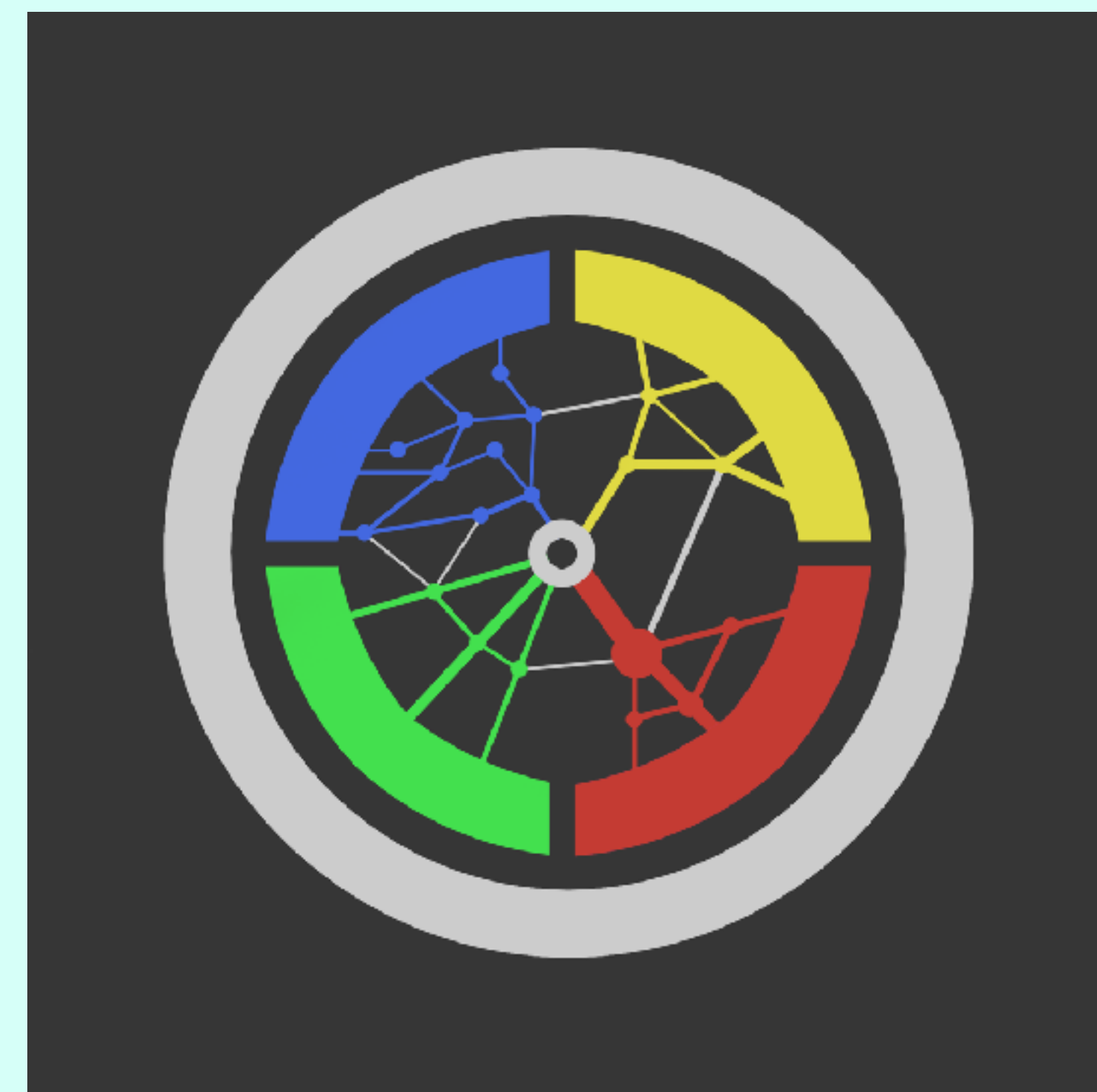


Certificate Transparency

Supporting Critical Internet Infrastructure

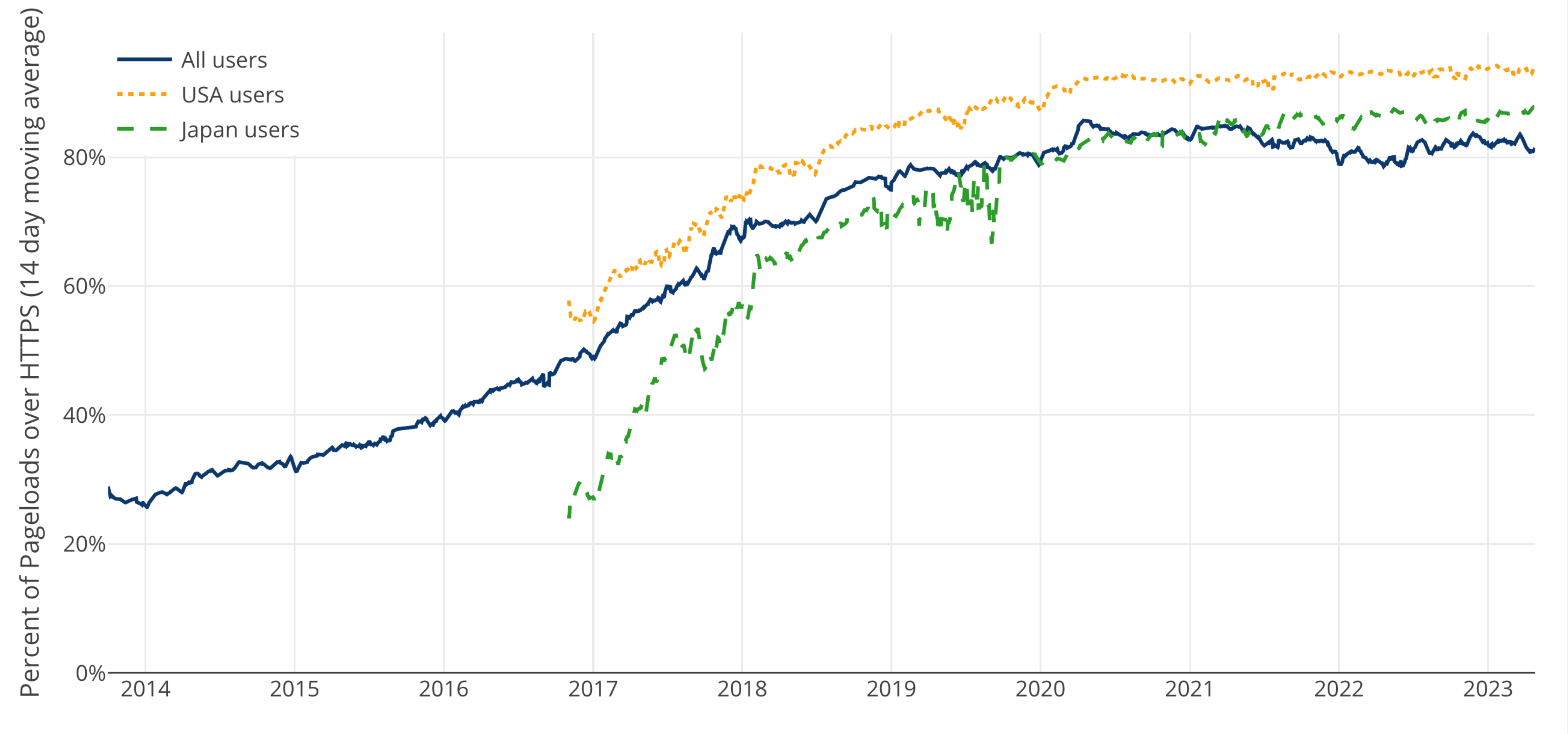
certificate.transparency.dev

Brought to you by:

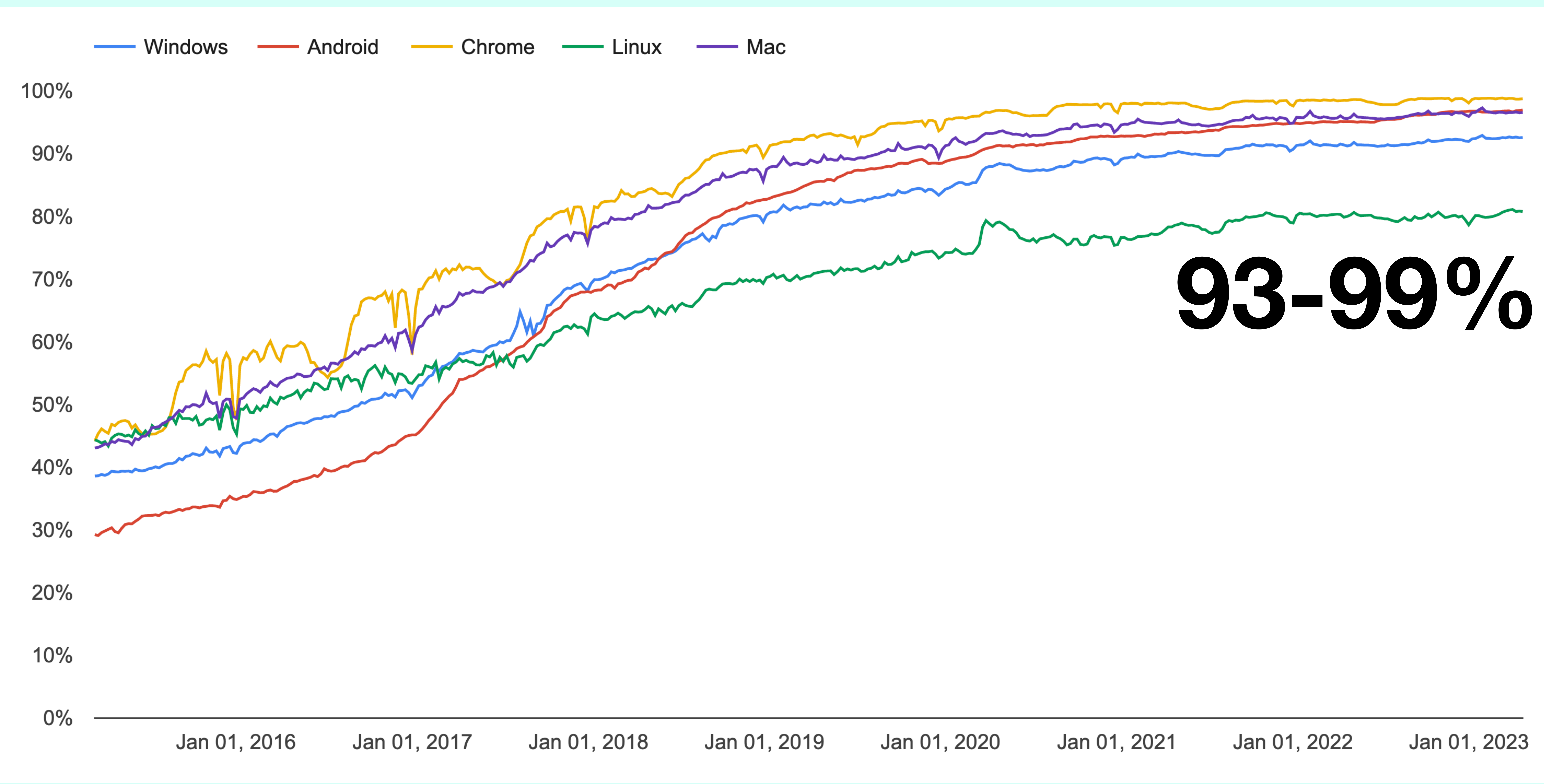


HTTP

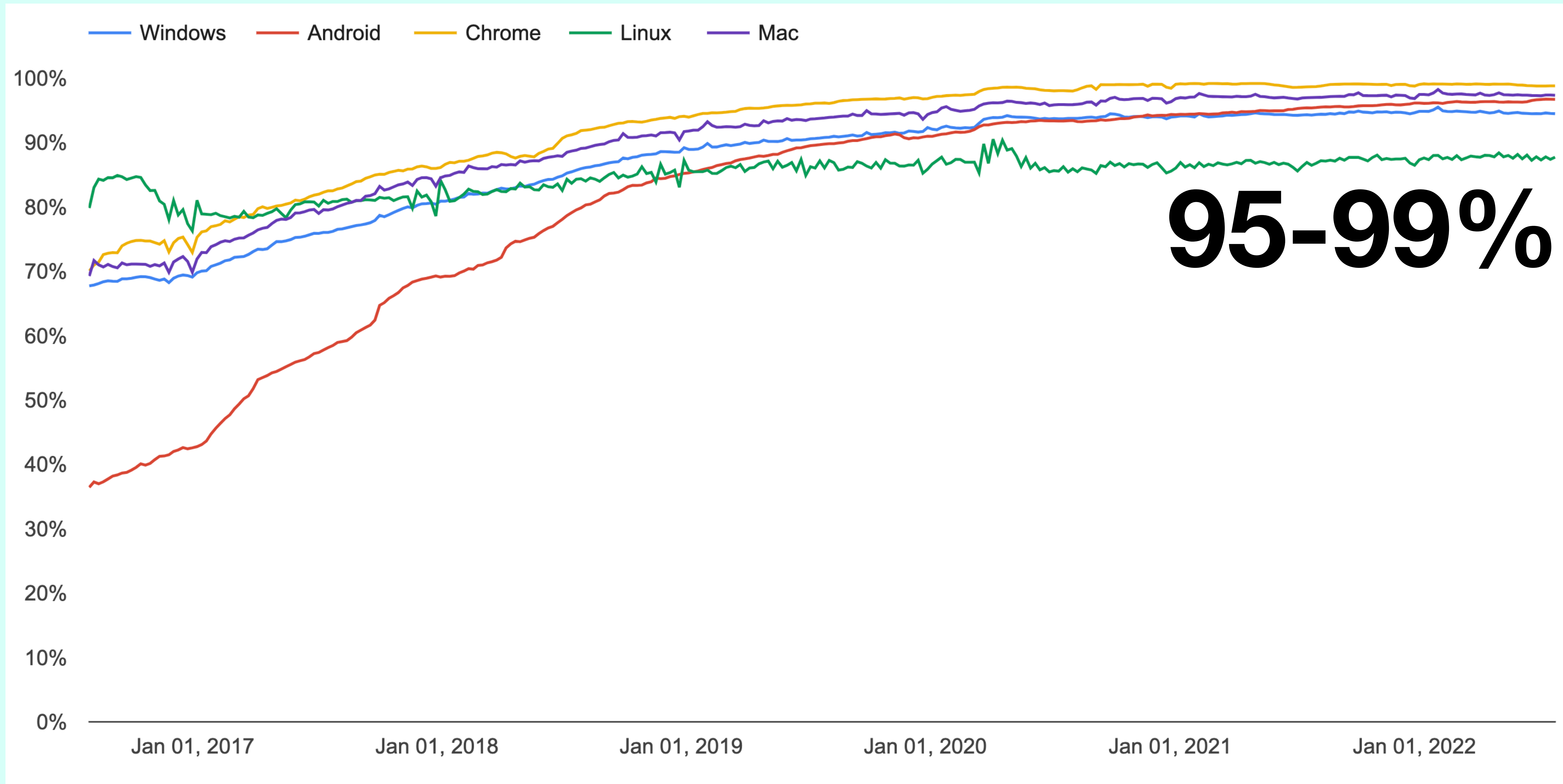
HTTPS



Percentage of Web Pages Loaded by Firefox Using HTTPS
Source: Mozilla



Chrome page loads over HTTPS (with TLS)
Source: Google



95-99%

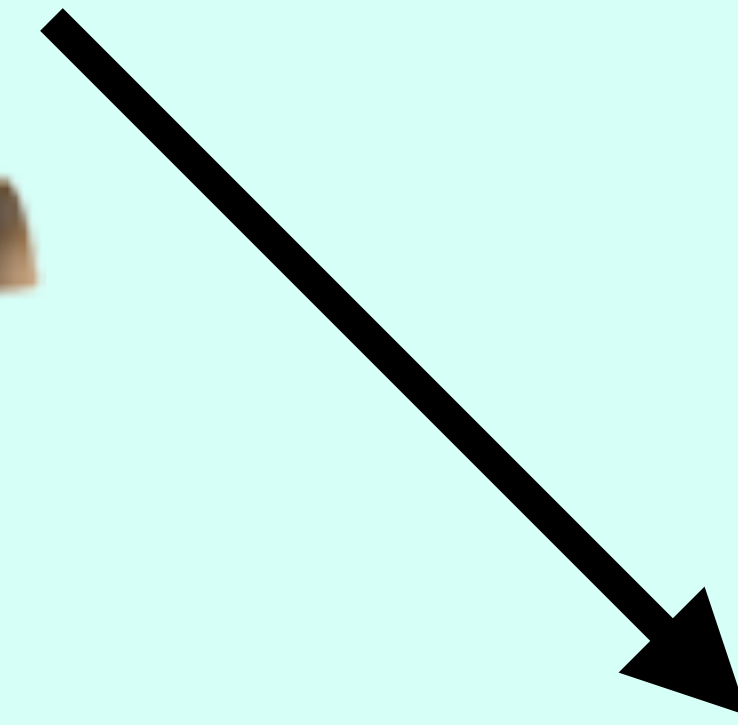
Chrome browsing time over HTTPS (with TLS)
Source: Google



