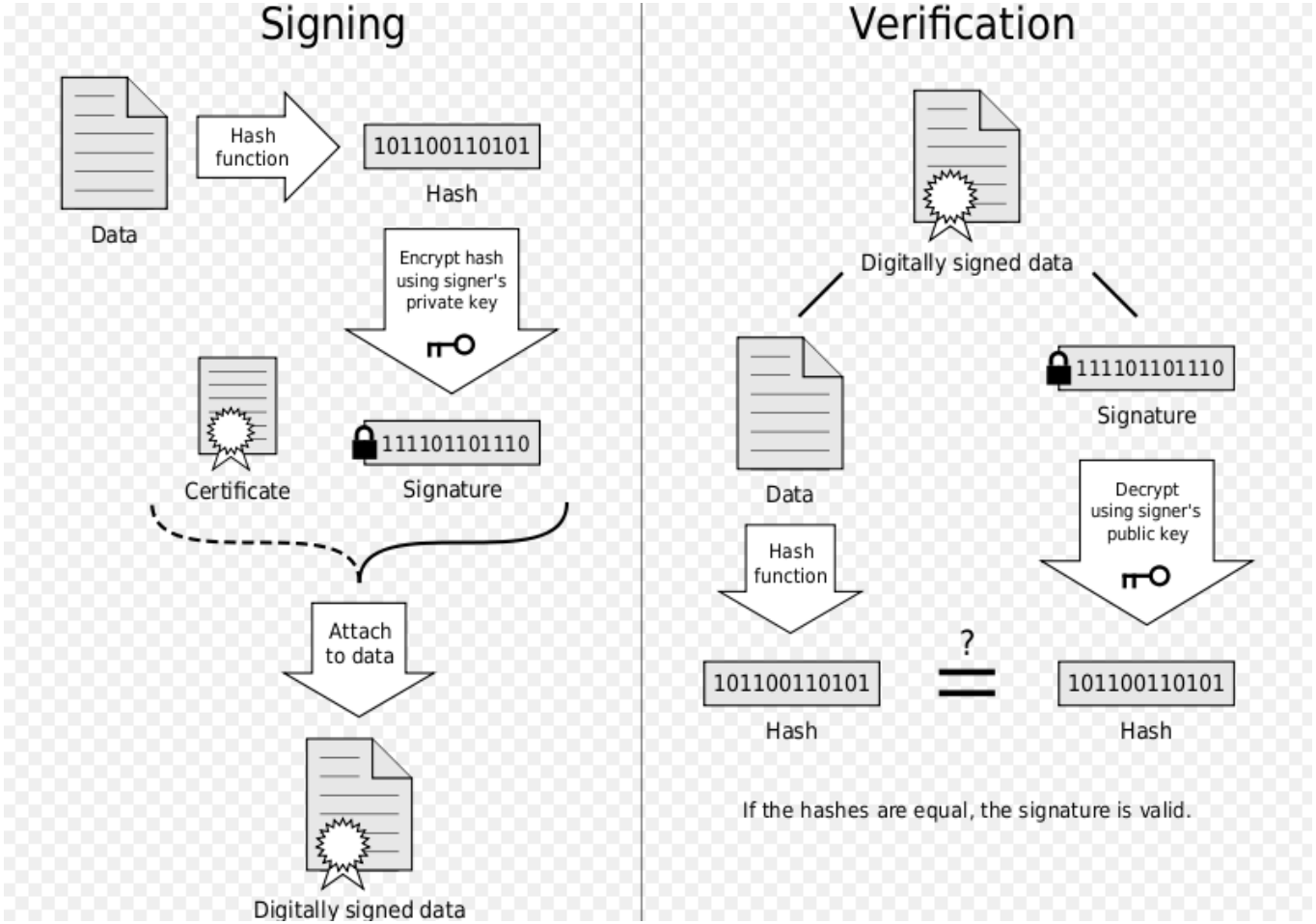
- Αν συνοδεύουν υπογραμμένο μήνυμα, βεβαιώνουν τη γνησιότητα του **Δημοσίου Κλειδιού** του αποστολέα (subject) κατά μια Τρίτη Έμπιστη Οντότητα **TTP - Third Trusted Party**: Την Αρχή Πιστοποίησης, **Certification Authority – CA**
- **Μη Κρυπτογραφημένα Πεδία Ψηφιακού Πιστοποιητικού**: Πληροφορίες για τον αποστολέα (subject) μηνύματος (**ID**, **Public Key**,…) και της **CA**
- **Κρυπτογραφημένο Πεδίο**: Ψηφιακή Υπογραφή Πιστοποιητικού από **CA**
- Η **CA** υπογράφει με το **Ιδιωτικό Κλειδί** της. Το **Δημόσιο Κλειδί** της πρέπει να είναι γνωστό στους παραλήπτες (π.χ. ενσωματωμένο στον Web Browser) ή αποδεκτό λόγω σχέσης εμπιστοσύνης (π.χ. σε περιπτώσεις **Self-Signed CA**)
- Αν χρειάζεται και έλεγχος του **Δημοσίου Κλειδιού** της **CA**, μπορεί να αποστέλλεται και 2ο (ή και 3ο, 4ο …πιστοποιητικό) από **ιεραρχικά δομημένες CA**



