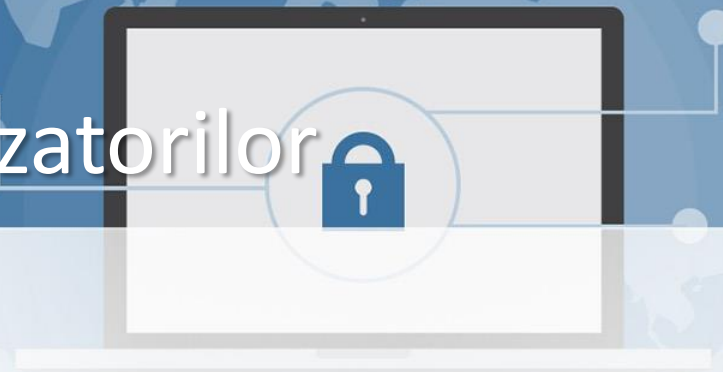
# Criptografie și Securitate Cibernetică

RCC - CSC 4

# Conținut

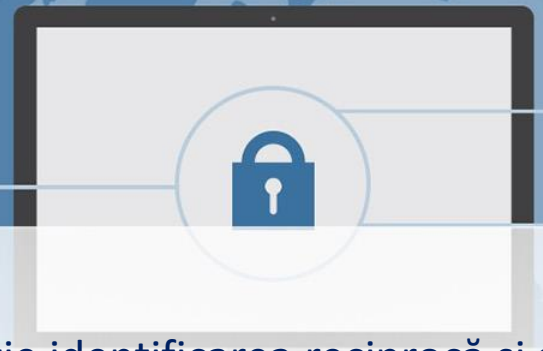
- Autentificarea utilizatorilor
  - Principii de autentificare
  - Autentificarea prin sisteme criptografice simetrice
  - Serviciu de autentificare (Kerberos)
  - Autentificarea prin sisteme criptografice asimetrice
  - Administrarea identității
- Controlul accesului la rețea
  - Elemente de controlul accesului la rețea
  - Metode de autentificare
  - Protocolul EAP
  - Controlul accesului la nivel Legătură de date (802.1X)
  - Concepte de cloud computing
  - Protecția datelor in cloud

# Autentificarea utilizatorilor



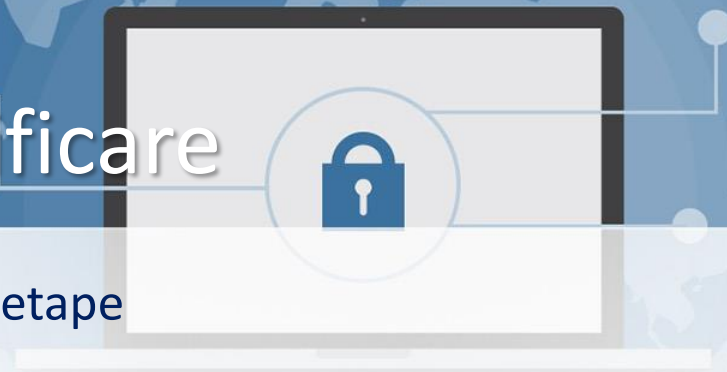
- Principii de autentificare
- Autentificarea prin sisteme criptografice simetrice
- Serviciu de autentificare (Kerberos)
- Autentificarea prin sisteme criptografice asimetrice
- Administrarea identității

# Autentificarea



- Protocoalele de autentificare
  - permit entităților dintr-o comunicație identificarea reciprocă și schimbul de chei de sesiune
- Serviciu de autentificare (ex. Kerberos)
  - este conceput pentru a fi utilizat într-un sistem de comunicație distribuit.
  - oferit printr-o terță parte de încredere care permite clienților și serverelor stabilirea de comunicații autentice
- Administrarea/managementul identității
  - o abordare centralizată, automată, pentru a oferi acces persoanelor autorizate
  - federalizarea identității, extinderea gestionării identității la domenii de securitate multiple.

# Principii de autentificare

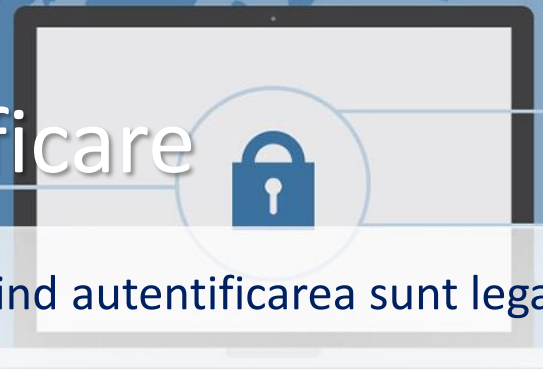


- Procesul de autentificare are 2 etape
  - Identificarea

    prezentarea unui identificator către sistemul de securitate
  - Verificarea

    prezentarea sau generarea informației de autentificare care permite realizarea legăturii dintre entitate și identificator
- Mijloace generale de certificare a identității
  - Elemente cunoscute de utilizatori (parolă, PIN, răspuns)
  - Elemente deținute de utilizatori (cheie, token, smart card)
  - Elementele biometrice statice (amprentă, retină, față)
  - Elementele biometrice dinamice (amprentă vocală, scris)

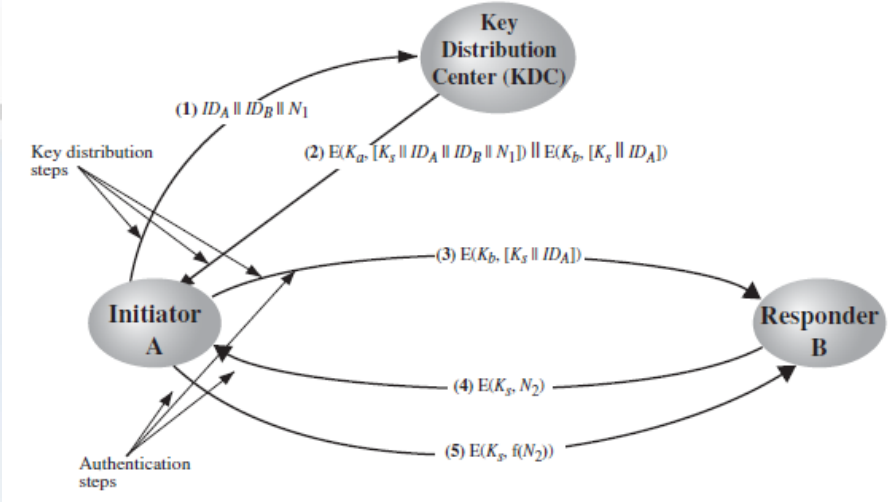
# Probleme de autentificare



- Principalele probleme privind autentificarea sunt legate de
  - Confidențialitate
    - elementele de identificare importante precum și cheile de sesiune trebuie transmise criptat
    - existența cheilor publice/private
  - Actualitatea informației
    - evitarea reluării/repetării mesajelor
    - repetarea mesajelor poate duce la compromiterea cheilor sesiune sau impersonalizarea cu succes a altei parți
  - Atacuri
    - prin reluarea mesajelor (copierea și reluarea mesajelor)
  - Autentificarea într-un singur sens
    - sistemul de poștă electronică (email)

# Autentificarea prin sisteme criptografice simetrice

- Autentificarea reciprocă
  - Ierarhie de cei simetrice
    - (sesiune, master)
  - Centre de distribuire a cheilor de securitate
    - servere pentru generarea cheilor sesiune (durată limitată)
    - distribuirea cheilor sesiune folosind chei master




1. $A \rightarrow KDC$: $ID_A \| ID_B \| N_1$
2. $KDC \rightarrow A$: $E(K_a, [K_s \| ID_B \| N_1 \| E(K_b, [K_s \| ID_A])])$
3. $A \rightarrow B$: $E(K_b, [K_s \| ID_A])$
4. $B \rightarrow A$: $E(K_s, N_2)$
5. $A \rightarrow B$: $E(K_s, f(N_2))$

# Prevenire atacuri

- Prevenirea atacului prin reluarea mesajelor

1. $A \rightarrow KDC: \quad ID_A \| ID_B \| N_1$
2. $KDC \rightarrow A: \quad E(K_a, [K_s \| ID_B \| N_1 \| E(K_b, [K_s \| ID_A])])$
3. $A \rightarrow B: \quad E(K_b, [K_s \| ID_A])$
4. $B \rightarrow A: \quad E(K_s, N_2)$
5. $A \rightarrow B: \quad E(K_s, f(N_2))$

