# Kubernetes Security

USWAY©

REINVENT YOURSELF

Students, write your response!

Pear Deck Interactive Slide

Do not remove this bar

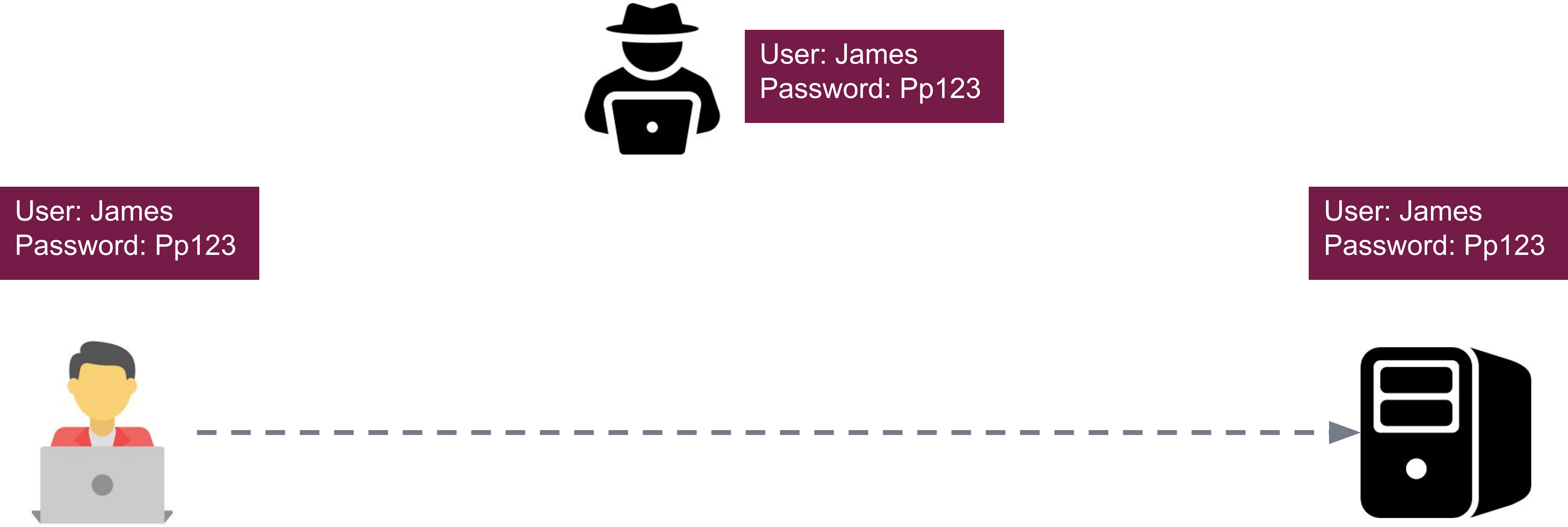
# Table of Contents

- SYMMETRIC ENCRYPTION
- ASYMMETRIC ENCRYPTION
- TLS/SSL CERTIFICATE

1

# SYMMETRIC ENCRYPTION

# SYMMETRIC ENCRYPTION



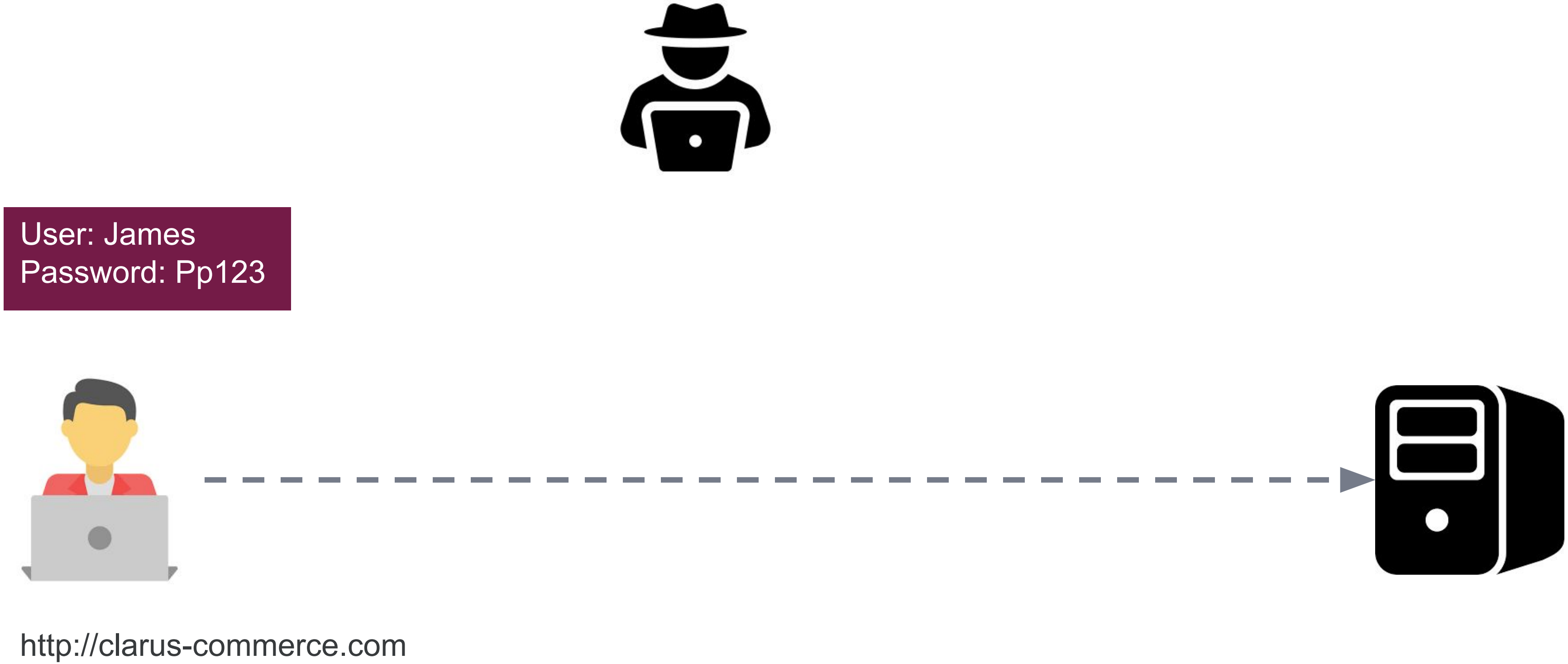
User: James
Password: Pp123

User: James
Password: Pp123

User: James
Password: Pp123

http://clarus-commerce.com

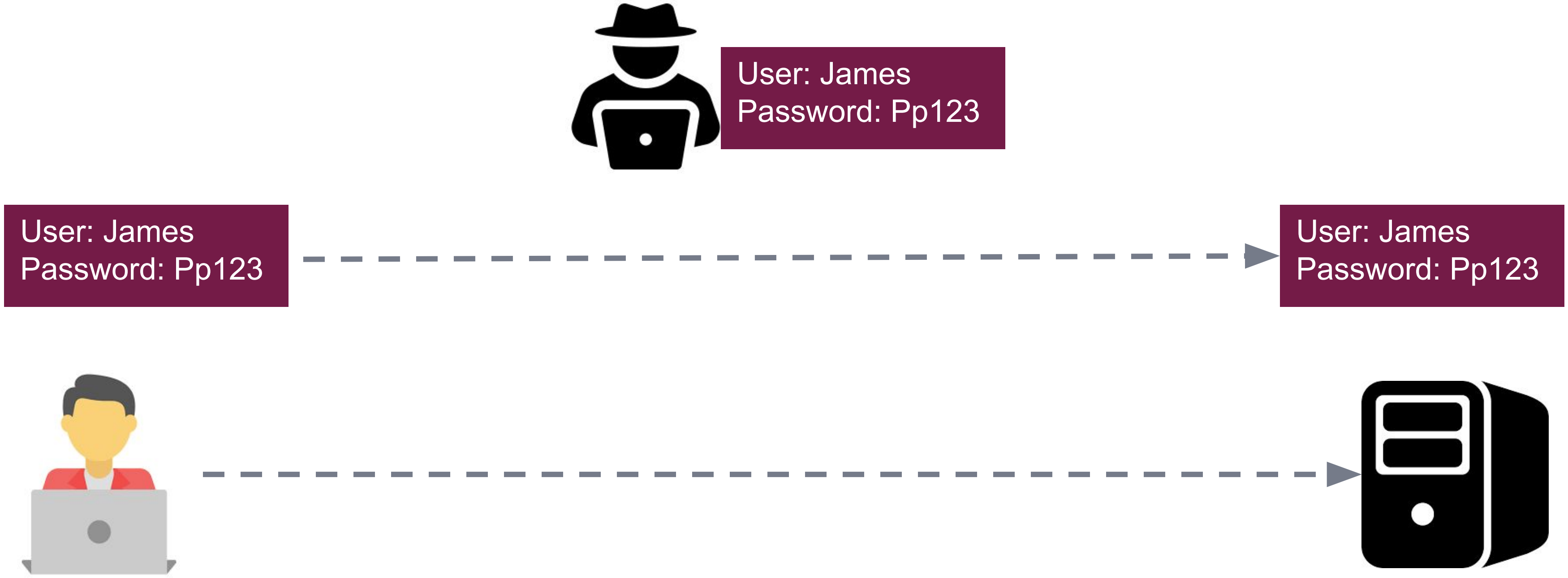
# SYMMETRIC ENCRYPTION



User: James
Password: Pp123

http://clarus-commerce.com

# SYMMETRIC ENCRYPTION



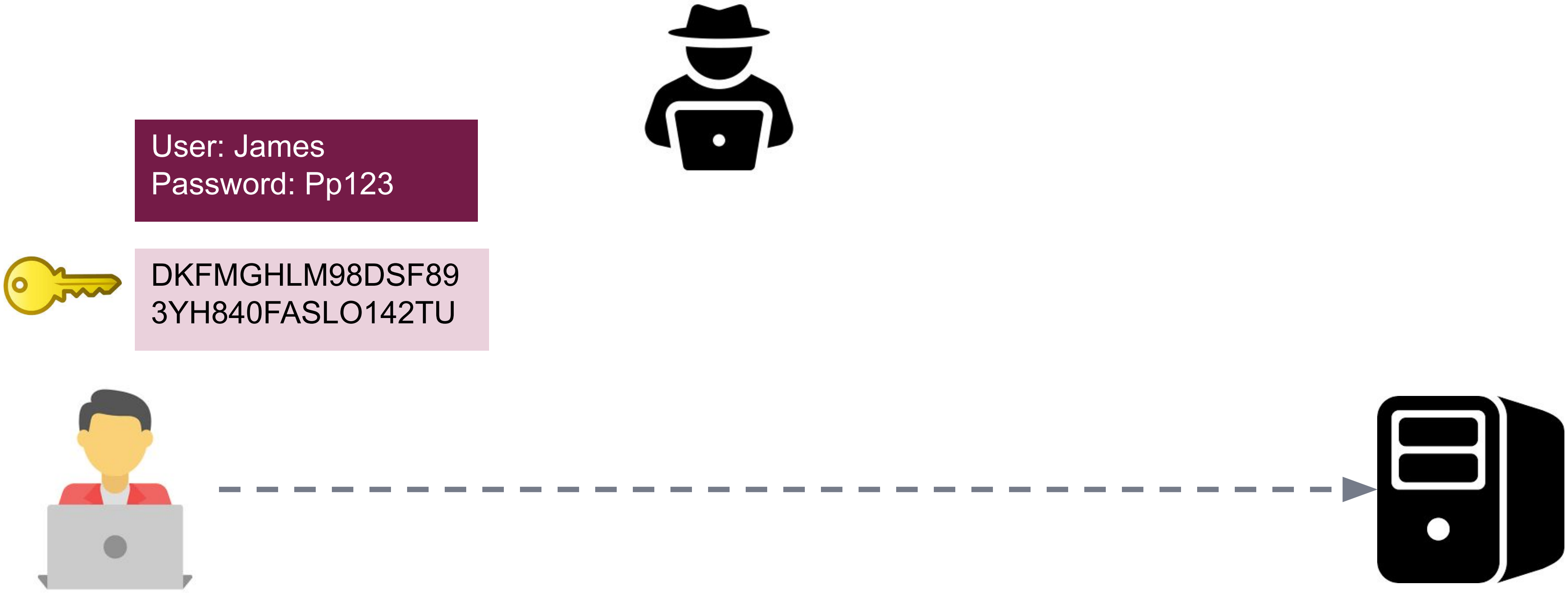
User: James
Password: Pp123

User: James
Password: Pp123

User: James
Password: Pp123

http://clarus-commerce.com

# SYMMETRIC ENCRYPTION

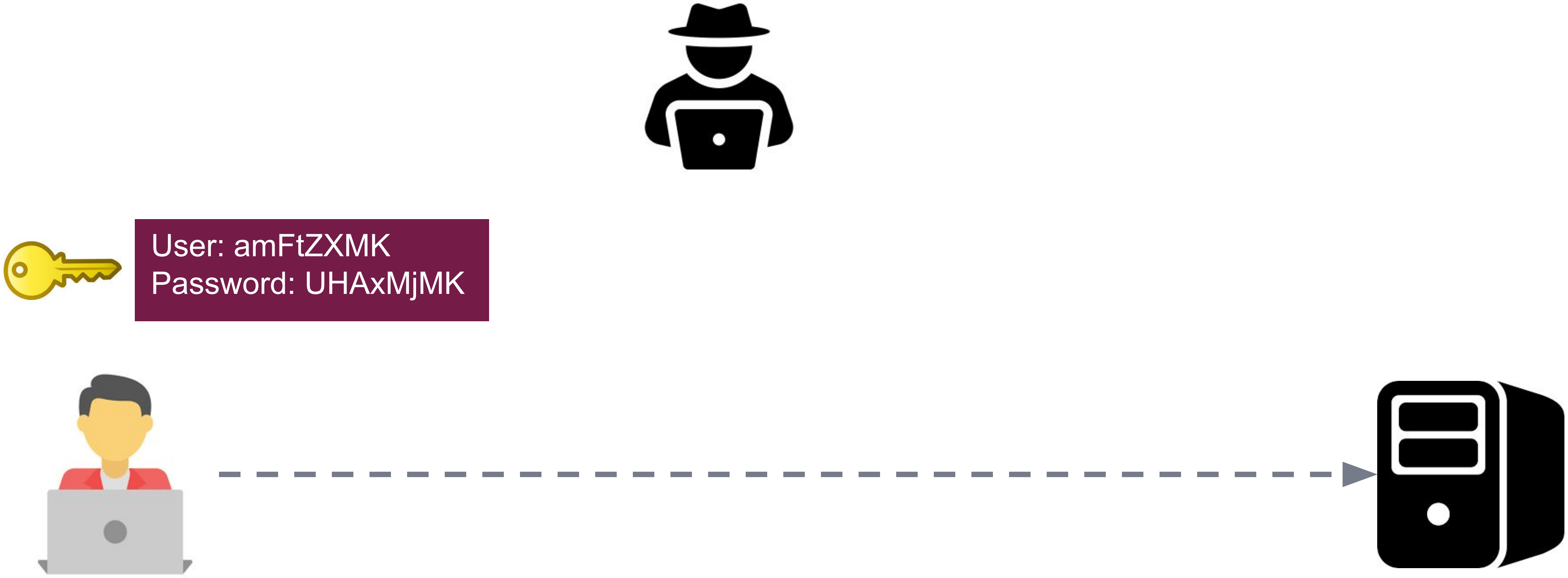


User: James
Password: Pp123

DKFMGHLM98DSF89
3YH840FASLO142TU

http://clarus-commerce.com

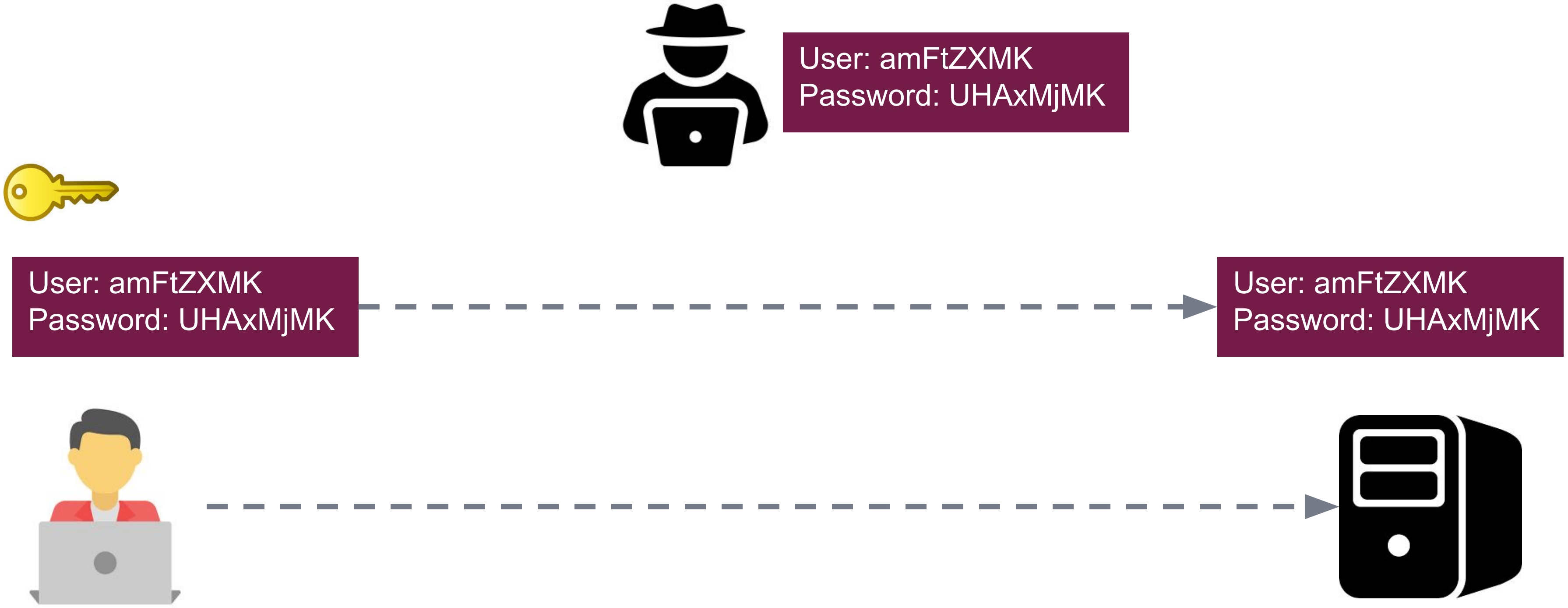
# SYMMETRIC ENCRYPTION



User: amFtZXMK
Password: UHAxMjMK

http://clarus-commerce.com

# SYMMETRIC ENCRYPTION

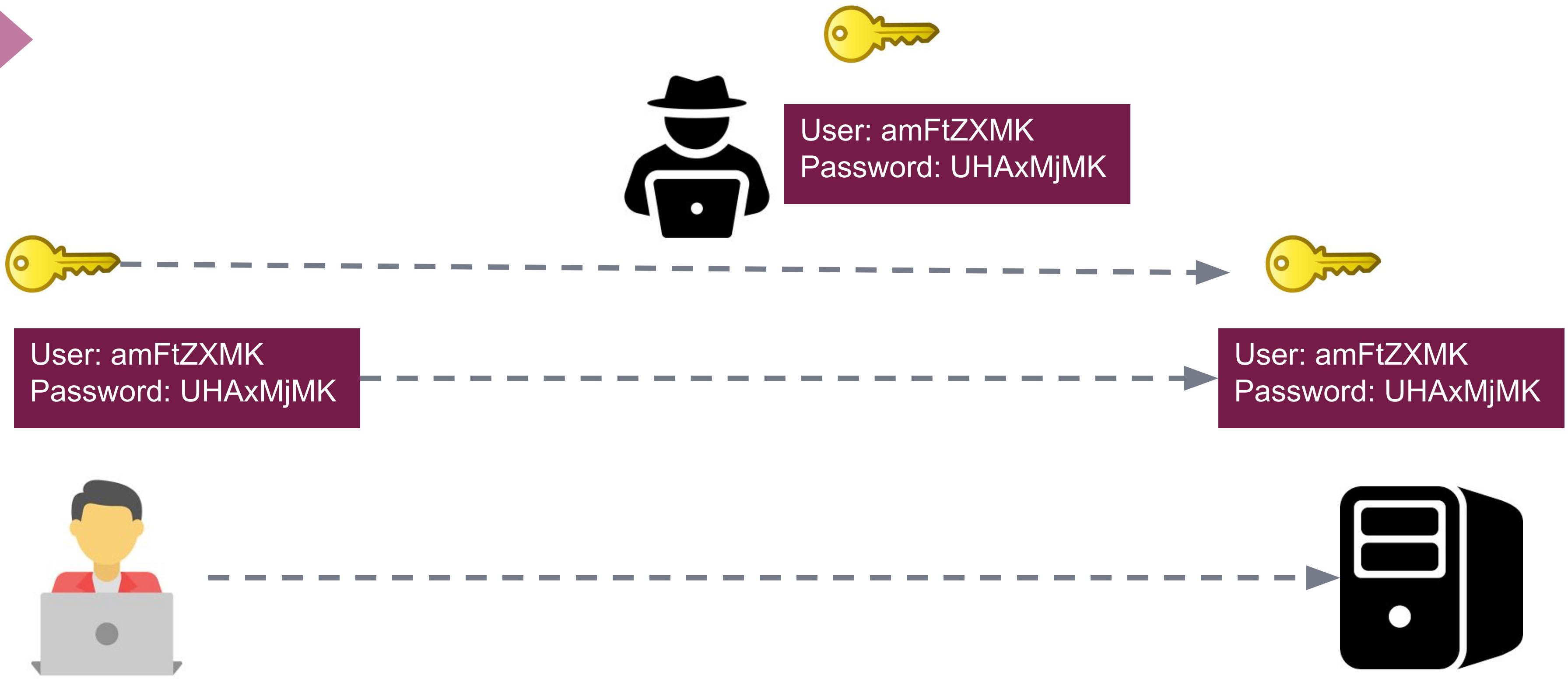


User: amFtZXMK
Password: UHAxMjMK

User: amFtZXMK
