Certificate Transparency Root Explorer

Nikita Korzhitskii
Niklas Carlsson

LINKÖPINGS UNIVERSITET

Web Public Key Infrastructure (WebPKI)

Root certificates of trusted Certificate Authorities
e.g. GlobalSign Root CA, Amazon Root CA, GoDaddy Root CA

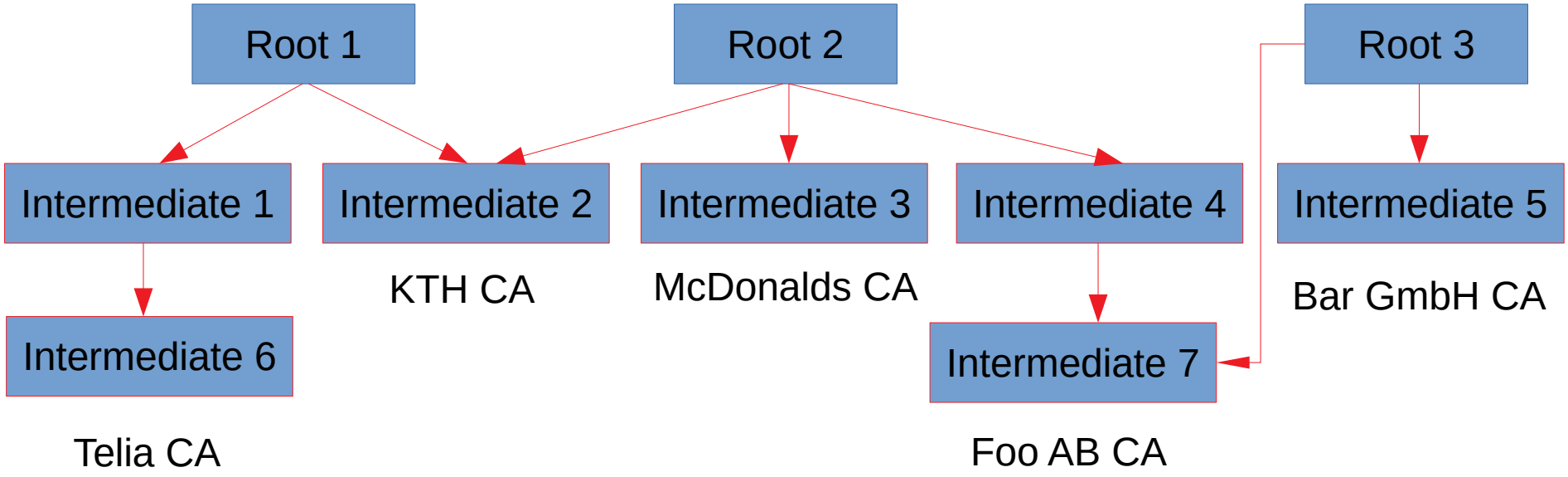
Root 1

Root 2

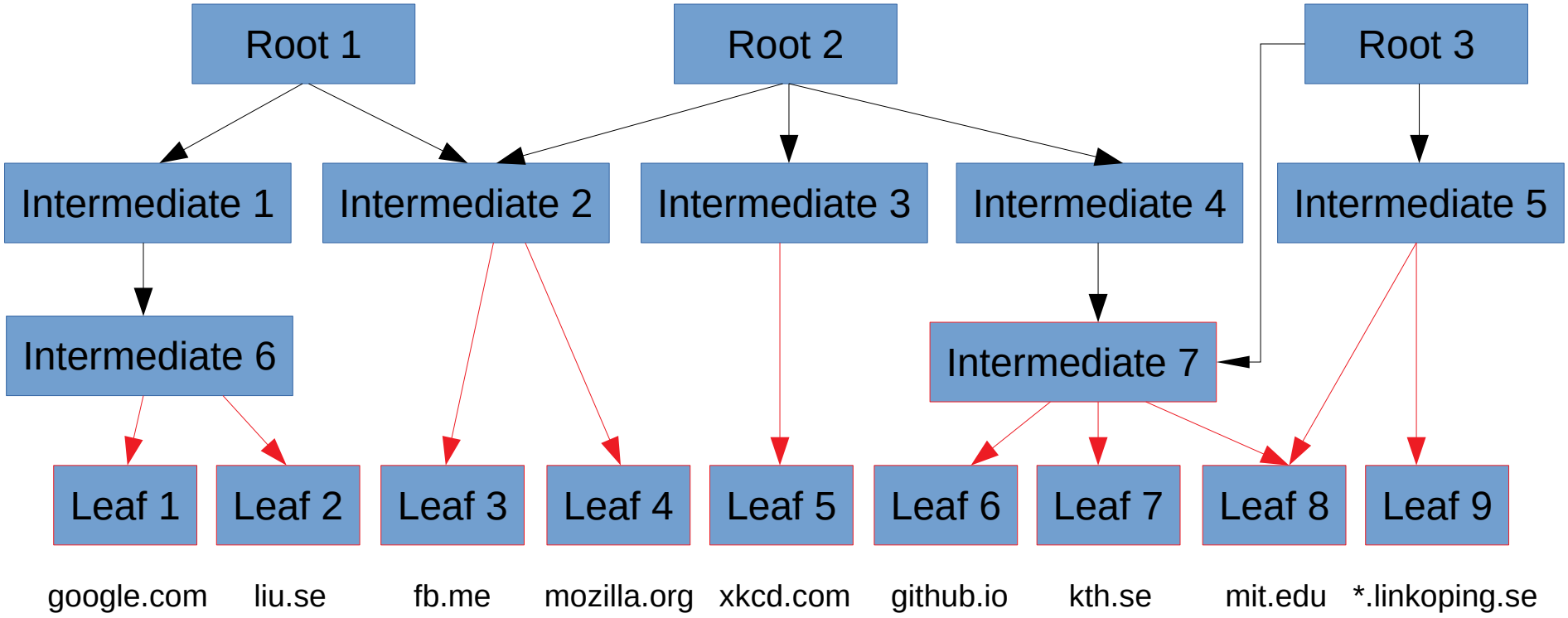
Root 3

Web Public Key Infrastructure (WebPKI)

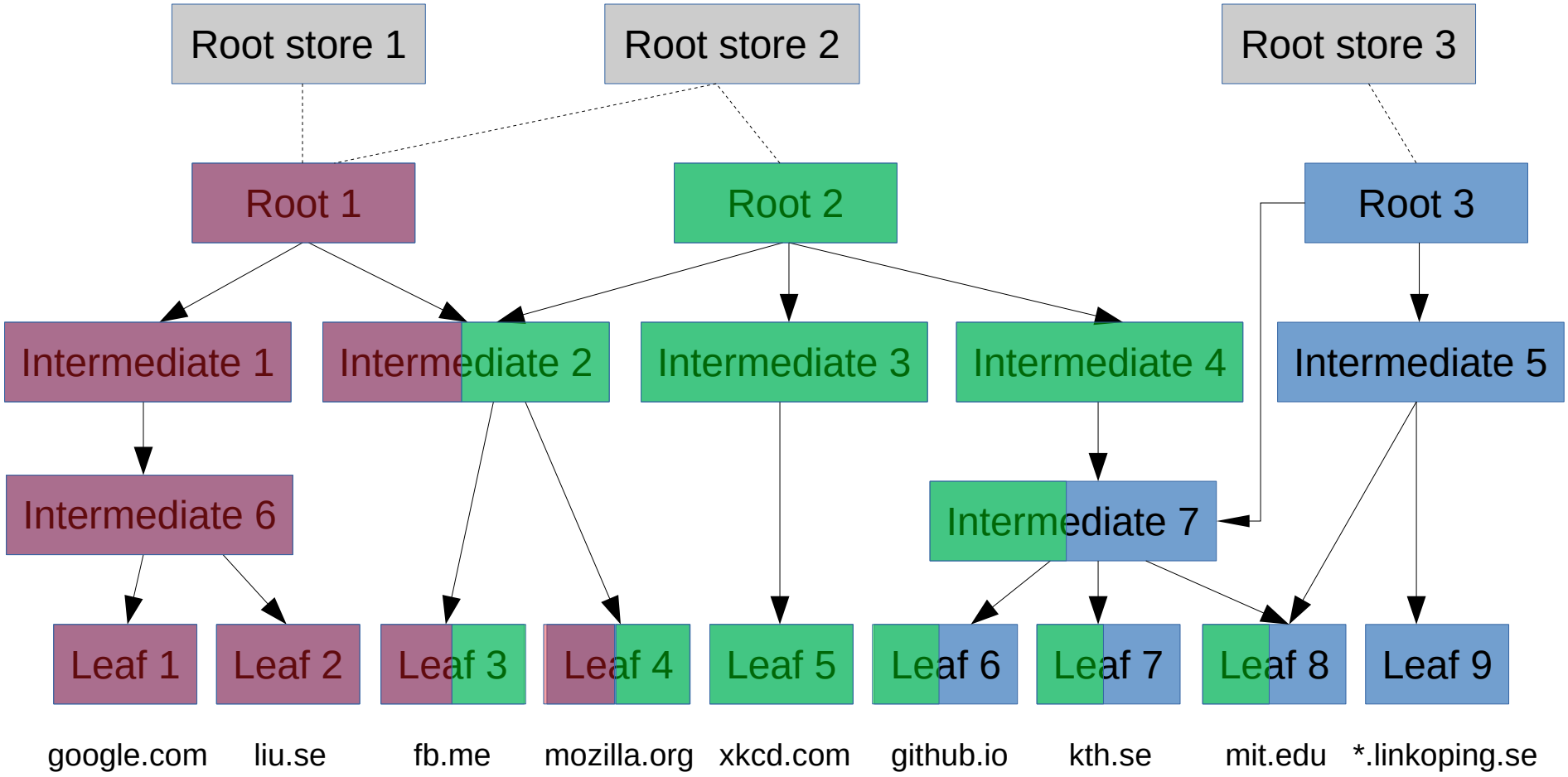
Root CAs issue Intermediate certificates to themselves or other organizations.



