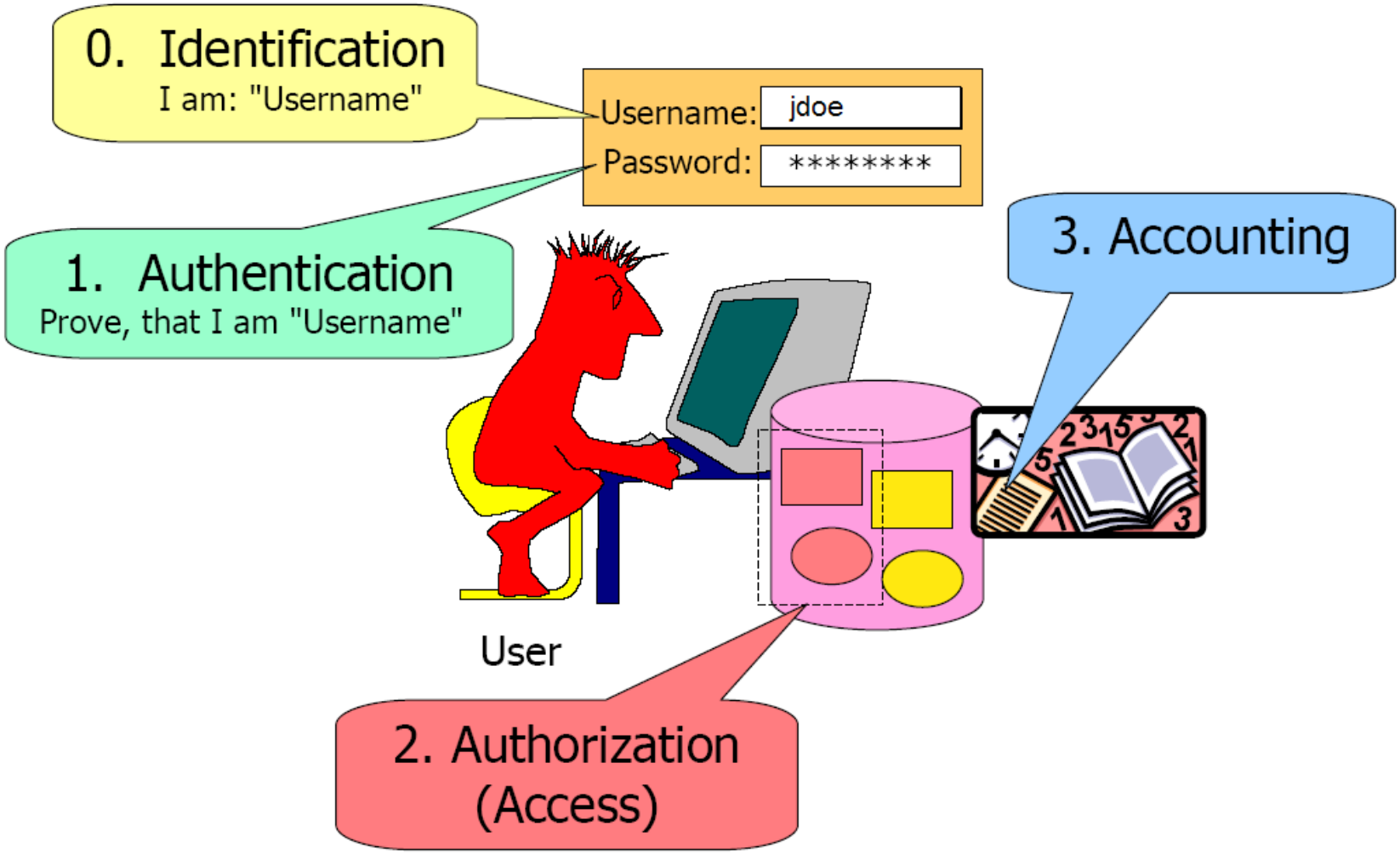
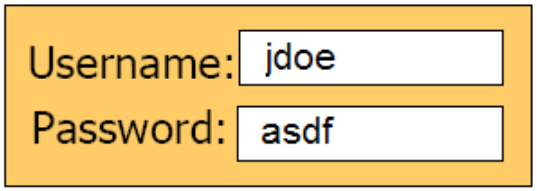
1. Protocoale de Autentificare

Authentication, Authorization, Accounting (AAA)



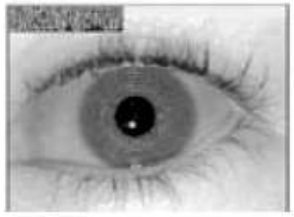
Autentificarea utilizatorilor

- **Ceea ce utilizatorul cunoaşte (parolă, PIN)**



- **Ceea ce utilizatorul deţine (Certificat, Token)**

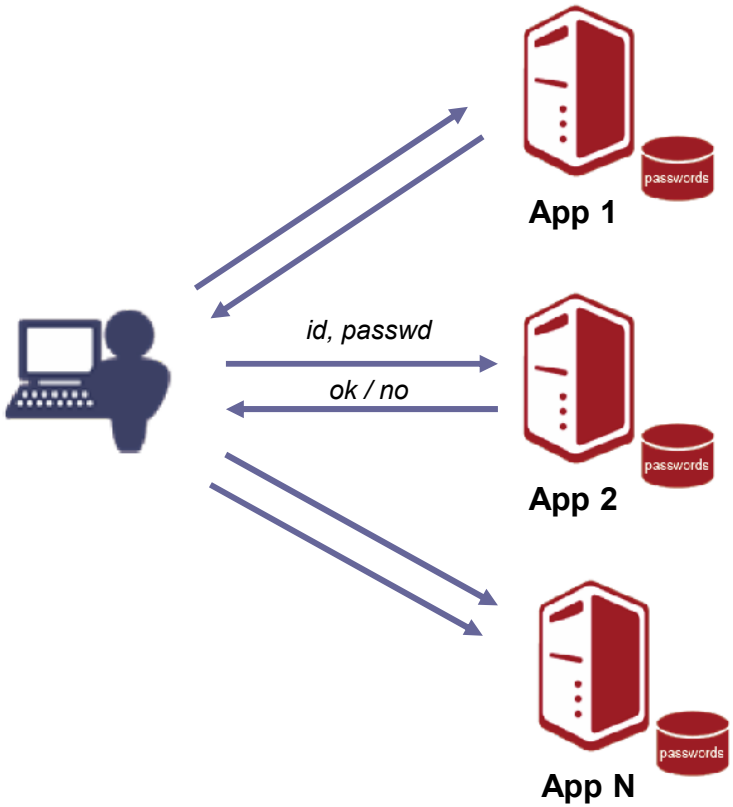

- **Ceea ce utilizatorul este (amprenta, voce)**

- **Autentificarea sigură a utilizatorilor presupune combinarea a cel puţin doi factori!**

