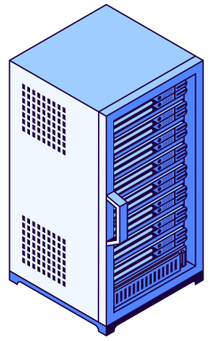
Bob envia Mensagem a Alice.

Bob



Server

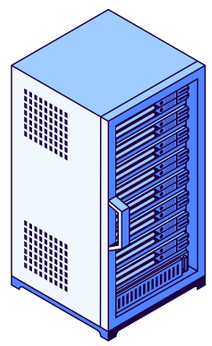
Alice

Bob envia Mensagem a Alice.

g^x

Bob

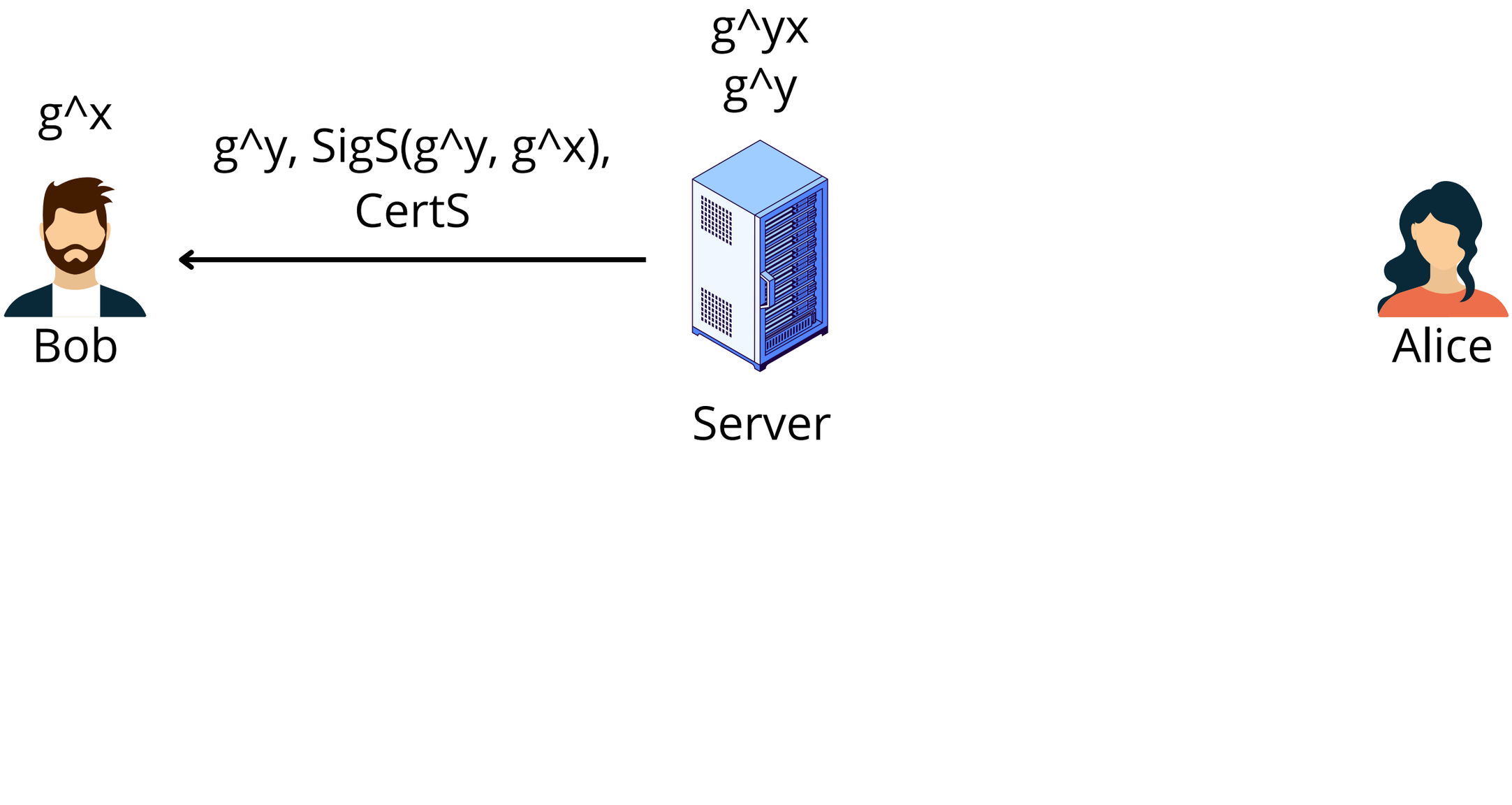
g,p,g^x



Server

Alice

Bob envia Mensagem a Alice.



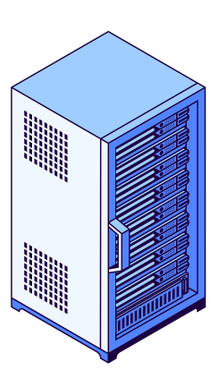
Bob envia Mensagem a Alice.

g^xy
g^x

g^yx
g^y

Bob

SigB(g^x, g^y), CertB



Server

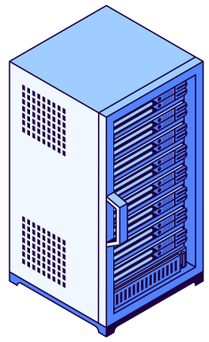
Alice

Bob envia Mensagem a Alice.

g^xy
g^x

g^yx
g^y

Conexão estabelecida



Bob

Server

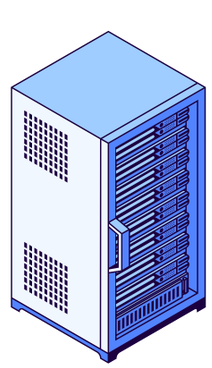
Alice

Bob envia Mensagem a Alice.

g^xy
g^x

g^yx
g^y

Bob



Server

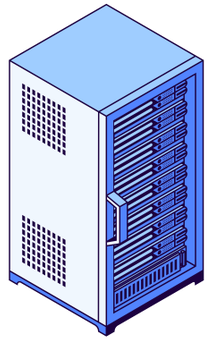
Alice