Password: UHAxMjMK

User: amFtZXMK
Password: UHAxMjMK

http://clarus-commerce.com



User: amFtZXMK
Password: UHAxMjMK

User: amFtZXMK
Password: UHAxMjMK

User: amFtZXMK
Password: UHAxMjMK

http://clarus-commerce.com

# SYMMETRIC ENCRYPTION

**Symmetric encryption** is a type of **encryption** where only one **key** (a secret **key**) is used to both **encrypt** and **decrypt** electronic information. The entities communicating via **symmetric encryption** must exchange the **key** so that it can be used in the decryption process.

2

# ASYMMETRIC ENCRYPTION

# ASYMMETRIC ENCRYPTION

Asymmetric Encryption, also known as **Public-Key Cryptography**, is an example of encryption method. Unlike **symmetric encryption**, Asymmetric Encryption encrypts and decrypts the data using **two separate** yet mathematically connected **cryptographic keys.** These keys are known as a **Public Key** and a **Private Key**. Together, they're called a **Public and Private Key Pair**.

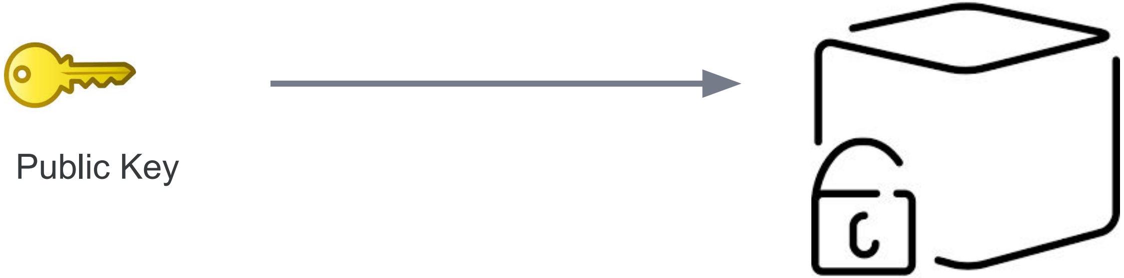
# ASYMMETRIC ENCRYPTION

private Key

**ASYMMETRIC ENCRYPTION**

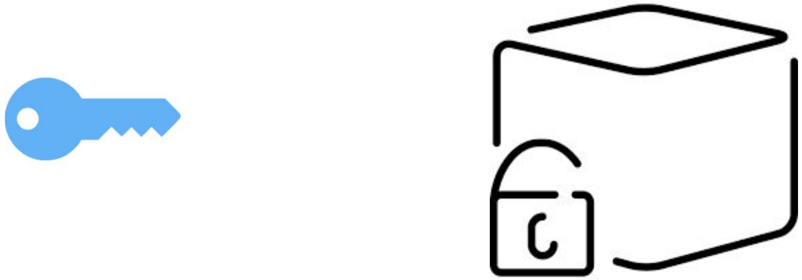
Public Key

To understand well, we symbolize public key as a lock box.

