

PKI on one page

How your browser decides to trust a website

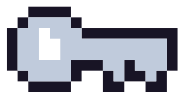


Rosa signs
key holder

Ken checks
relying party

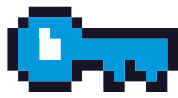
1 One key or two?

ONE KEY



both need a copy

TWO KEYS, ONE PAIR



public



private

Public key: share it with anyone.

Private key: it never leaves its owner.

2 A Fingerprint (hash)

Meet at 6

SHA-256

d02f2430...

Meet at 9

813f2905...

Any data gets a short fingerprint.

Change one character: a whole new one.

3 A signature



Meet at 6

signed



VALID

Rosa signs with her **private** key.

Anyone checks with her **public** key.

The message stays readable.

4 A certificate

CERTIFICATE

Name: www.example.com

Public key: 

Signed by: a CA



It ties a **name** to a **public key**.

A certificate authority (CA) checks the name, then signs it.

5 The chain of trust

Each one is signed by the next:

example.com
website

Intermediate
CA

trust store

Root CA

The root is trusted because it is already in your trust store, not because it signed itself.

6 The TLS handshake



browser

1 fresh keys (ECDHE)

2 certificate chain

3 signature made with
its private key (proof)



website

Fresh session keys do the encrypting.
The certificate encrypts nothing.

7 When trust breaks

 EXPIRED

past its end date

 REVOKED

cancelled early by its CA

 WRONG NAME

made for another address

 Public logs (Certificate Transparency)
let anyone spot a fake.

8 Shorter lives ahead

Longest life of a website certificate

2020		398 days
2026		200 days
2027		100 days
2029		47 days

From 15 March 2029: at most 47 days.
Renew at least eight times a year:
let robots do it (ACME).