https://technet.microsoft.com/en-us/library/cc962029.aspx

ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

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



ΜΕΙΚΤΟ ΣΥΣΤΗΜΑ ΑΣΦΑΛΟΥΣ ΠΡΟΣΒΑΣΗΣ

(SSL/TLS - Secure Sockets Layer / Transport Layer Security)

- **1η Φάση: Handshaking**
  - Ο χρήστης (User) **U** λαμβάνει γνώση του **Δημοσίου Κλειδιού** του εξυπηρετητή (Server) **S** με Ψηφιακό Πιστοποιητικό από Certification Authority **CA** self-signed ή υπογραμμένο από 3ης έμπιστη οντότητα – Third Trusted Party **TTP**, στα πλαίσια αρχιτεκτονικής **Public Key Infrastructure PKI**
  - Ο **U** δημιουργεί Κοινό **Συμμετρικό Κλειδί** με τυχαίο αλγόριθμο και το κοινοποιεί στον **S** κρυπτογραφημένο με το **Δημόσιο Κλειδί** του **S**
- **2η Φάση: Κρυπτογραφημένος Διάλογος με Κοινό Συμμετρικό Κλειδί**
  - Γρήγορη συμμετρική κρυπτογραφία σε **Secure Channel** μεταξύ **S – U** (το Συμμετρικό Κλειδί ισχύει μόνο για το συγκεκριμένο session)
- **ΠΑΡΑΤΗΡΗΣΗ:**
  - Ο **U** δεν απαιτείται να έχει Πιστοποιητικό με **Δημόσιο Κλειδί** (ψηφιακή υπογραφή), μόνο ο **S** έχει Πιστοποίηση μέσω TTP ή self-signed (**Server Based Authentication**)
  - Για Ταυτοποίηση – Εξουσιοδότηση του **U** από τον **S** (**Client & Server Based Authentication**) απαιτείται μετάδοση από το secure channel της **Digital Identity** του Client (συνήθως **User_Name/Password** ή **Client Certificates** αν υπάρχουν) → έλεγχος στον **S** σε Βάση Δεδομένων Χρηστών (με πρωτόκολλο **LDAP - TCP** για εφαρμογές Web, Mail… ή με πρωτόκολλο **RADIUS - UDP** αν μεσολαβεί **Remote Access Server** π.χ. για πρόσβαση σε υπηρεσία DSL, WiFi roaming…)

ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΧΡΗΣΤΗ, AAI Single Sign-On, ΠΑΡΟΧΟΙ ΤΑΥΤΟΤΗΤΑΣ IdP

