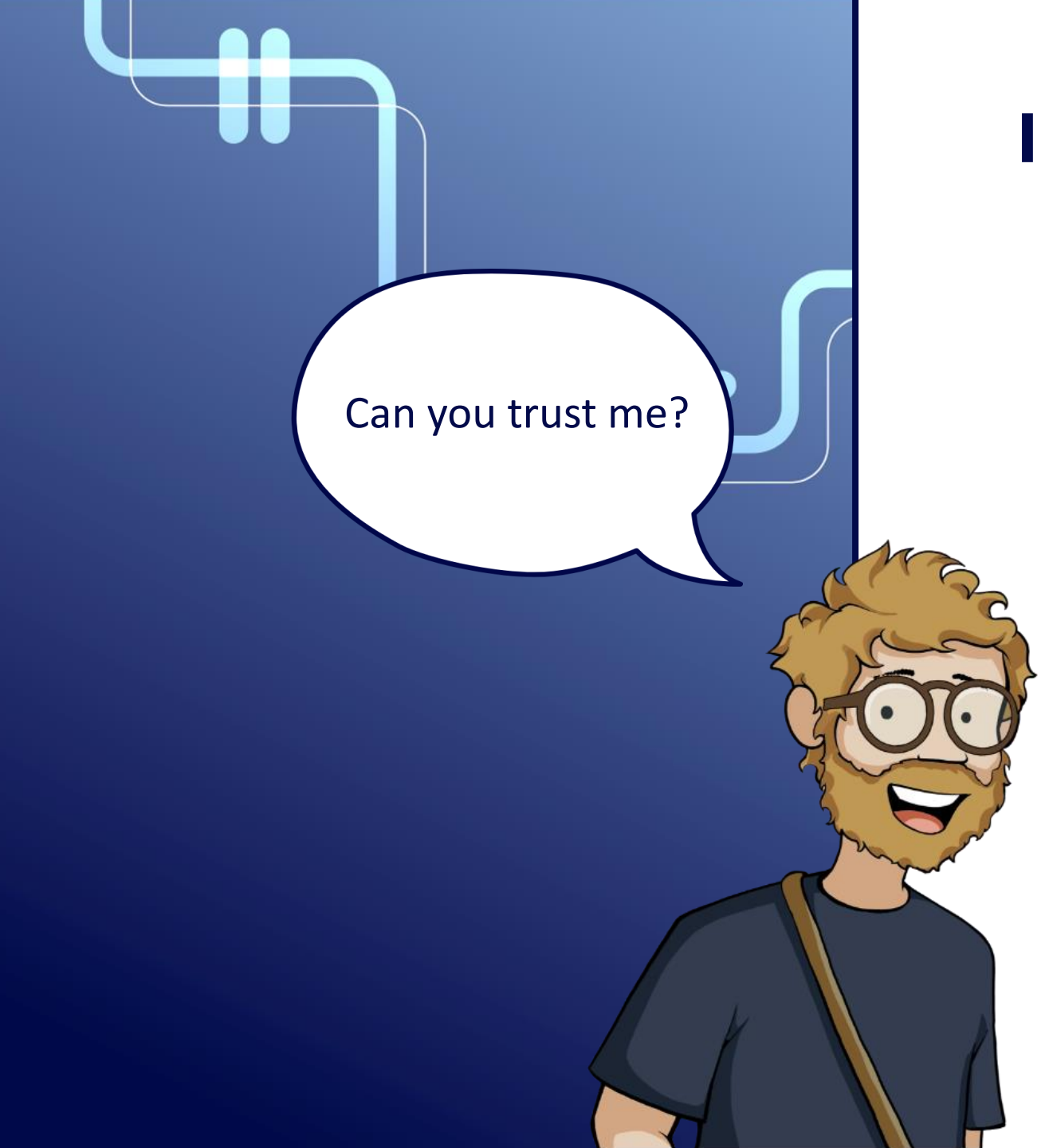
The trust in the digital world

Seb Ferrer

OVHcloud

Introduction



- Make sure you are communicating with the right person

- Ensure that no one else is involved in the exchange

How can you trust a person who's not physically in front of you?

