

MODELLO RSA

crittografia a chiave asimmetrica

KpuA

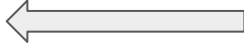


chiunque può richiederle

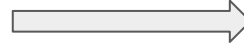


KpuB

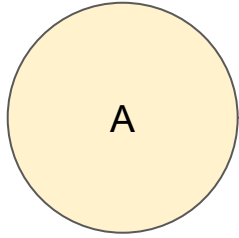
KprA



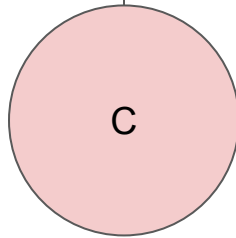
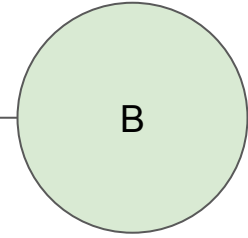
nessuno può richiederle



KprB

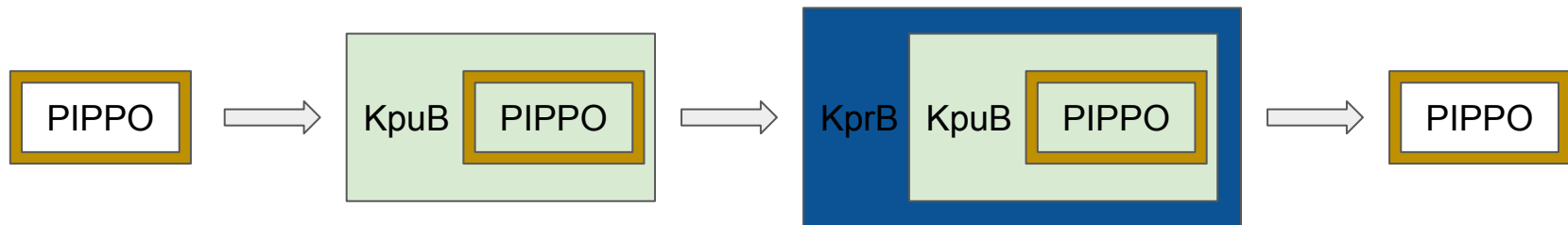
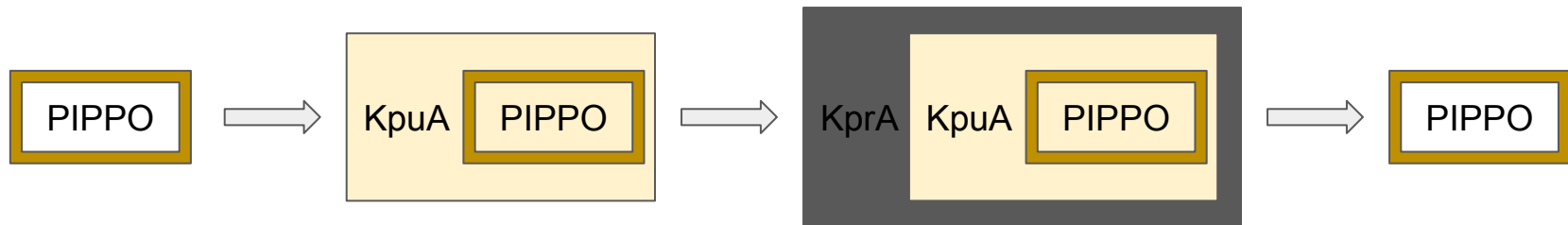


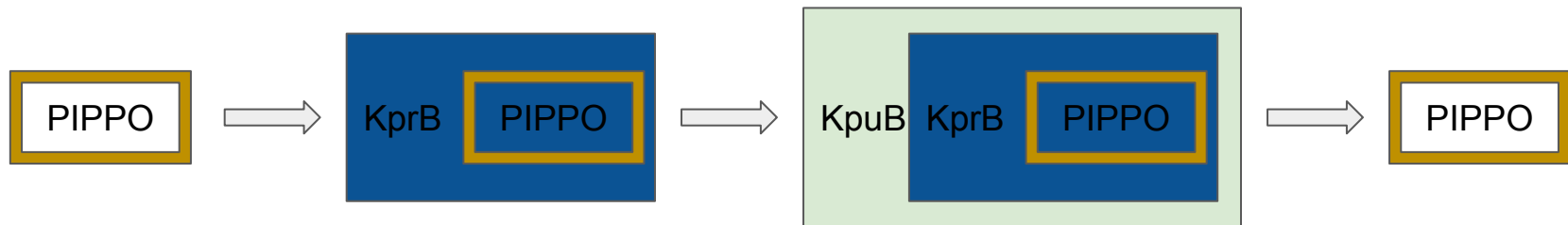
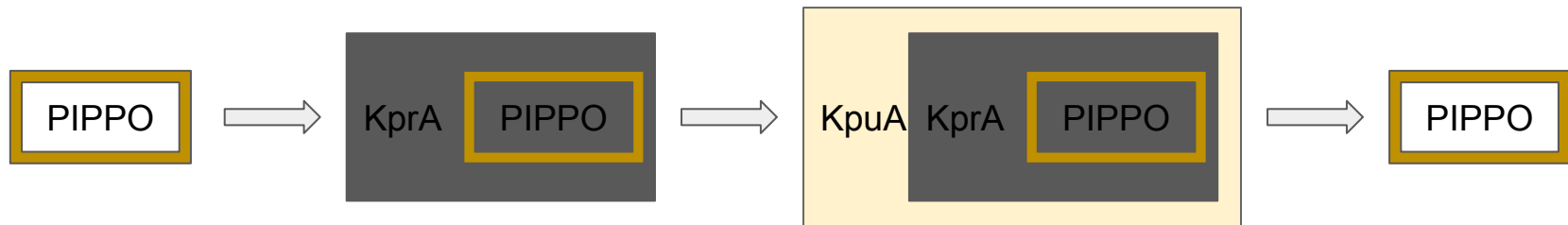
PIPPO



CHIAVI

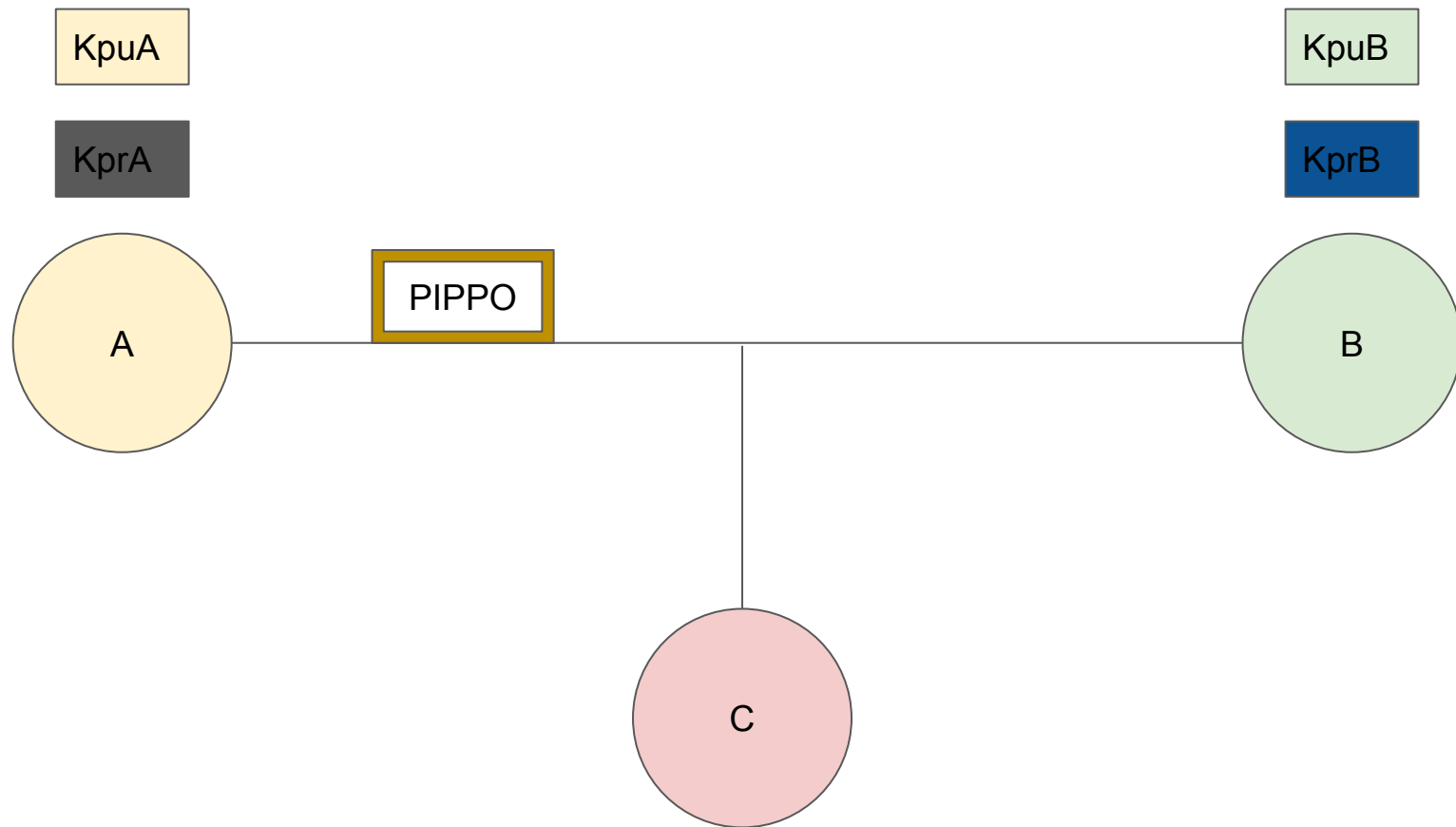
chiavi pubbliche e chiavi private

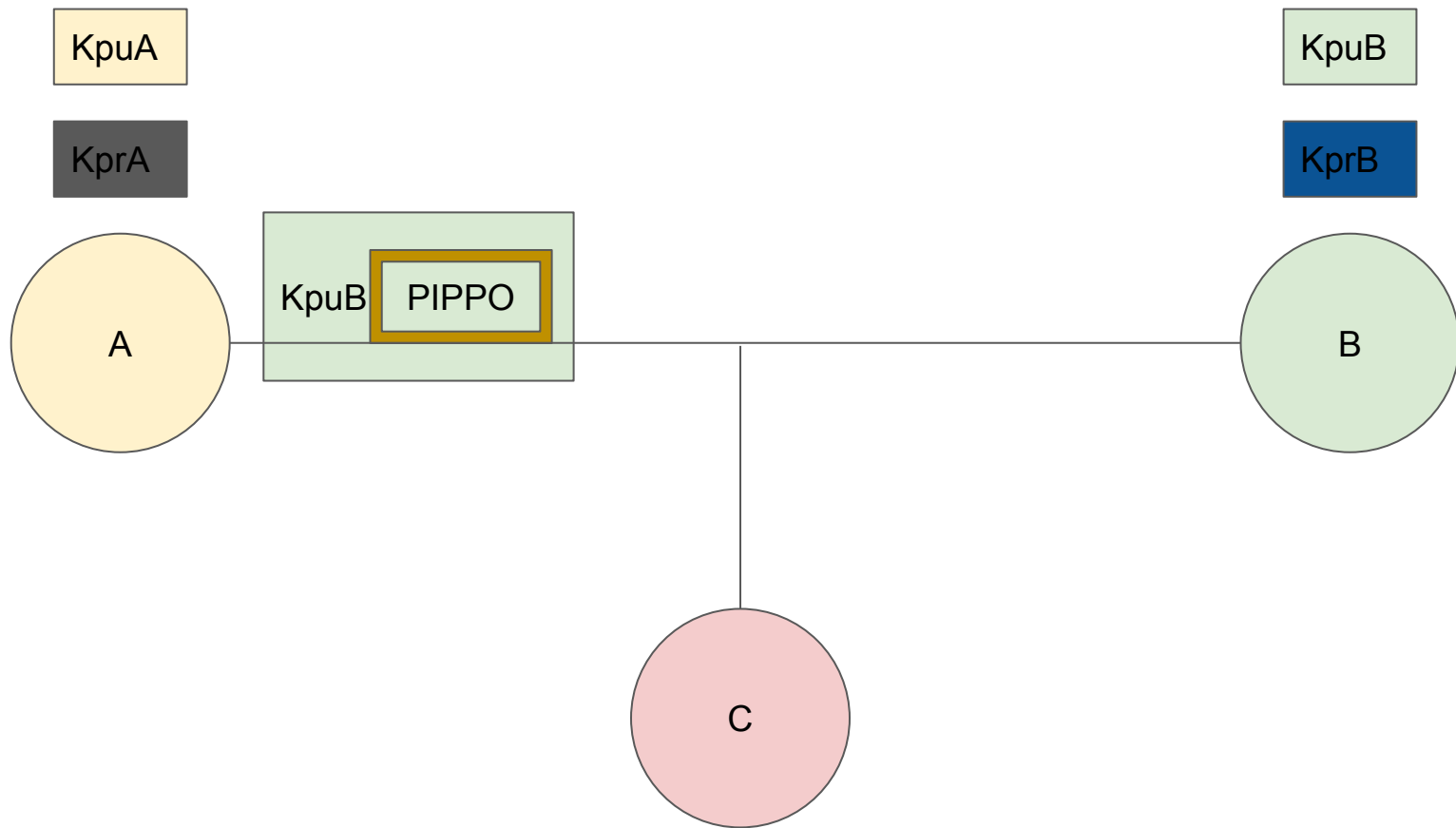


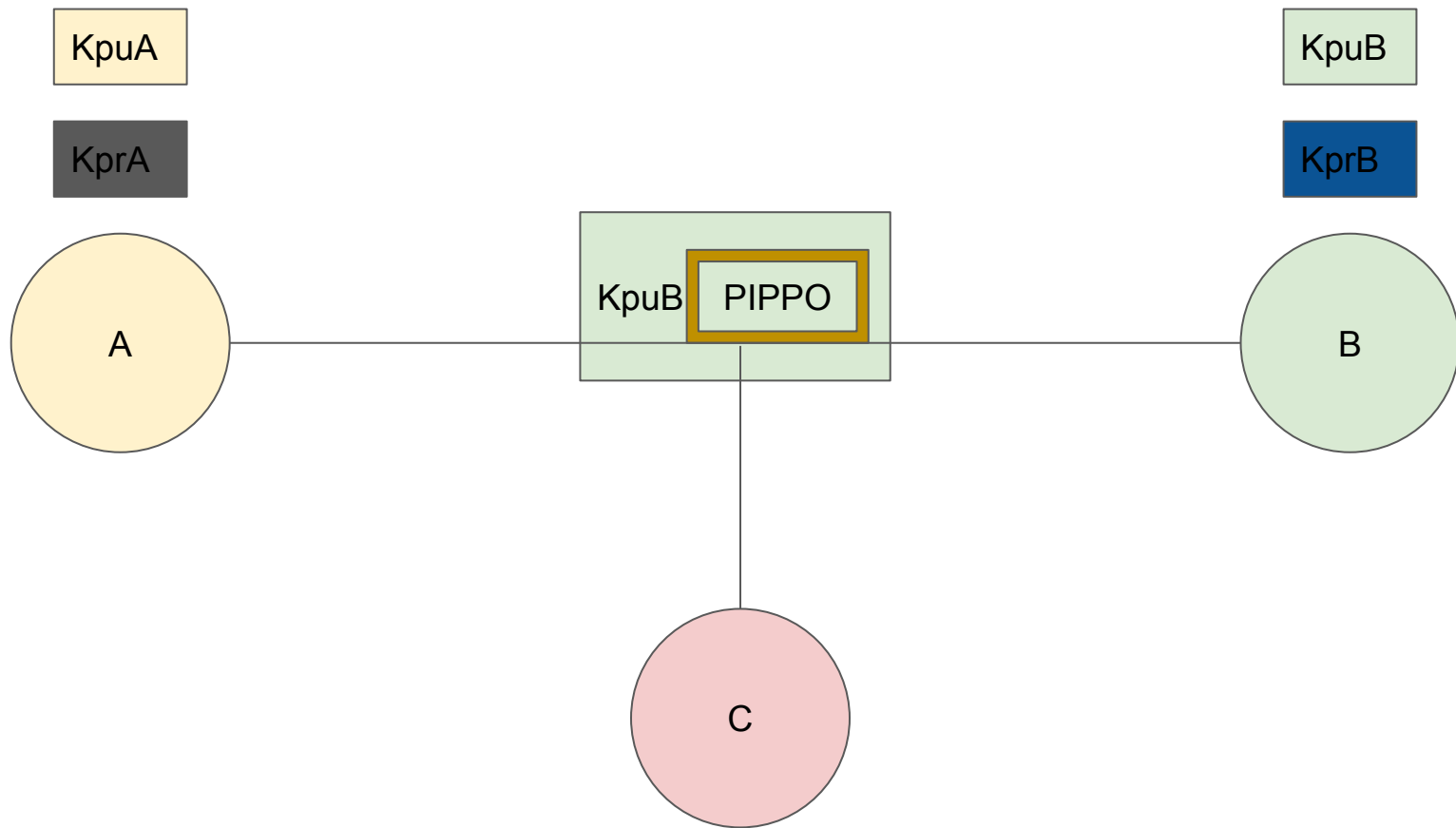


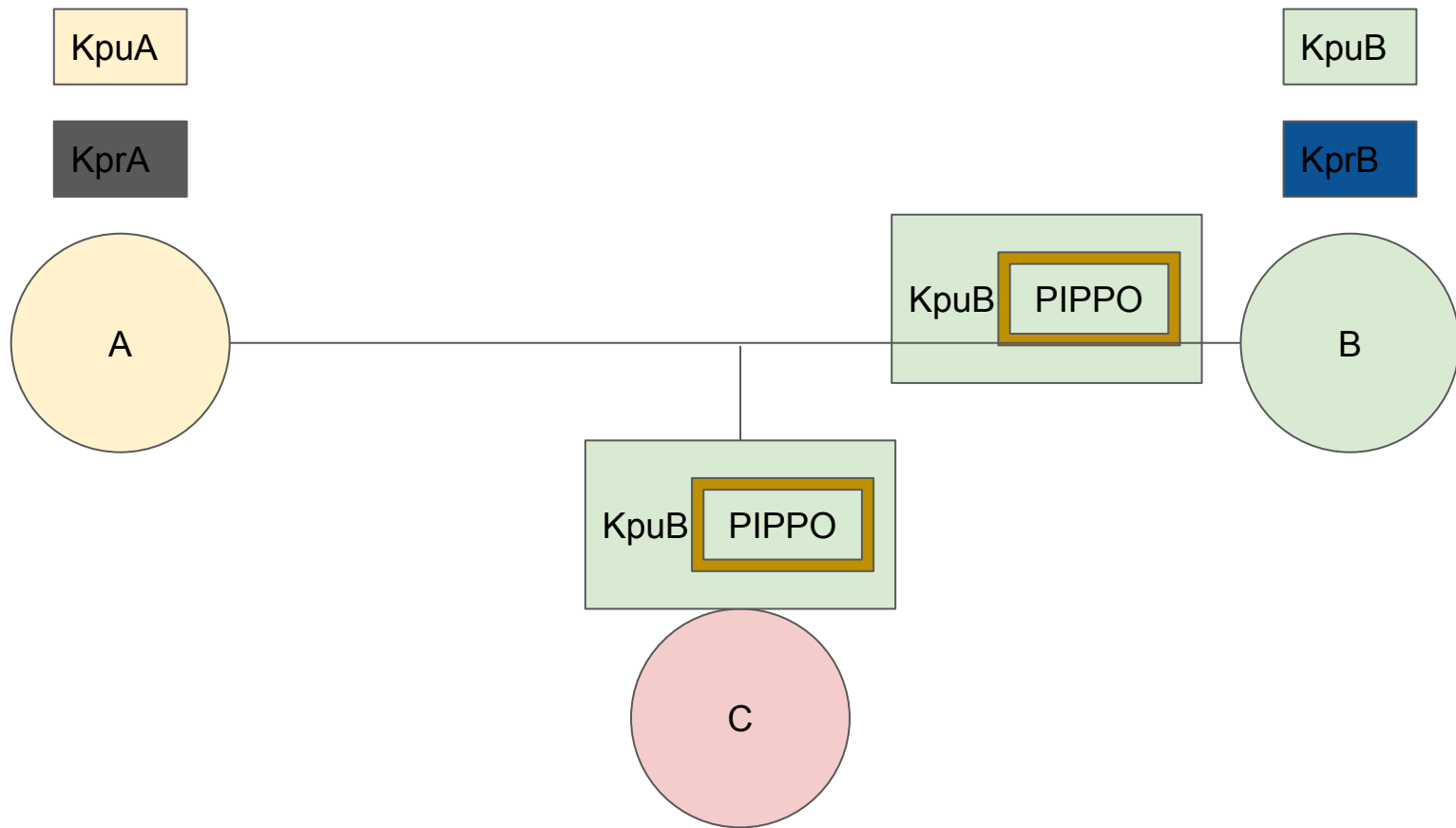
CONFIDENZIALITÀ

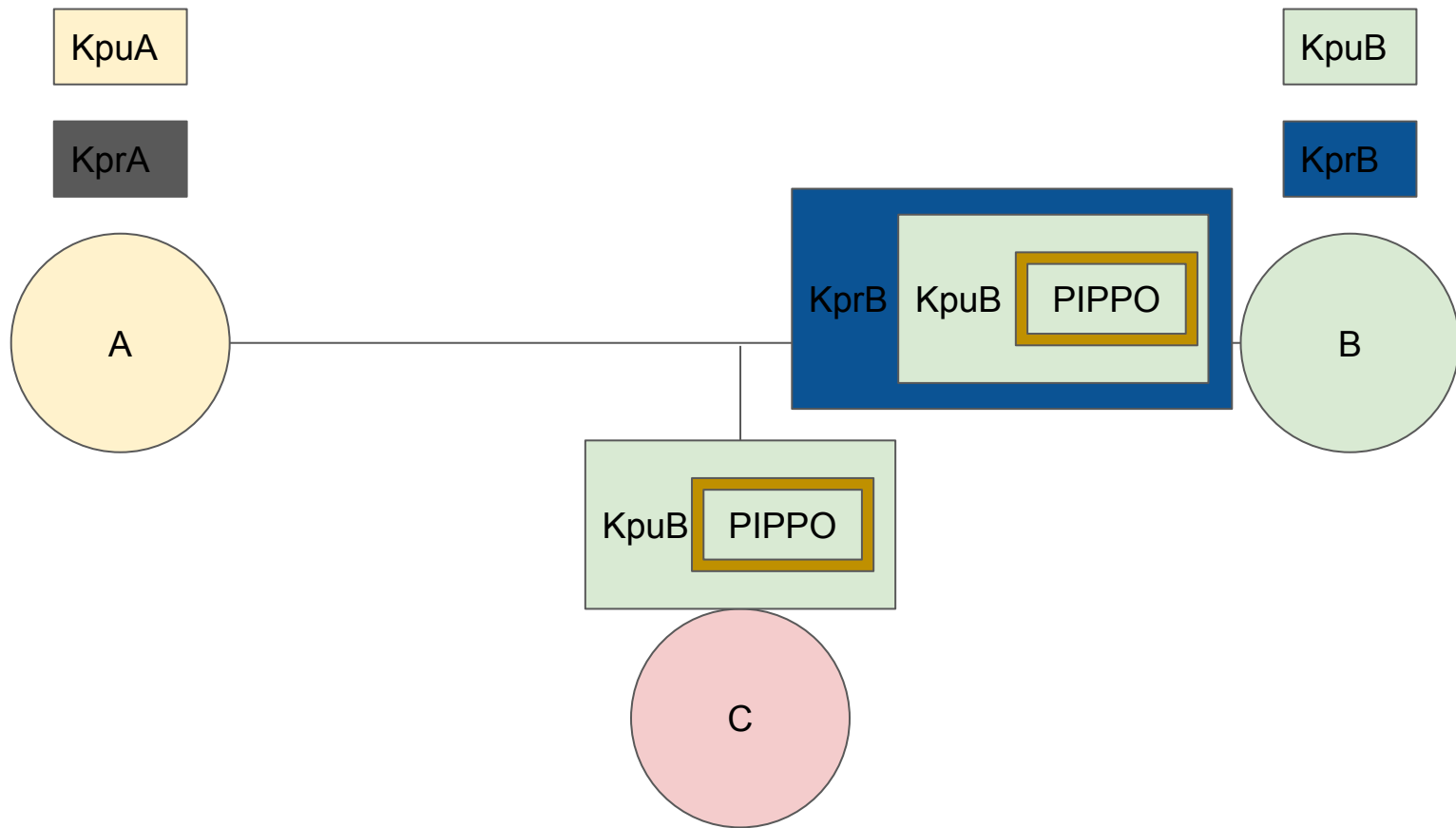
garantire la riservatezza di un messaggio

