

# Certificate Transparency Root Explorer

Nikita Korzhitskii  
Niklas Carlsson

# Web Public Key Infrastructure (WebPKI)

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

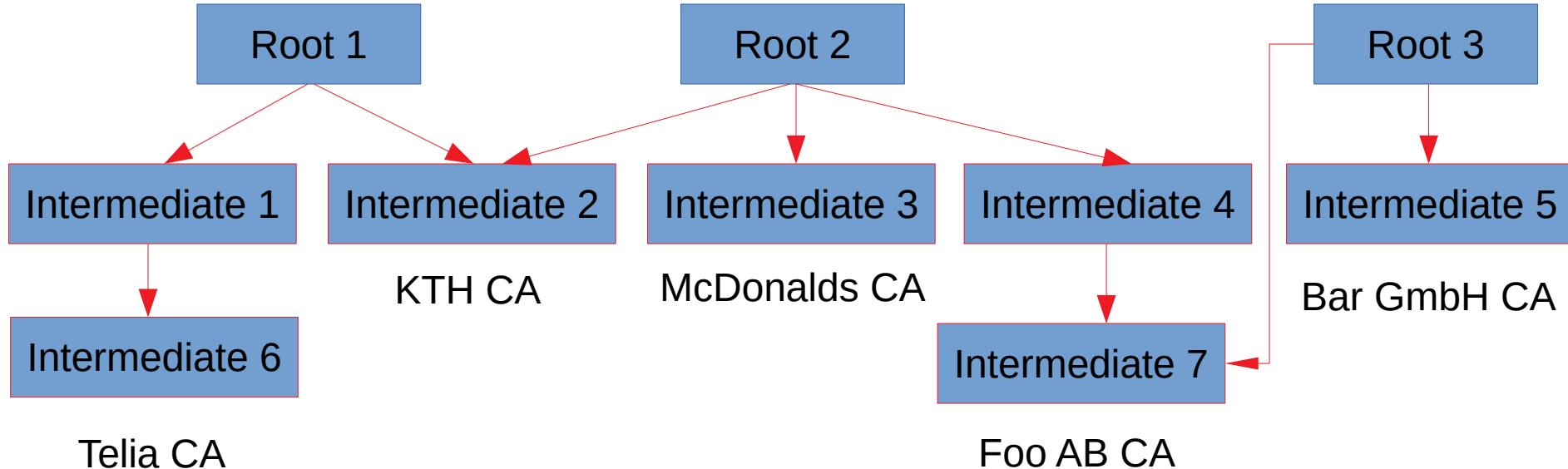
Root 1