Expected communication

« Hi, I’m Alice! »

« Hey Alice, I’m Bob! »

Alice

Bob

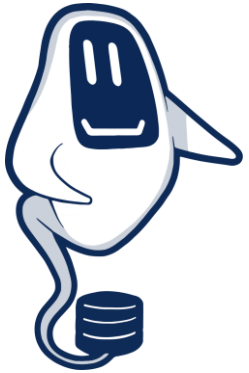
Man-in-the-middle

Alice

Bob

« Hi, I’m Alice! »

« Hey Alice, I’m Bob! »



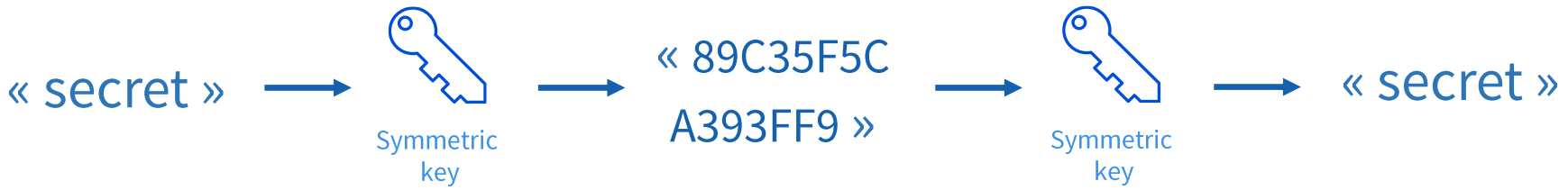
Eve

« Hi, I’m Alice! »

« Hey Alice, I’m Bob! »

End-to-end encryption

Symmetric keys



End-to-end encryption

« Hey Alice, I'm Bob! »

89C35F5CA393FF9392 5C24D9B7070A5AD42

Encrypted message 2

« Hi, I'm Alice! »

0E9490A68F7AD5C11E A794858A4045473491

Encrypted message 1

Symmetric key

« Hi, I'm Alice! »

0E9490A68F7AD5C11E A794858A4045473491

Encrypted message 1

« Hey Alice, I'm Bob! »

89C35F5CA393FF9392 5C24D9B7070A5AD42

Encrypted message 2

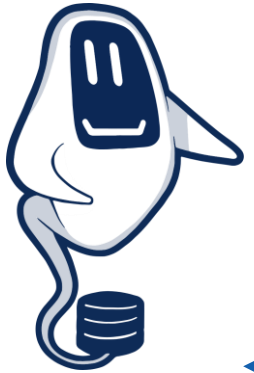
Alice

0E9490A68F7AD5C11E A794858A4045473491

Encrypted message 1

89C35F5CA393FF9392 5C24D9B7070A5AD42

Encrypted message 2



Eve

0E9490A68F7AD5C11E A794858A4045473491

Encrypted message 1

89C35F5CA393FF9392 5C24D9B7070A5AD42

Encrypted message 2

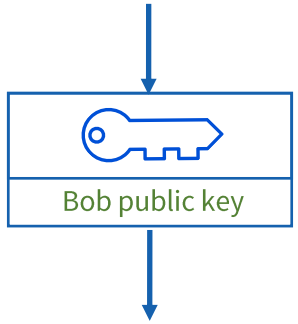
Bob

End-to-end encryption

Asymmetric key pairs

Trust : Asymmetric key pairs

« Here's my secret »



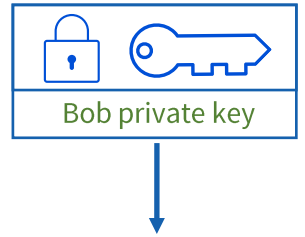
« 0E9490A68
F7AD5C11E
A794858A4
045473491 »

Alice

« 0E9490A68
F7AD5C11E
A794858A4
045473491 »