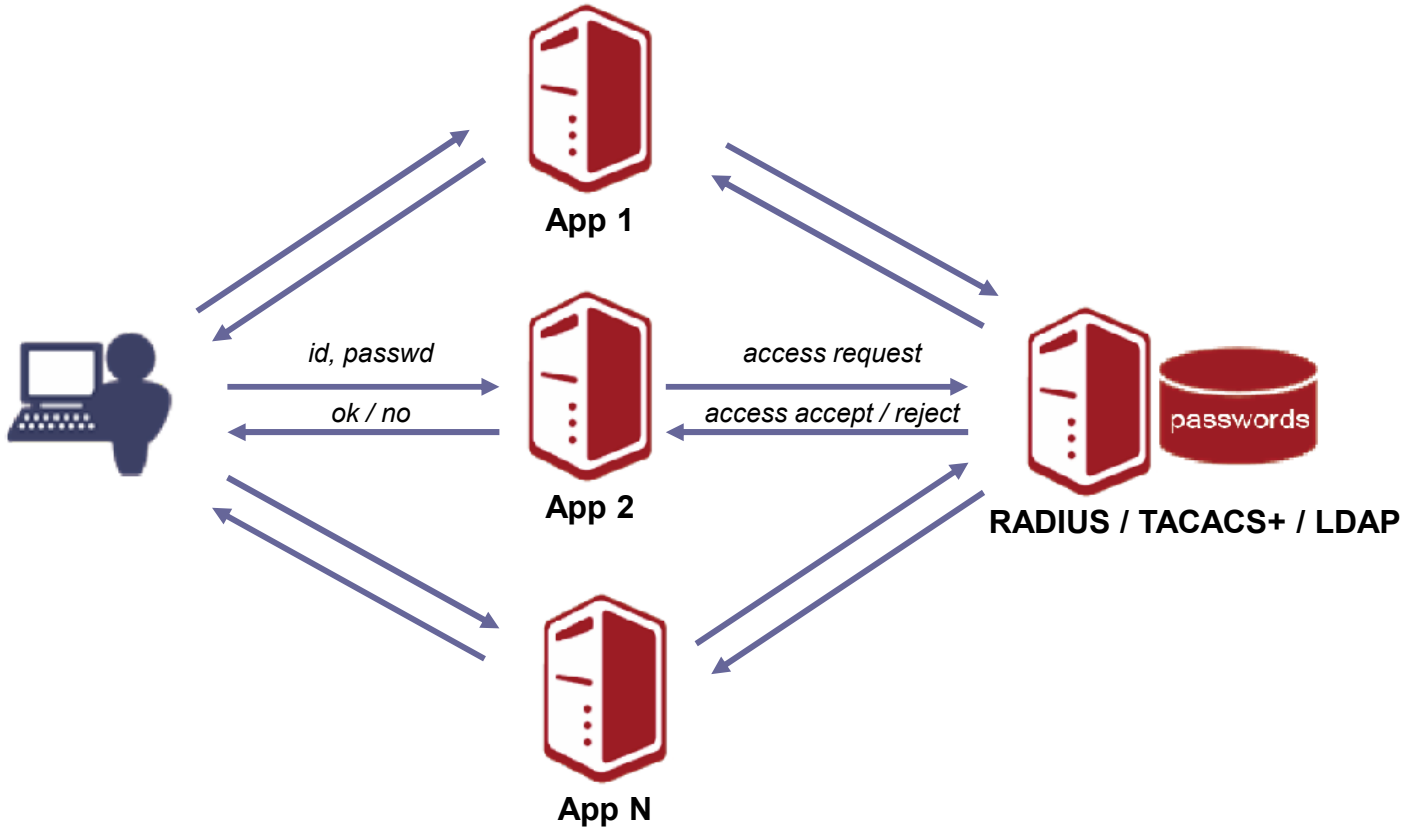
Autentificare directă

- Fiecare sistem are o bază de date proprie pentru autentificarea utilizatorilor
- Ok, pentru site-uri cu un număr mic de utilizatori / aplicaţii



Autentificare indirectă

- Bază de date centrală folosită în comun de mai multe sisteme
  - RADIUS, TACACS+, LDAP
- Management centralizat al utilizatorilor

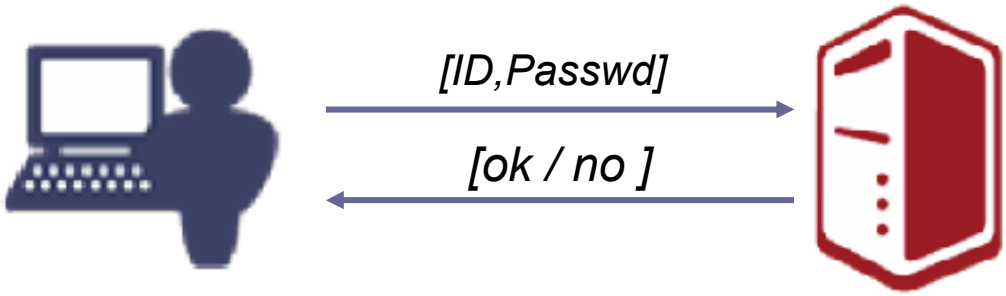


Protocoale de autentificare

- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Windows NT LAN Manager (NTLM)
- Kerberos
- Certificate digitale
- Generatoare de parole de unică folosinţă
- Biometrice

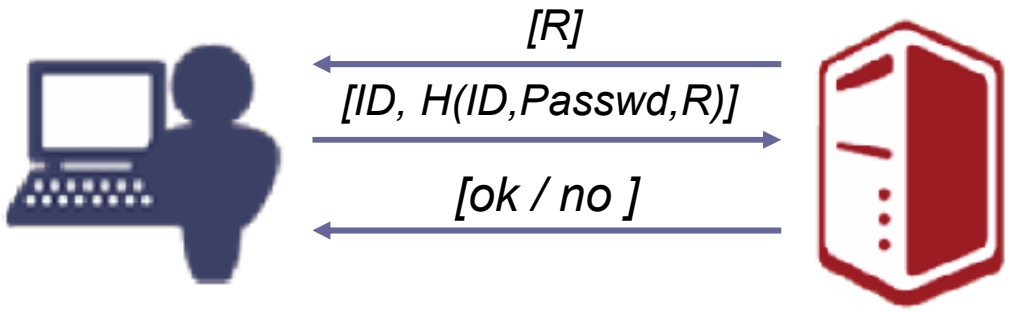
PAP

- Transmiterea în clar a username-ului şi parolei
- IETF RFC 1334



CHAP

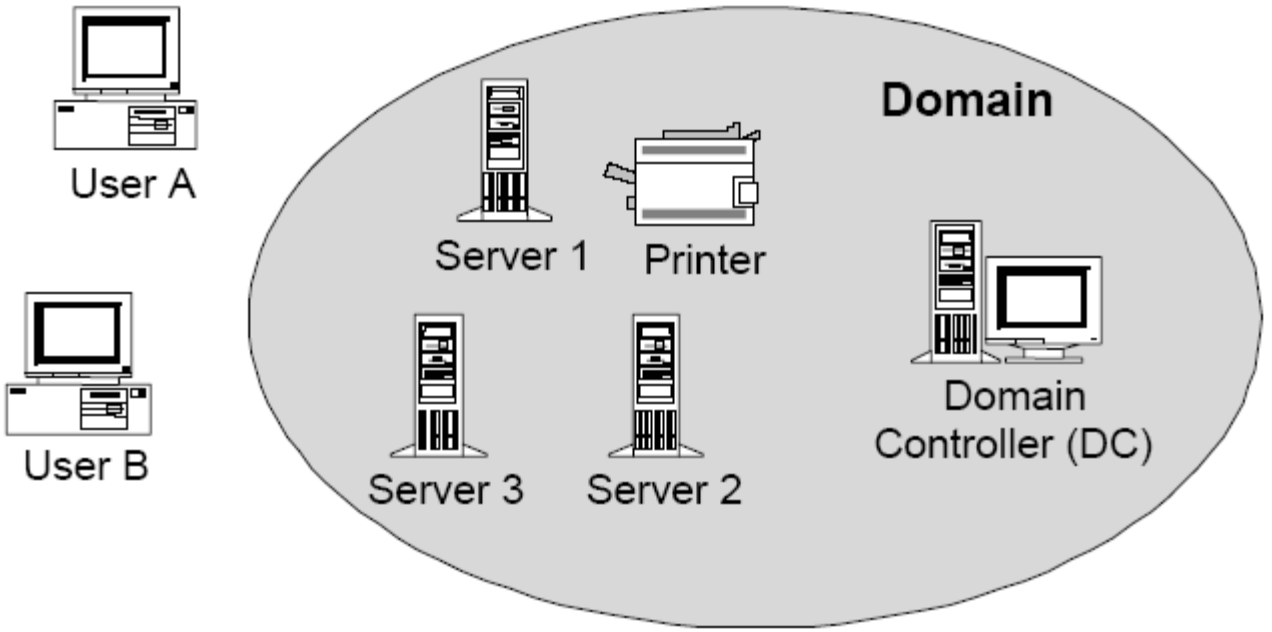
- Protocol în trei paşi:
  - Provocare (Challenge)
  - Răspuns
  - Succes / Failure
- Parola nu circulă niciodată în clar prin reţea
- Valoarea aleatoare (provocarea) trebuie să fie de fiecare dată alta pentru a evita atacurile prin reluare
- IETF RFC 1994



NTLM

- Autentificare în Domenii Windows
- Un domeniu este o colecţie de servicii (E-mail, File Sharing, Printing, etc) administrate prin intermediul unui Domain Controller (DC)
- Administrare centralizată:
  - Fiecare utilizator are un singur cont pentru un domeniu, gestionat de către Domain Controller (DC)
  - Nu este nevoie ca utilizatorii să aibă conturi pe fiecare server din domeniu
- Flexibilitate ridicată:
  - Administrare la nivel de grup
  - Domenii multiple (relaţii de încredere între domenii)
- Toată lumea trebuie să aibă încredere în Domain Controller.

