COPENHAGEN BUSINESS ACADEMY

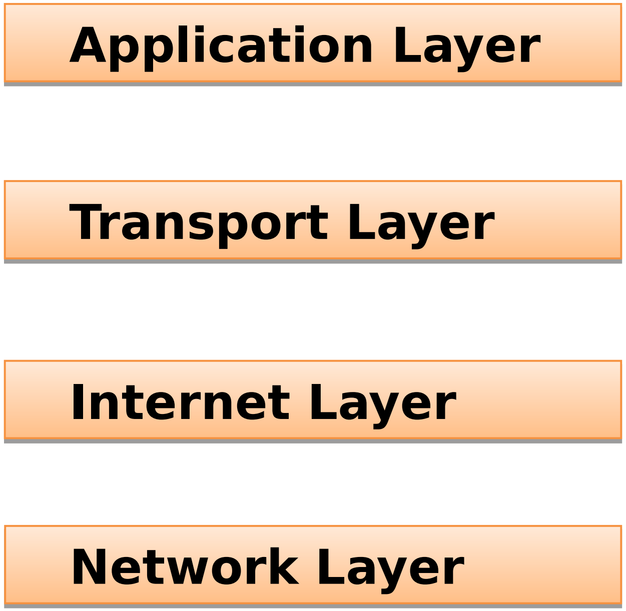
HTTPS and certificates

Jens Egholm Pedersen
<jeep@cphbusiness.dk>

Networking so far

- IP
- TCP
- HTTP

→ Everything‘s visible!