Web Public Key Infrastructure (WebPKI)



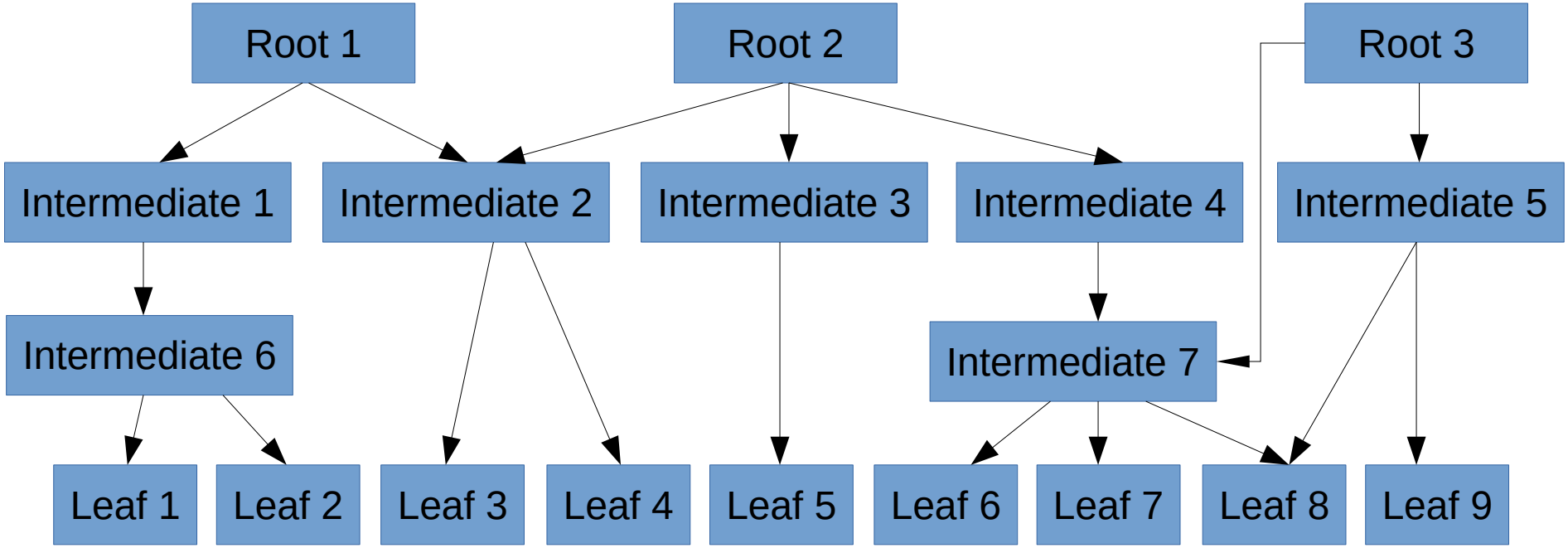
Web Public Key Infrastructure (WebPKI)



Client w/ Root Store 1: google.com, liu.se, fb.me, mozilla.org
Client w/ Root Store 2: google.com, liu.se, fb.me, mozilla.org, xkcd.com, github.io, kth.se, mit.edu
Client w/ Root Store 3: github.io, kth.se, mit.edu, *.linkoping.se

