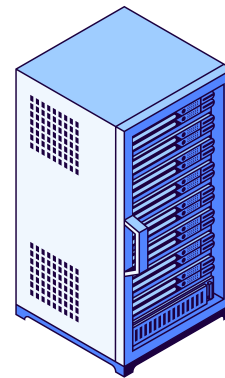


Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



Bob



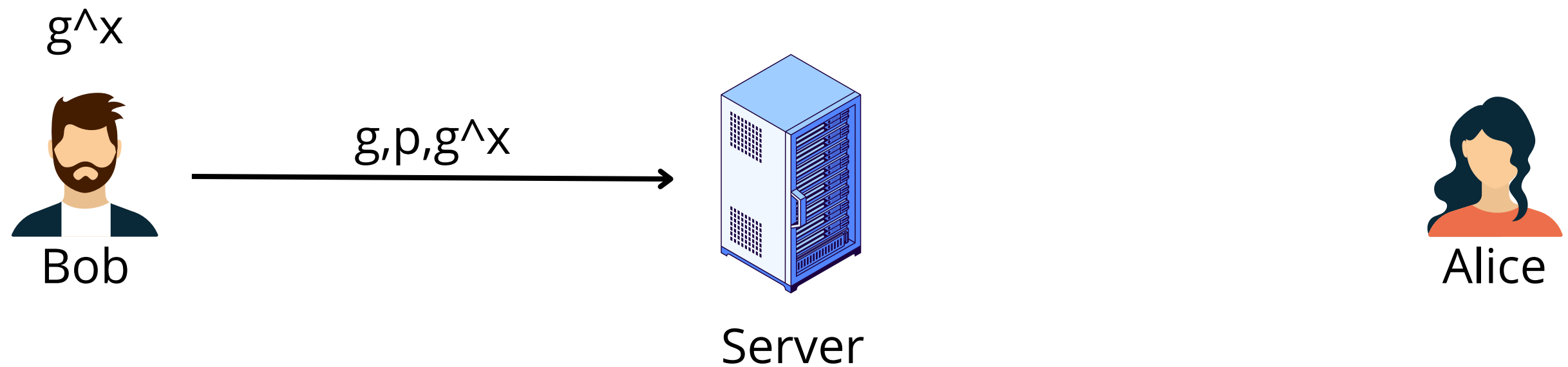
Server



Alice

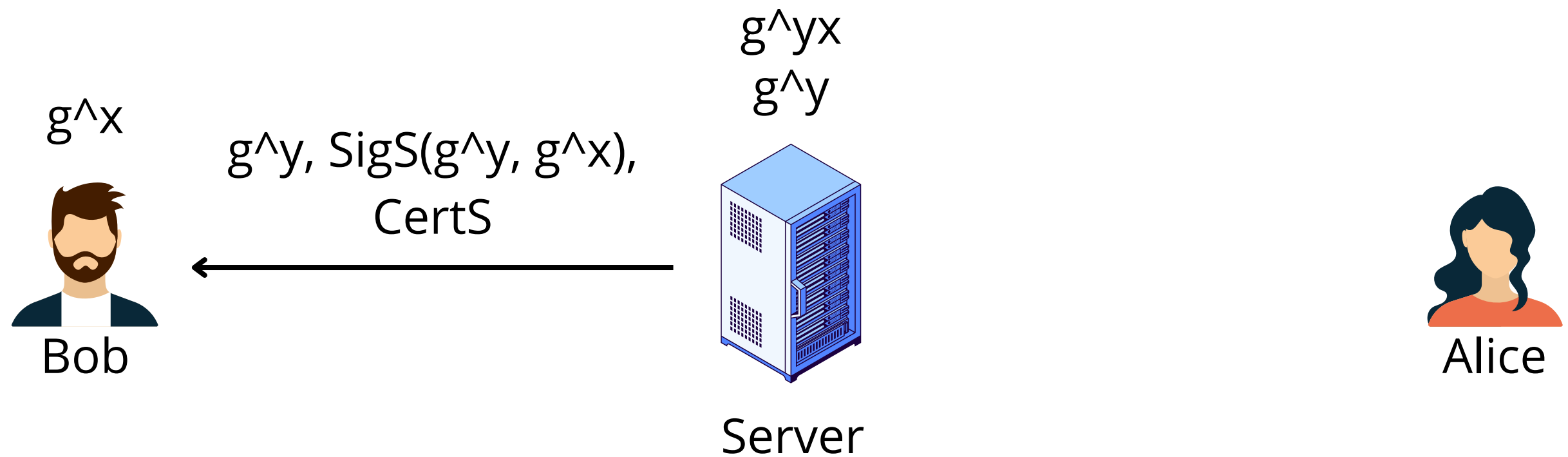
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