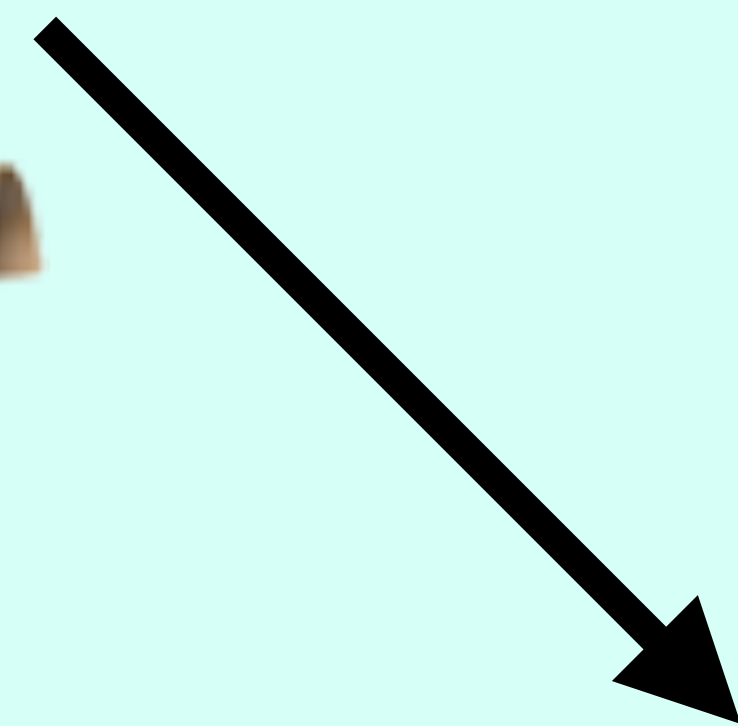
TLS



ISRG Root X1



R3

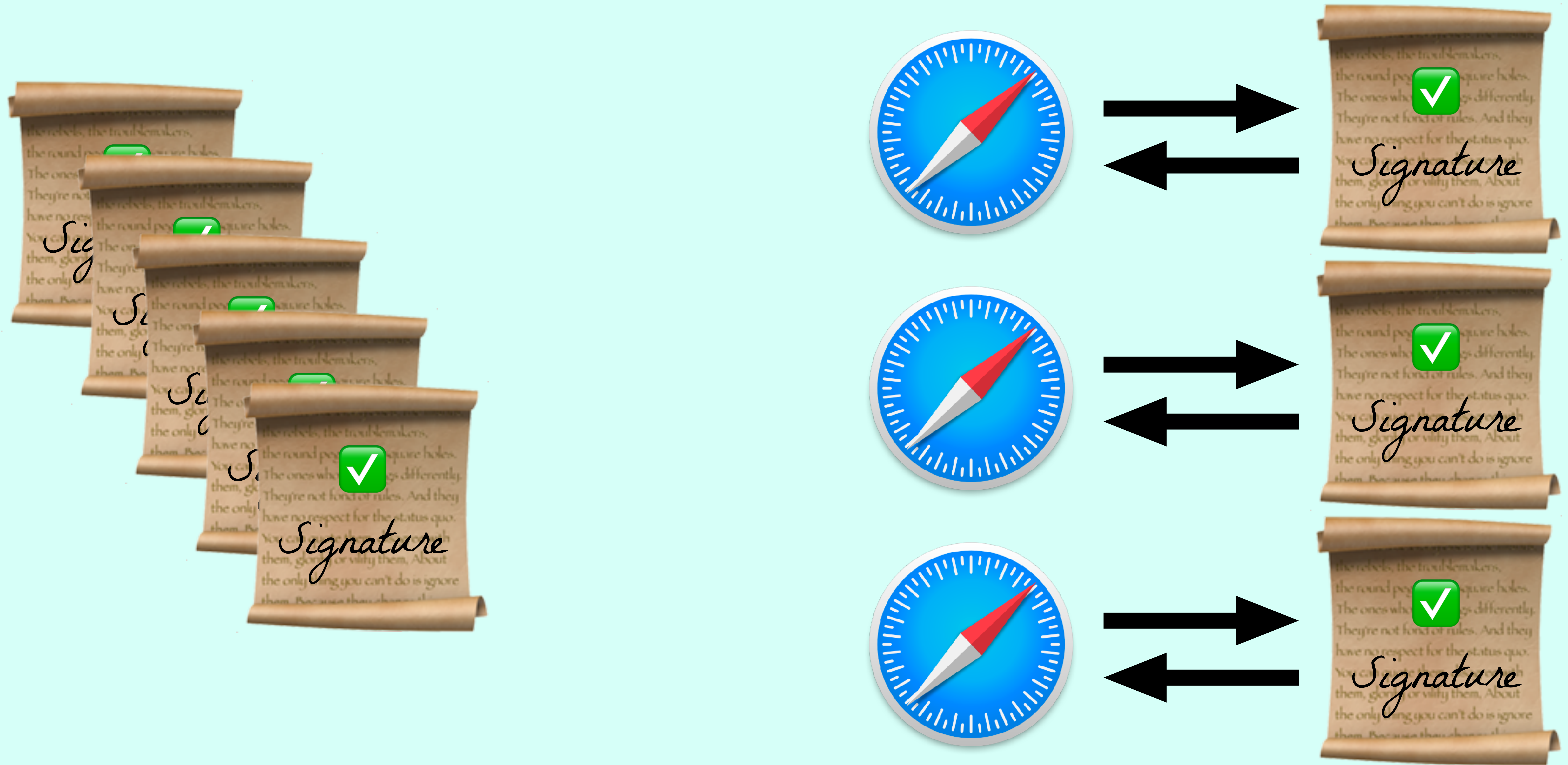


uknof.org.uk



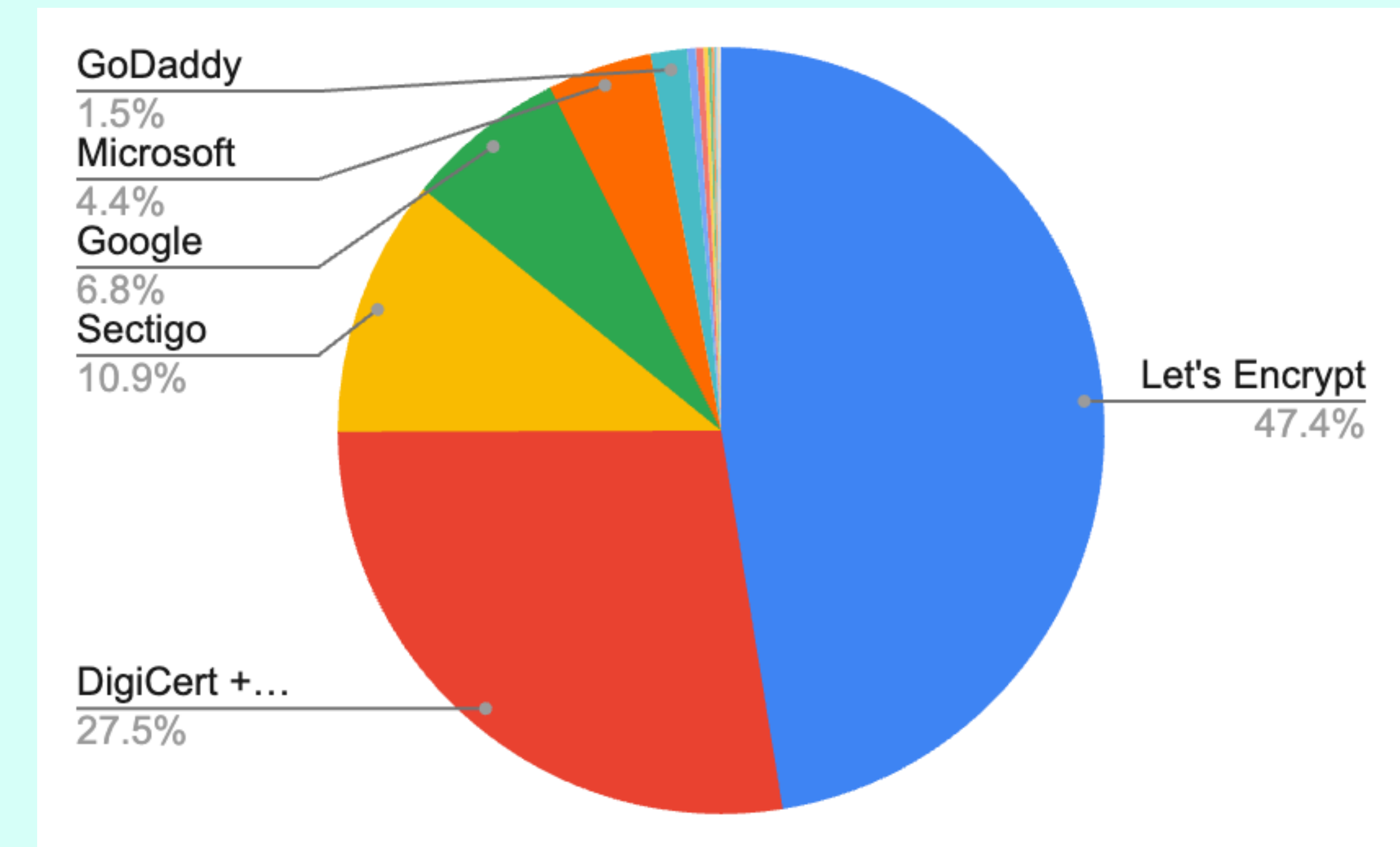
WebPKI

RPKI vs WebPKI

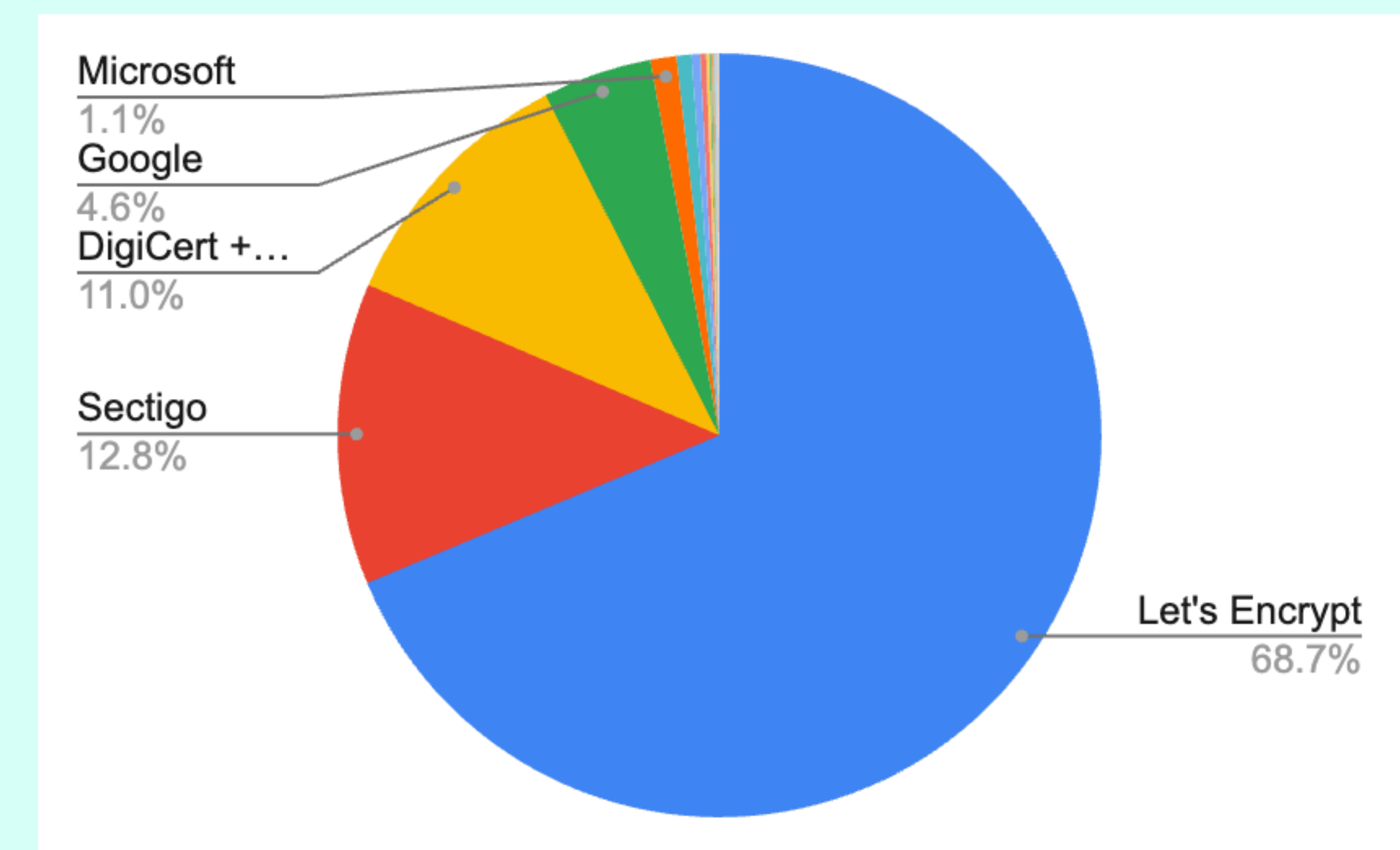


WebPKI Size

- Over 4.8 **Billion** Certificates stored
- Over 0.5 Billion Active / Unexpired
- Over 250,000 new certificates per hour



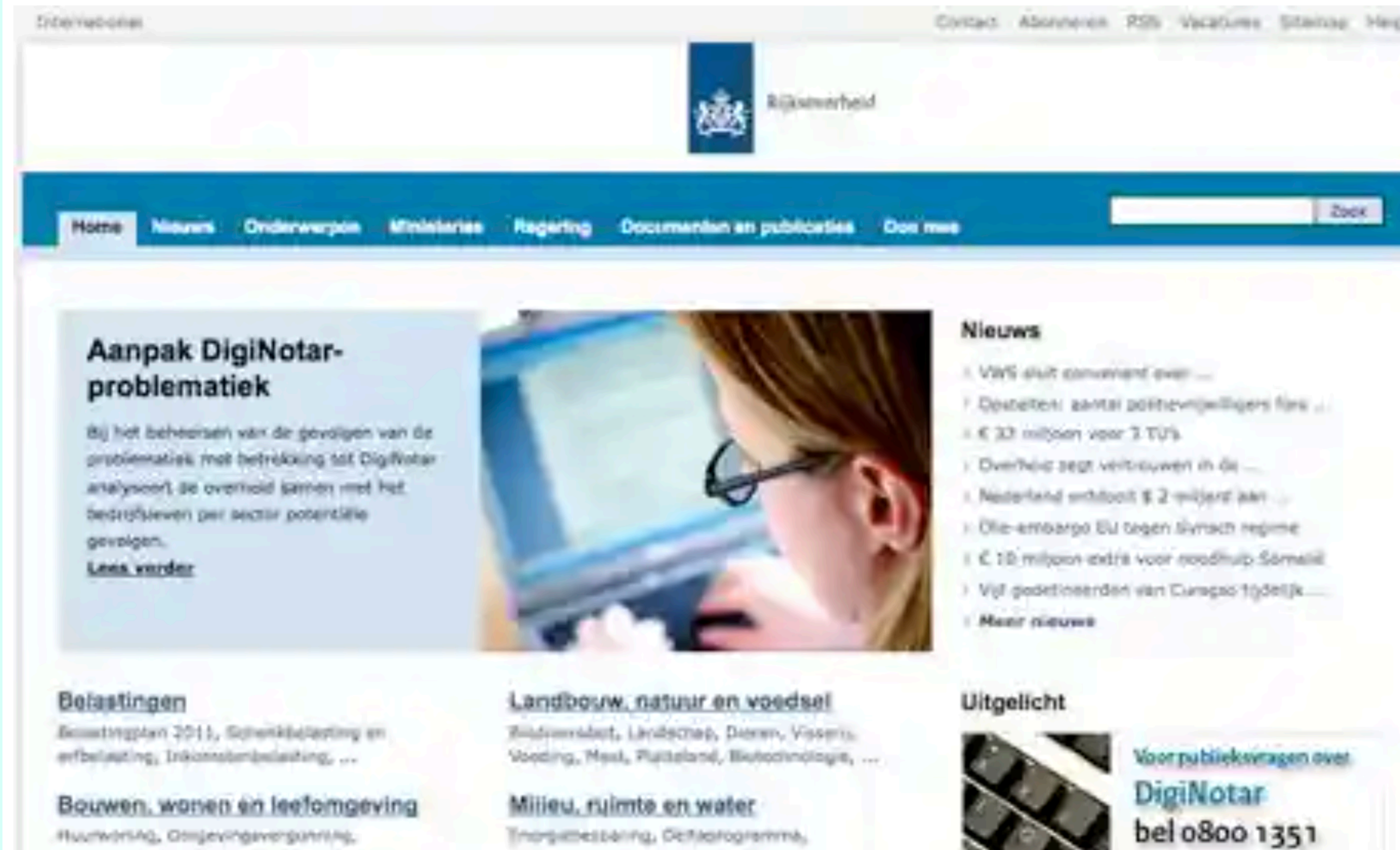
Currently Active / Unexpired



Total collected

DigiNotar SSL certificate hack amounts to cyberwar, says expert

Dutch government revokes certificates used for all its secure online transactions, while CIA, Google, Microsoft and others affected by hack called 'worse than Stuxnet'

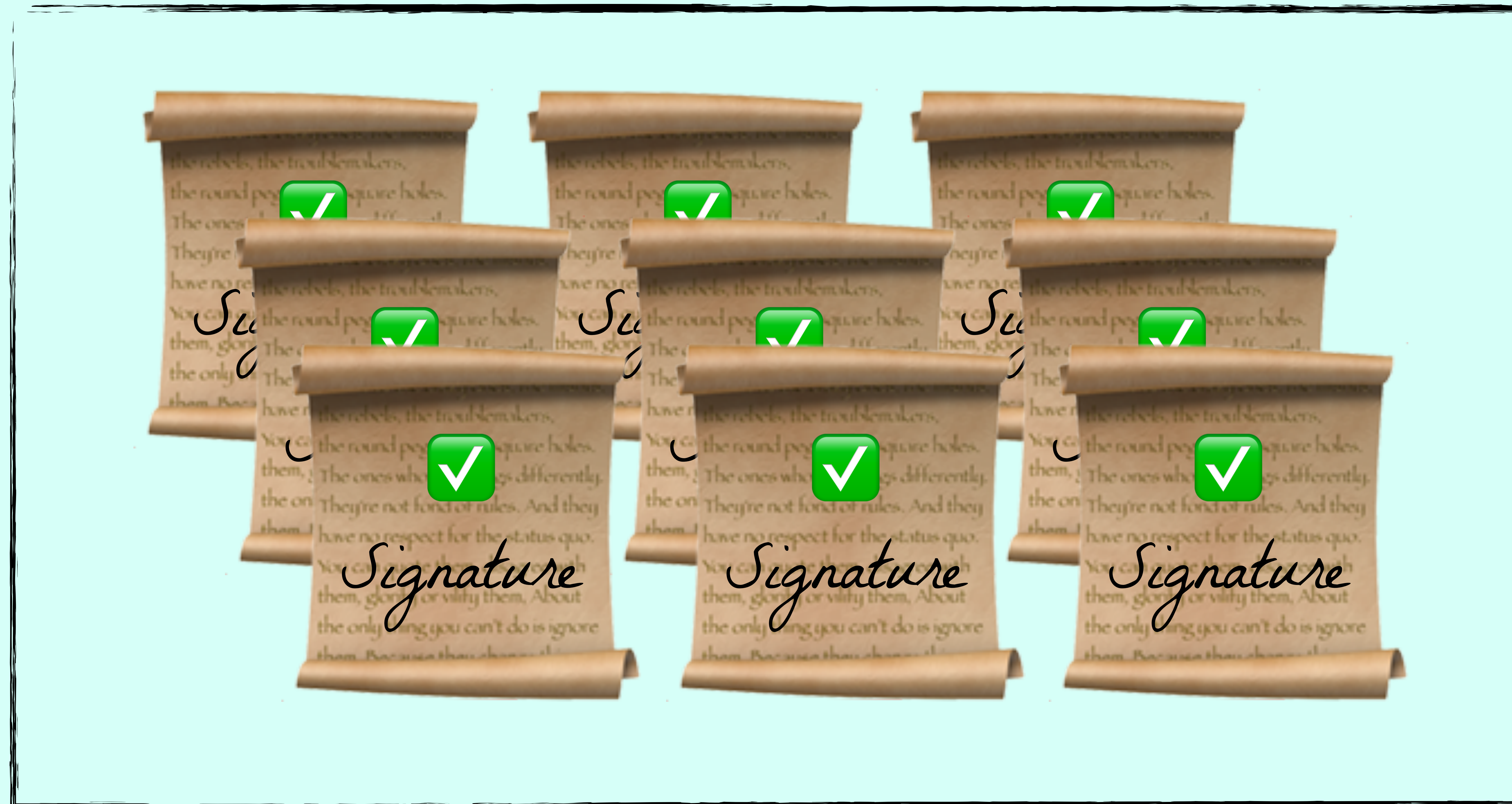


The screenshot shows the Dutch government website (Rijksverheid) with a news article titled "Aanpak DigiNotar-problematiek". The article discusses the consequences of the DigiNotar SSL certificate hack and mentions that the government has revoked all trust in digital certificates issued by DigiNotar. The article is dated 11/11/2011. The website also features a navigation menu with links to Home, Nieuws, Onderwerpen, Ministeries, Regering, Documenten en publicaties, and Doe mee. There is a search bar and a "Zoek" button. The main content area includes a large image of a woman looking at a laptop, a "Nieuws" section with a list of news items, and several category sections: Belastingen, Landbouw, natuur en voedsel, Milieu, ruimte en water, Bouwen, wonen en leefomgeving, and Uitgelicht. The "Uitgelicht" section features a call to action for public questions about DigiNotar, with the phone number 0800 1351.