1. $A \rightarrow KDC: \quad ID_A \| ID_B$
2. $KDC \rightarrow A: \quad E(K_a, [K_s \| ID_B \| T \| E(K_b, [K_s \| ID_A \| T])])$
3. $A \rightarrow B: \quad E(K_b, [K_s \| ID_A \| T])$
4. $B \rightarrow A: \quad E(K_s, N_1)$
5. $A \rightarrow B: \quad E(K_s, f(N_1))$

Actualitatea informației poate fi verificată

$$|\text{Clock} - T| < \Delta t_1 + \Delta t_2$$

$\Delta t_1$ - diferența dintre ceasul local și al centrului

$\Delta t_2$ - întârzierea la nivelul rețelei

# Prevenire atacuri (2)

- Reluarea mesajelor în cazul desincronizării ceasurilor

1. A → B: $ID_A \| N_a$
2. B → KDC: $ID_B \| N_b \| \mathrm{E}(K_b, [ID_A \| N_a \| T_b])$
3. KDC → A: $\mathrm{E}(K_a, [ID_B \| N_a \| K_s \| T_b]) \| \mathrm{E}(K_b, [ID_A \| K_s \| T_b]) \| N_b$
4. A → B: $\mathrm{E}(K_b, [ID_A \| K_s \| T_b]) \| \mathrm{E}(K_s, N_b)$

Un nou mesaj, in fereastra de timp corespunzătoare

1. A → B: $\mathrm{E}(K_b, [ID_A \| K_s \| T_b]) \| N'_a$
2. B → A: $N'_b \| \mathrm{E}(K_s, N'_a)$
3. A → B: $\mathrm{E}(K_s, N'_b)$

Autentificarea într-un singur sens
(sistem de poștă electronică securizat)

1. A → KDC: $ID_A \| ID_B \| N_1$
2. KDC → A: $\mathrm{E}(K_a, [K_s \| ID_B \| N_1 \| \mathrm{E}(K_b, [K_s \| ID_A])])$
3. A → B: $\mathrm{E}(K_b, [K_s \| ID_A]) \| \mathrm{E}(K_s, M)$

# Kerberos

- Kerberos
  - Dezvoltat la Universitatea MIT (http://web.mit.edu/kerberos/)
  - Network Authentication Protocol
  - Serviciu de autentificare în rețea bazat pe o terță parte sigură
  - Folosește un sistem bazat pe criptografia simetrică
  - Exista 2 versiuni folosite curent
    - Kerberos 4
    - Kerberos 5
  - Specificații
    - Securizare (previne intruziunile și impersonalizarea)
    - Sigur (disponibilitatea trebuie sa fie permanentă)
    - Transparent (utilizatorul nu sesizează procedurile specifice)
    - Scalabil (număr mare de servere și clienți, arhitectură modulară)

# Mesaje de autentificare

- Versiunea 4 Kerberos
  - Se bazează pe DES (*Data Encryption Standard* )
  - Dialog simplu de autentificare Kerberos

(1) C → AS: $ID_C \| P_C \| ID_V$

(2) AS → C: $Ticket$

(3) C → V: $ID_C \| Ticket$

$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$

C = client
AS = authentication server
V = server
$ID_C$ = identifier of user on C
$ID_V$ = identifier of V
$P_C$ = password of user on C
$AD_C$ = network address of C
$K_v$ = secret encryption key shared by AS and V

# Dialog de autentificare securizat

- Probleme
  - Solicitare de tichete pentru fiecare serviciu
  - Introducerea de fiecare data a parolei
  - Parole transmise in clar
- Soluție
  - Server intermediar

  TGS (Ticket-Granting Server)
  - acordarea tichetelor

**Once per user logon session:**

(1) $C \rightarrow AS$: $ID_C \| ID_{tgs}$

(2) $AS \rightarrow C$: $E(K_c, Ticket_{tgs})$

**Once per type of service:**

(3) $C \rightarrow TGS$: $ID_C \| ID_V \| Ticket_{tgs}$

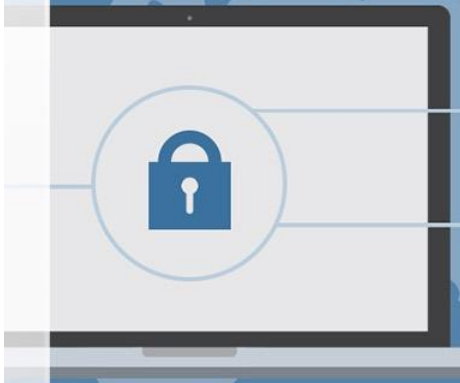
(4) $TGS \rightarrow C$: $Ticket_v$

**Once per service session:**

(5) $C \rightarrow V$: $ID_C \| Ticket_v$

$$Ticket_{tgs} = E(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$$
$$Ticket_v = E(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$$

# Mesaje Kerberos 4



(1) $\mathbf{C} \rightarrow \mathbf{AS}$ $ID_c \| ID_{tgs} \| TS_1$

(2) $\mathbf{AS} \rightarrow \mathbf{C}$ $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$$

**(a) Authentication Service Exchange to obtain ticket-granting ticket**

(3) $\mathbf{C} \rightarrow \mathbf{TGS}$ $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) $\mathbf{TGS} \rightarrow \mathbf{C}$ $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$$

$$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$$

$$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$$

**(b) Ticket-Granting Service Exchange to obtain service-granting ticket**

(5) $\mathbf{C} \rightarrow \mathbf{V}$ $Ticket_v \| Authenticator_c$

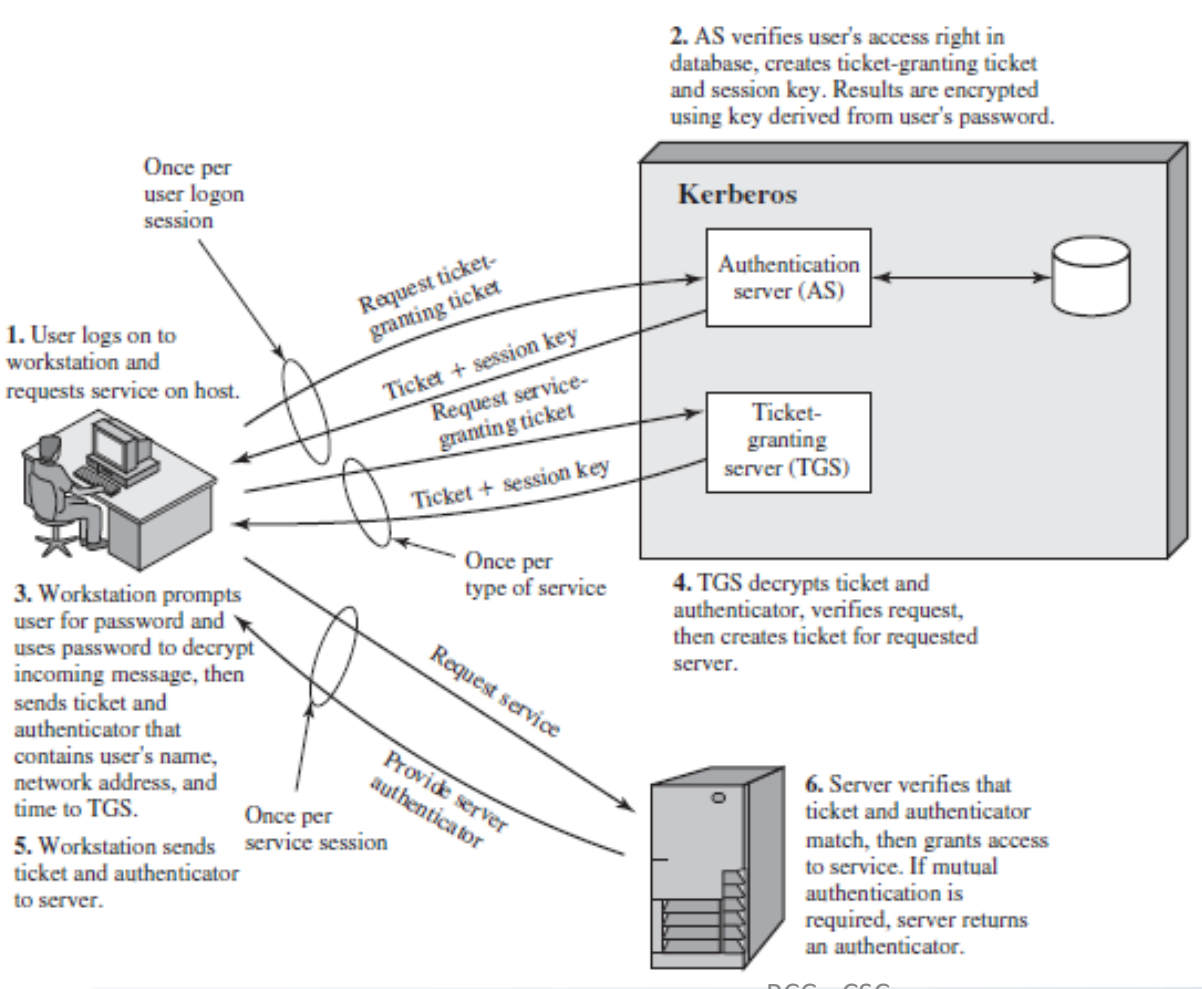
(6) $\mathbf{V} \rightarrow \mathbf{C}$ $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$$