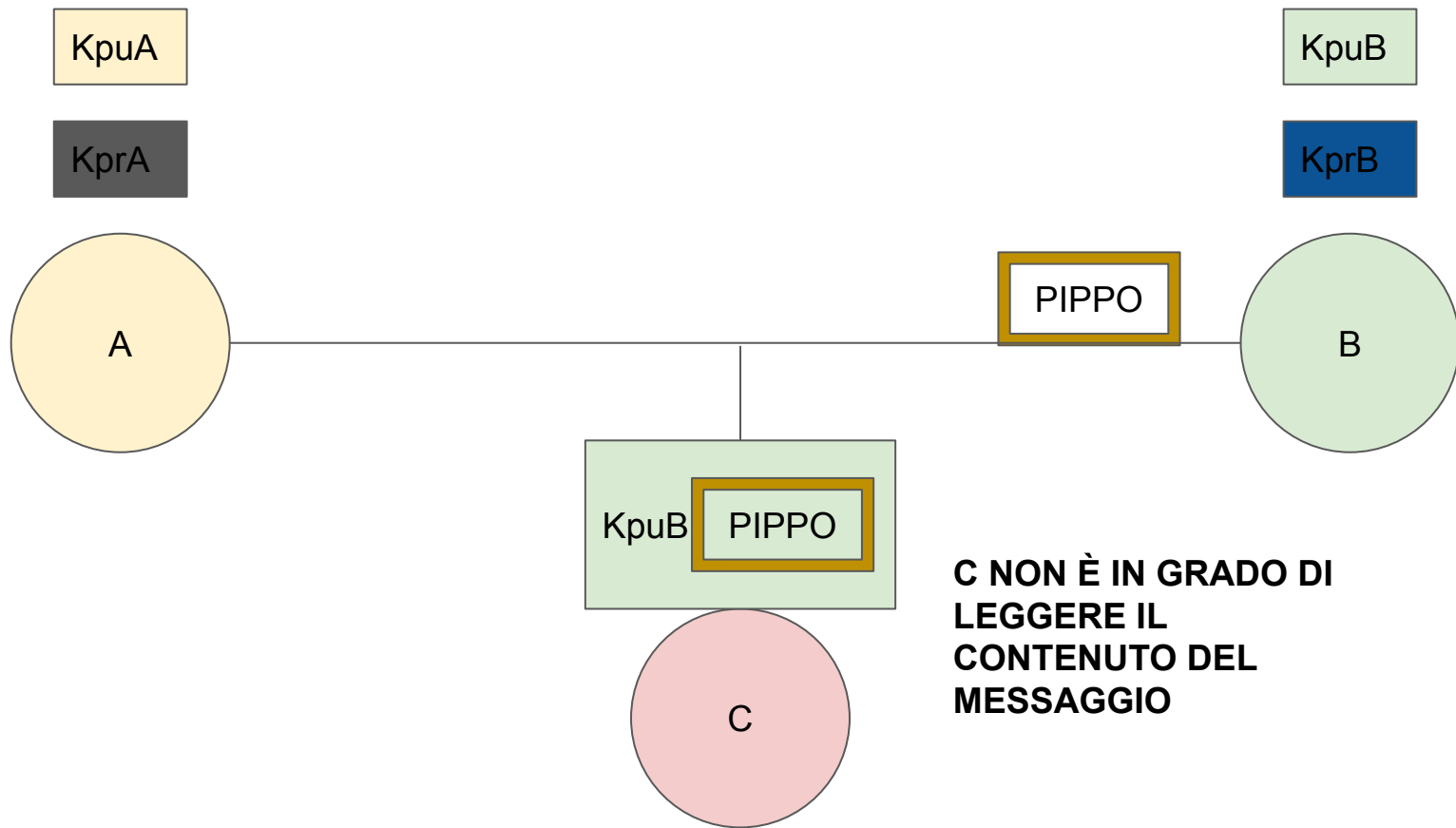


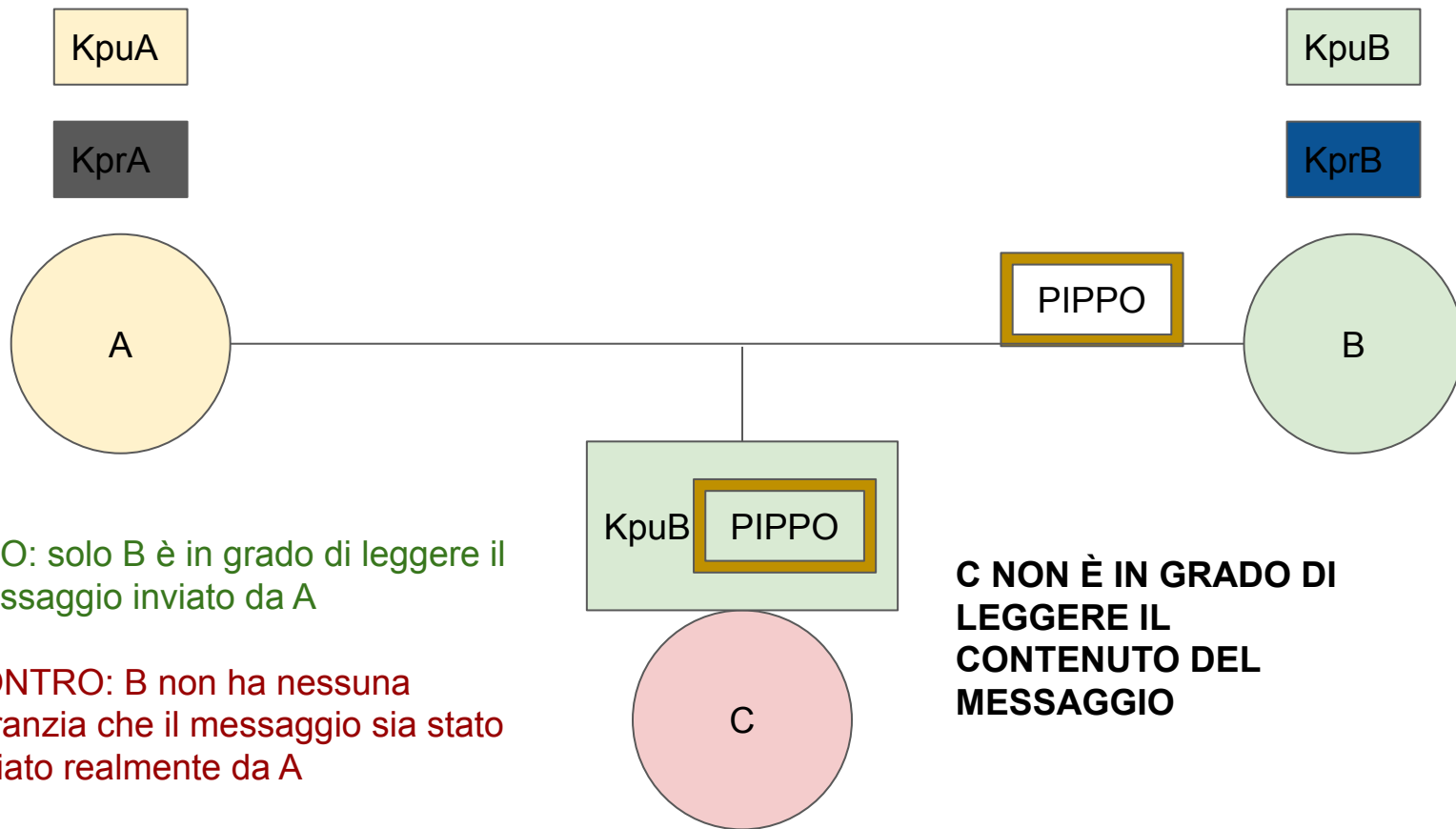






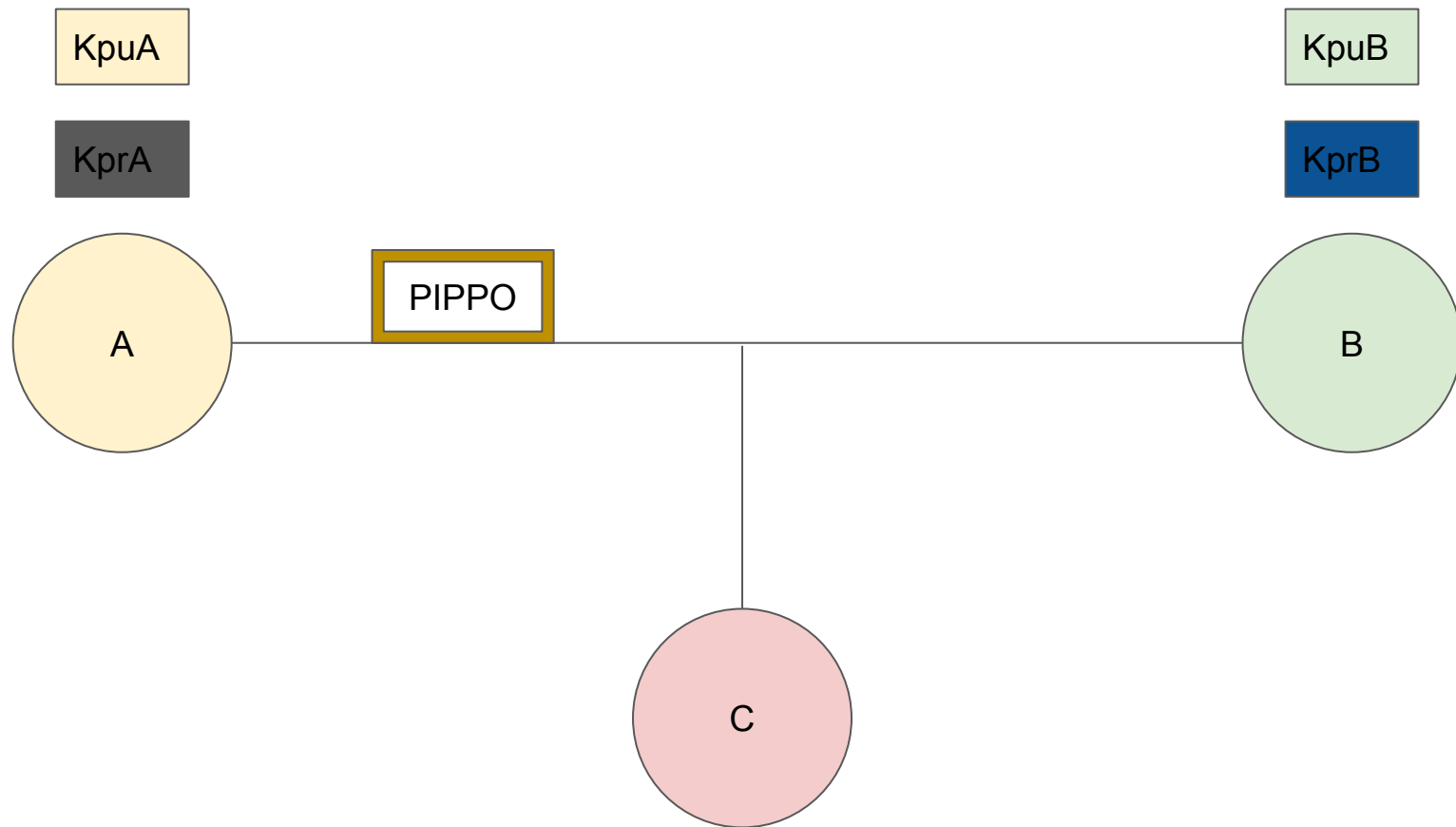


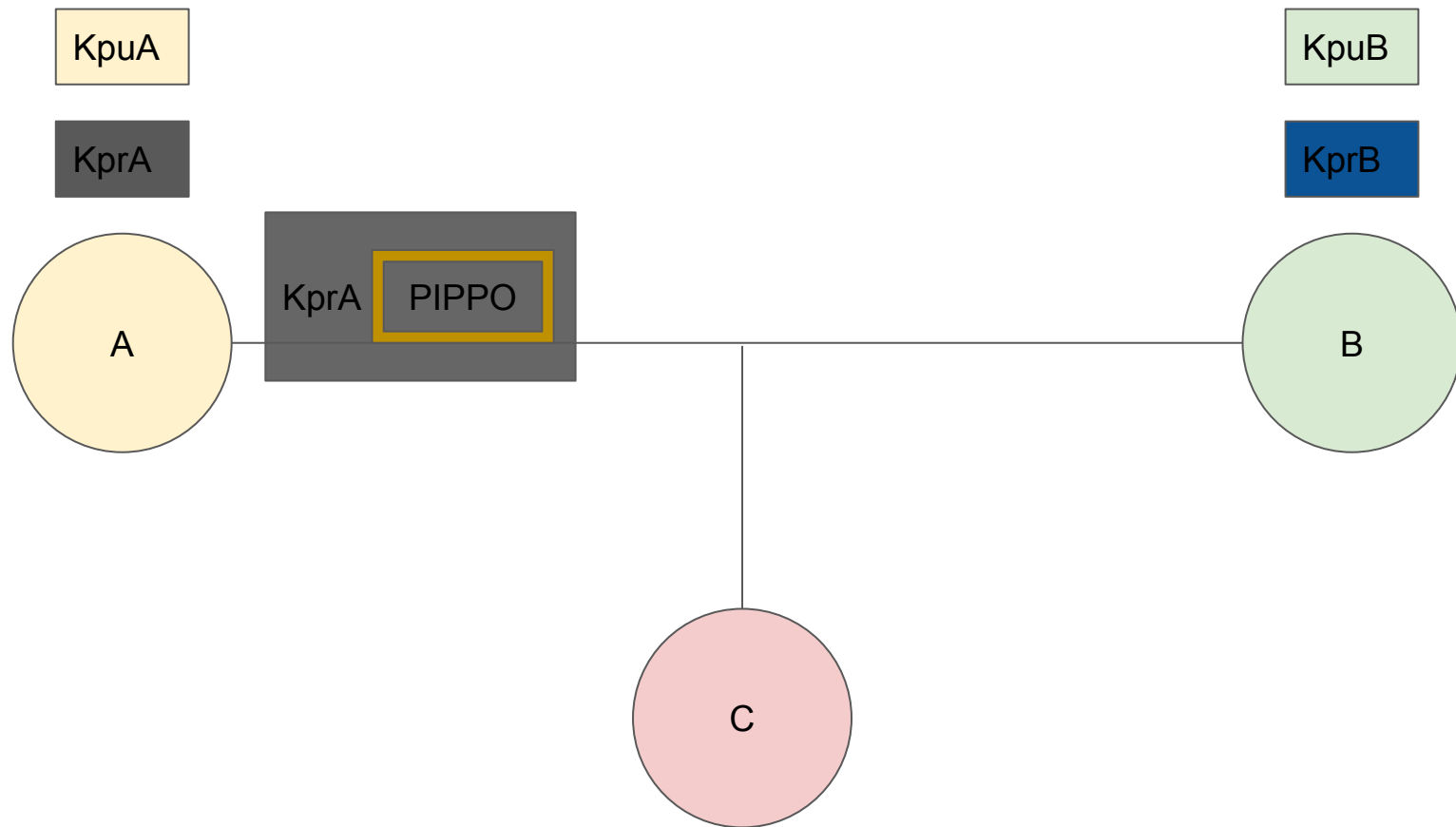


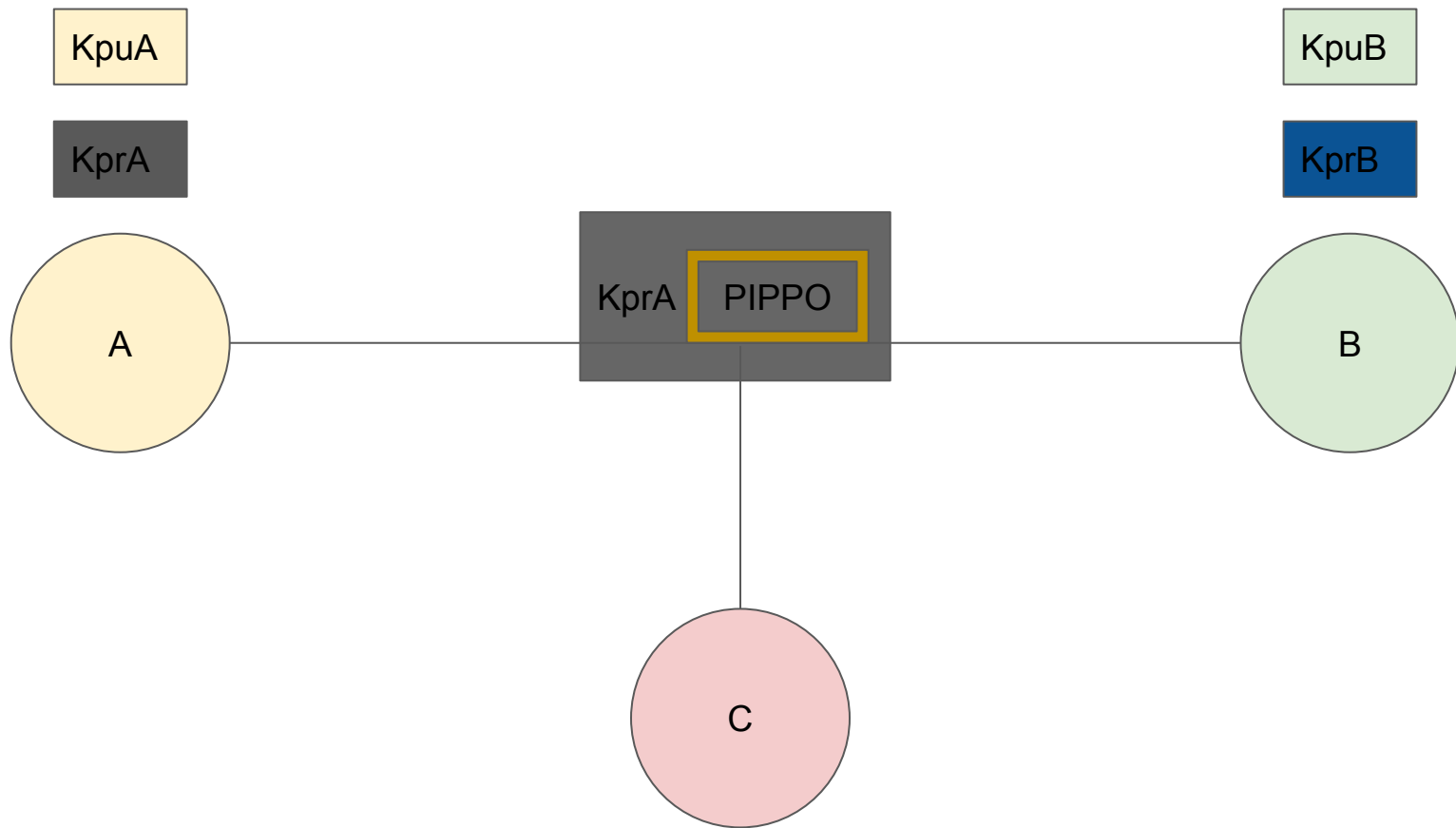


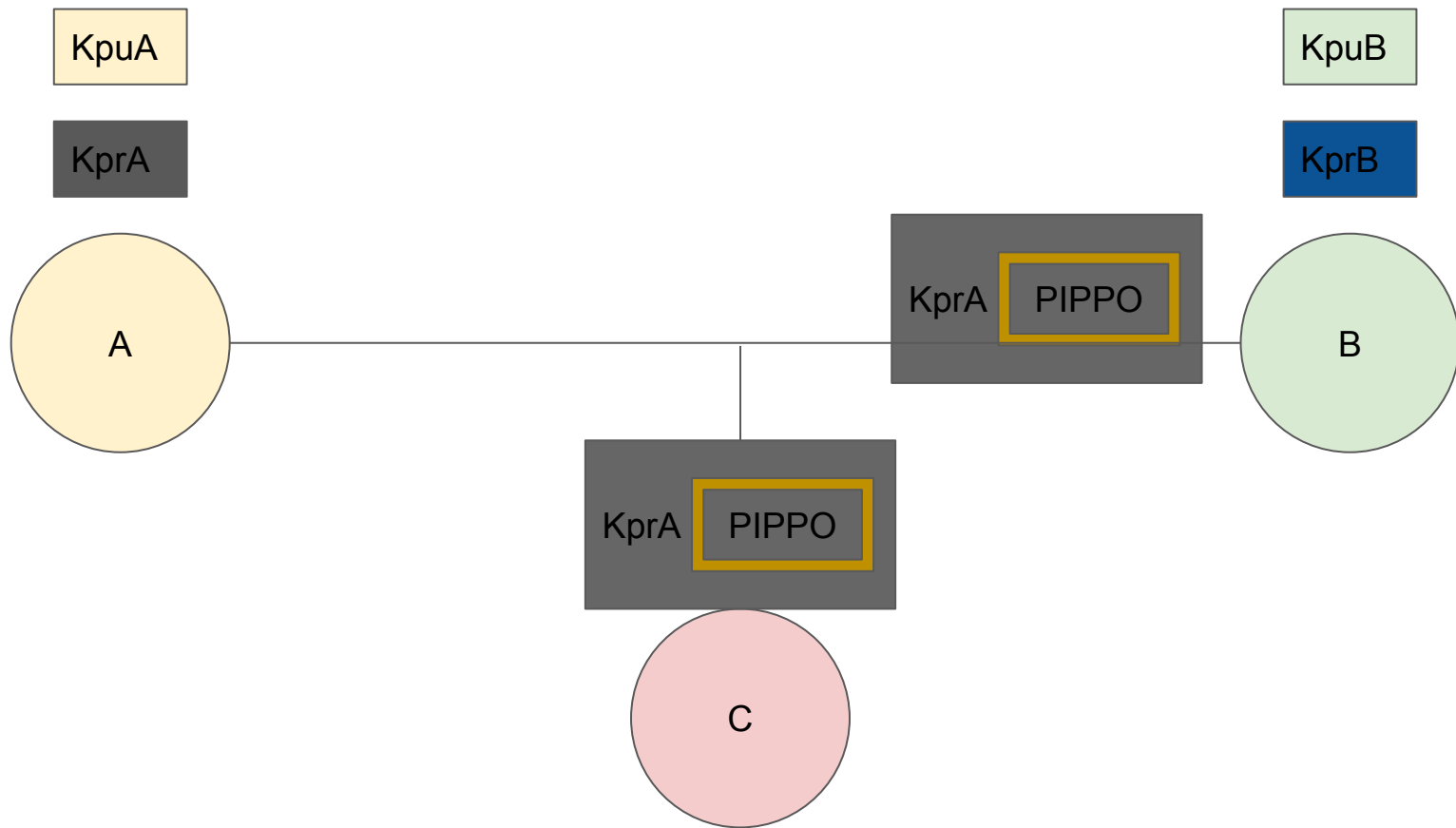
AUTENTICITÀ

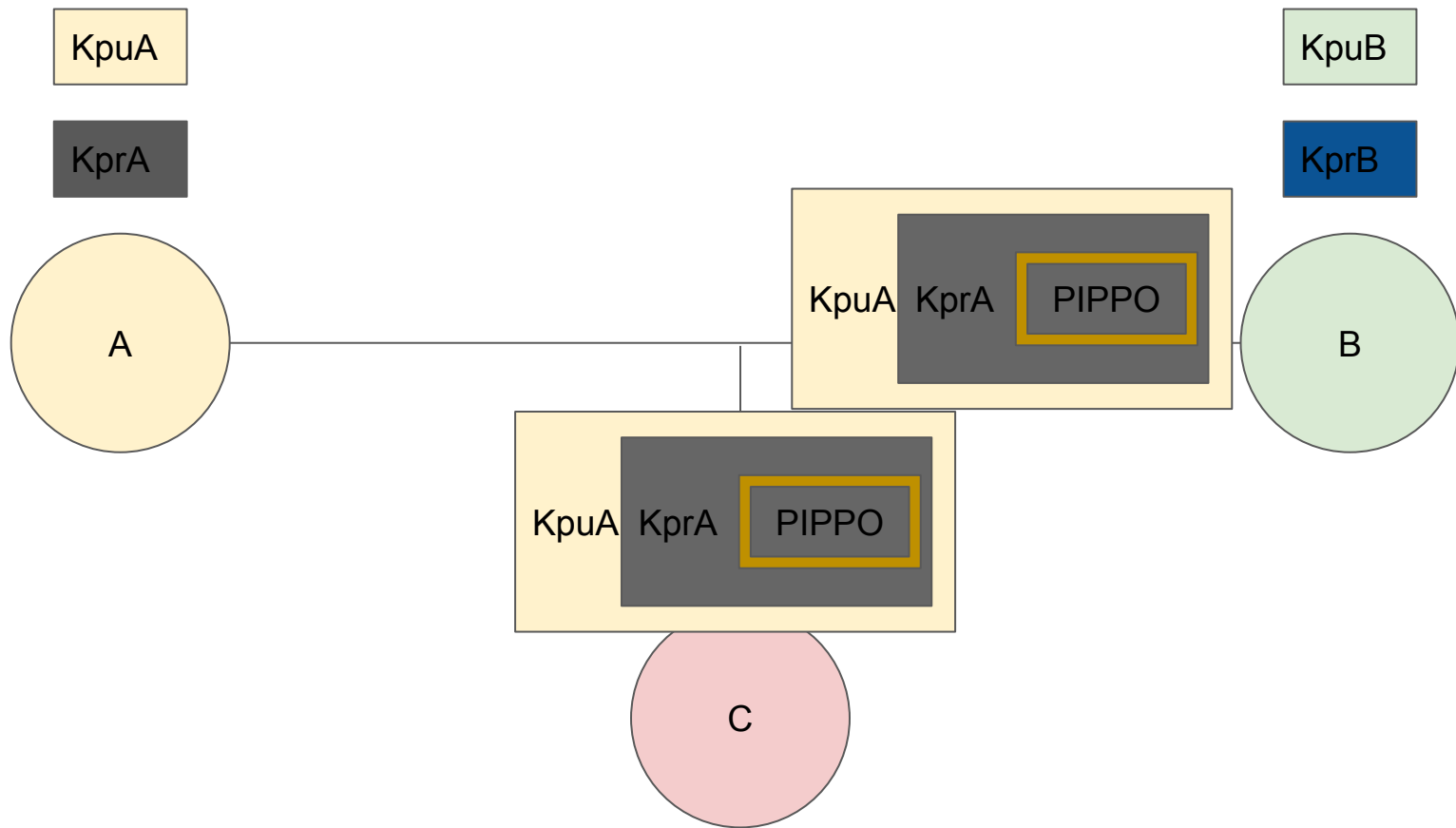
firma digitale

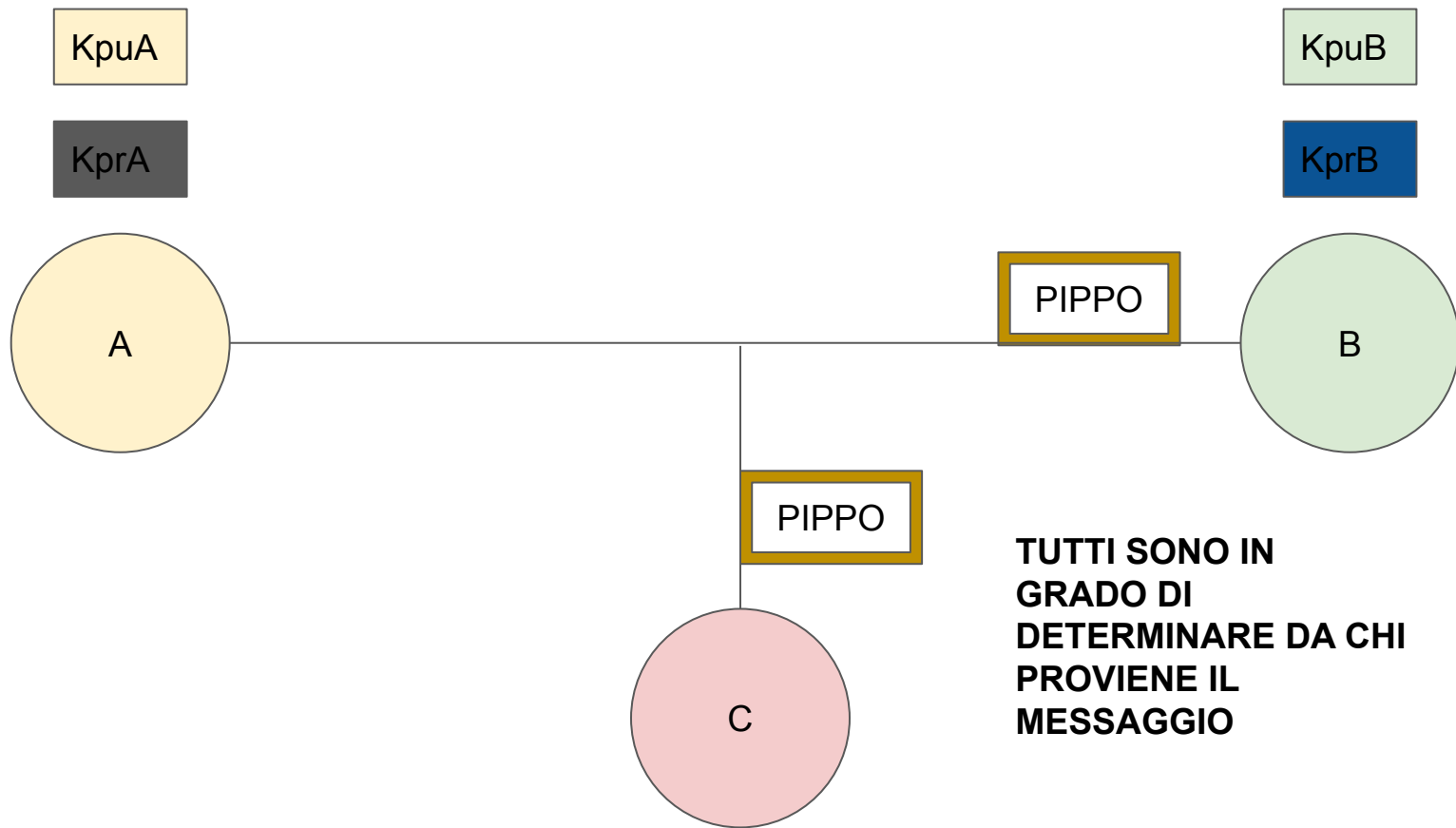


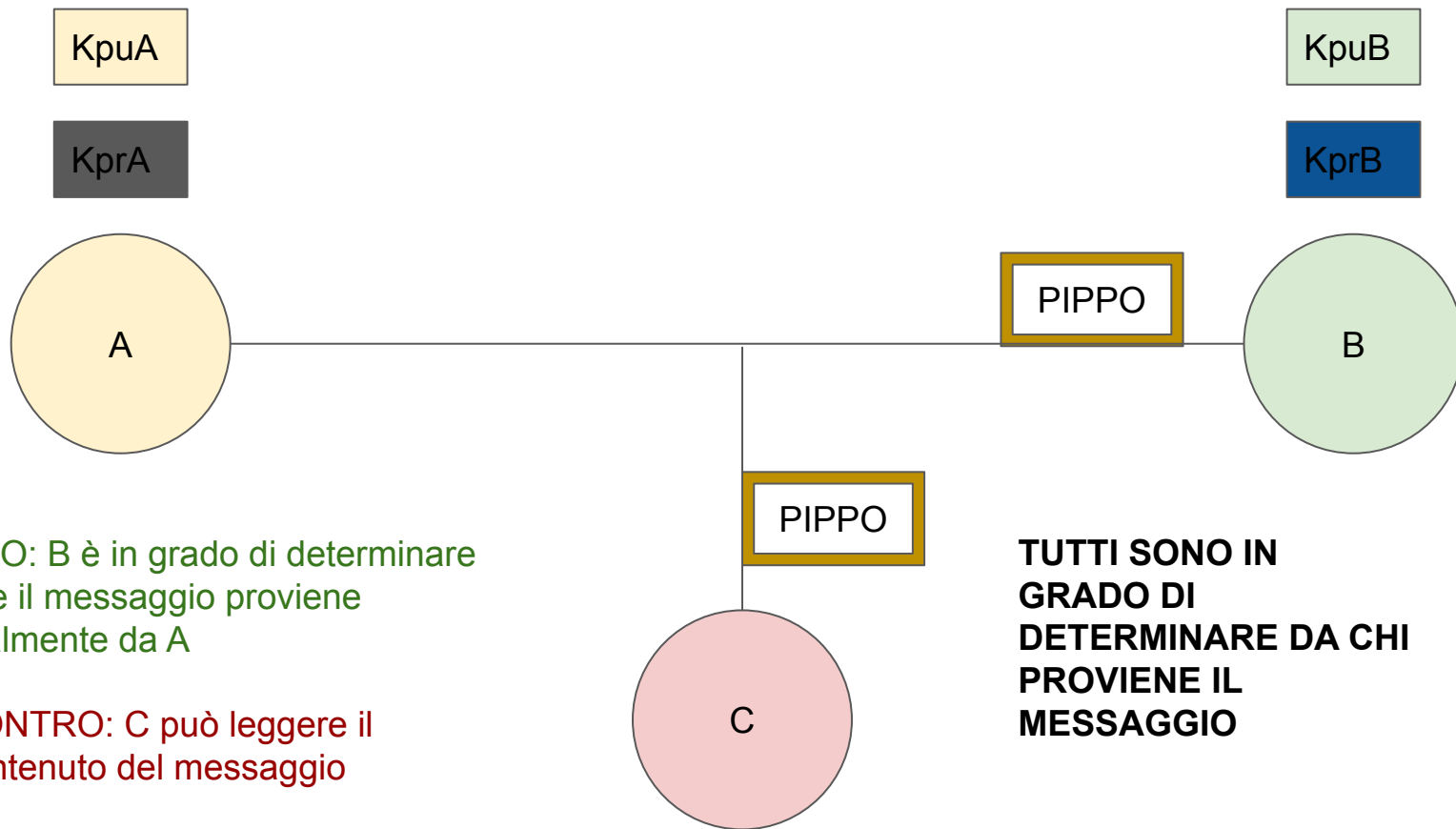












PRO: B è in grado di determinare
che il messaggio proviene
realmente da A

CONTRO: C può leggere il
contenuto del messaggio

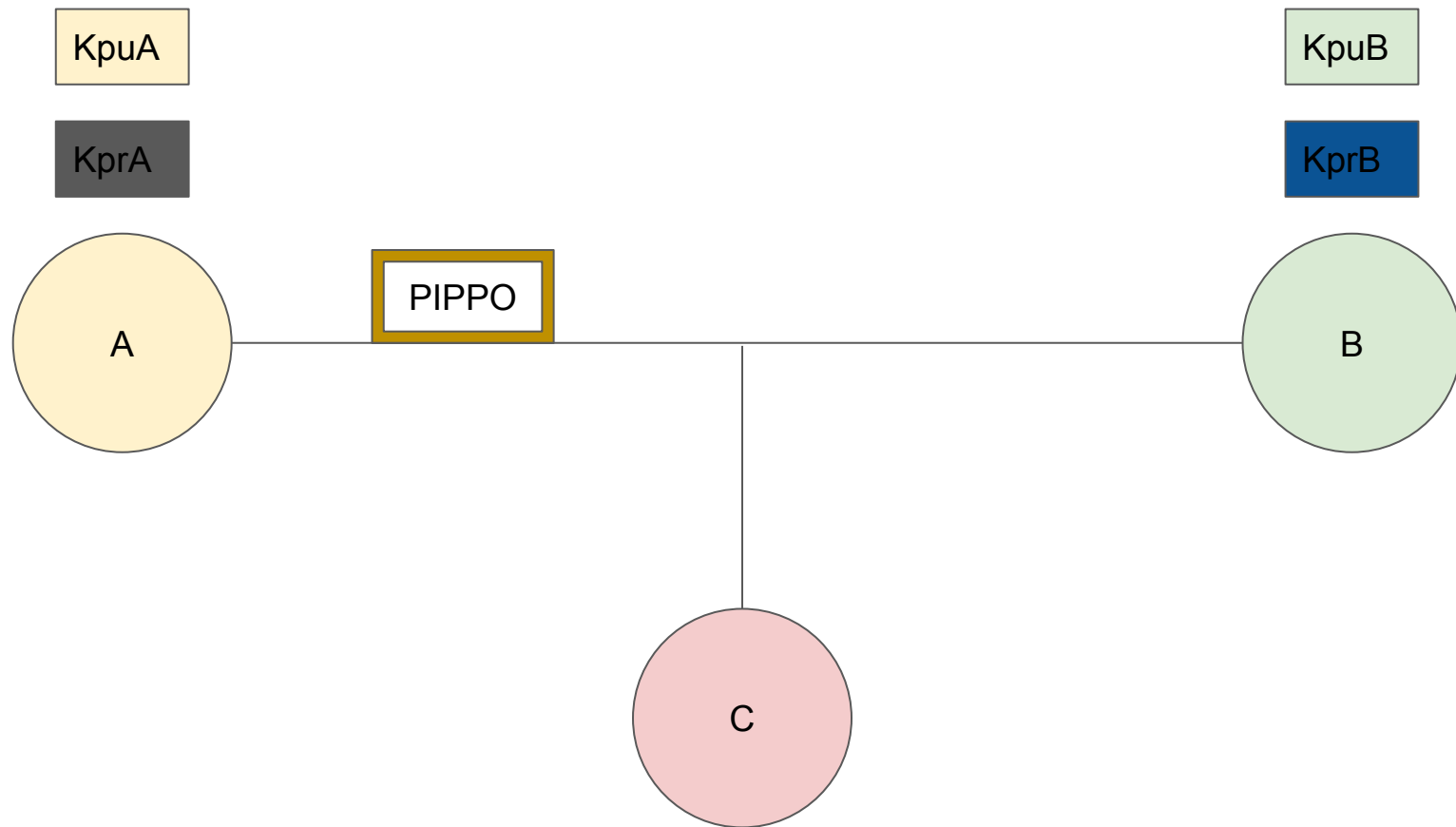
**TUTTI SONO IN
GRADO DI
DETERMINARE DA CHI
PROVIENE IL
MESSAGGIO**

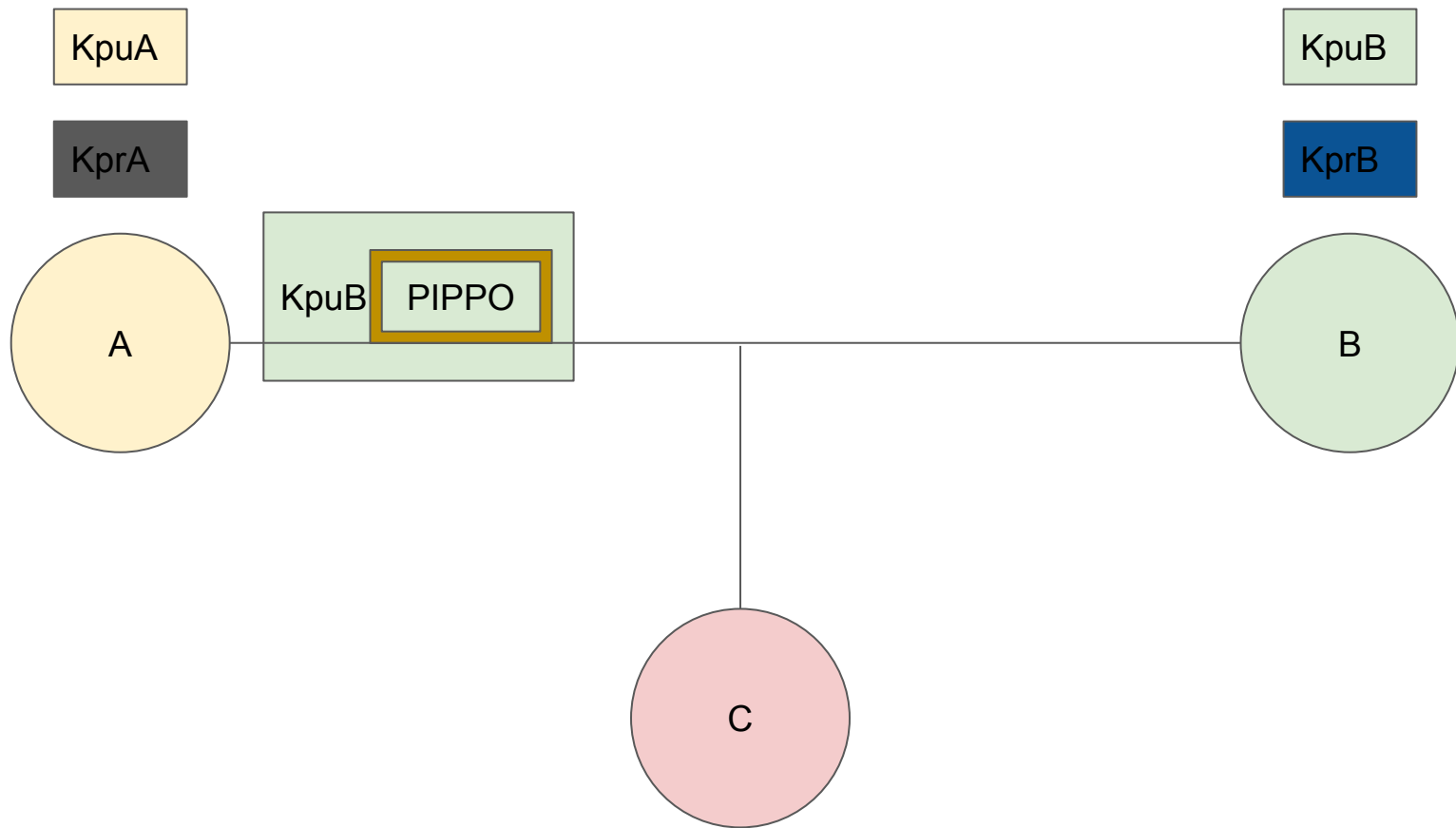
INTEGRITÀ

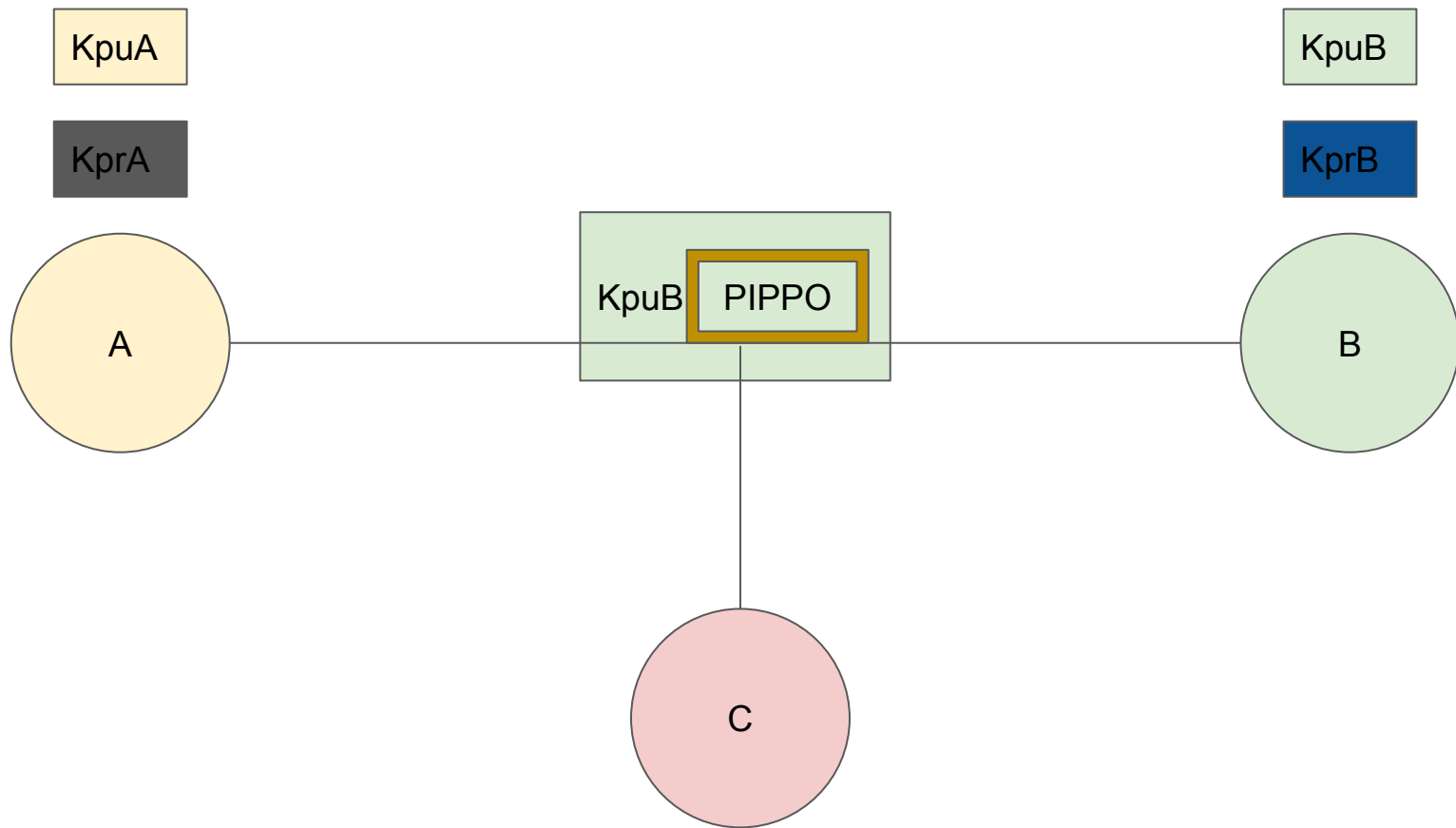
garantire la non modificabilità di un messaggio

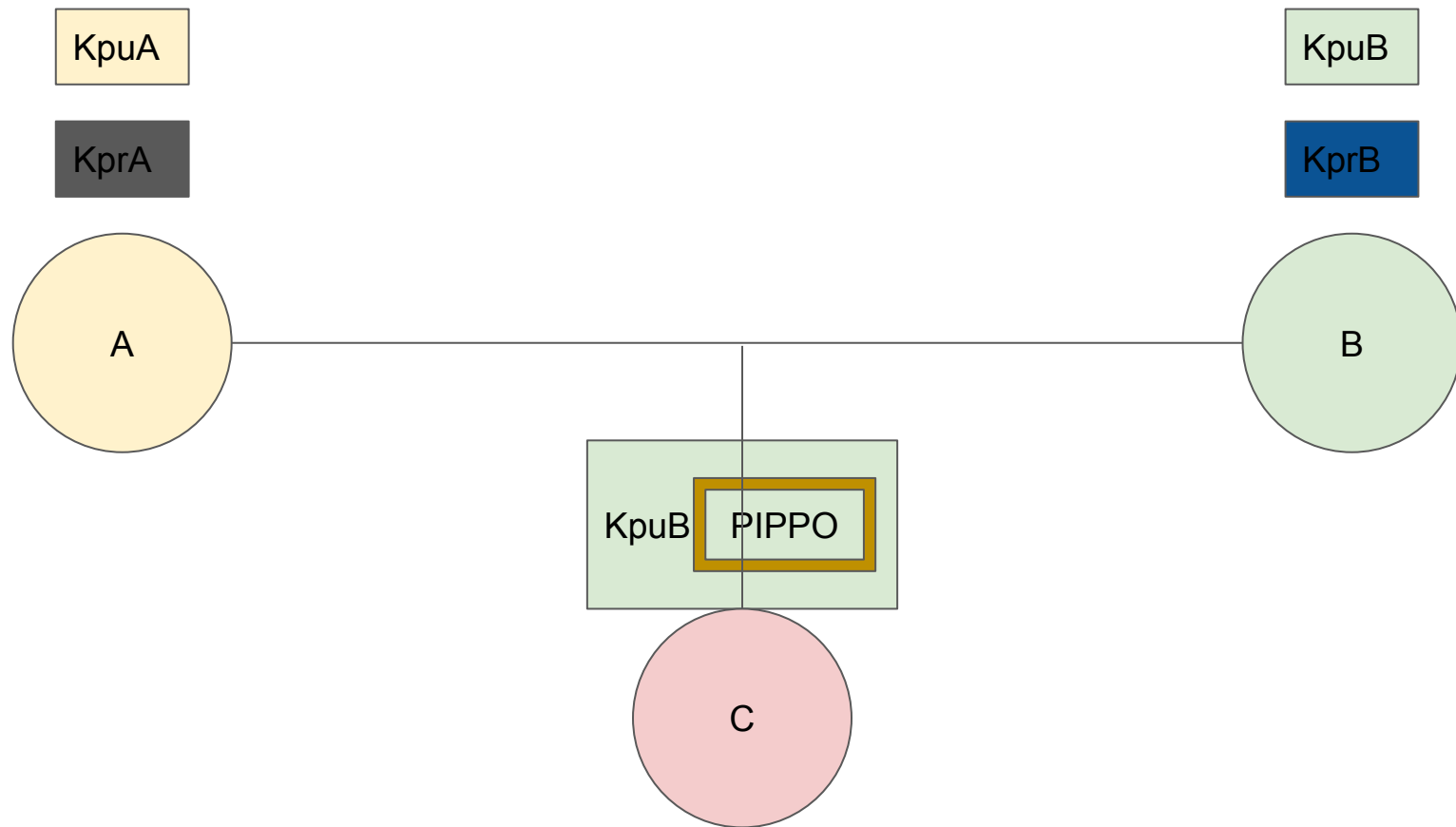
PROBLEMA

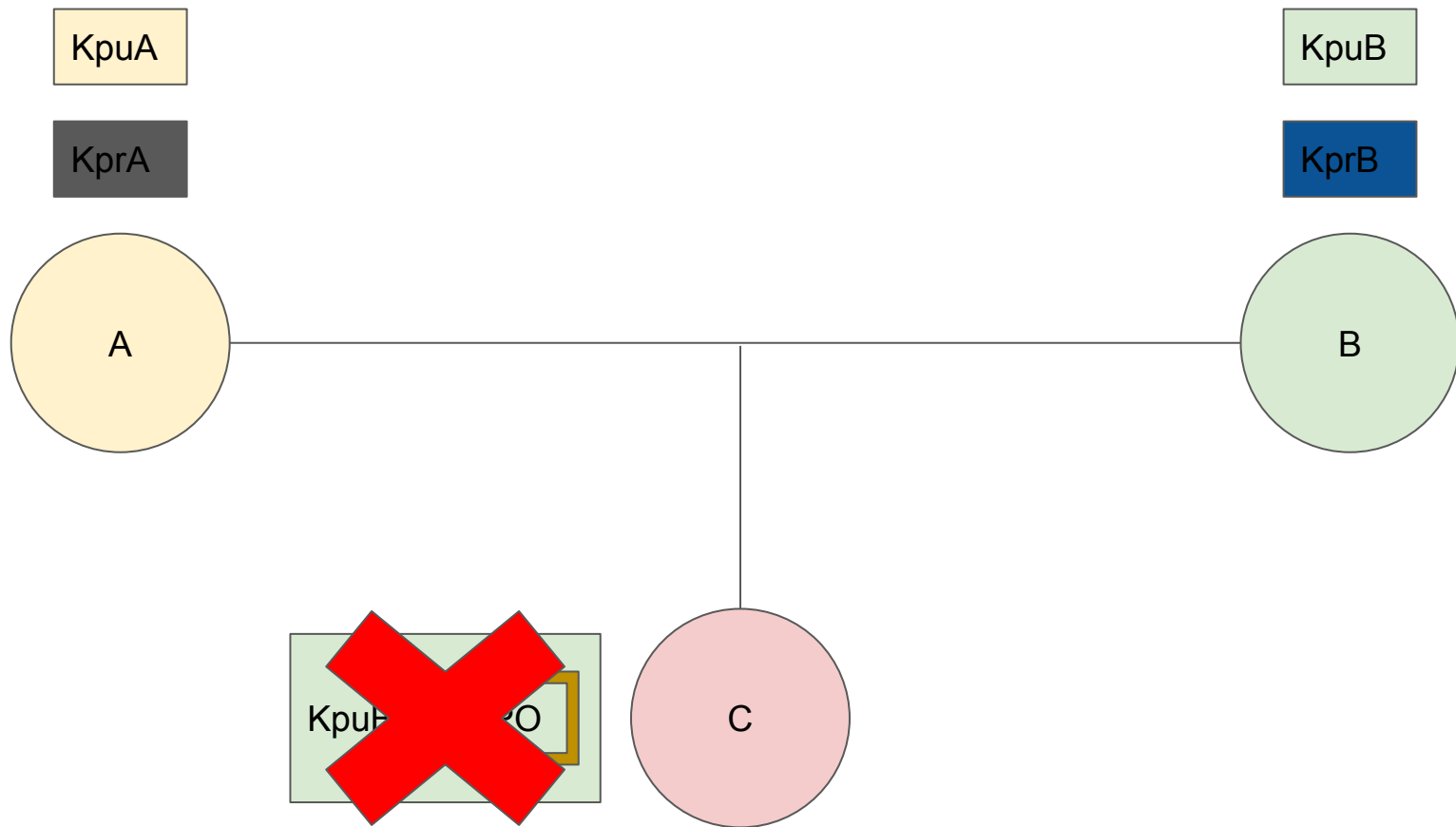
possibile attacco all'integrità di un messaggio