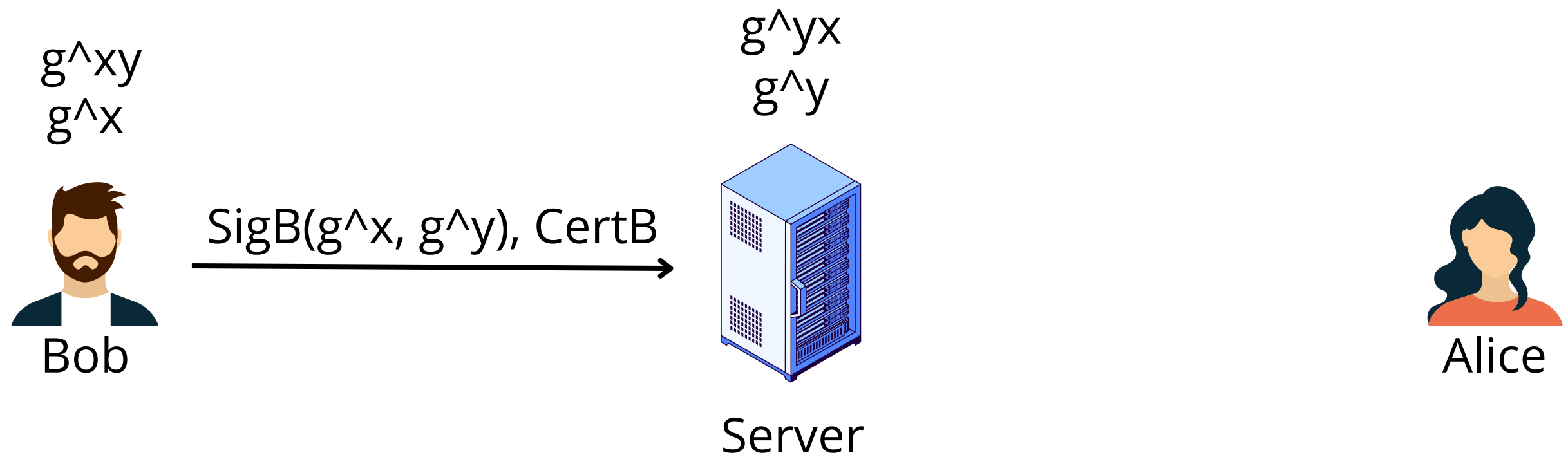
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



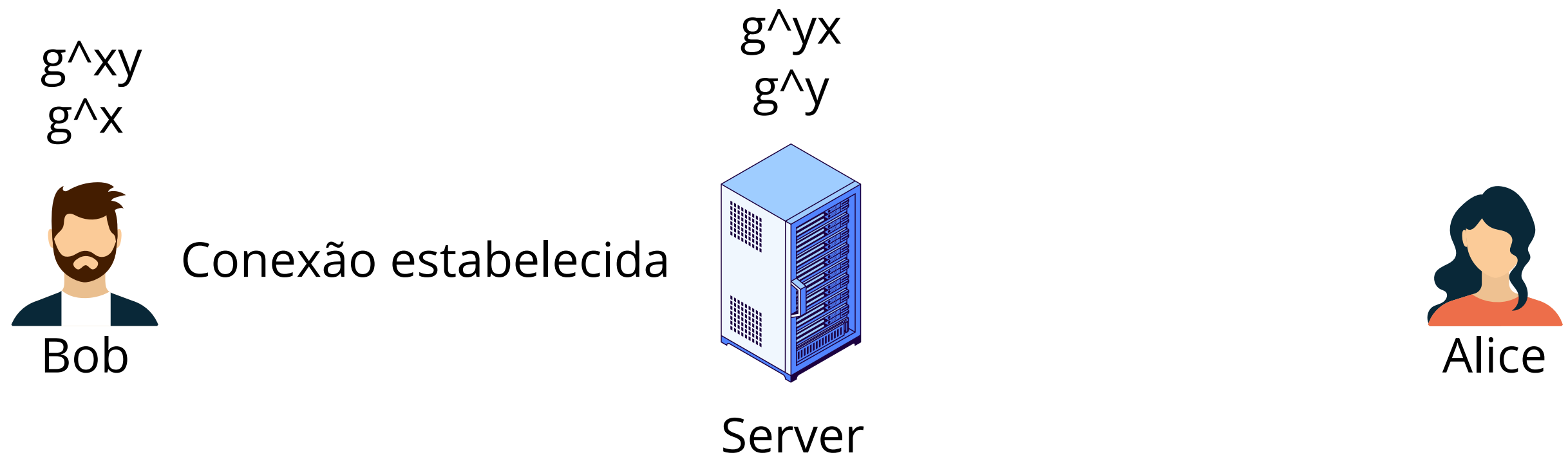
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