📷 The Dutch government has revoked all trust in digital certificates issued by DigiNotar

Certificate Transparency

CT Log





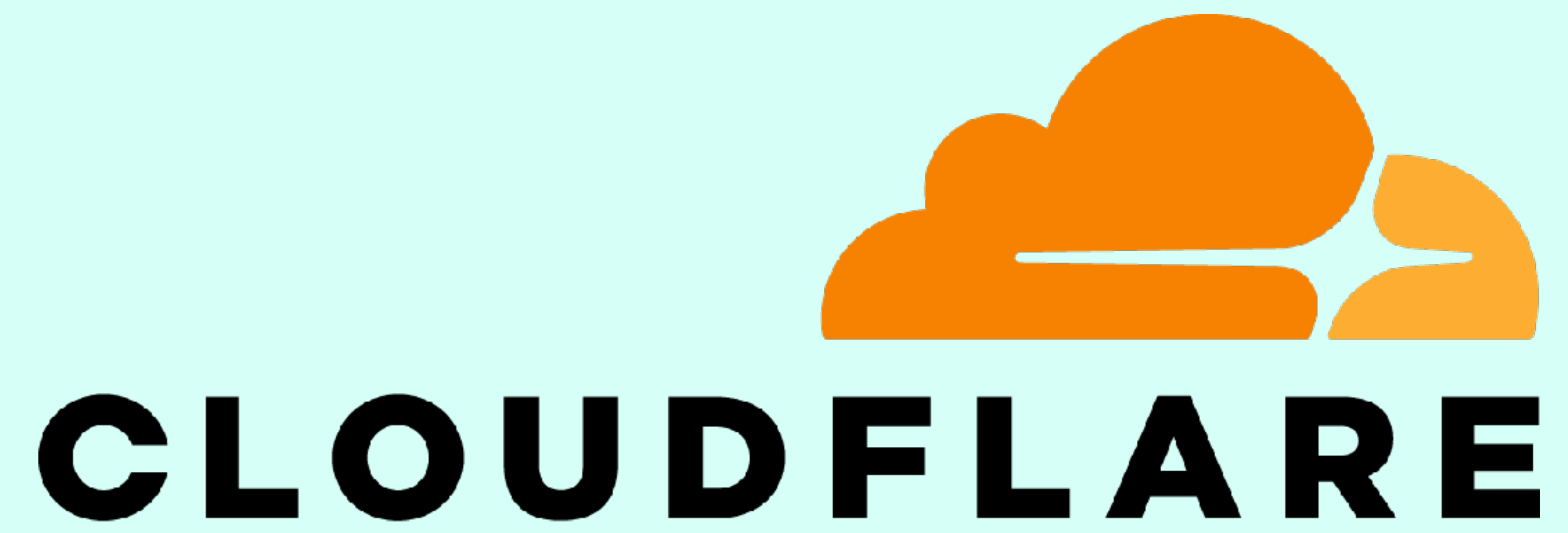
Your connection is not private

Attackers might be trying to steal your information from **fincen.gov** (for example, passwords, messages, or credit cards). [Learn more](#)

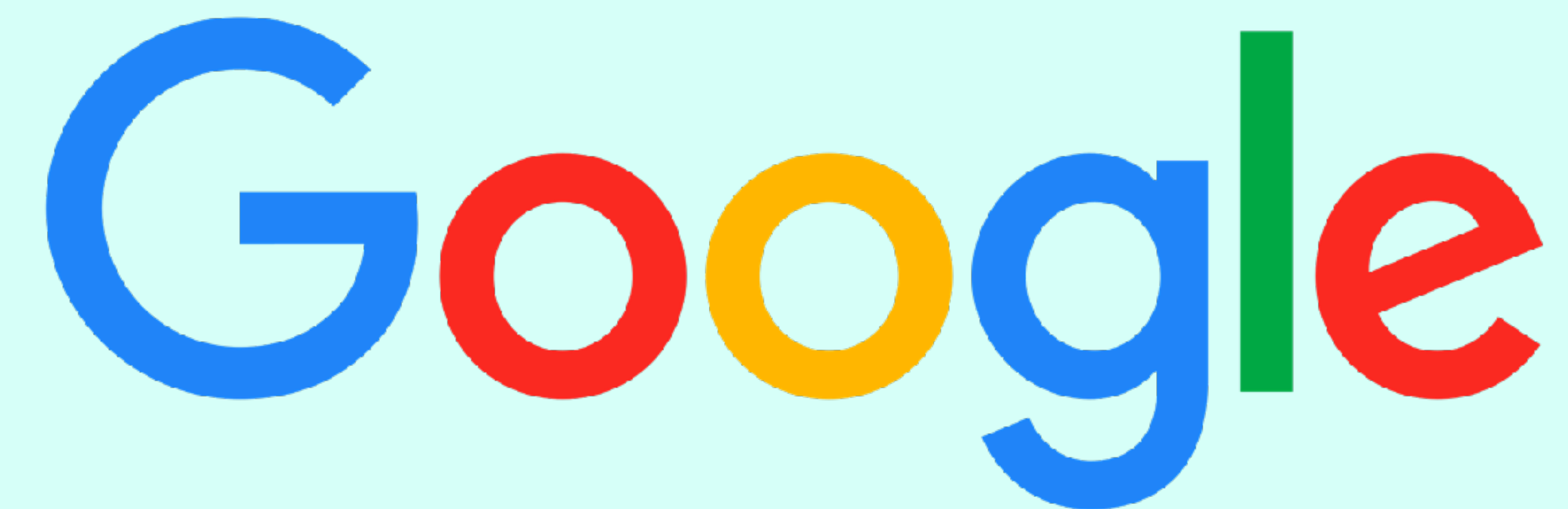
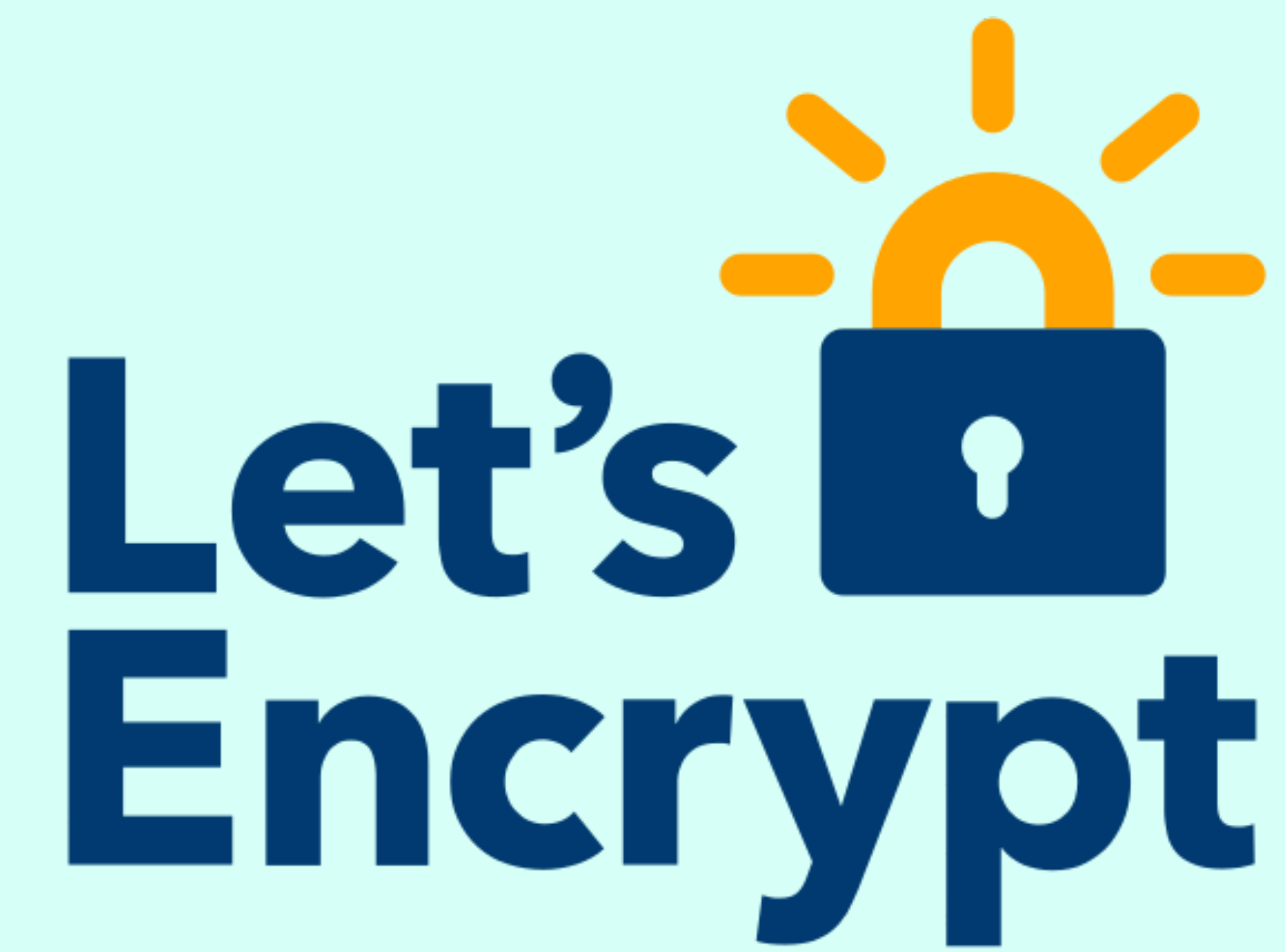
NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

Advanced

Back to safety



digicert®



**Phil, what does it take to
operate one of these?**



Operating Reliable CT Logs

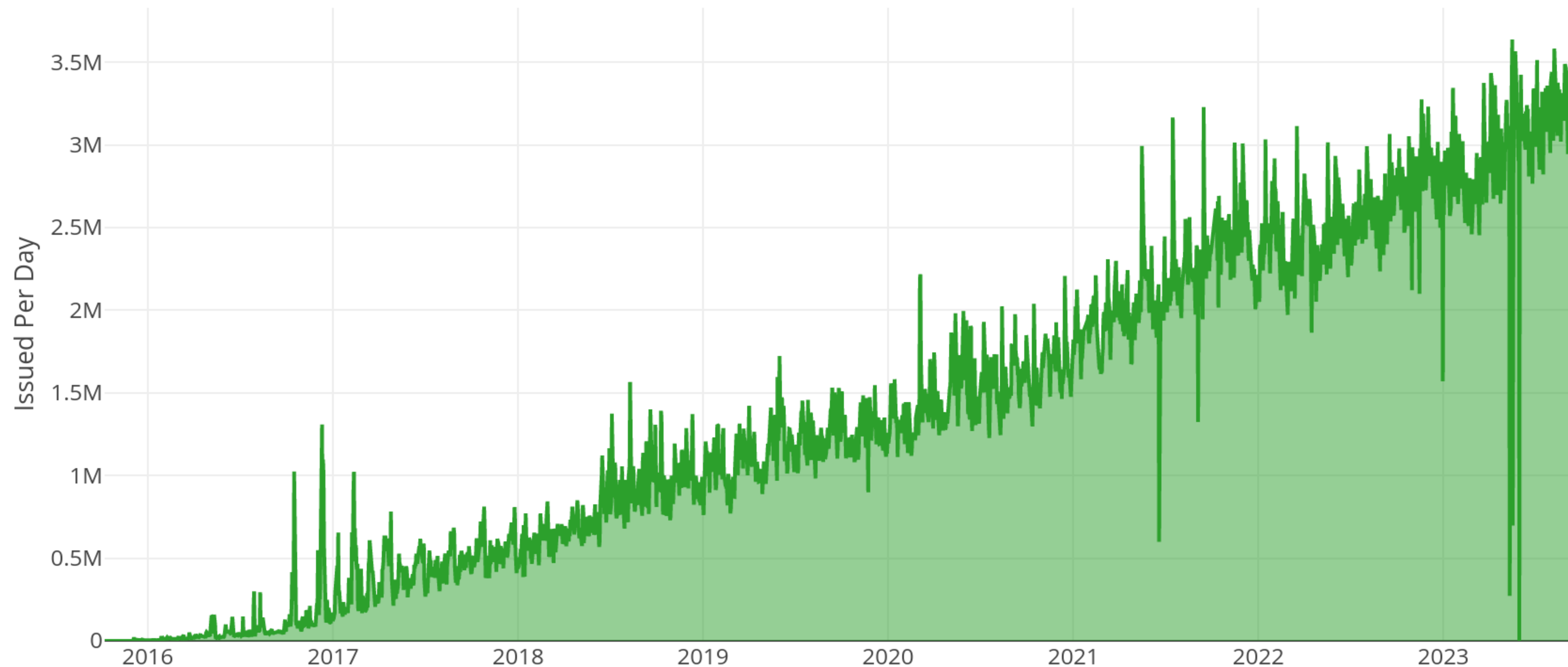
Who am I?

- phil@letsencrypt.org
- github.com/pgporada
- [linkedin.com/in/philporada](https://www.linkedin.com/in/philporada)



What is Let's Encrypt?