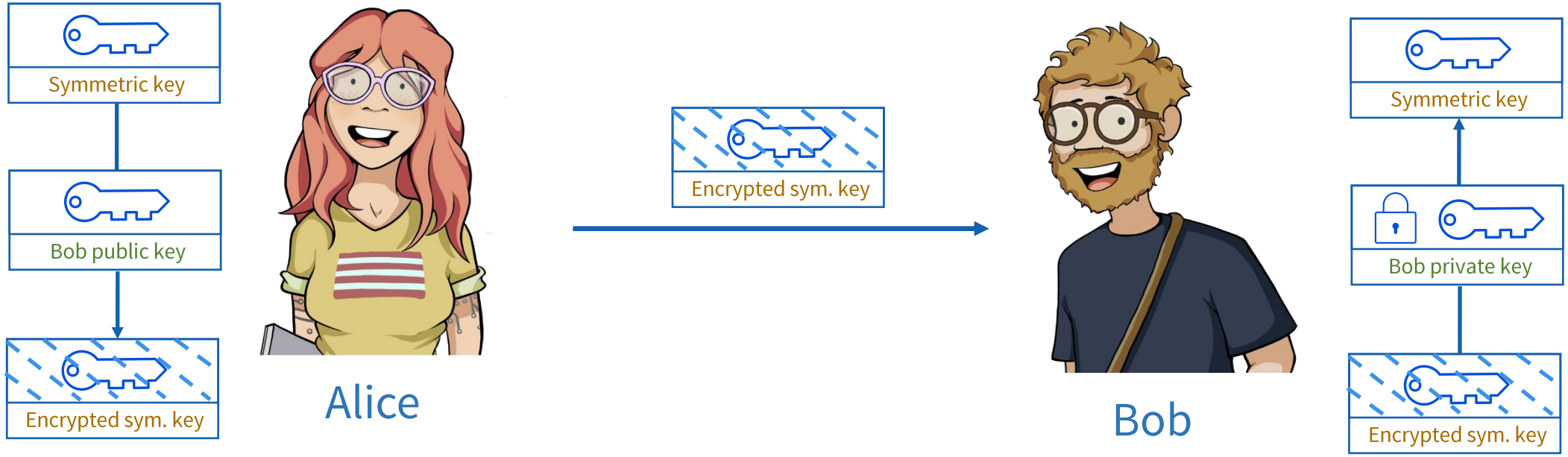
Bob

« 0E9490A68
F7AD5C11E
A794858A4
045473491 »

