Securitate în rețele
Autentificarea

Universitatea “Transilvania” din Brasov

Autentificarea

Cuprins

- 1 Cunoștințe și posesie
- 2 Metode challenge-response
- 3 Kerberos
- 4 Biometrie și chip-carduri
- 5 Infrastructură de chei publice (PKI) și semnătura digitală

Autentificarea

Starea sistemelor:

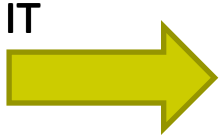
Utilizatorii de sisteme IT se autentifică prima data la sistem pentru a avea ulterior acces la toate datele, procesele, serviciile de pe serverele sistemului informatic.

Accesul la informațiile digitale este necesar utilizatorului direct prin intermediul calculatorului, dar și proceselor utilizator ce rulează pe servere de aplicatii, care actionează in numele utilizatorilor.

Logarea simpla doar pe baza de parola și acces forfetar la toate serviciile oferite de sistem nu mai este suficienta in sistemele distribuite deschise.

Nu este sigur daca utilizatorul sau procesele utilizator comunica cu sistemul sau cu serverul de aplicatii.

Tel: Acces autorizat la servicii autentice in retele deschise de sisteme IT



Prevenirea Spoofing-Attack și Man-in-the-middle-Attack

Autentificarea

Autentificarea și autorizarea

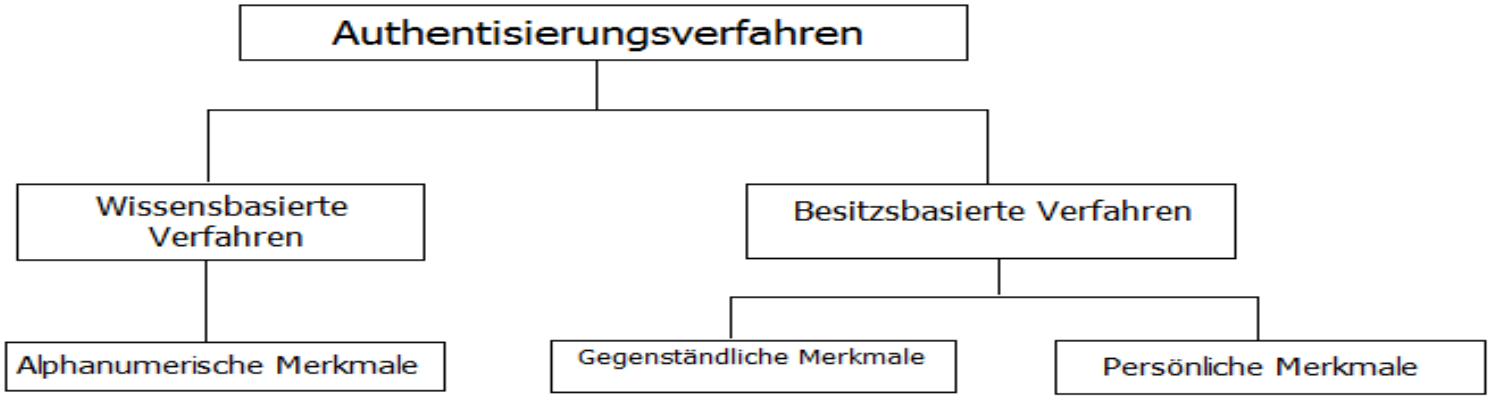
Identificare: recunoașterea identității unei persoane, unui calculator sau proces
ex: User-ID, adrese de internet

Autentificare: examinarea pretinsei identități a persoanei, calculatorului sau procesului
ex: interogare parola

Autorizare: daca autentificarea a avut succes, persoana, calculatorul sau procesul are acces la serviciile sau componentele de sistem corespunzatoare

Caracteristici de autentificare- caracteristici bazate pe o autentificare lipsita de ambiguitate pentru autorizare
ex: PIN/TAN, semnatura digitala, amprente digitale, voce, fata