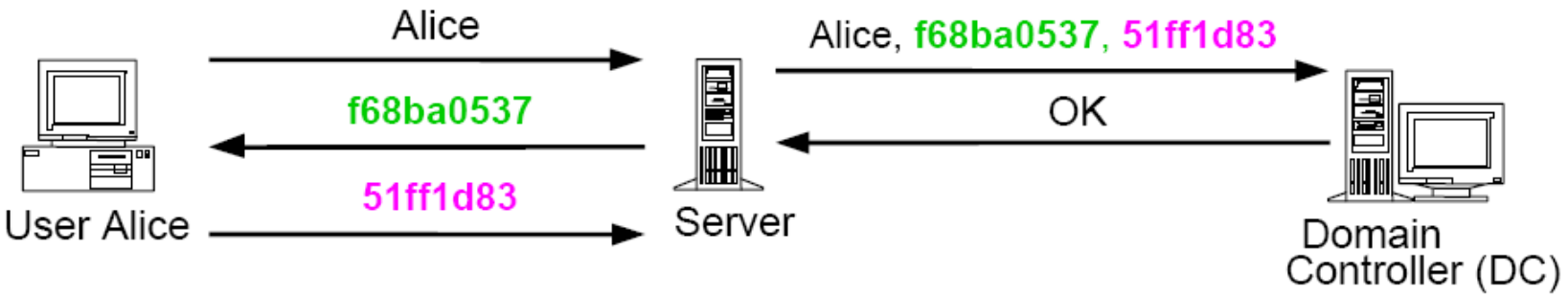
NTLM (cont.)



Protocolul NTLM

Domain: **Wonderland**
Username: **Alice**
Password: **2Uh7&**

User Alice: **Key_A**



H(2Uh7&) = Key_A
E(f68ba0537, Key_A) = 51ff1d83

Challenge: f68ba0537

E(f68ba0537, Key_A) = 51ff1d83
Comparison with 51ff1d83 – ok?

H: Hash function
E(x, k): Encryption of x with key k

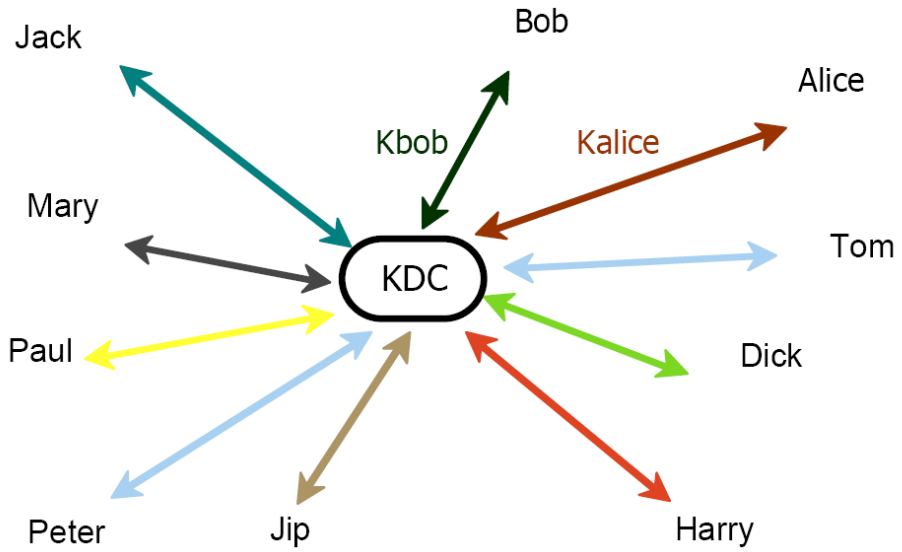
Securitatea NTLM

- **Avantaje:**
  - **Parola utilizatorului nu este niciodată transmisă în clar**
  - **Parola utilizatorului este cunoscută numai de către DC**
  - **Protocol simplu şi eficient dacă de folosesc parole sigure**
- **Dezavantaje:**
  - **Protocolul de autentificare trebuie repetat pentru fiecare server în parte**
  - **DC reprezintă un element critic (BDC)**
  - **Parolele slabe sau scurte pot fi sparte offline prin atacuri de tip dicţionar**
    - **L0phtcrack (http://www.atstake.com/research/lc/)**
    - **Cain & Abel (http://www.oxid.it/cain.html)**

Kerberos

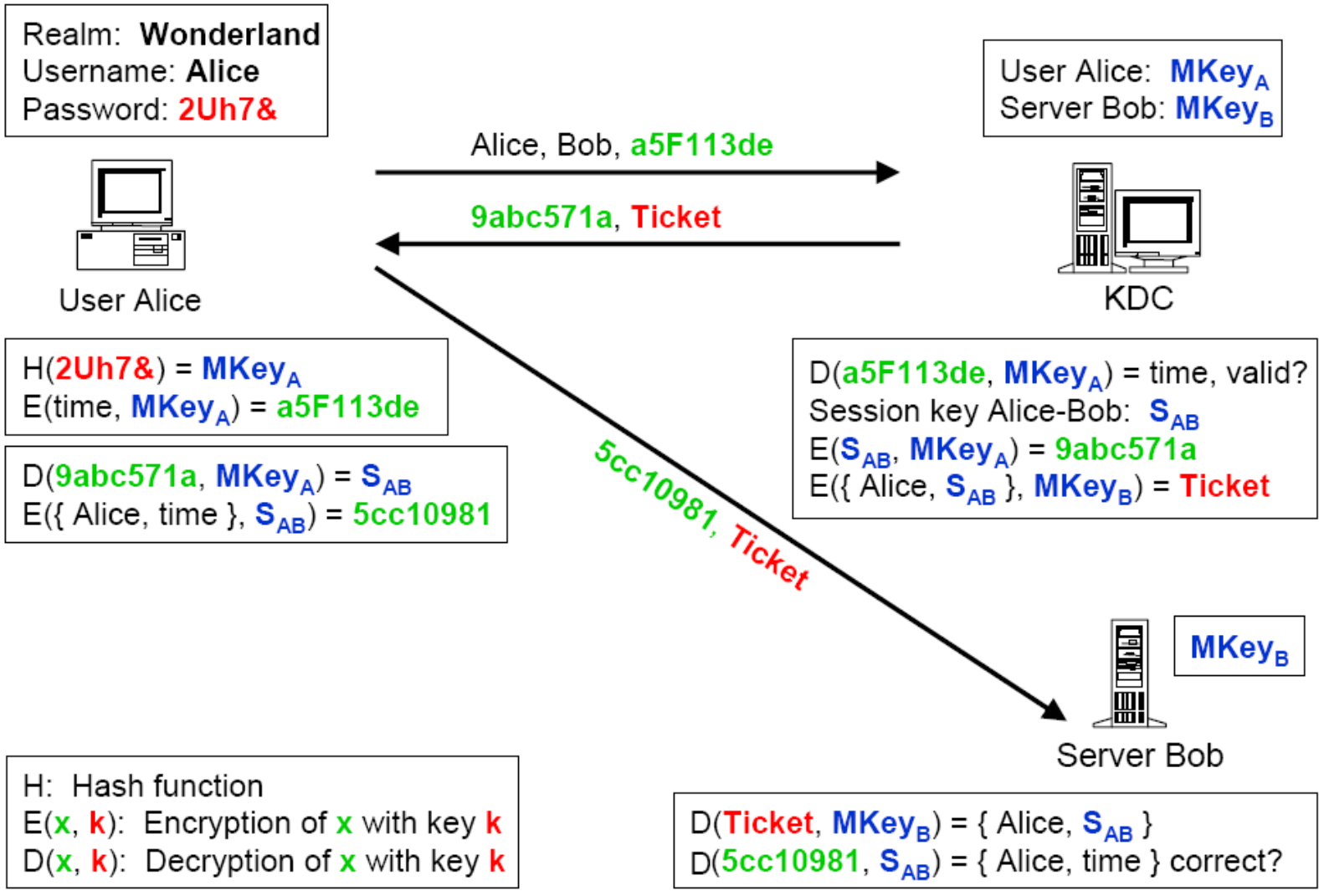
- Dezvoltat în 1983 în cadrul proiectului Athena de la Massachusetts Inst Technology (MIT)
  - http://web.mit.edu/kerberos/www/
- Autentificarea în reţele TCP/IP bazate pe sisteme Unix
- Algoritmi criptografici simetrici (DES)
- Se bazează pe serviciile de mediere oferite de un terţ de încredere (KDC - Key Distribution Center)
- Autentificare mutuală între entităţi
- Versiunea curentă v5 (IETF RFC 1510, 1993).
- Windows 2000 / 2003 / 2008 foloseşte o versiune extinsă de Kerberos v5
  - suport pentru certificate digitale (PKINIT)
  - http://www.microsoft.com/windows2000/techinfo/howitworks/security/kerberos.asp

Kerberos KDC



- **Key Distribution Center (KDC)**
- **Fiecare entitate (principal) are câte o cheie secretă master pe care o înregistrează la KDC**
  - **cheile master ale utilizatorilor sunt derivate din parola de login**
- **Toate cheile master ale entităţilor sunt stocate în baza de date a KDC, criptată folosind cheia master a KDC**
  - **securitatea KDC!**
- **Fiecare acces securizat este "mediat" prin intermediul unor tickete Kerberos**

Protocolul Kerberos Simplificat



Protocolul Kerberos Simplificat (cont.)