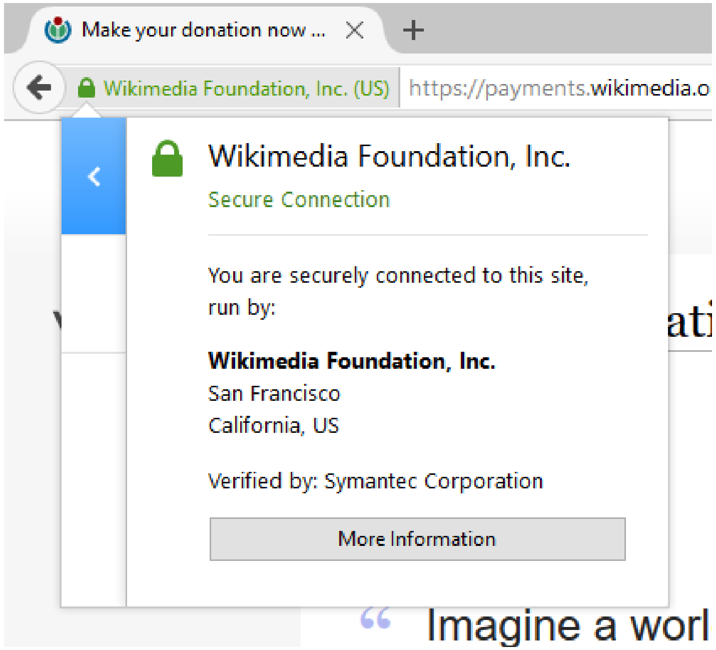


- Which layer should be encrypted?
  - Transport Layer

See also: Transport Layer Security

HTTPS

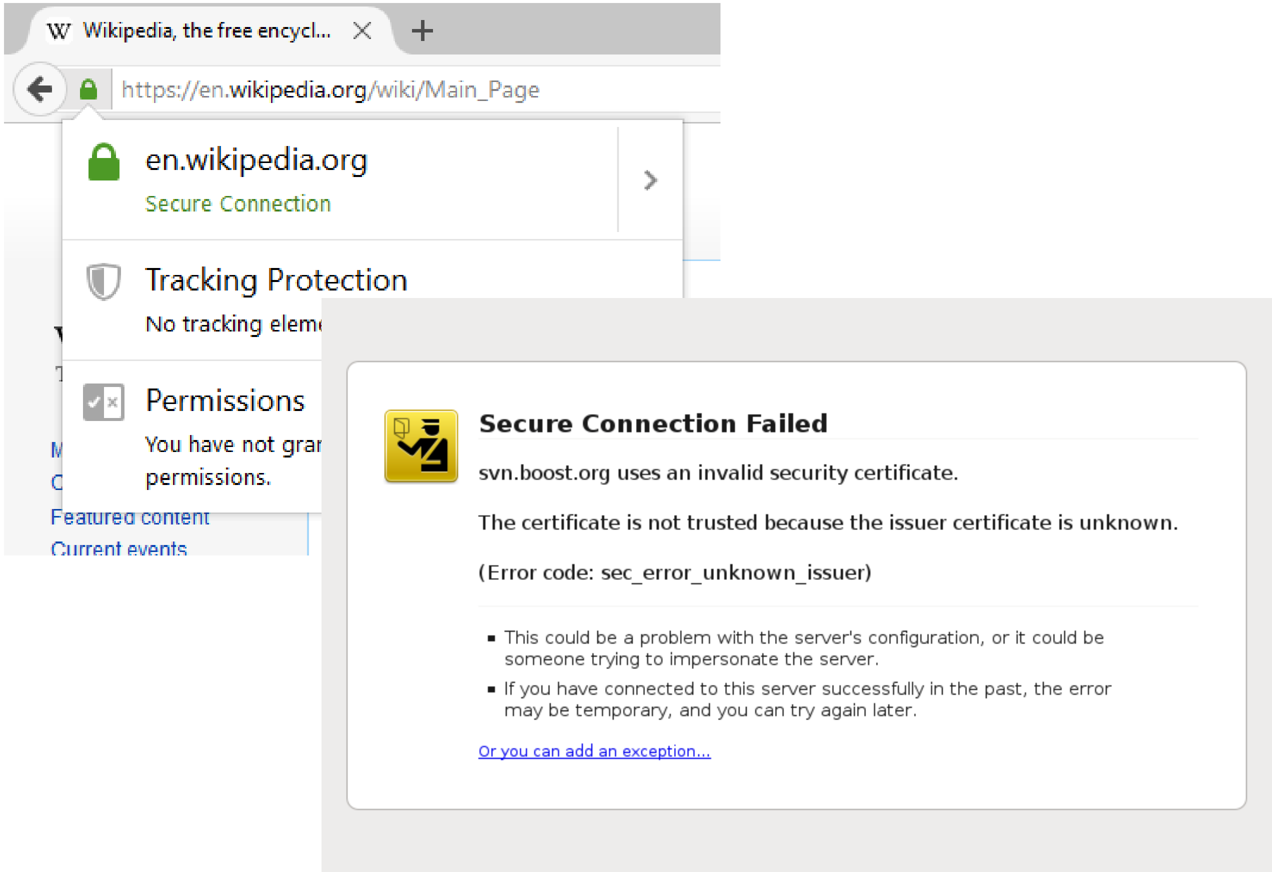
- HTTP over TLS (on what port?)
- Simply HTTP inside a TLS tunnel


Make your donation now ...
Wikimedia Foundation, Inc. (US)
https://payments.wikimedia.o
Wikimedia Foundation, Inc.
Secure Connection
More Information
ati
Imagine a worl

You are securely connected to this site, run by:

Wikimedia Foundation, Inc.
San Francisco
California, US

Verified by: Symantec Corporation



Secure Connection Failed

svn.boost.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception…

See also: HTTPS

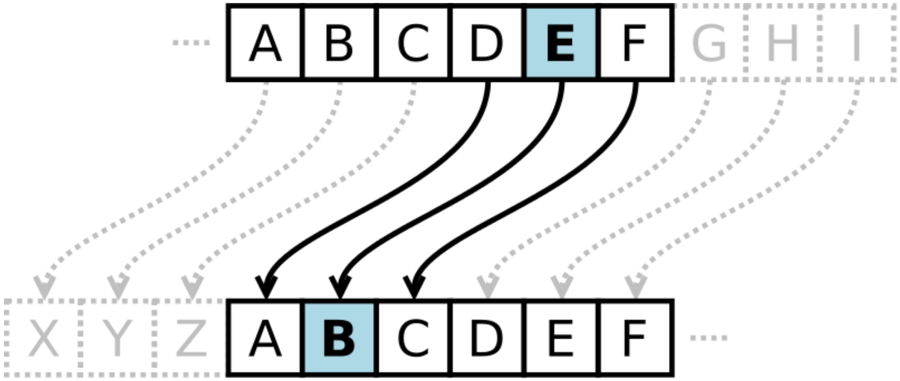
Security

- Hiding the content of a communication
  - Coding/encrypting
- Hiding the parties in the communication
  - Anonymisation
- Hiding that a communication takes place
  - Security by obscurity

See also: Secure communication

Cryptography

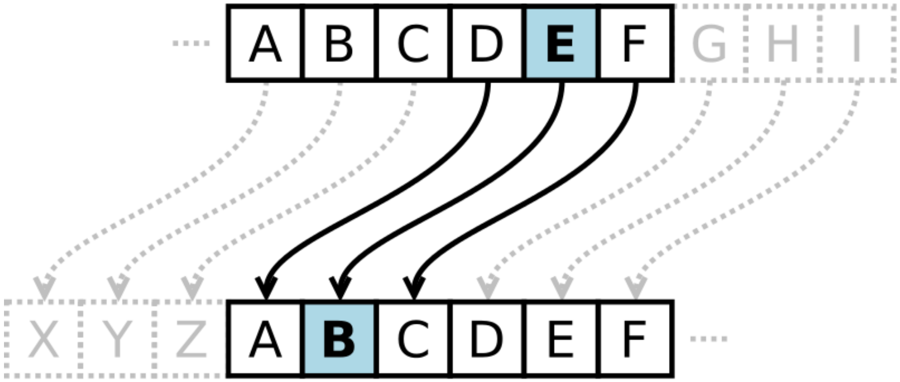
- Study of secure communication
- Classic: Caesar cipher



- Now: Symmetric-key and public-key

Symmetric-key cryptography

- Decryption by key
- Classic: Caesar cipher

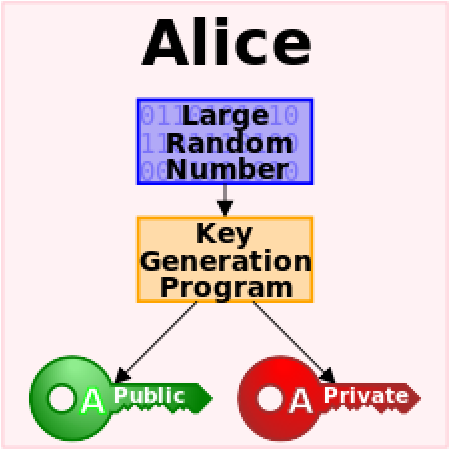


- Modern: AES, DES, ...

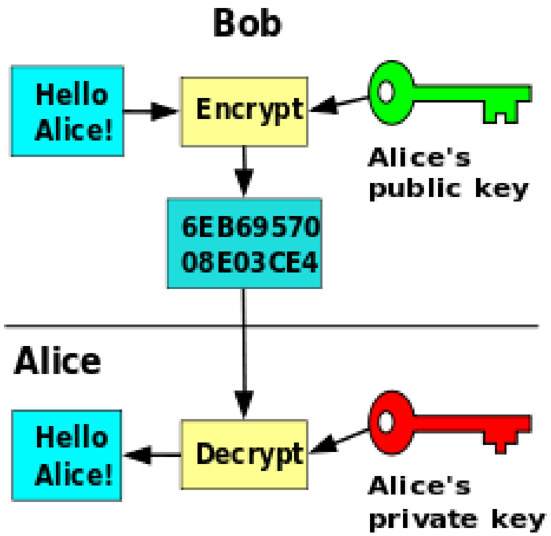
See also: Advanced Encryption Standard (AES)