Let's Encrypt Certificates Issued Per Day



We've written about CT

2019

Introducing Oak, a Free and Open Certificate Transparency Log

<https://letsencrypt.org/2019/05/15/introducing-oak-ct-log.html>

How Let's Encrypt Runs CT Logs

<https://letsencrypt.org/2019/11/20/how-le-runs-ct-logs.html>

2022

Nurturing Continued Growth of Our Oak CT Log

<https://letsencrypt.org/2022/05/19/nurturing-ct-log-growth.html>

How does a CT log benefit a CA?

crt.sh Certificate Search

Criteria ID = '8092441842'

[8092441842](#)

Precertificate

Log entries for this certificate:

| Timestamp | Entry # | Log Operator | Log URL |
|-------------------------|-----------|---------------|---|
| 2022-12-01 01:55:09 UTC | 389039413 | Google | https://ct.googleapis.com/logs/argon2023 |
| 2022-12-01 01:55:09 UTC | 222434106 | Let's Encrypt | https://oak.ct.letsencrypt.org/2023 |
| 2022-12-01 01:55:09 UTC | 2578 | Let's Encrypt | https://oak.ct.letsencrypt.org/2024h1 |
| 2022-12-01 01:55:09 UTC | 437567201 | Google | https://ct.googleapis.com/logs/xenon2023 |

| Mechanism | Provider | Status | Revocation Date | Last Observed in CRL | Last Checked (Error) |
|------------------------|-----------|-------------|-----------------|----------------------|-------------------------|
| OCSP | The CA | Good | n/a | n/a | 2023-04-27 19:52:23 UTC |
| CRL | The CA | Not Revoked | n/a | n/a | 2023-04-27 17:21:44 UTC |
| CRLSet/Blocklist | Google | Not Revoked | n/a | n/a | n/a |
| disallowedcert.stl | Microsoft | Not Revoked | n/a | n/a | n/a |
| OneCRL | Mozilla | Not Revoked | n/a | n/a | n/a |

SHA-256 [670770F5932718312ED3F88679A8C9F76778D45368524FCCD81666519A206694](#) **SHA-1** CB1EAF2773A345D0

[Certificate:](#)

Data:

Version: 3 (0x2)

[Serial Number:](#)

02:da:37:36:34:23:55:cd:c3:21:36:95:29:05:0f:eb

Signature Algorithm: sha256WithRSAEncryption

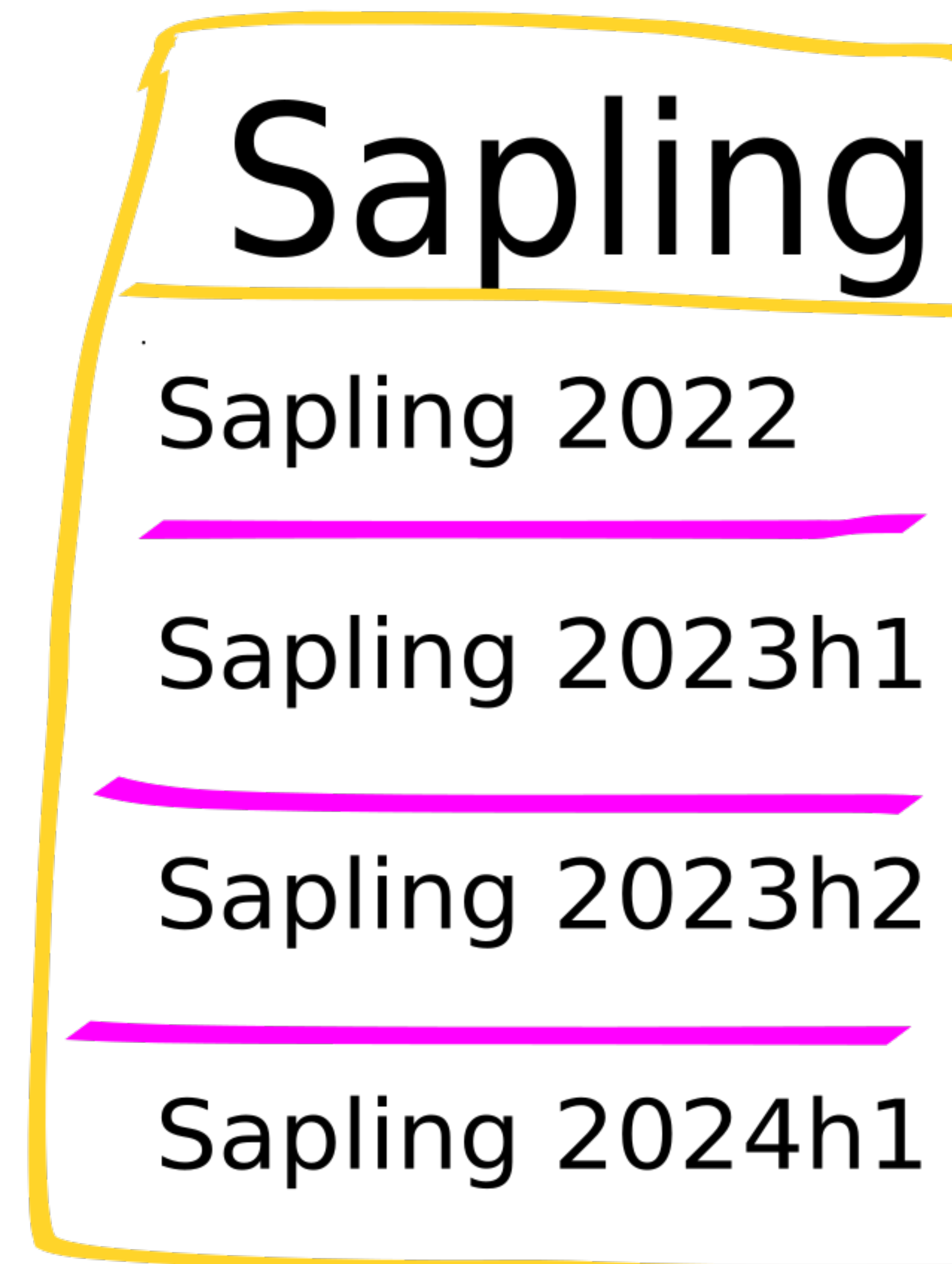
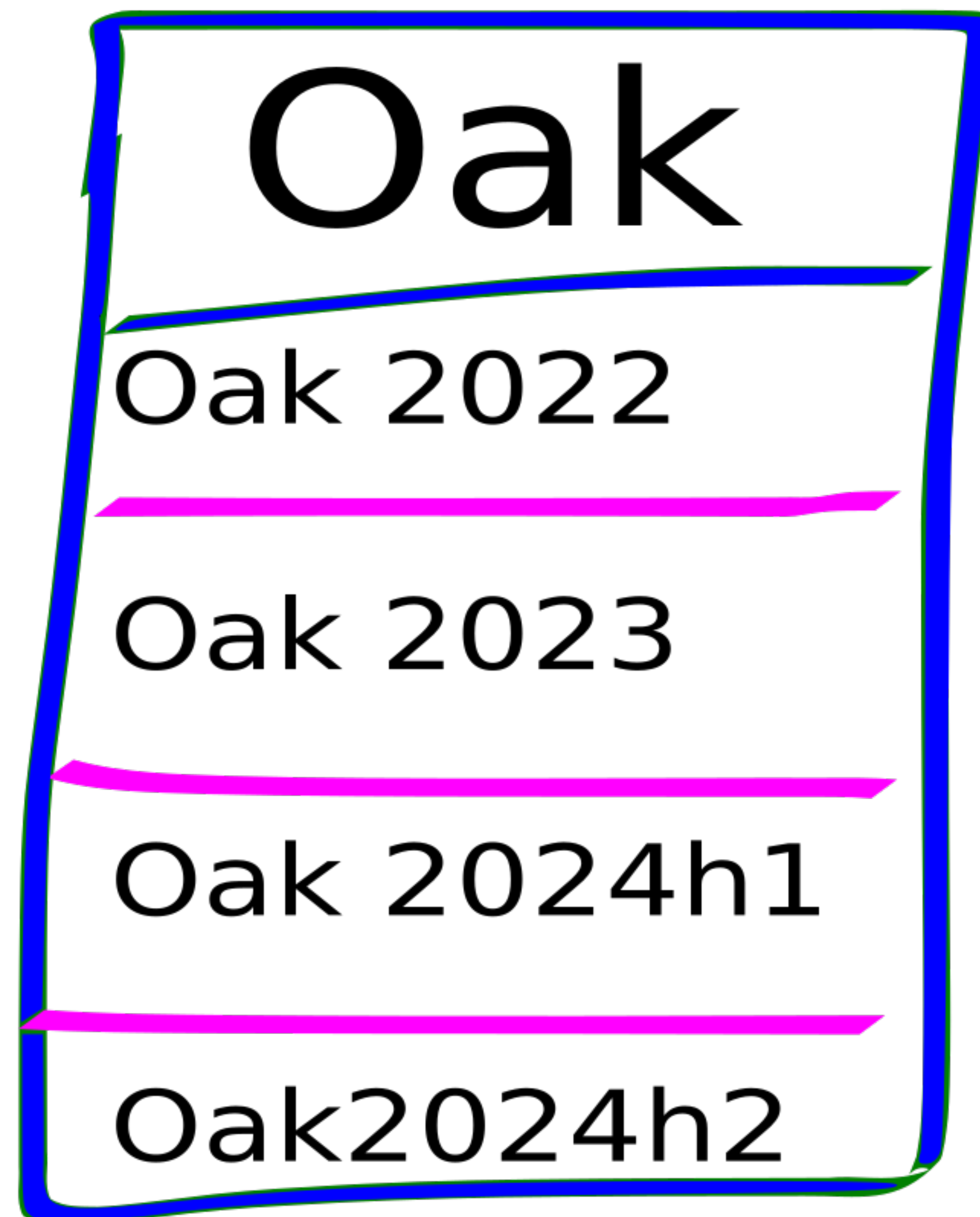
[Issuer:](#) (CA ID: 9324)

commonName = Amazon

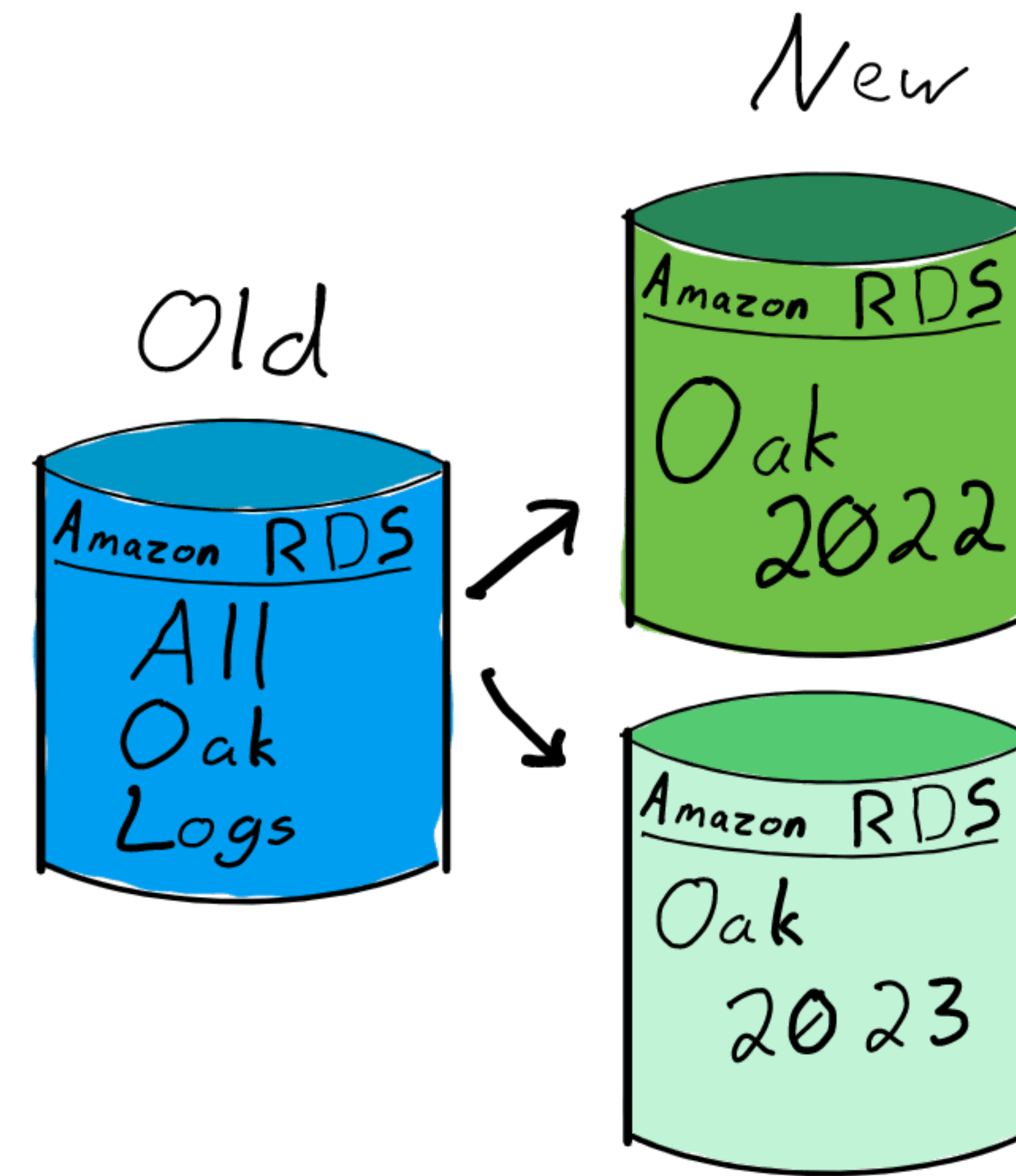
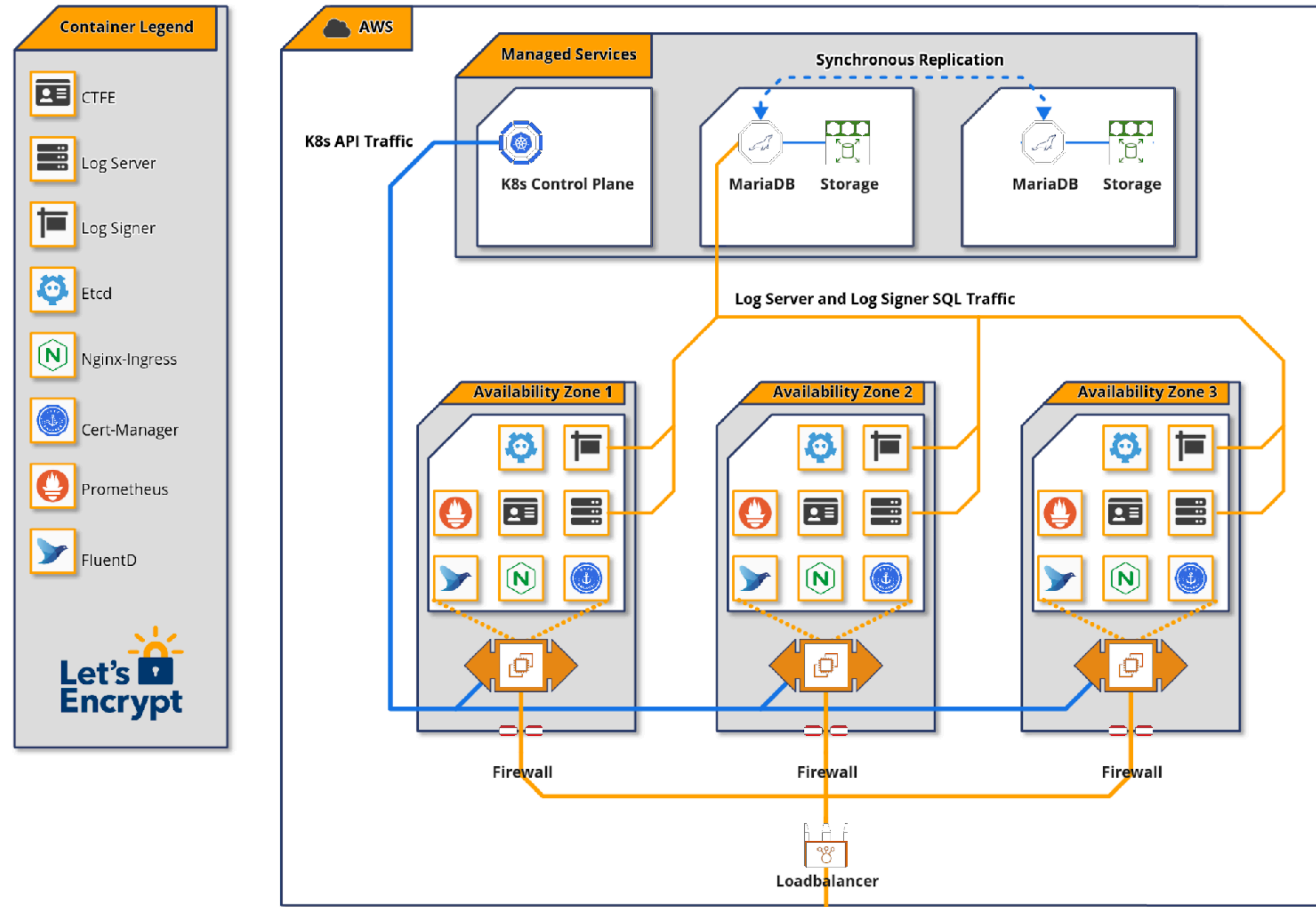
organizationalUnitName = Server CA 1B