- **Dezavantaje:**
  - **cheia master a utilizatorului trebuie folosită de fiecare dată când se accesează un server şi trebuie emis un nou ticket de către KDC (in special dacă timpul de viaţă al ticket-ului este foarte scurt)**
  - **utilizatorul trebuie să introducă de fiecare dată parola atunci când se trimite o cerere de emitere ticket către KDC, sau cheia master a utilizatorului trebuie ţinută într-o memorie temporală (risc de securitate!)**
- **Soluţie: emiterea unei chei de sesiune şi a unui ticket special de către KDC (Ticket-Granting Ticket) având un timp de viaţă mai lung (8-24 ore)**
  - **utilizatorul trebuie să introducă mai rar parola**

Protocolul Kerberos
Autentificarea Iniţială

Realm: **Wonderland**
Username: **Alice**
Password: **2Uh7&**

User Alice

AS_REQ [Alice, **a5F113de**] →

← AS_REP [**27LnZ8vU**]

User Alice: $MKey_A$
Server Bob: $MKey_B$

KDC

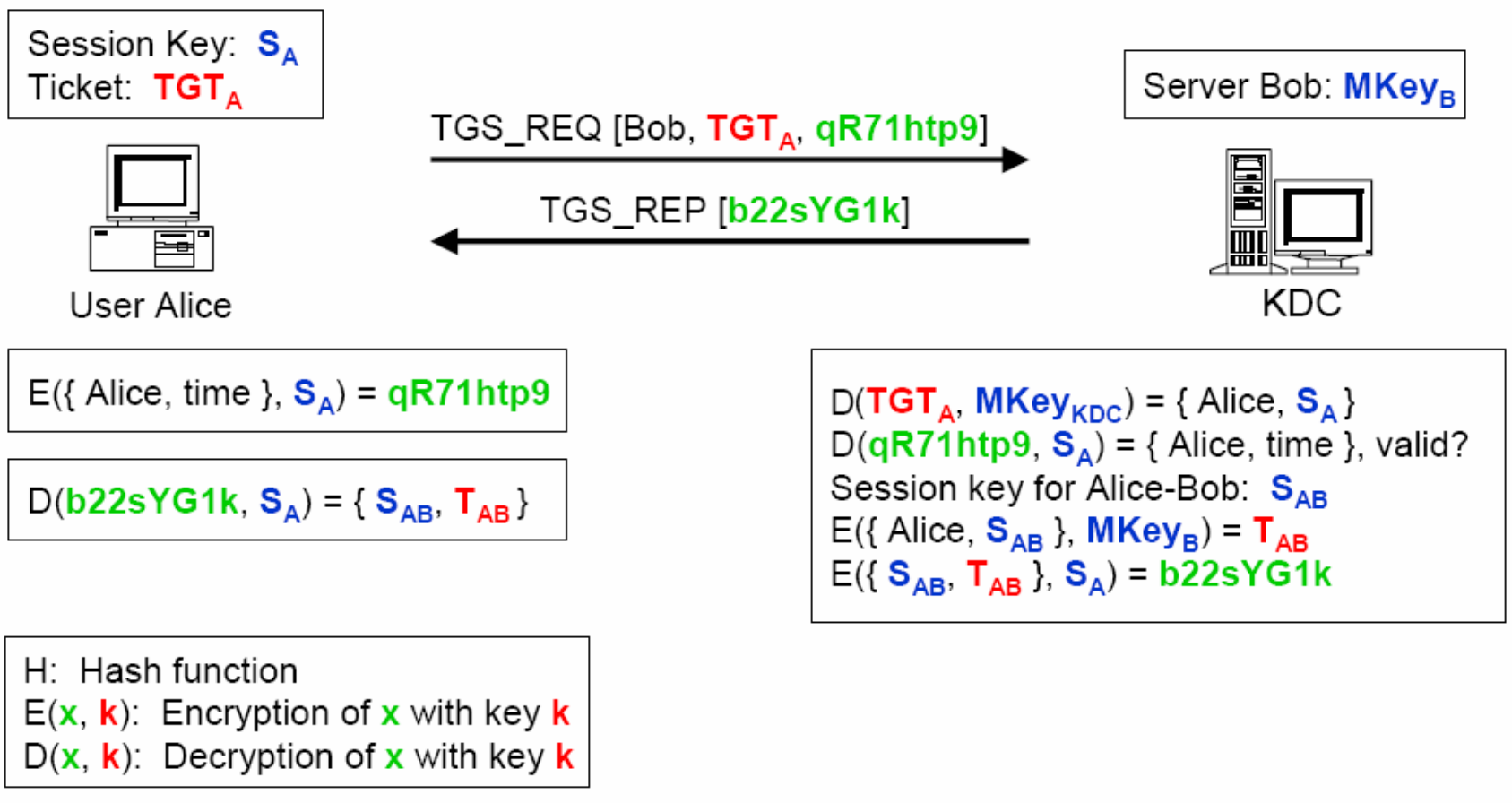
$H(2Uh7\&) = MKey_A$
$E(time, MKey_A) = a5F113de$

$D(27LnZ8vU, MKey_A) = \{ S_A, TGT_A \}$

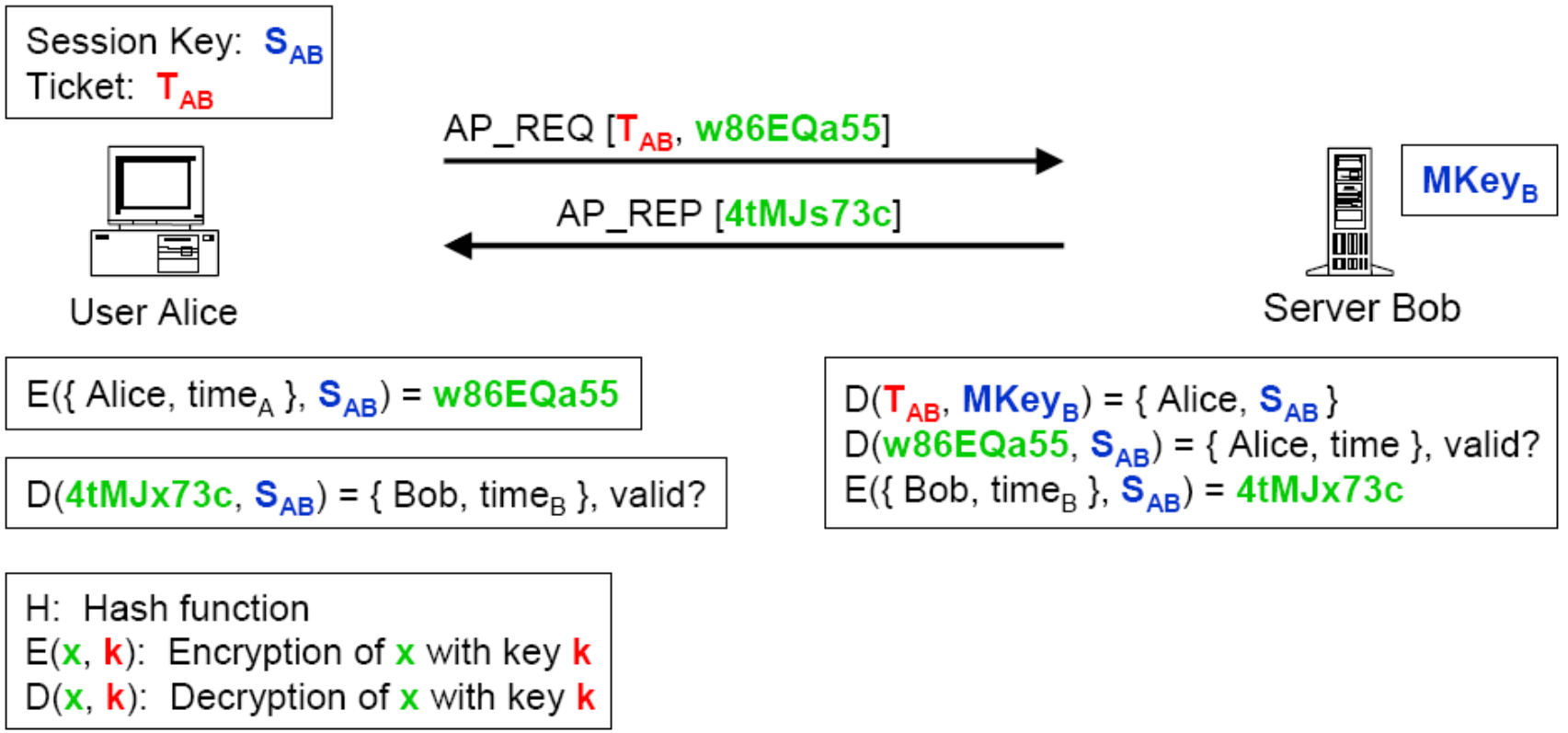
$D(a5F113de, MKey_A)$ = time, valid?
Session key for Alice: S_A
$E(\{ Alice, S_A \}, MKey_{KDC}) = TGT_A$
$E(\{ S_A, TGT_A \}, MKey_A) = 27LnZ8vU$