Public-key cryptography

- Asymmetric
  - *public* and *private* key



- *Encryption* by the public key
- *Decryption* by the private key



TLS

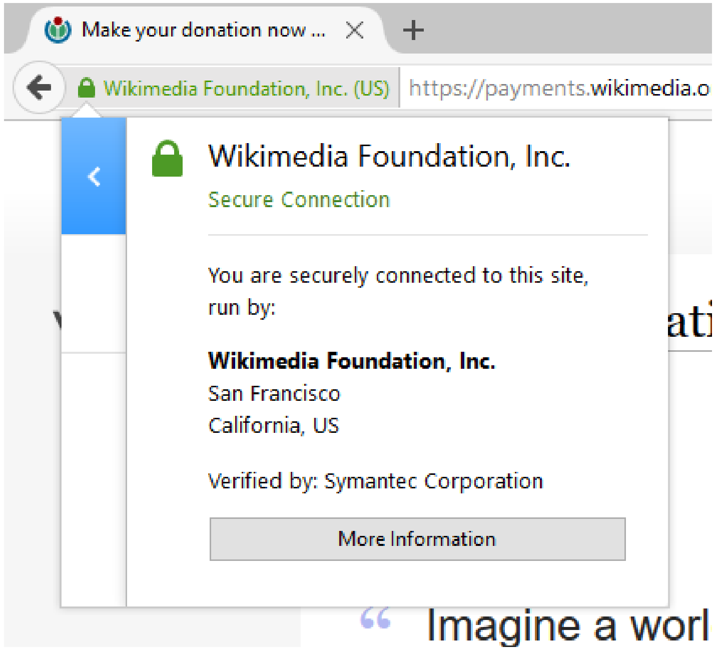
- Transport layer security
  - Protects the transport layer with public-private keys

- Problem solved?

- Where do you get the public key from?
  - The server
- Who is the server?
  - ?!

HTTPS

- HTTP over TLS
- Need trusted third party to authenticate the server



Make your donation now ...
Wikimedia Foundation, Inc. (US)
https://payments.wikimedia.o

Wikimedia Foundation, Inc.