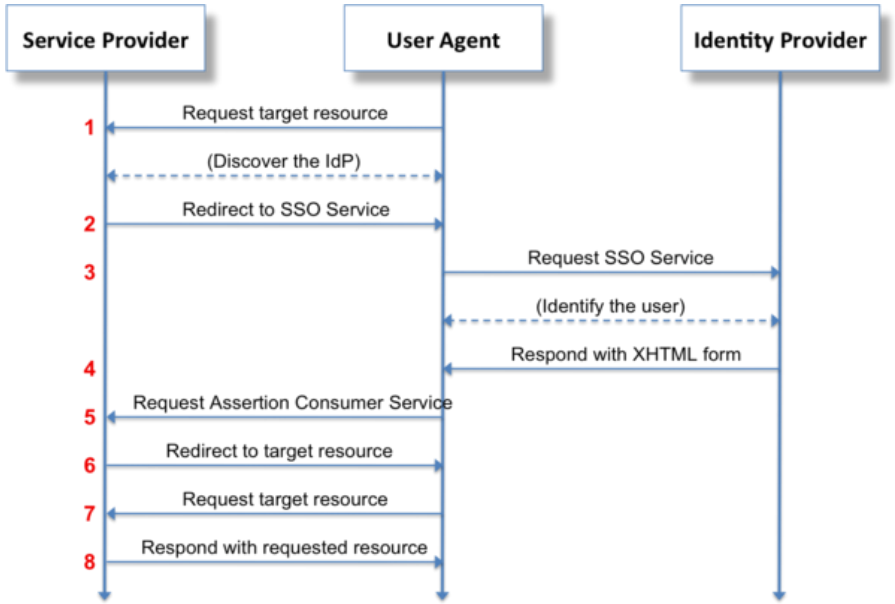
AAI – Authentication & Authorization Infrastructure

- Ταυτοποίηση (**Authentication**) & Εξουσιοδότηση (**Authorization**) χρήστη με:
  - Username, Password
  - LDAP Server (Lightweight Directory Access Protocol)
  - RADIUS (Remote Authentication Dial-In User Service)
  - Active Directory (MS Windows)
- Οι Υποδομές Ταυτοποίησης & Εξουσιοδότησης (**AAI**) επιτρέπουν πρόσβαση **Single Sign-On (SSO)** σε χρήστες διαδικτυακών πόρων κατανεμημένων σε παρόχους με αμοιβαία εμπιστοσύνη:
  - Ταυτοποίηση (Authentication) μια φορά
  - Εξουσιοδότηση (Authorization) ξεχωριστά με κάθε πάροχο
- Μεσολάβηση Παρόχου Ταυτότητας (**Identity Provider - IdP**) π.χ. **Facebook, Twitter, Google User Accounts** για
  - Εξουσιοδότηση Single Sign-On σε υπηρεσίες με σχετικό security token συνδρομητή από IdP σε **Service Providers** που το εμπιστεύονται (π.χ. **OAuth** – Open standard for Authorization**,** **SAML** - Security Assertion Markup Language)
  - Επιβεβαίωση Ισχυρισμών Ταυτότητας (**Identity Assertion**) από **WAYF** (Where Are You From) servers μέσω πρωτοκόλλου **SAML** ή από **LDAP** servers με πιστοποιητικά **X509**
- Συνέργεια **IdP** σε ομόσπονδα σχήματα **AAI** (π.χ. US Internet2 **Shibboleth**, GÉANT **eduGAIN**)

ΡΟΗ SAML ΓΙΑ ΠΡΟΣΒΑΣΗ Single Sign-On (SSO)