H: Hash function
E(x, k): Encryption of x with key k
D(x, k): Decryption of x with key k

Protocolul Kerberos
Obţinere Ticket de Acces



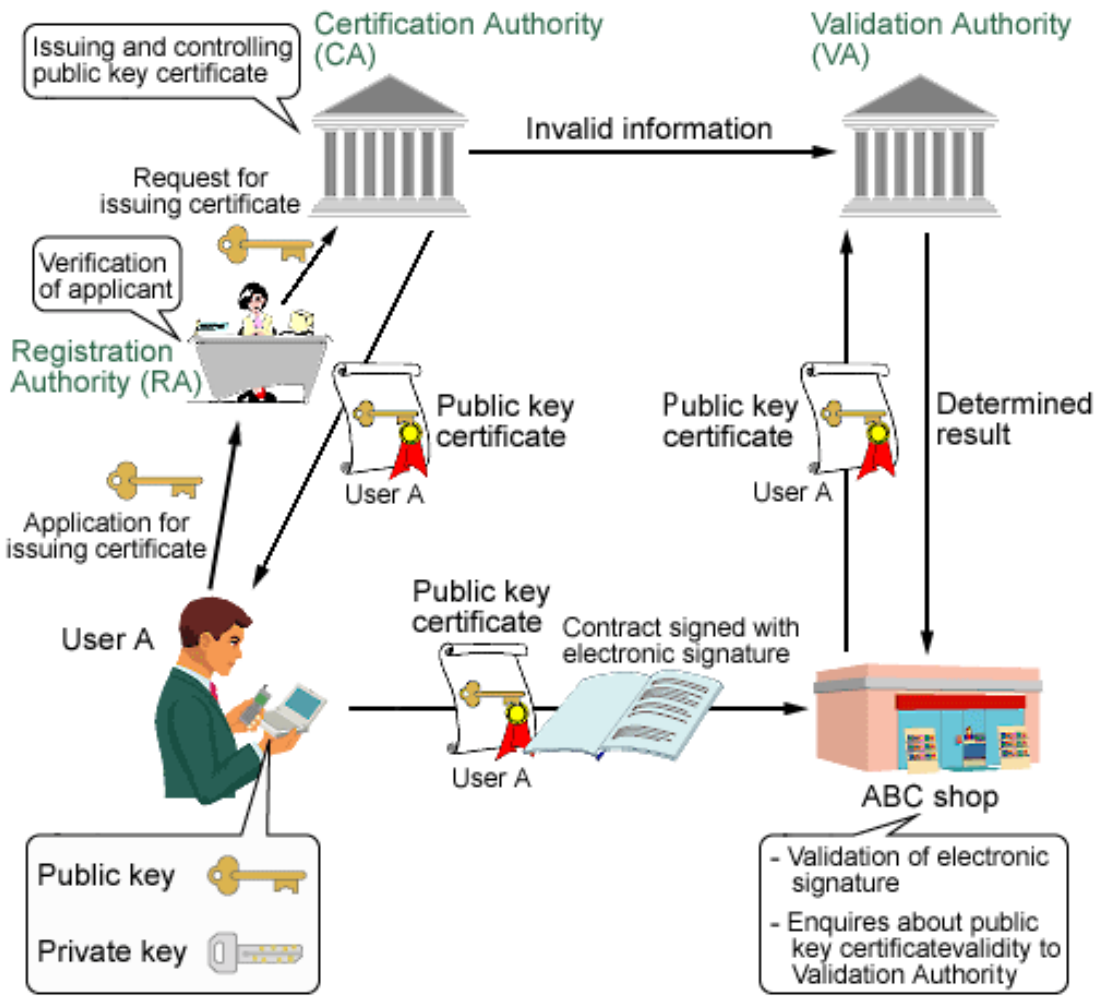
Protocolul Kerberos
Autentificarea Client / Server



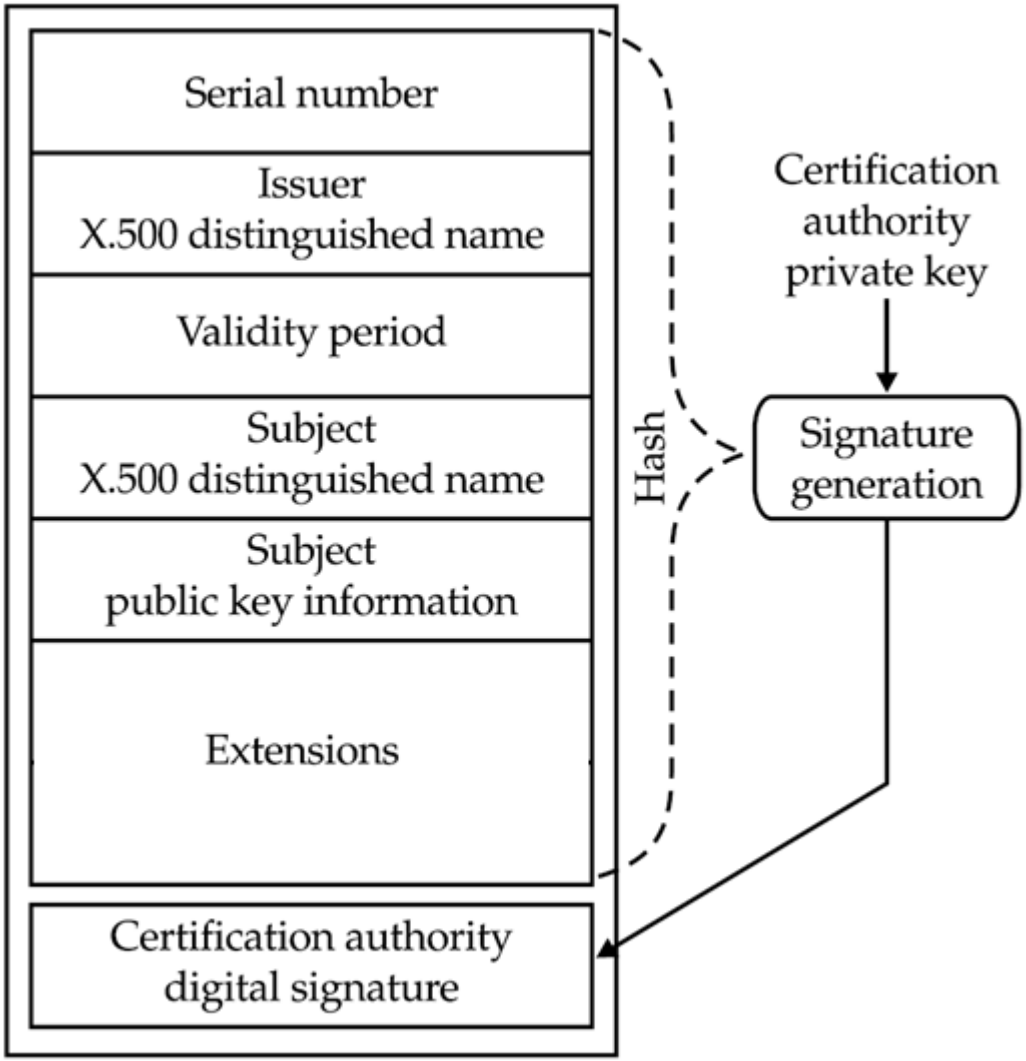
Autentificarea cu Certificate Digitale

- ITU-T Recommendation X.509: Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
- Infrastructuri de Chei Publice (PKI)
  - Autoritate de Certificare (CA) = terţ de încredere care garantează faptul că o cheie aparţine unei entităţi
  - certificate digitale de chei publice

