Securitate în Tehnologia Informației

Universitatea “Transilvania” din Brasov

5 Autentificare - Kerberos

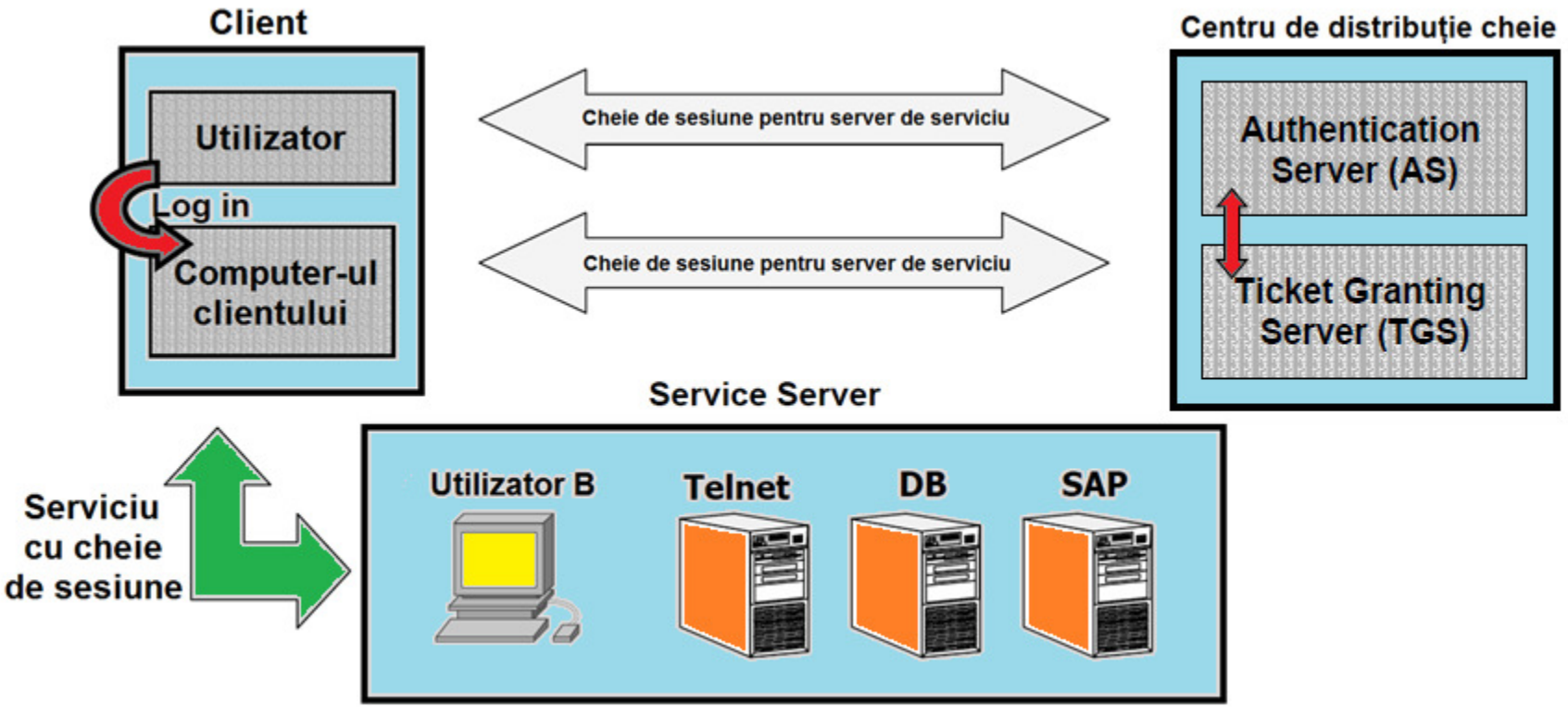
1. Cunoștințe și posesie
2. Metoda Challenge Response
3. Kerberos
4. Smart card și elementele biometrice integrate
5. Single Sign On