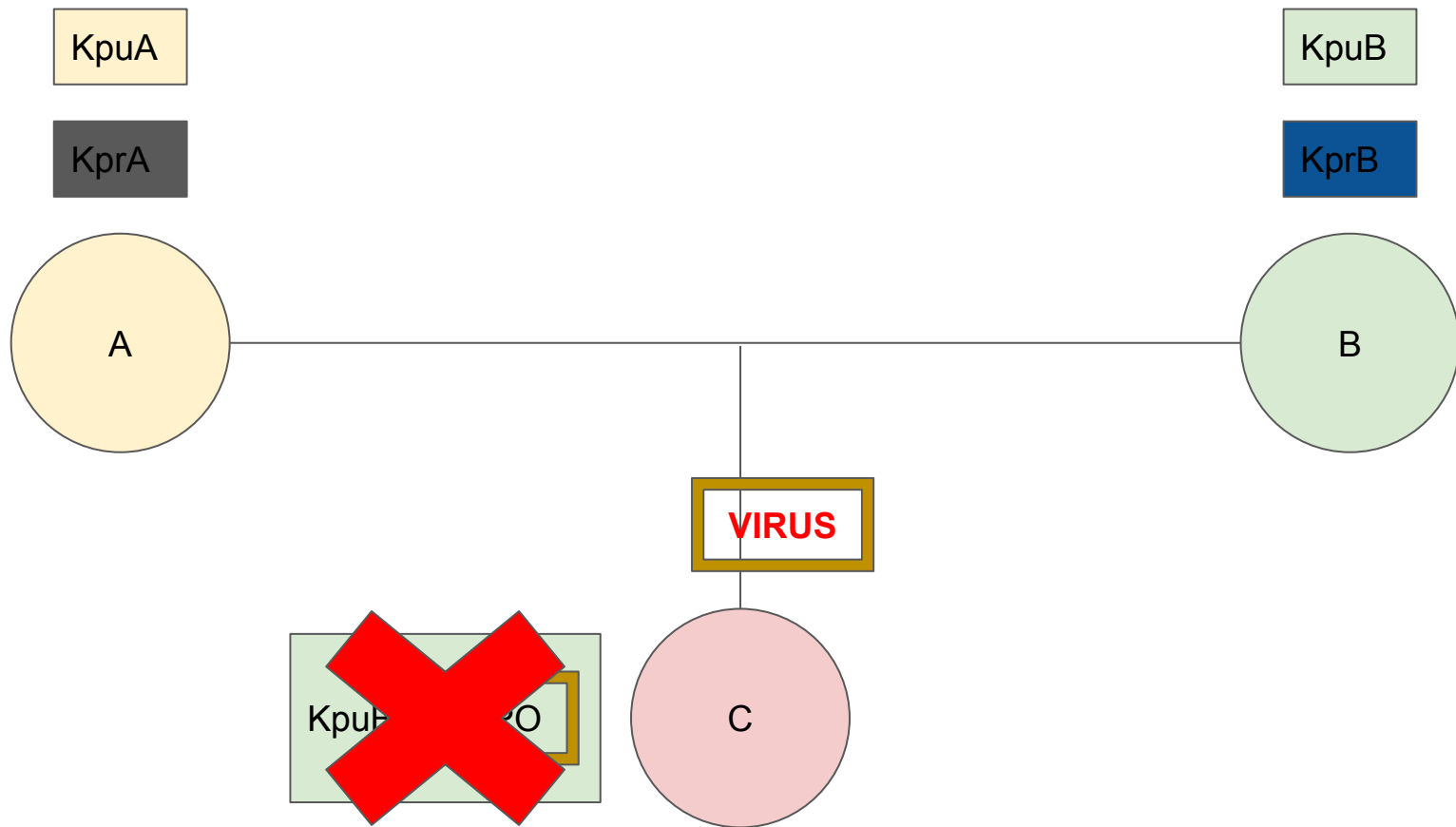


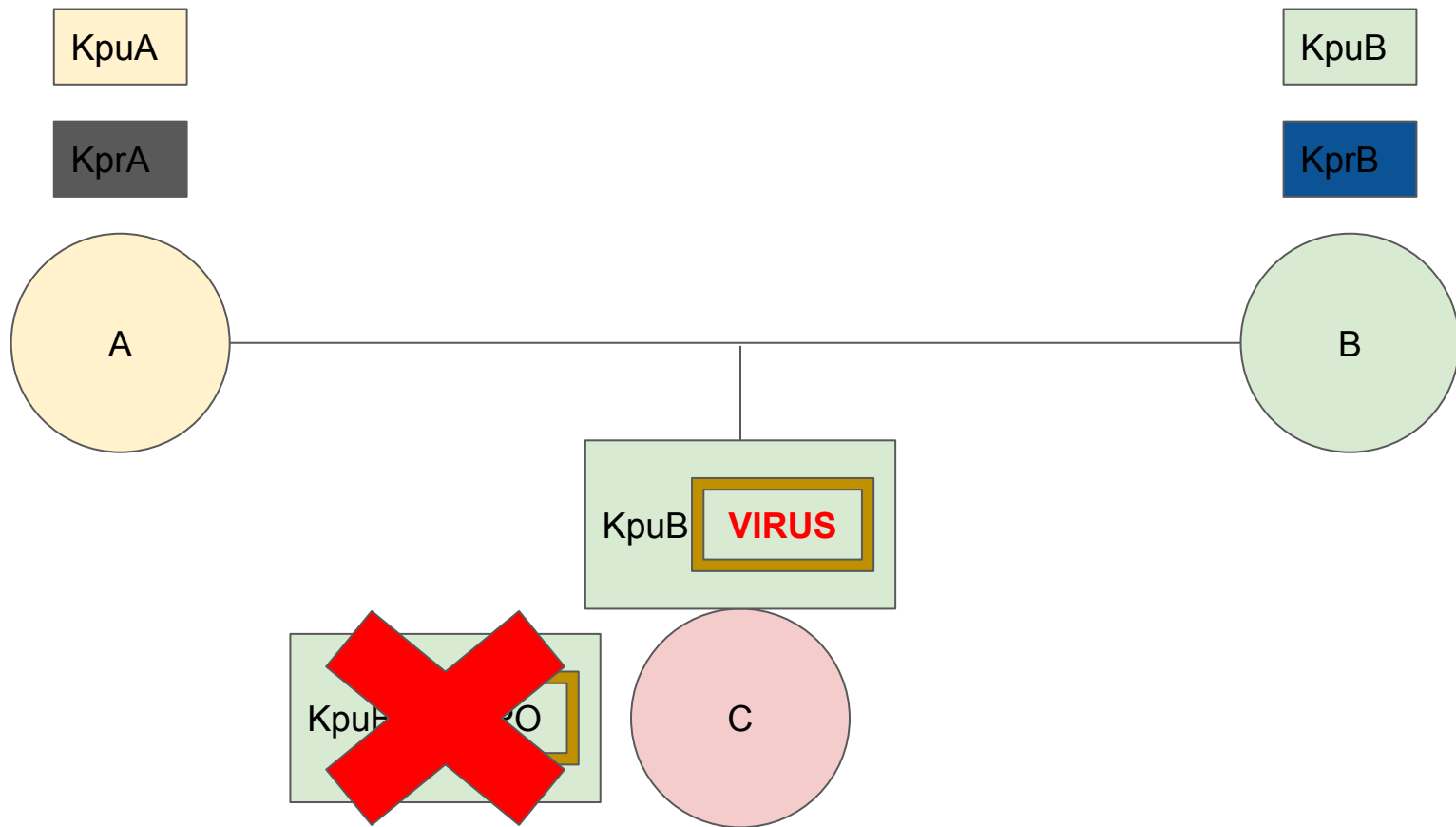


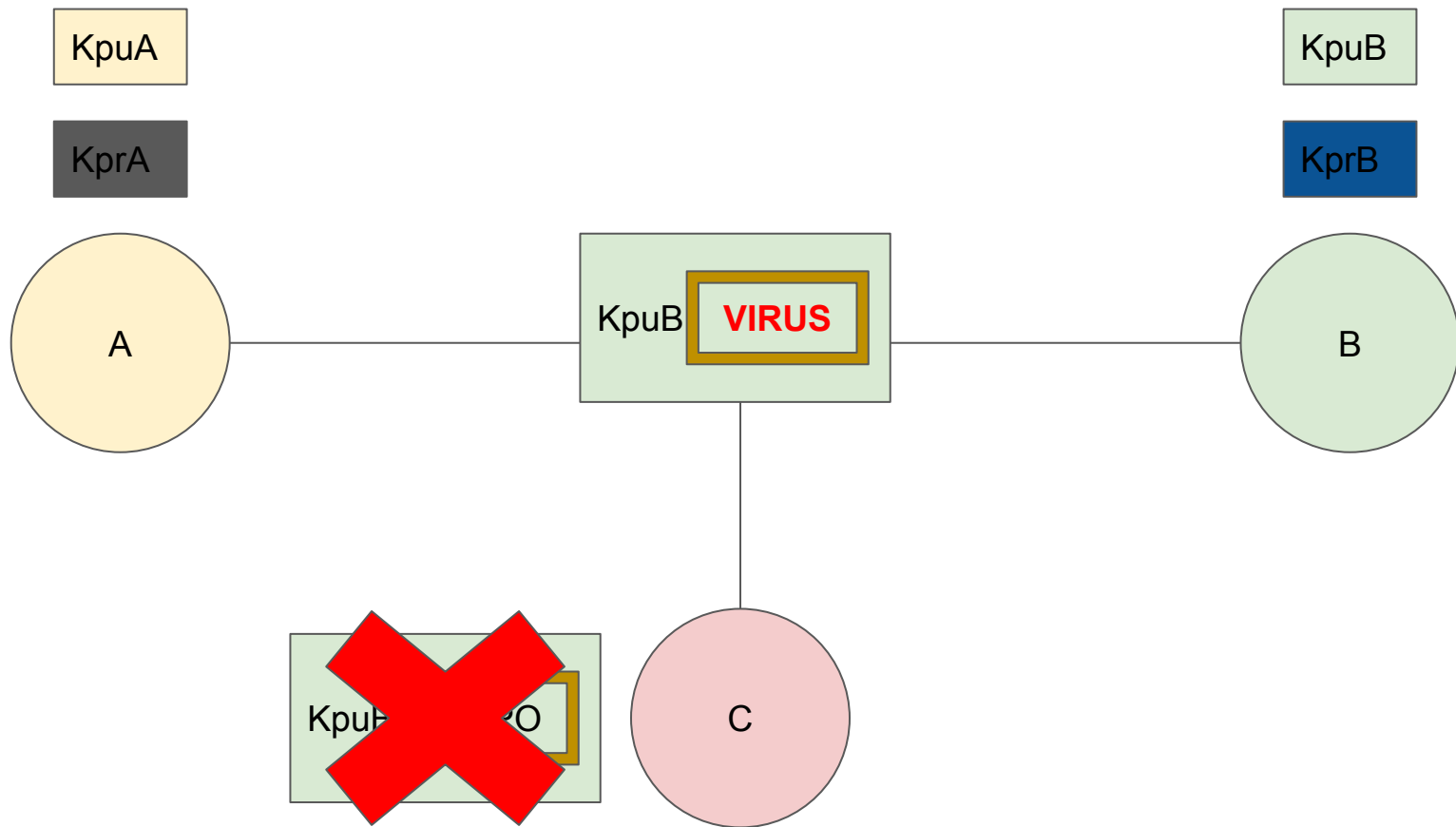


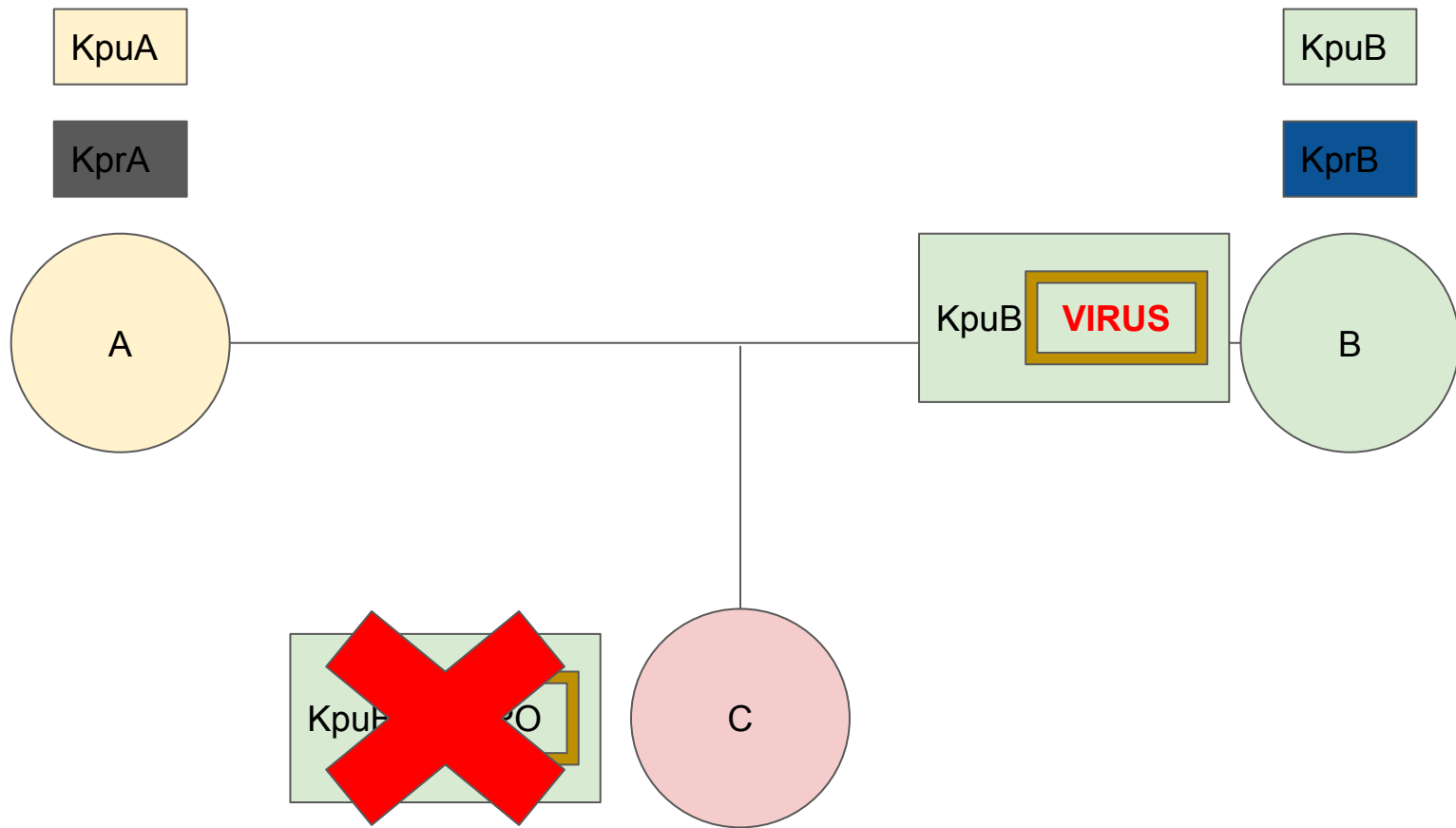


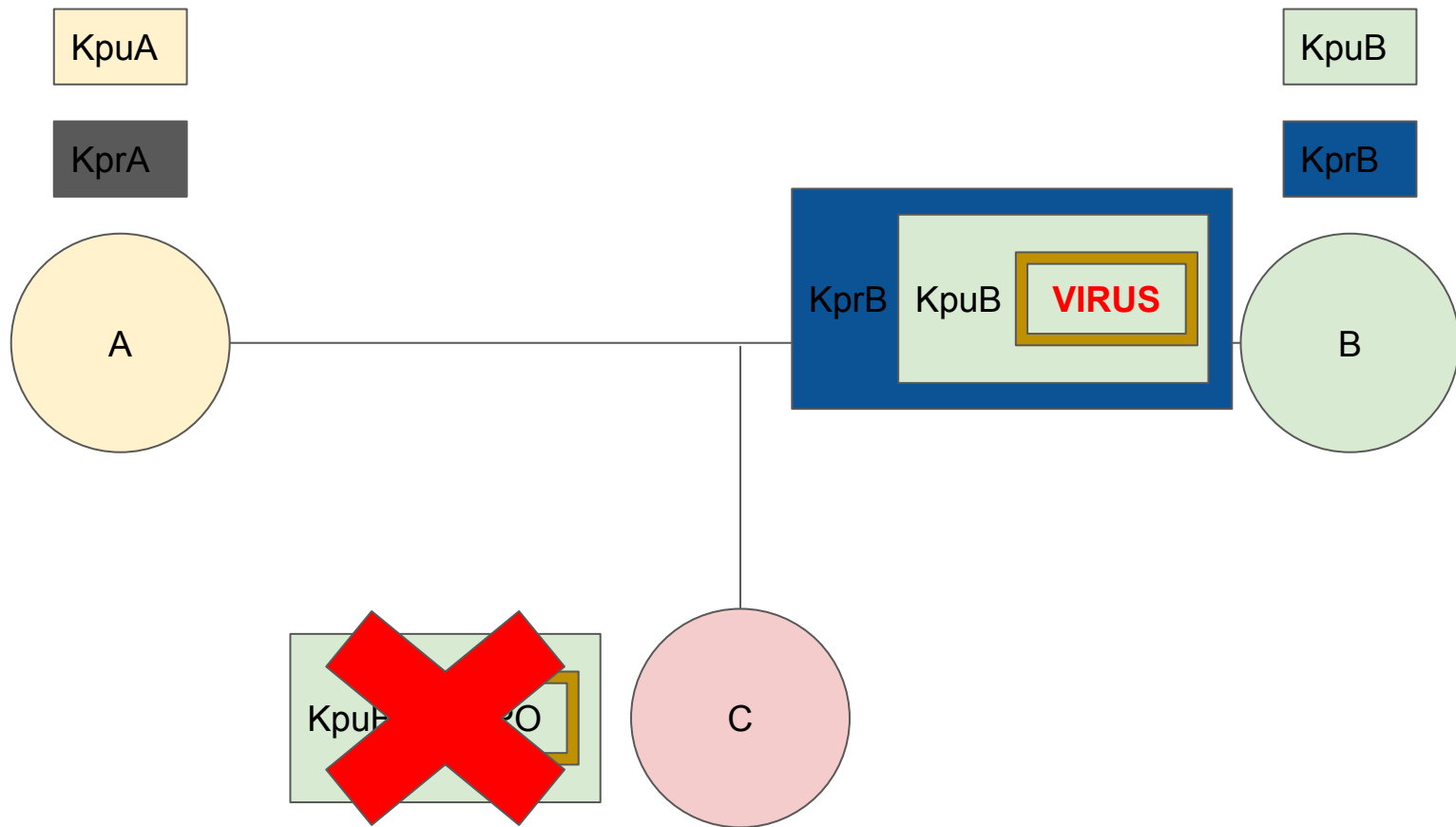


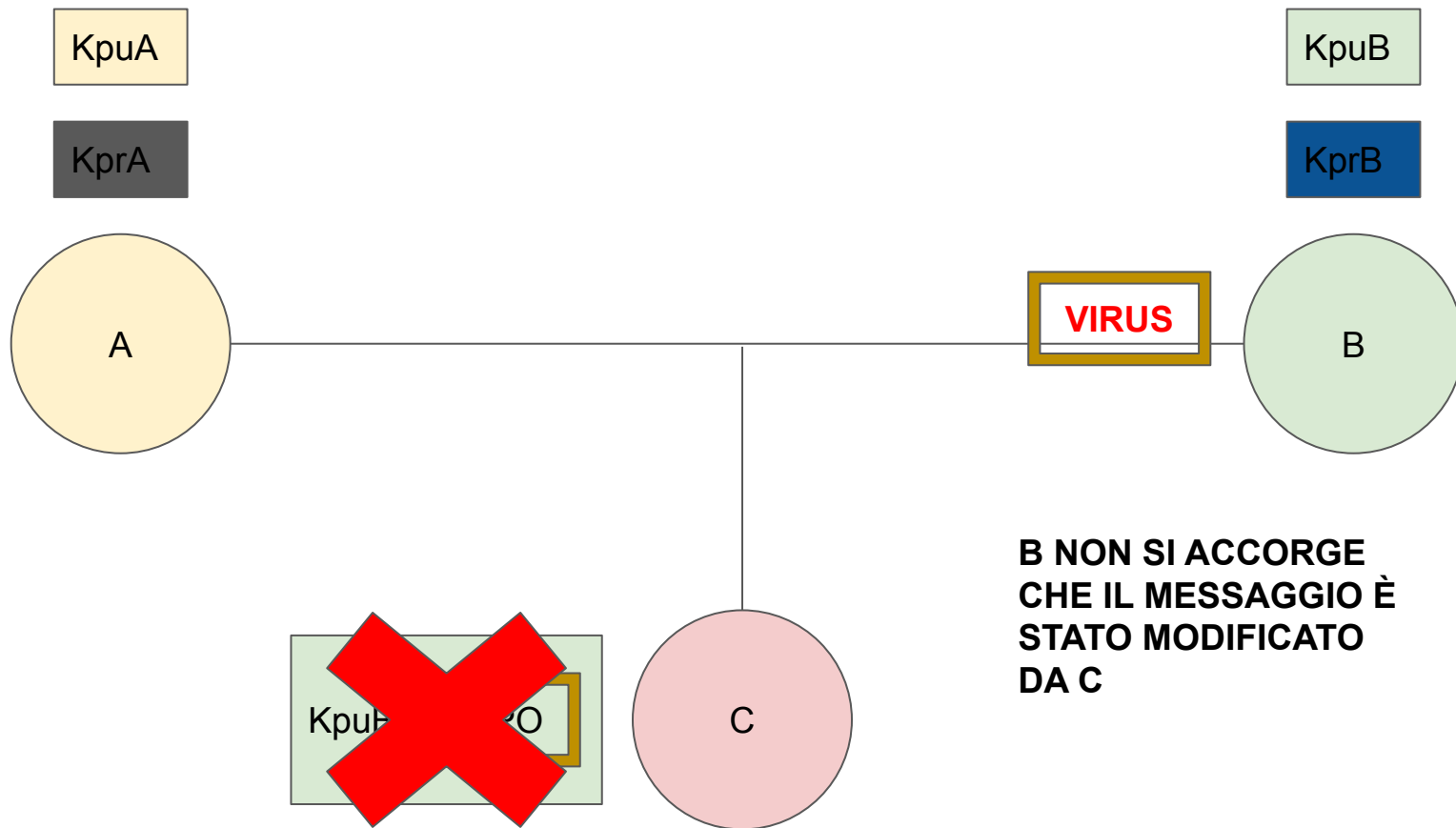






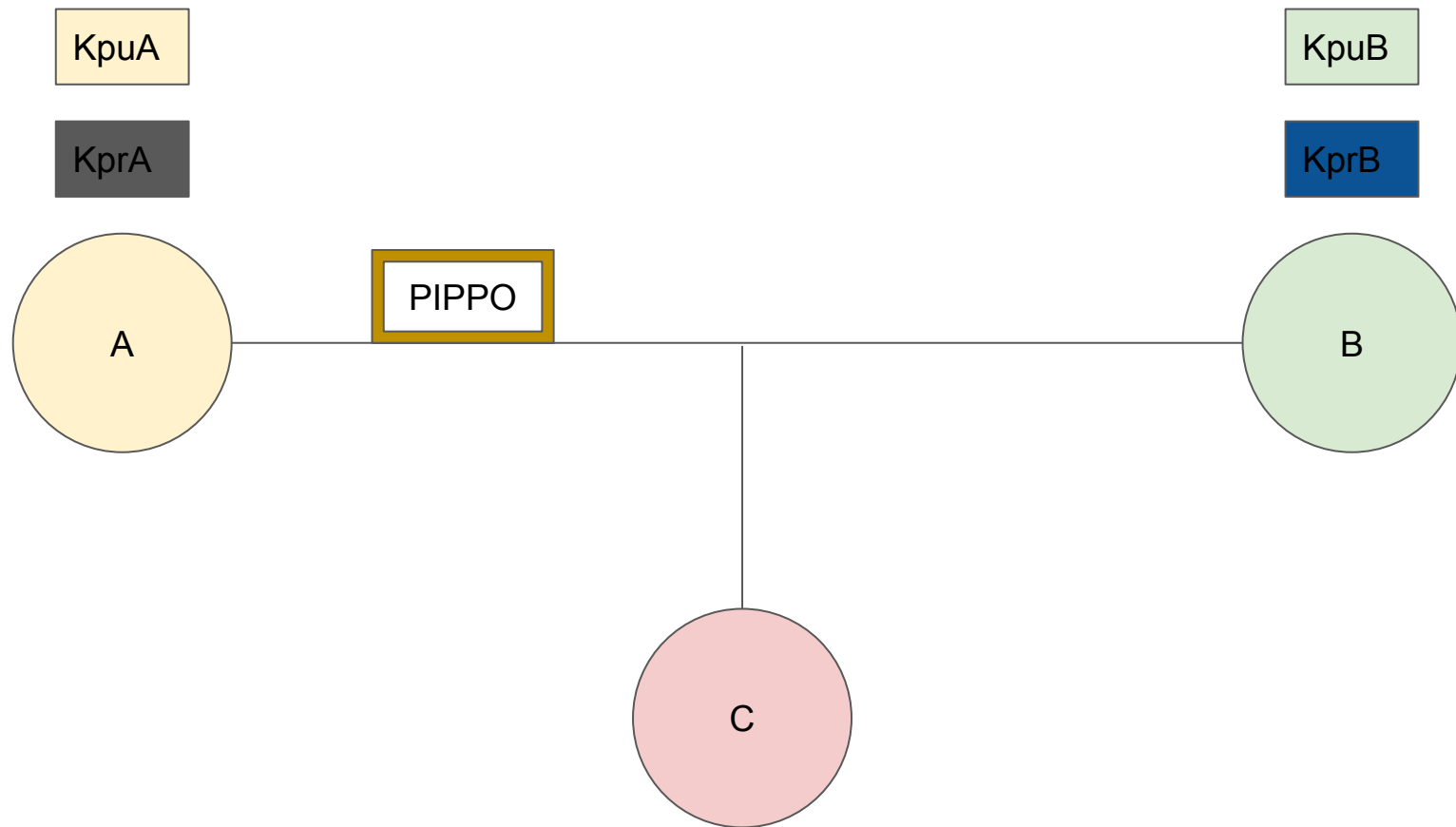


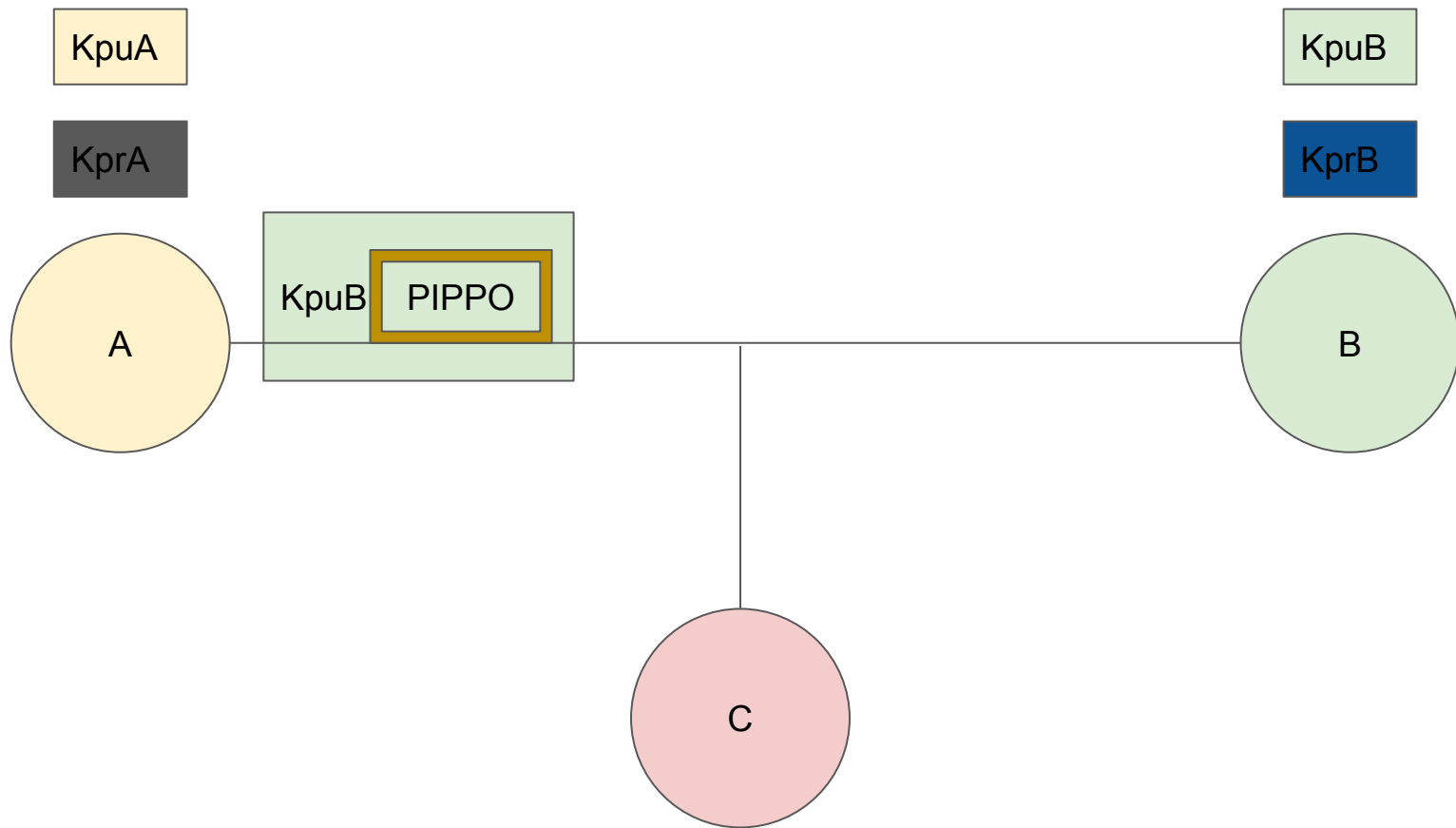


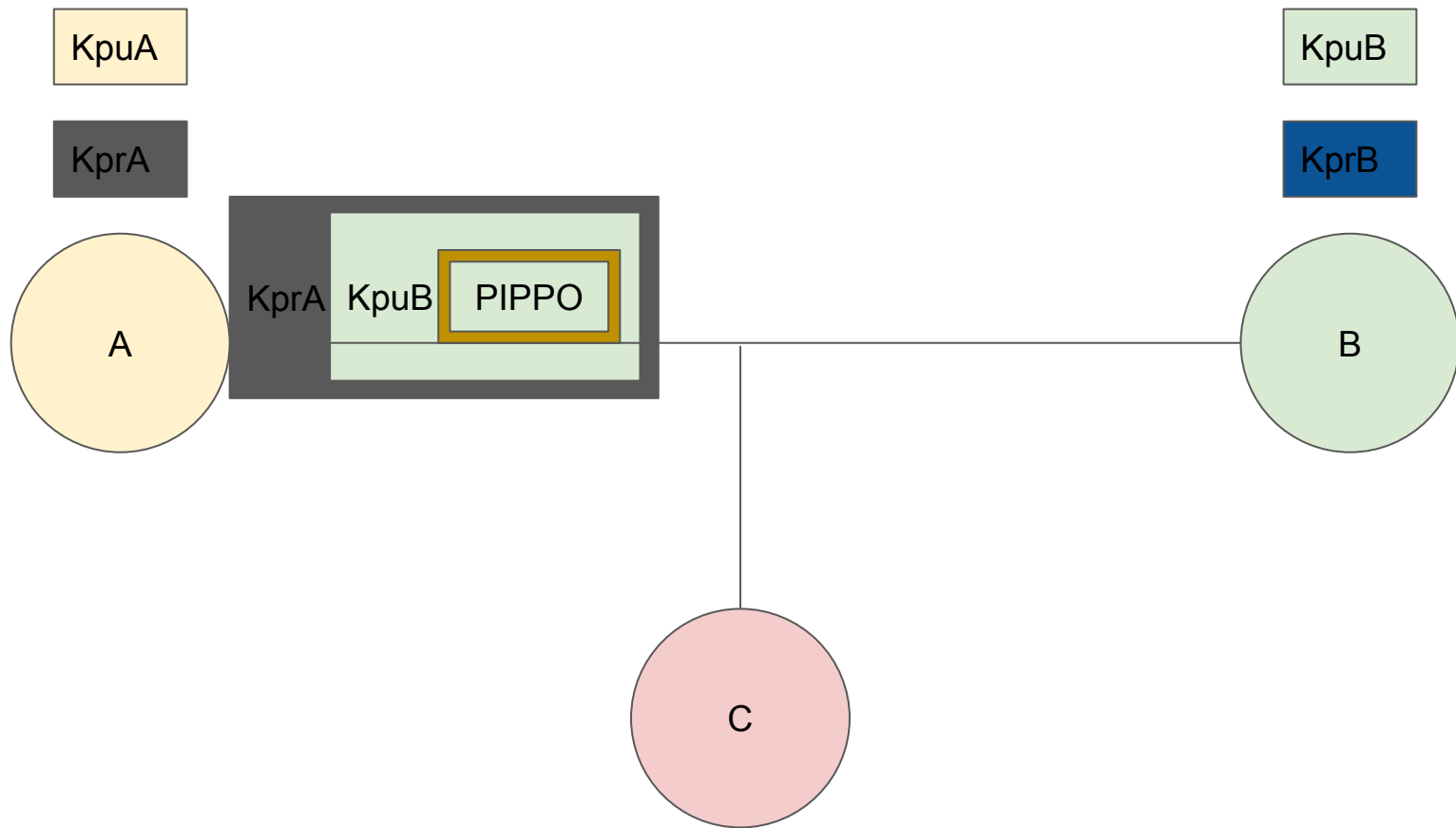