Infrastructuri de Chei Publice (PKI)



Certificate digitale X.509



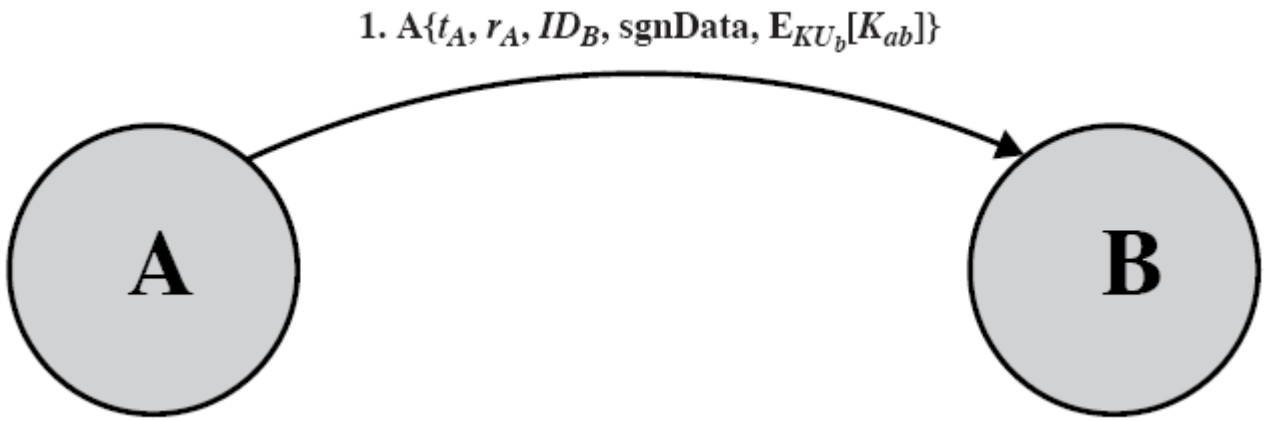
Certificate digitale X.509 (cont.)

- Subject X.500 Name
  - C = RO, O = MTA, CN = Ion Bica, E = ibica@mta.ro
- Subject Alternative Name
  - Adresa de e-mail (rfc822Name)
  - Windows username (UPN)
- Subject Public Key
- Key Usage
  - digitalSignature (short term signatures)
  - nonRepudiation (long term signatures)
  - keyEncipherment
  - keyAgreement
- Extended Key Usage
  - serverAuthentication
  - clientAuthentication
  - codeSigning
  - emailProtection
- CRL Distribution Points

Protocoale de autentificare X.509

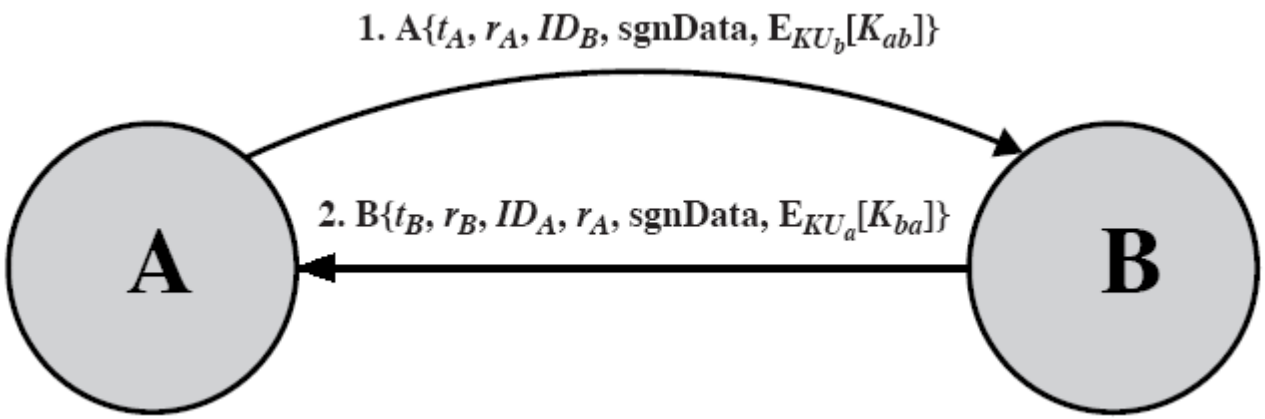
- Autentificarea se realizează făcând dovada posesiei cheii private asociate cheii publice din certificat
  - semnarea digitală a unor date arbitrare
- Certificatul digital în sine nu constituie un factor de autentificare (este public şi poate fi obţinut de oricine)!
  - certificatul se foloseşte doar pentru validarea datelor semnate de entitatea ce urmează a fi autentificată
- Protocoale de autentificare X.509
  - One-way authentication
  - Two-way authentication
  - Three-way authentication

One-way authentication



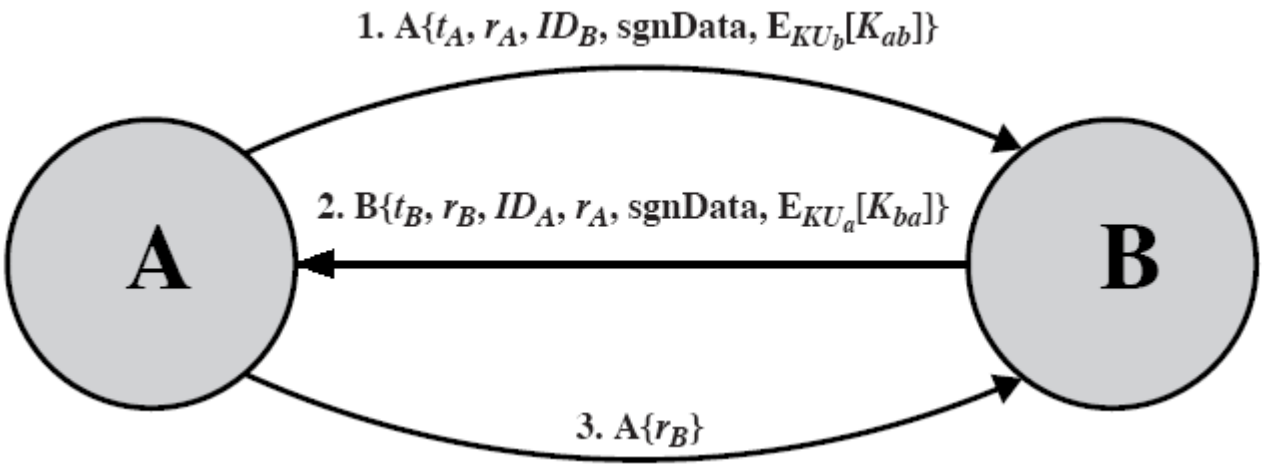
- Un singur schimb de mesaje
- Protocolul asigură:
  - autentificarea lui A la B
  - integritatea şi originalitatea datelor (mesajul nu a fost trimis de mai multe ori)

Two-way authentication



- Două schimburi de mesaje
- Protocolul asigură în plus:
  - autentificarea lui B la A
  - integritatea şi originalitatea răspunsului