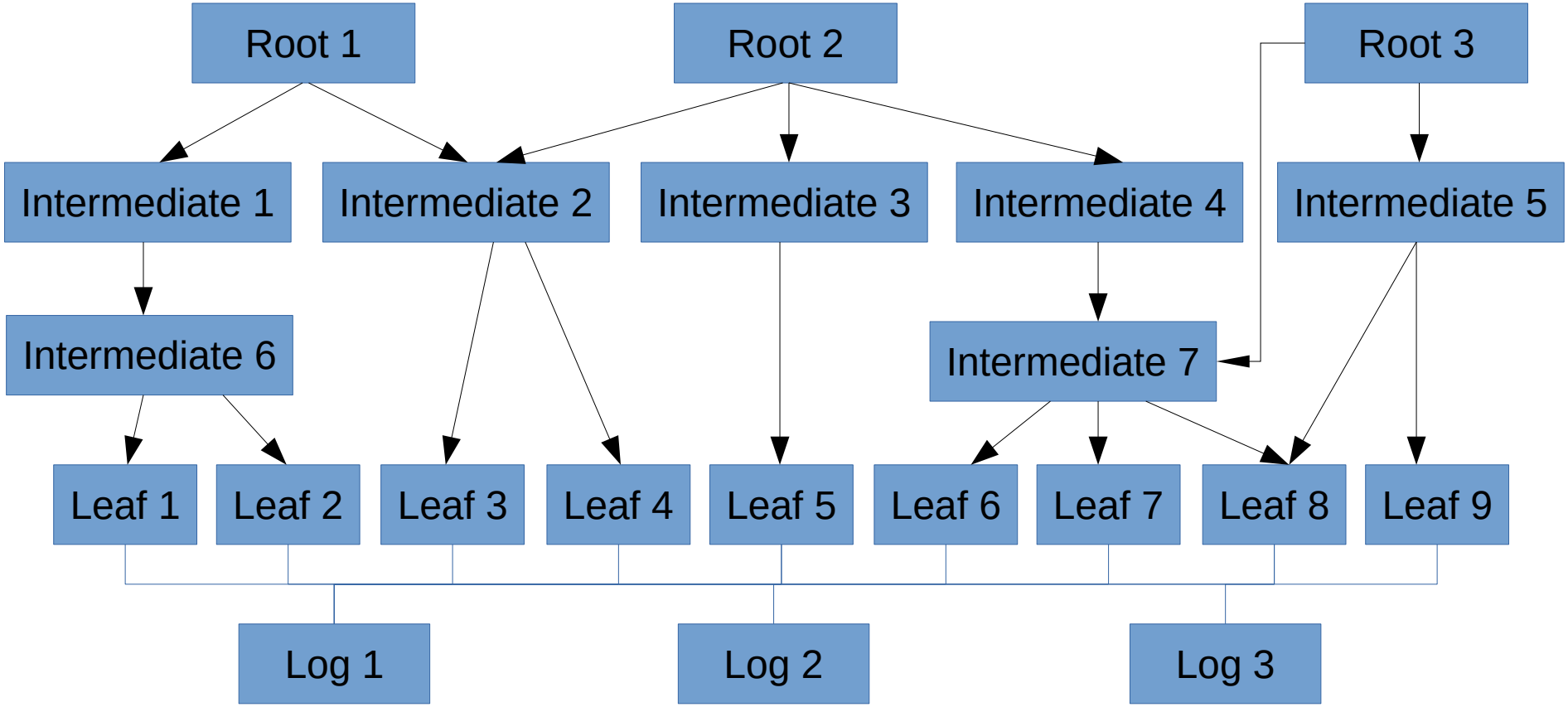
Certificate Transparency

- An internet standard, RFC 6962
- Append-only logging of issued certificates

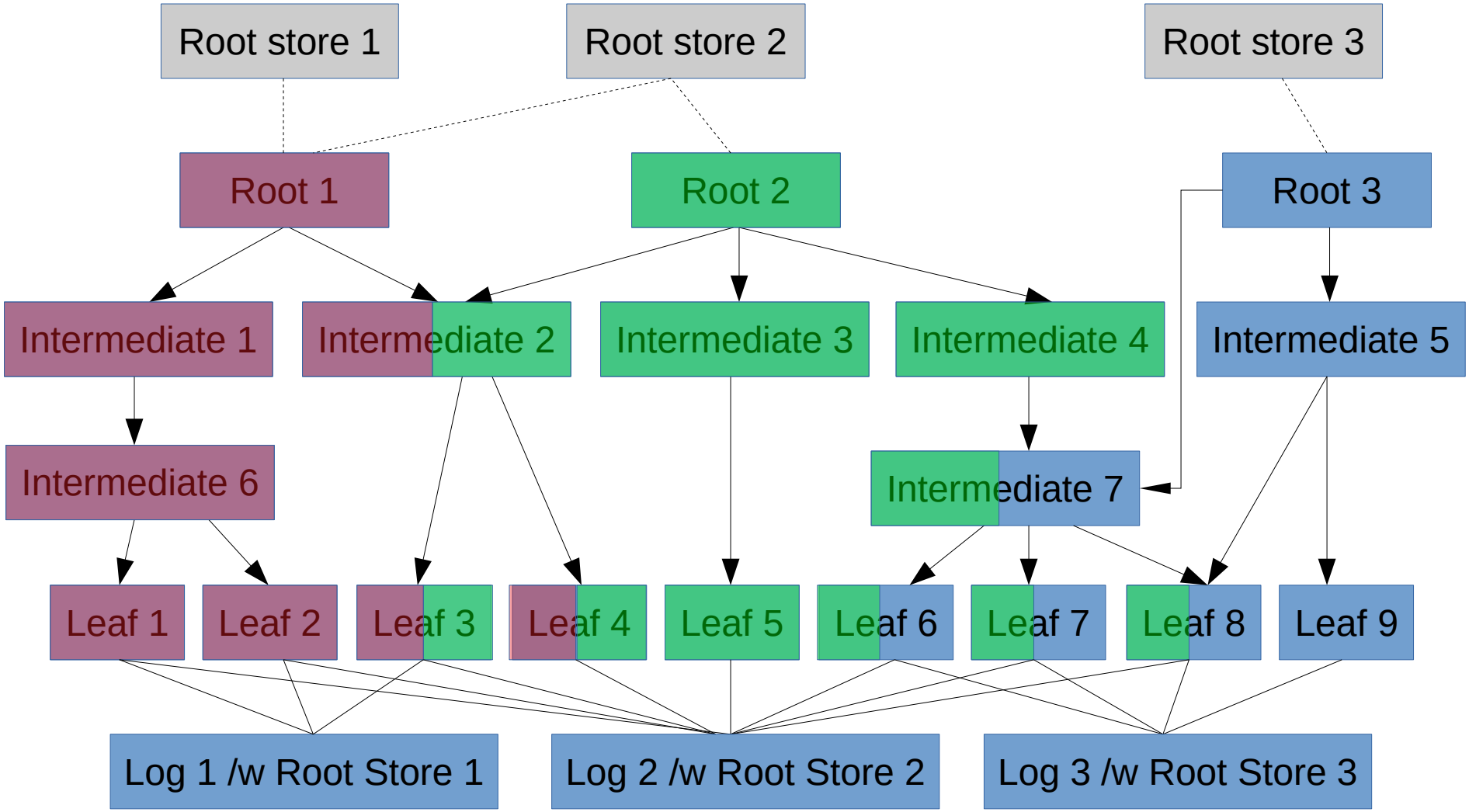


Certificate Transparency

- An internet standard, RFC 6962
- Append-only logging of issued certificates



Certificate Transparency (in practice)



Certificate Transparency

- A *CT log* is a signed binary append-only Merkle tree of certificate chains
- Any party can submit certificates
- Logs can be checked for consistency

- Initially developed and adopted by Google
- Recently adopted by Apple
- Most CAs log their certificates upon issuance
- CT extends beyond WebPKI to RPKI

Applications of Certificate Transparency

- Connection verification
- Detection of misissued certificates
- Detection of active, phishing, other domains (privacy issues)
- Representation of the Internet structure
- Many more…

We are interested in end-to-end security applications of CT

Certificate Transparency Root Explorer

...is a tool for exploring certificate stores.

