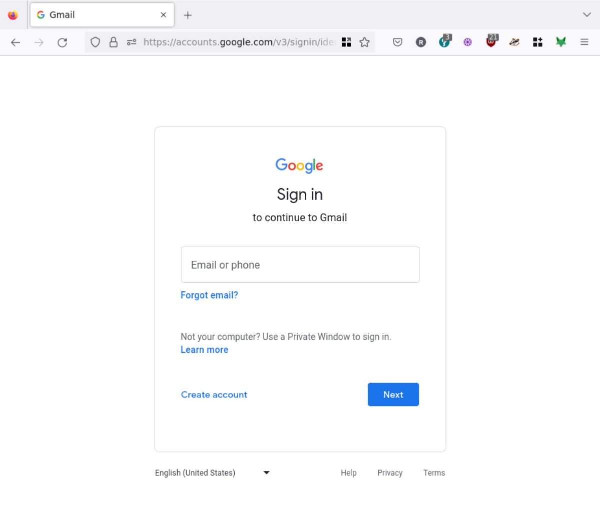
The web's public-key infrastructure

November 14, 2022

Rasmus Dahlberg

rasmus.dahlberg@kau.se

Are we really connected to the real Google?



https://accounts.google.com/v3/signin/ide

Google

Sign in

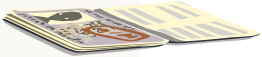
to continue to Gmail

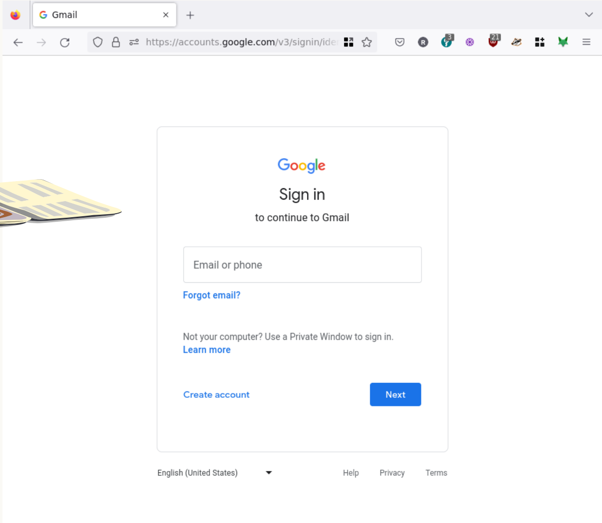
Email or phone

Forgot email?

Not your computer? Use a Private Window to sign in. Learn more

Are we really connected to the real Google?





Sign in

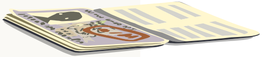
to continue to Gmail

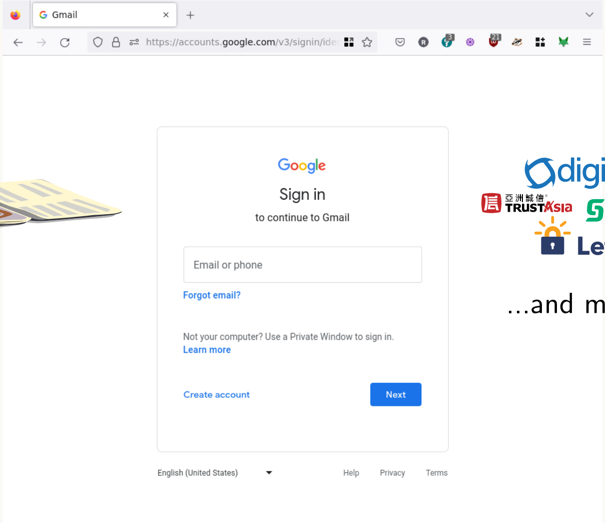
Email or phone

Forgot email?

Not your computer? Use a Private Window to sign in.
Learn more

Are we really connected to the real Google?





Google

Sign in

to continue to Gmail

Email or phone

Not your computer? Use a Private Window to sign in.

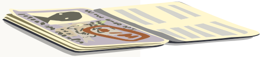
digicert® Google

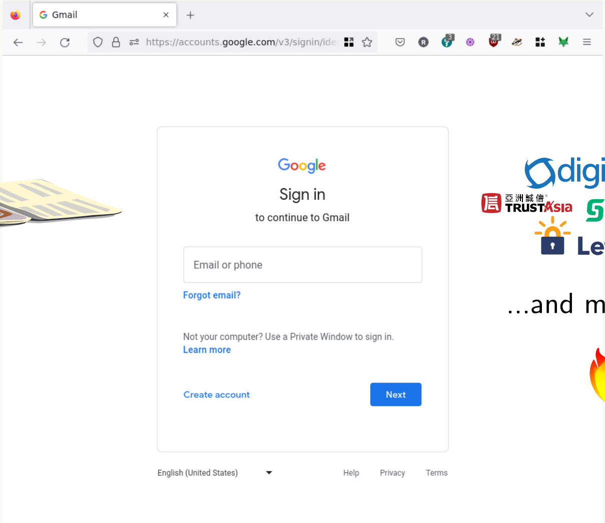
亞洲誠信® TRUSTAsia SECTIGO®

Let's Encrypt

...and many more

Are we really connected to the real Google?