Three-way authentication

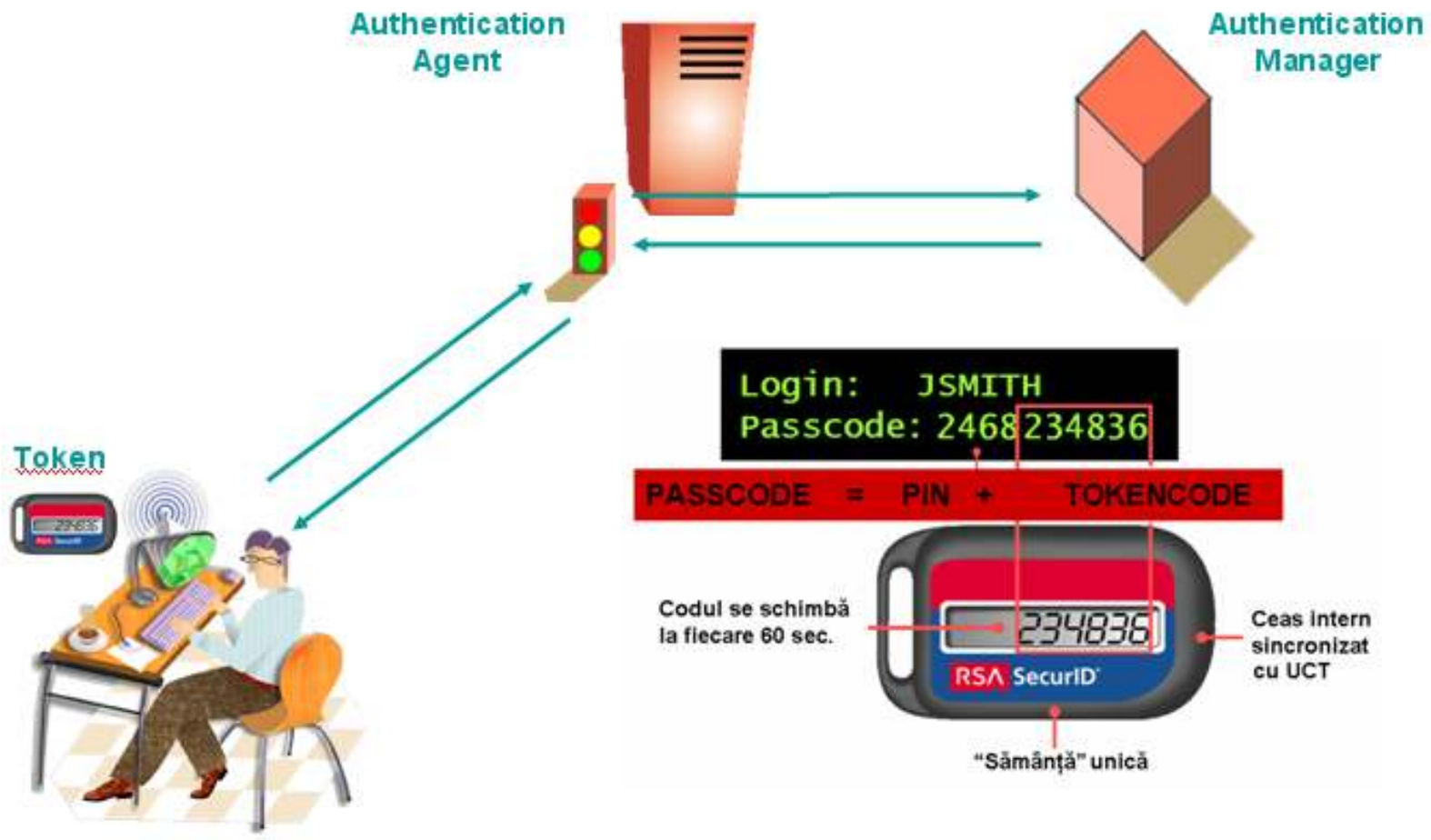


- Trei schimburi de mesaje
- Protocolul asigură în plus:
  - evitarea atacurilor prin reluare în cazul în care ceasurile celor două sisteme nu se pot sincroniza

Generatoare de parole de unică folosinţă

- Parolele sunt vulnerabile la o serie de atacuri
  - pot fi interceptate
  - pot fi ghicite sau sparte prin încercări repetate
- Soluţia: parole de unică folosinţă
  - nu pot fi refolosite dacă sunt interceptate
  - RSA SecurID (www.rsa.com) – standard de facto
  - Vasco (www.vasco.com)
  - Cryptocard (www.cryptocard.com)
  - ActivIdentity (www.actividentity.com)
  - Secure Computing (www.securecomputing.com)

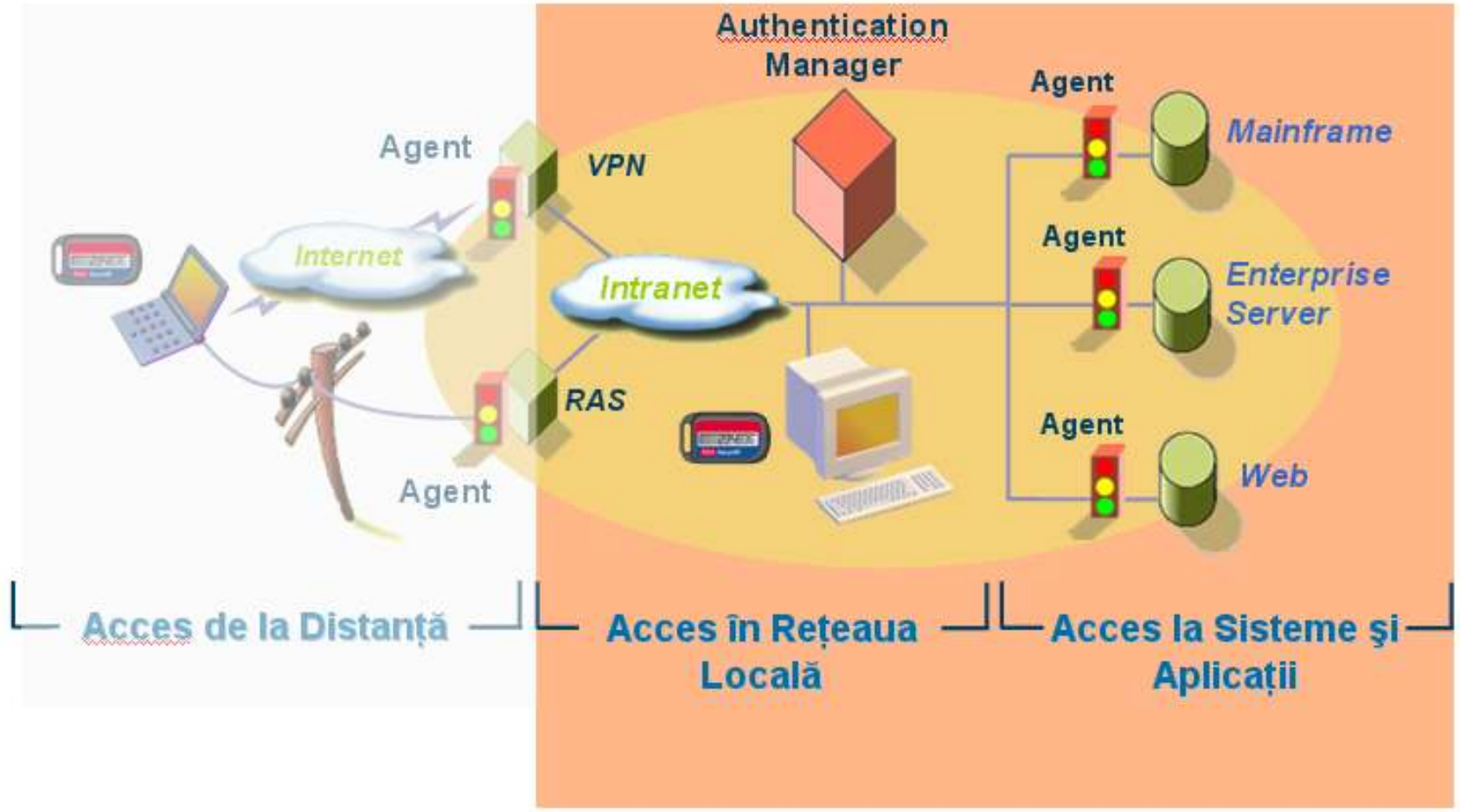
RSA SecurID



RSA SecurID (cont.)

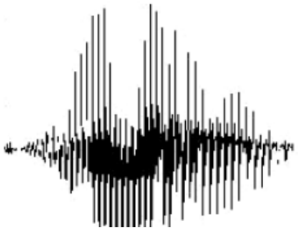
- **Dispozitive de autentificare**
  - Key Fob
  - Card
  - PIN Pad
  - Software + Smart Card
  - PDA, Mobil

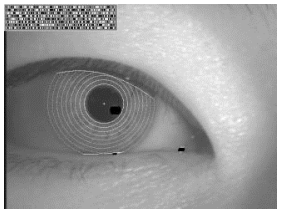
RSA SecurID (cont.)