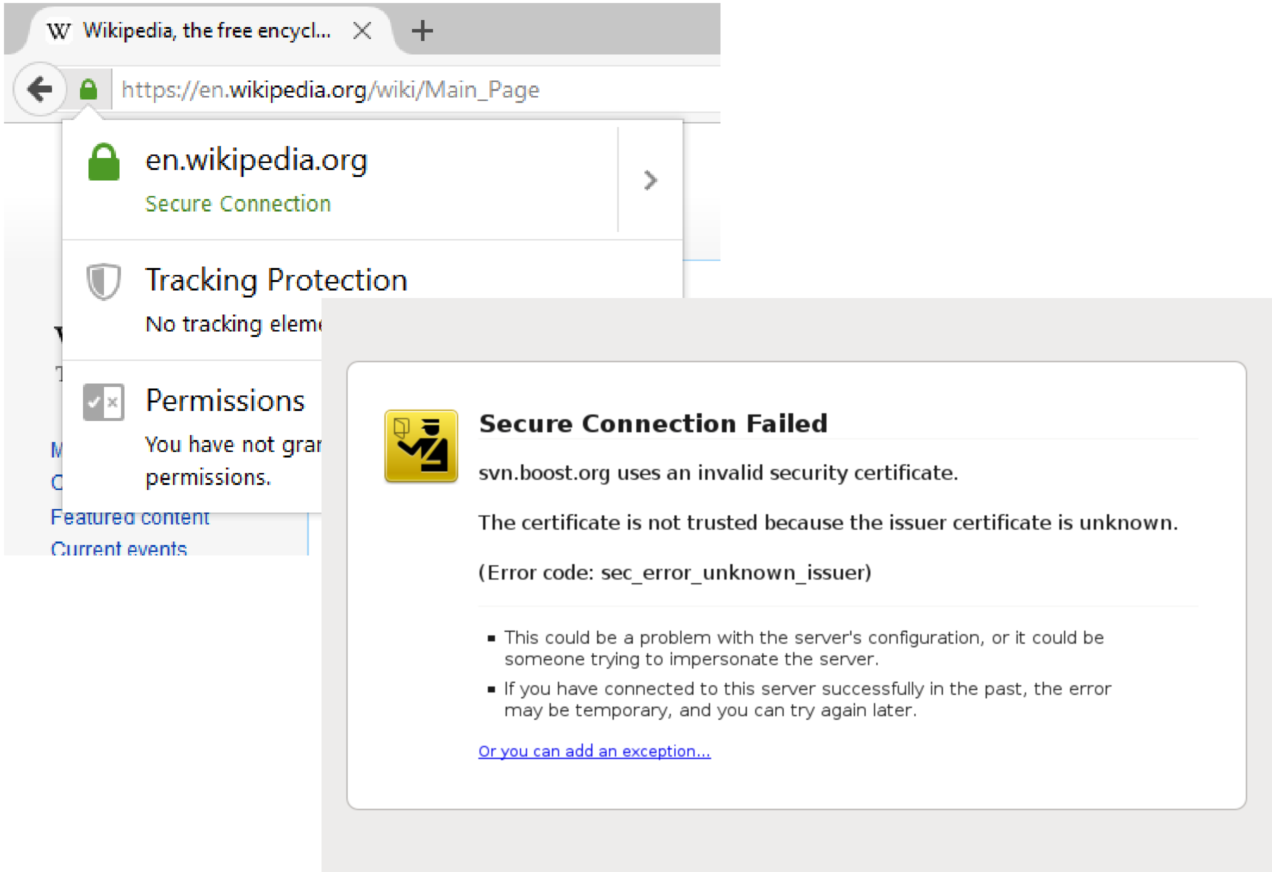
Secure Connection

You are securely connected to this site, run by:

Wikimedia Foundation, Inc.
San Francisco
California, US

Verified by: Symantec Corporation

More Information
ati
Imagine a worl



Wikipedia, the free encycl...
https://en.wikipedia.org/wiki/Main_Page

en.wikipedia.org

Secure Connection

Tracking Protection

No tracking elem

Permissions

You have not gran permissions.

Featured content
Current events

Secure Connection Failed

svn.boost.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception...

See also: Certificate Authority

HTTPS certificate

- We will use Let‘s encrypt
- Because it‘s free!

