How to communicate secure?

By encrypting/decrypting messages that have to be transmitted over the internet.
Secure systems nowadays tend to use asymmetric algorithms, where a different key is used to encrypt and decrypt the message: the public and private key.
In cryptography, a certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party.
A digital certificate is a digital document that certifies that a certain public key is owned by a particular user and it has to be signed by a CA.
The signature is actually a digital signature generated with the CA's private key. Therefore, we can verify the integrity of the certificate using the CA's public key.
A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates. The CA does not itself take place in the secure conversation.