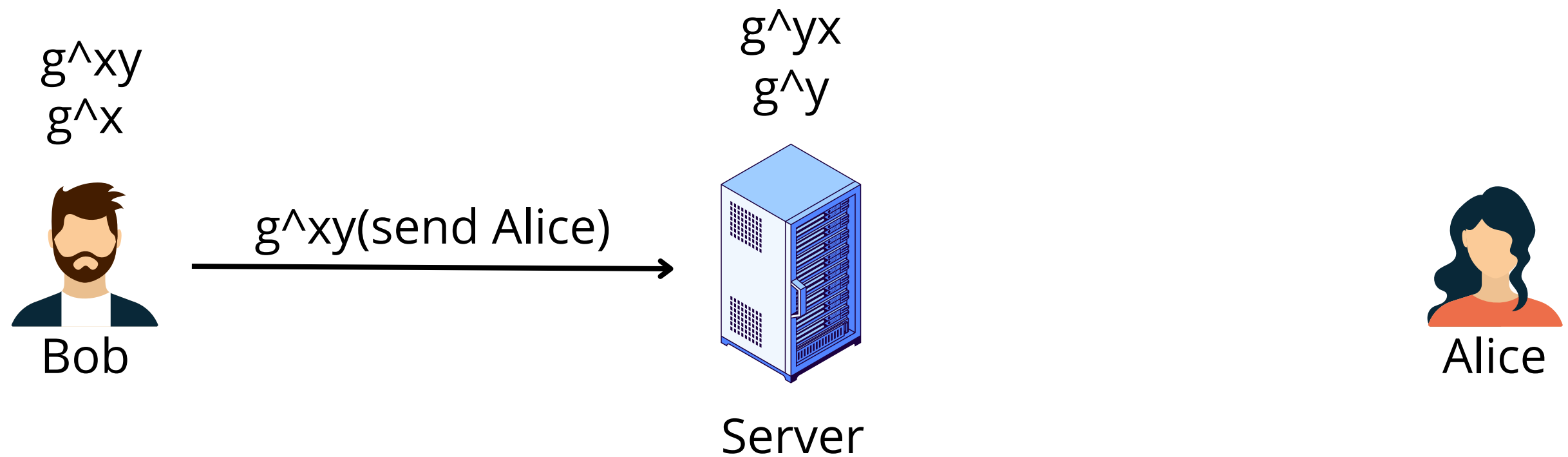
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