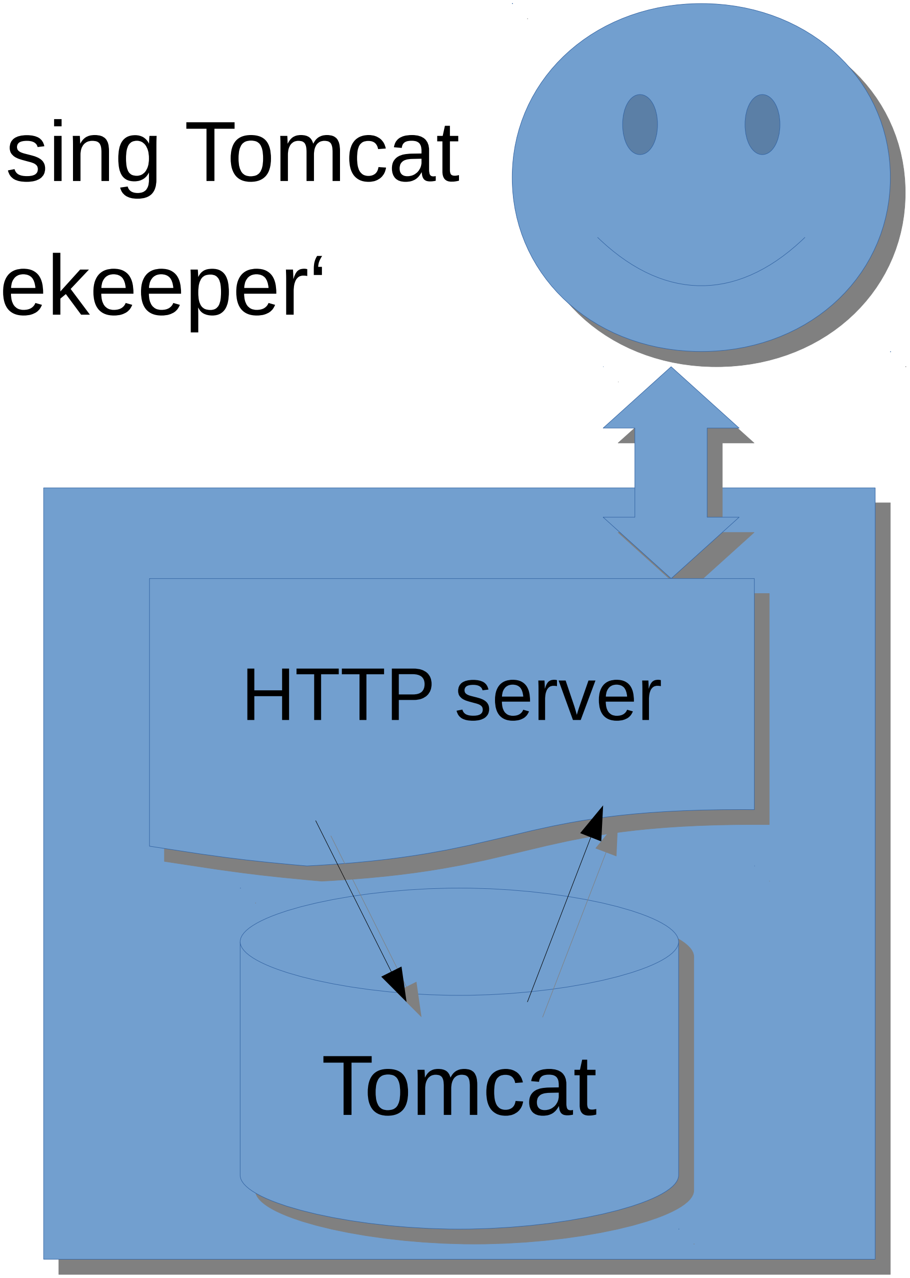
`https://letsencrypt.org/`

HTTPS certificate

- Cerifies that a domain belongs to a server
- Certificates only for domains
- DNS hack! `http://xip.io/`