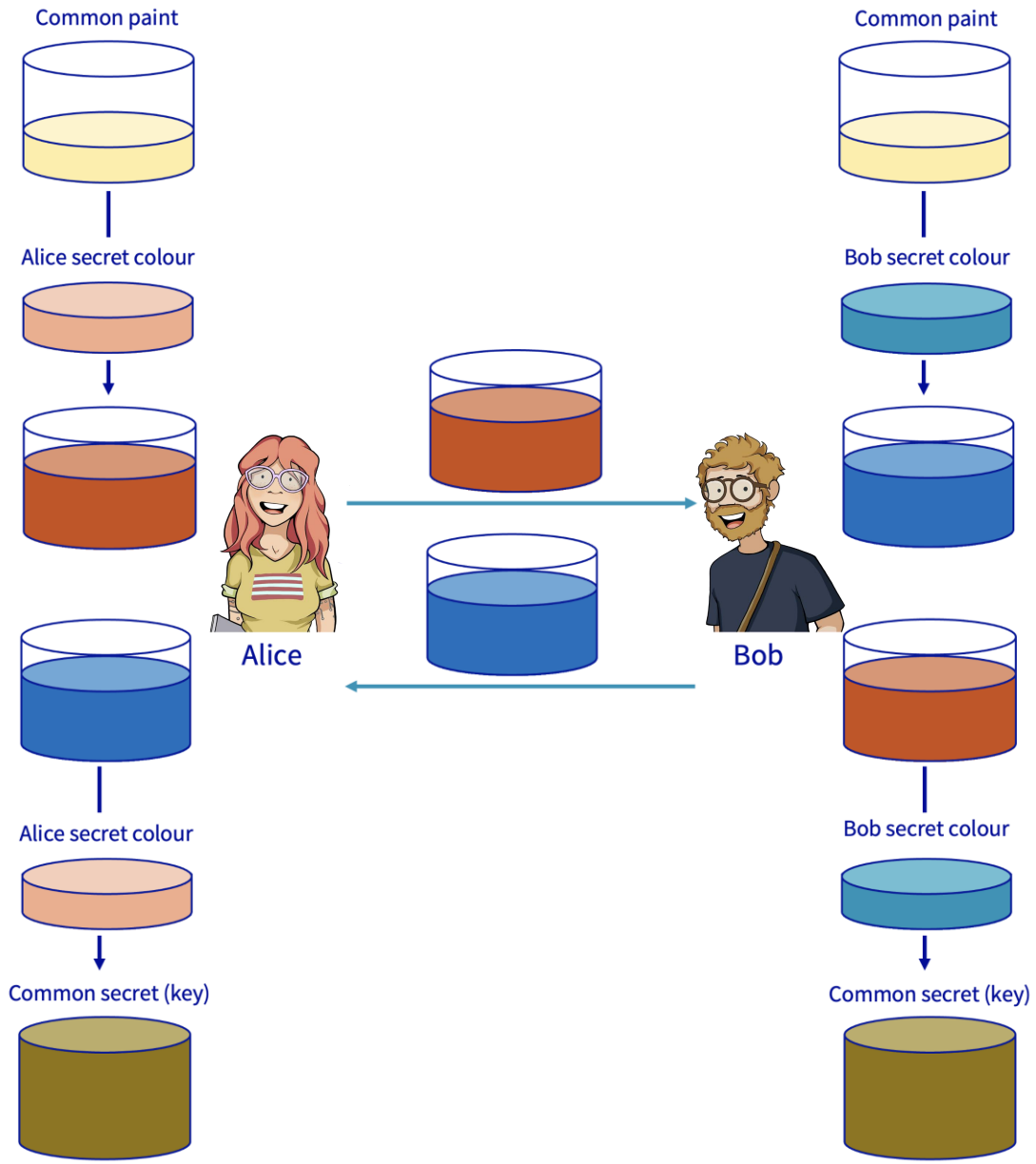


« Here's my secret »

