



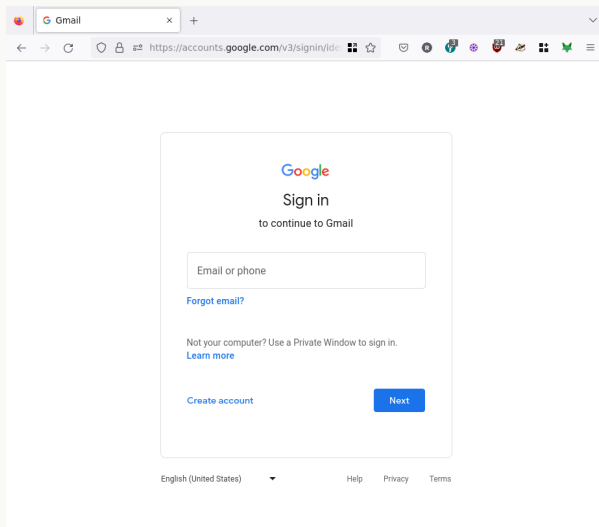
The web's public-key infrastructure

November 14, 2022

Rasmus Dahlberg

`rasmus.dahlberg@kau.se`

Are we really connected to the real Google?



The image shows a web browser window with the address bar displaying "https://accounts.google.com/v3/signin/ide". The page content is a sign-in form for Gmail. At the top, it says "Google" in its multi-colored logo, followed by "Sign in" and "to continue to Gmail". Below this is a text input field labeled "Email or phone". Under the input field is a link "Forgot email?". Further down, it says "Not your computer? Use a Private Window to sign in." followed by a link "Learn more". At the bottom left of the form is a link "Create account", and at the bottom right is a blue button labeled "Next". Below the form, at the very bottom of the page, are links for "English (United States)" (with a dropdown arrow), "Help", "Privacy", and "Terms".

Gmail

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

Google

Sign in
to continue to Gmail

Email or phone

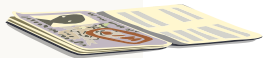
[Forgot email?](#)

Not your computer? Use a Private Window to sign in.
[Learn more](#)

[Create account](#) [Next](#)

English (United States) [Help](#) [Privacy](#) [Terms](#)

Are we really connected to the real Google?

A screenshot of a web browser showing the Google Sign-in page for Gmail. The browser's address bar displays the URL "https://accounts.google.com/v3/signin/ide". The page features the Google logo at the top, followed by the text "Sign in to continue to Gmail". Below this is a text input field labeled "Email or phone". A link for "Forgot email?" is positioned below the input field. A message states "Not your computer? Use a Private Window to sign in." with a "Learn more" link. At the bottom of the sign-in box are links for "Create account" and a blue "Next" button. The footer of the page includes "English (United States)" with a dropdown arrow, and links for "Help", "Privacy", and "Terms".

Gmail

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

Google

Sign in
to continue to Gmail

Email or phone

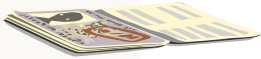
[Forgot email?](#)


Not your computer? Use a Private Window to sign in.
[Learn more](#)



[Create account](#) [Next](#)


English (United States) [Help](#) [Privacy](#) [Terms](#)

Are we really connected to the real Google?



 Gmail x +

← → ↻  <https://accounts.google.com/v3/signin/ide> 


Sign in
to continue to Gmail

[Forgot email?](#)

Not your computer? Use a Private Window to sign in.
[Learn more](#)


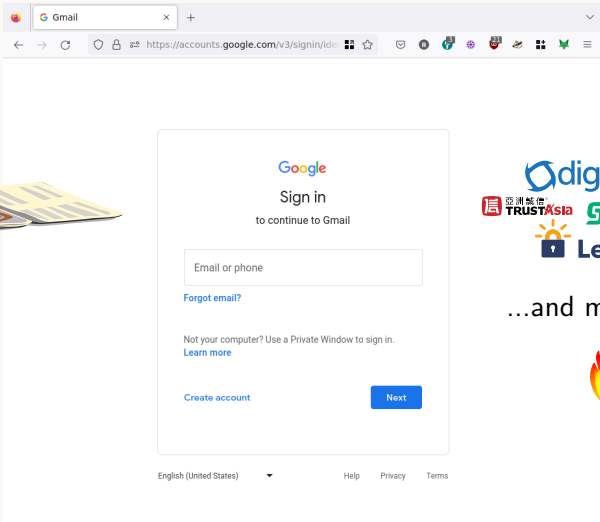
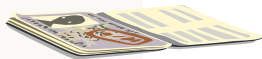
[Create account](#) [Next](#)

English (United States) ▼ [Help](#) [Privacy](#) [Terms](#)




...and many more

Are we really connected to the real Google?



...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, ...



Certificate Authorities
Ecosystem, validation, ...

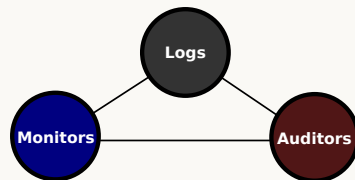
Learning outcomes



X.509 certificates
Format, fields, ...



Certificate Authorities
Ecosystem, validation, ...



Certificate Transparency
Theory, practise, ...

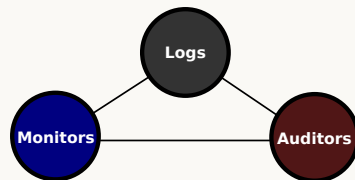
Learning outcomes



X.509 certificates
Format, fields, ...



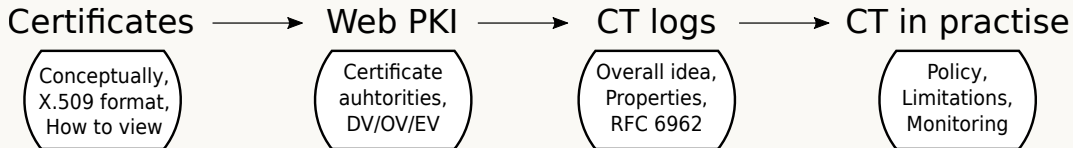
Certificate Authorities
Ecosystem, validation, ...



Certificate Transparency
Theory, practise, ...

Why is this useful for me?

Middle part—Cronological



Middle part—Segway to the end

CT logs and monitoring → no undetected 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