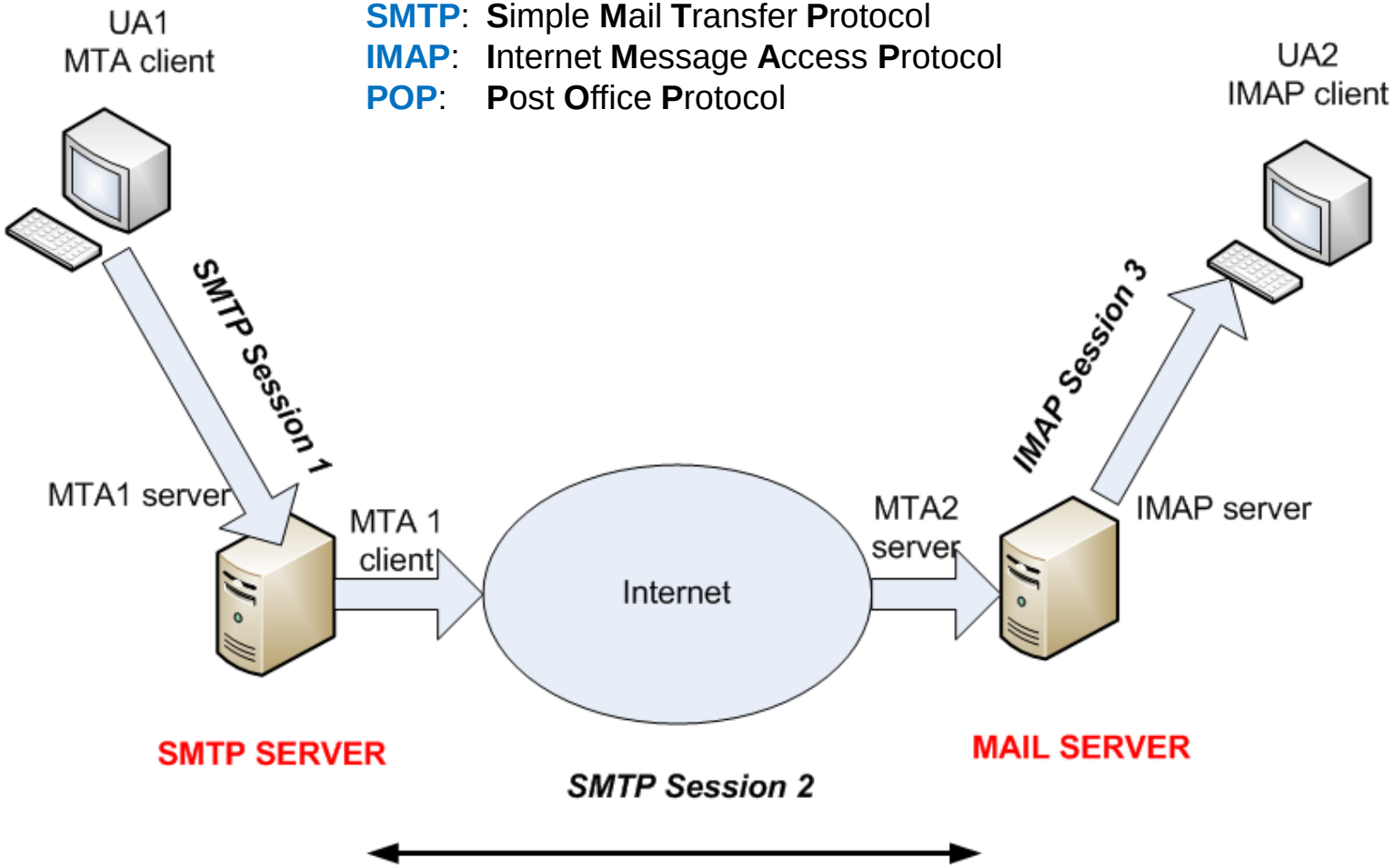
https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

- Ρόλοι οριζόμενοι στο πρότυπο **SAML** (OASIS Standard):
  - Τελικός χρήστης (Principal User, **P**)
  - Πάροχος Υπηρεσιών (Service Provider, **SP**)
  - Πάροχος Ταυτότητας (Identity Provider, **IdP**)
- SAML:
  - Μηχανισμός Επιβεβαίωσης Ισχυρισμών Ταυτοποίησης & Εξουσιοδότησης (**Authentication & Authorization Assertions**) Τελικού Χρήστη (**P**) προς Πάροχο Υπηρεσιών (**SP**) με την βοήθεια Παρόχων Ταυτότητας (**IdP**)
  - Ανταλλαγής μηνυμάτων SAML μεταξύ **P** (User Agent), **SP**, **IdP**: Με φόρμες **XML** (για σιγουριά προστατευμένες από πρωτόκολλα TLS και XML encryption)



ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ (1/3)

UA: **U**ser **A**gent
MTA: **M**essage **T**ransfer **A**gent
SMTP: **S**imple **M**ail **T**ransfer **P**rotocol
IMAP: **I**nternet **M**essage **A**ccess **P**rotocol
POP: **P**ost **O**ffice **P**rotocol



ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ (2/3)

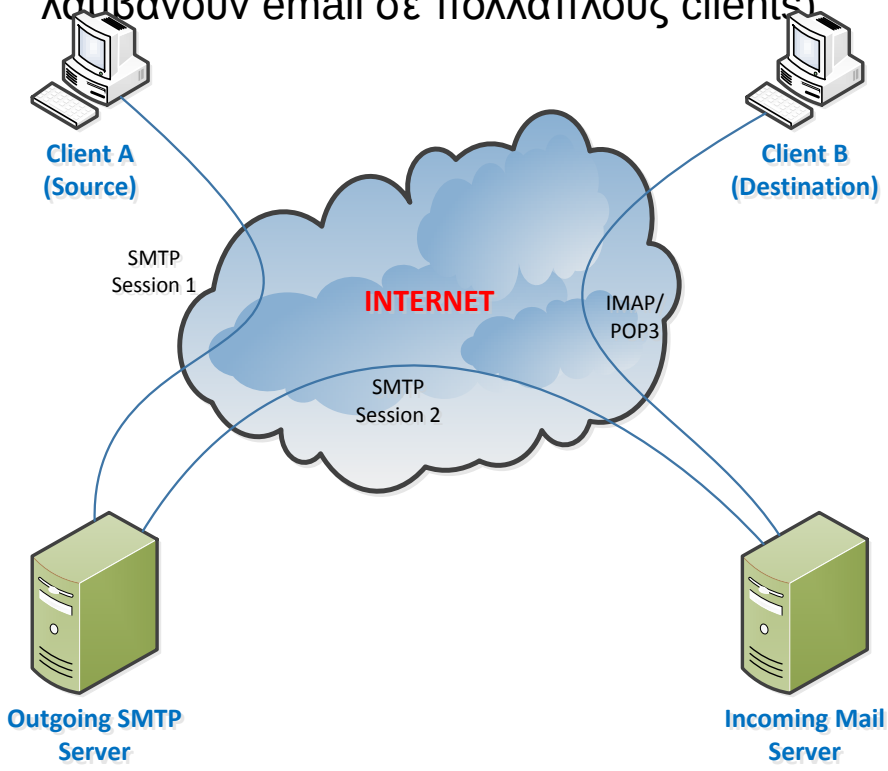
- **UA 1 → MTA 1 (Session 1)**
  - User Agent → Message Transfer Agent
  - SMTP (TCP Session 1)
  - Δυνατότητα SSL/TLS security
- **MTA 1 → MTA 2 (Session 2)**
  - SMTP (TCP Session 2)
  - Δυνατότητα κρυπτογράφησης (αν υποστηρίζεται από το Mail S/W – π.χ. sendmail)
- **MTA 2 (Mail Server) → UA 2 (Session 3)**
  - Πρωτόκολλα POP/IMAP (TCP Session 3)
  - Δυνατότητα SSL/TLS

ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ (3/3)