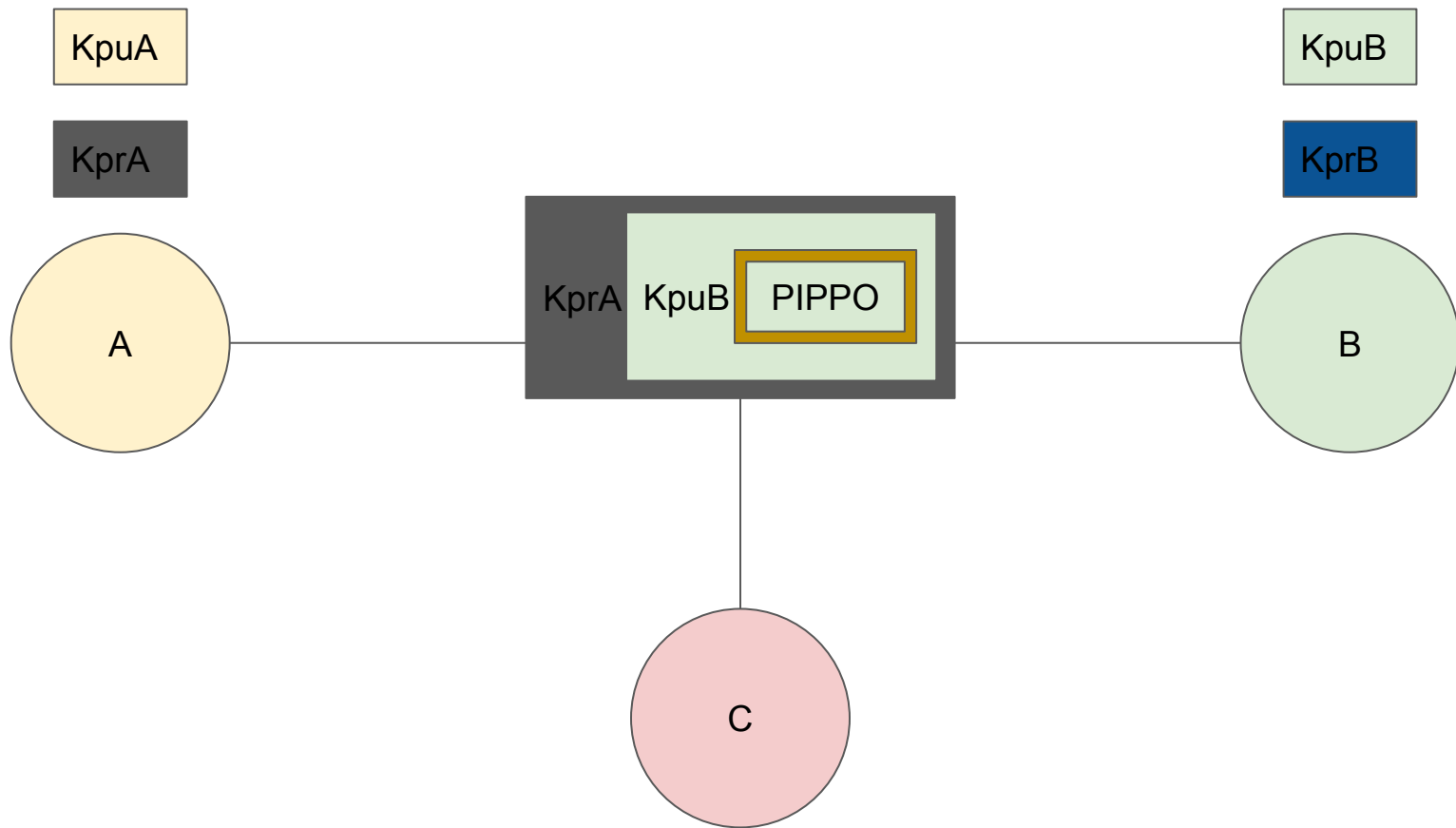
SOLUZIONE

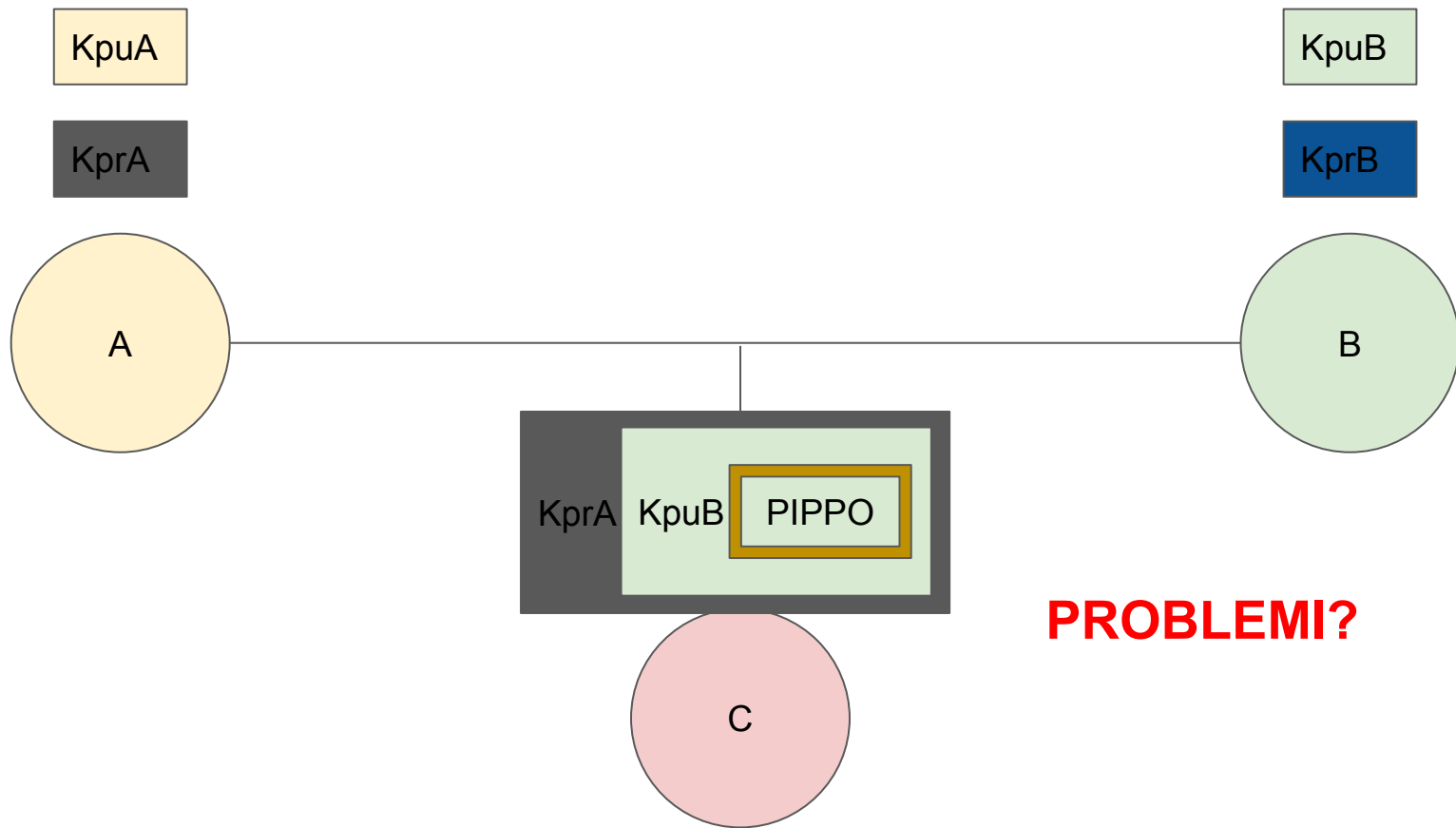
possibile attacco all'integrità di un messaggio



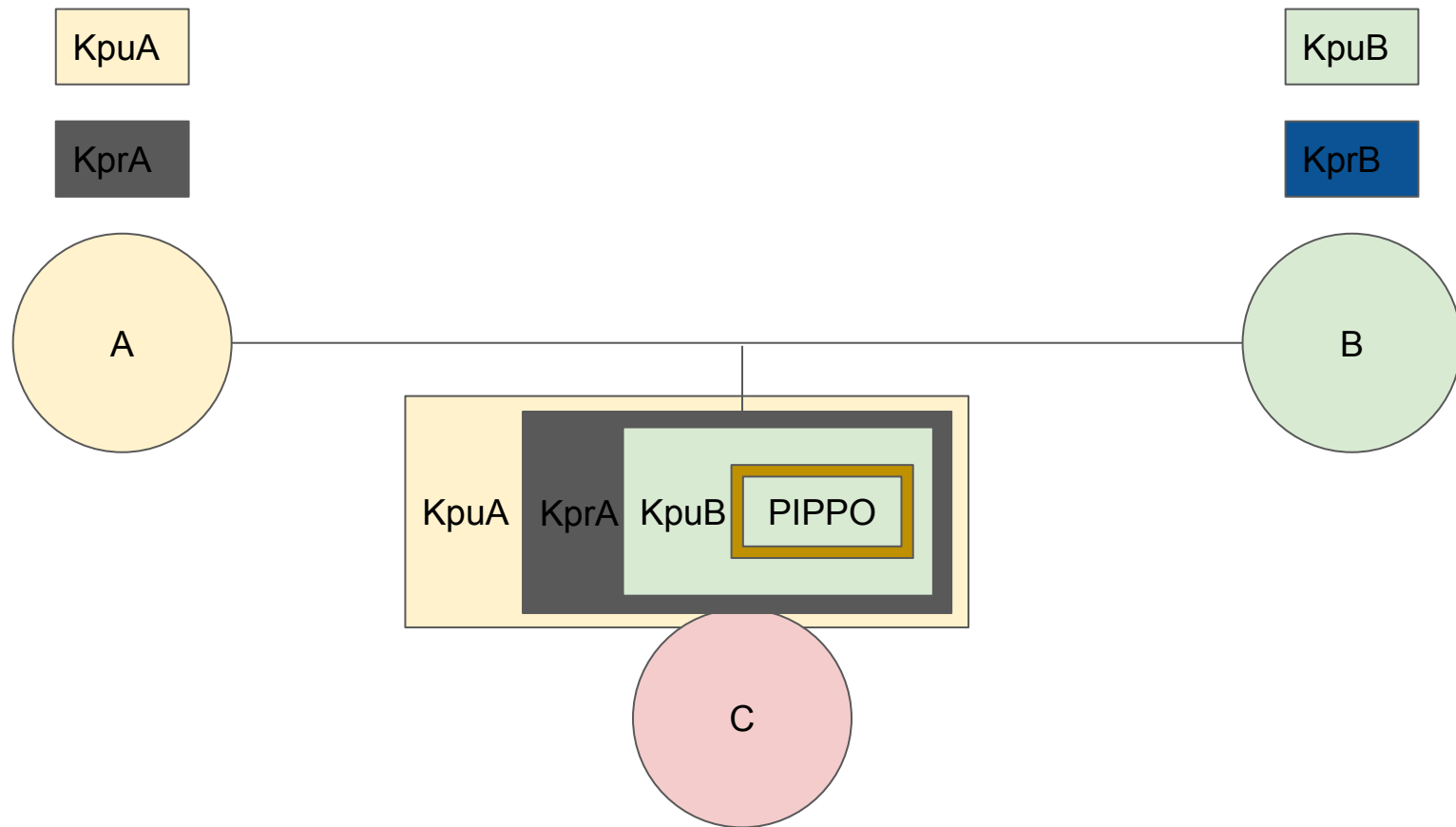


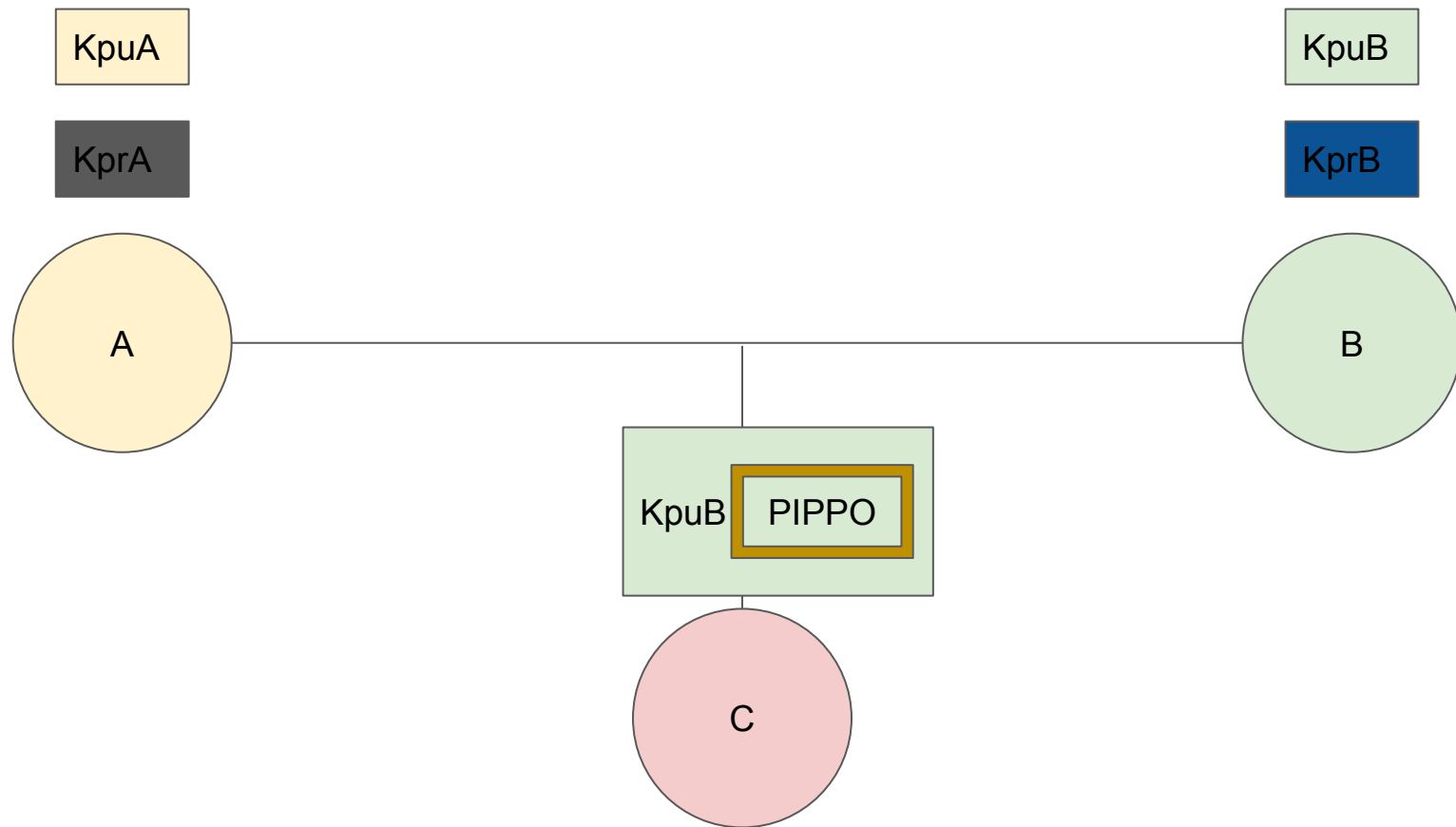


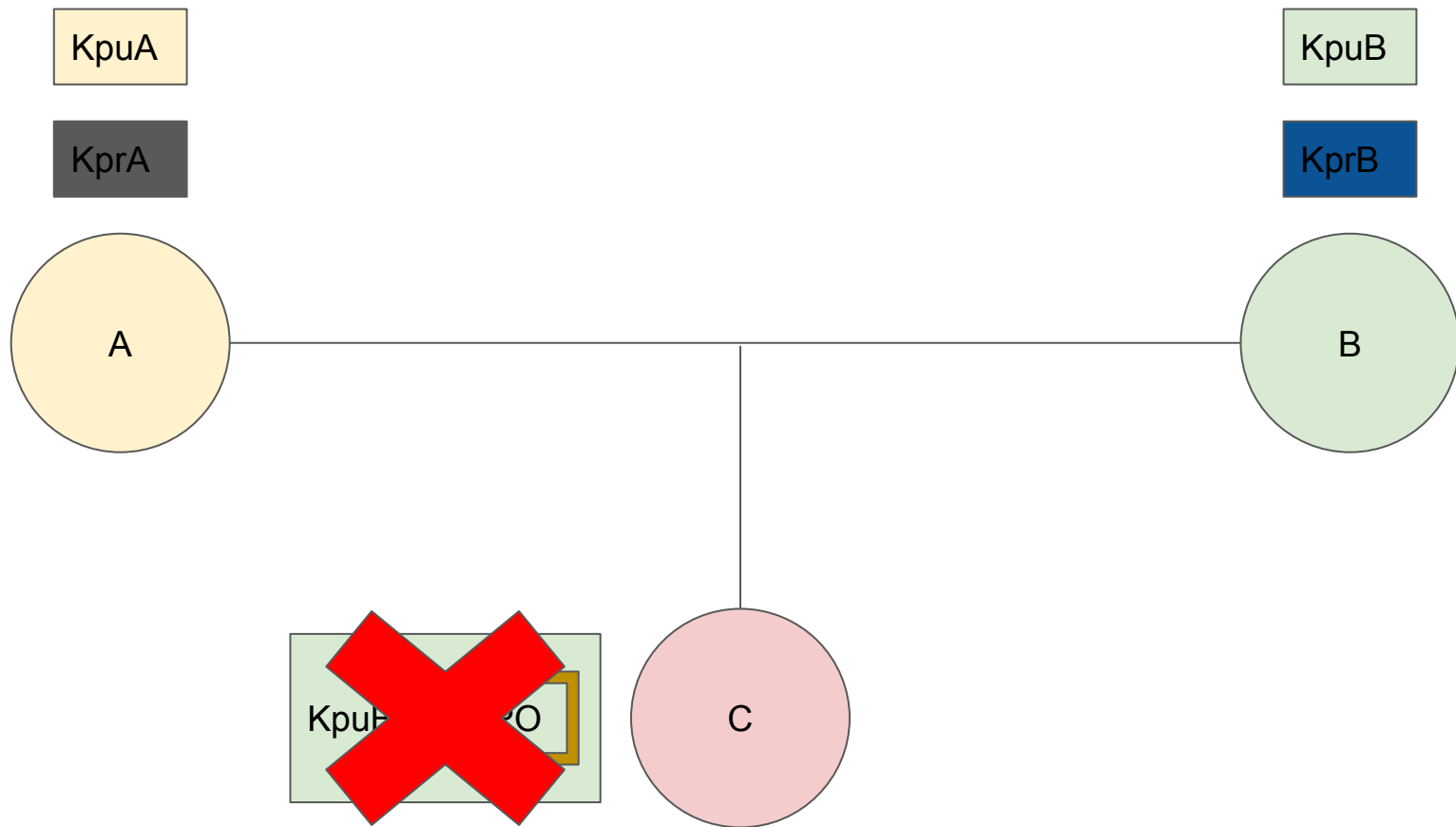


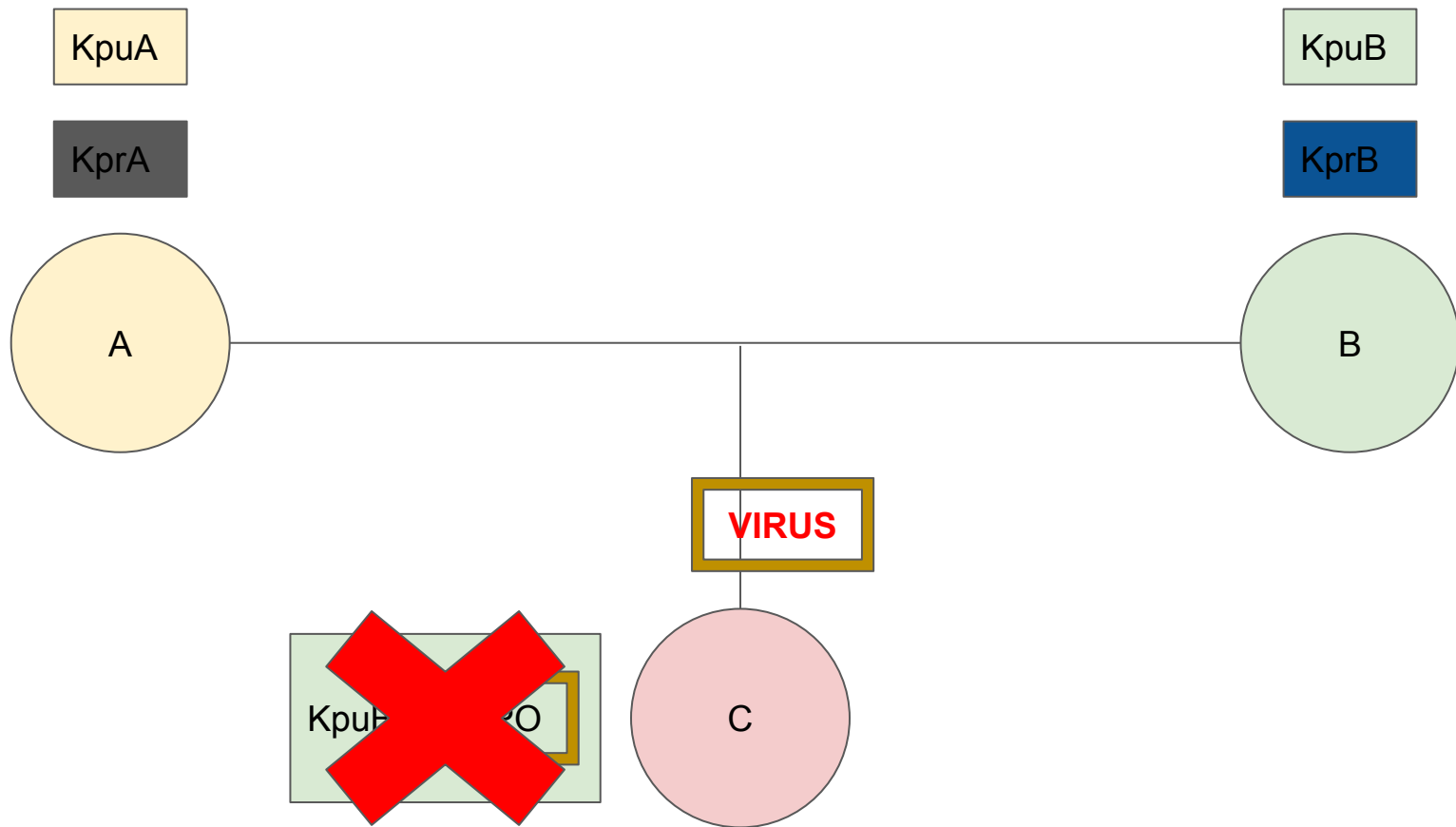


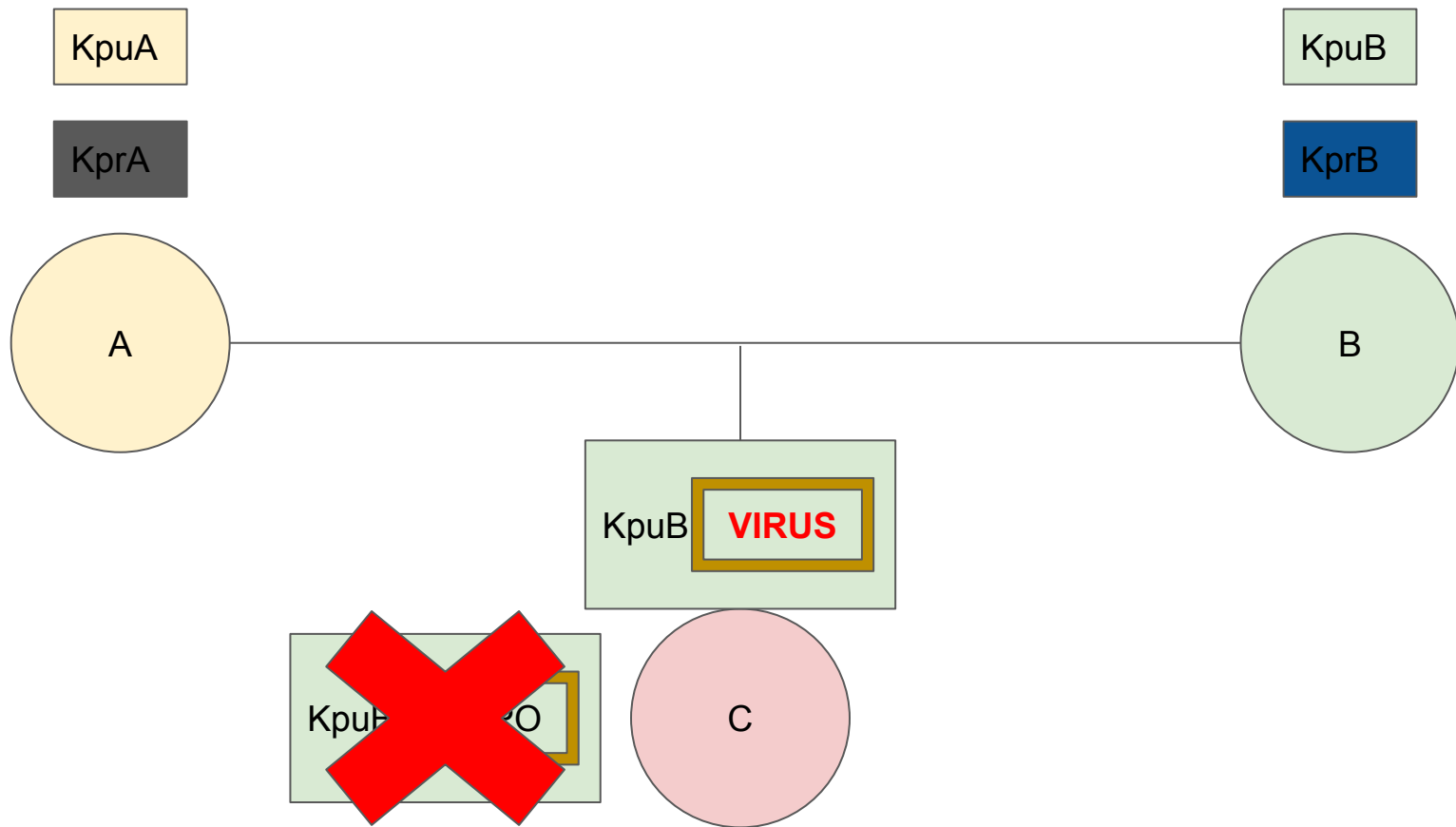
PROBLEMI?