organizationName = Amazon

Logs? Shards? Oh my!



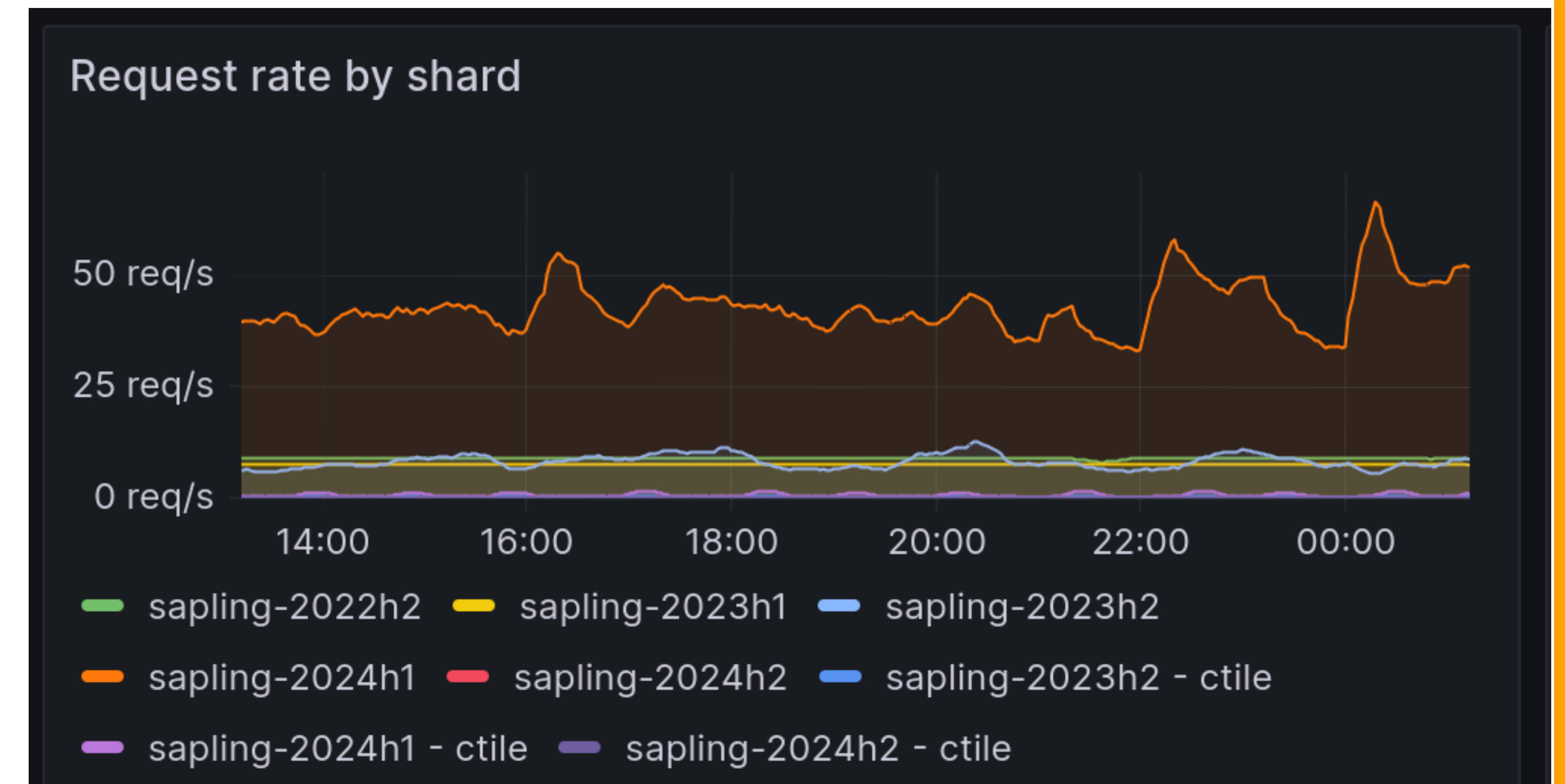
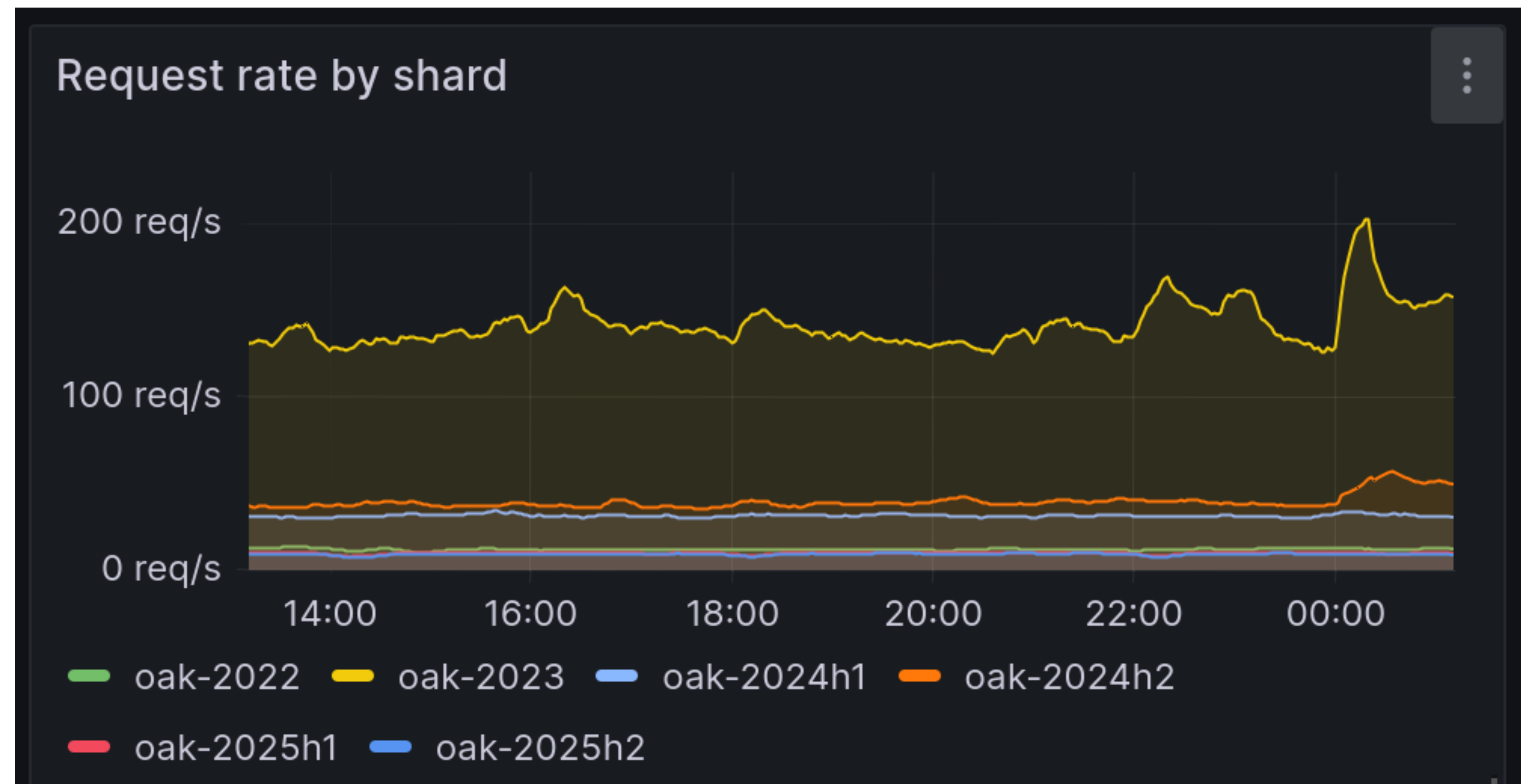
Architecture