Autentificarea



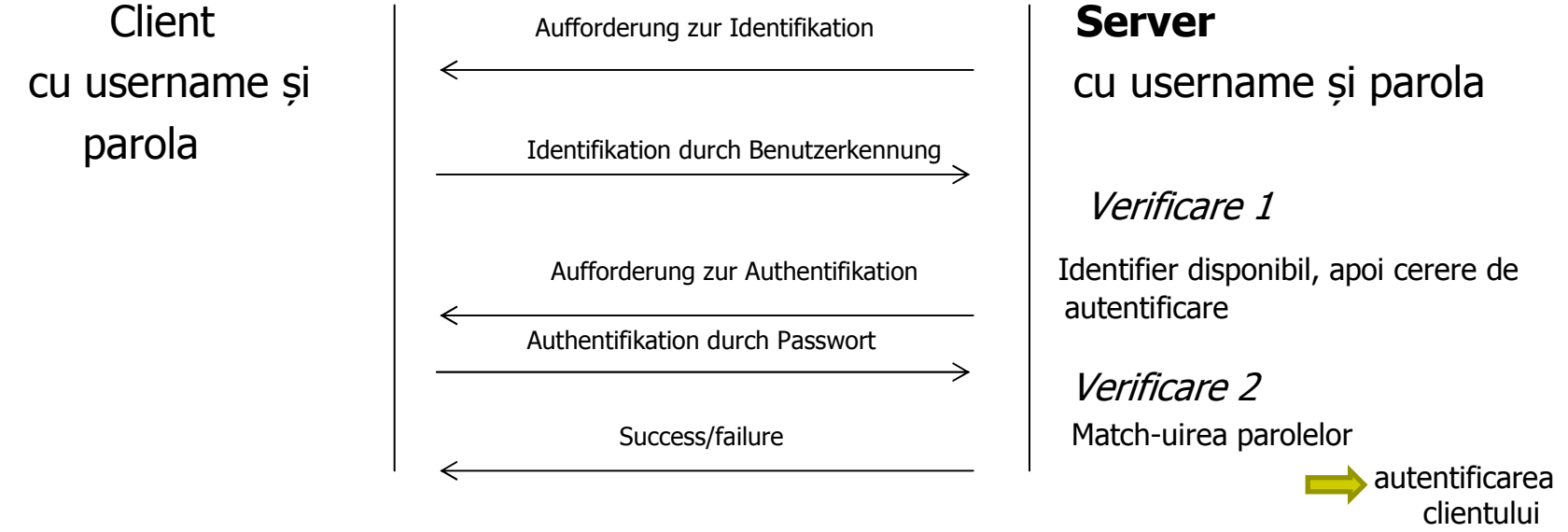
Protocoale de autentificare diferite

intre Client și Server

Autentificarea

(A) Caracteristici alfa numerice

clasic: controlul de acces prin parola



dezavantaj: schimb de texte pentru autentificarea clientului

Autentificarea

(A) Caracteristici alfa numerice

Imbunatățiri: conturile de utilizator și parolele sa se transfere criptat!

Cerinte pentru parola: minimum 8 caractere, incluzand litere, cifre, caractere speciale, timp de degradare scurt, fara nicio repetitie