Trust : Asymmetric key pairs



Trust : Diffie-Hellman exchange



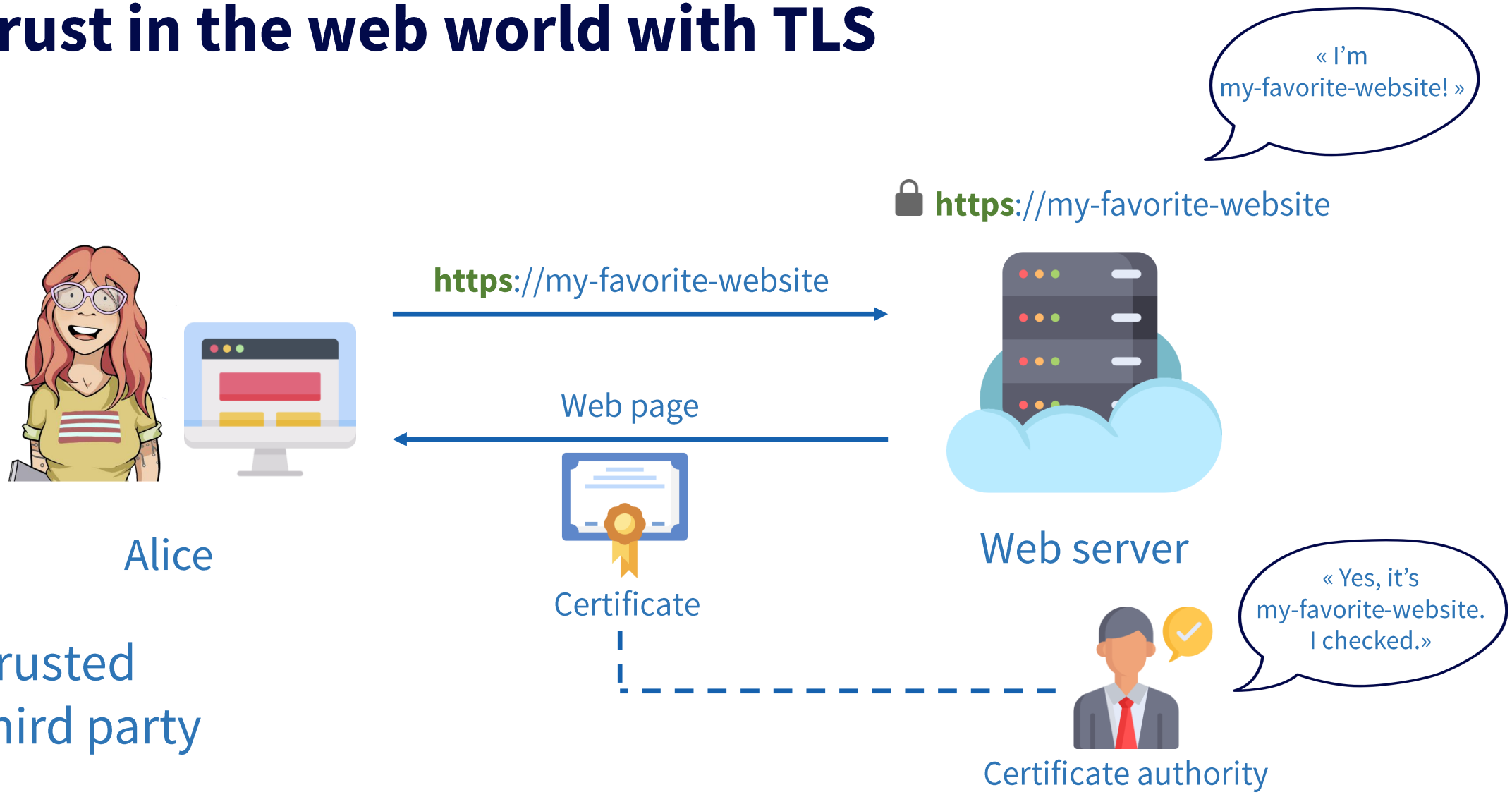
Trust in the web world with TLS

HTTPS

HyperText Transfer Protocol Secure

Trust in the web world with TLS

Trust in the web world with TLS



