pas 2.

Serverul T (admin) se uită în matricea de acces -(verifică regulile bell LaPadula) referitor la $\underbrace{U}_{\text{subiect}}$ și $\underbrace{S}_{\text{obiect}}$.

Dacă totul ok. => T îi trimite lui U inf. care îi permit lui U să acceseze S ulterior

-> a) o cheie K : $\{K, U, L, S\}$ criptată cu cheia ~~U~~ K_{UT}.

-> b) mesaj cu destinație server.

$\{K, U, L\}_{KST}$ (criptată cu K_{ST}}

-> stocată într-o bază de date în server; generată la înreg. serviciului

cheia tr. să ajungă la U și la S, criptată cu cheile K_{UT}, și K_{ST} ; L = durata de viață. $\rightarrow$ $\boxed{\text{TIMESTAMP}}$

K e generată de T. și are durată de viață -

-> criptare cu ~~AES~~ sau DES gata impl.

U obt cheia K din prima parte a msg primit de la T

- important să identifice sesiunea în care sunt

3) U trimite lui ~~S~~ mesajul

$\{K, U, L\}_{KST}$ -> criptată cu cheia K

$\{U, t, L\}_K$

cheia K_{UT} partajată între U și T

cheia K_{ST} e partajată între S T