One can visualize intersections, compare, parse, search and export certificate information.

An SQLite database of logs and roots could be imported and exported.

CT logs could be scanned online.

Available root stores (Snapshot from 27th December, 2018):

Mozilla, Microsoft, Apple and multiple Certificate Transparency Logs.

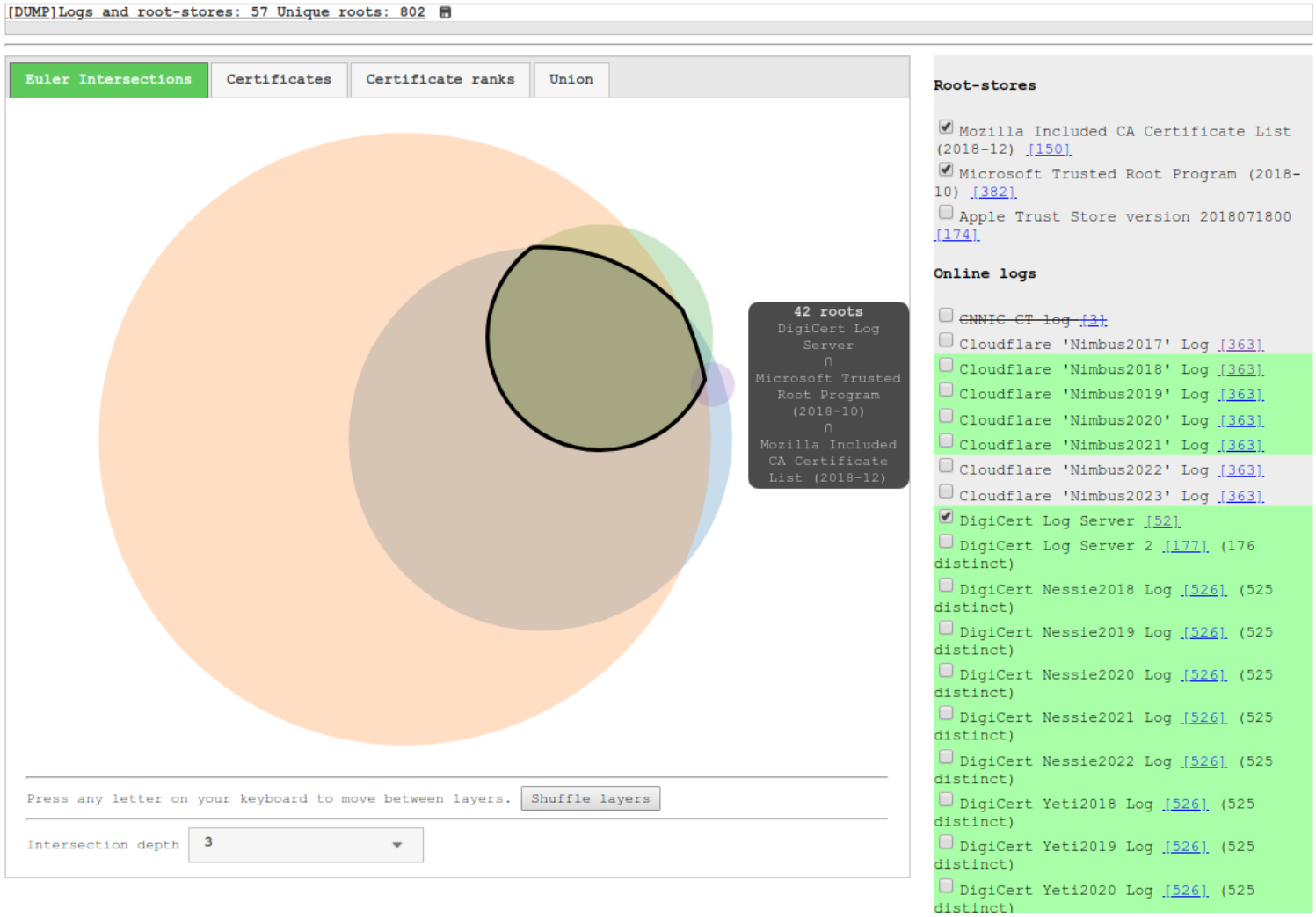
Requirements:

Chrome or Chromium Browser.

By default, only logs by Google are available for live log scanning. The rest of the logs have not explicitly configured response headers related to the CORS policy.