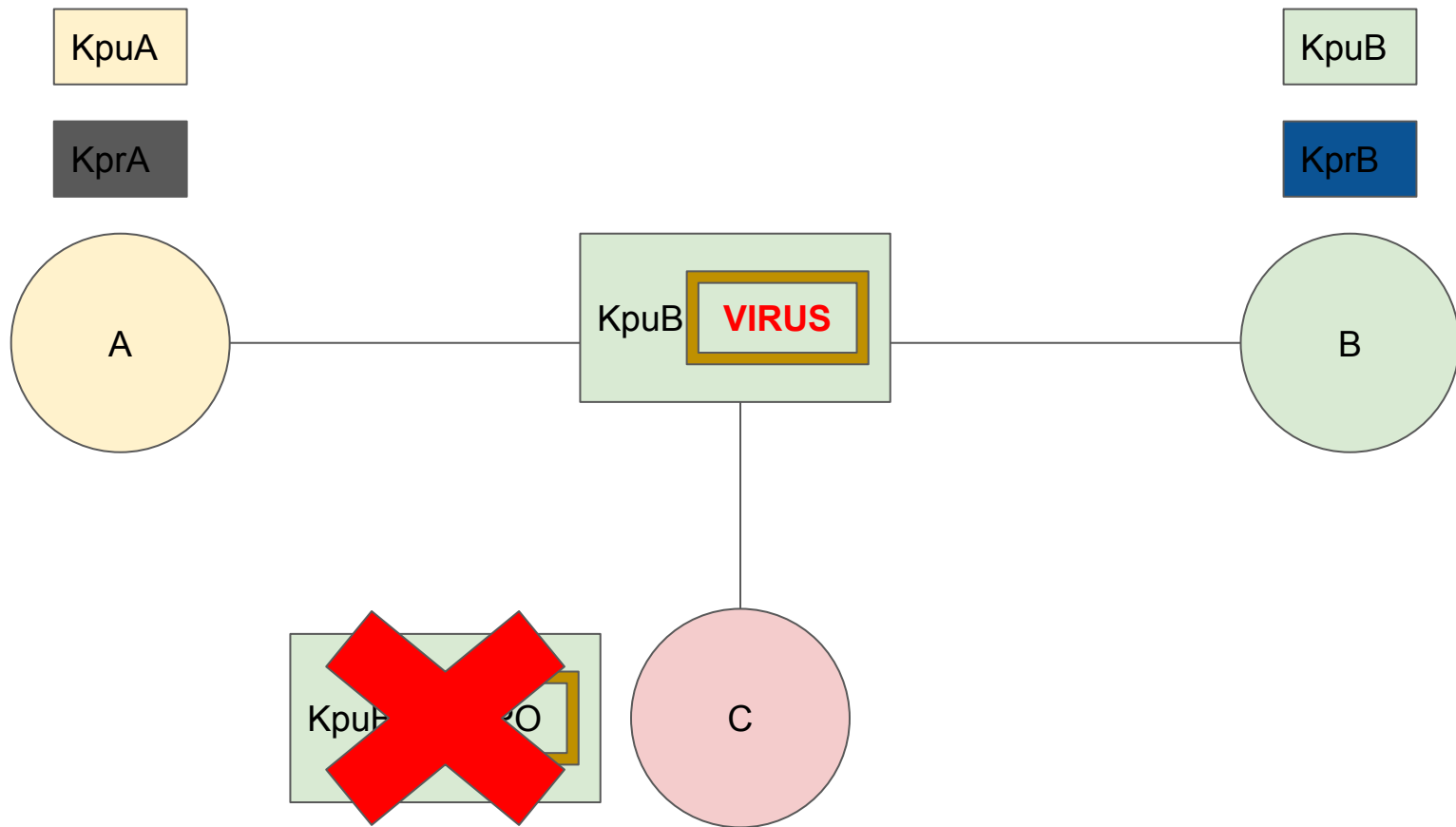


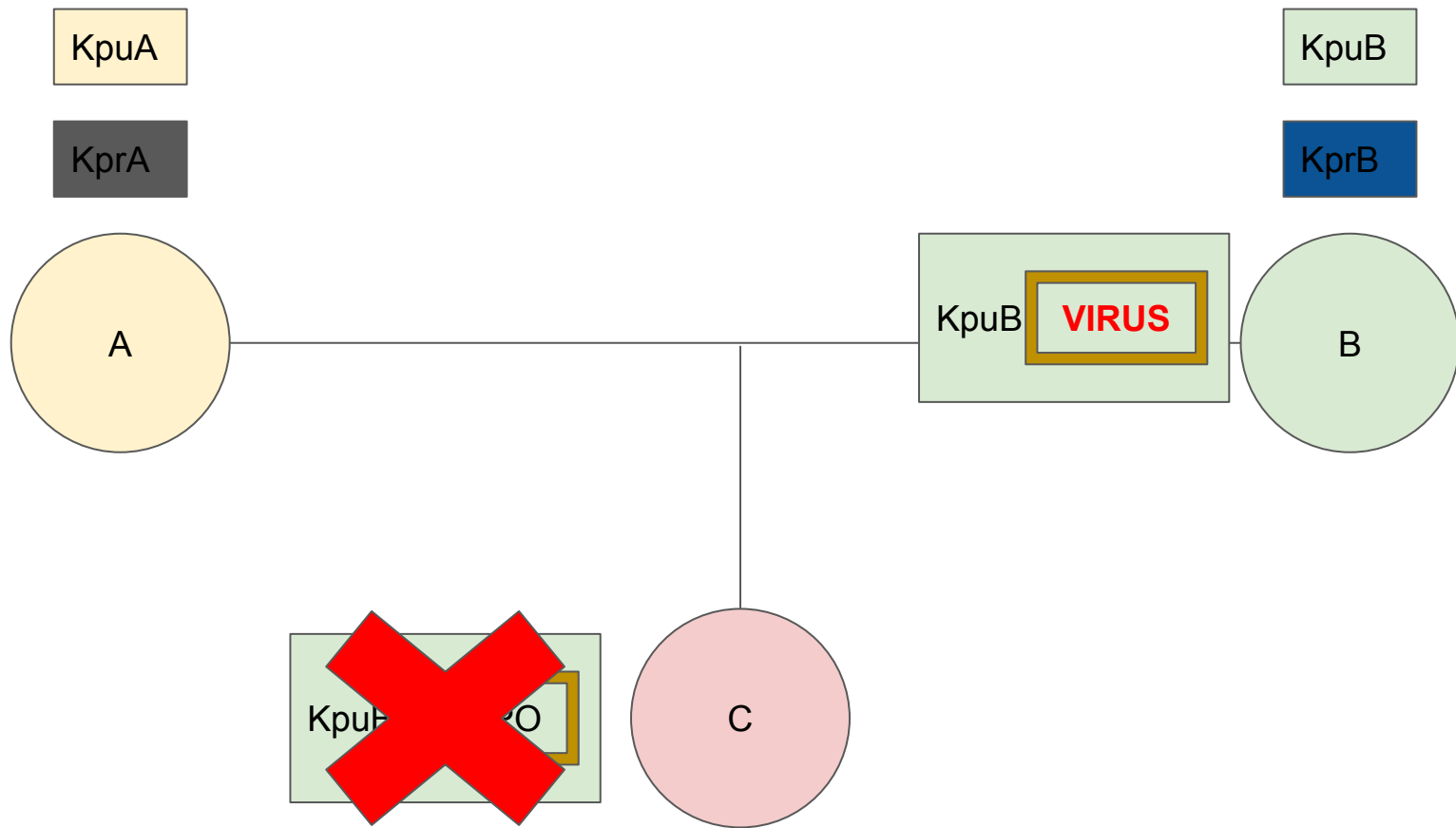


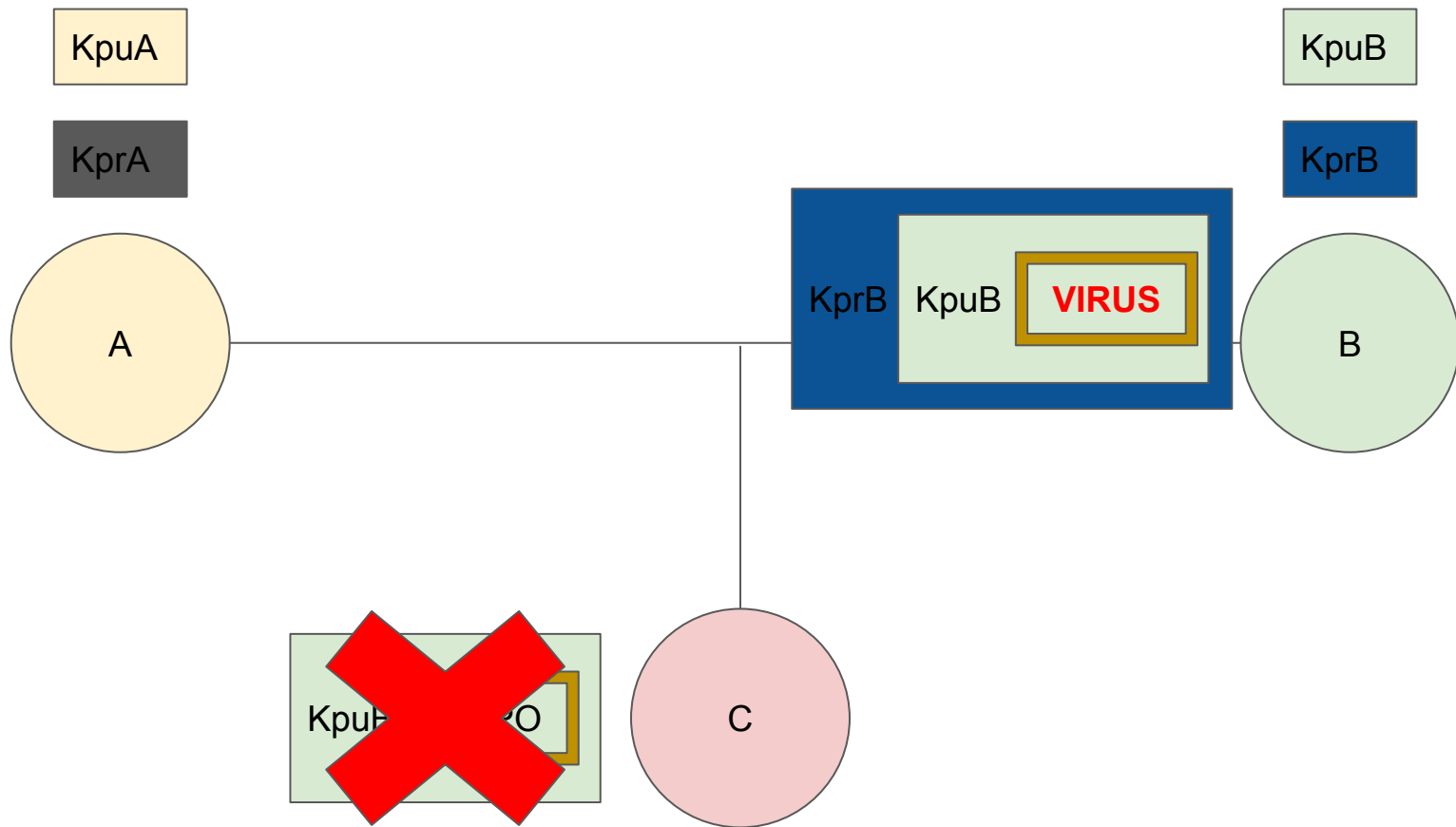


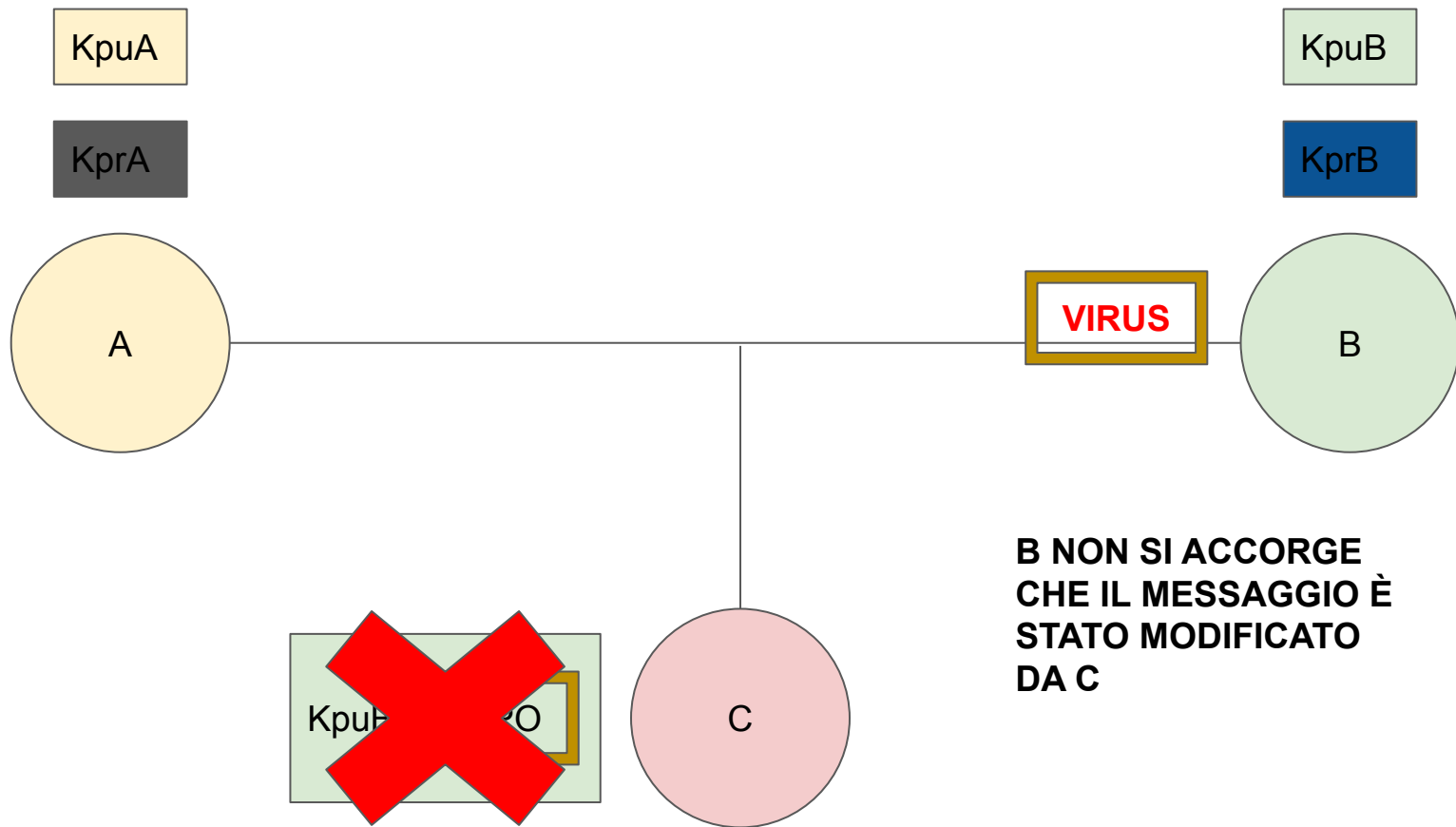






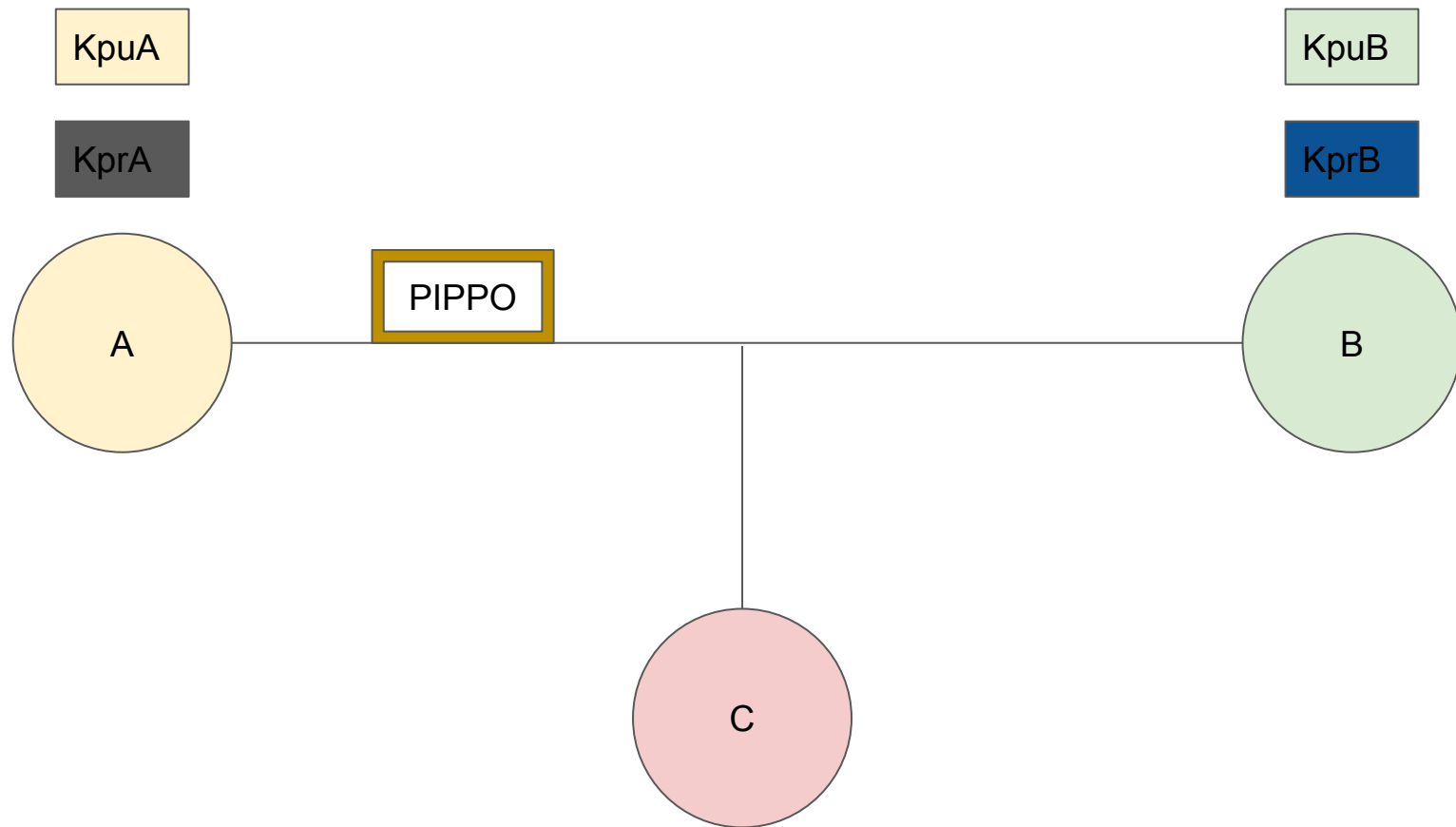


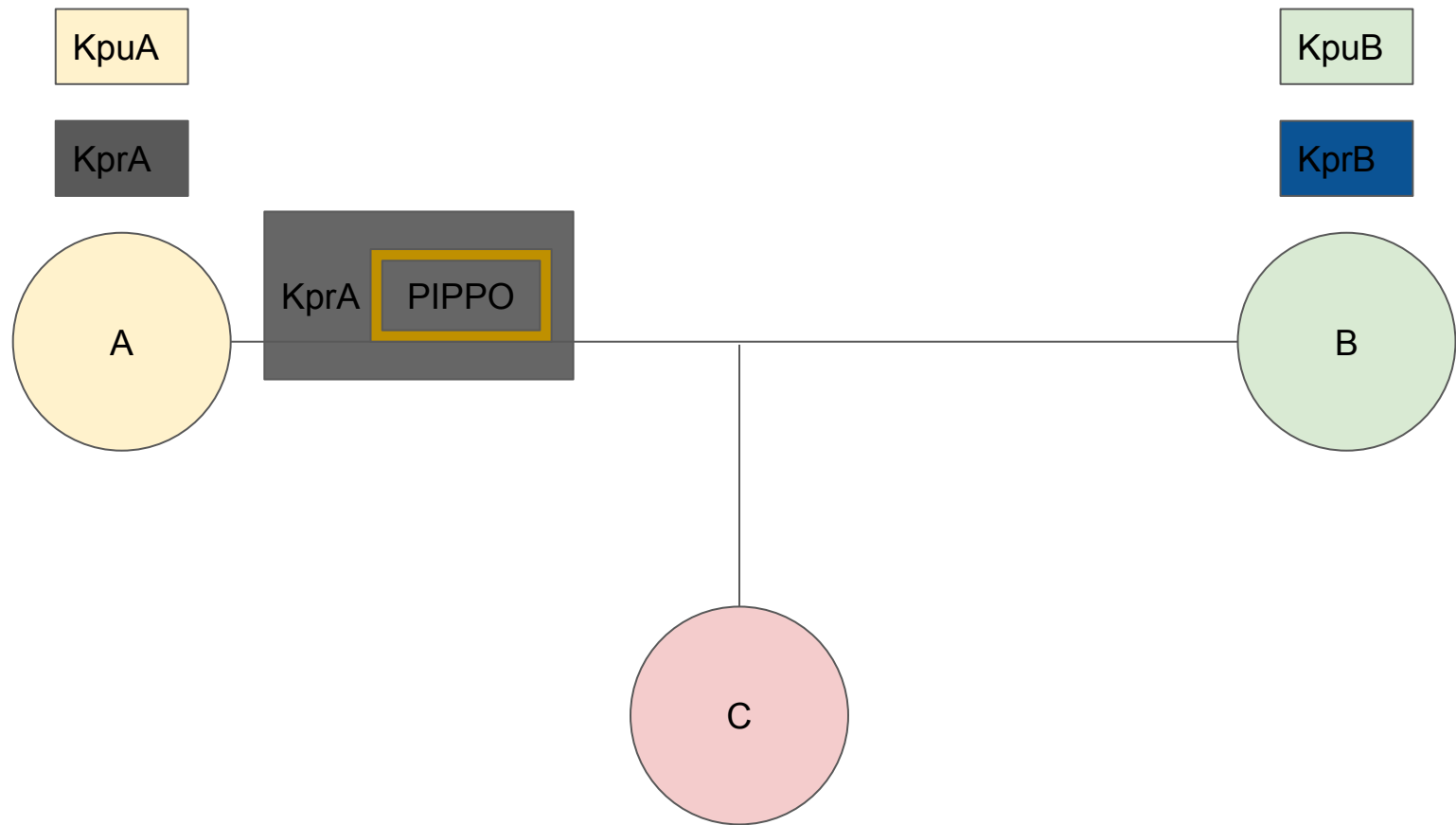


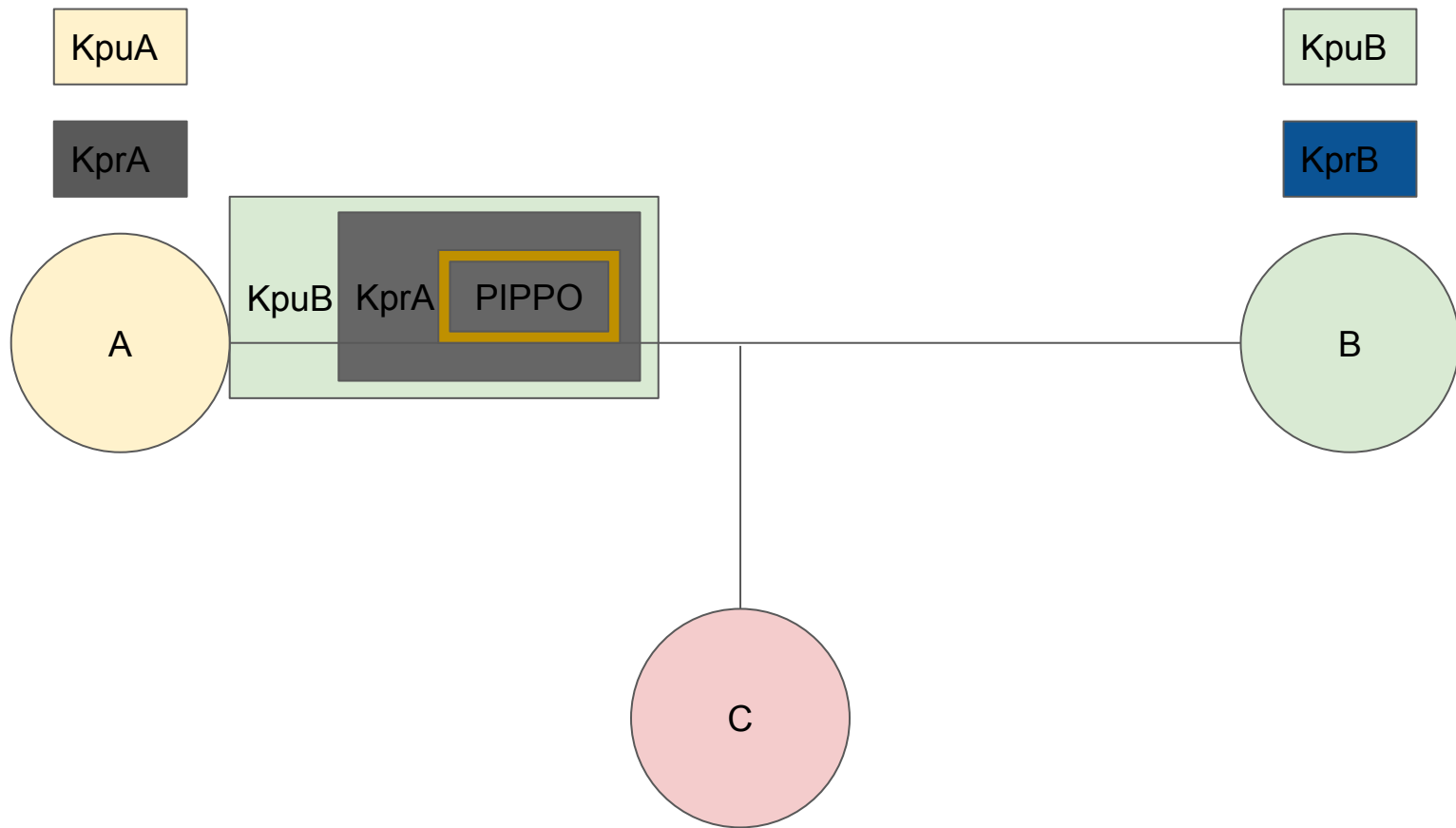


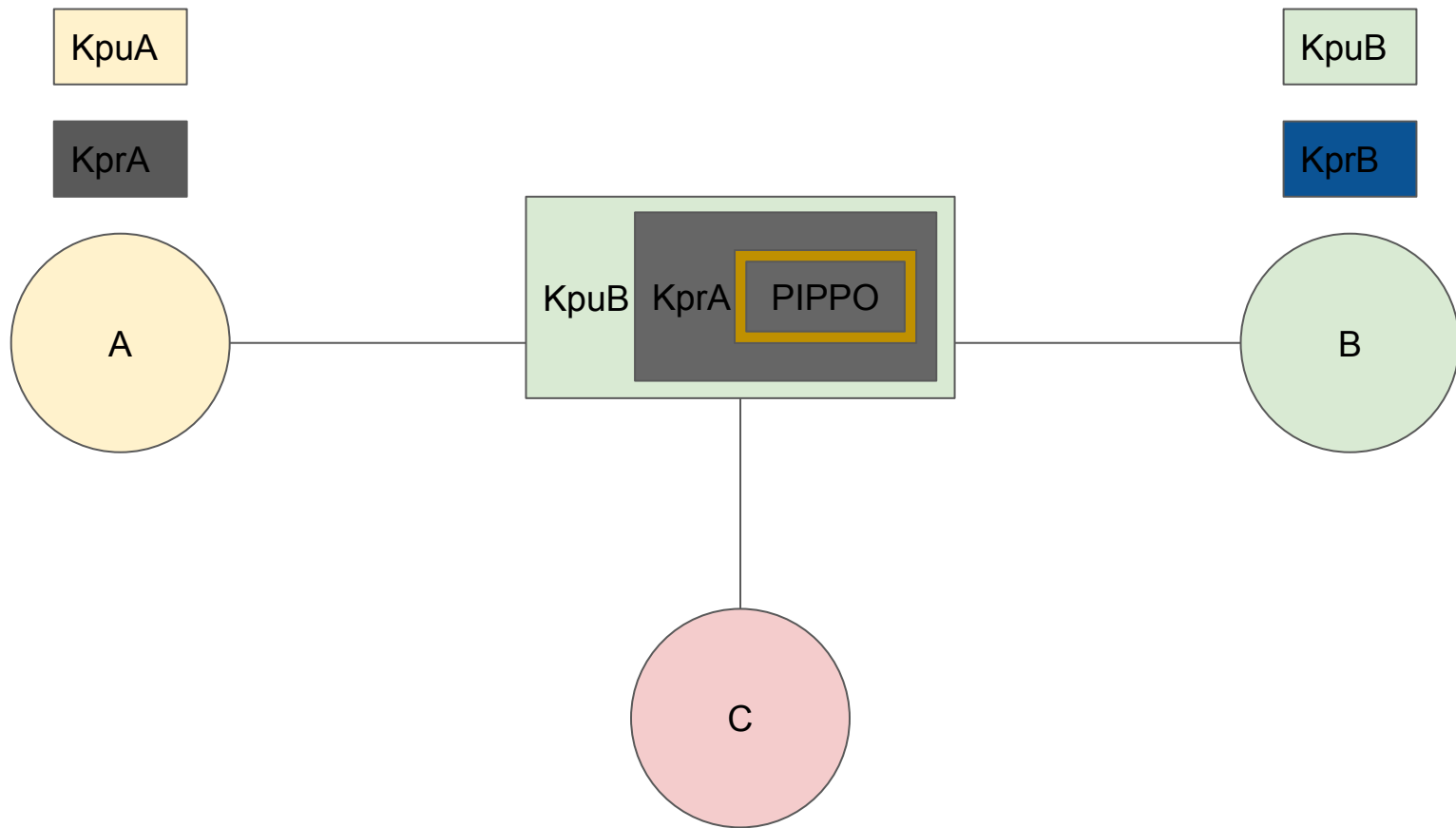
VERA SOLUZIONE

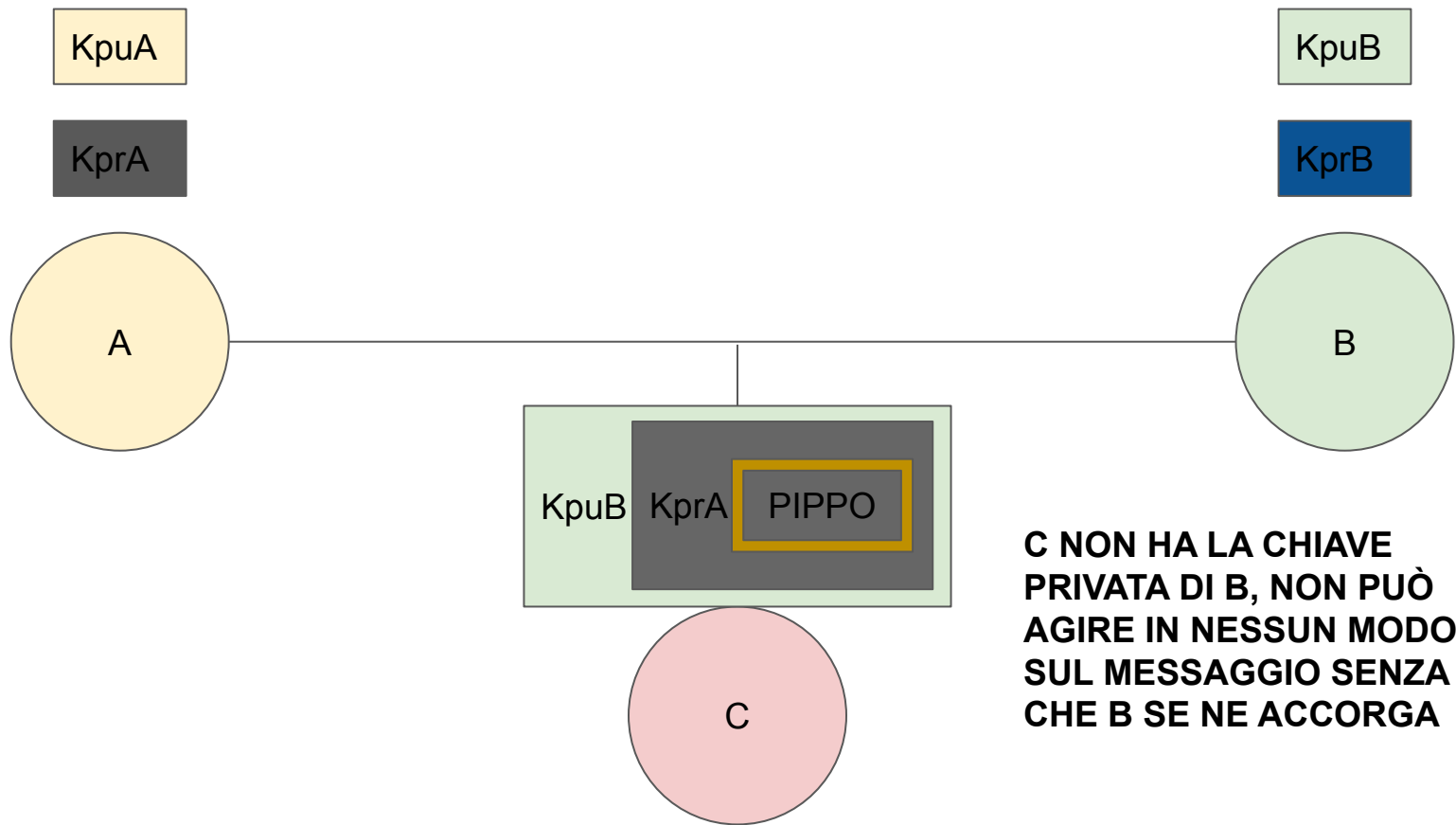
possibile attacco all'integrità di un messaggio