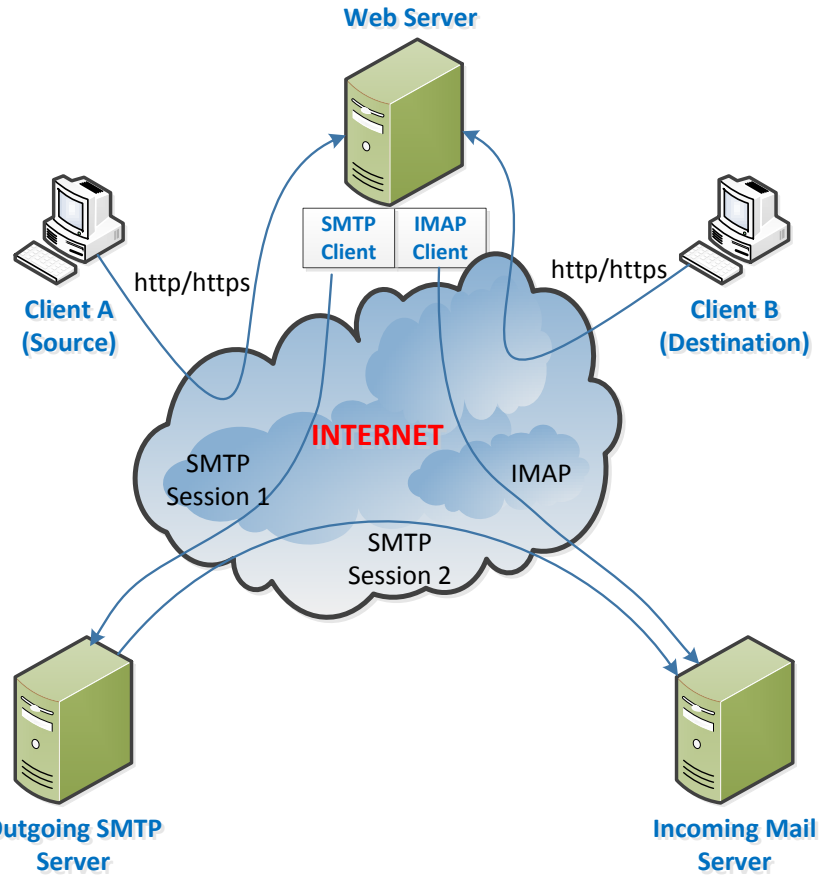
Σχήμα με IMAP/POP3 Clients
(Outlook, Thunderbird, Fedora…)

IMAP: Κρατάει αντίγραφα emails και συντηρεί mail folders των users στον server

POP3: Δεν κρατάει αντίγραφα emails στον server αφού διώξει τα emails στον client (πρόβλημα για χρήστες που λαμβάνουν email σε πολλαπλούς clients)



Παράδειγμα Web Mail



ΣΥΣΤΗΜΑΤΑ ΔΙΚΤΥΑΚΗΣ ΠΡΟΣΤΑΣΙΑΣ (1/3)
Firewalls

- Τι είναι ένα **Firewall**:
  Ένα σύστημα ή συνδυασμός συστημάτων που ελέγχουν την πρόσβαση και παρέχουν έναν βαθμό ασφάλειας μεταξύ δικτύων, ***Marcus J. Ranum***, δημιουργός του πρώτου firewall

- Λειτουργία
  - Δρομολογητής που ελέγχει την κίνηση (Screening router / Bastion Host). Μπορεί να συνδυαστεί με την ύπαρξη ιδιωτικών εσωτερικών διευθύνσεων και μετάφραση στο σύνορο (**NAT** - Network Address Translation).
  - Ο πιο απλός Firewall είναι ο δρομολογητής (router) με σωστά στημένες Access Lists (**ACLs**)

- Για να χρησιμοποιήσουμε Firewall χρειάζεται να σχεδιαστεί κατάλληλα το δίκτυο, σύμφωνα με τις πολιτικές ασφαλείας

ΣΥΣΤΗΜΑΤΑ ΔΙΚΤΥΑΚΗΣ ΠΡΟΣΤΑΣΙΑΣ (2/3)
Firewalls

- Βασικοί κανόνες

  <RuleGroup>

  <Action> Deny ή Allow

  <Protocol> IP, TCP, UDP, ICMP, κ.λπ.