Trust in the web world with TLS

Certificate

- Authenticity
- Encryption
- Integrity

Let's Encrypt

digicert®

COMODO

Trust in the web world with TLS

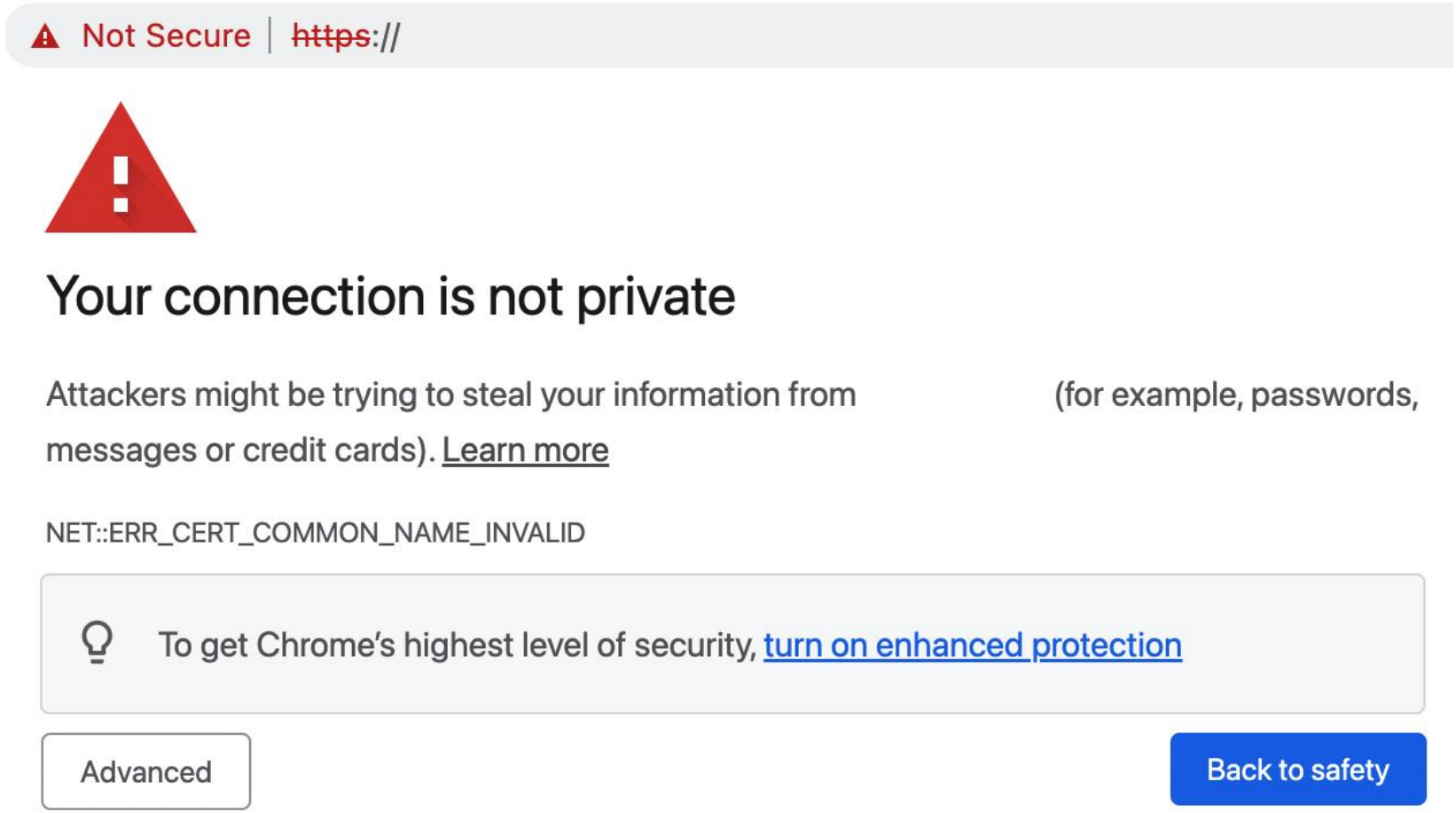
- Domain Common Name
- CA Signature
- CA Public Key