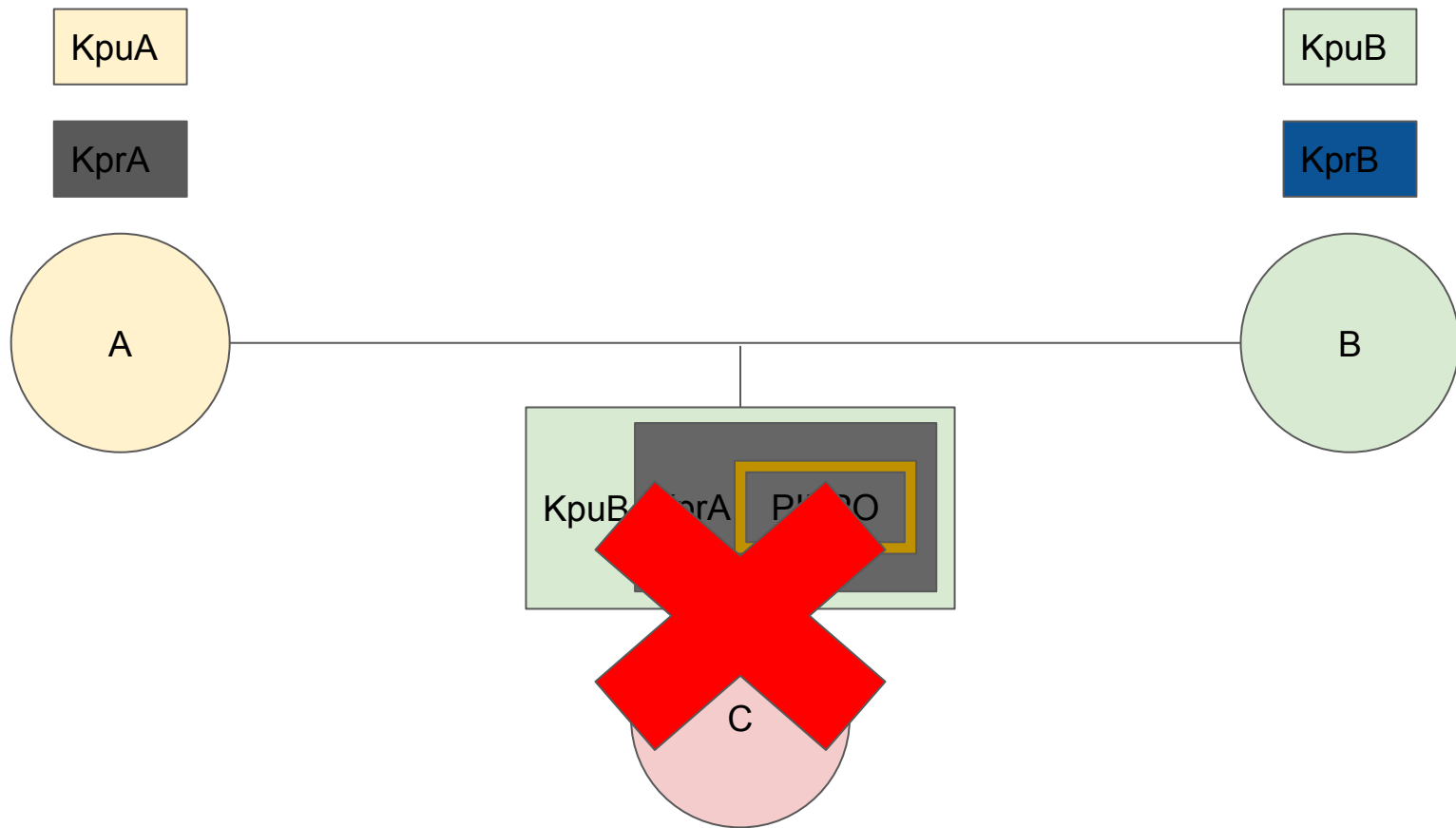


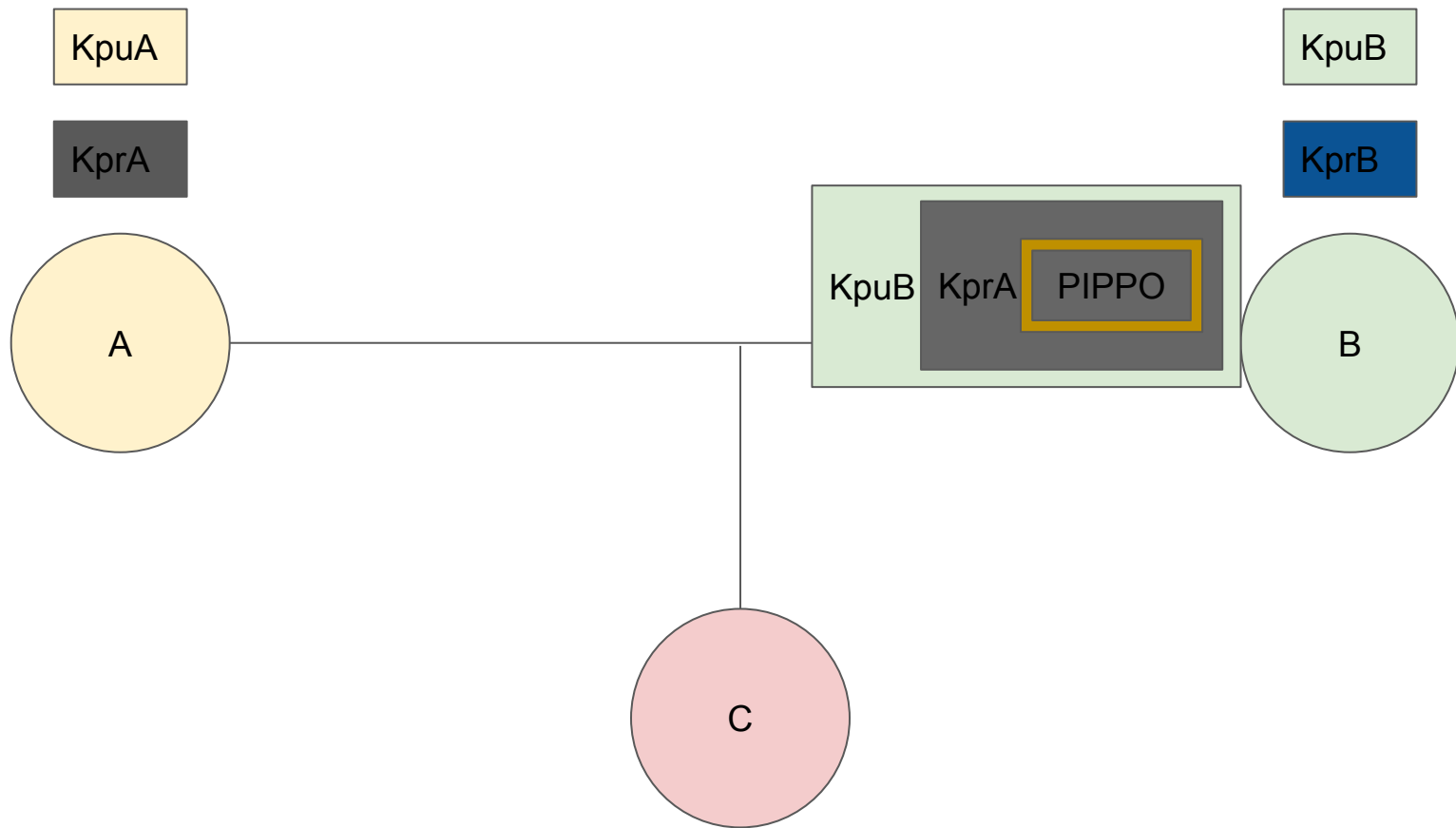


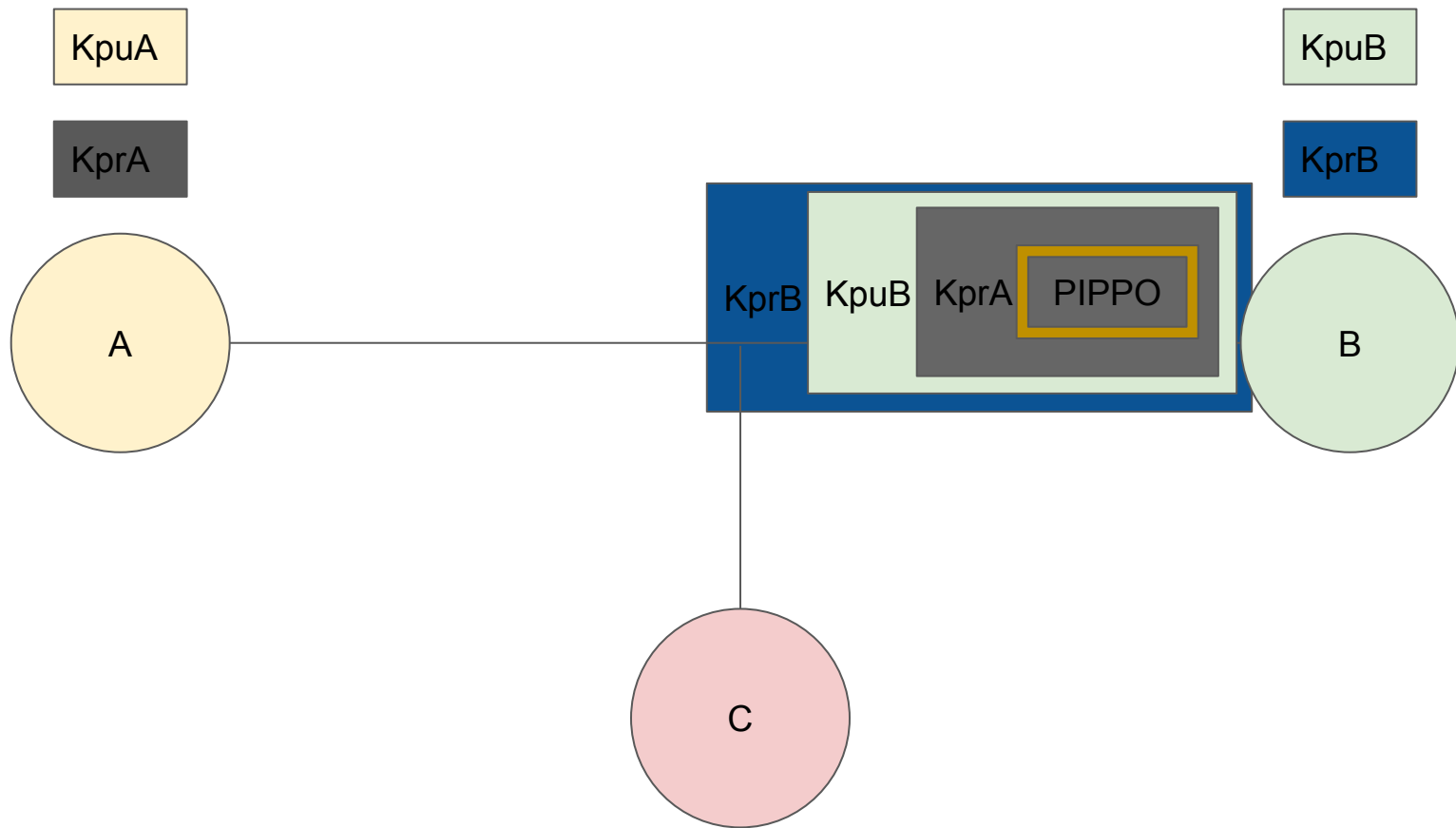


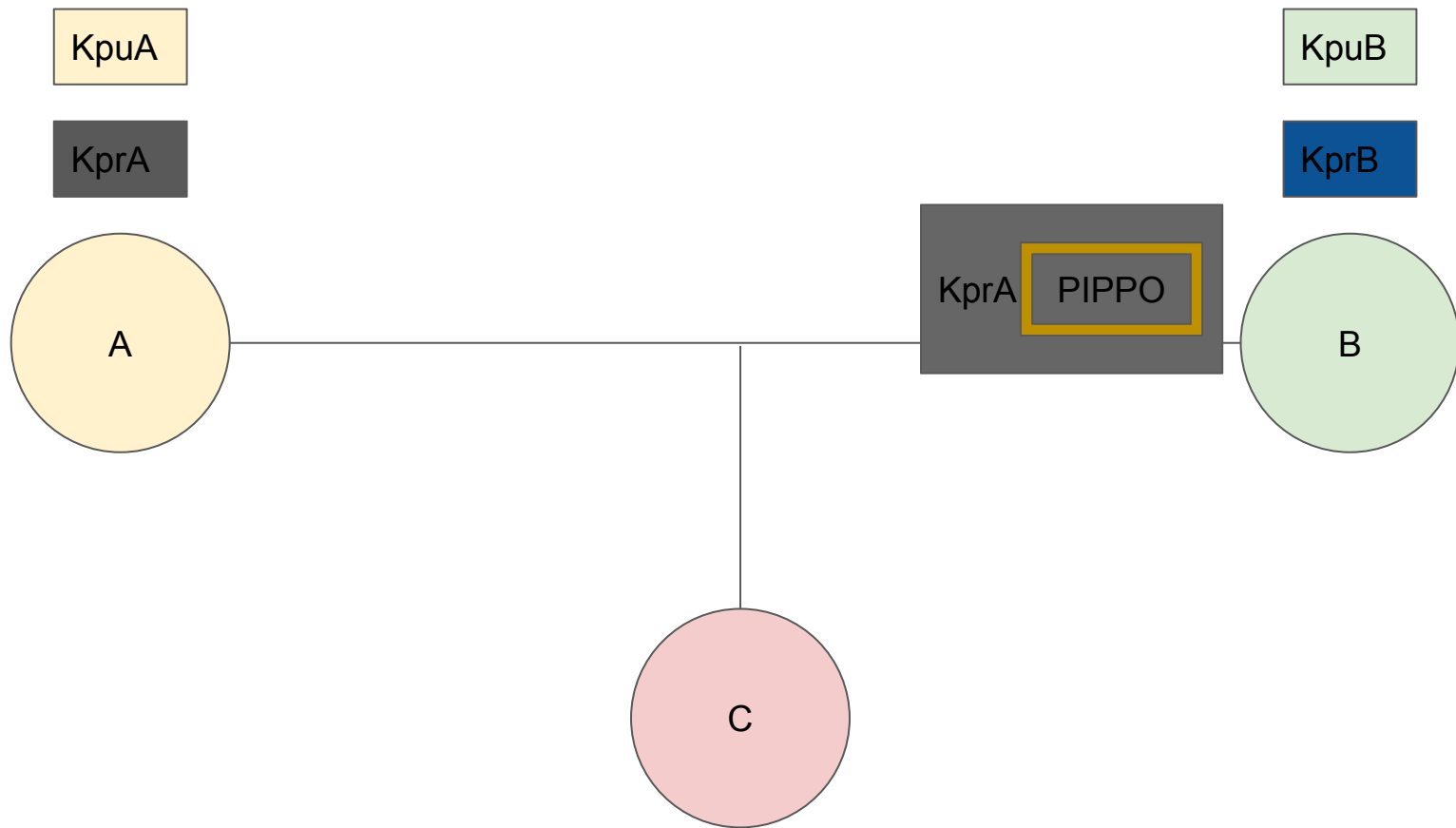


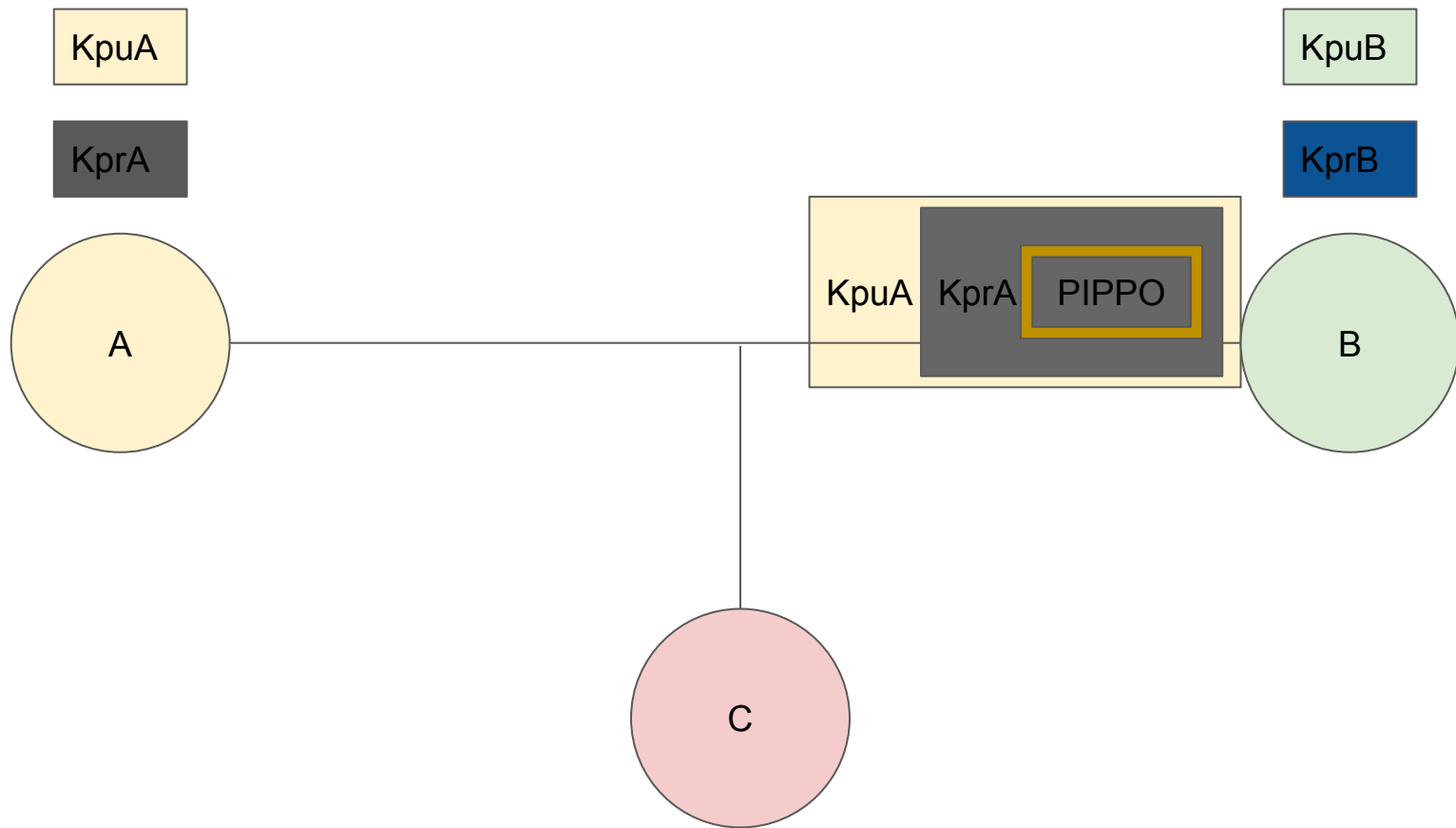


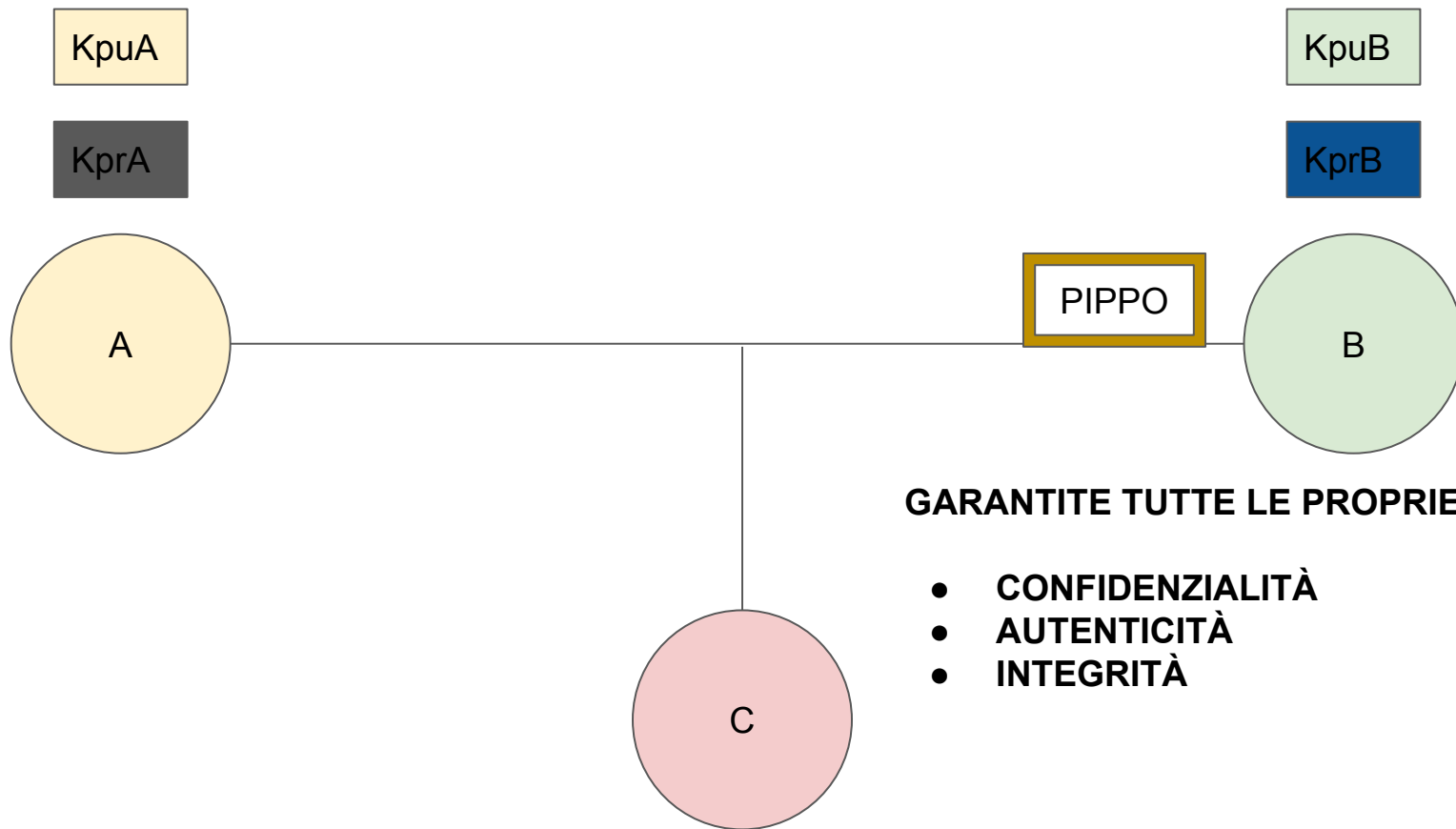










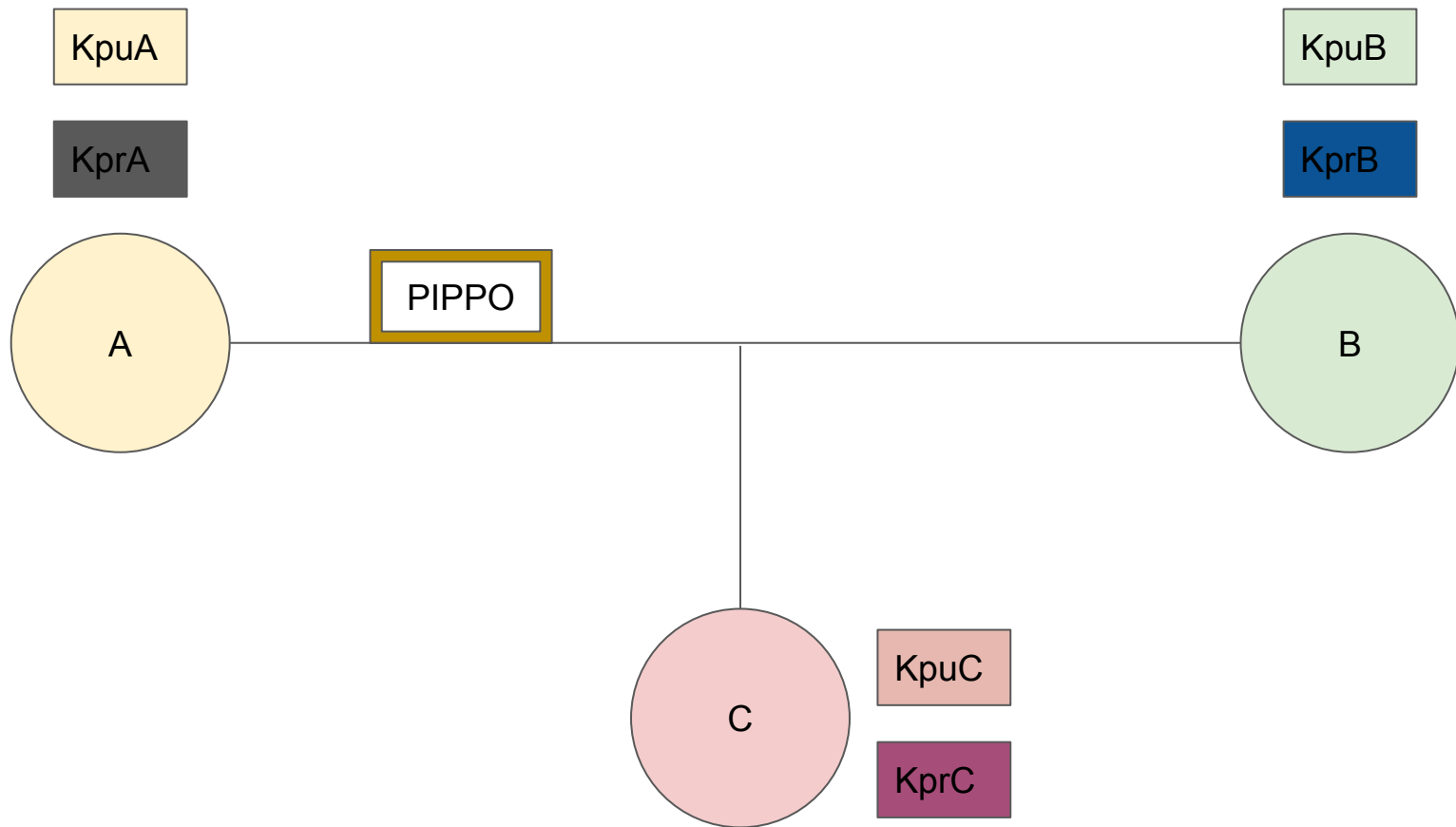


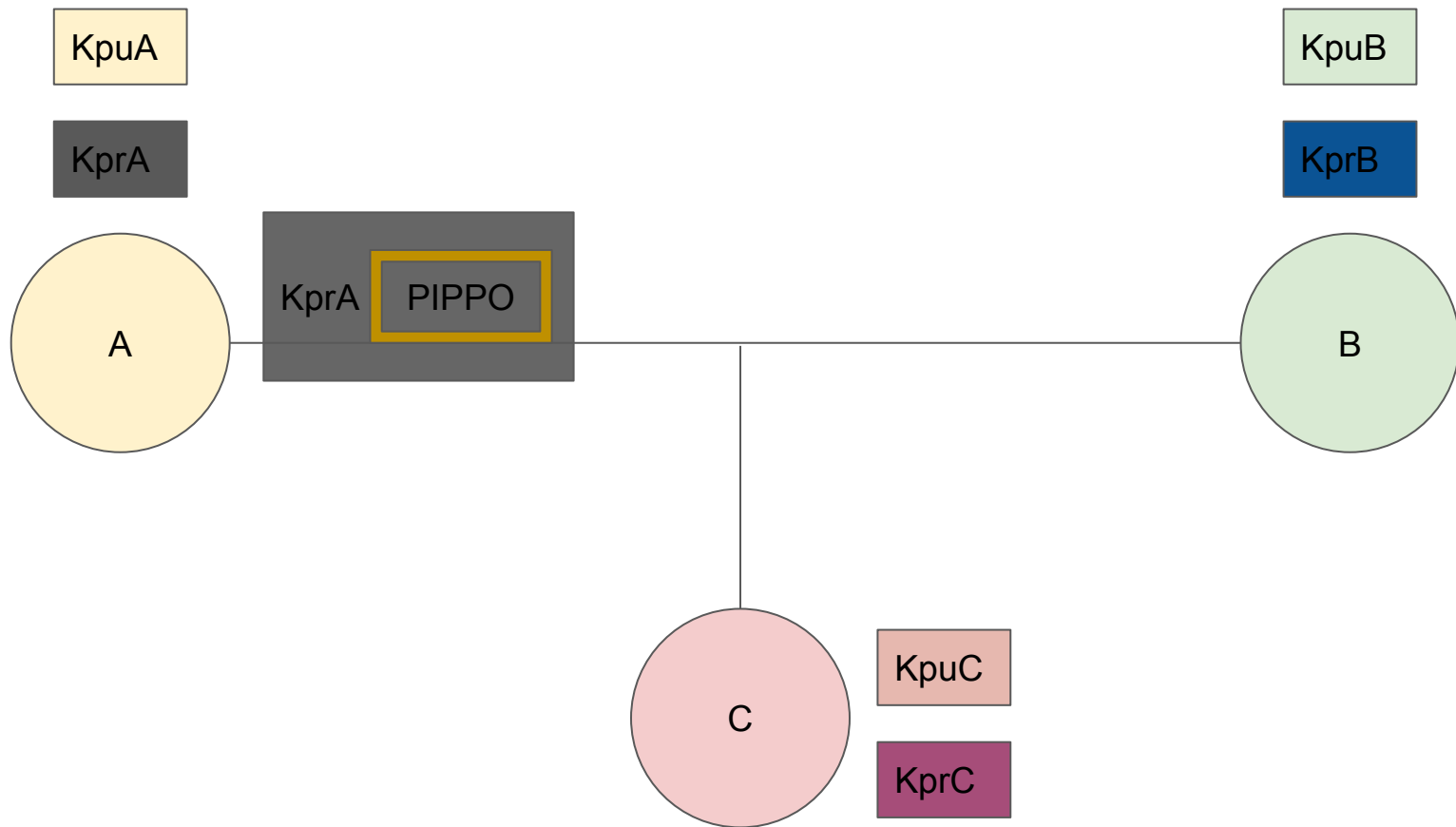
GARANTITE TUTTE LE PROPRIETÀ

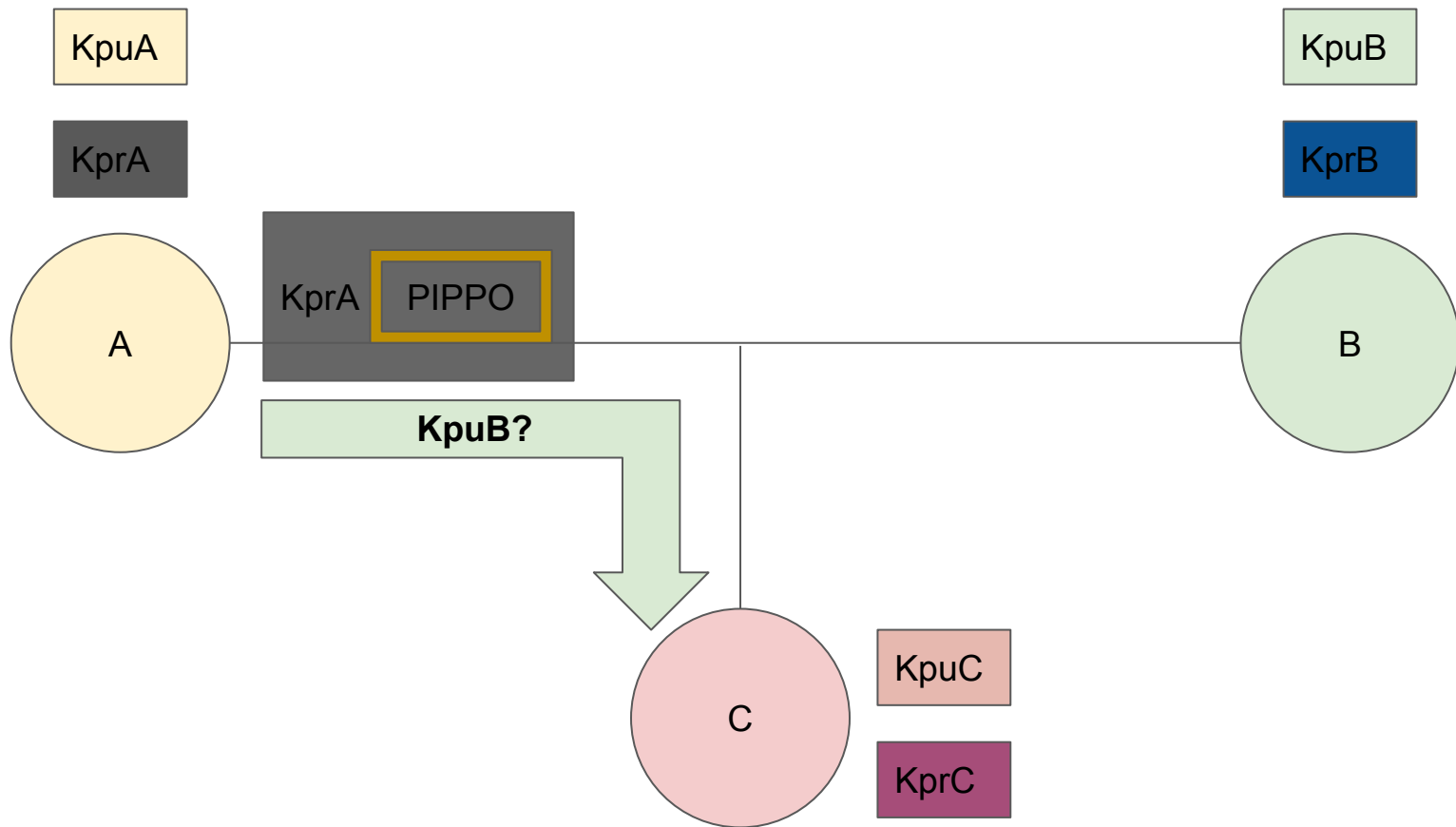
- **CONFIDENZIALITÀ**
- **AUTENTICITÀ**
- **INTEGRITÀ**