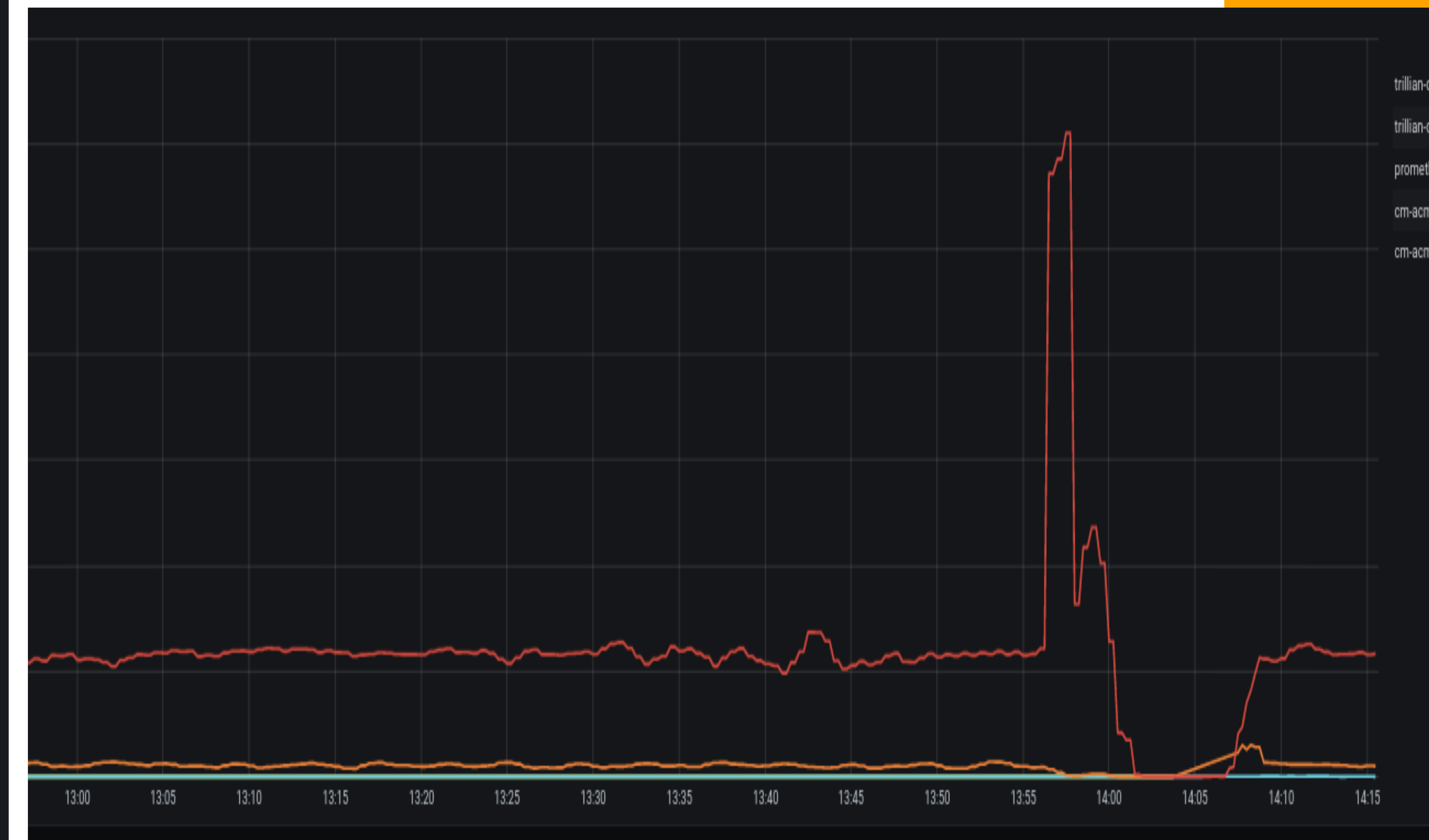
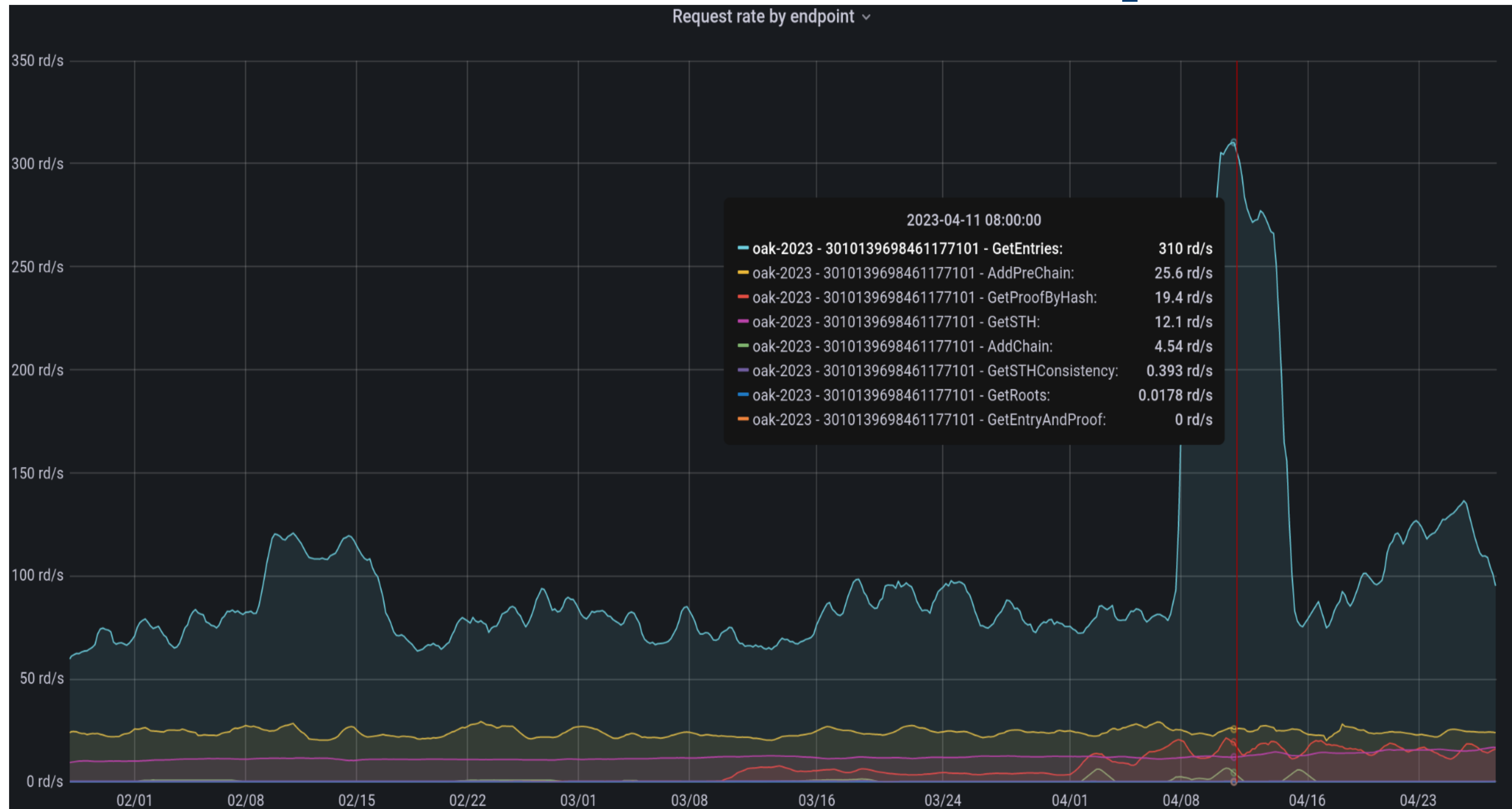
```
$ kubectl get pods -n sapling-2024h1
```

| NAME | READY | STATUS | RESTARTS | AGE |
|---|-------|---------|-------------|-----|
| ctile-deployment-5b99ff57d-8nqdj | 1/1 | Running | 0 | 9d |
| ctile-deployment-5b99ff57d-mxkk7 | 1/1 | Running | 0 | 9d |
| sapling-2024h1-etcd-operator-etcd-operator-etcd-operator-8fkvbj | 1/1 | Running | 0 | 61d |
| trillian-ctfe-deployment-c95b9ccd-bnmpm | 1/1 | Running | 0 | 12d |
| trillian-ctfe-deployment-c95b9ccd-gpk7h | 1/1 | Running | 0 | 61d |
| trillian-etcd-cluster-99zrxgzsms | 1/1 | Running | 0 | 61d |
| trillian-etcd-cluster-nldzwsbwmf | 1/1 | Running | 0 | 61d |
| trillian-etcd-cluster-sdj9bpcs9d | 1/1 | Running | 0 | 12d |
| trillian-logserver-deployment-6cdf6bc979-fnmjg | 1/1 | Running | 0 | 61d |
| trillian-logserver-deployment-6cdf6bc979-hwtfk | 1/1 | Running | 0 | 12d |
| trillian-logsigner-deployment-86b4d7d775-5lsvf | 1/1 | Running | 1 (12d ago) | 61d |
| trillian-logsigner-deployment-86b4d7d775-nqlnf | 1/1 | Running | 0 | 61d |

Aggregate Requests Per Shard



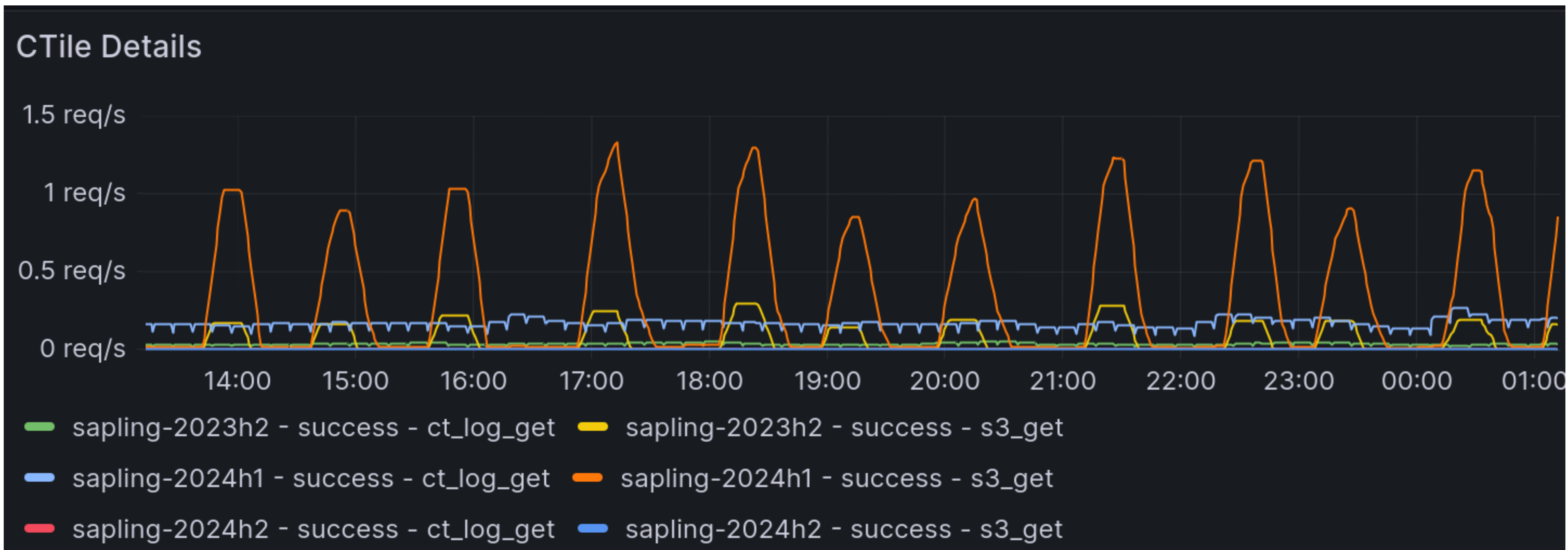
Active Shard Request Rates



| | max | current |
|---|-------------|-------------|
| oak-2023 - 3010139698461177101 - AddChain | 6.71 rd/s | 0.323 rd/s |
| oak-2023 - 3010139698461177101 - AddPreChain | 29.3 rd/s | 24.0 rd/s |
| oak-2023 - 3010139698461177101 - GetEntries | 310 rd/s | 95.2 rd/s |
| oak-2023 - 3010139698461177101 - GetEntryAndProof | 0.0495 rd/s | 0 rd/s |
| oak-2023 - 3010139698461177101 - GetProofByHash | 21.3 rd/s | 16.0 rd/s |
| oak-2023 - 3010139698461177101 - GetRoots | 0.0189 rd/s | 0.0179 rd/s |
| oak-2023 - 3010139698461177101 - GetSTH | 16.8 rd/s | 16.8 rd/s |

CFile

<https://github.com/letsencrypt/ctile>



Cost of running our CT logs

Human

- 1 - 2x SREs spending ~3 months worth of time over the course of a year just for maintenance.

Compute

- Compute nodes are basically commodity hardware.
- Storage and RAM for compute nodes is also negligible. Just enough to run the various applications.

Database

- A single database per shard continues to be our solution, though it gets pricey. Vertically scaling the active shard's database up and downsizing the other shards helps save cost.
- Faster storage will give better log performance to a point when data is read from disk.

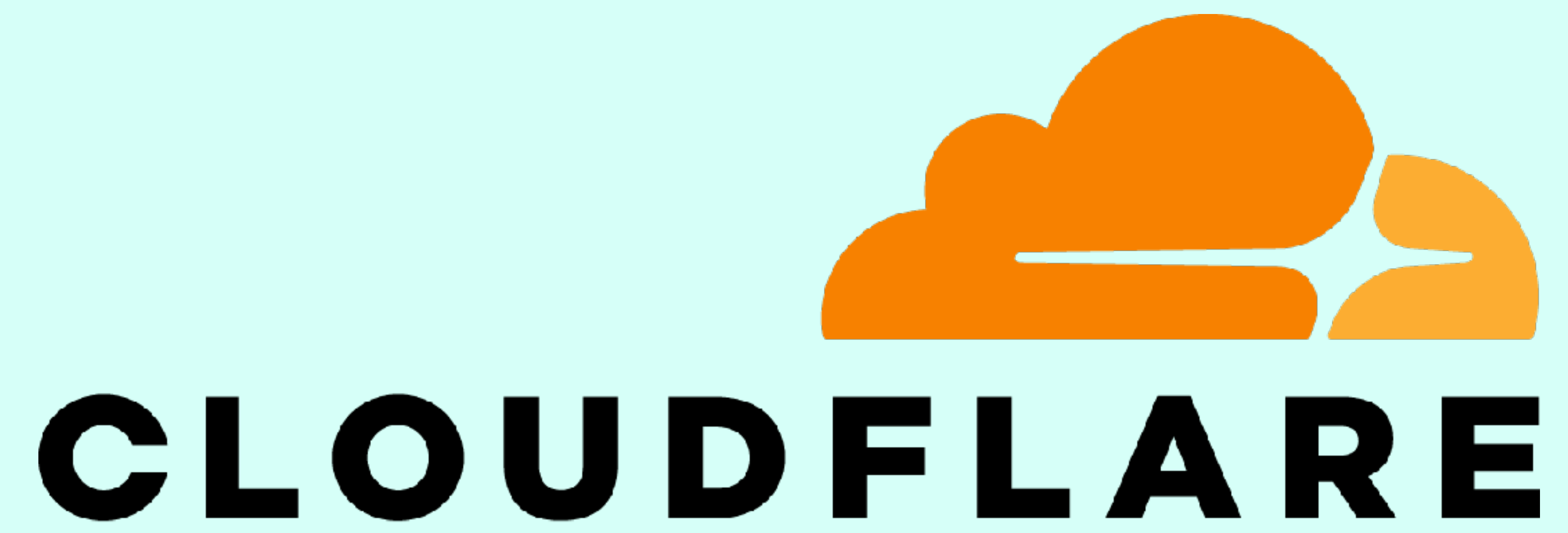
CTile and S3:

- For each currently existing shard in Oak and Sapling, a grand total of ~\$300/mo.