GitHub: nikita-kun/certificate-transparency-root-explorer

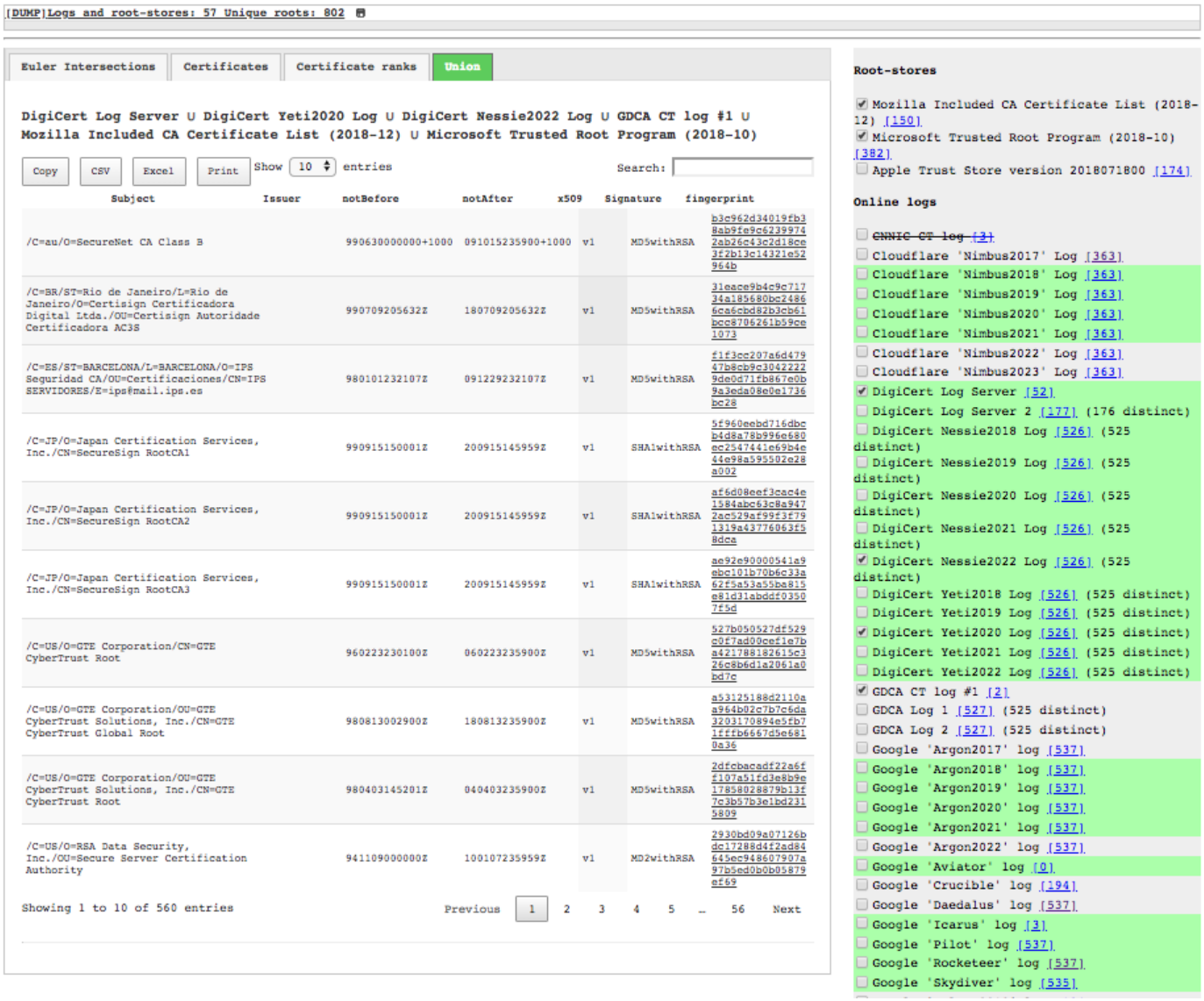
Certificate Transparency Root Explorer



LINKÖPINGS UNIVERSITET

GitHub: nikita-kun/certificate-transparency-root-explorer

Certificate Transparency Root Explorer



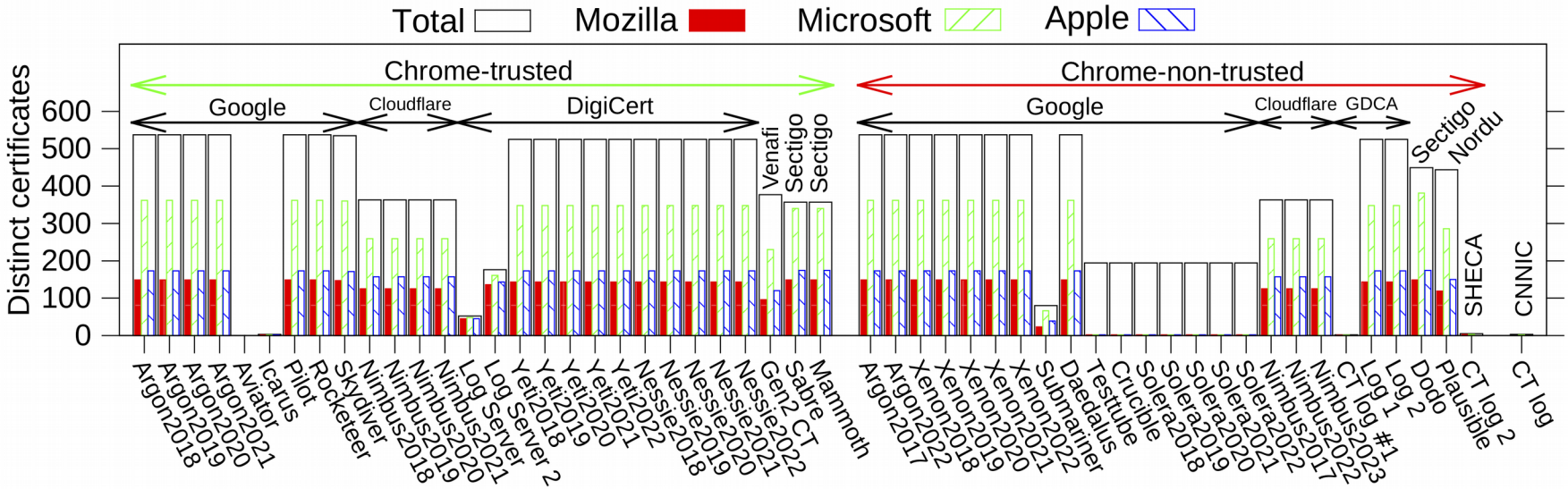
LINKÖPINGS UNIVERSITET

GitHub: nikita-kun/certificate-transparency-root-explorer

The dataset

- Collected on December 27th, 2018