$$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$$

**(c) Client/Server Authentication Exchange to obtain service**

# Diagrama kerberos



# Mesaje Kerberos 5

(1) $C \rightarrow AS$ $\quad Options \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) $AS \rightarrow C$ $\quad Realm_C \| ID_C \| Ticket_{tgs} \| E(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

**(a) Authentication Service Exchange to obtain ticket-granting ticket**

(3) $C \rightarrow TGS$ $\quad Options \| ID_v \| Times \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) $TGS \rightarrow C$ $\quad Realm_c \| ID_C \| Ticket_v \| E(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

$$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$$

$$Authenticator_c = E(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$$

**(b) Ticket-Granting Service Exchange to obtain service-granting ticket**

(5) $C \rightarrow V$ $\quad Options \| Ticket_v \| Authenticator_c$

(6) $V \rightarrow C$ $\quad E_{K_{c,v}}[TS_2 \| Subkey \| Seq\#]$

$$Ticket_v = E(K_v, [Flag \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$$

$$Authenticator_c = E(K_{c,v}, [ID_C \| Relam_c \| TS_2 \| Subkey \| Seq\#])$$

**(c) Client/Server Authentication Exchange to obtain service**

# Autentificarea prin sisteme criptografice asimetrice

- Autentificarea reciprocă

1. $A \rightarrow AS: \quad ID_A \| ID_B$
2. $AS \rightarrow A: \quad E(PR_{as}, [ID_A \| PU_a \| T]) \| E(PR_{as}, [ID_B \| PU_b \| T])$
3. $A \rightarrow B: \quad E(PR_{as}, [ID_A \| PU_a \| T]) \| E(PR_{as}, [ID_B \| PU_b \| T]) \| E(PU_b, E(PR_a, [K_s \| T]))$

Soluție care nu necesită sincronizare de ceas

1. $A \rightarrow KDC: \quad ID_A \| ID_B$
2. $KDC \rightarrow A: \quad E(PR_{auth}, [ID_B \| PU_b])$
3. $A \rightarrow B: \quad E(PU_b, [N_a \| ID_A])$
4. $B \rightarrow KDC: \quad ID_A \| ID_B \| E(PU_{auth}, N_a)$
5. $KDC \rightarrow B: \quad E(PR_{auth}, [ID_A \| PU_a]) \| E(PU_b, E(PR_{auth}, [N_a \| K_s \| ID_B]))$
6. $B \rightarrow A: \quad E(PU_a, [E(PR_{auth}, [(N_a \| K_s \| ID_B)]) \| N_b])$
7. $A \rightarrow B: \quad E(K_s, N_b)$

# Soluție îmbunătățită

Adăugarea identificatorului A (pas 5 și 6)

1. $A \rightarrow KDC: \quad ID_A \| ID_B$
2. $KDC \rightarrow A: \quad E(PR_{auth}, [ID_B \| PU_b])$
3. $A \rightarrow B: \quad E(PU_b, [N_a \| ID_A])$
4. $B \rightarrow KDC: \quad ID_A \| ID_B \| E(PU_{auth}, N_a)$
5. $KDC \rightarrow B: \quad E(PR_{auth}, [ID_A \| PU_a]) \| E(PU_b, E(PR_{auth}, [N_a \| K_s \| ID_A \| ID_B]))$
6. $B \rightarrow A: \quad E(PU_a, [E(PR_{auth}, [(N_a \| K_s \| ID_A \| ID_B) \| N_b]))$
7. $A \rightarrow B: \quad E(K_s, N_b)$

# Autentificarea prin sisteme criptografice asimetrice

- Autentificarea unidirecțională

Mesaj criptat cu o cheie de unică utilizare

$$A \rightarrow B: \quad E(PU_b, K_s) \| E(K_s, M)$$

Dacă se urmărește în primul rând autentificarea

$$A \rightarrow B: \quad M \| E(PR_a, H(M))$$

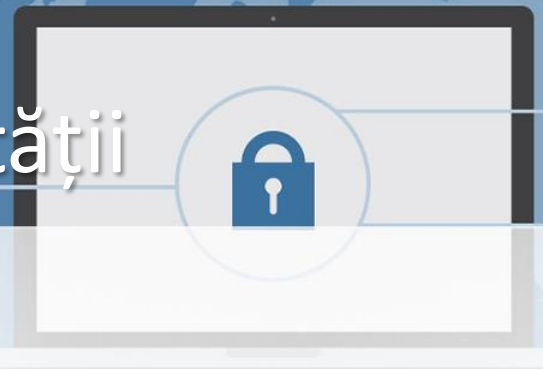
Criptarea mesajului și semnăturii cu cheile publice

$$A \rightarrow B: \quad E(PU_b, [M \| E(PR_a, H(M))])$$

Soluție cu certificare digitală

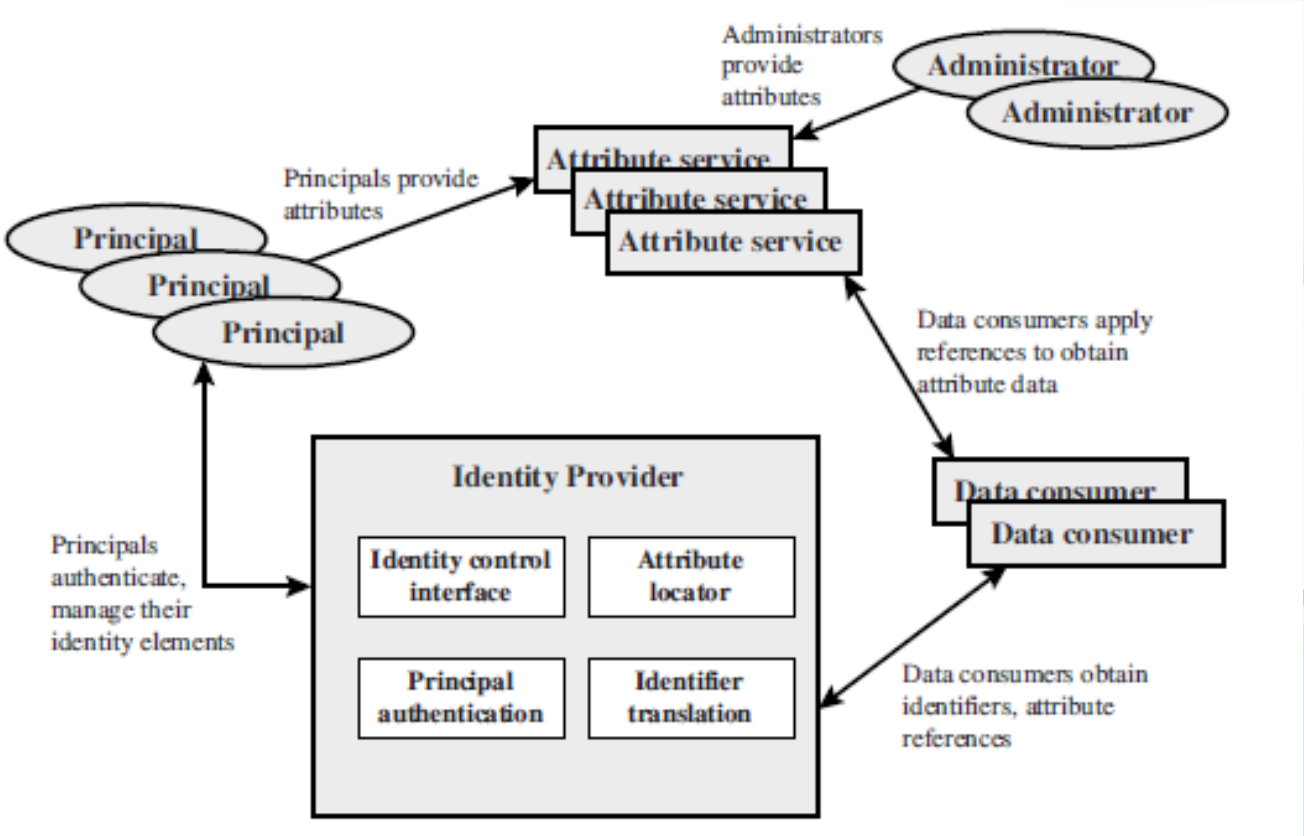
$$A \rightarrow B: \quad M \| E(PR_a, H(M)) \| E(PR_{as}, [T \| ID_A \| PU_a])$$