Root 2

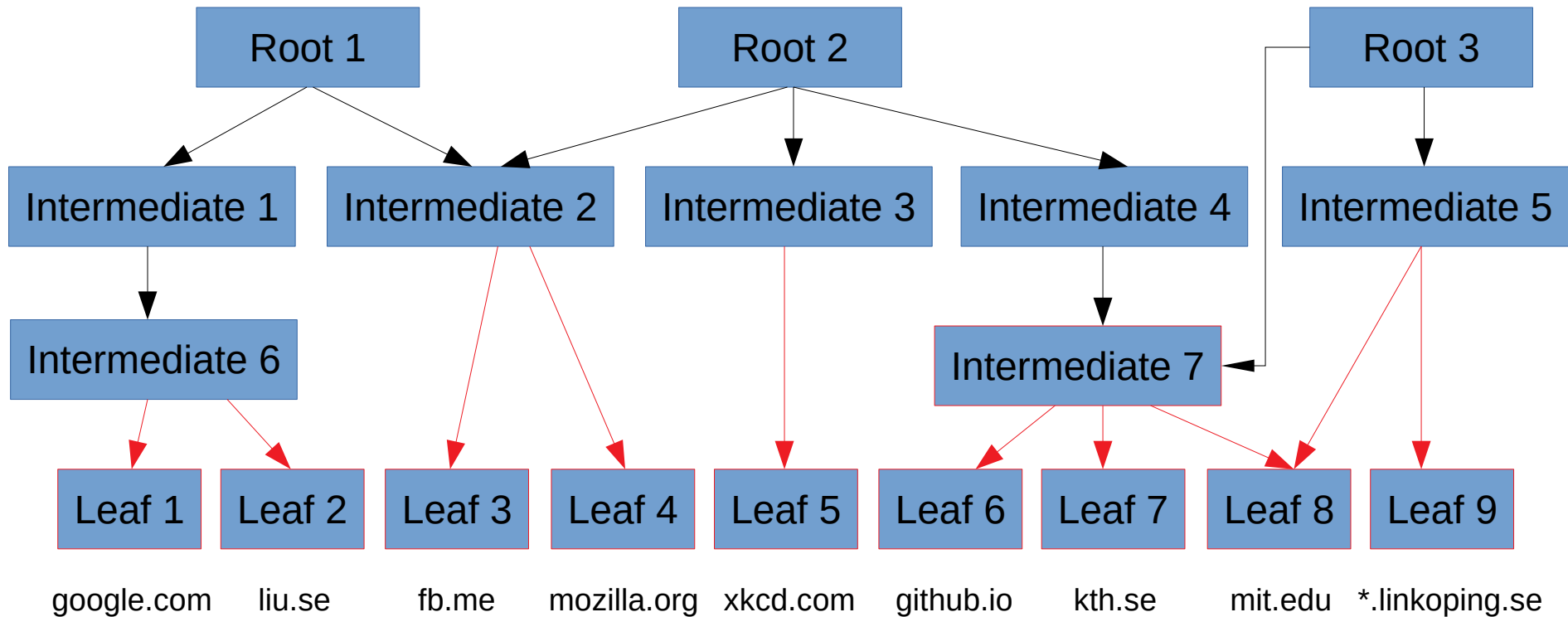
Root 3

# Web Public Key Infrastructure (WebPKI)

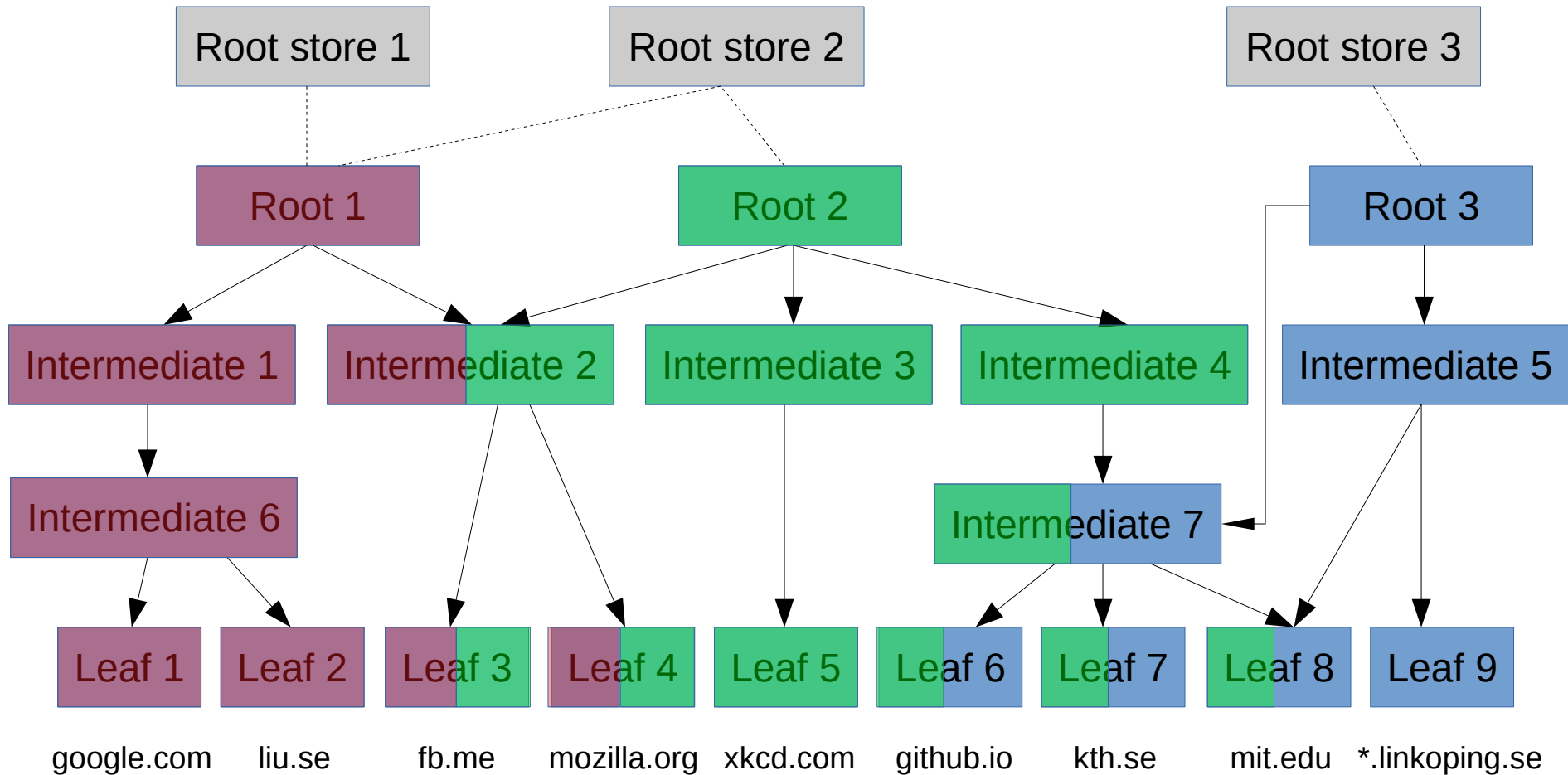
Root CAs issue Intermediate certificates to themselves or other organizations.