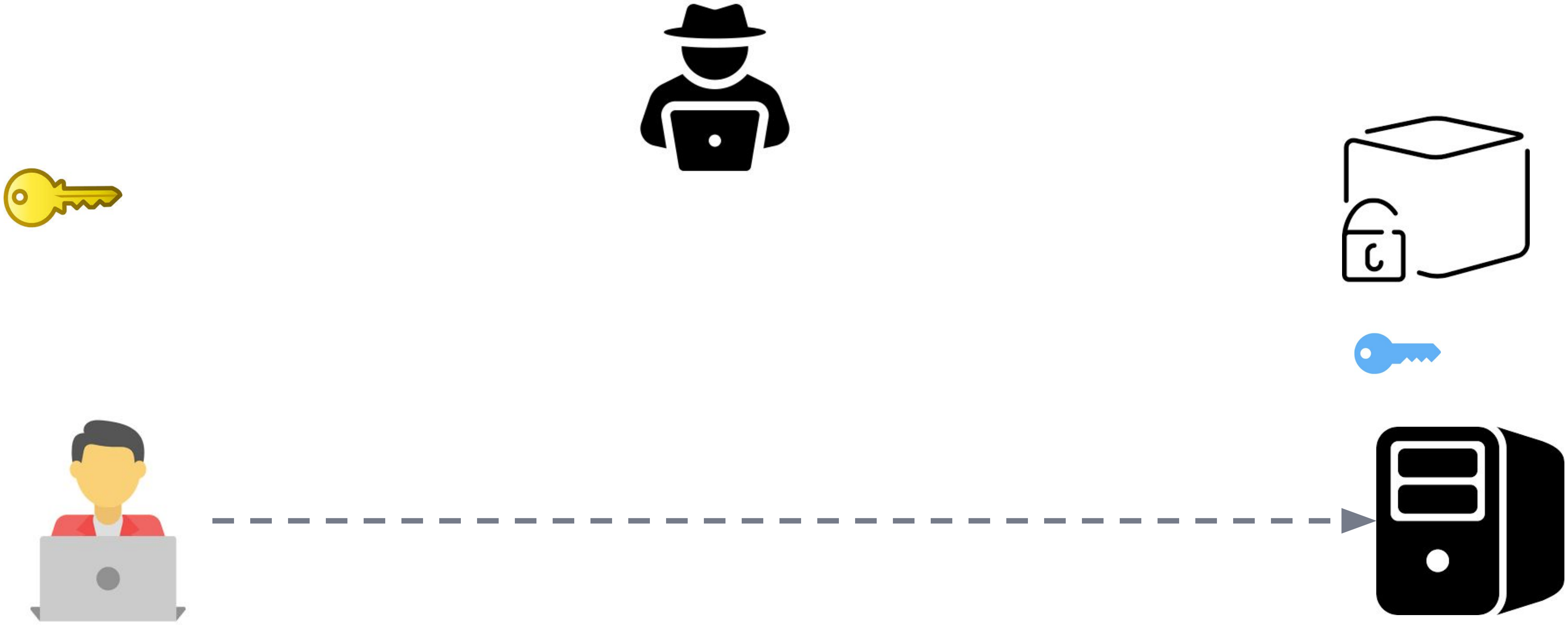


Public Key

# ASYMMETRIC ENCRYPTION

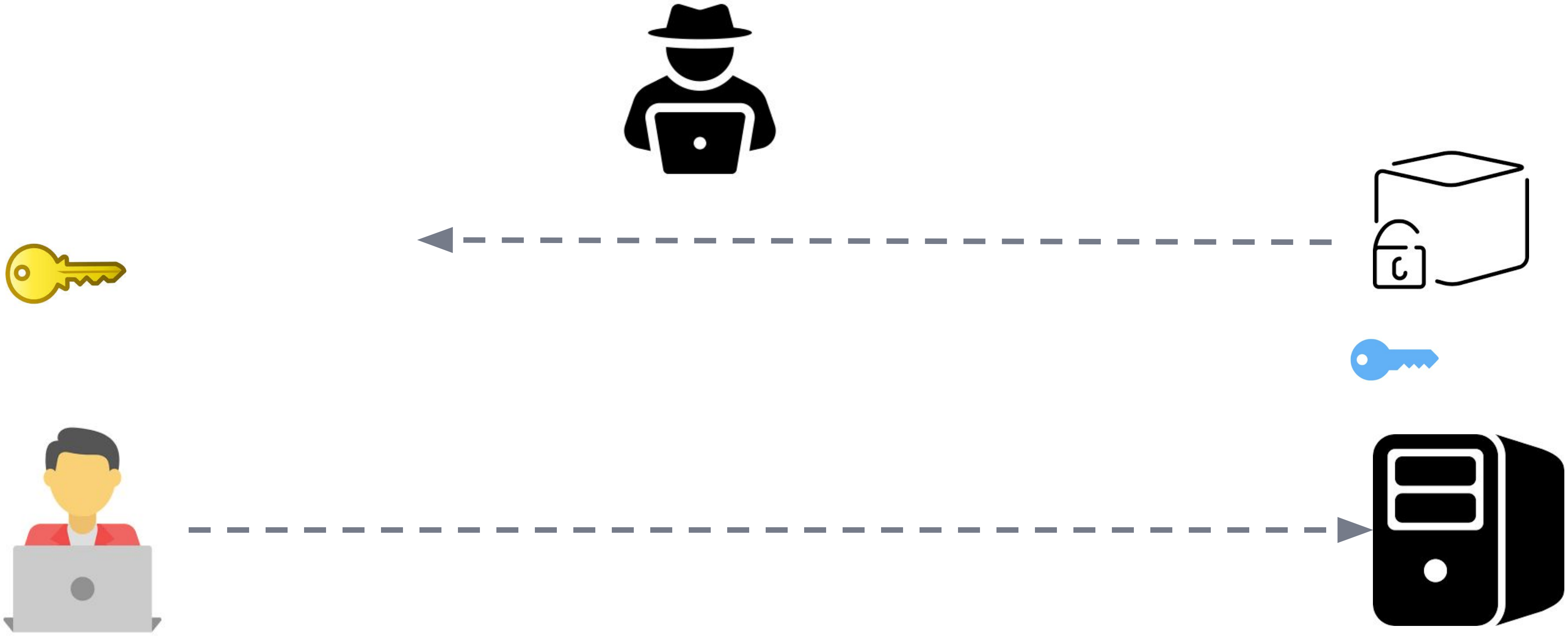


# ASYMMETRIC ENCRYPTION



http://clarus-commerce.com

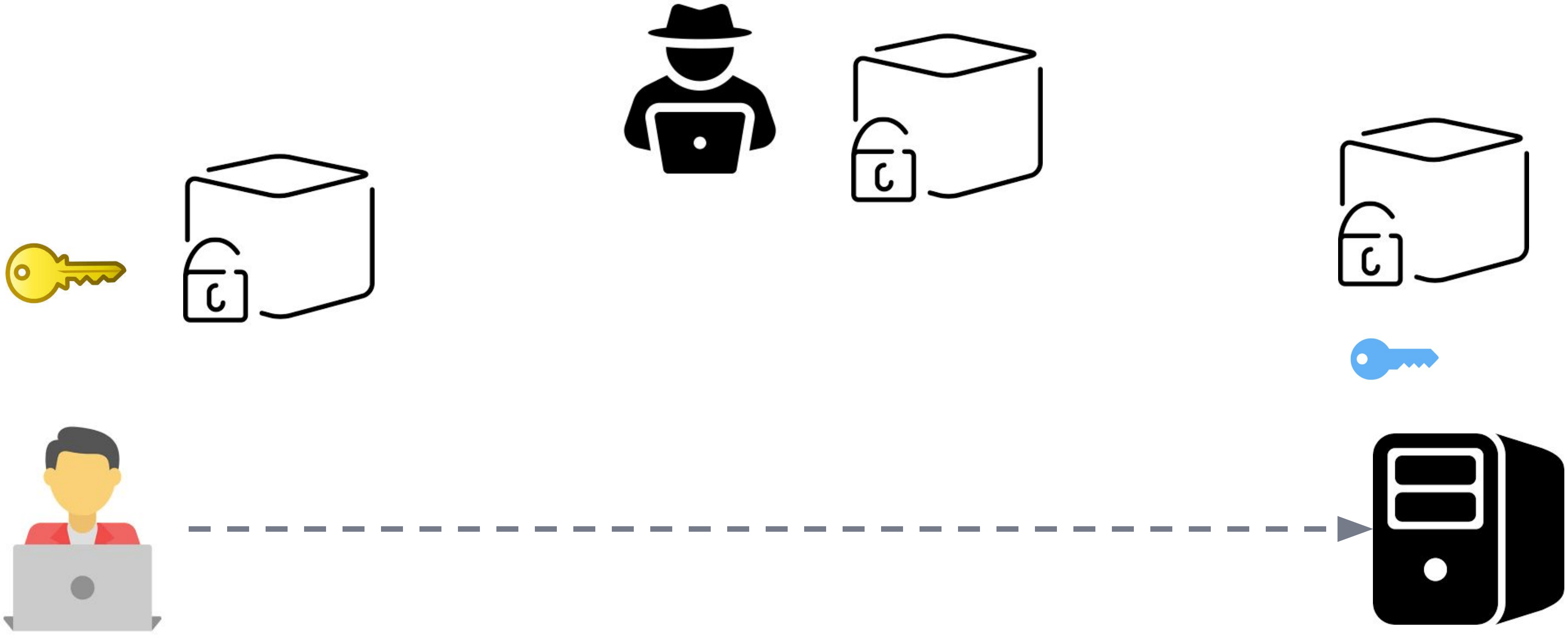
# ASYMMETRIC ENCRYPTION



https://clarus-commerce.com

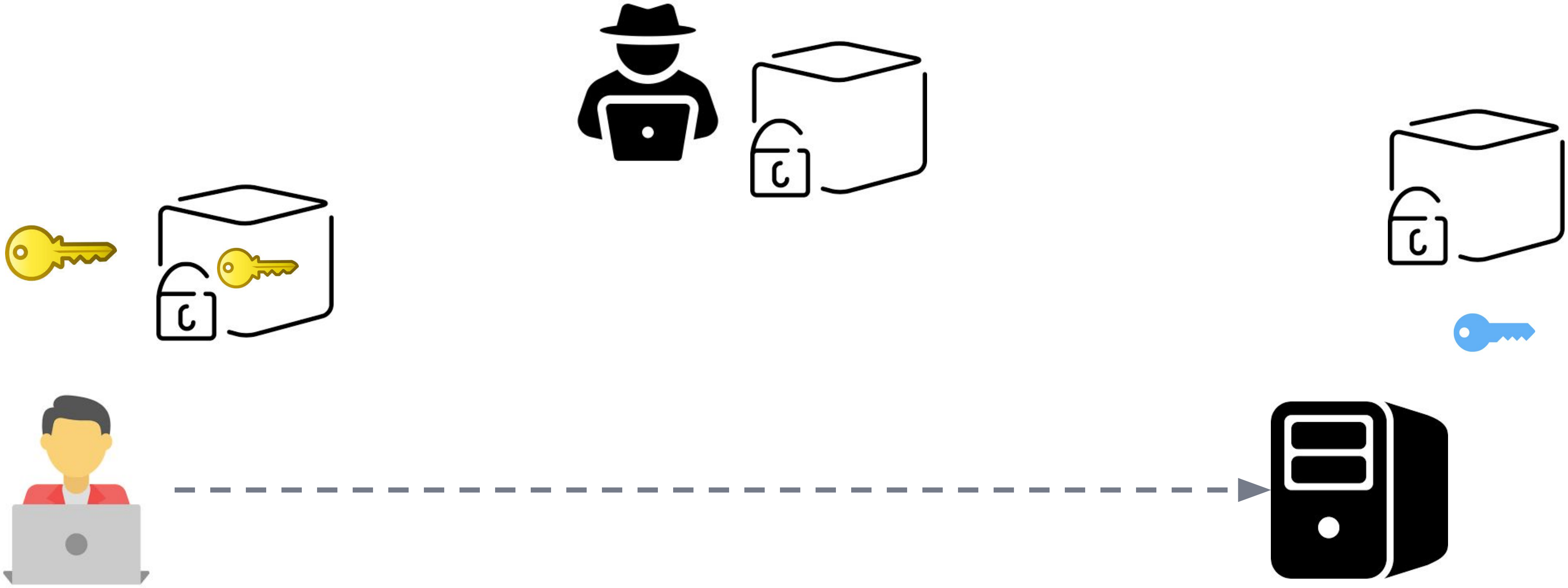
http turn to https