# Administrarea identității

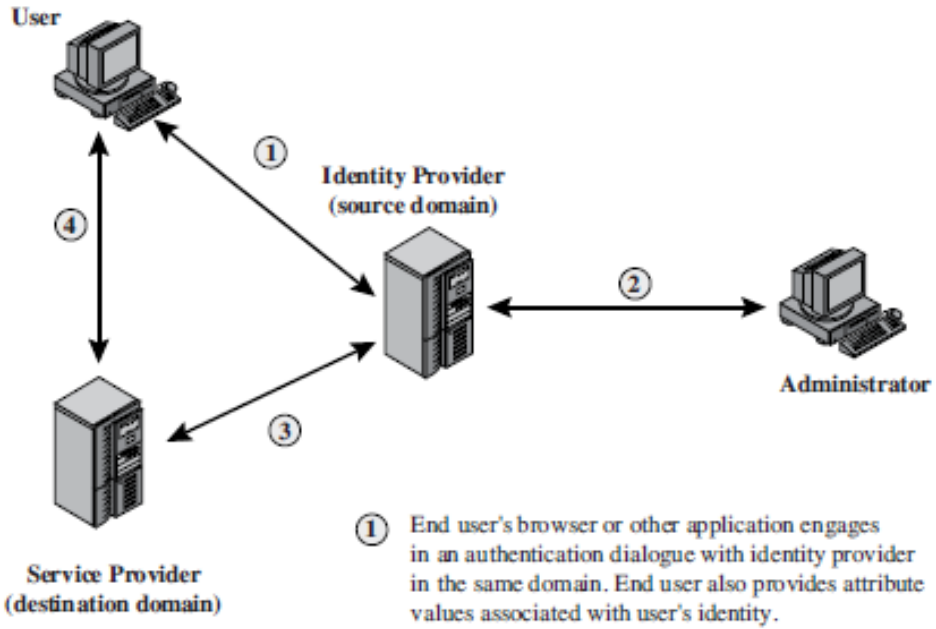


- Managementul identității
  - soluție centralizată, automată
  - furnizarea accesului la resurse
  - concept conectare unică (SSO single sign-on)
- Elemente
  - Autentificare (confirmarea veridicității)
  - Autorizare (permiterea accesului)
  - Contabilizare (menținerea înregistrărilor - log-uri)
  - Aprovizionare (introducerea utilizatorilor in sistem)
  - Automatizare (fluxurile de date)
  - Administrare (delegarea responsabilităților de administrare)
  - Sincronizare (sincronizarea parolelor, profilelor de utilizator)
  - Auto-administrare (resetarea parolelor)
  - Federalizare (mai multe domenii de securitate)

# Arhitectură generică




# Federalizare




1. End user's browser or other application engages in an authentication dialogue with identity provider in the same domain. End user also provides attribute values associated with user's identity.

2. Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.

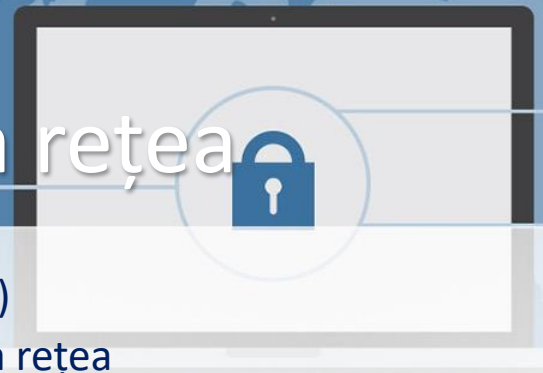
3. A service provider in a remote domain, which the user wishes to access, obtains identity information, authentication information, and associated attributes from the identity provider in the source domain.

4. Service provider opens session with remote user and enforces access control restrictions based on user's identity and attributes.

# Controlul accesului la rețea

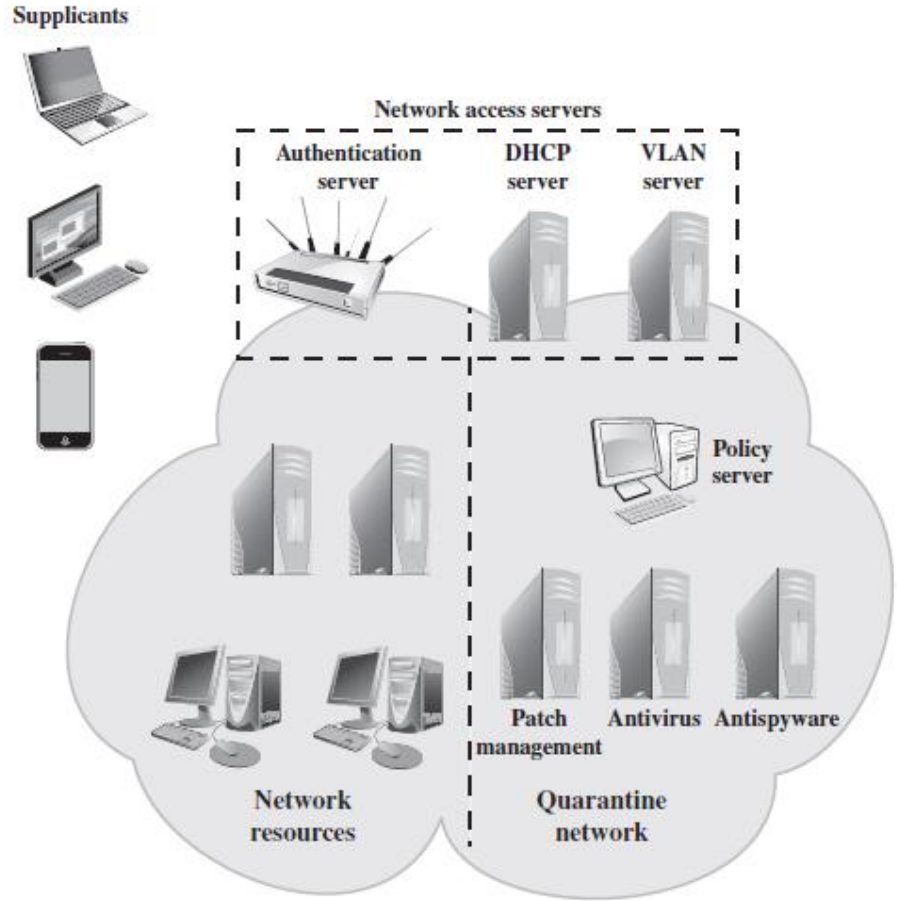
- Elemente de control al accesului la rețea
- Metode de autentificare
- Protocolul EAP
- Controlul accesului la nivel Legătură de date (802.1X)
- Concepte de cloud computing
- Protecția datelor in cloud

# Controlul accesului la rețea



- Network Access Control (NAC)
  - Administrarea accesului la rețea
  - Autentificarea utilizatorilor
  - Identificarea drepturilor (acces la date/ acțiuni permise în rețea)
  - Determină starea dispozitivelor de rețea
- Elementele unui sistem NAC
  - Solicitant acces (client)
    nodul de rețea (orice echipament de rețea IP) care solicită acces în rețea
  - Server de reguli de acces
    determină starea și drepturile de acces acordate clienților
  - Server de acces (gateway/server de acces la distanță)
    punct de control al accesului pentru clienți din locații la distanță