# Web Public Key Infrastructure (WebPKI)



# Web Public Key Infrastructure (WebPKI)



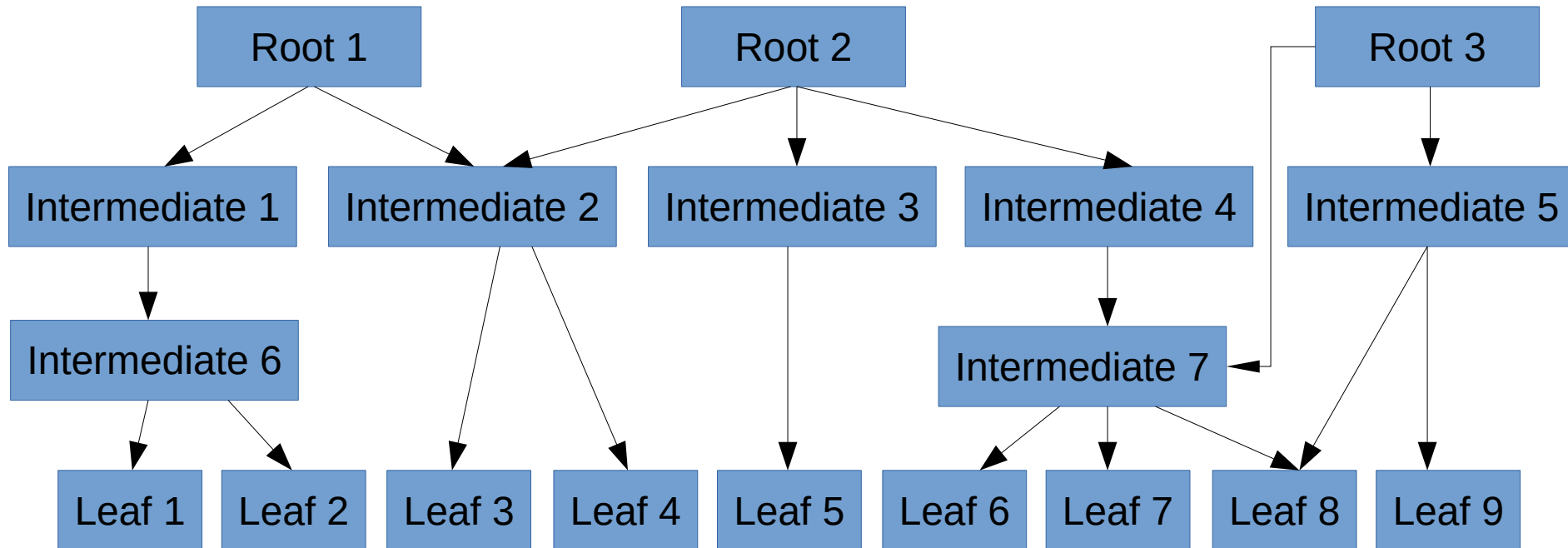
Client w/ Root Store 1: google.com, liu.se, fb.me, mozilla.org