# ASYMMETRIC ENCRYPTION



https://clarus-commerce.com

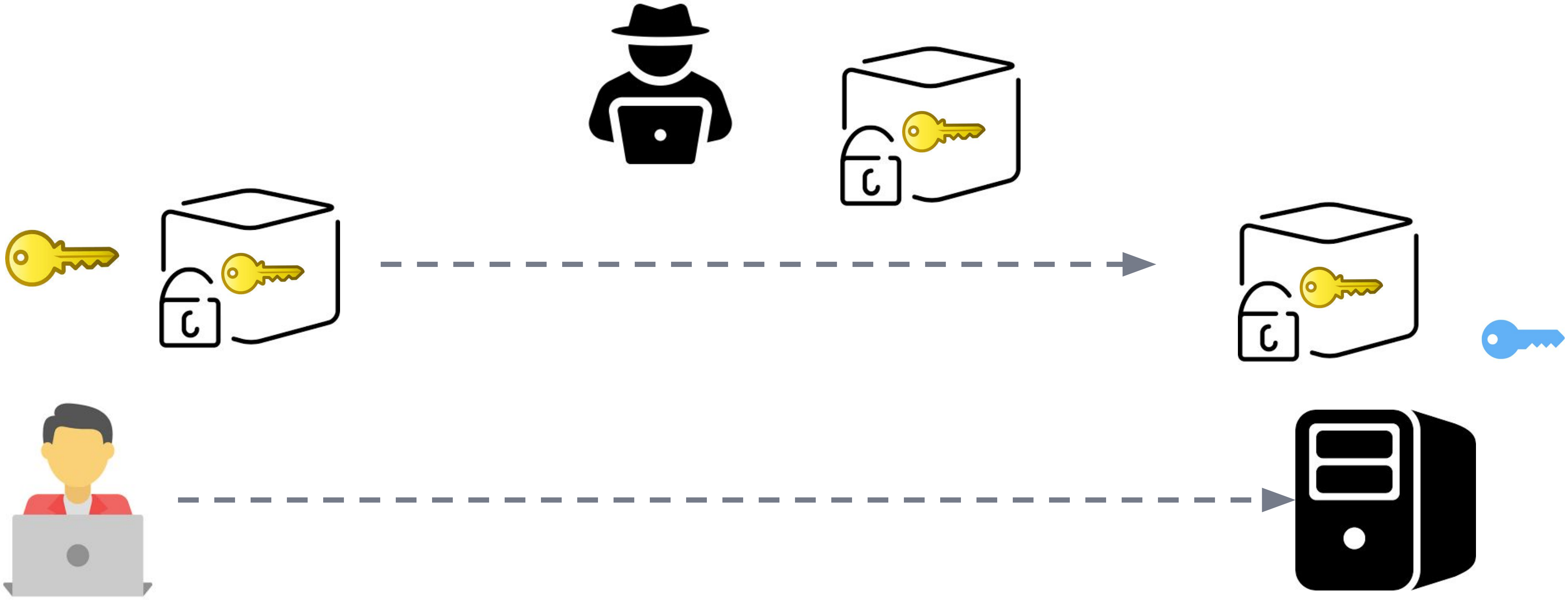
# ASYMMETRIC ENCRYPTION



https://clarus-commerce.com

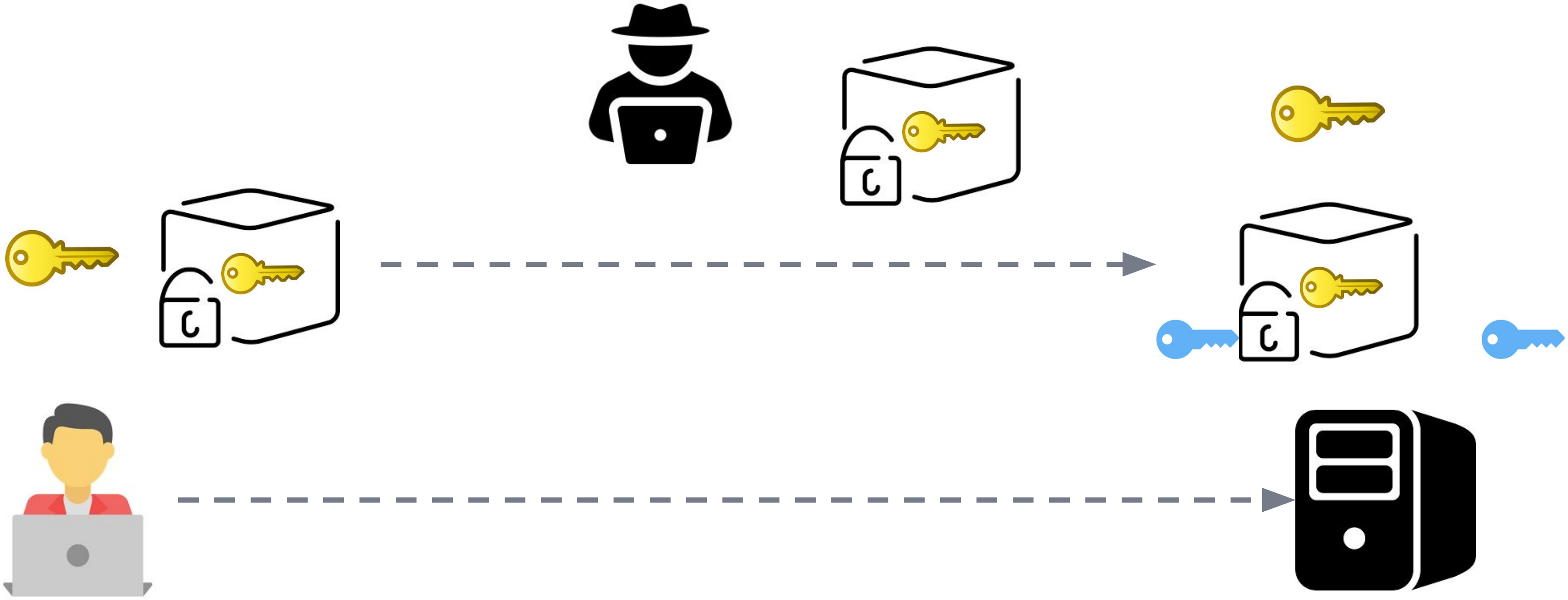
We make our private key secure with server public key

# ASYMMETRIC ENCRYPTION



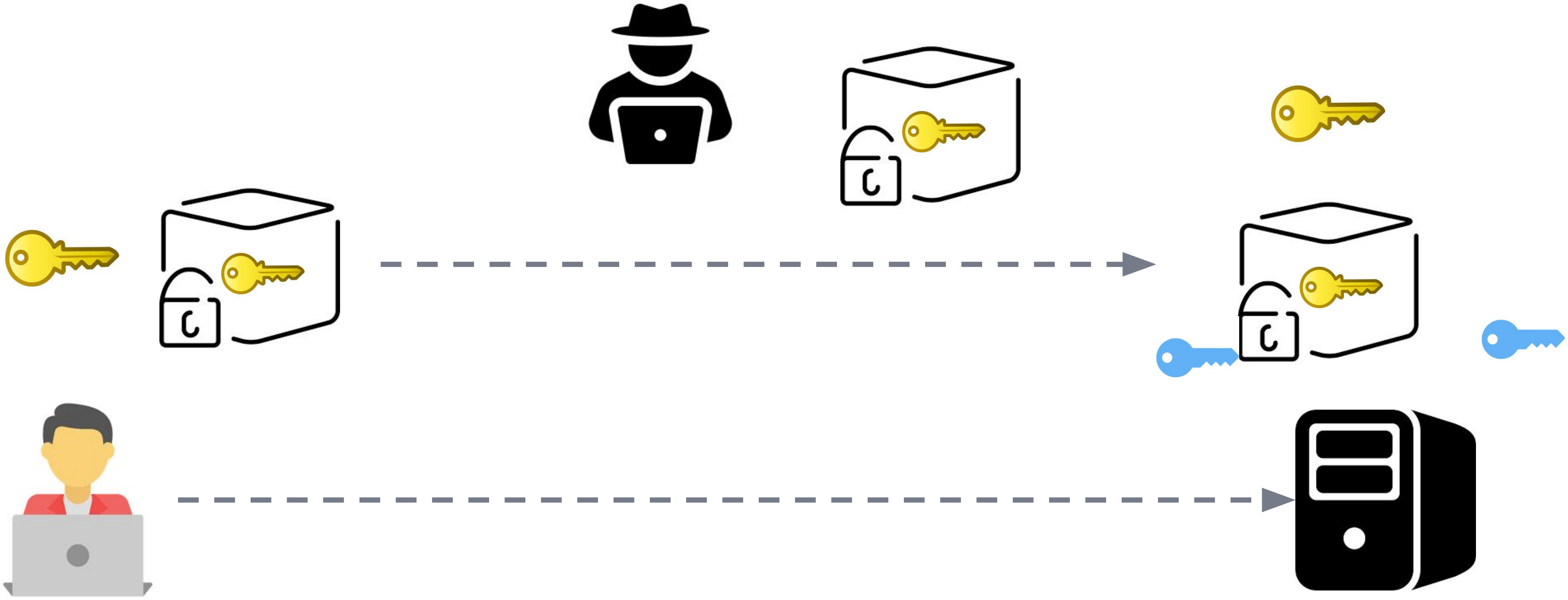
https://clarus-commerce.com