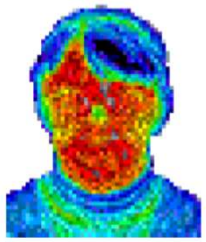


Metode Biometrice

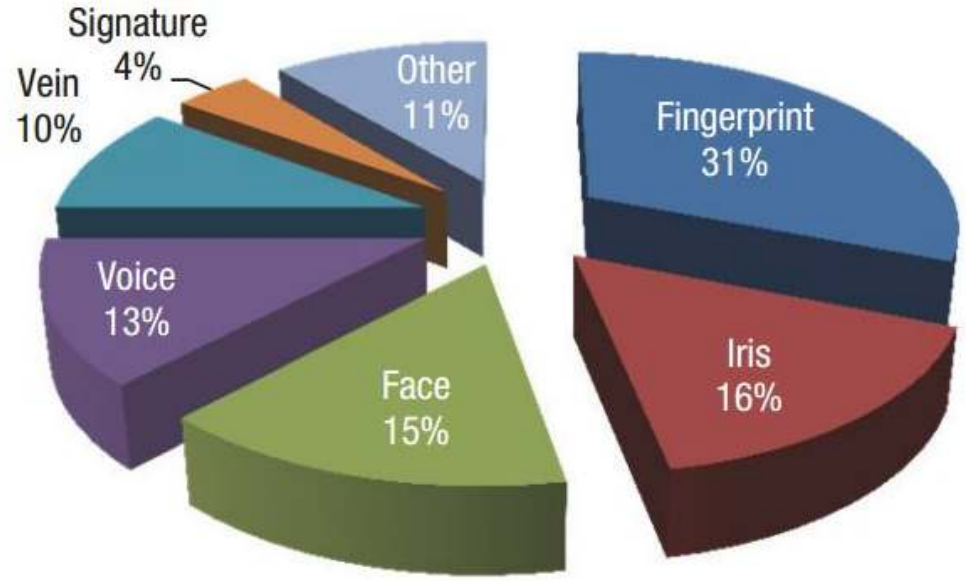
- Amprenta
- Voce
- Iris
- Geometria feţei
- Geometria mâinii
- Semnătura olografă
- Scanarea retinei
- Amprenta termică a feţei
- ADN
- …





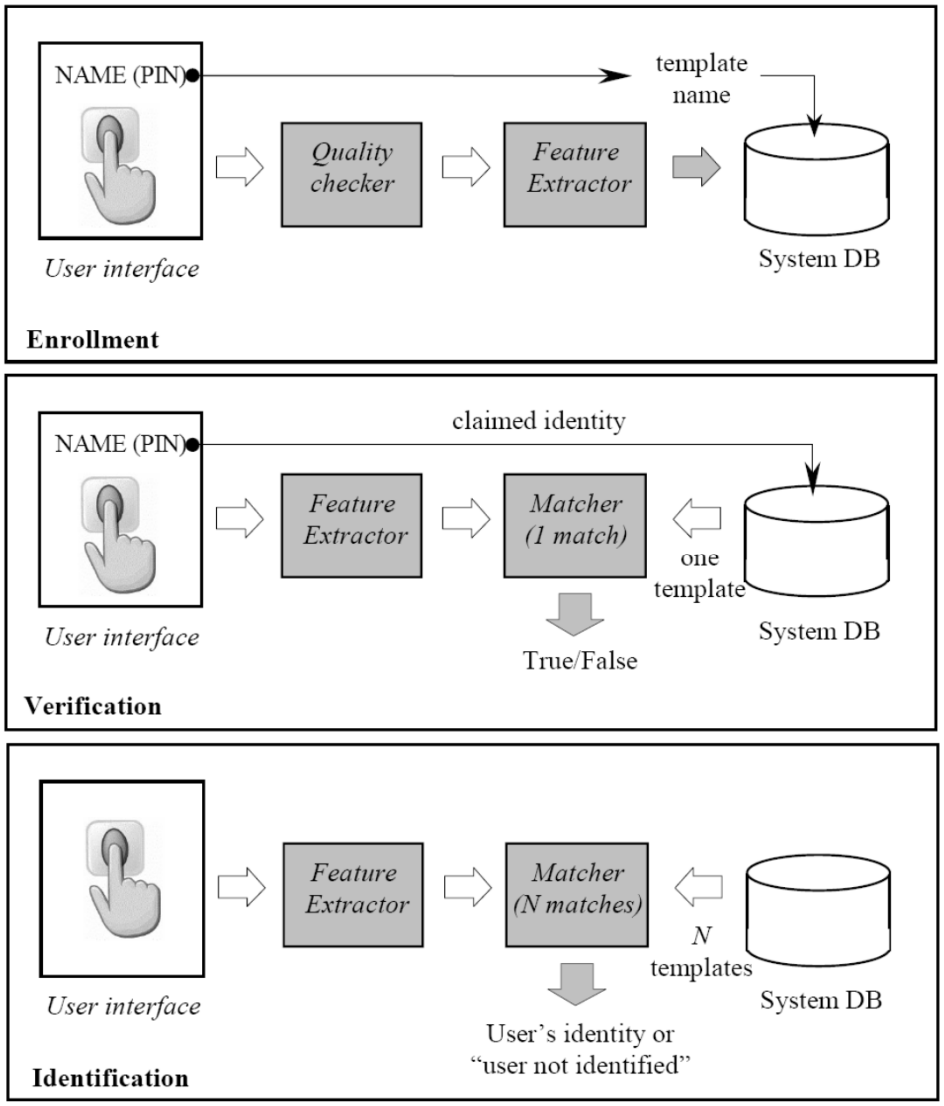


Metode Biometrice (cont.)

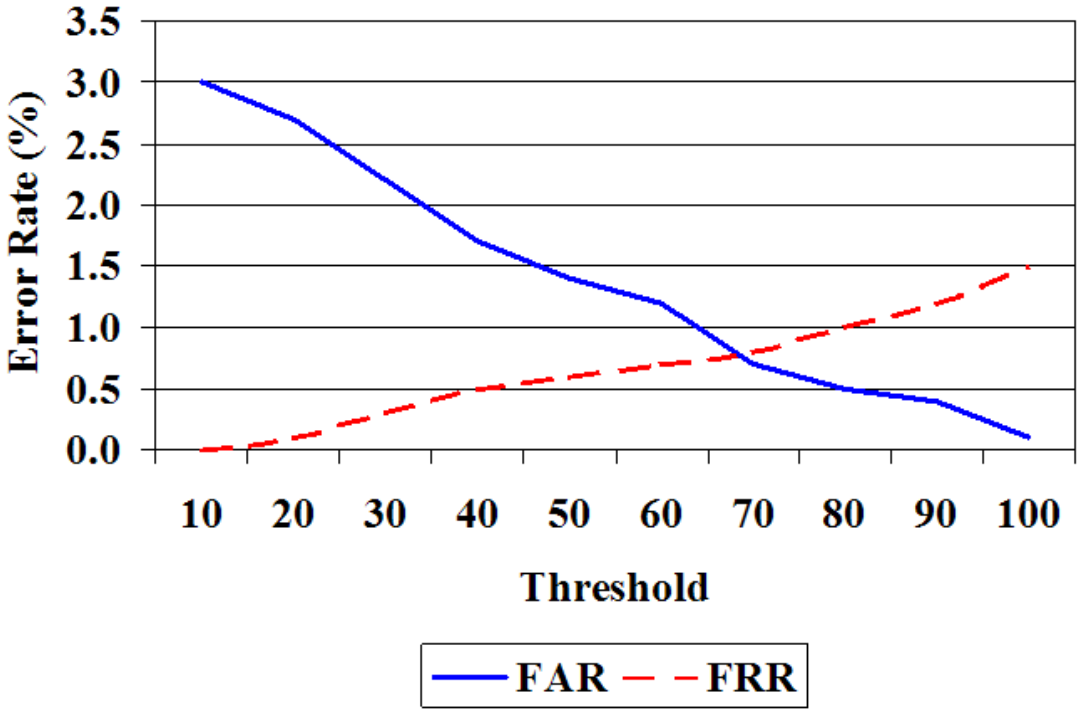


Biometrics market share (2015)

Sistem Biometric



Performanţa Sistemelor Biometrice



- False Acceptance Rate (FAR) – Procentul de impostori acceptaţi în mod greşit de către sistem
- False Rejection Rate (FRR) – Procentul de utilizatori valizi rejectaţi în mod greşit de către sistem
- Threshold – Valoare ce trebuie setată pentru a controla rata erorilor