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

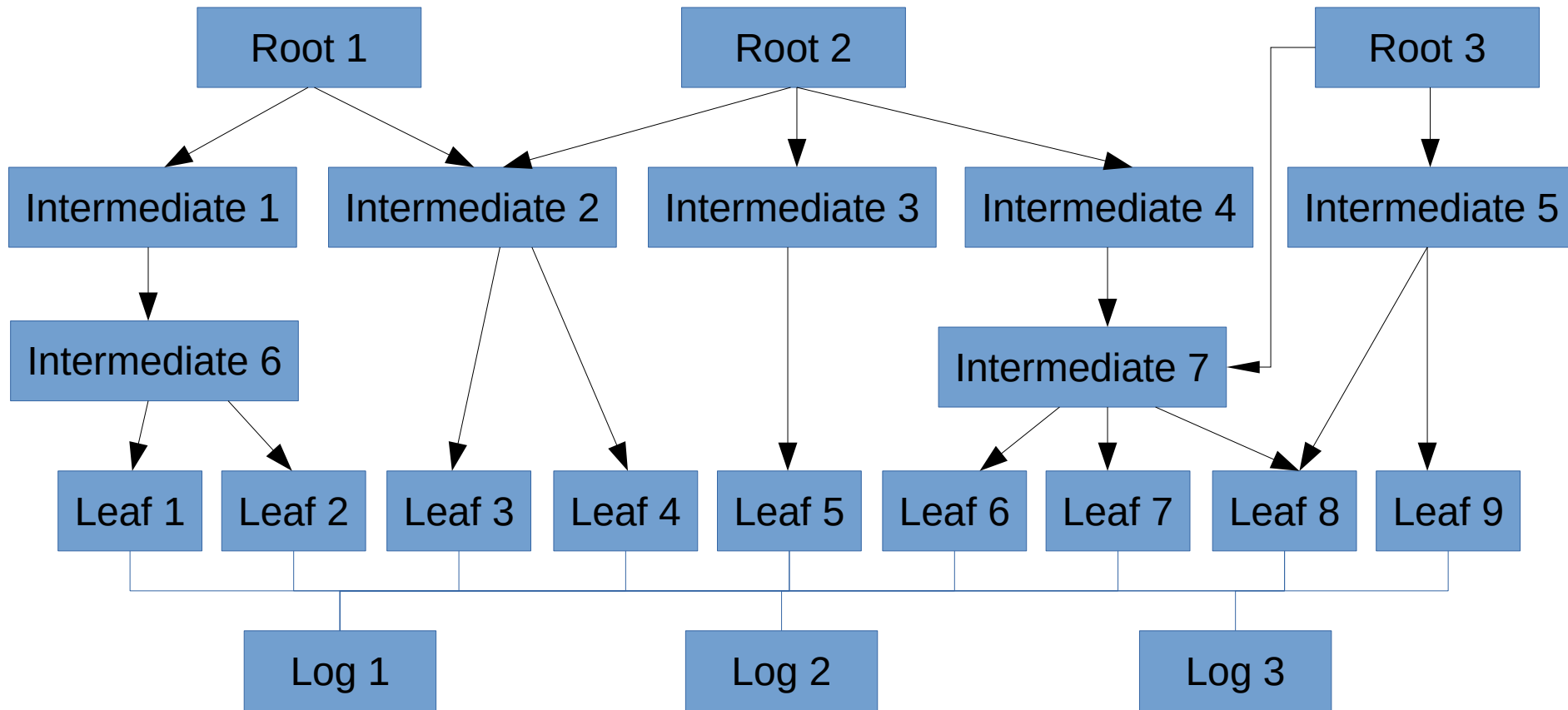
# Certificate Transparency

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

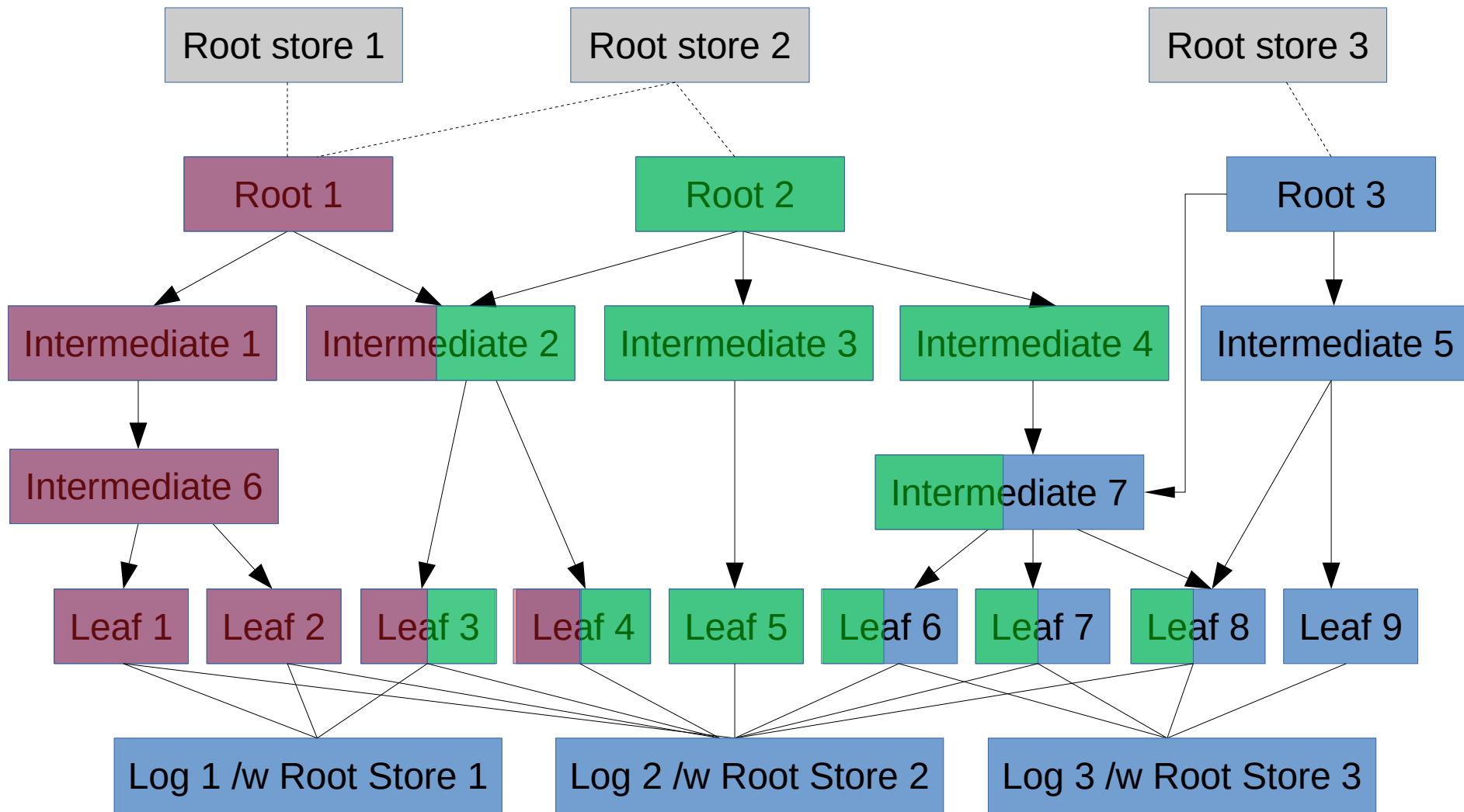


# Certificate Transparency

- 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.



# Certificate Transparency Root Explorer

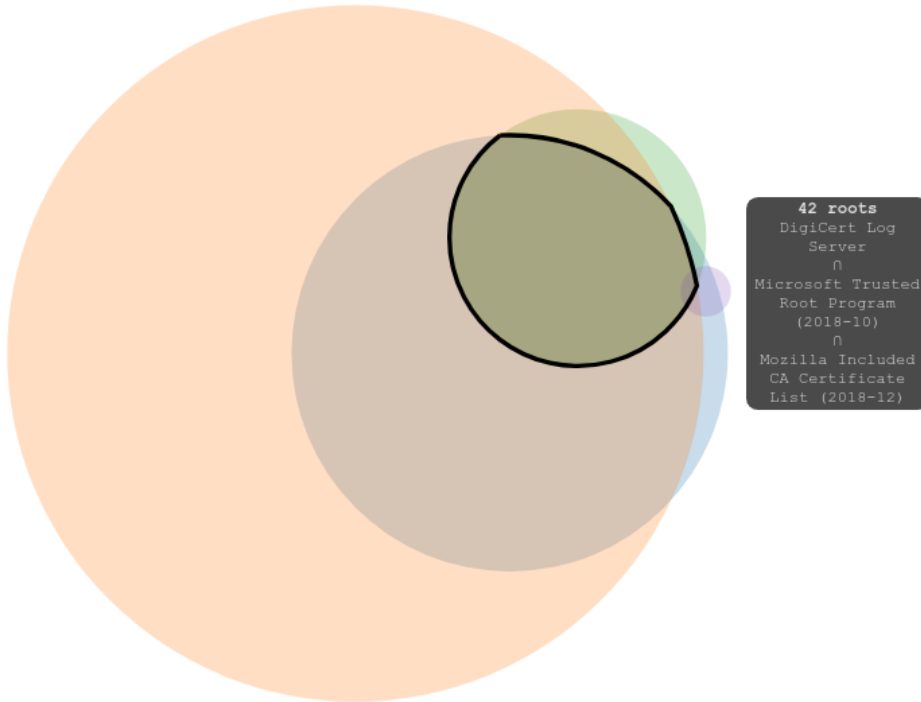
[DUMP] Logs and root-stores: 57 Unique roots: 802

Euler Intersections

Certificates

Certificate ranks

Union



Press any letter on your keyboard to move between layers.

Shuffle layers

Intersection depth

3

## Root-stores

- ☒ Mozilla Included CA Certificate List (2018-12) [\[150\]](#)
- ☒ Microsoft Trusted Root Program (2018-10) [\[382\]](#)
- ☐ Apple Trust Store version 2018071800 [\[174\]](#)

## Online logs

- ☐ CNNIC CT log [\[2\]](#)