# Diagramă generică NAC



# Metode de control al accesului

- Metode NAC

  Regulile aplicate clienților pentru a permite accesul în rețea

  – IEEE 802.1X

    Protocol L2 ,autorizarea înainte de asocierea unui port către o adresă IP, protocolul EAP (*Extensible Authentication Protocol*)

  – VLAN (*Virtual Local Area Networks*)

    Segmentare logică a rețelei LAN în rețele virtuale, asocierea unui client la VLAN este decisa de NAC, un host poate face parte din mai multe rețele virtuale

  – Firewall

    Permite sau nu tranzitul pachetelor de trafic între client și rețea

  – Alocarea adreselor în rețea

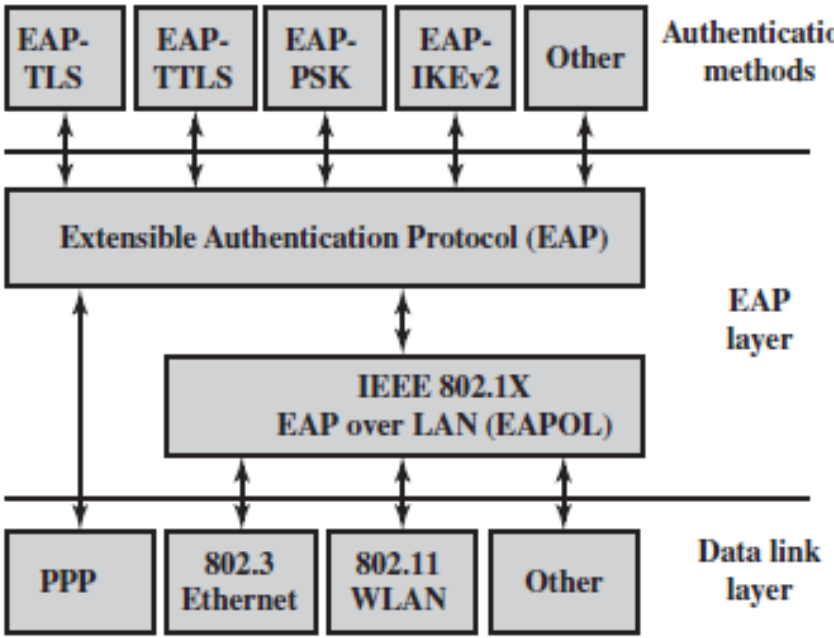
    DHCP - Dynamic Host Configuration Protocol

# EAP

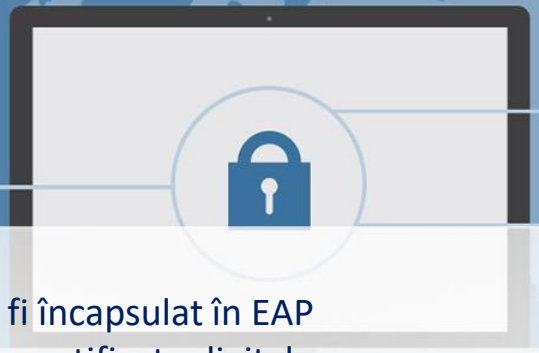
- EAP - Extensible Authentication Protocol (RFC 3748)
  - Cadru de lucru pentru protocoalele pentru controlul accesului și autentificare
  - Furnizează un set de mesaje protocol ce pot conține diverse metode de autentificare între client și server
  - Funcționează la diferite niveluri de comunicație
  - Poate adapta cerințele de autentificare pentru diverse soluții de interconectare

# Structura EAP

- Context EAP



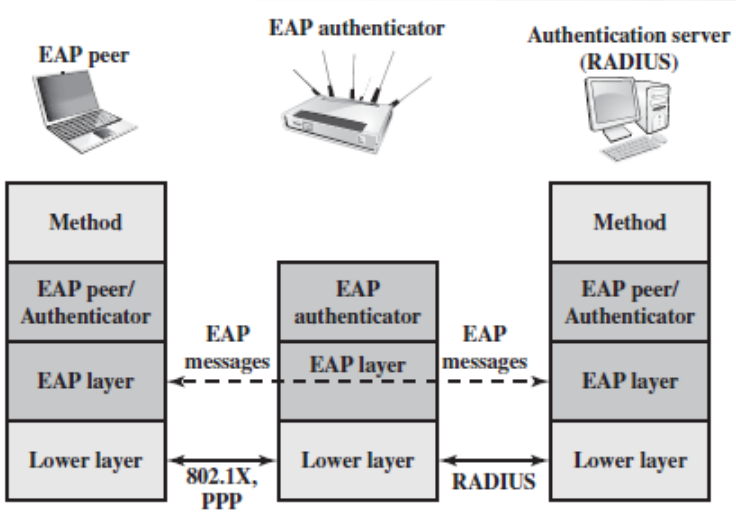
# Metode EAP

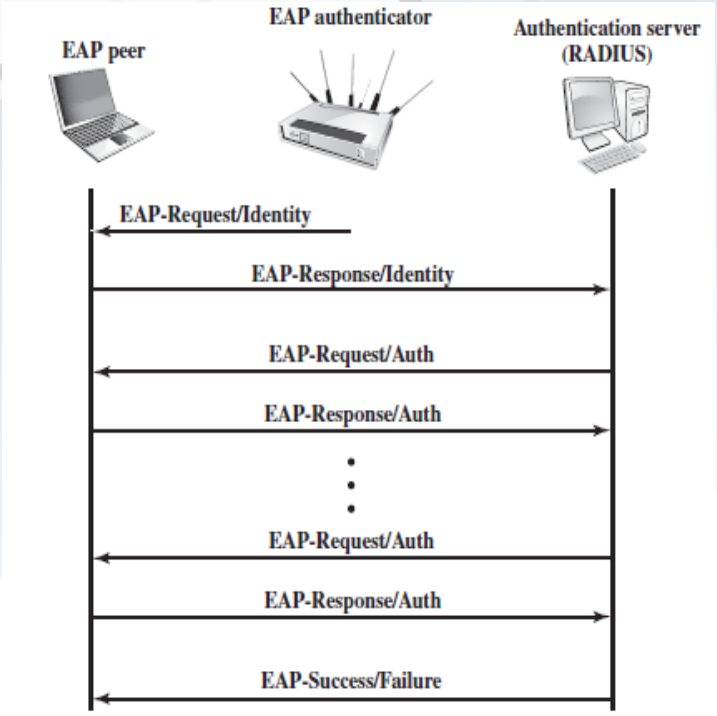


- EAP-TLS (EAP Transport Layer Security):
  - Definește modul în care protocolul TLS poate fi încapsulat în EAP
  - Clientul și serverul se autentifica reciproc prin certificate digitale
  - Clientul generează o cheie secretă pre-master prin criptarea unui număr aleator cu cheia publică a serverului și o trimite la server
  - Atât clientul cât și serverul folosesc cheia pre-master pentru a genera aceeași cheie secretă.
- EAP-TTLS (EAP Tunneled TLS)
  - Doar serverul are un certificat pentru a se autentifica la client
  - Conexiunea securizată (tunel) este realizată cu cheia secretă iar autentificarea cu EAP sau versiuni anterioare de protocoale de autentificare PAP (*Password Authentication Protocol*) sau CHAP (*Challenge-Handshake Authentication Protocol*).
- EAP-GPSK (EAP Generalized Pre-Shared Key)
  - Autentificarea reciprocă și derivarea cheilor de sesiune cu o cheie pre-partajată (PSK - Pre-Shared Key)
- EAP-IKEv2
  - Folosește protocolul IKEv2 - Internet Key Exchange pentru autentificarea reciprocă și schimbul de chei

# Mesaje EAP

- Componente implicate
  - Client EAP
  - Autentificator EAP
  - Server de autentificare