# ASYMMETRIC ENCRYPTION



https://clarus-commerce.com

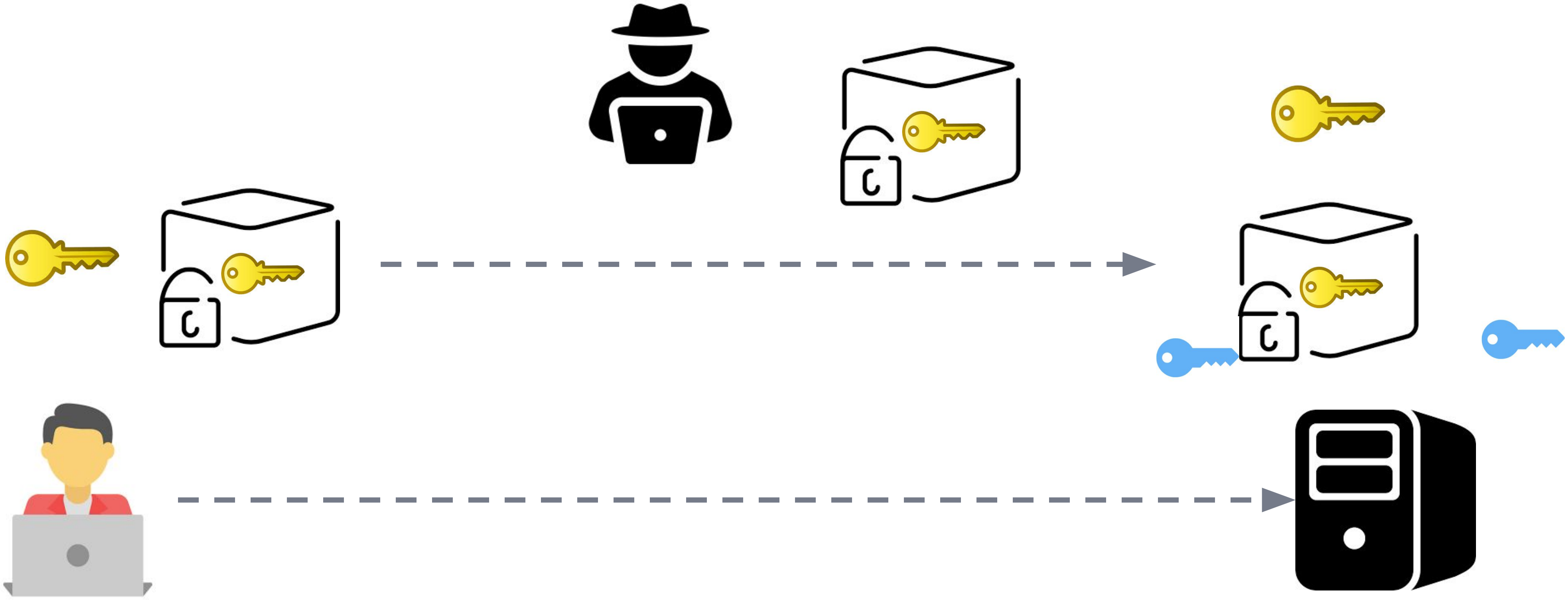
# ASYMMETRIC ENCRYPTION



https://clarus-commerce.com

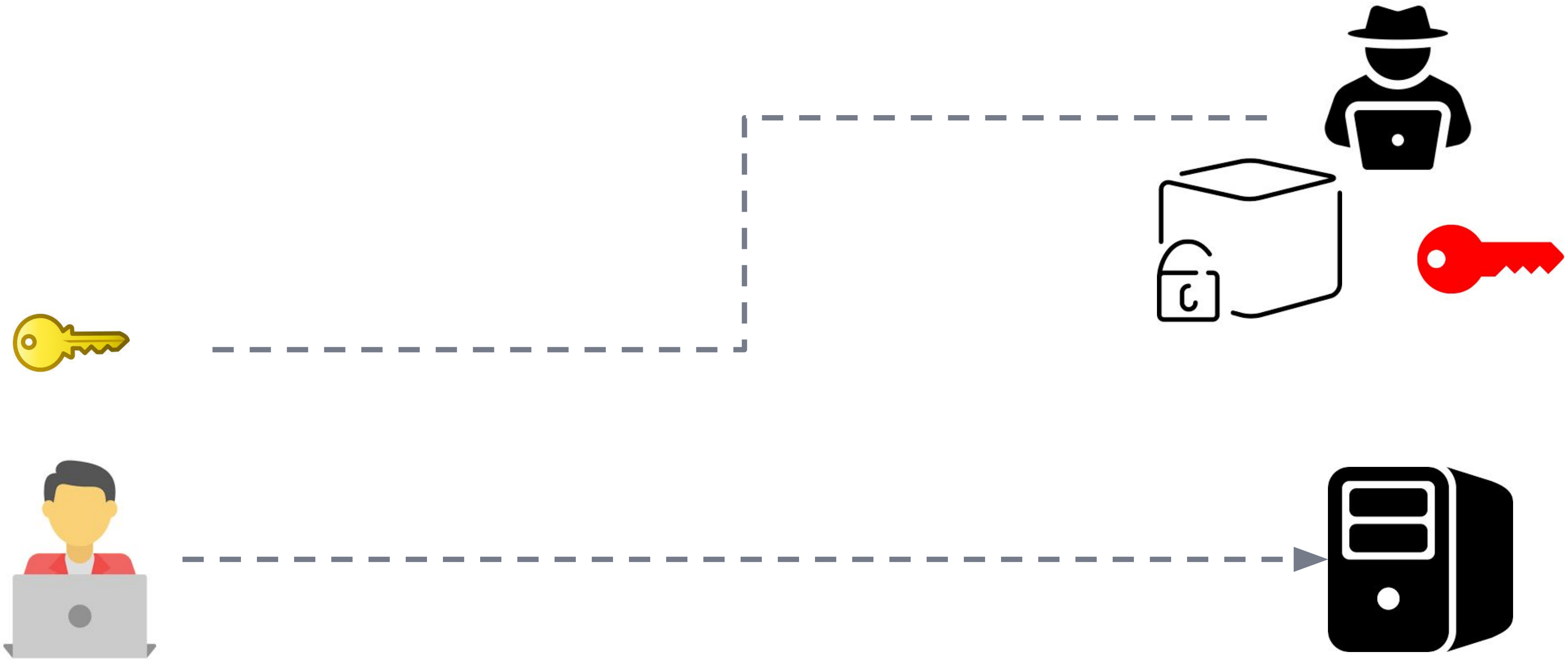
Server decrypt our private key with server private key. Hacker doesn't have private key of server. So the hacker couldn't get our private key.