- ☐ Cloudflare 'Nimbus2017' Log [\[363\]](#)
- ☐ Cloudflare 'Nimbus2018' Log [\[363\]](#)
- ☐ Cloudflare 'Nimbus2019' Log [\[363\]](#)
- ☐ Cloudflare 'Nimbus2020' Log [\[363\]](#)
- ☐ Cloudflare 'Nimbus2021' Log [\[363\]](#)
- ☐ Cloudflare 'Nimbus2022' Log [\[363\]](#)
- ☐ Cloudflare 'Nimbus2023' Log [\[363\]](#)
- ☒ DigiCert Log Server [\[32\]](#)
- ☐ DigiCert Log Server 2 [\[177\]](#) (176 distinct)
- ☐ DigiCert Nessie2018 Log [\[526\]](#) (525 distinct)
- ☐ DigiCert Nessie2019 Log [\[526\]](#) (525 distinct)
- ☐ DigiCert Nessie2020 Log [\[526\]](#) (525 distinct)
- ☐ DigiCert Nessie2021 Log [\[526\]](#) (525 distinct)
- ☐ DigiCert Nessie2022 Log [\[526\]](#) (525 distinct)
- ☐ DigiCert Yeti2018 Log [\[526\]](#) (525 distinct)
- ☐ DigiCert Yeti2019 Log [\[526\]](#) (525 distinct)
- ☐ DigiCert Yeti2020 Log [\[526\]](#) (525 distinct)



