4) S va obține k descriptând mesajul pe care l primește
- decriptează al doilea mesaj, (și face o potrivire între inf din mesajul 1 și mesajul 2, plus Timestamp-ul să fie valid, înainte de expirare).
- ultimul mesaj are rol de confirmare.

$S \xrightarrow{\{t_u, L-1\}_K} U$.

Aici e sfârșitul protocolului cu confirmare
Vezi la fiecare pas

U răspunde lui S $U \xrightarrow{\{\text{rezultat}\}_K} S$

→ S răspunde lui U, $S \xrightarrow{\{m\}_K} U$

Comparație Bell-LaPadula ⇔ Biba.

- high confid. -

- high integrity -

confid. + integritate -

Dată o rețea, clasele de securitate îți dă confid. dar și integritate ⇒ îți o etichetă comună.

- În acest caz, deoarece subiectul Δ poate citi ob. O dacă

$\lambda(\Delta) \geq \lambda(O)$ (pt confid.)
iar $\lambda(S) \leq \lambda(O)$ (pt integritate) $\Rightarrow \lambda(S) = \lambda(O)$.

⇒ un subiect poate citi ob doar de pe același nivel de confidențialitate cu el. ⇒ nu avem curgere de informație - (în niv. de securit. diferite nu avem flux informațional) ⇒ irelevant în