# ASYMMETRIC ENCRYPTION



Server decrypt our private key with server private key. Hacker doesn’t have private key of server. So the hacker couldn’t get our private key.

# ASYMMETRIC ENCRYPTION

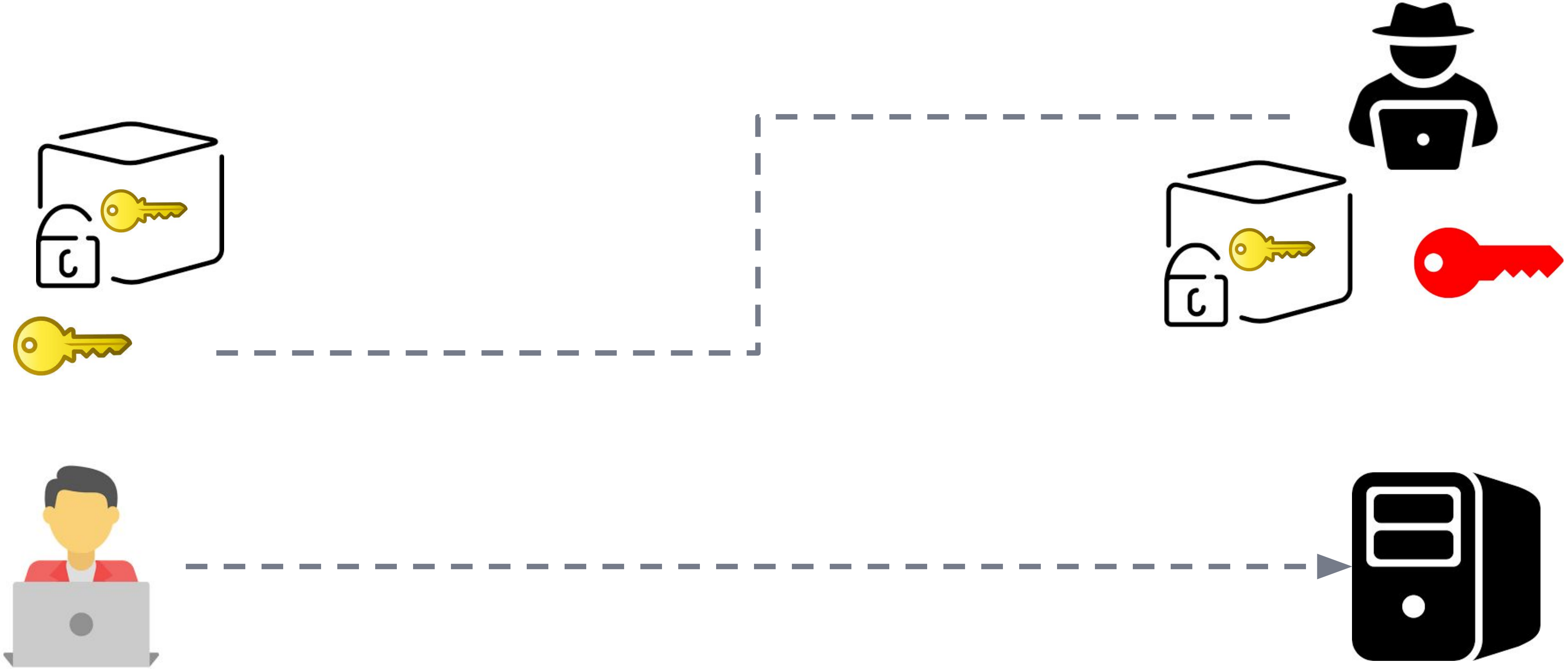


https://clarus-commerce.com

Hacker can allure and trick us. Hacker can get our private key.

CLARUSWAY©
WAY TO REINVENT YOURSELF

# ASYMMETRIC ENCRYPTION



https://clarus-commerce.com

Hacker can allure and trick us. Hacker can get our private key.

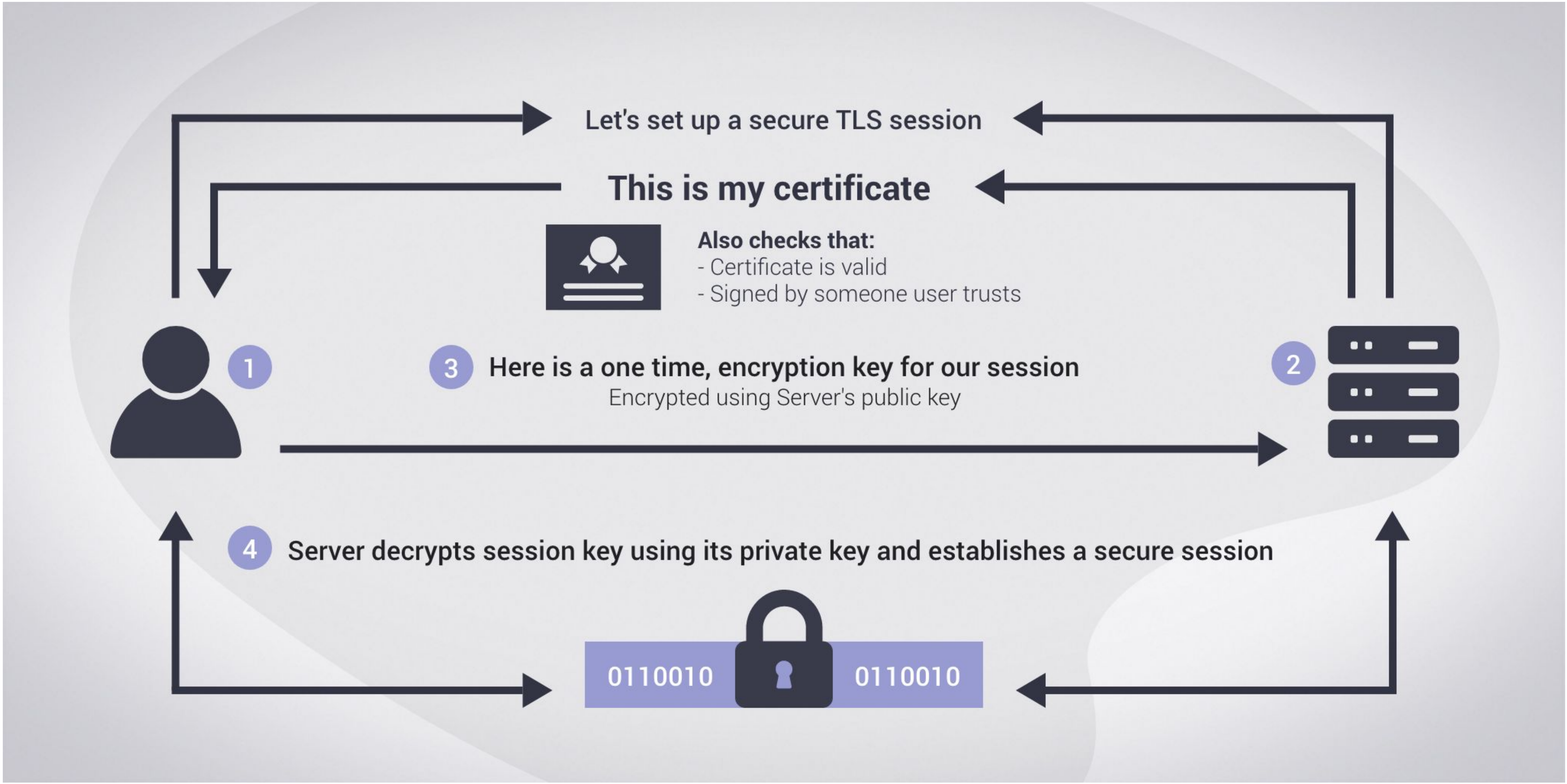
3

# TLS/SSL CERTIFICATE

# TLS/SSL CERTIFICATE

Transport Layer Security is a protocol that establishes an encrypted session between two computers on the Internet. It verifies the identity of the server and prevents hackers from intercepting any data.

# TLS/SSL CERTIFICATE



Let's set up a secure TLS session

This is my certificate

**Also checks that:**
- Certificate is valid
- Signed by someone user trusts

3 Here is a one time, encryption key for our session

Encrypted using Server's public key

4 Server decrypts session key using its private key and establishes a secure session

# TLS/SSL CERTIFICATE

What is a TLS certificate?

Digital certificates, also known as identity certificates or public key certificates, are digital files that are used to certify the ownership of a public key. TLS certificates are a type of digital certificate, issued by a **Certificate Authority (CA)**. **The CA signs the certificate**, certifying that they have verified that it belongs to the owners of the domain name which is the subject of the certificate.