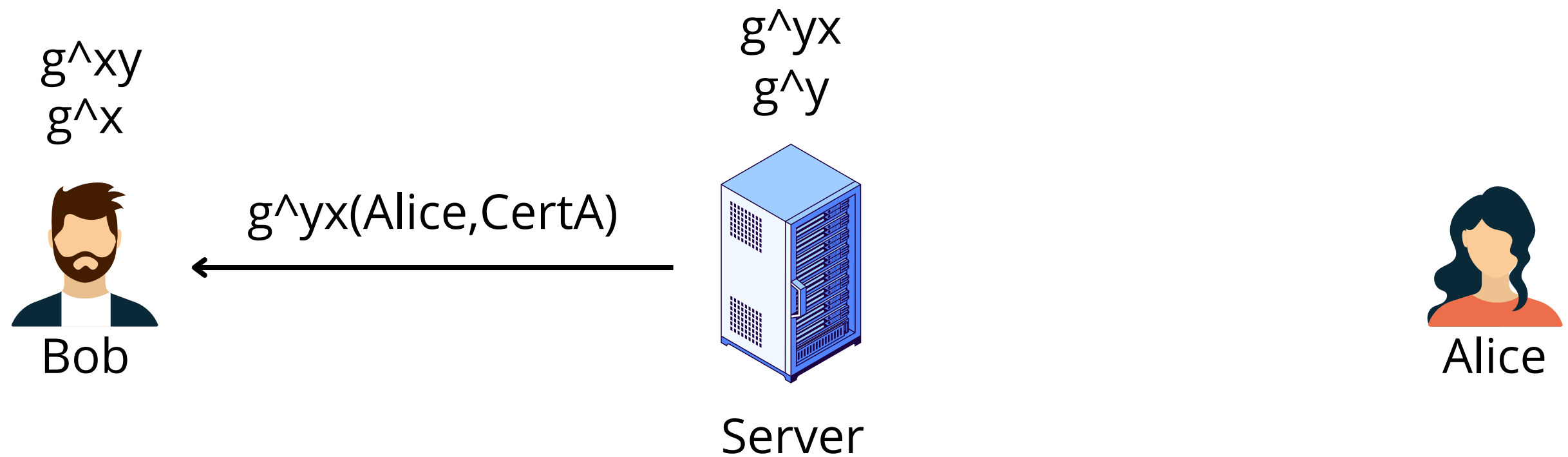
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



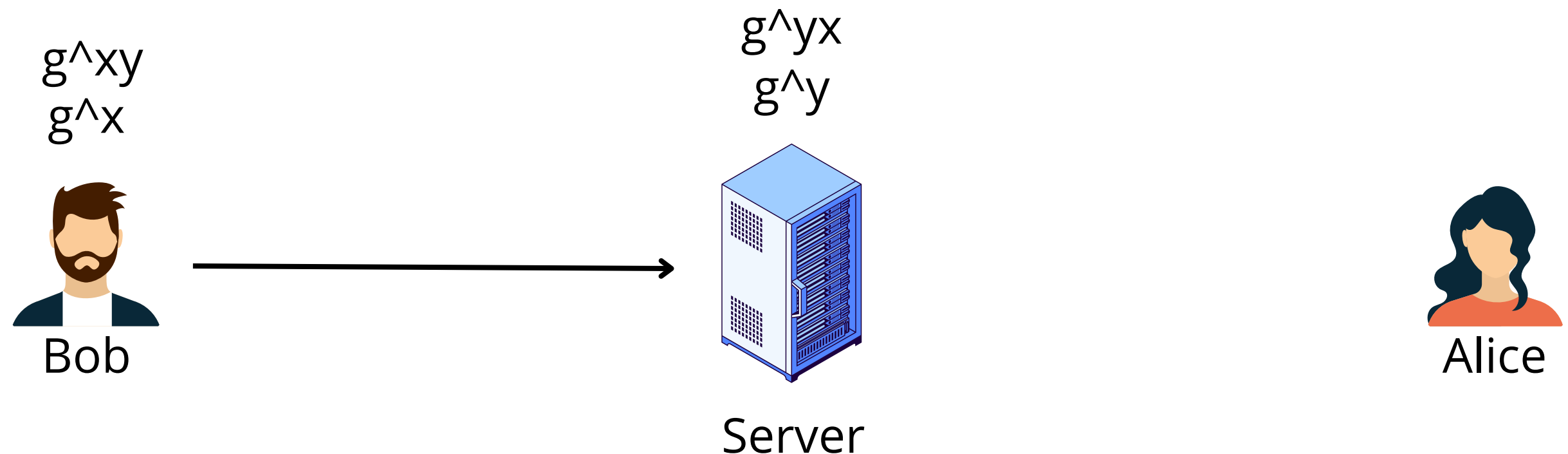
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



