



✓ **HTTPS = HTTP + TLS**

➔ TLS - Transport Layer Security (a.k.a SSL) provides

- **confidentiality** : end-to-end secure channel
- **integrity** : one-way authentication handshake

This how HTPS works









|   |                               |
|---|-------------------------------|
|  | <hr/> <hr/> <hr/> <hr/> <hr/> |
|---|-------------------------------|



example.com



*HTTPS request*

A long, solid black arrow pointing horizontally to the right, spanning the width of the image below the text.



*HTTPS response*



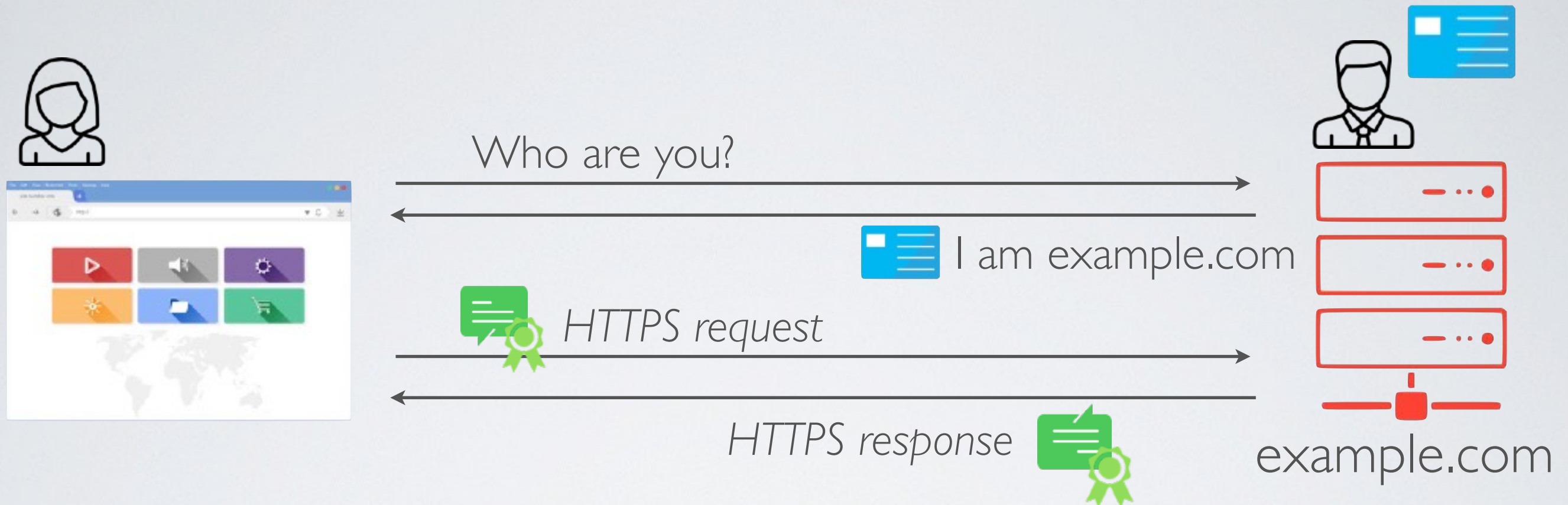
Who are you?





I am example.com

# This how HTTPS works



✓ **HTTPS = HTTP + TLS**

- ➔ TLS - Transport Layer Security (a.k.a SSL) provides
- **confidentiality** : end-to-end secure channel
  - **integrity** : one-way authentication handshake

# simplified and one-way authentication

## TLS 1.2 (2008)