Kerberos

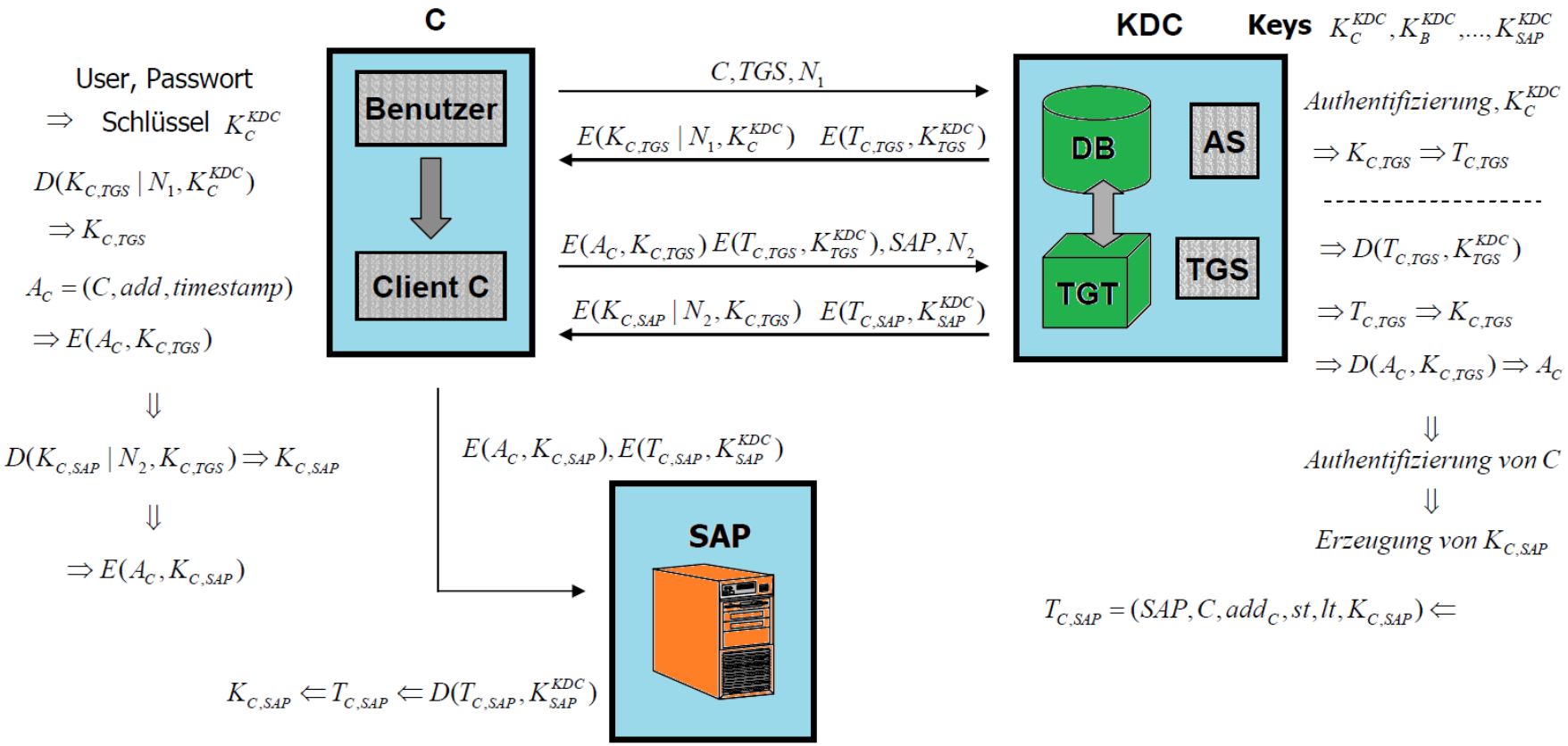
- **Mecanism de autentificare** pentru sisteme distribuite client / server.
- Dezvoltat in 1986 de MIT (Massachusetts Institute of Technology), în colaborare cu IBM și DEC.
- **Obiectiv:** acces la serviciile de rețea pe baza autentificării.
- **Funcționalitate:** (A) Autentificarea directorilor
  (B) Producția si distribuția de chei de sesiune, valabile o singură dată
- **Idee:** Acordarea de bilete la vânzare pentru a obține un bilet de serviciu dupa autentificare
- Bazat pe protocolul Needham-Schroeder extins cu ștampilă de timp
- Criptare folosind **metodă simetrică de criptare**, care poate fi negociată odată cu versiunea 5
- Printr-o ierarhie de **servere de autentificare,** fiecare autonom in zona lor(engl. Realm (tărâm)) de bilete acordate pentru cheie de sesiune, chiar și servicii pentru clienții din afara sferei de competență fară a cere clientului să se re-autentifice; se vorbește asadar de clienți si servere kerebosate în sisteme de rețea (single Sing On).

Principiul protocolului Kerberos

- Țel: Chei simetrice secrete pentru comunicare între client si servicii de server



Kerberos – decurgerea protocolului



Protocolul Kerberos

- **Autentificarea reciprocă**: De asemeanea, serverul de servicii trebuie să se autentifice in fața clientului; acest lucru este pur si simplu posibil, deoarece acesta schimbă ștampila de timp cuprinsa în autentificatorul de client, in funcție de acord și trimite la client cheia secretă de sesiune $K_{C,S}$ criptată. Serverul se face în acest fel credibil in fața clientului deoarece el cunoaște cheile secrete K_S^{KDC}, $K_{C,S}$ și doar el cunoaște ștampila de timp care de exemplu poate a crescut cu 1.
- **Integritatea datelor și non-repudiere :** Conform proiectării Kerberos este data fie integritatea datelor si de non-repudierea mesajului.

Deficiențe ale protocolului Kerberos

- Neajunsurile semnificative ale protocolului de la versiunea 4 au fost eliminate cu versiunea 5.
- In plus, in versiunea 5, este oferită o metoda Challenge-Response.
- Vulnerabilitatea este secretul în siguranța și gestionarea cheii de sesiune (in calculatorul clientului) pentru comunicare confidențială intre client și server.
- Daca un atacator reușește sa compromită cheia secreta pentru autentificator, poate masca adresa de IP conținută.
- Cu toate acestea, **principalul punct slab** este autentificarea bazată pe parolă, care ar trebui înlocuită cu o semnatură digitală bazată pe Smart Card (Legea semnăturii).
- **În viitor:** metoda asimetrică cu PKI conform legii semnăturii.
- **Sincronizarea de timp:** Deoarece serverul de acordare bilet depinde în emiterea cheii secrete pentru sesiunea de comunicare între client si server de amprenta de timp în autentificatorul client, prin manipulari de timp ale unui atacator pot fi inregistrate din nou autentificatorii deja depășiți.

Redirecționarea Kerberos

- Biletele sunt valabile numai în domeniul de aplicație a KDS (Realm), care a eliberat biletul pentru un client; daca ar dori să absoarbă un serviciu, care se află în afara intervalului valid, atunci are nevoie de un bilet valid pentru competențele
- KDS-urile schimbă datele intre ele (mai tarziu).