# TLS/SSL CERTIFICATE

TLS certificates usually contain the following information:

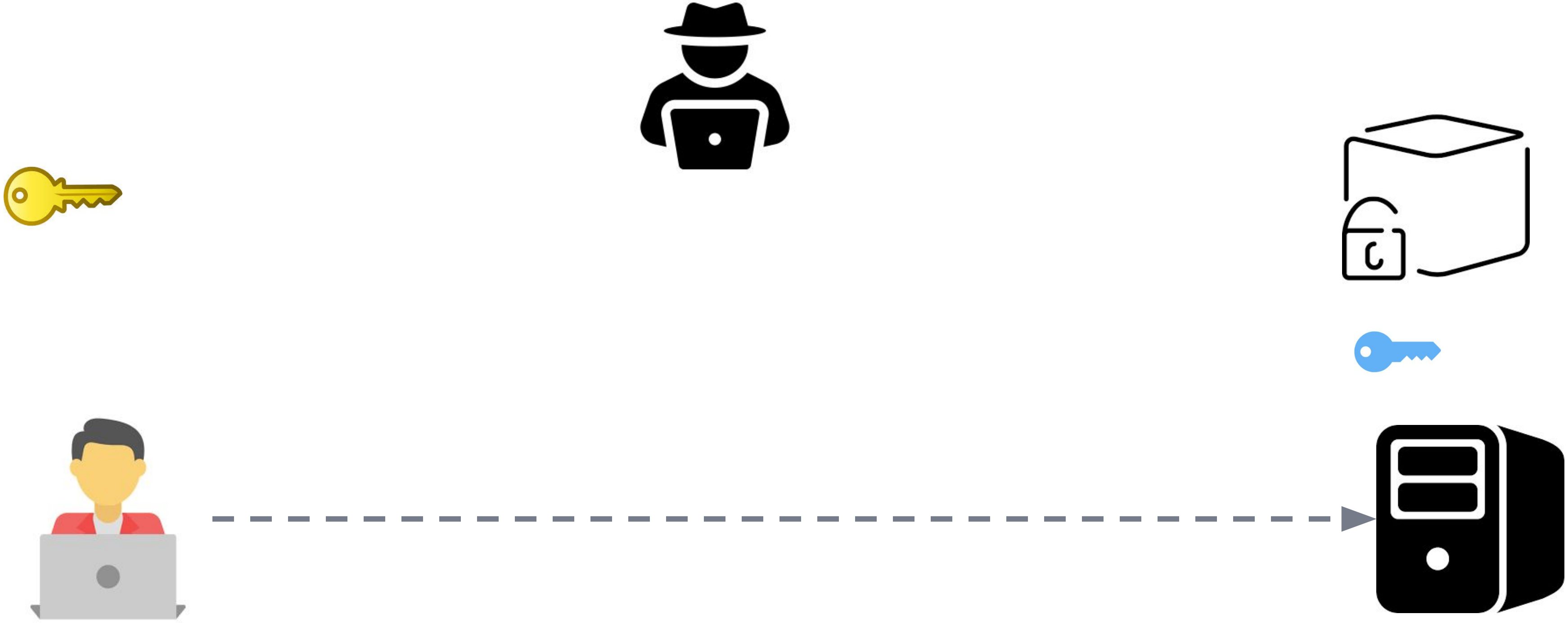
- The subject domain name
- The subject organization
- The name of the issuing CA
- Additional or alternative subject domain names, including subdomains, if any
- Issue date
- Expiry date
- The public key (The private key, however, is a secret.)
- **The digital signature by the CA**

# TLS/SSL CERTIFICATE

## How does a TLS certificate work?

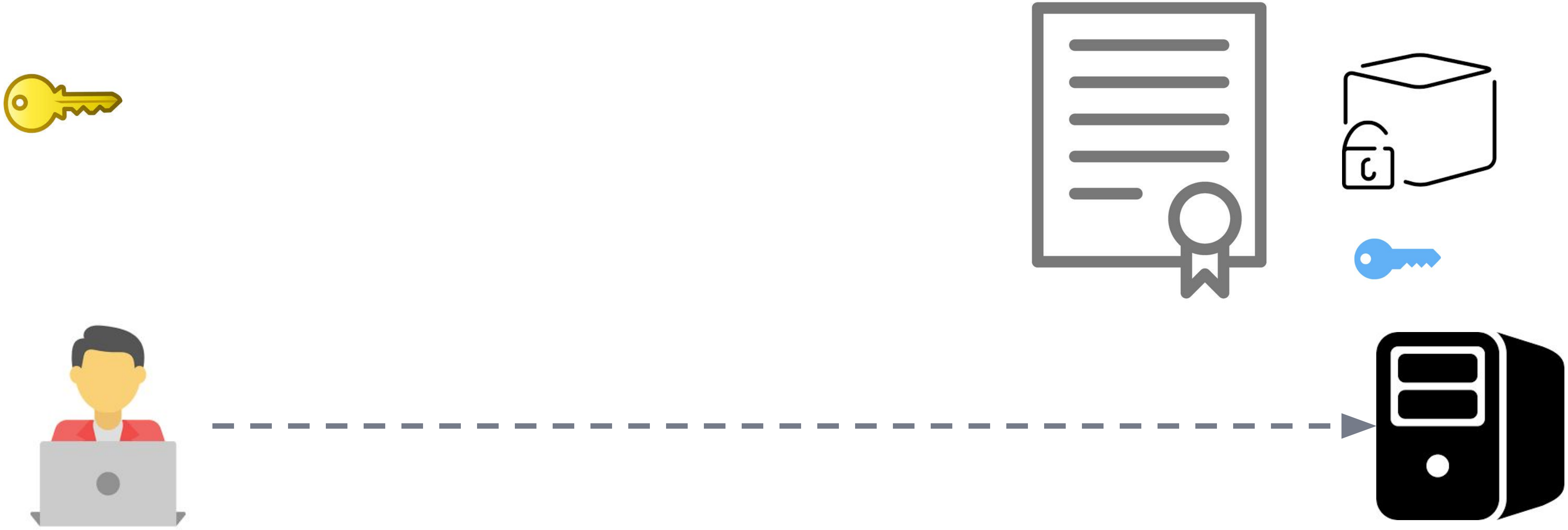
When a user tries to connect to a server, the server sends them its TLS certificate. The user then verifies the server’s certificate using CA certificates that are present on the user’s device to establish a secure connection. This verification process uses public key cryptography, such as RSA or ECC, to prove the CA signed the certificate. As long as you trust the CA, this demonstrates you are communicating with the server certificate’s subject