Parole generate de sistem: aleatoare, de inalta calitate necesare

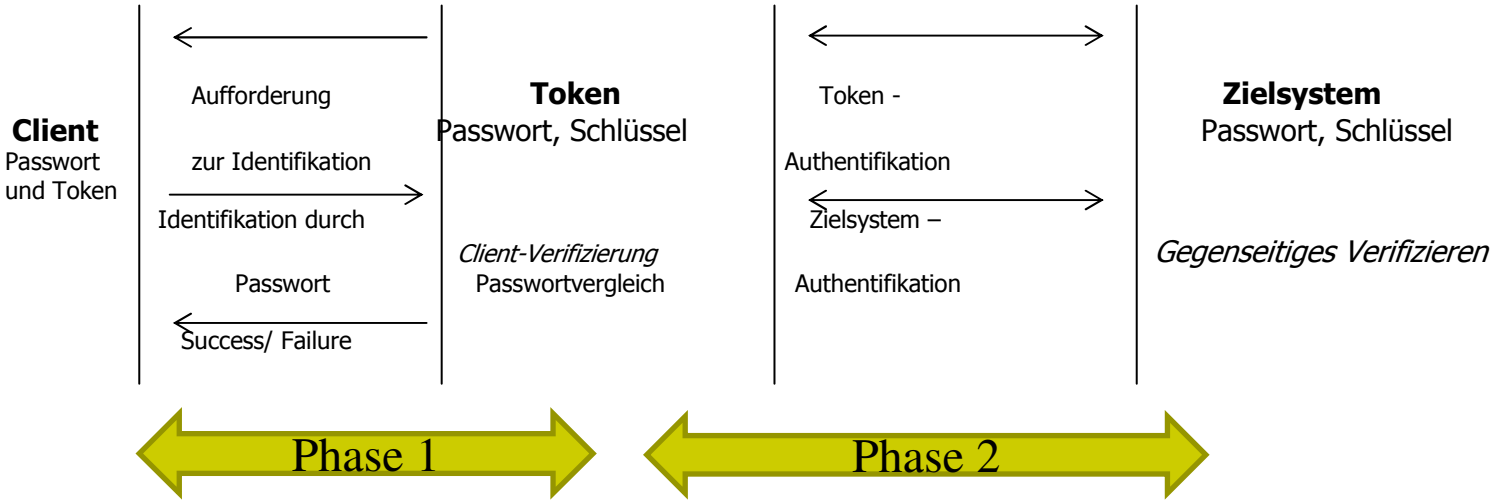
Ex: PIN

Autentificarea doar prin parole sau PIN este suficienta doar in cadrul retelelor protejate

Autentificarea

(B) Caracteristici alfa-numerice și de reprezentare

Utilizatorul se afla in posesia unui token personal(smart-card)
Autentificare in 2 faze: client-token, token-sistem tinta



Combinatie intre cunostinta(parola) și posesie(token) in faza 1
Autentificarea in faza 2 se face prin protocoale challenge-response

Autentificarea

(B) Caracteristici alfa-numerice și de reprezentare

Autentificarea prin combinatia parolei cu token creste considerabil siguranta

Autentificarea se face prin metode de criptare simetrice sau asimetrice (ex: 3DES, IDEA, RSA, ElGamal)

Tokenii in forma de carduri cu chip de memorie salvează parolele, cheile simetrice si/sau asimetrice și calculează valorile hash precum și semnaturile digitale

Baza de date de utilizator in sistemul tinta este in special pentru protectie

Autentificarea reciproca intre token și sistemul tinta previne atacurile Maskerade

Autentificarea bazata pe carduri cu chip de memorie este dezvoltata prin metode biometrice

Smart-Card: solutiile bazate furnizează optimizarea autentificarii și controlului de acces

Autentificarea

(C) Caracteristici concrete și personale

Autentificarea prin combinatia de token-uri și caracteristici fizice de utilizatori, cum ar fi amprentele digitale și recunoasterea irisului, asigura verificarea individuala a utilizatorului

Fiecare utilizator este un individ iar caracteristicile sale fizice sunt unice !

Utilizatorul se identifica printr-o caracteristica fizica, cum ar fi amprentele, opuse token-ului personal și sistemului tinta