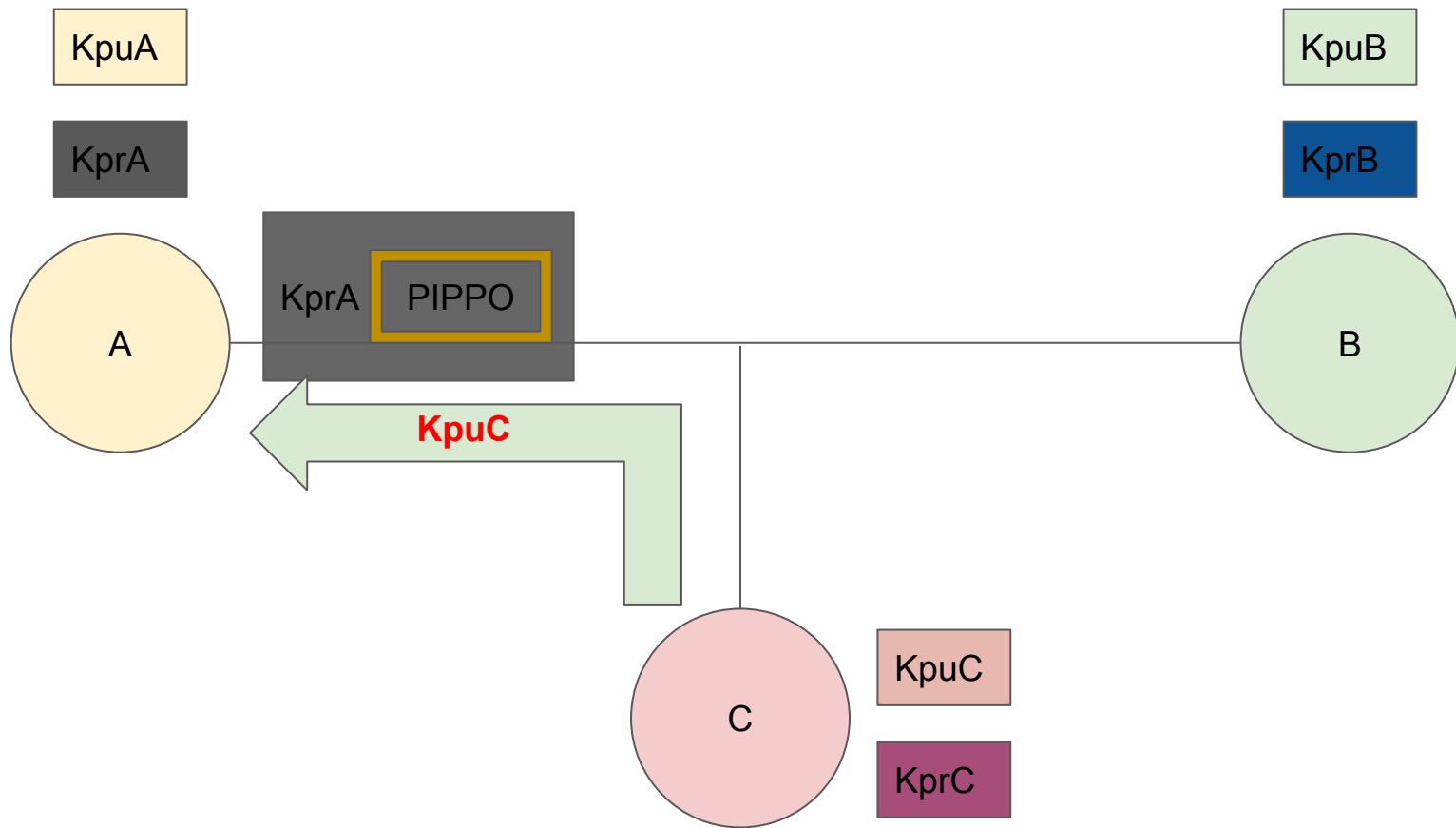
MAN IN THE MIDDLE

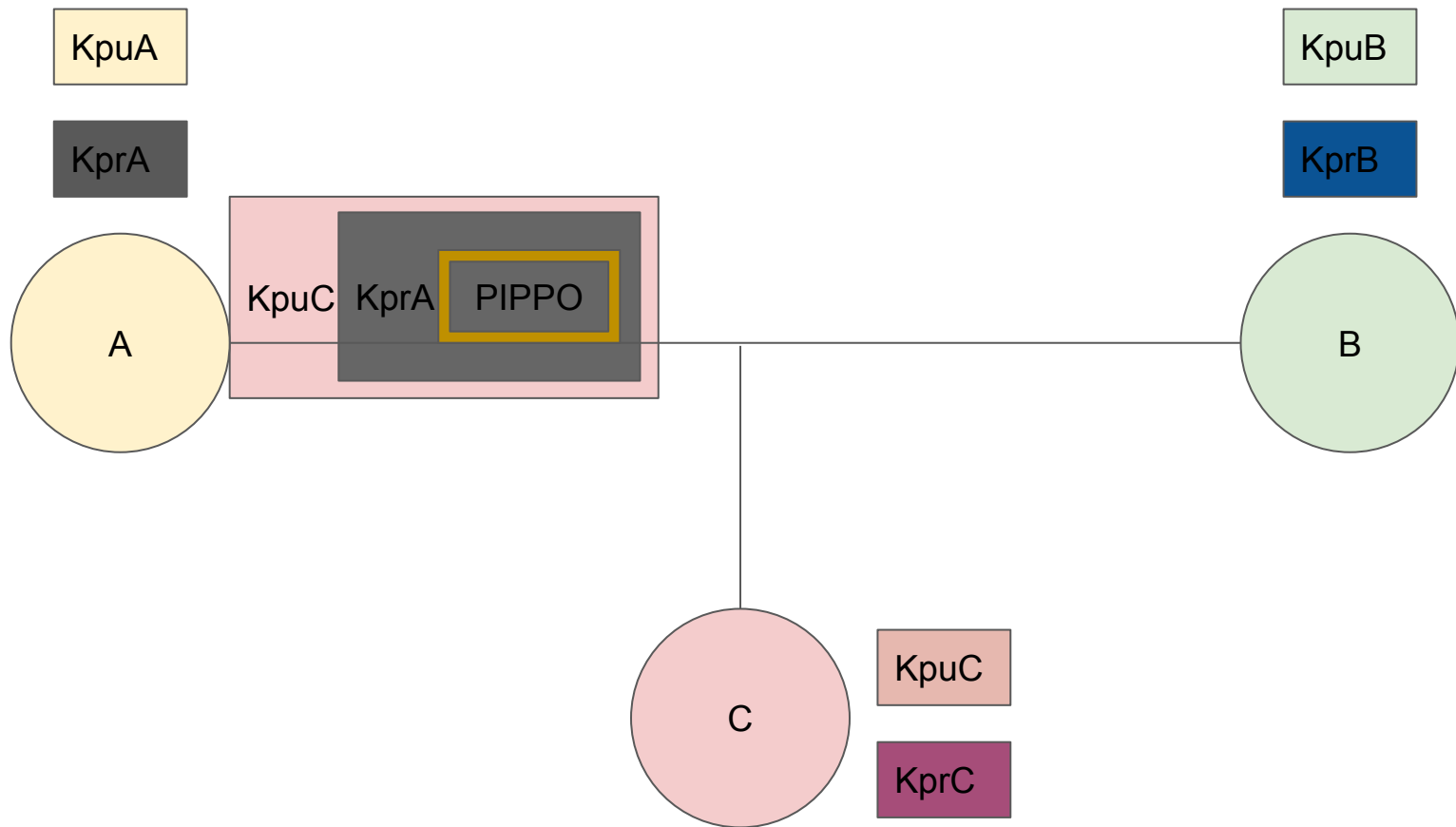
attacco al modello RSA

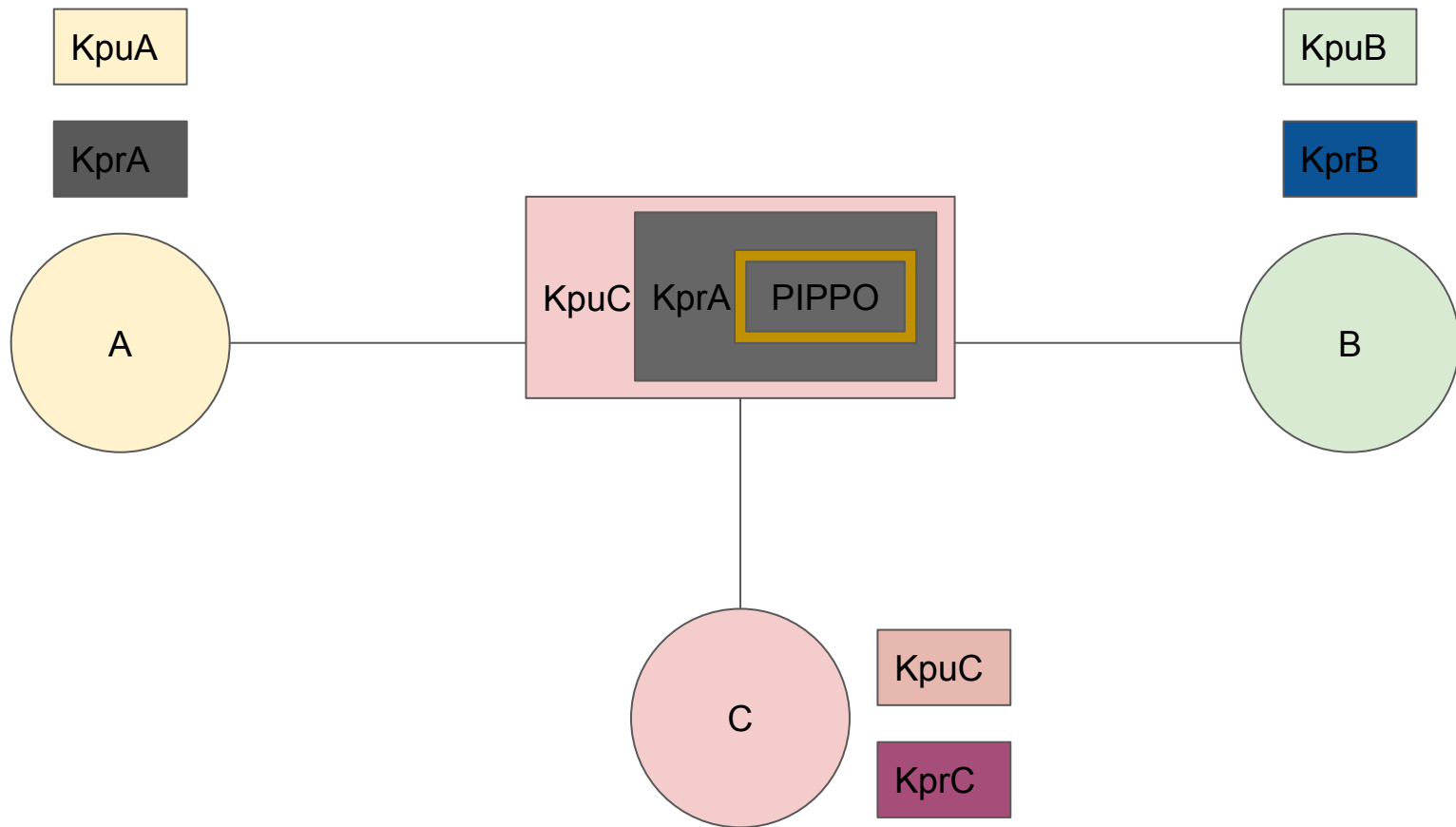


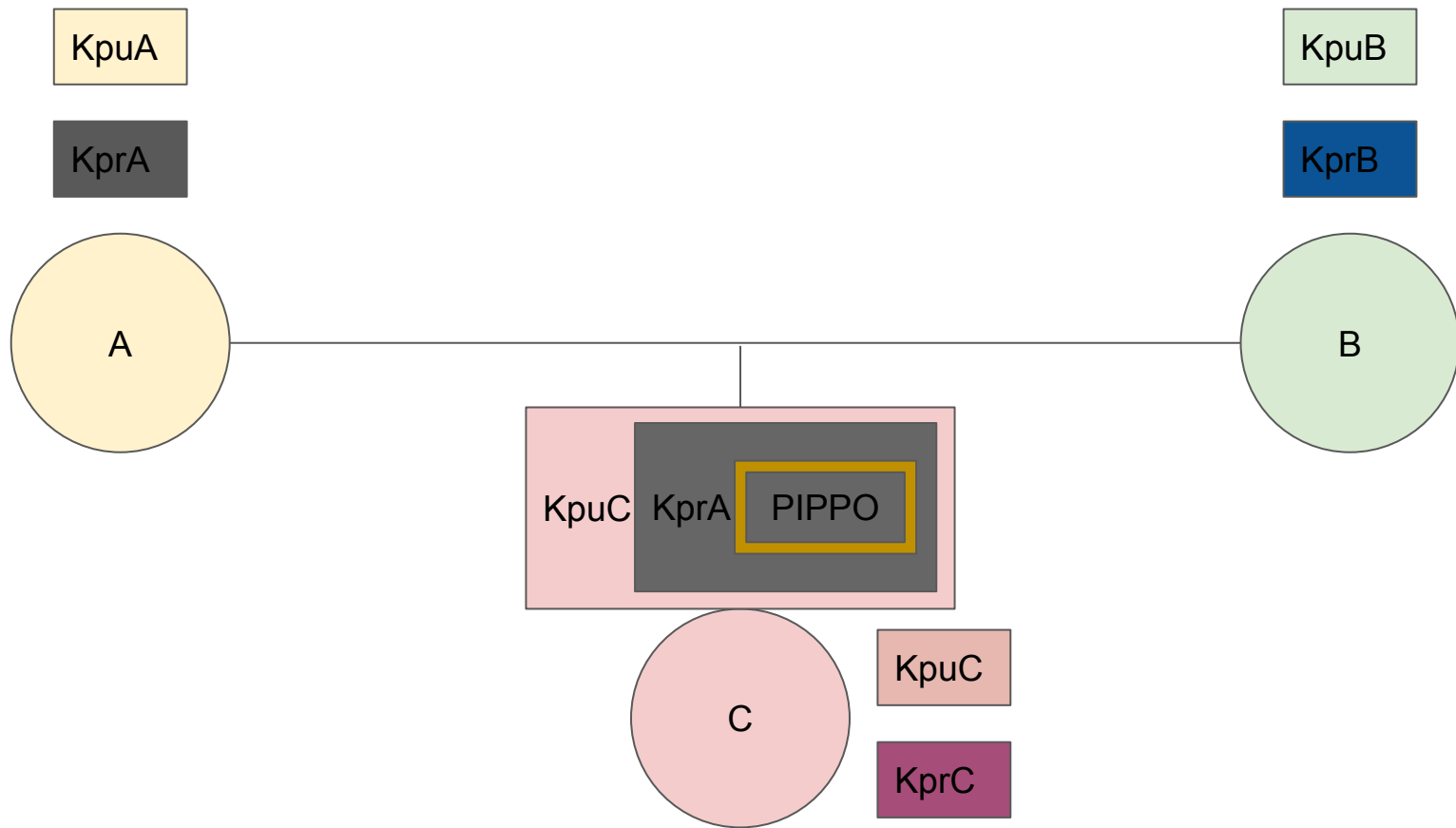


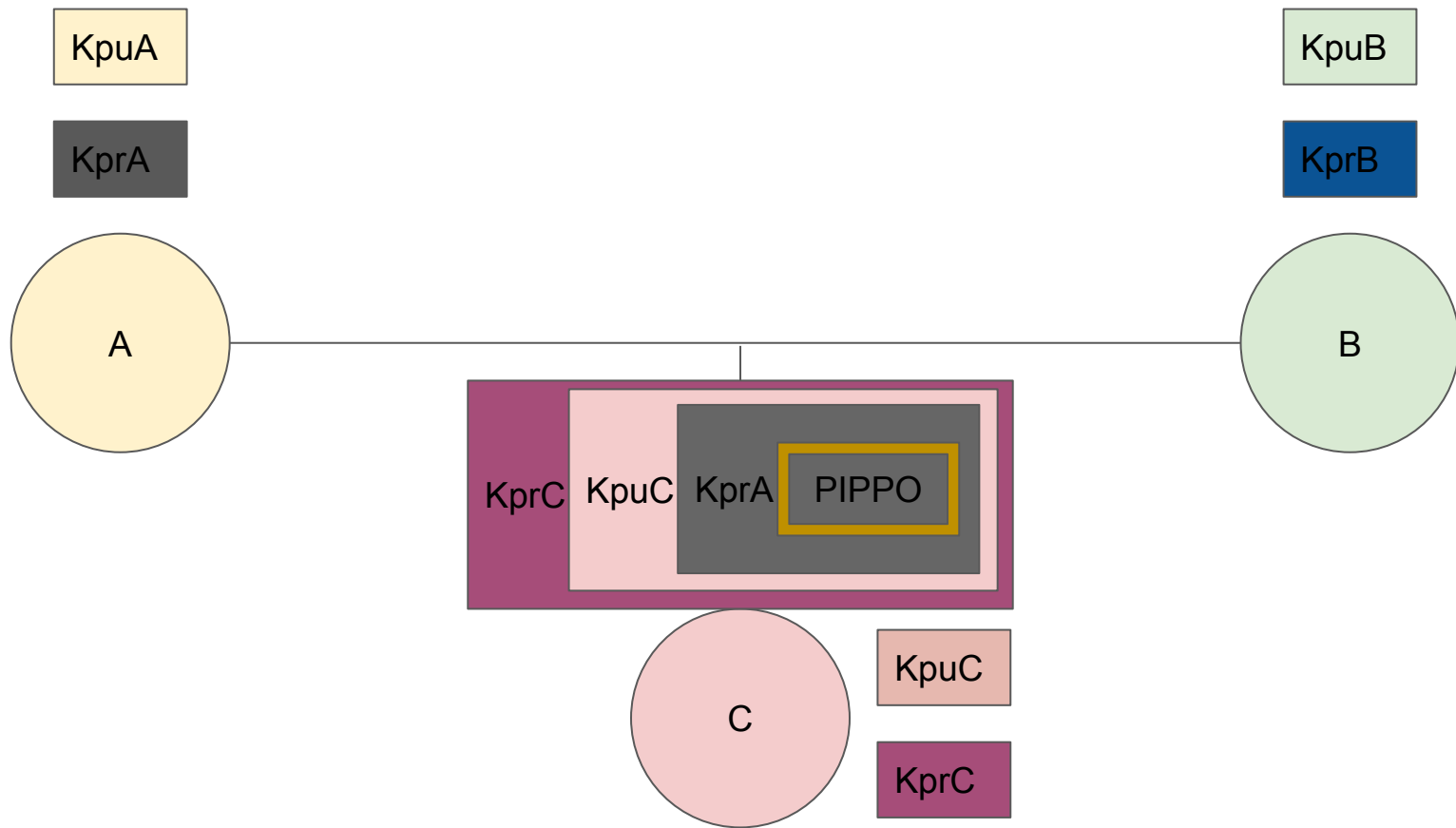


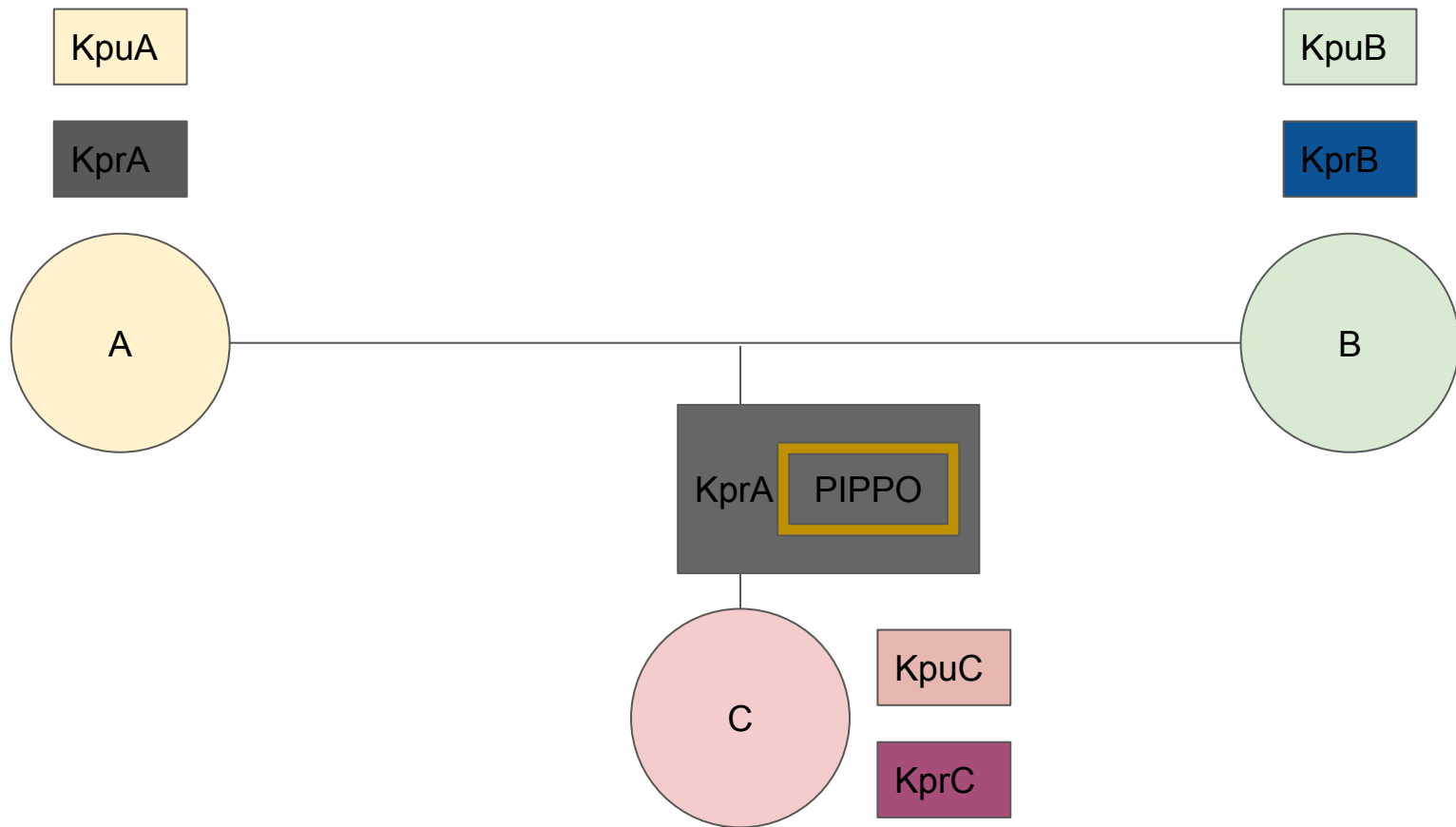


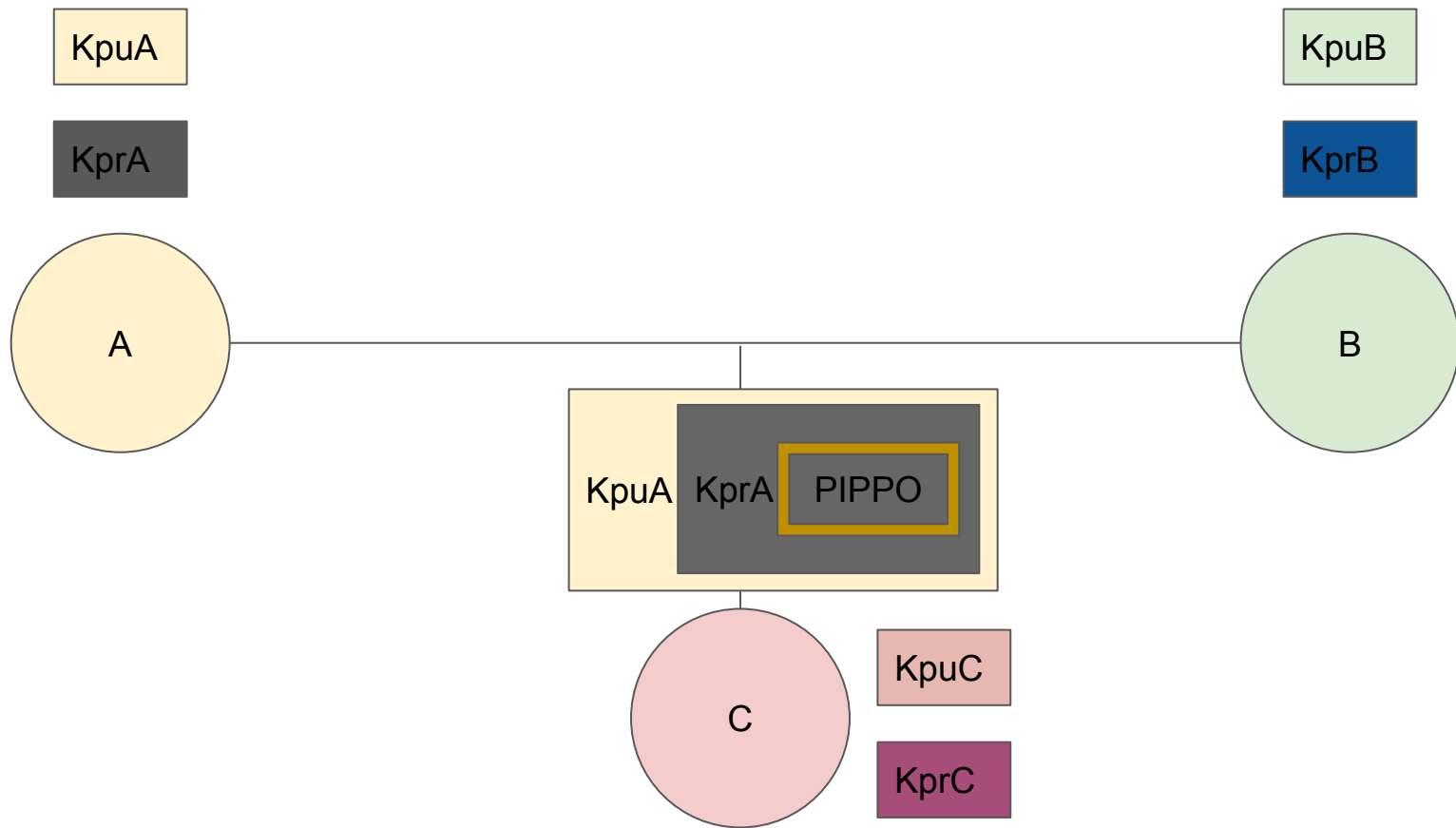


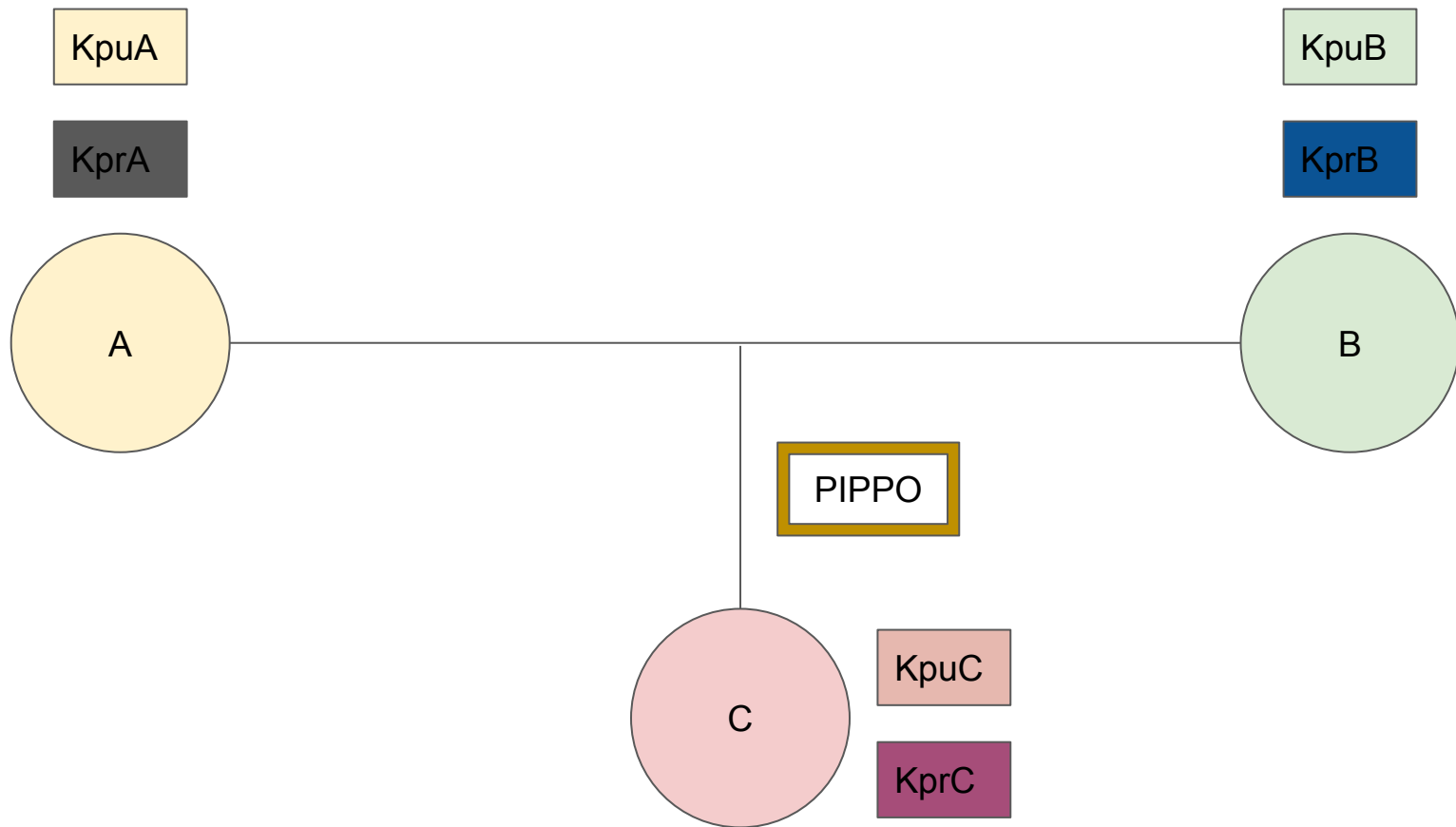


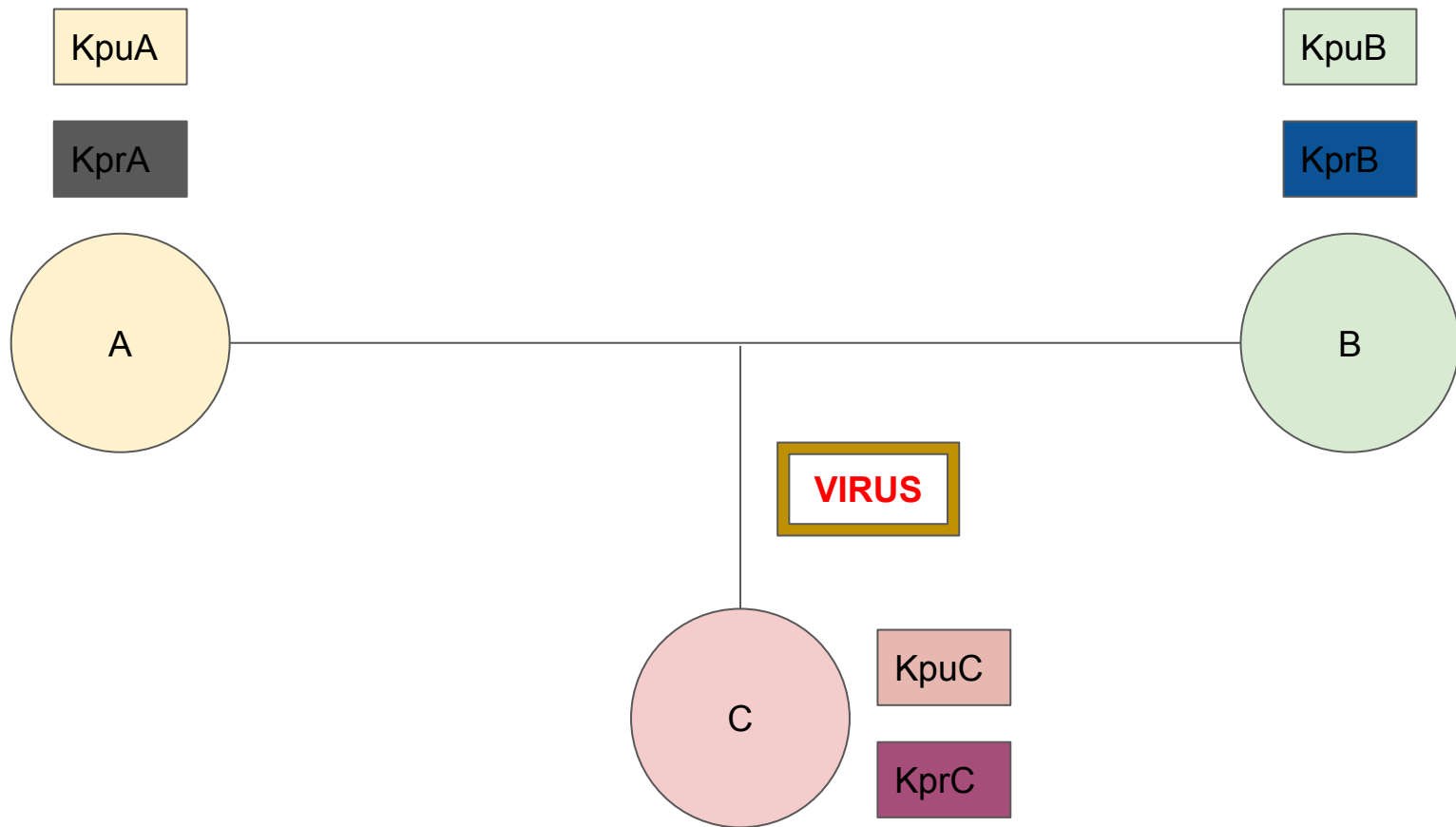


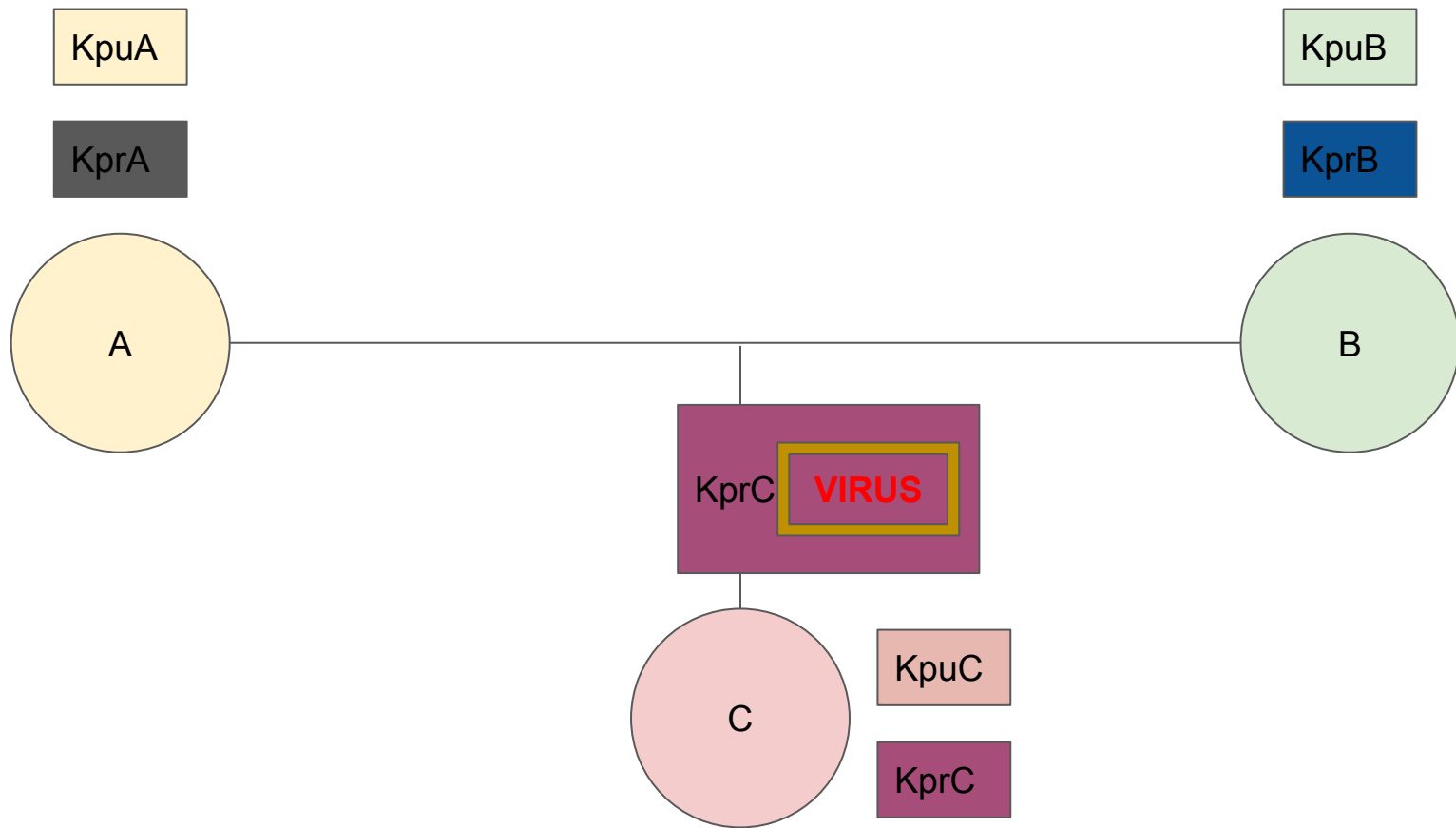


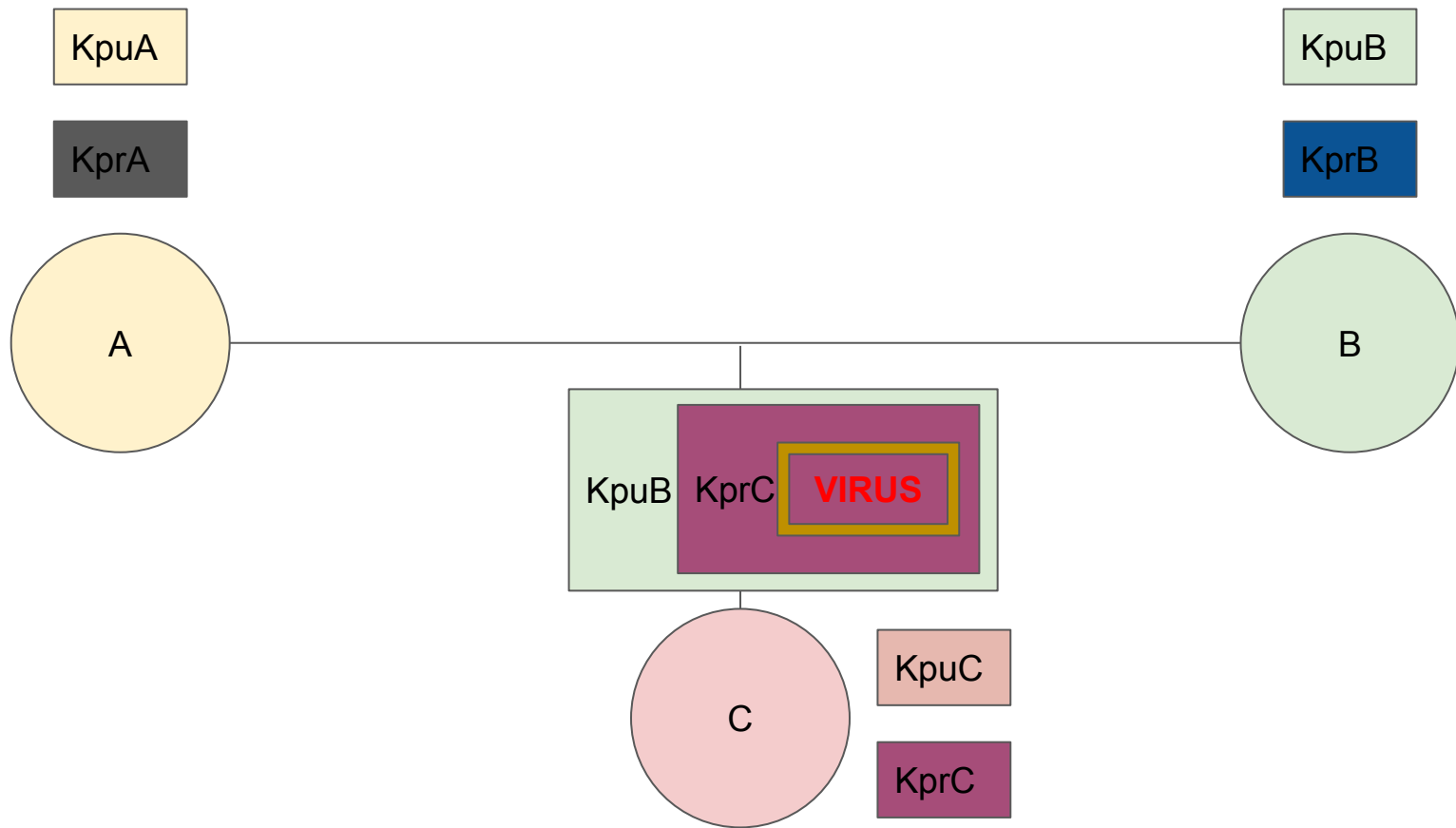


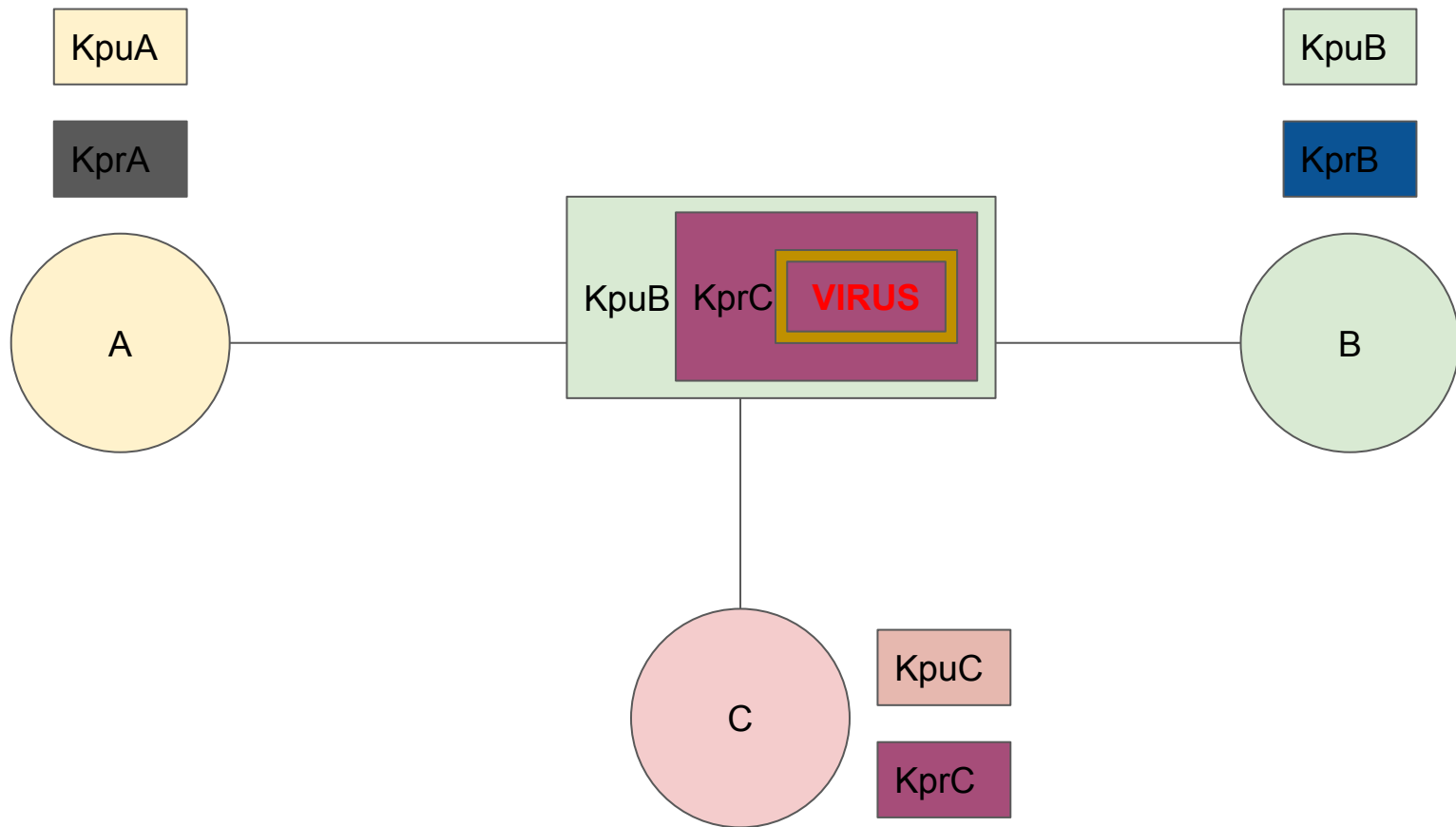


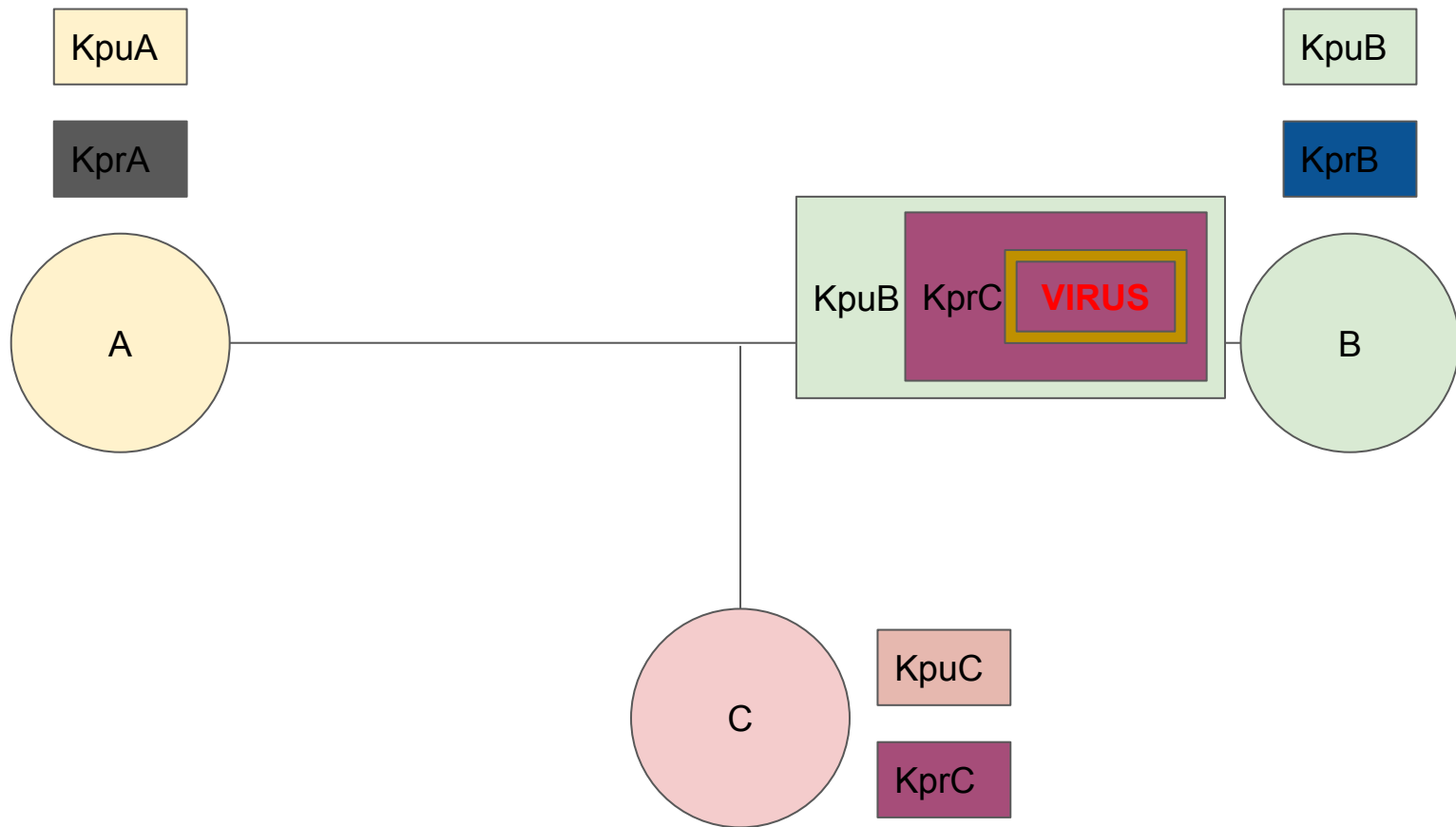


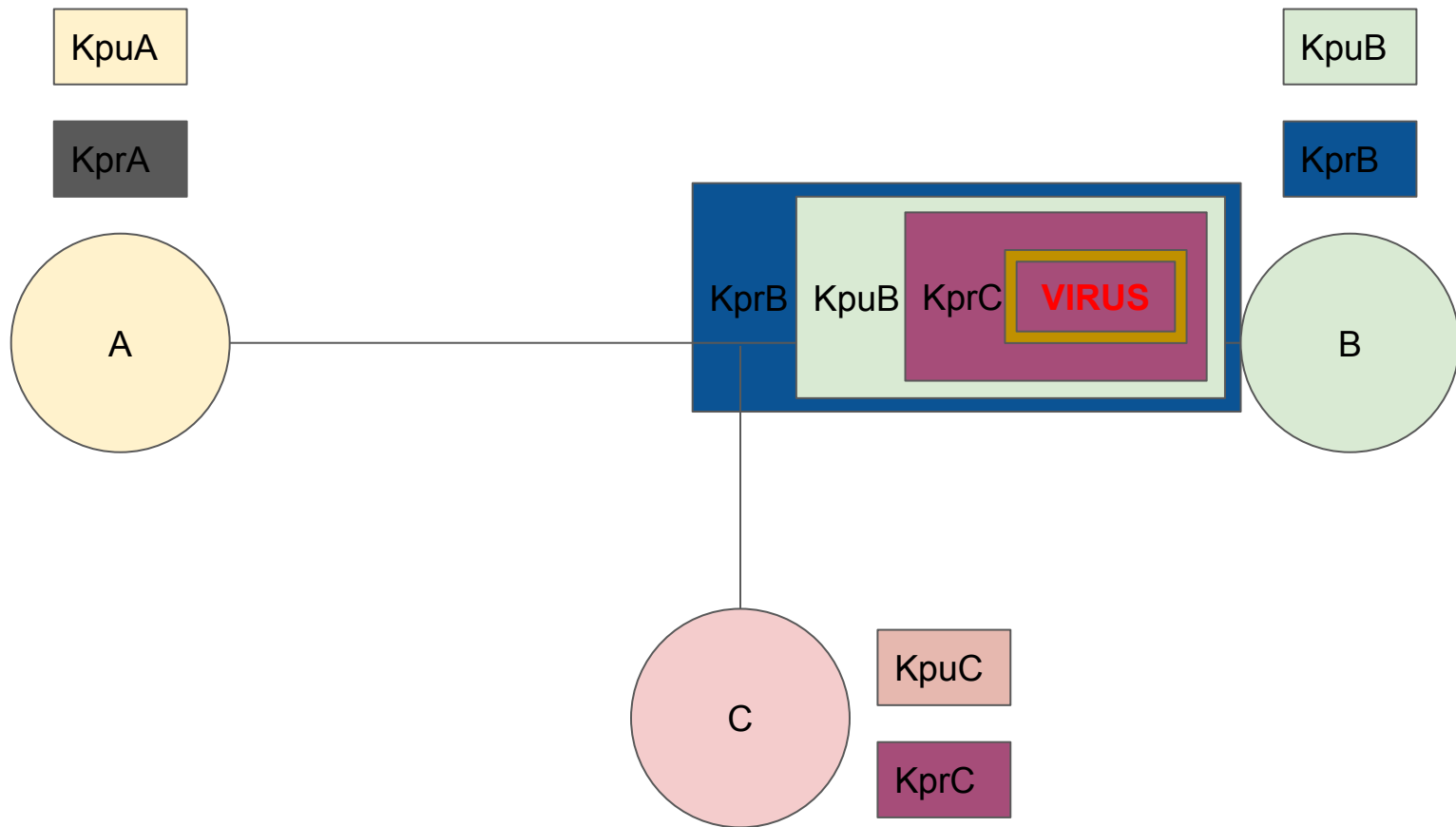


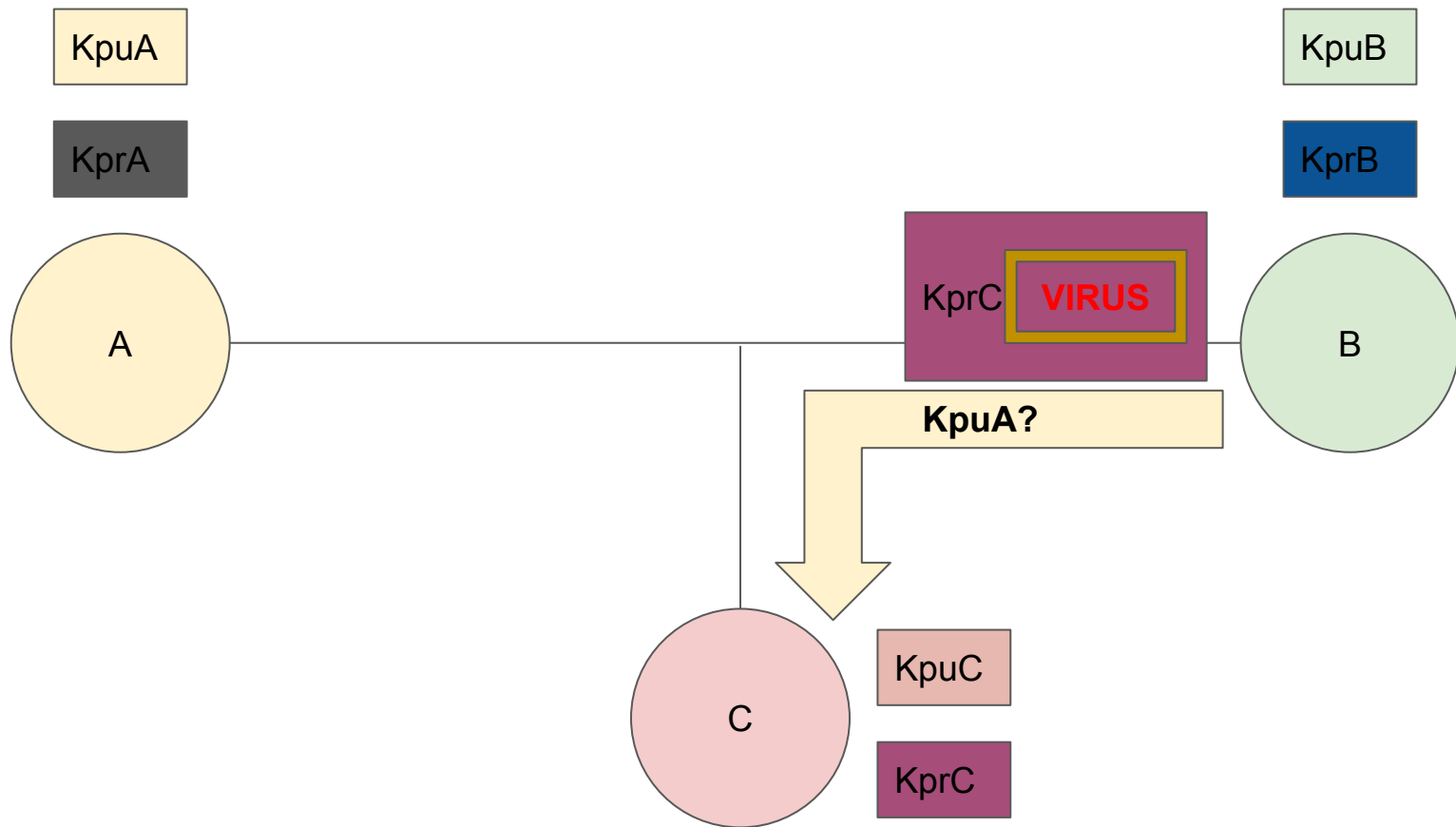


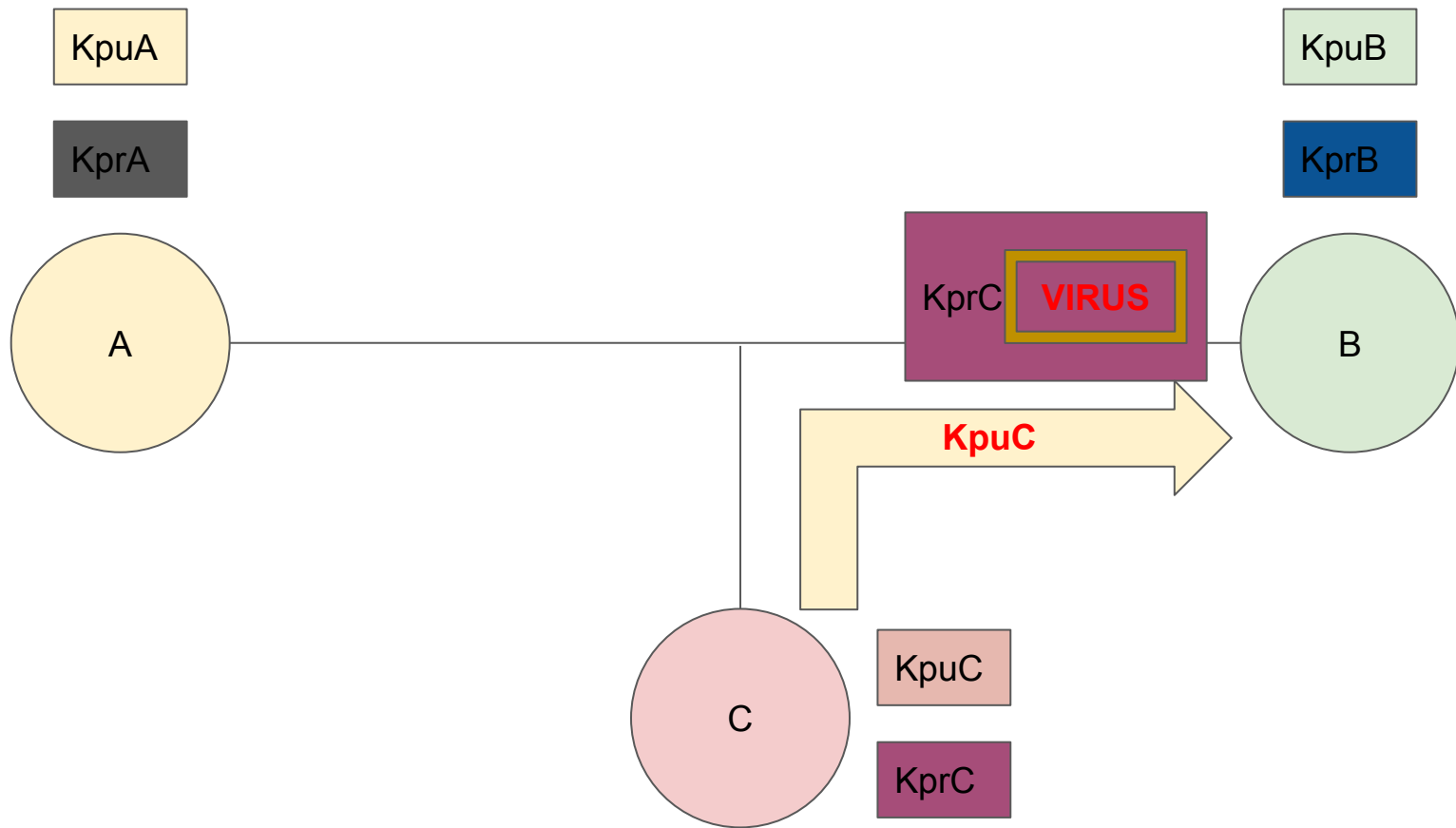


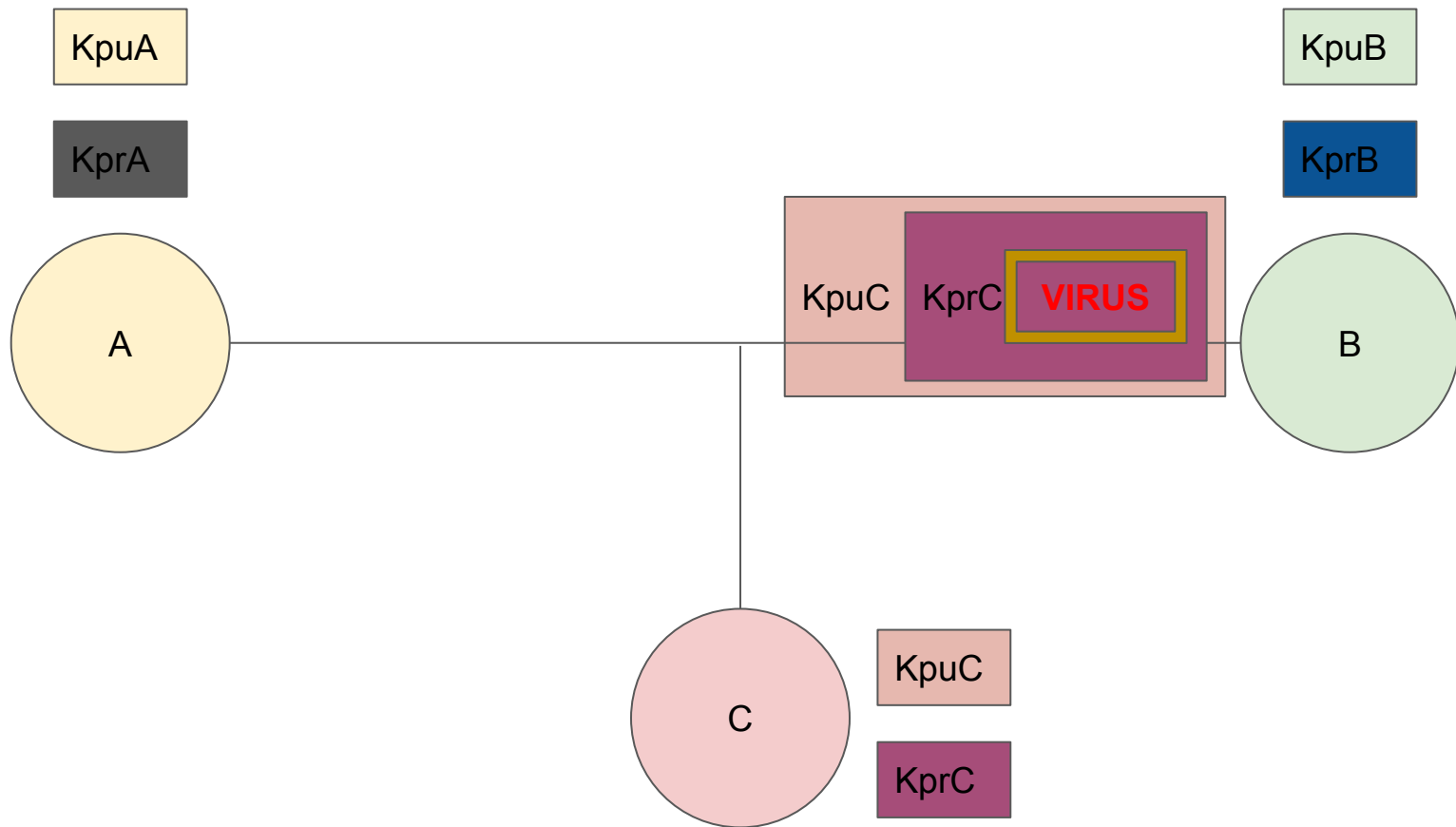