# TLS/SSL CERTIFICATE



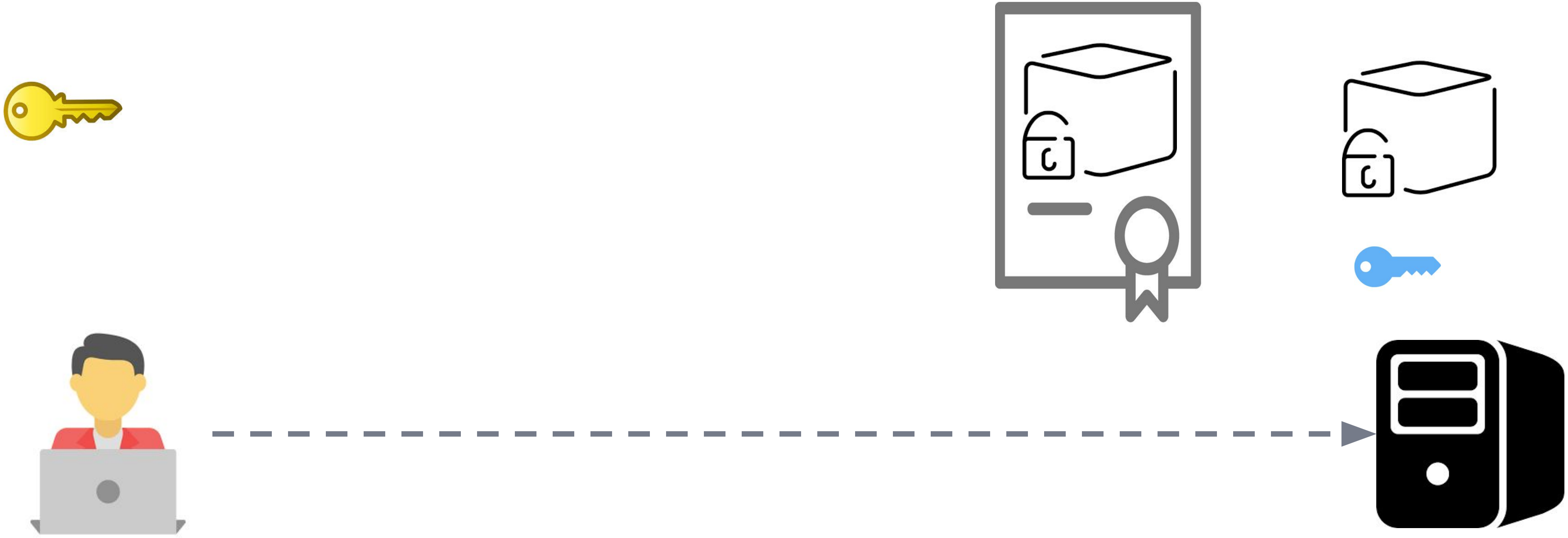
http://clarus-commerce.com

# TLS/SSL CERTIFICATE



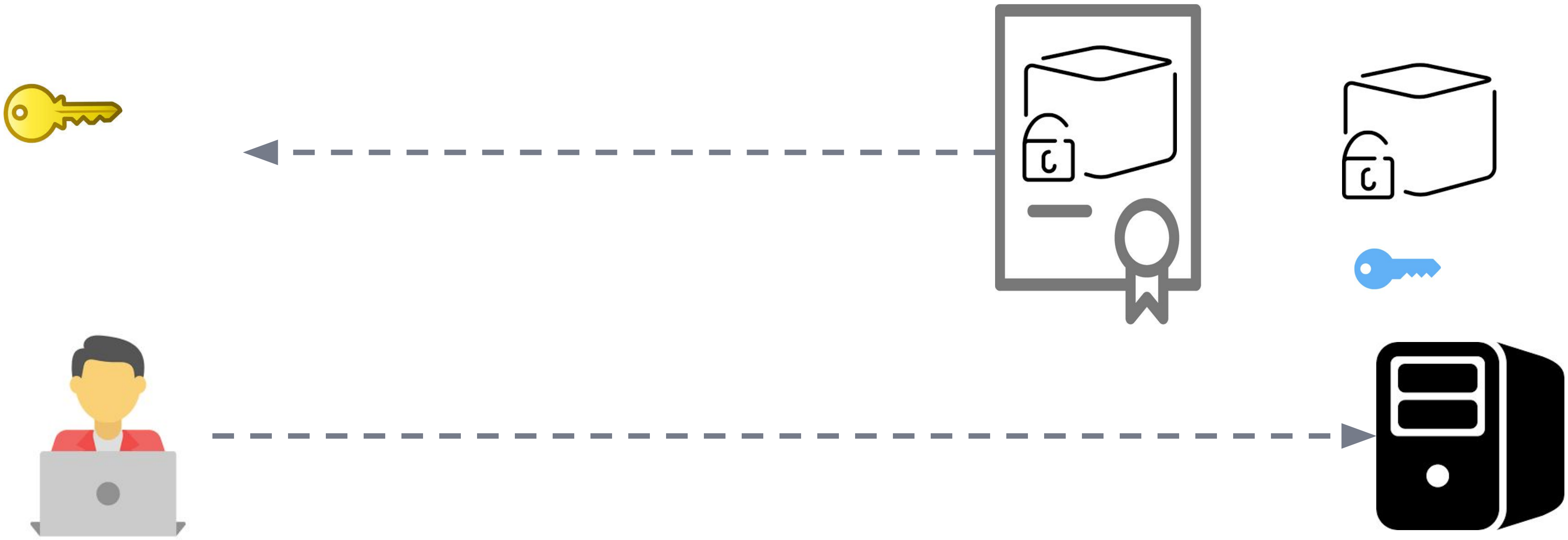
http://clarus-commerce.com

# TLS/SSL CERTIFICATE



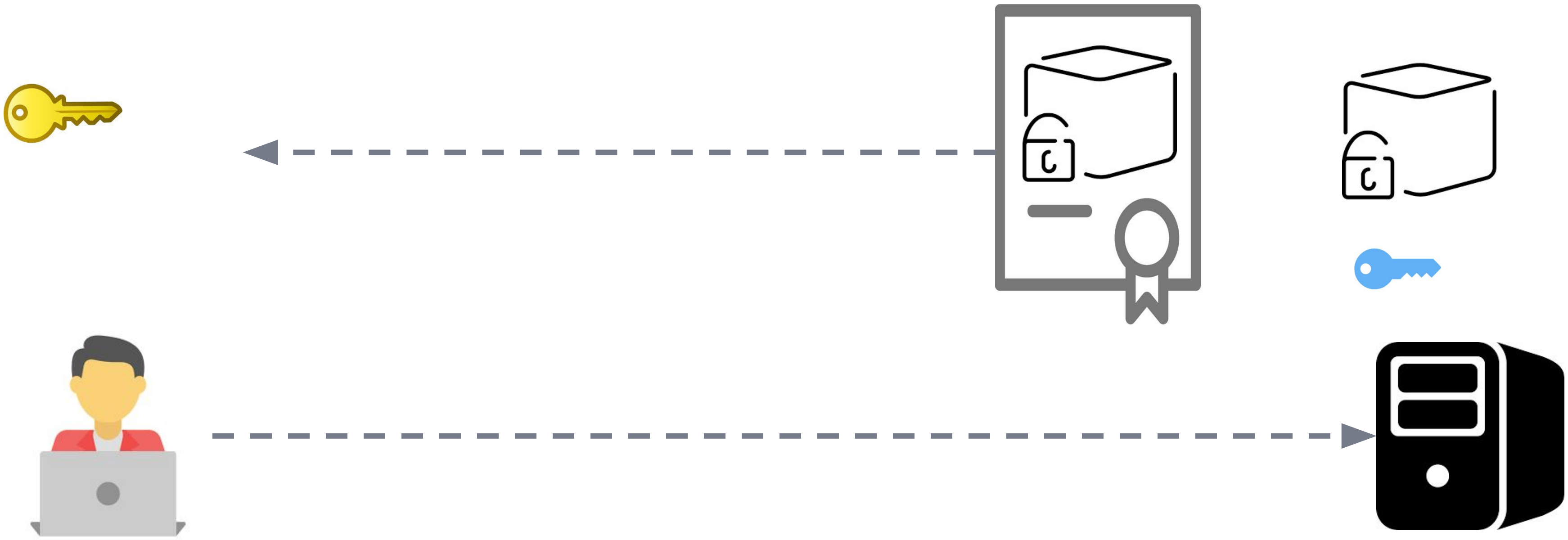
http://clarus-commerce.com

# TLS/SSL CERTIFICATE



http://clarus-commerce.com

# TLS/SSL CERTIFICATE

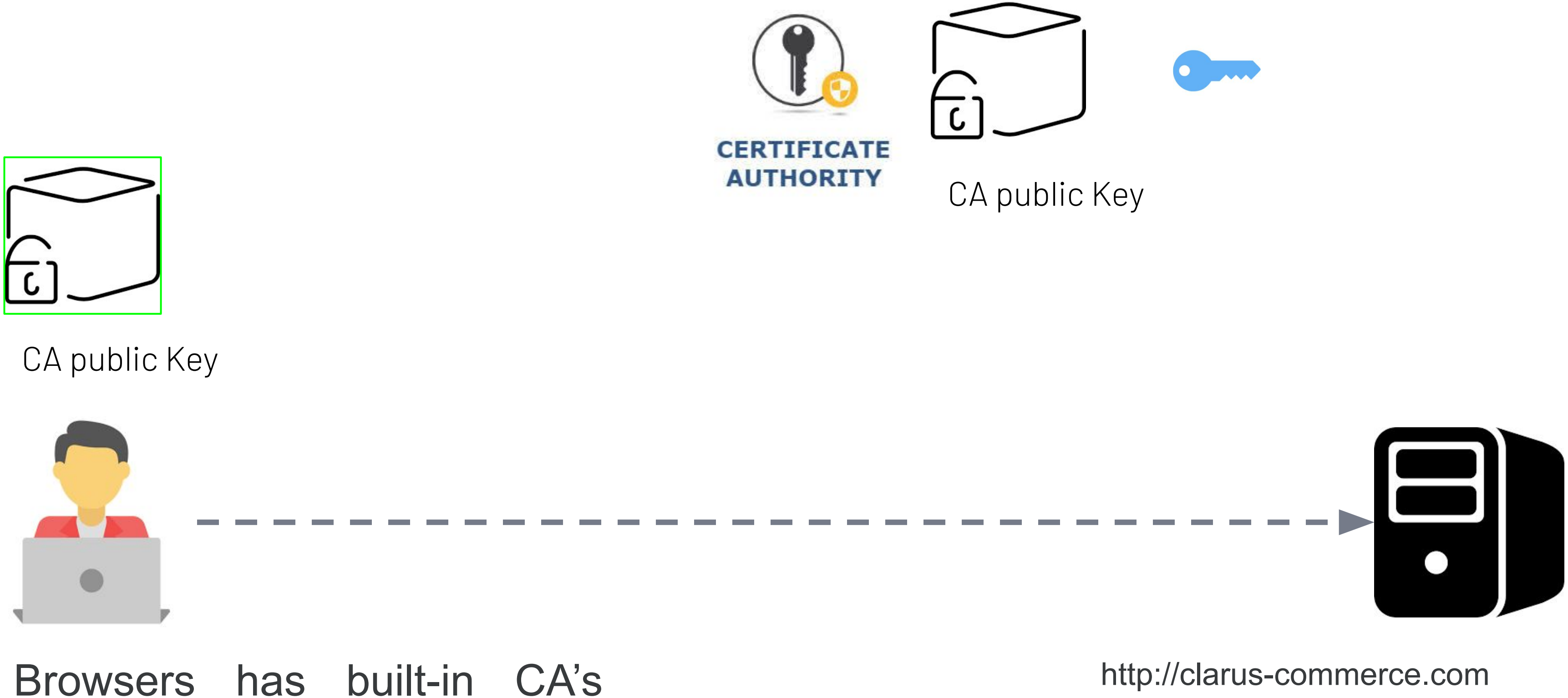


https://clarus-commerce.com

# How does a TLS certificate work?

1. We request a CSR(Certificate Signing Request) from any CA (Certificate Authority).
2. CA validate our request.
3. CA send signed certificate to us.

# How does a browser know TLS certificate is valid?



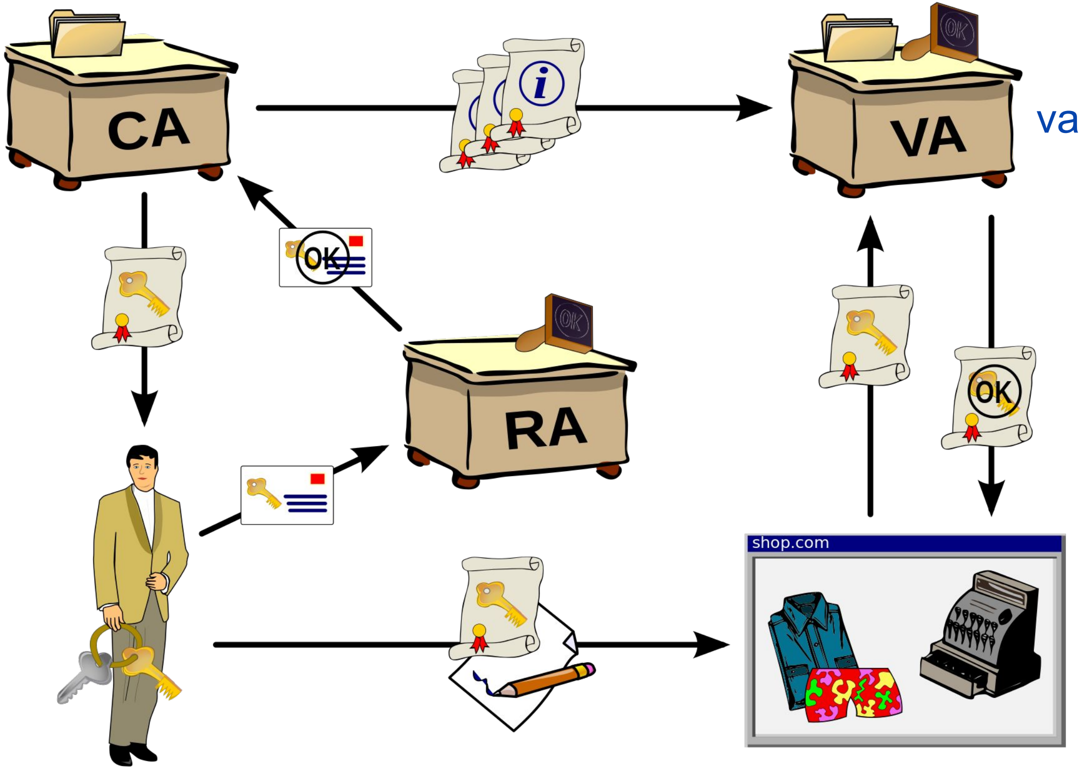
Browsers has built-in CA’s public keys.

# A public key infrastructure (PKI)

**A public key infrastructure (PKI)** is *a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption*.

The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

# A public key infrastructure (PKI)



validation authority (VA)

*registration authority* (RA)

# THANKS!

## Any questions?

You can find me at:

- james@clarusway.com

USWAY©
REINVENT YOURSELF

Students, write your response!

Pear Deck Interactive Slide
Do not remove this bar