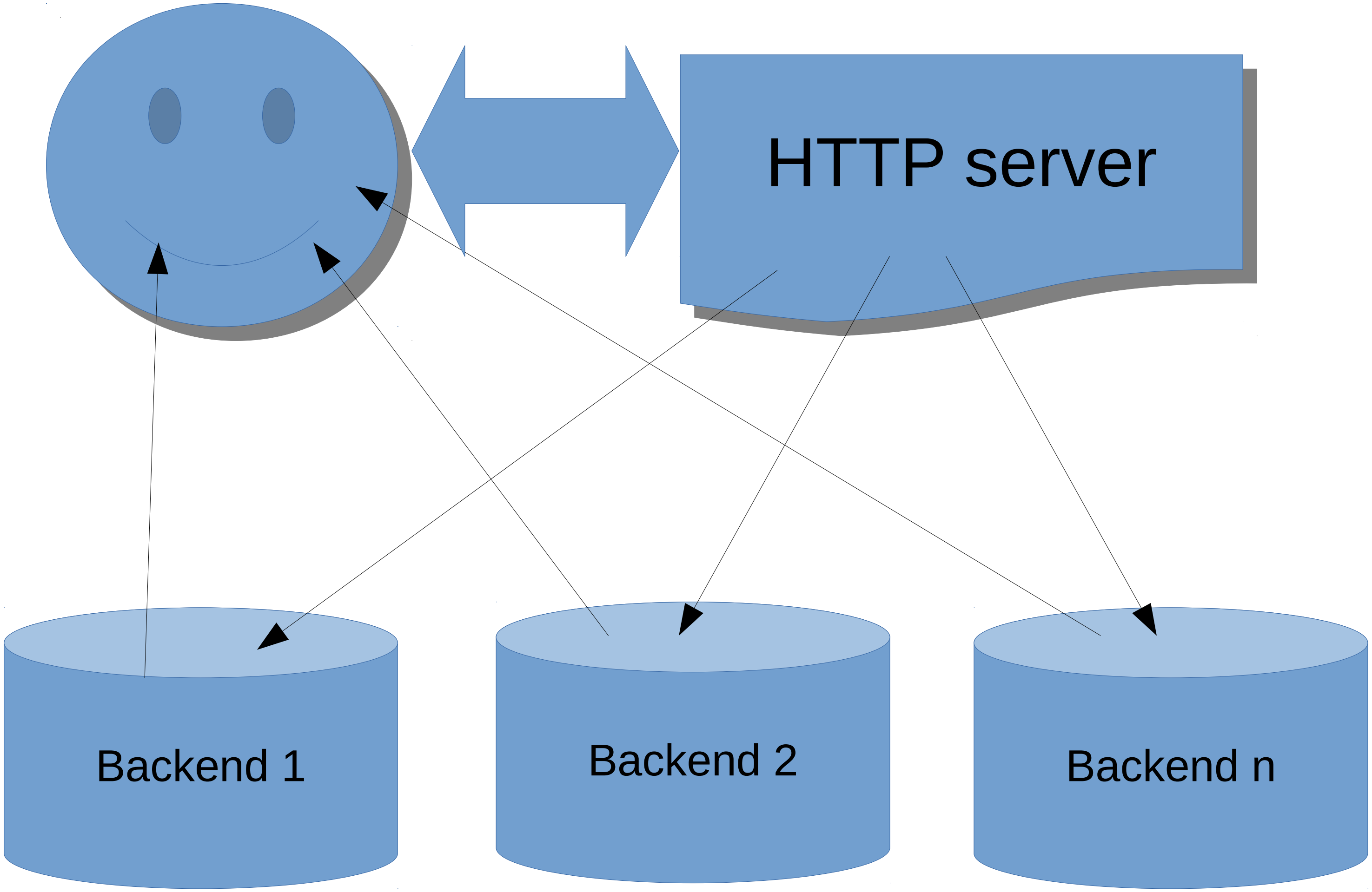
Reverse proxy

- It‘s possible to install using Tomcat
- We will be using a ‚gatekeeper‘
  - Reverse proxy



Load balancing

- How many connections can a computer have?
  - 65536



Our gatekeeper

- **Nginx**

In Ubuntu:

```
sudo apt-get install nginx
```

Now open port 80 on your host

HTTPS

- What port is used for HTTPS?
  - 443

- How can we fix this with the HTTP protocol?
  - Redirect
  - 301 Moved permanently

Installing certificate

- Let‘s encrypt Certbot

`https://certbot.eff.org/`

→ Choose Nginx and your OS

Exercises for today

1) Getting a Digital Ocean server running
2) Installing a reverse proxy
3) Installing a certificate via https://certbot.eff.org
4) Installing the certificate in Nginx
5) Watching the fruits of your labour!