

RequestCall

Alice

Generate random r

$\text{REQUEST_CALL}, \text{alias}_{\text{Bob}}, \text{alias}_{\text{Alice}},$
 $r, K_{\text{SharedKey}}(r), K_{\text{Bob}}(\text{"Alice"})$



Network

Verify a phone with alias
 $\text{alias}_{\text{Alice}}$ is registered to
current LA.

Send a call requests if
phone with alias
 $\text{alias}_{\text{Bob}}$ is found.

WAITING or NOT_FOUND



CONNECTING or TIMEOUT



AcceptCall

Bob

$\text{INCOMING_CALL}, K_{\text{Bob}}(\text{"Alice"}), \text{alias}_{\text{Alice}}, K_{\text{sharedKey}}(r)$



Network

Check if decryption of K_{Bob}
("Alice") is intelligible and
corresponds to a contact
whose current alias is
 $\text{alias}_{\text{Alice}}$.

If answer,
decrypt:

$r' = K_{\text{sharedKey}}^{-1}(K_{\text{sharedKey}}(r))$

$\text{ANSWER_CALL}, r'$



Check if $r' = r$.
Connect call if so,
reject if not