# Certificate Transparency Root Explorer

[DUMP] Logs and root-stores: 57 Unique roots: 802

Euler Intersections Certificates Certificate ranks **Union**

DigiCert Log Server U DigiCert Yeti2020 Log U DigiCert Nessie2022 Log U GDCA CT log #1 U Mozilla Included CA Certificate List (2018-12) U Microsoft Trusted Root Program (2018-10)

Copy CSV Excel Print Show 10 entries Search:

Subject	Issuer	notBefore	notAfter	x509	Signature	fingerprint
/C=au/O=SecureNet CA Class B		990630000000+1000	091015235900+1000	v1	MD5withRSA	b3c962d34019fb1 8ab9fe9c6229974 2ab26c43c2d18ce 3f2b13c14321e52 964b
/C=BR/ST=Rio de Janeiro/L=Rio de Janeiro/O=Certisign Certificadora Digital Ltda./OU=Certisign Autoridade Certificadora AC3S		990709205632Z	180709205632Z	v1	MD5withRSA	31eace9b4c9c717 34a185680bc2486 6ca6cbd82b3cb61 bcc8706261b59ce 1073
/C=ES/ST=BARCELONA/L=BARCELONA/O=IPS Seguridad CA/OU=Certificaciones/CN=IPS SERVIDORES/E=ips@mail.ips.es		980101232107Z	091229232107Z	v1	MD5withRSA	f1f3cc207a6d479 47b8cb9c3042222 9de0d71fb67e0b 9a3eda08e0e1736 bc28
/C=JP/O=Japan Certification Services, Inc./CN=SecureSign RootCA1		990915150001Z	200915145959Z	v1	SHA1withRSA	5f960eebd716dbc b4d8a78b996e680 ac2547441e69b4e 44e98a595502e28 a002
/C=JP/O=Japan Certification Services, Inc./CN=SecureSign RootCA2		990915150001Z	200915145959Z	v1	SHA1withRSA	af6d08eef3cac4e 1584abc63c8a947 2ac529ef99f3f79 1319a43776063f9 8dca
/C=JP/O=Japan Certification Services, Inc./CN=SecureSign RootCA3		990915150001Z	200915145959Z	v1	SHA1withRSA	ae92e90000541a9 ebc101b70b6c33a 62f5a3a55be815 a81d31abddcf0390 7f5a
/C=US/O=GTE Corporation/CN=GTE CyberTrust Root		960223230100Z	060223235900Z	v1	MD5withRSA	527b050527df529 c0f7ad00ce1e7b a421788182613c3 26c8bd1a2061a9 bd7c
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root		980813002900Z	180813235900Z	v1	MD5withRSA	a53125188d2110a a94ab02c7b7c6da 3203170896e52b7 1fff6b667d5e681 0a36
/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Root		980403145201Z	040403235900Z	v1	MD5withRSA	2dfcbacaddf22a6f f107ab1fd3e8b9e 17858028879b13f 7c3b57b3e1bd231 5809
/C=US/O=RSA Data Security, Inc./OU=Secure Server Certification Authority		941109000000Z	100107235959Z	v1	MD2withRSA	2930bd09a07126b dc17288d4f2ed84 645ec948607907a 97b5ed0b0b05879 af69

Showing 1 to 10 of 560 entries Previous 1 2 3 4 5 ... 56 Next

**Root-stores**

☒ Mozilla Included CA Certificate List (2018-12) [150]

☒ Microsoft Trusted Root Program (2018-10) [382]

☐ Apple Trust Store version 2018071800 [174]

**Online logs**

☐ CNNIC CT log [32]

☐ Cloudflare 'Nimbus2017' Log [363]

☐ Cloudflare 'Nimbus2018' Log [363]

☐ Cloudflare 'Nimbus2019' Log [363]

☐ Cloudflare 'Nimbus2020' Log [363]

☐ Cloudflare 'Nimbus2021' Log [363]

☐ Cloudflare 'Nimbus2022' Log [363]

☐ Cloudflare 'Nimbus2023' Log [363]

☒ DigiCert Log Server [52]

☐ DigiCert Log Server 2 [377] (176 distinct)

☐ DigiCert Nessie2018 Log [526] (525 distinct)

☐ DigiCert Nessie2019 Log [526] (525 distinct)

☐ DigiCert Nessie2020 Log [526] (525 distinct)

☐ DigiCert Nessie2021 Log [526] (525 distinct)

☒ DigiCert Nessie2022 Log [526] (525 distinct)

☐ DigiCert Yeti2018 Log [526] (525 distinct)

☐ DigiCert Yeti2019 Log [526] (525 distinct)