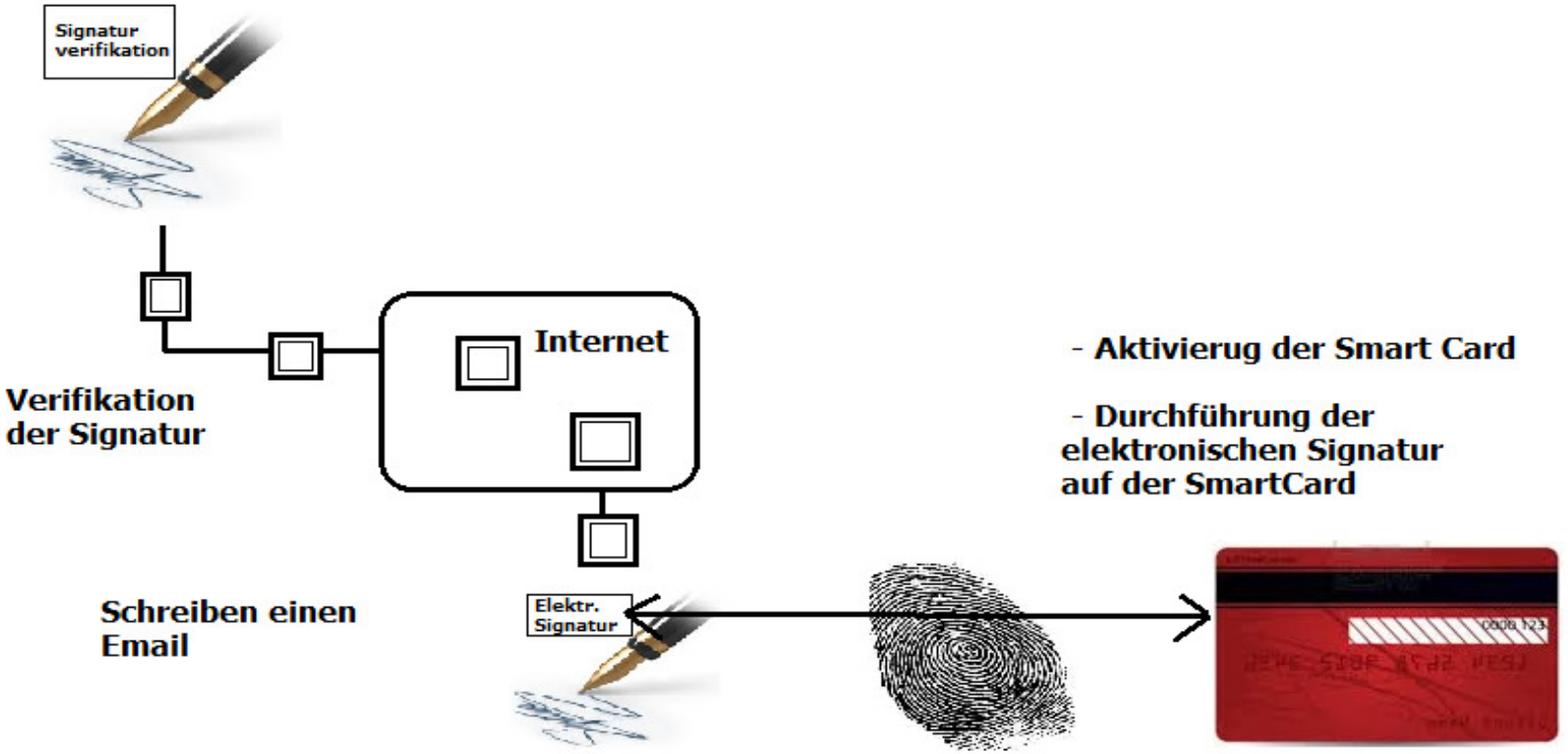
Caracteristicile fizice sunt foarte dificil de creat

Single sign-on este posibil și are acces la toate aplicatiile și sistemele la care utilizatorul este autorizat

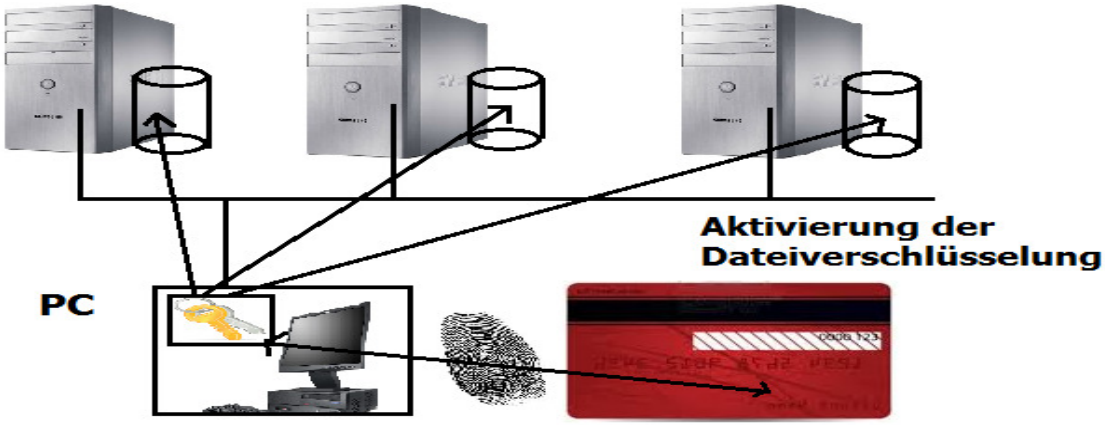
Smart-card: solutii bazate pe caracteristici biometrice, asigura o mai mare securitate autentificarii și controlului de acces