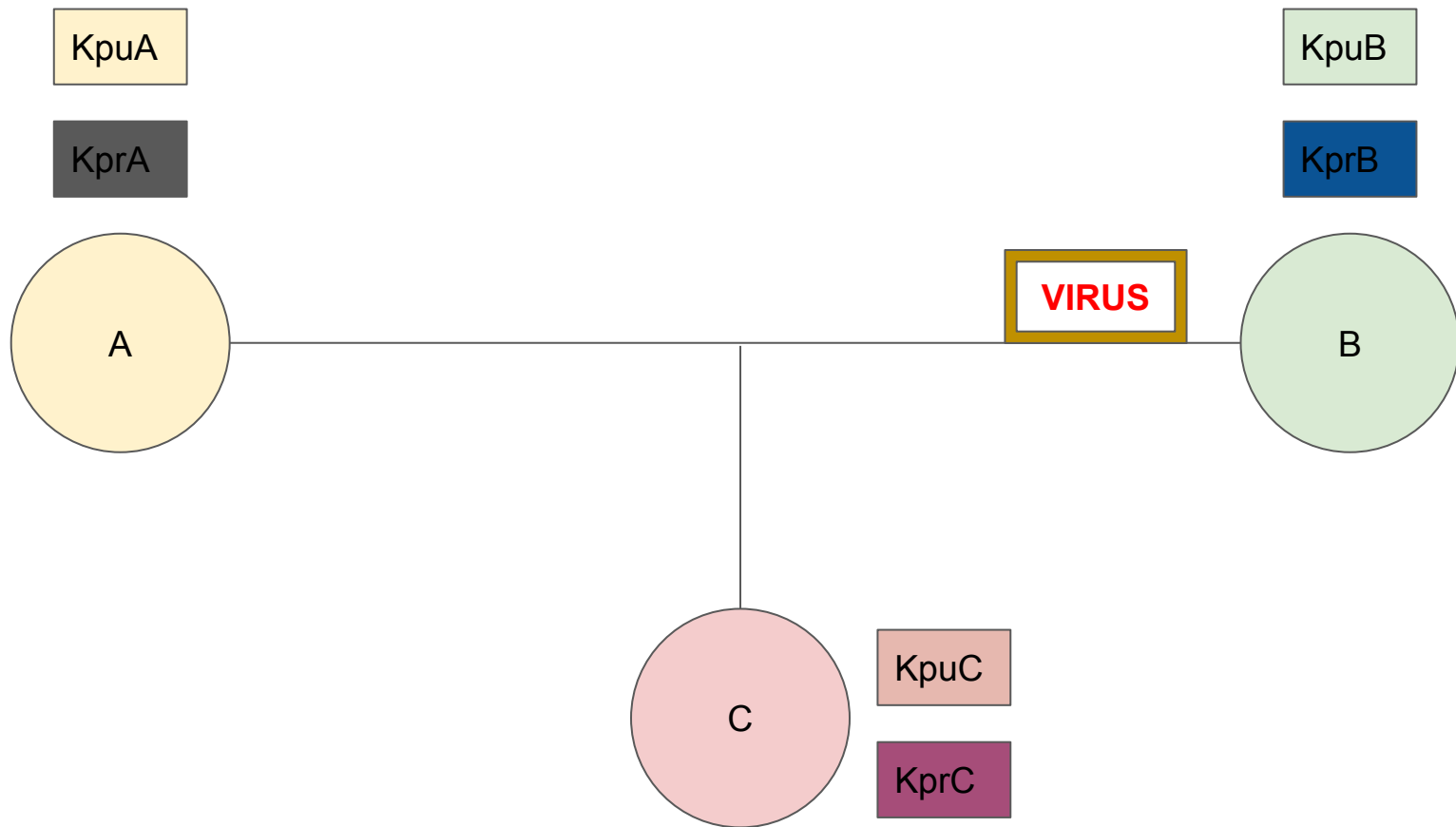






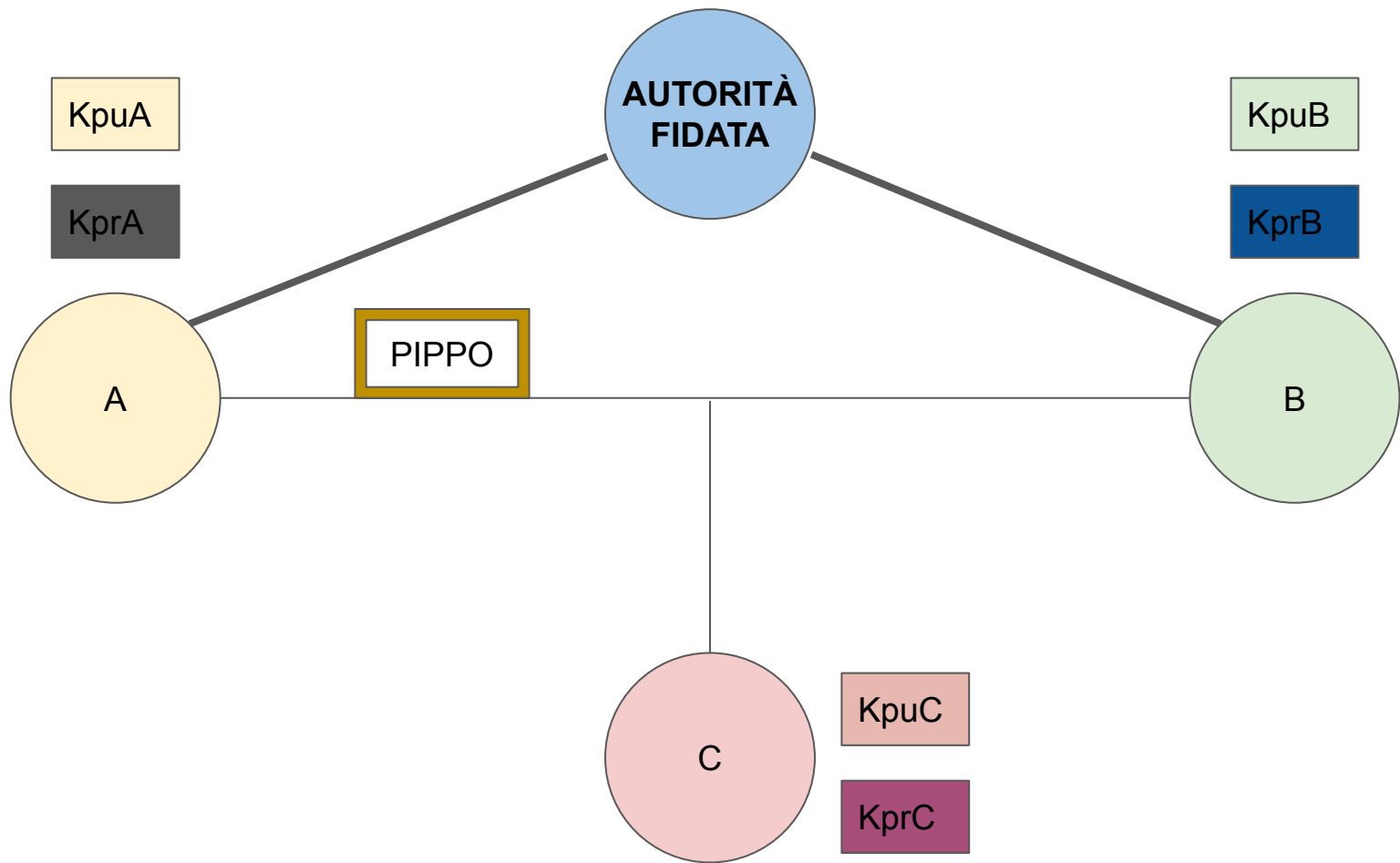


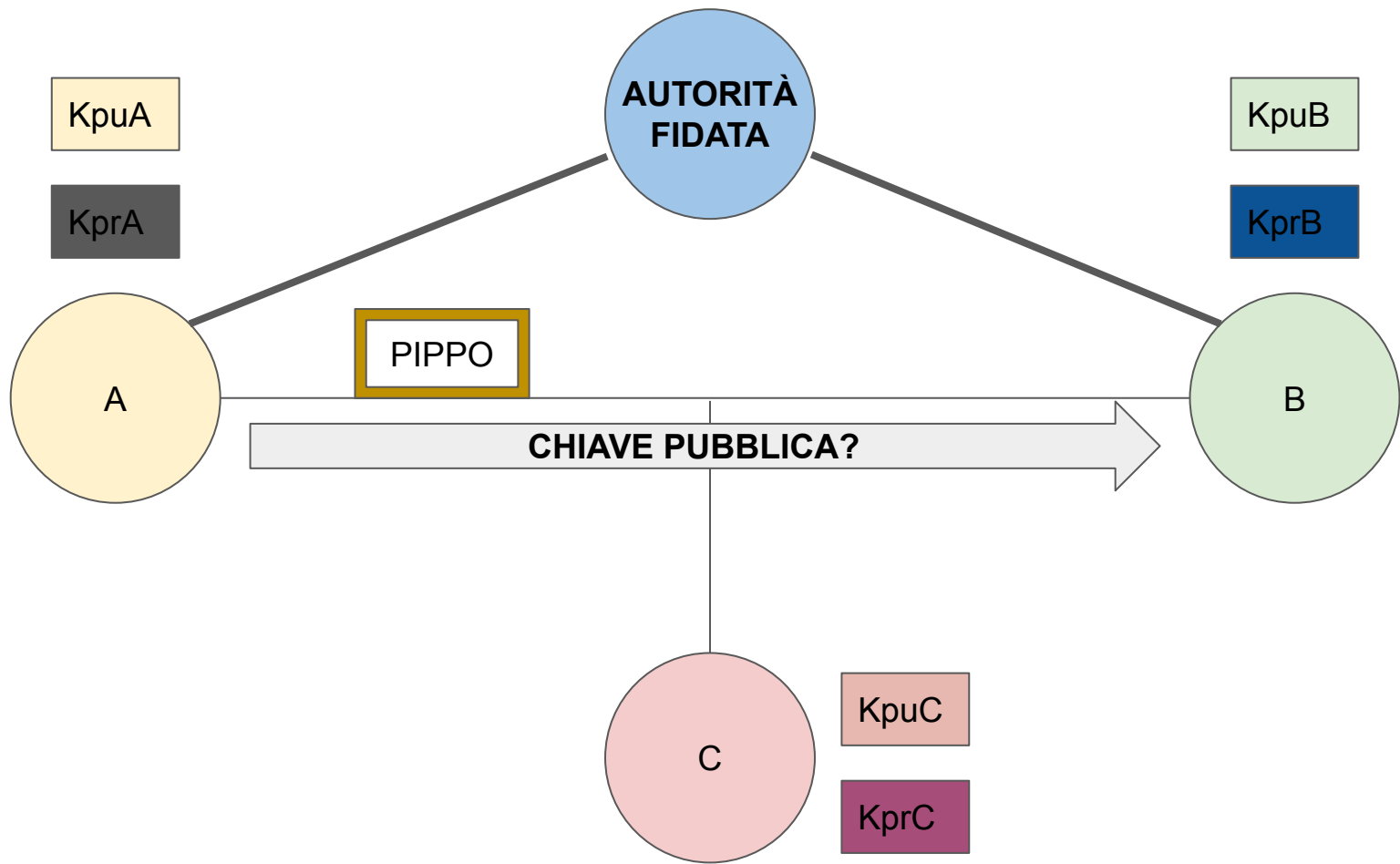


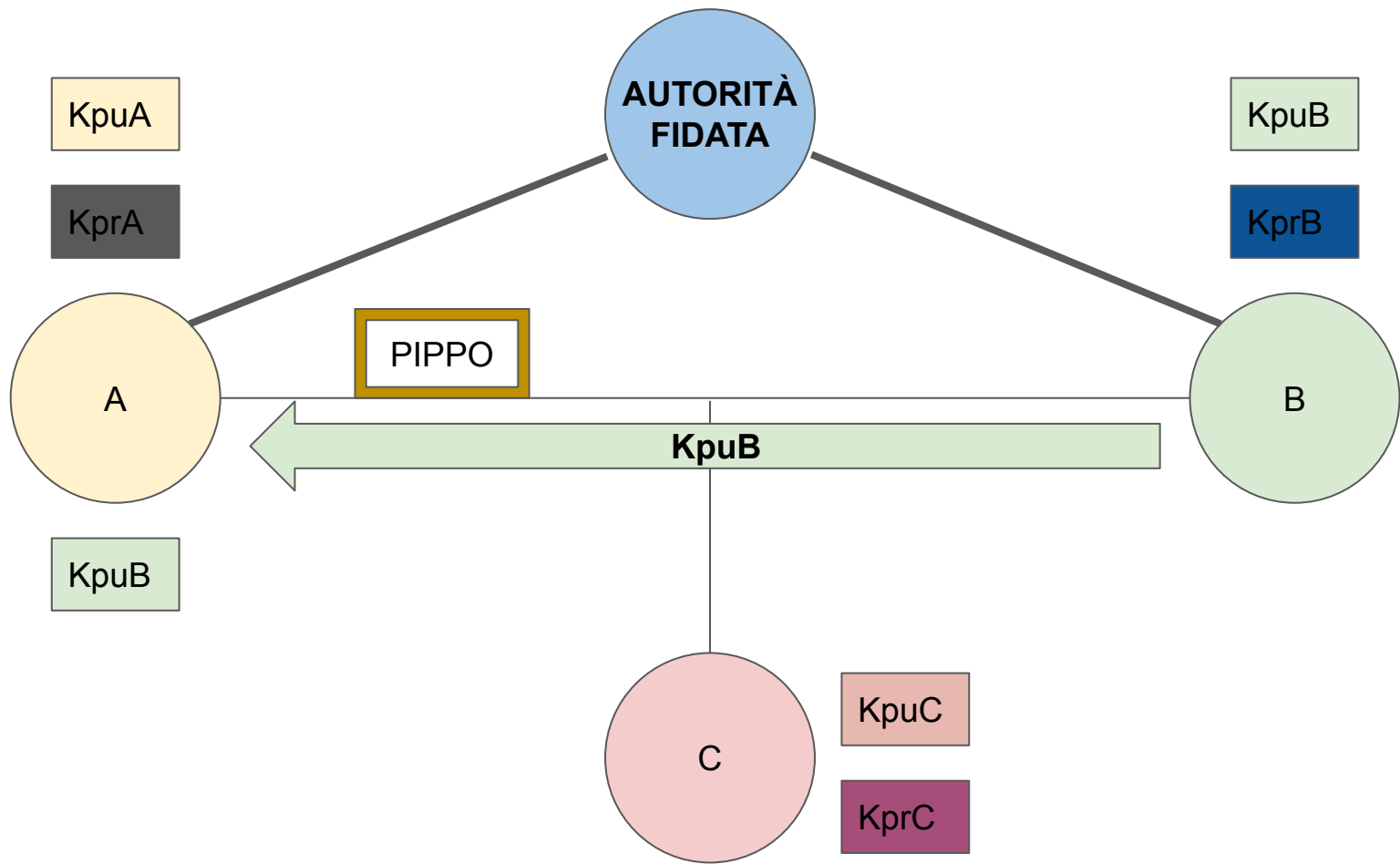


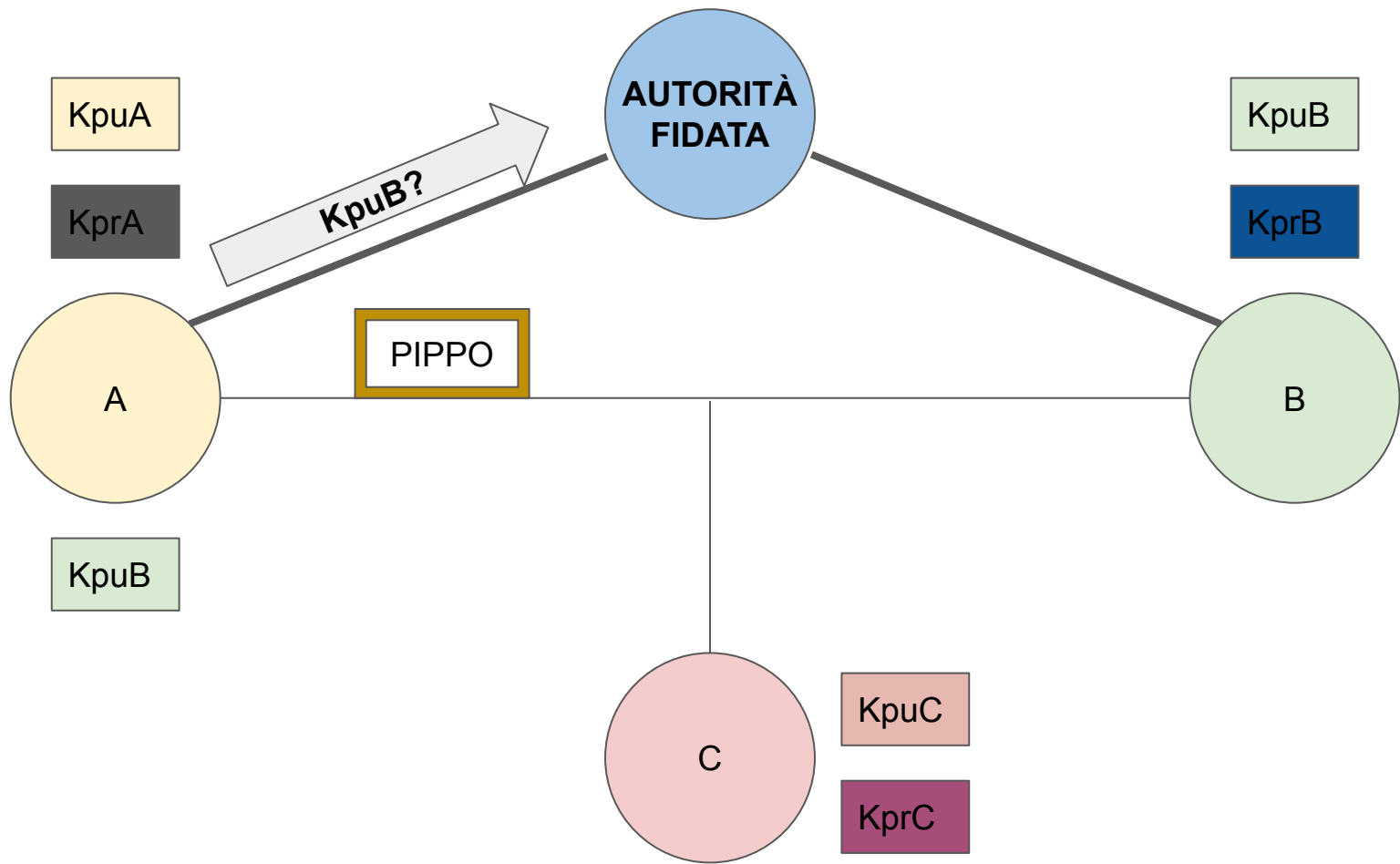
SOLUZIONE

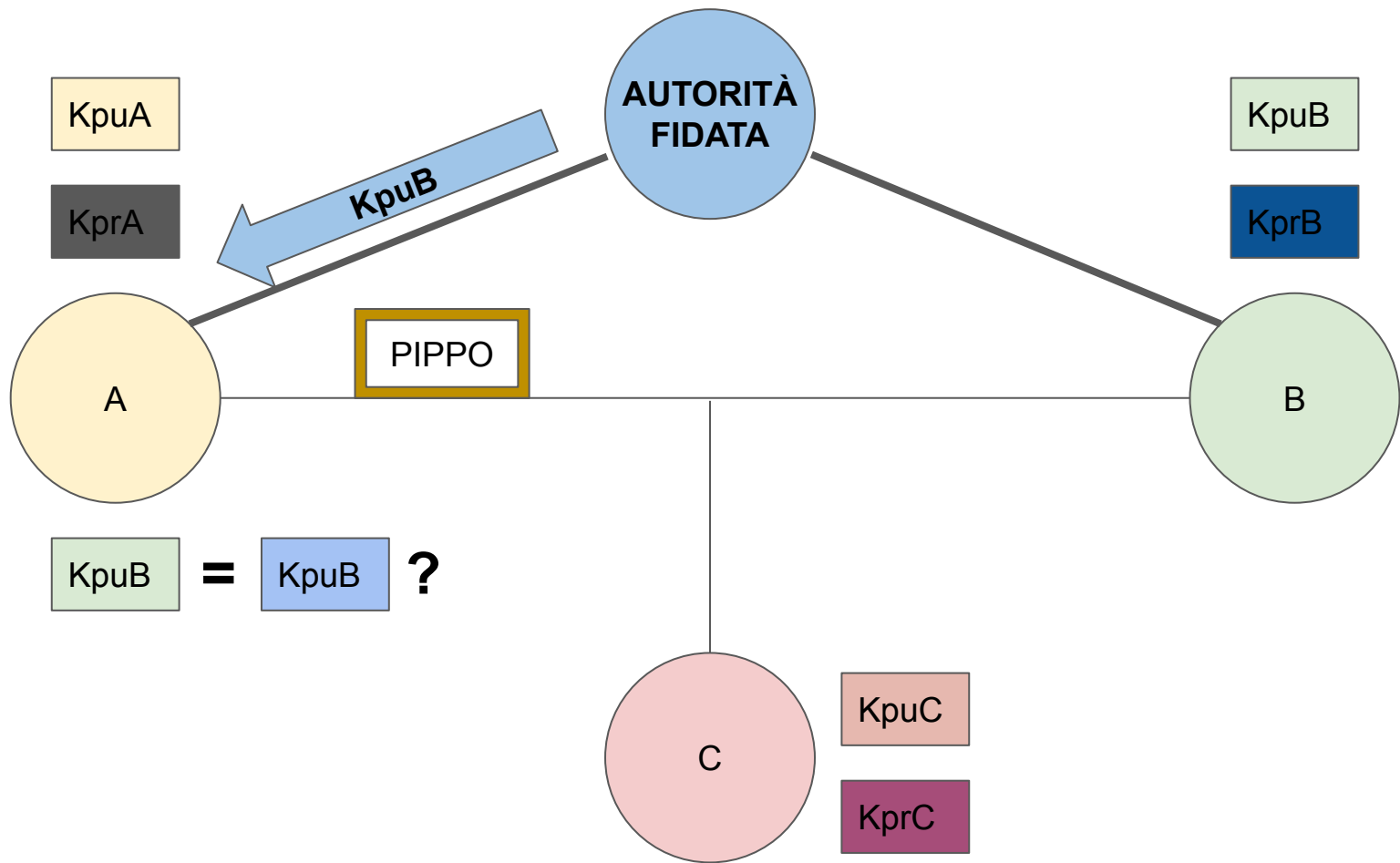
certificato digitale

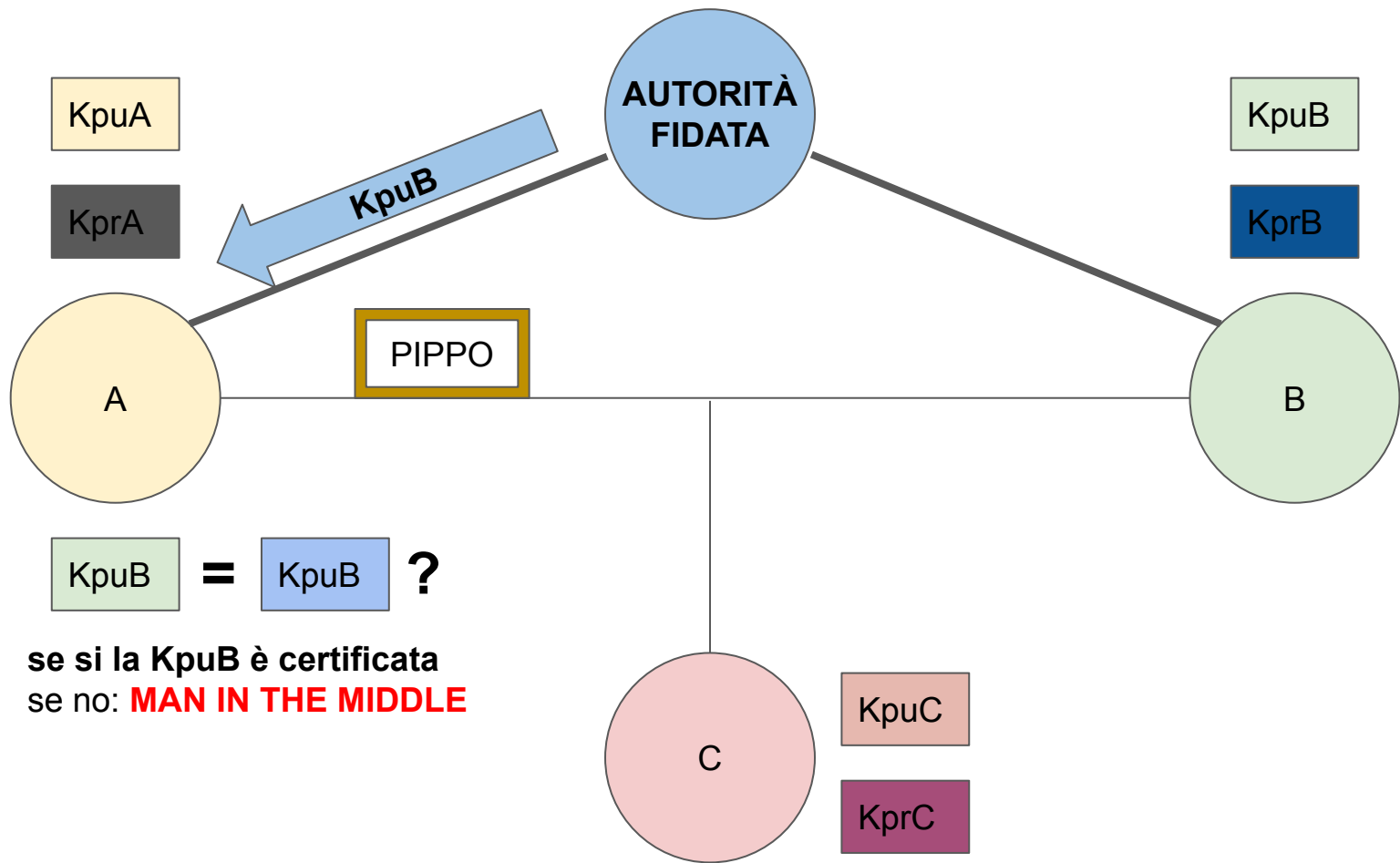




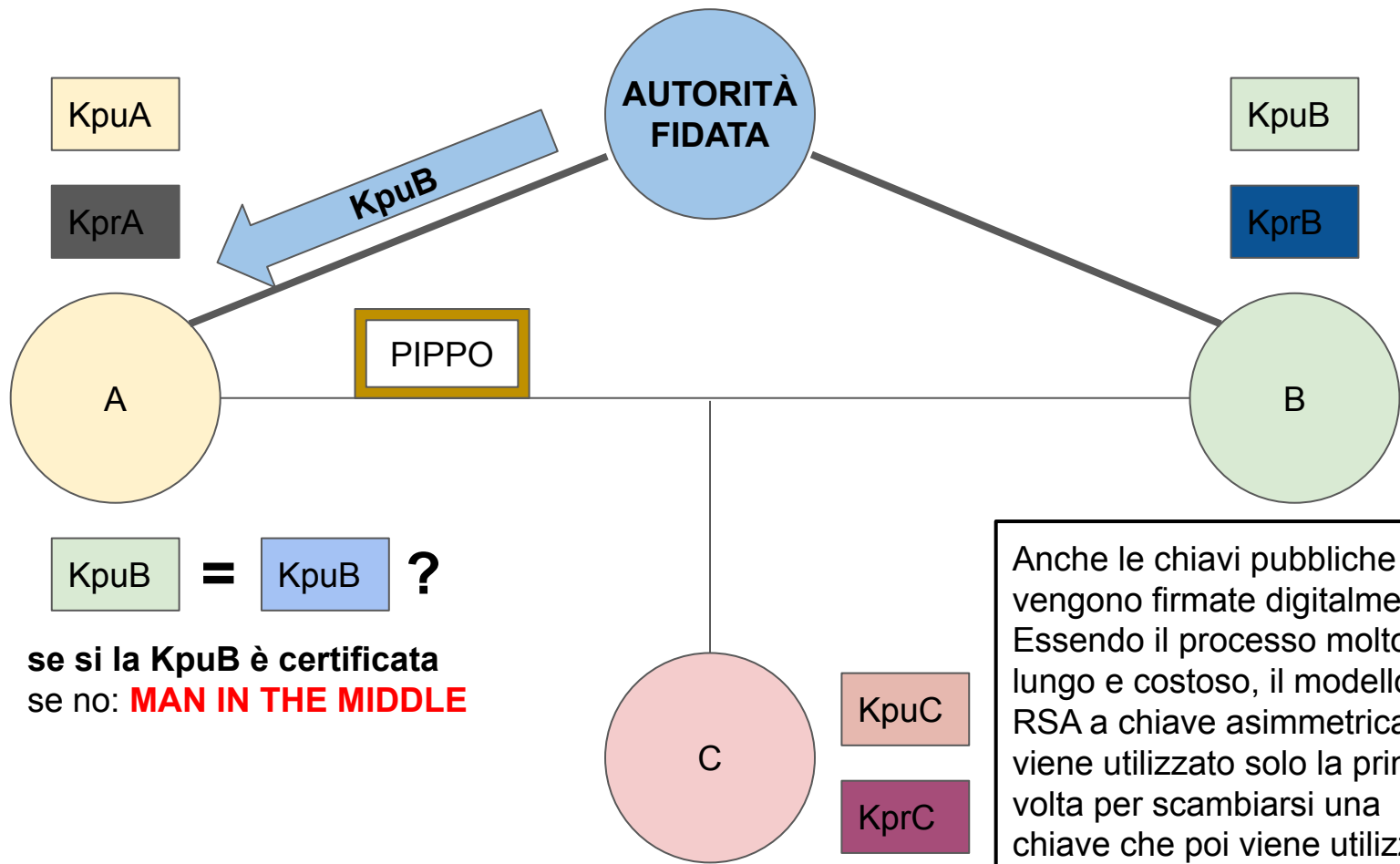








- se sì la **KpuB** è certificata
- se no: **MAN IN THE MIDDLE**



- se si la **KpuB** è certificata
- se no: **MAN IN THE MIDDLE**

Anche le chiavi pubbliche vengono firmate digitalmente. Essendo il processo molto lungo e costoso, il modello RSA a chiave asimmetrica viene utilizzato solo la prima volta per scambiarsi una chiave che poi viene utilizzata in modo simmetrico.