☒ DigiCert Yeti2020 Log [526] (525 distinct)

☐ DigiCert Yeti2021 Log [526] (525 distinct)

☐ DigiCert Yeti2022 Log [526] (525 distinct)

☒ GDCA CT log #1 [21]

☐ GDCA Log 1 [527] (525 distinct)

☐ GDCA Log 2 [527] (525 distinct)

☐ Google 'Argon2017' log [537]

☐ Google 'Argon2018' log [537]

☐ Google 'Argon2019' log [537]

☐ Google 'Argon2020' log [537]

☐ Google 'Argon2021' log [537]

☐ Google 'Argon2022' log [537]

☐ Google 'Aviator' log [0]

☐ Google 'Crucible' log [394]

☐ Google 'Daedalus' log [537]

☐ Google 'Icarus' log [3]

☐ Google 'Pilot' log [537]

☐ Google 'Rocketeer' log [537]

☐ Google 'Skydiver' log [535]

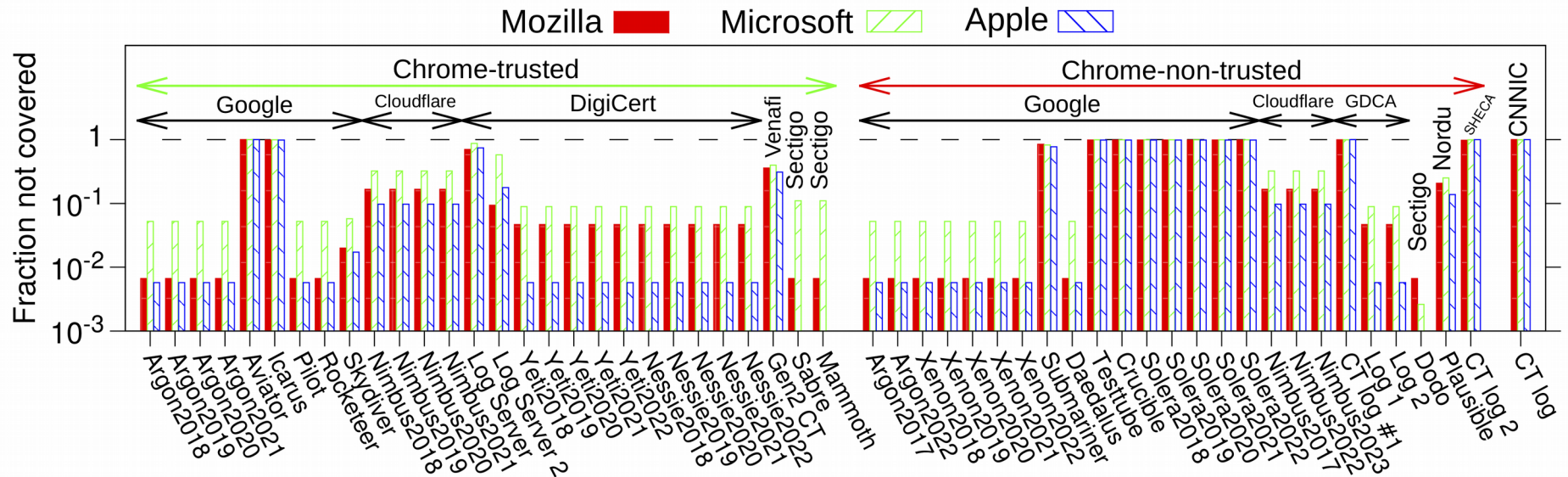