End-entity Certificate

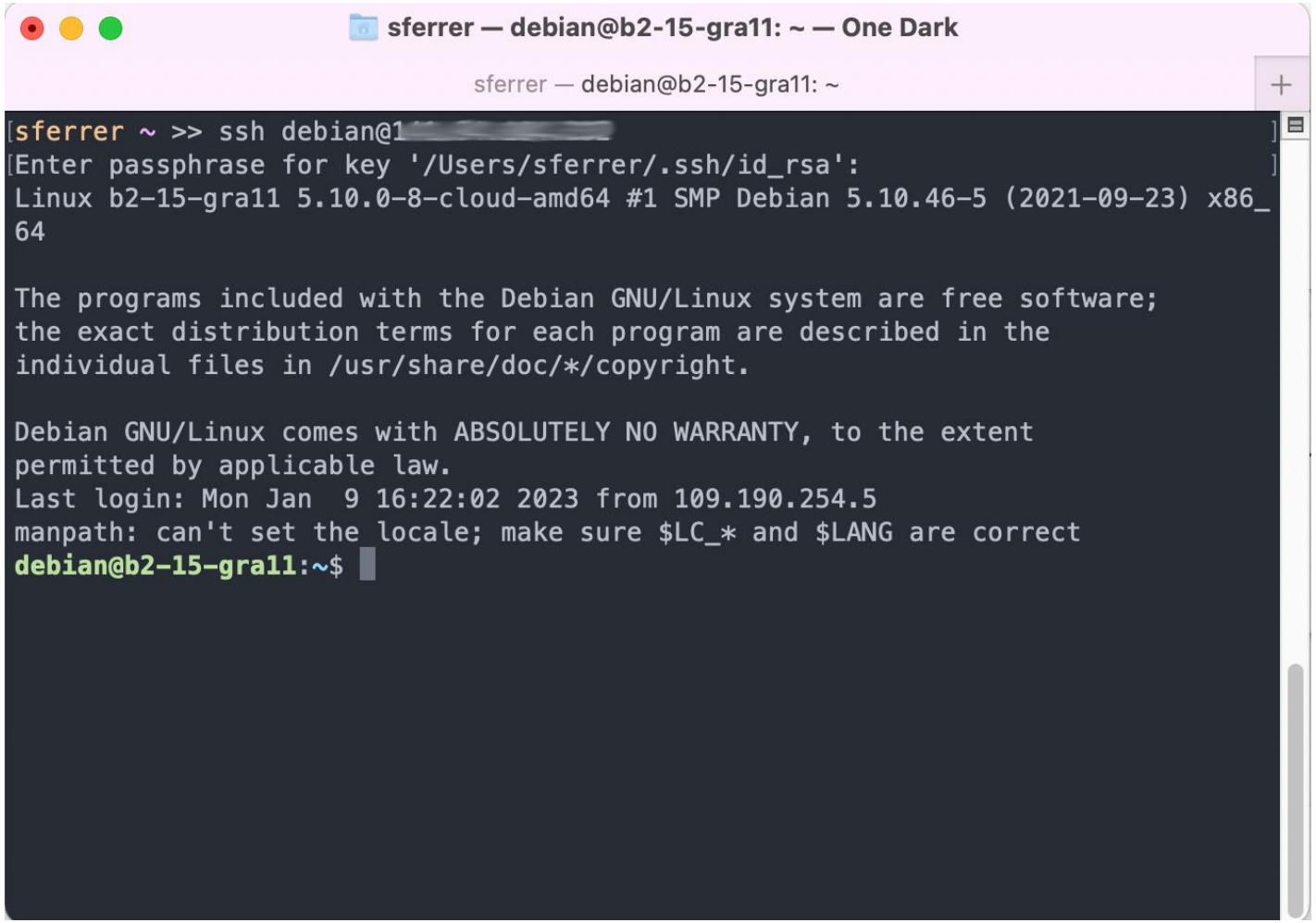
Intermediate CA Certificate

Root CA Certificate

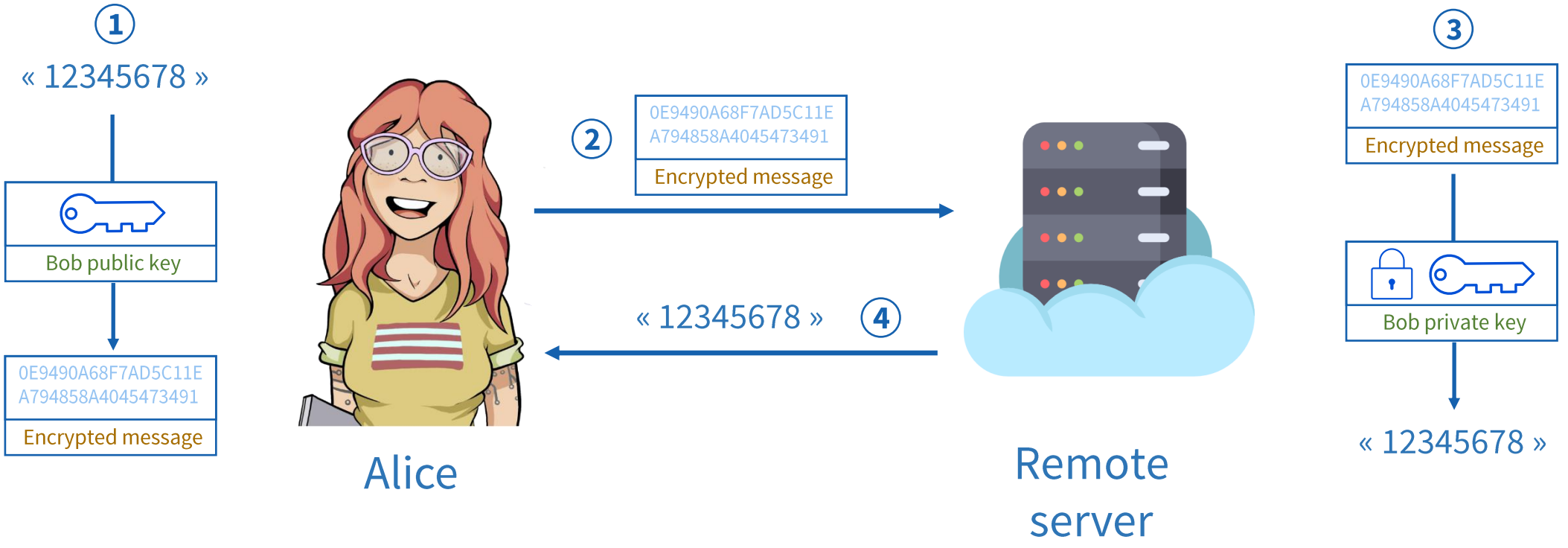
Trust in the web world with TLS



Trust with SSH



Trust with SSH



References

Encryption:

- https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/
- https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

TLS:

- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811(v=ws.10)
- https://en.wikipedia.org/wiki/Transport_Layer_Security
- https://letsencrypt.org/documents/isrg-cp-v3.1/
- https://www.keyfactor.com/blog/certificate-chain-of-trust/
- https://en.wikipedia.org/wiki/OCSP_stapling
- https://en.wikipedia.org/wiki/X.509#Certificate_chains_and_cross-certification
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
- https://security.stackexchange.com/questions/119364/how-can-i-detect-https-inspection
- https://learn.microsoft.com/en-us/windows-hardware/drivers/install/certificate-stores

SSH:

- https://www.digitalocean.com/community/tutorials/ssh-essentials-working-with-ssh-servers-clients-and-keys
- https://security.stackexchange.com/questions/182804/how-does-ssh-know-which-public-key-to-use-from-authorized-keys
- https://www.rfc-editor.org/rfc/rfc4252.html
- https://en.wikipedia.org/wiki/Secure_Shell
- https://docs.microsoft.com/en-us/azure/devops/repos/git/use-ssh-keys-to-authenticate?view=azure-devops

Kimi, my cat

sebferrer

seb-ferrer

https://blog.kimi.ovh

A more detailed blog post about federated identities here

OVHcloud