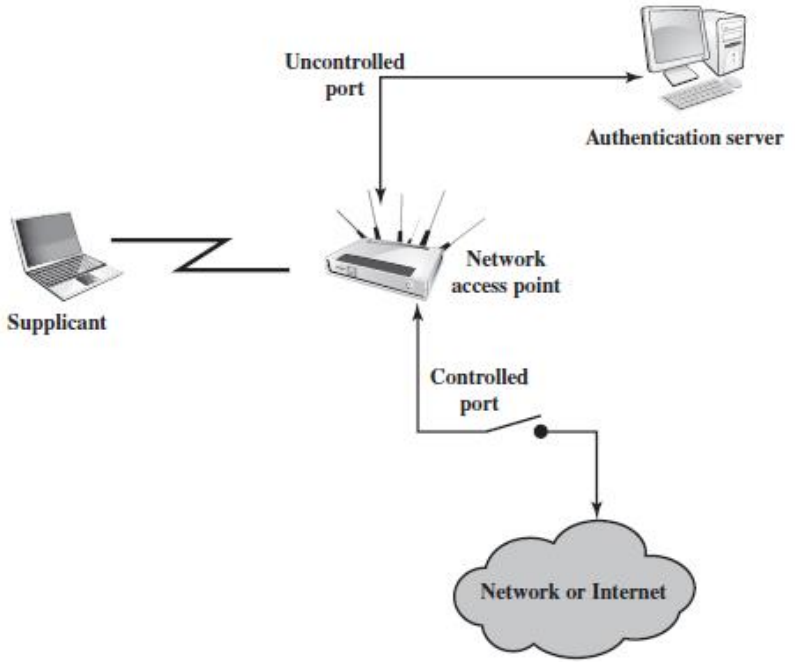
# Controlul accesului la nivel de port - 802.1X

| Frame Type | Definition |
|---|---|
| EAPOL-EAP | Contains an encapsulated EAP packet. |
| EAPOL-Start | A supplicant can issue this packet instead of waiting for a challenge from the authenticator. |
| EAPOL-Logoff | Used to return the state of the port to unauthorized when the supplicant if finished using the network. |
| EAPOL-Key | Used to exchange cryptographic keying information. |

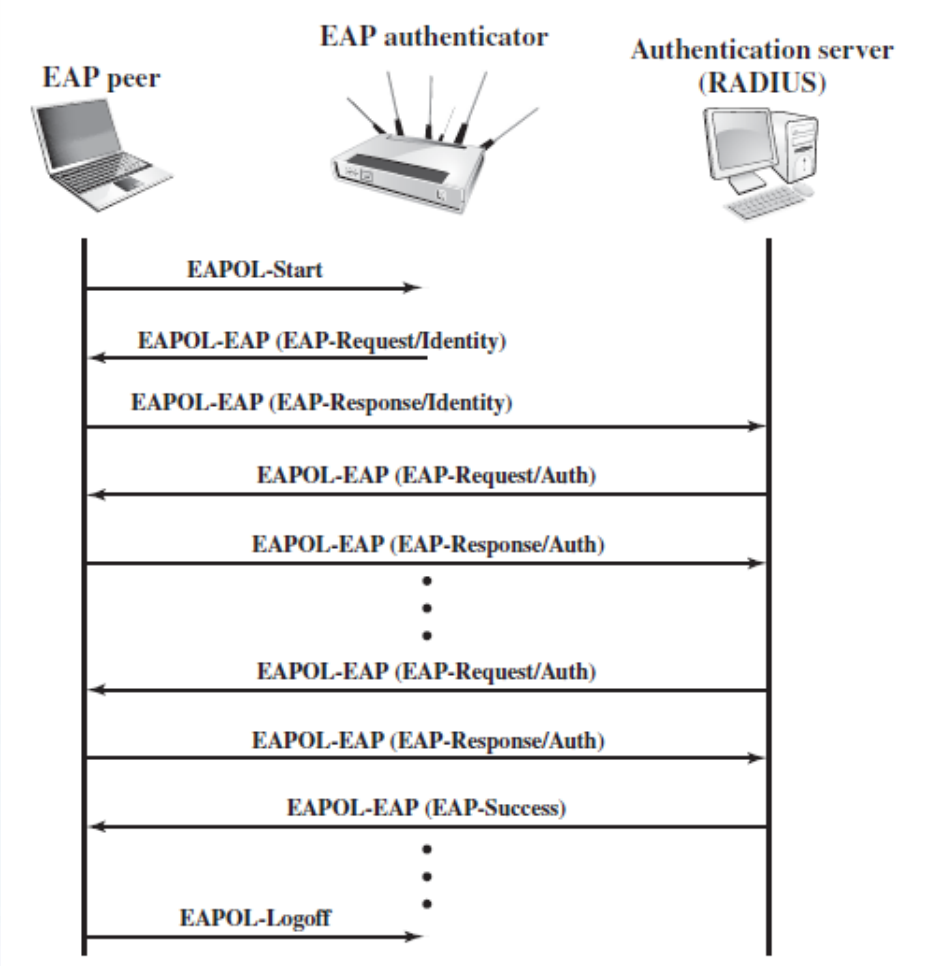
- IEEE 802.1X
  - Port-Based Network Access Control
  - Funcții de controlul accesului la LAN
  - Termeni *peer*, *authenticator*, and *authentication server*
  - Conceptele de porturi controlate și necontrolate
  - Autentificatorul definește o serie de porturi logice asociate porturilor fizice (controlate și necontrolate)
  - Portul necontrolat permite doar mesaje intre client si server
  - Un port controlat permite accesul si către alte stații în rețea
  - Protocol EAPOL (EAP over LAN)

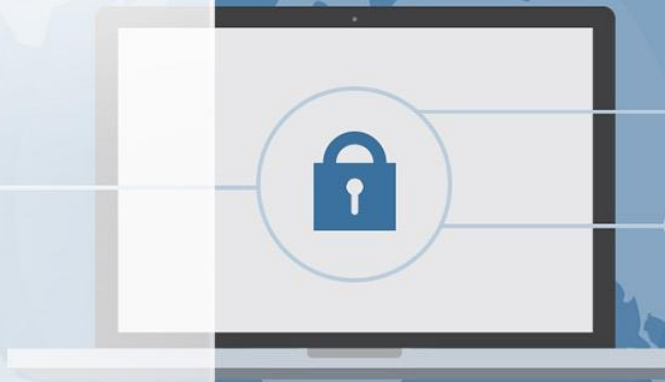
# 802.1X

- Arhitectura/principiu
- Până când AS autentifică un client (folosind un protocol de autentificare),
- autentificatorul trece doar mesaje de control și autentificare între client și AS; canalul de control 802.1X este deblocat, dar datele sunt blocate.
- Odată ce un clientul este autentificat și cheile sunt furnizate,
- autentificatorul poate transmite date de la client, sub rezerva limitărilor de control de acces predefinite pentru client în rețea.
- În aceste condiții, canalul de date este deblocat.