  <SrcPort> <DstPort>

  <SrcIP> <SrcMask> Πηγή - Ξεχωριστές διευθύνσεις IP ή ομαδοποιήσεις τους

  <DstIP> <DstMask> Προορισμός

- Παράδειγμα από δρομολογητή Cisco:

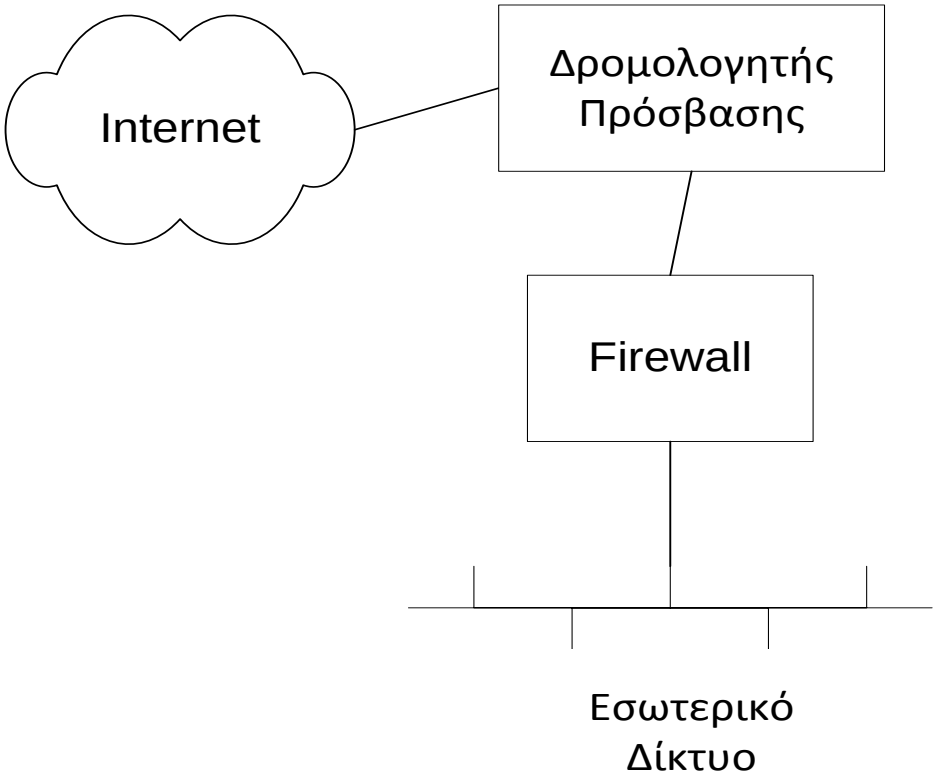
```
access-list 100 permit tcp any host 171.16.23.1 eq 80
```

- Οι σύγχρονες Firewall έχουν πολλά επιπλέον χρήσιμα χαρακτηριστικά:
  - Γραφικό περιβάλλον
  - Ορισμό ομάδων κανόνων
  - Ορισμό περιοχών προστασίας και ομάδων χρηστών
  - Διαδικασία ενημέρωσης κανόνων μέσω εξυπηρετητών και σύμφωνα με τις εταιρικές πολιτικές ασφαλείας κ.λπ.