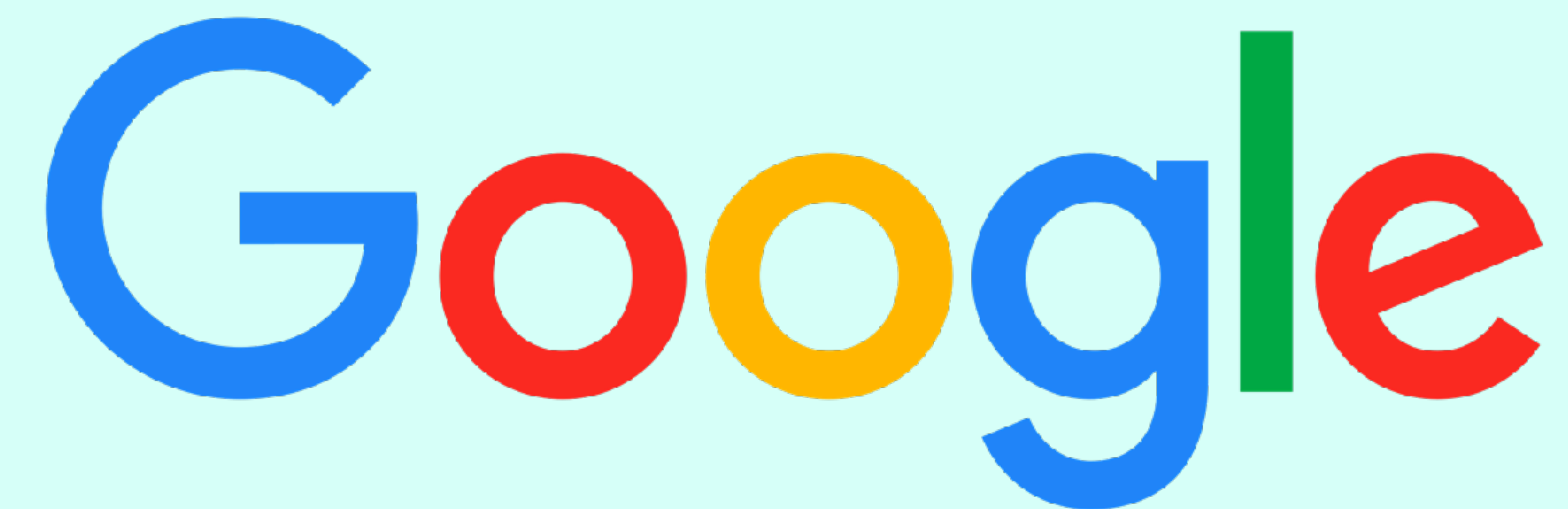
Takeaways

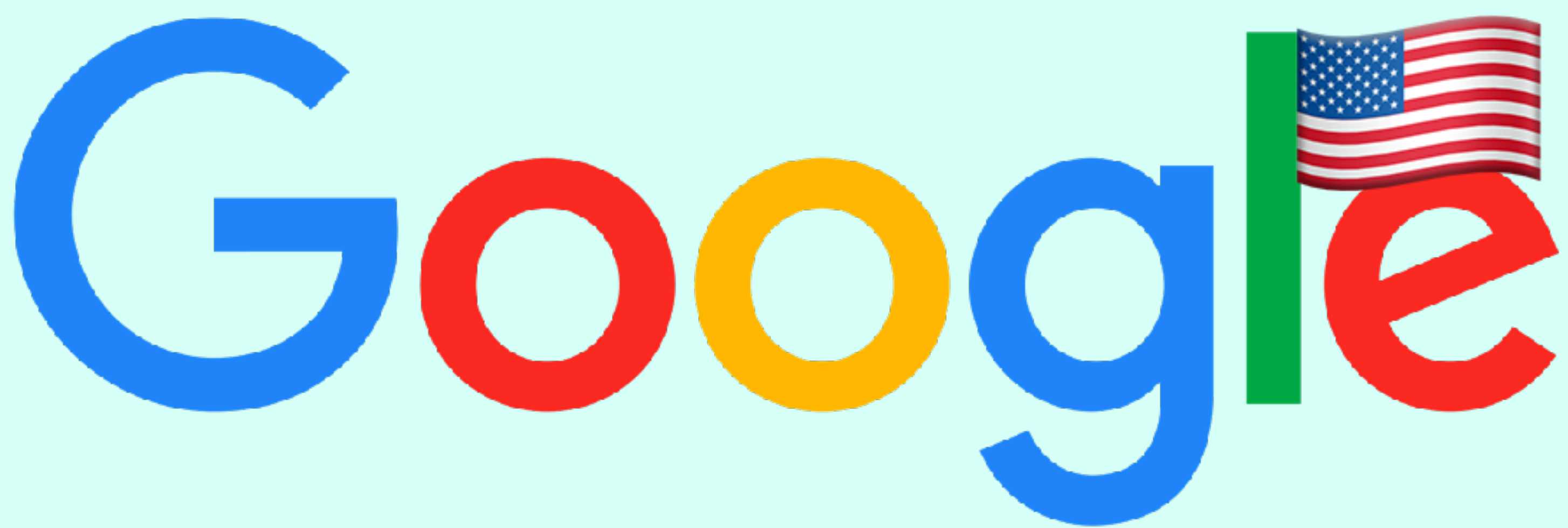
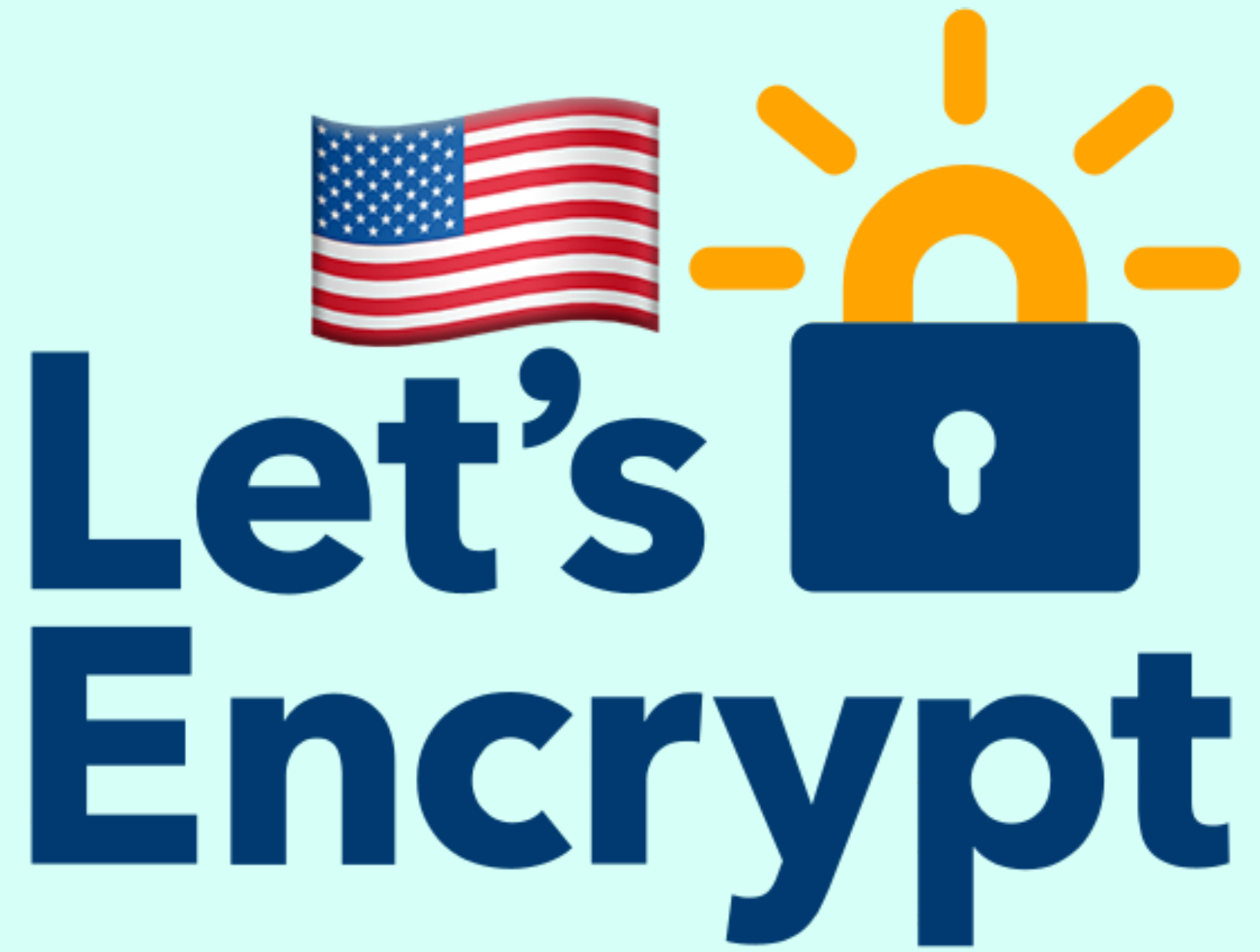
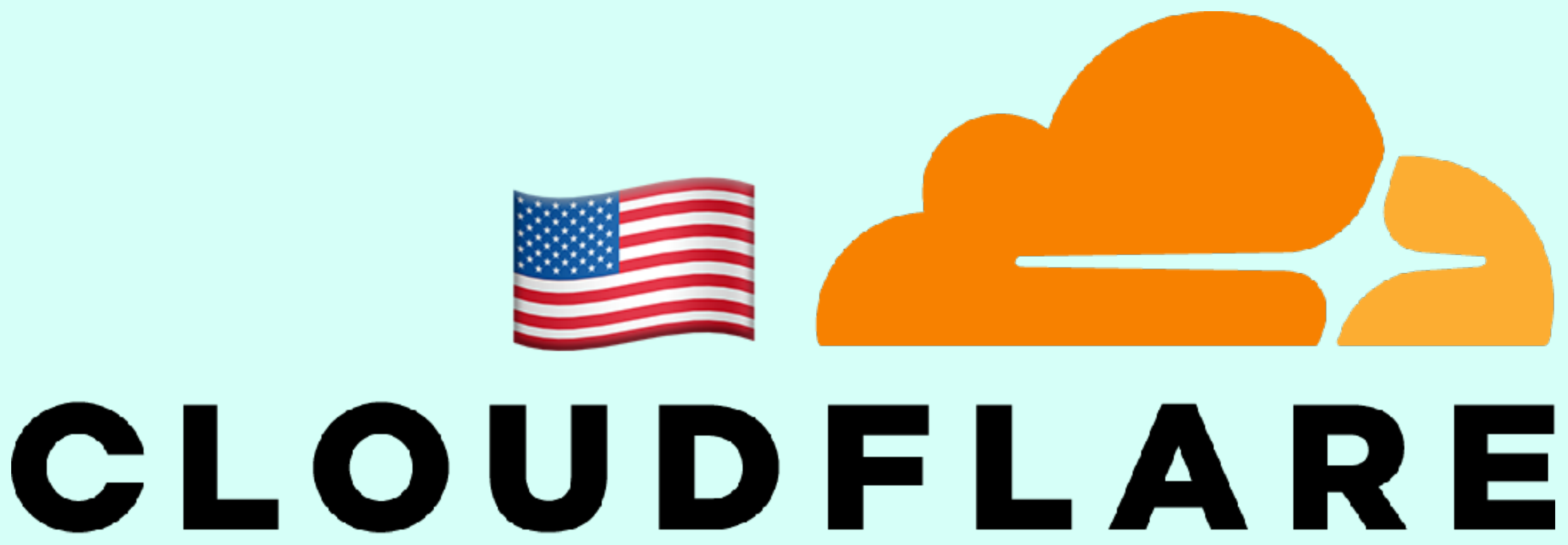
- Have a testing log so you don't prematurely ruin your production log.
- Logs are ephemeral. When your log fails, root cause why and build a new better log with the lessons learned.
- Separation of concerns: run each application in a different container, VM, or physical host in different namespaces. You're after reliability.
- The log_signers (sequencers) perform an etcd election to determine which cluster member will communicate with the database. Alert if more than 1 cluster member has mastership for a particular shard because it will indicate a split brain scenario and cause an incident. We've been there.
- Have rate limiting to protect your log at both the loadbalancer (Nginx) and via Trillian.
- We don't run database backups for CT logs.
- Use CTile to shed read load from the database for the /ct/v1/get-entries endpoint.

Cool!



digicert®





We need more CT Logs!

Setting up a CT Log

- Apple & Google have guidelines & requirements
- You can apply like this for consideration
- You can join the community mailing list

You're not alone!

Use the mailing list, or feel free to contact morectlogs@daknob.net for discussion, help, insights, advice, or anything we can do at any phase of the project :)