- 56 CT logs (54 were mentioned in Google's list of known logs)
- 3 Vendor Root Stores
- 802 Root/Intermediate Certificate

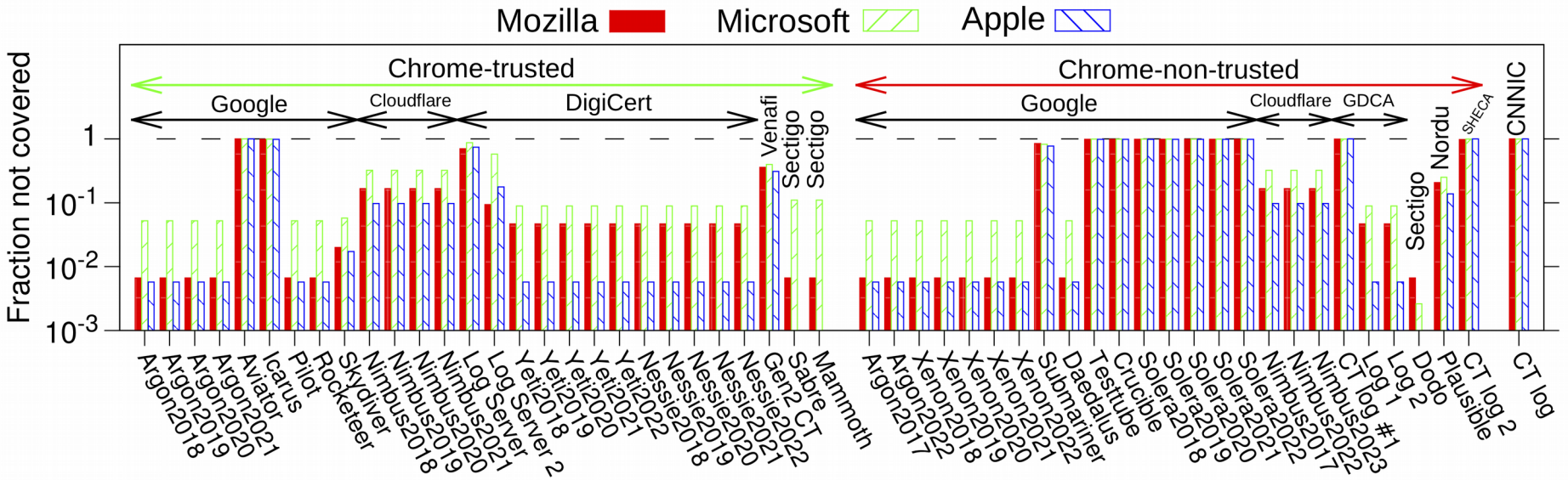
Certificates in root stores of CT logs and their relation to major vendor root stores



In order to enable
attribution of each logged certificate to its issuer, the log SHALL
publish a list of acceptable root certificates
(this list might usefully be the union of root certificates trusted by major browser vendors).