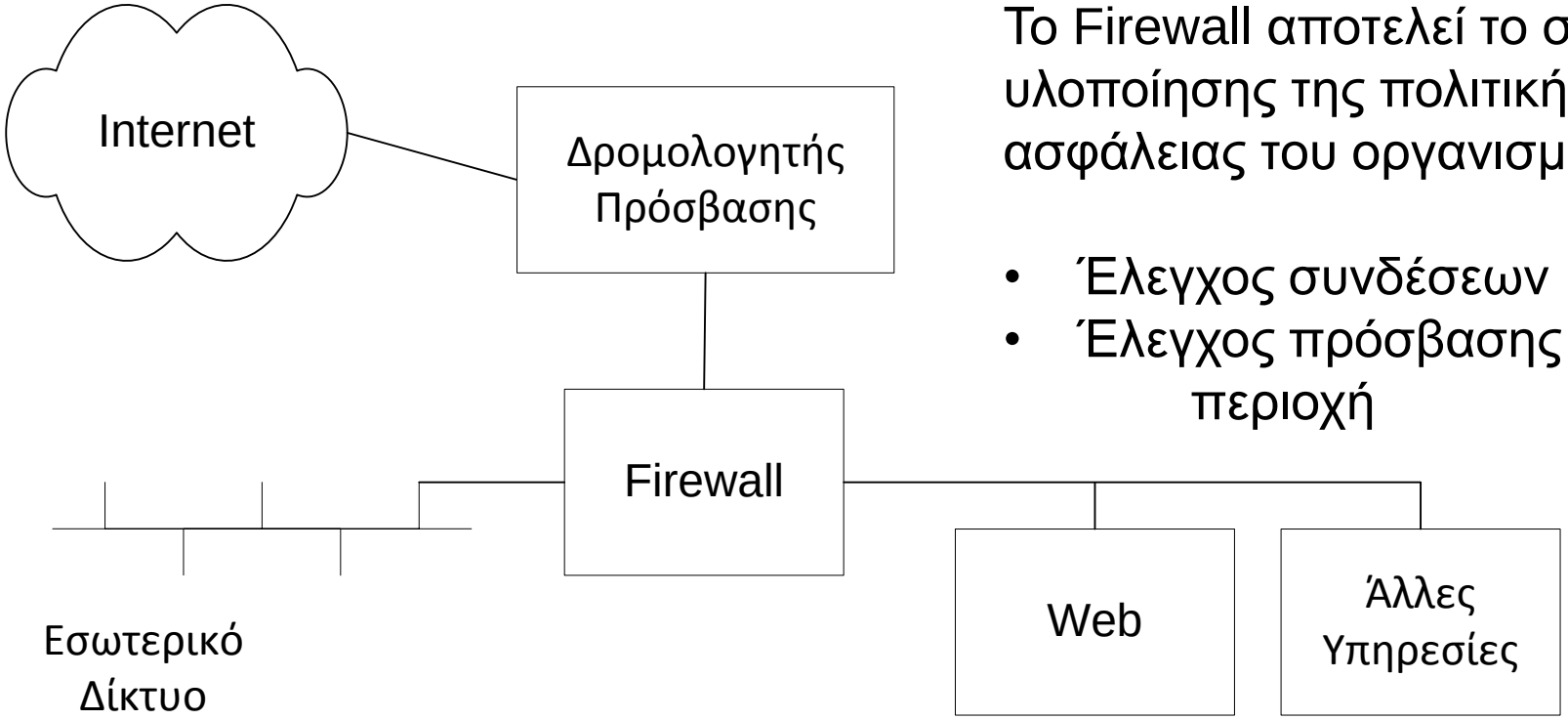
ΣΥΣΤΗΜΑΤΑ ΔΙΚΤΥΑΚΗΣ ΠΡΟΣΤΑΣΙΑΣ (3/3)
Firewalls

- Πολιτικές πρόσβασης
  - Απαγόρευση όλων των συνδέσεων πλην εξαιρέσεων ("Deny unless allowed") – χρησιμοποιείται για ισχυρή προστασία, συνήθως στην εισερχόμενη κίνηση ενός δικτύου
  - Διέλευση όλων πλην εξαιρέσεων ("Allow unless denied") – δίνει μεγαλύτερη ελευθερία
  - Επιπλέον δυνατότητες:
    - Διέλευση κίνησης που έχει ήδη ολοκληρώσει το TCP Three Way Handshake (Established)
    - Απαγόρευση πακέτων που δεν έχουν τις προβλεπόμενες διευθύνσεις προέλευσης (προστασία από το spoofing)

ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ - Firewalls (1/3)



ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ - Firewalls (2/3)



Το Firewall αποτελεί το σημείο υλοποίησης της πολιτικής ασφάλειας του οργανισμού:

- Έλεγχος συνδέσεων
- Έλεγχος πρόσβασης ανά περιοχή

"Αποστρατικοποιημένη Ζώνη"
Demilitarized Zone - DMZ
Παρέχει αυξημένη πρόσβαση σε κάποια συστήματα του δικτύου χωρίς να θέτει σε κίνδυνο το υπόλοιπο

ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ - Firewalls (3/3)

Το Firewall υλοποιεί πολιτικές πρόσβασης ανάμεσα στα διάφορα τμήματα του οργανισμού