Autentificarea

Securitatea Semnaturii și Email-ului



Autentificarea



Autentificarea

Protocol de autentificare prin metode Challenge-Response

- autentificarea clientului catre server, dupa functionarea cu succes a protocolului
- Clientul și serverul au schimbat anterior secrete
- informatiile secrete nu sunt transmise in mod direct

Principiu Clientul primeste de la server, la cerere, un numar aleator o singura data, pe care ulterior il trimite inapoi la server impreuna cu link-urile secrete. Serverul verifica clientul pe baza link-urilor secrete și astfel se poate efectua autentificarea

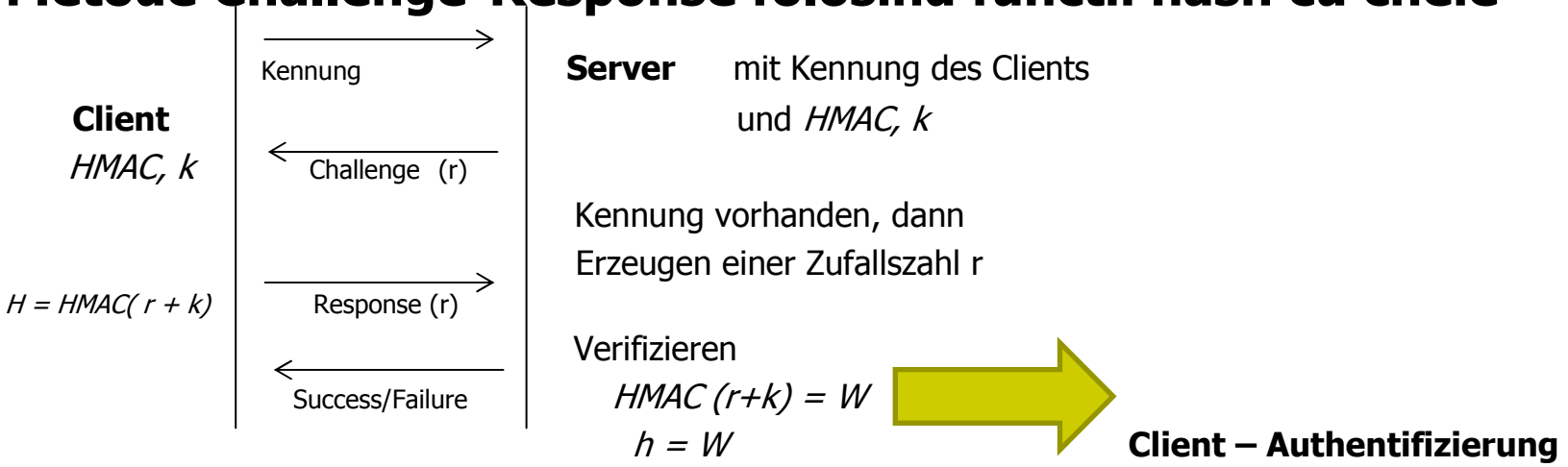
Clase de metode

Autentificare bazata pe valori hash(criptare simetrica)

Autentificare bazata pe semnaturi digitale (criptare asimetrica)