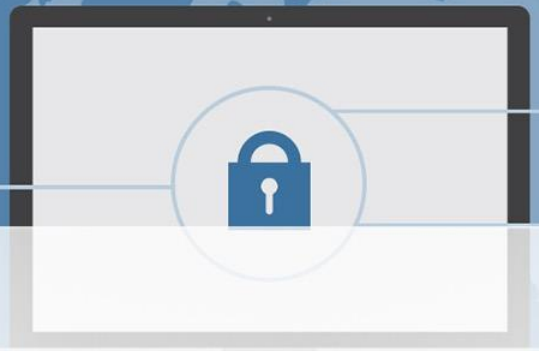


# Exemplu EAPOL



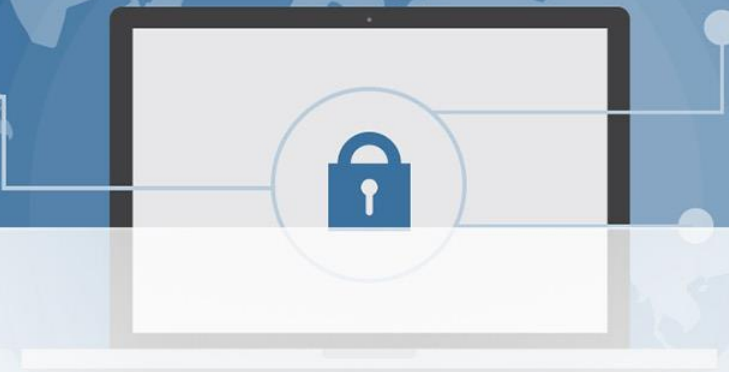



# Cloud computing



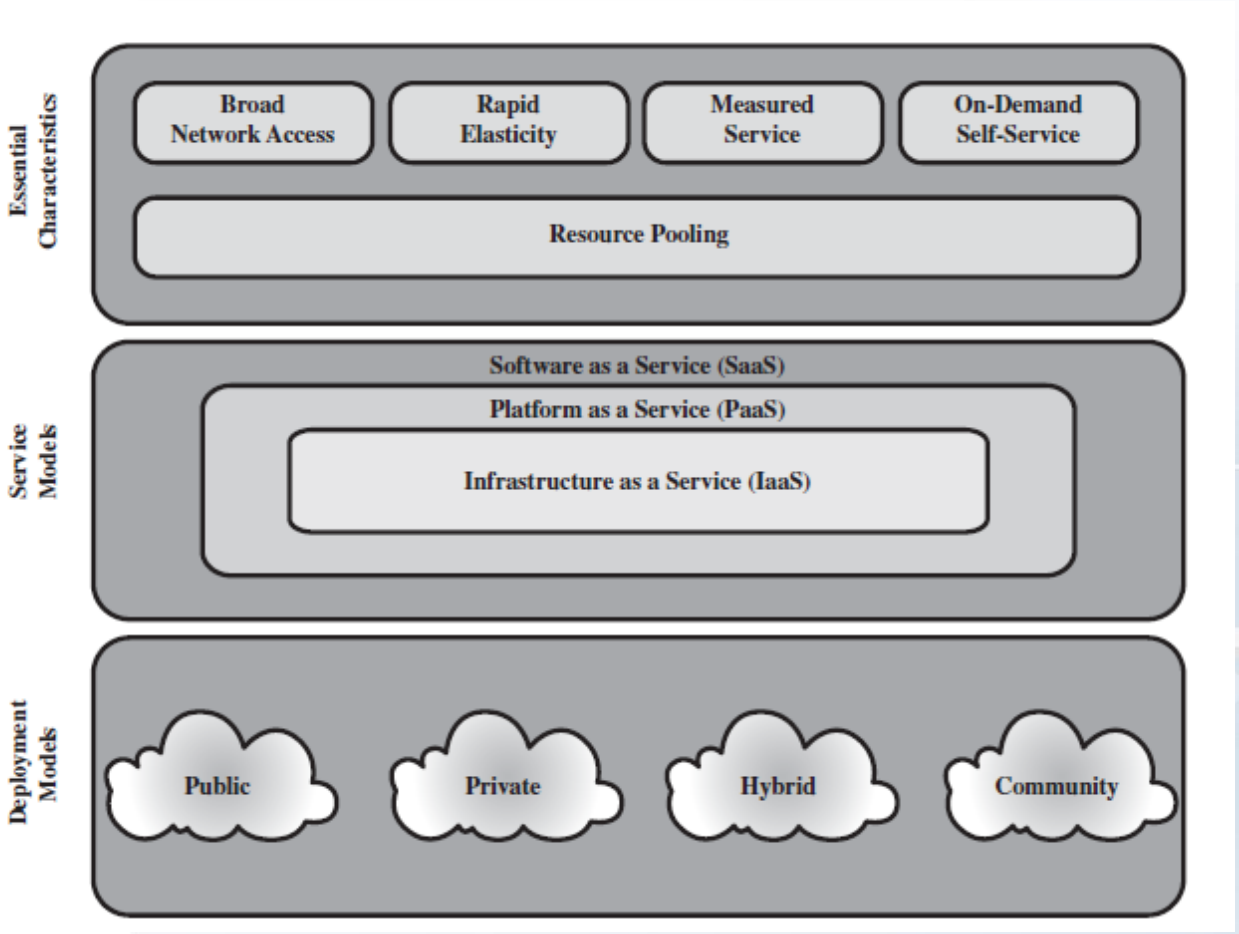
- Cloud computing
  - Infrastructură Internet
  - Acces la resurse online (rețele, servere, aplicații, stocare, servicii)
  - Efort de administrare minim
  - 3 modele de servicii de bază (SaaS, PaaS, IaaS)
  - 4 modele de implementare (public, privat, hibrid, comunitar)
- Caracteristici
  - Access la rețea de bandă largă
  - Elasticitate (extindere/reducere rapidă a resurselor)
  - Capacitatea de măsurare (servicii contorizate)
  - Auto administrare, la cerere (punere la dispoziție către utilizator)
  - Punerea în comun a resurselor (resursele deservesc mulți utilizatori)

# Modele cloud

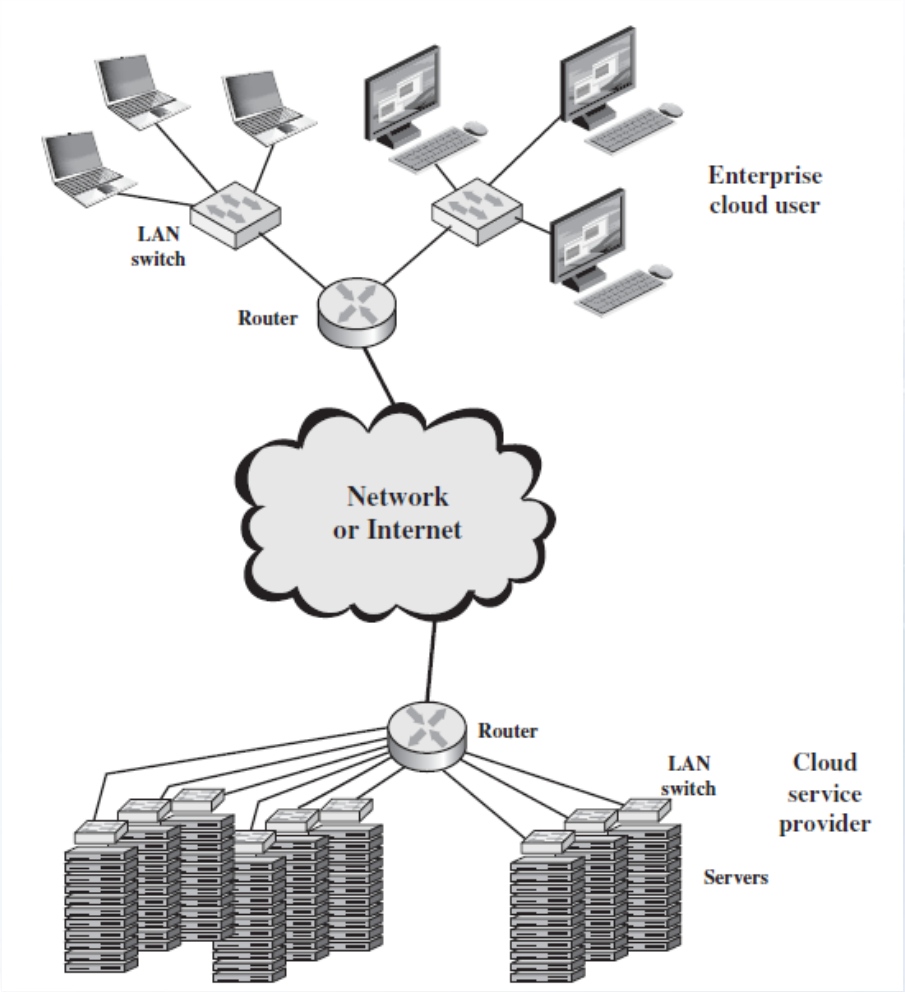


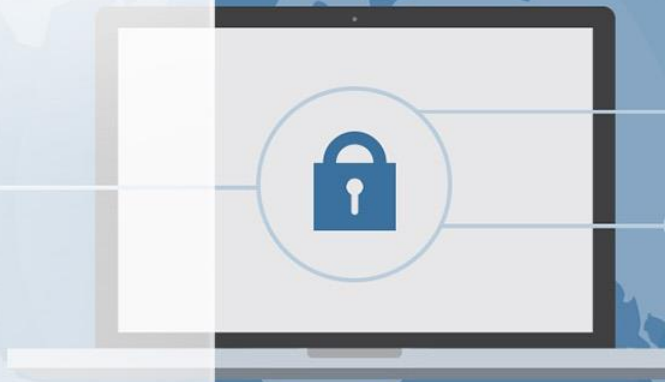
- Modele de servicii
  - SaaS - Software as a service
    folosirea aplicațiilor puse la dispoziție in cloud
  - PaaS - Platform as a service
    sisteme de operare în cloud
  - IaaS - Infrastructure as a service
    putere de calcul, stocare, infrastructură de rețea
- Modele de implementare
  - Public (la dispoziția publicului larg)
  - Privat (exploatat numai de o organizație)
  - Comunitar (partajat de mai multe organizații)
  - Hibrid (combinații de 2 sau multe soluții cloud)