RFC 6962

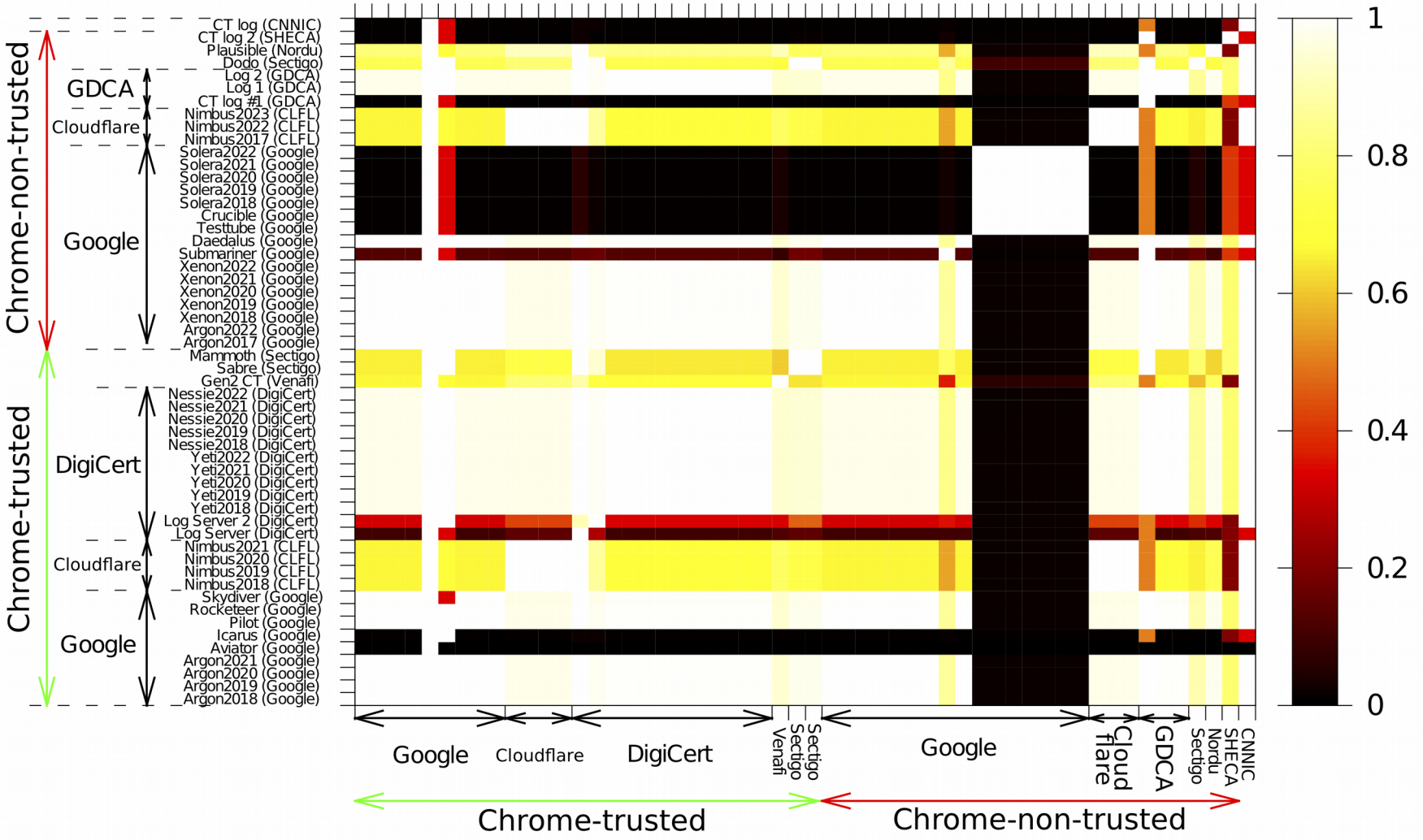
Fraction of trusted vendor certificates not covered by CT logs



In order to enable
attribution of each logged certificate to its issuer, the log SHALL
publish a list of acceptable root certificates
(this list might usefully be the union of root certificates trusted by major browser vendors).

RFC 6962

Intersections of Logs' root stores

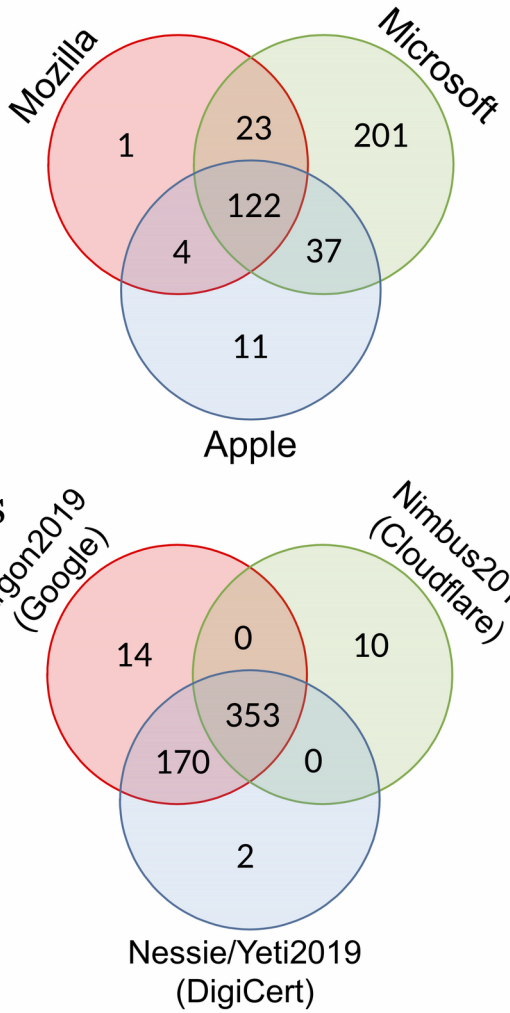


Conclusion

- Certificate Transparency is rapidly developing
- As of January 2019, CT logs contained 3 billion entries
- CT is already in your Chrome browser and Apple OSes
- Many potential applications

However:

- Internet is not fully covered by CT
- Google and Apple rely on logs maintained by 4 operators
  - ➔ Cloudflare, DigiCert, Google and Sectigo



Intersection of root stores by Mozilla, Microsoft and Apple (top); Argon2019, Nimbus2019 and Nessie/Yeti2019 logs (bottom)

Thank you!

www.liu.se

LINKÖPINGS UNIVERSITET