Gmail

https://accounts.google.com/v3/signin/ide

Google

Sign in

to continue to Gmail

Email or phone

Forgot email?

Not your computer? Use a Private Window to sign in. Learn more

Create account

Next

English (United States)

Help Privacy Terms

digicert® Google

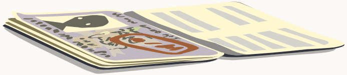
亞洲誠信 TRUSTAsia SECTIGO®

Let's Encrypt

…and many more

[1] Summary of the DigiNotar incidence: https://www.enisa.europa.eu/media/news-items/operation-black-tulip/ (2011)

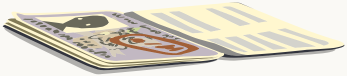
Learning outcomes



X.509 certificates

Format, fields, ...

Learning outcomes



X.509 certificates

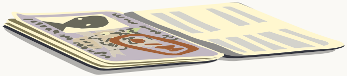
Format, fields, ...

digicert®
Google
亞洲誠信® TRUSTAsia
SECTIGO®
Let's Encrypt

Certificate Authorities

Ecosystem, validation, ...

Learning outcomes

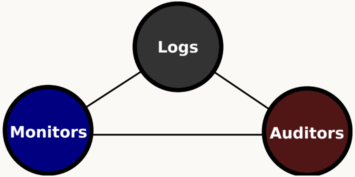


X.509 certificates

Format, fields, …

Certificate Authorities

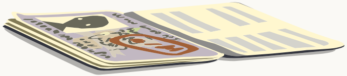
Ecosystem, validation, …



Certificate Transparency

Theory, practise, …

Learning outcomes

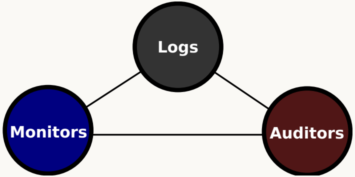


X.509 certificates

Format, fields, …

Certificate Authorities

Ecosystem, validation, …

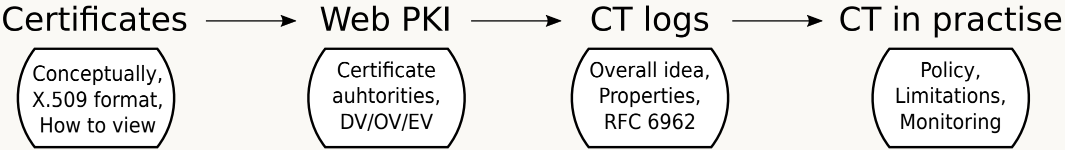


Certificate Transparency

Theory, practise, …

Why is this useful for me?

Middle part—Cronological



Certificates → Web PKI → CT logs → CT in practise

Certificates: Conceptually, X.509 format, How to view

Web PKI: Certificate auhtorities, DV/OV/EV

CT logs: Overall idea, Properties, RFC 6962

CT in practise: Policy, Limitations, Monitoring

Middle part—Segway to the end

CT logs and monitoring → no undeteted DigiNotar-style attacks

Middle part—Example of engagement

Select all statements that are true:

□ An X.509 certificate proves ownership of a website

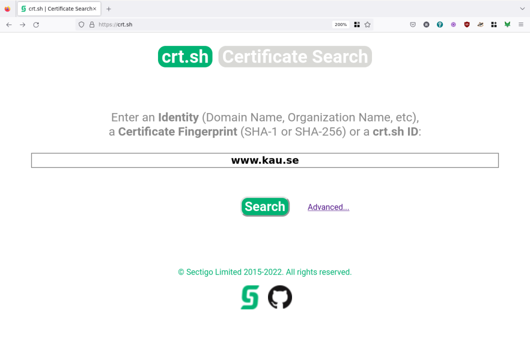
□ An EV certificate is more secure than a DV certificate

□ Only Swedish CAs can issue `.se` certificates

□ There are hundreds of CAs across the globe

Take away

- X.509 certificates
  - “Driver’s licence for websites”
  - Am I connected to the right site?
- Certificate Authorities (CAs)
  - “Transportstyrelsen for websites”
  - DV/OV/EV validated certificates
  - Weakest-link security
- Certificate Transparency (CT)
  - Holds CAs accountable (detection)
  - Enforced by Chrome, Safari, Edge
  - Monitor your own websites



crt.sh Certificate Search

Enter an **Identity** (Domain Name, Organization Name, etc),
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

www.kau.se

Search   Advanced...

© Sectigo Limited 2015-2022. All rights reserved.