# Elemente cloud

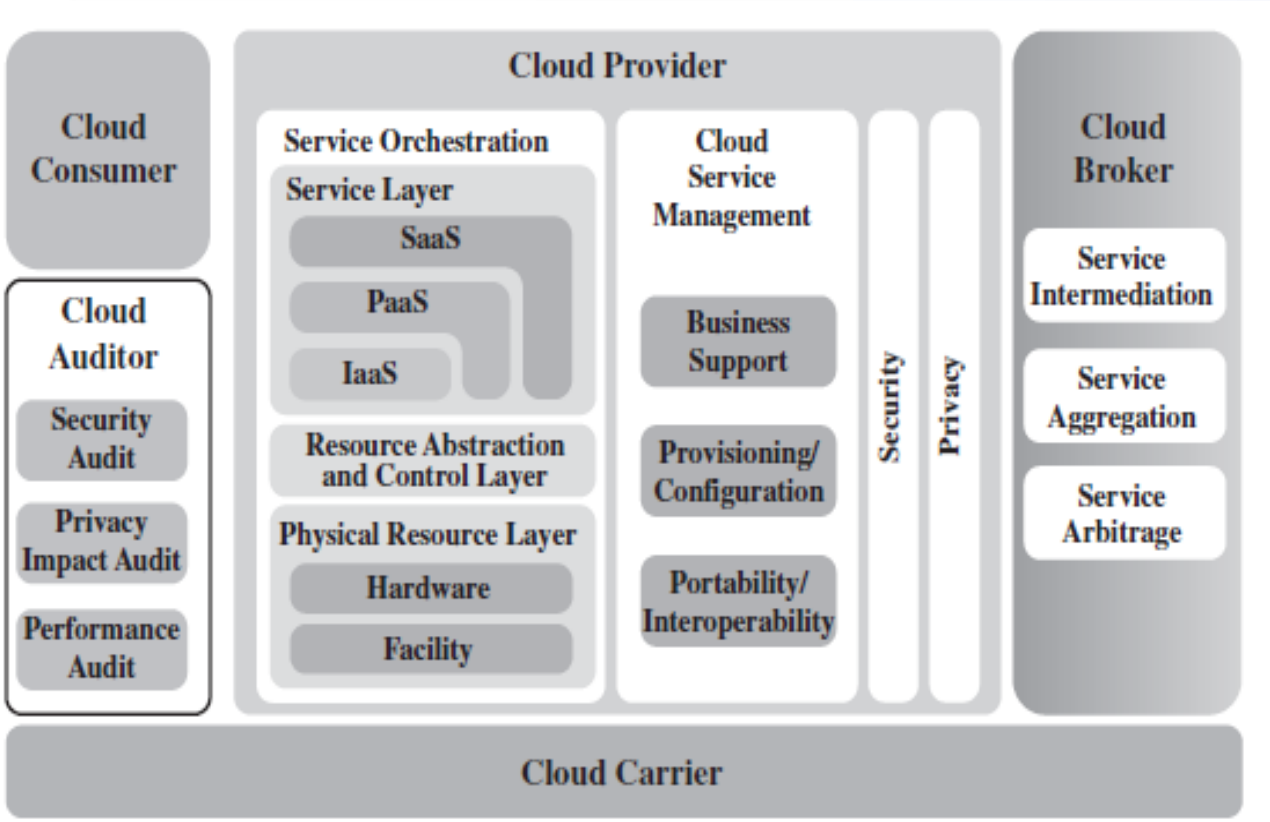



# Context CLOUD



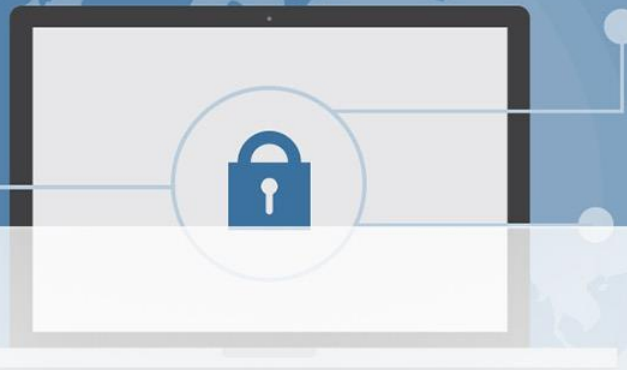



# Arhitectura Cloud



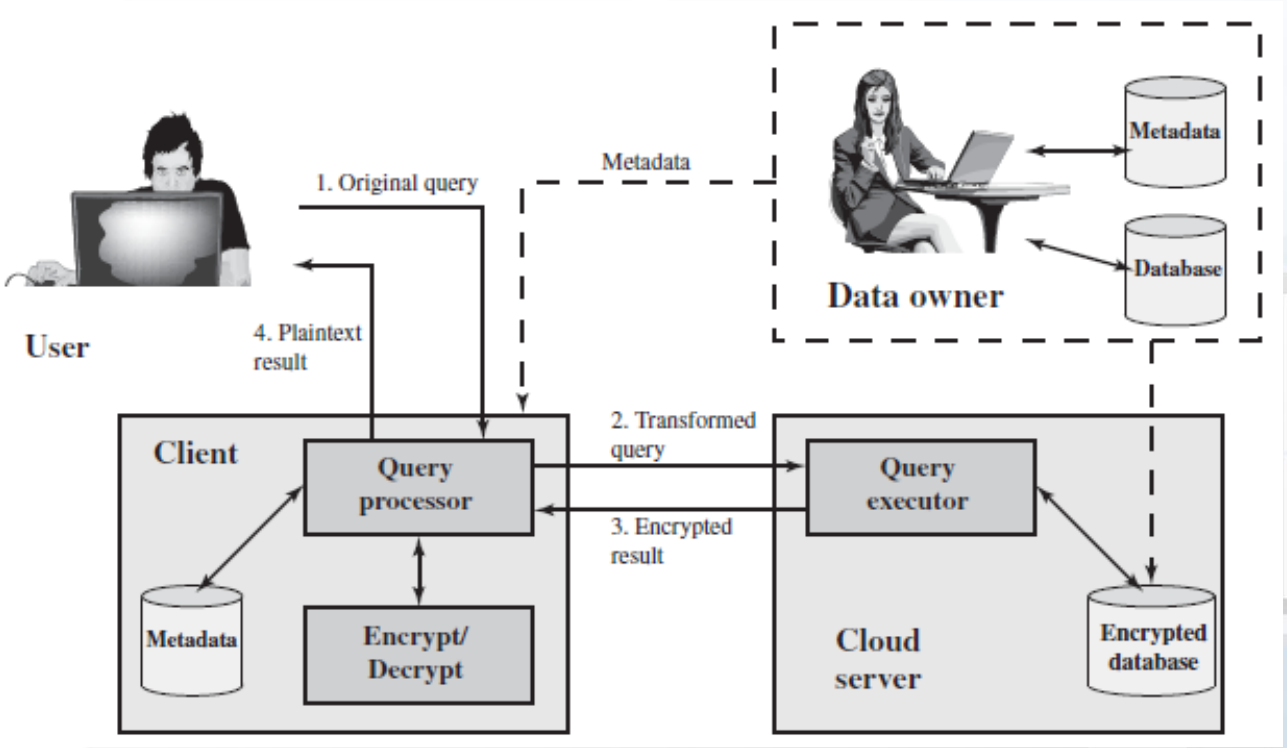

Abonat - Furnizor - Auditor - Agent - Transportator

# Riscuri de securitate



- Amenințări de securitate
  - Abuzul și utilizarea nefastă a cloud computing
  - Interfețe și API-uri nesigure
  - Persoane rău intenționate din interiorul furnizorilor
  - Probleme tehnologice la resursele partajate
  - Pierderea sau scurgerea de date
  - Deturnarea conturilor sau serviciilor
  - Profilul de risc necunoscut

# Protecția datelor




- Schema de criptare

# Securitatea in cloud

- Security as a service (SecaaS)
  - Management identitate și acces
  - Prevenirea pierderii datelor
  - Securitate web
  - Securitate email
  - Evaluarea securității
  - Managementul intruziunilor
  - Criptarea
  - Recuperarea datelor
  - Securitatea rețelelor