$g^{xy}(\text{CifA}(\text{message}), \text{Sig}(\text{CifA}(\text{message})))$
Ciframos a mensagem com o certificado da
Alice

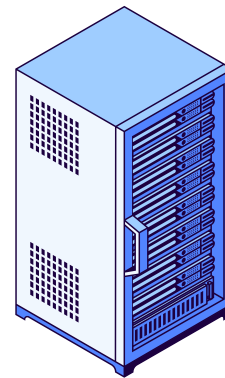
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

$1, \text{CifA}(\text{message}), \text{Sig}(\text{CifA}(\text{message}))$



Bob



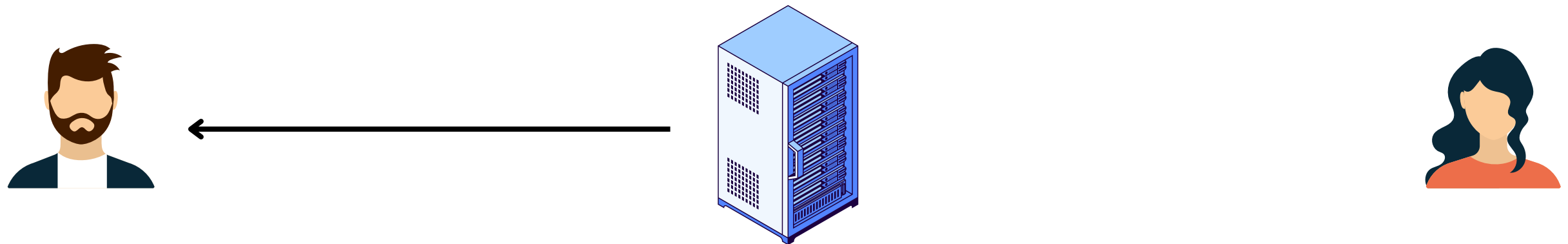
Server



Alice

Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



$g^{yx}(\text{Sucessmessage}, \text{SigS}(\text{Sucessmessage}))$

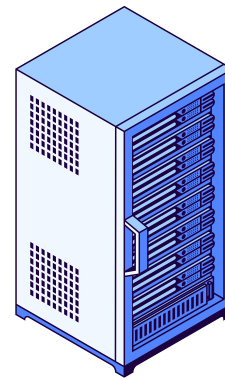
Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