Autentificarea

Metode Challenge-Response folosind functii hash cu cheie



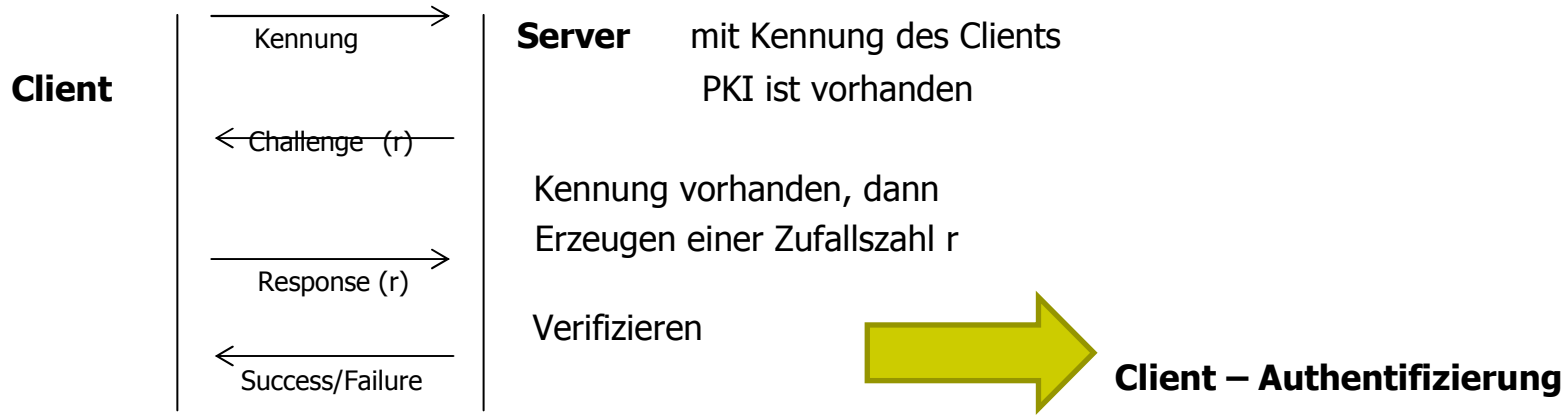
Orice mesaj protocol este autentificat folosind valorarea hash a mesajului

Avantaj: niciun schimb de secrete ptr autentificarea clientului

Dezavantaj: cheia secreta trebuie schimbata in siguranta intre fiecare partener de comunicare corespunde unei singure și sigure semnaturi digitale

Autentificarea

Metode Challenge-Response cu sistem criptografic asimetric



Avantaj: In cazul in care fiecare semnatura de pe un smartcard are drept de semnatura corespunzator, atunci exista o autentificare obligatorie a clientului

Autentificare pe baza chip-card:

1. Autentificare la Smart Card(PIN)

2. Smart Card se autentifica la PC(CRV)

3. Pc se autentifica la Smart Card(CRV)

Autentificarea

Protocol de autentificare prin metode zero-knowledge

Caz special de metoda challenge-response

Serverul nu are secrete stocate despre client și acestea pot inca autentifica

Informatiile dintre client și server sunt in asa fel schimbate incat un tert fara cunostinte obtine secretele pentru autentificare

o metoda cunoscuta este cea Fiat-Shamir

Autentificarea

Protocol de autentificare PPP

Ofera doua tipuri diferite de autentificare a clientilor:

1. **Password Authentication Protocol (PAP)**
2. **Challenge-Handshake Authentication Protocol (CHAP)**

Dupa configurarea conexiunii, protocolul CHAP defineste 3 pachete, unde este transmis campul informatie din cadrele PPP(PAP doar 2)

In PAP, parolele sunt transmise printr-un text clar, in schimb in CHAP sunt criptate prin valorile hash

Valoarea hash H este o combinatie intre secventa aleatoare C si parola PW a aplicata utilizatorului

Autentificarea este o parte a protocolului LCP și se efectuează in conformitate cu faza de configurare a conexiunii

Autentificarea este constructia unei conexiuni-PPP optionale

Autentificarea

Protocol de autentificare Kerberos

Tel: autentificarea clientului și cheia secreta simetrica ptr comunicarea intre Client și Server Service

Autentificarea

Protocol de autentificare WLAN 802.1x/EAP

1. Mobile Client (MAC) se conectează la Punctul de Acces (AP)
2. AP blochează toate cererile IP ale clientului și solicita identificare(username și parola)
3. Acreditarile user-ului sunt trimise de catre AP (prin protocol necontrolat) la serverul de autentificare AS, care porneste dialogul de autentificare intre MC și AS
4. AS și MC realizează un dialog de autentificare EAP (mai multe cereri și raspunsuri aferente) despre AP (mesajele EAP intre MC și AP sunt frame-uri LAN și intre AP și AS sunt incapsulate in pachete Radius)
5. Dupa autentificarea cu succes a MC, se deschid porturile controlate ale AP pentru a se produce conectarea unica cu MC-ul (doar MC-ul a fost autentificat, one way authentification!)
6. Transferul criptat de date dintre MC și AP, prin intermediul protocolului WEP, poate incepe