# The dataset

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

R1C 0902

## Fraction of trusted vendor certificates not covered by CT logs

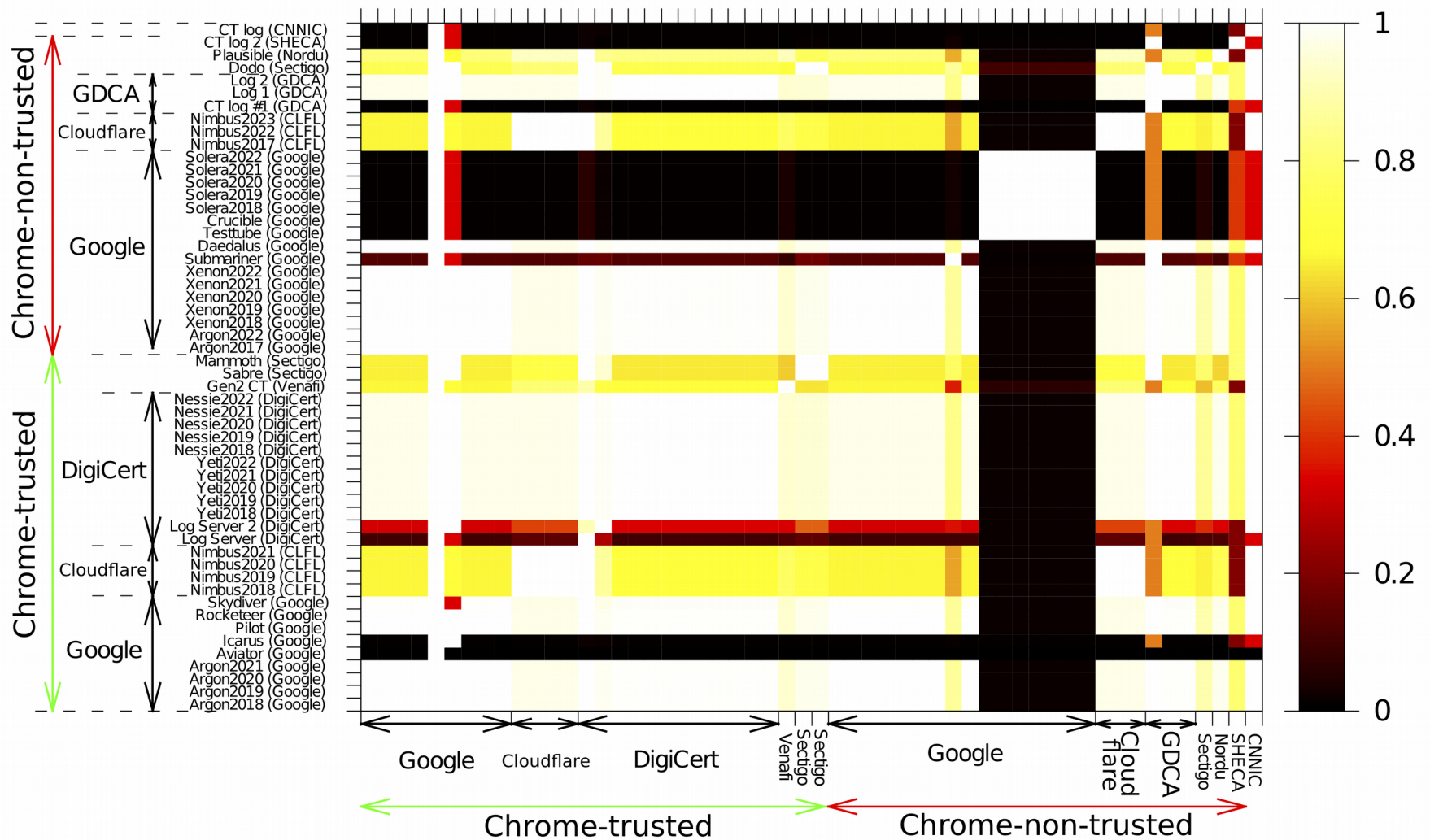


In order to enable attribution of each logged certificate to its issuer, the log SHALL publish a list of acceptable root certificates (this list might usefully be the union of root certificates trusted by major browser vendors).

RFC 6962



# Intersections of Logs' root stores

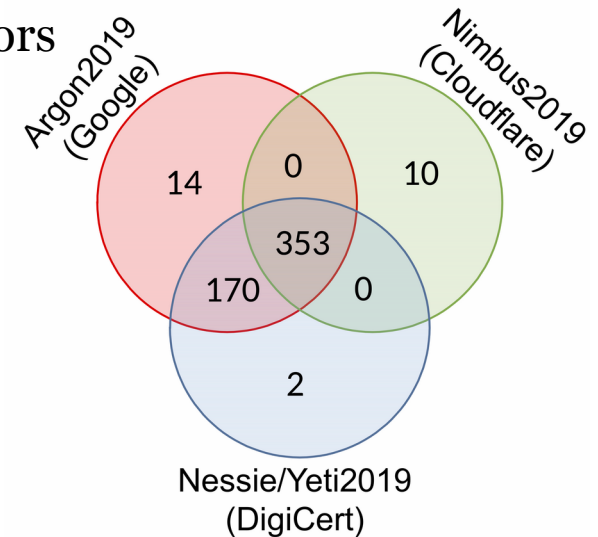
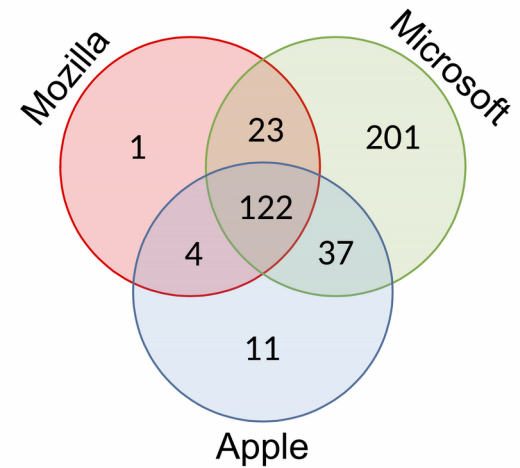


# Conclusion

- 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



Thank you!

[www.liu.se](http://www.liu.se)