$1, \text{CifA}(\text{message}), \text{Sig}(\text{CifA}(\text{message}))$



Bob



Server



Alice

g^{wz}

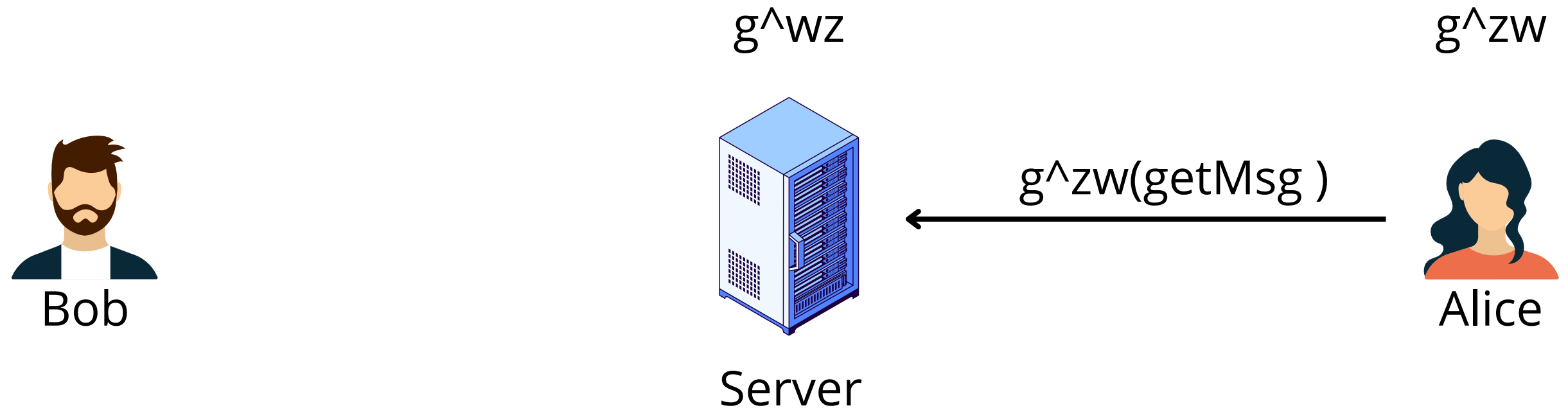
g^{zw}

Alice estabelece a conexão

Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

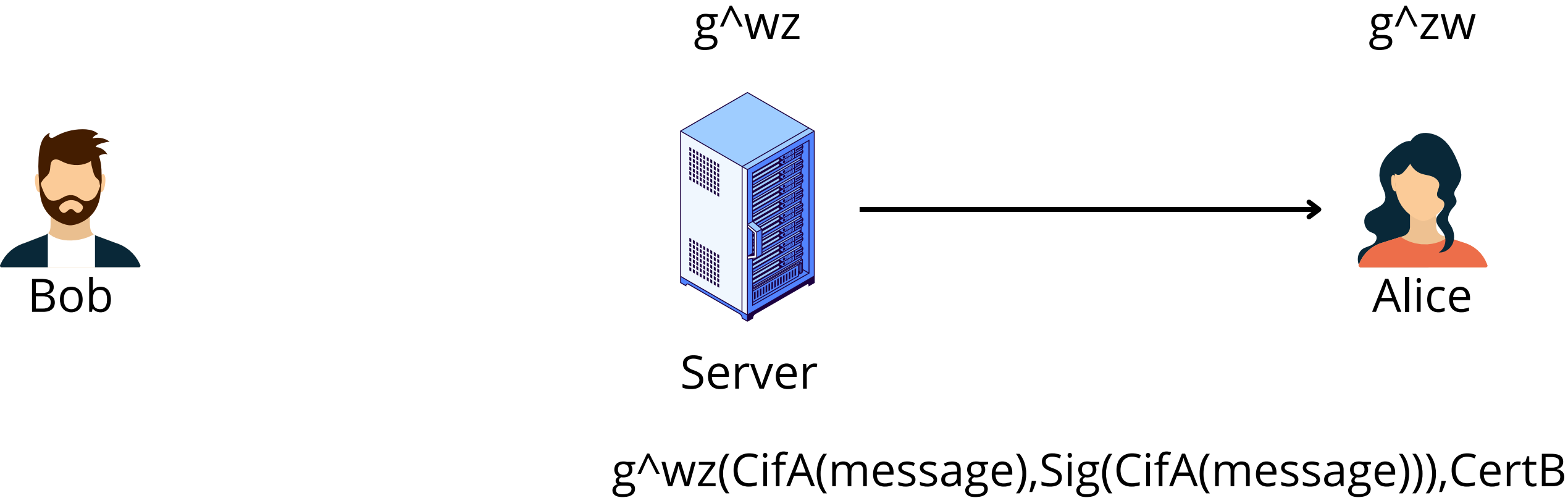
$1, \text{CifA}(\text{message}), \text{Sig}(\text{CifA}(\text{message}))$



Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede

$1, \text{CifA}(\text{message}), \text{Sig}(\text{CifA}(\text{message}))$

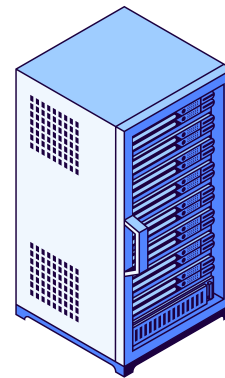


Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



Bob



Server



Alice

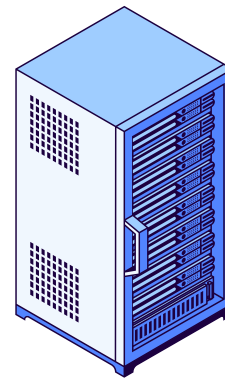
Alice pode verificar a assinatura do Bob, e
pode decifrar a mensagem com a sua chave
privada

Bob envia Mensagem a Alice.

Pressuposto: O servidor conhece os certificados dos membros da rede



Bob



Server



Alice

Assim, o servidor não consegue ler as mensagens do Bob para a Alice