g^xy(message,sigB(message))

Bob envia Mensagem a Alice.

1,message,sigB(message)

Bob



Server

Alice

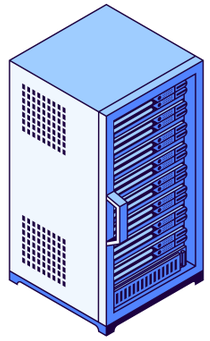
Bob envia Mensagem a Alice.

1,message,sigB(message)

g^wz

g^zw

Bob



Server

Alice

Alice estabelece a conexão

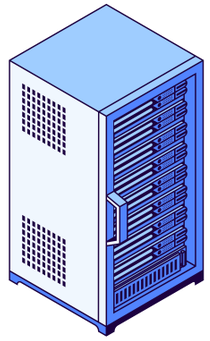
Bob envia Mensagem a Alice.

1,message,sigB(message)

g^wz

g^zw

Bob



Server

g^zw(getMsg)

Alice

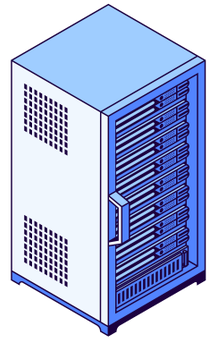
Bob envia Mensagem a Alice.

1,message,sigB(message)

g^wz

g^zw

Bob



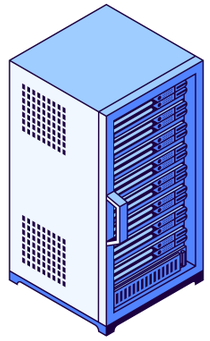
Server

Alice

g^wz(message,sigB(message)),CertB

Bob envia Mensagem a Alice.

Bob



Server

Alice

Alice pode verificar a assinatura do Bob