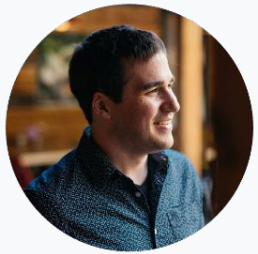
Google

Scaling transparency ecosystems

Lessons learned from CT



Joe DeBlasio
Chrome Security team
jdeblasio at chromium.org

Philippe
Boneff
TrustFabric team
phboneff at google.com

Chrome + TrustFabric

Oct 2024
Transparency.dev days

How to draw an owl

1.

2.

1. Draw some circles

2. Draw the rest of the fucking owl

Agenda

01 Introduction: CT

02 From one log to multiple logs

03 From one operator to multiple operators

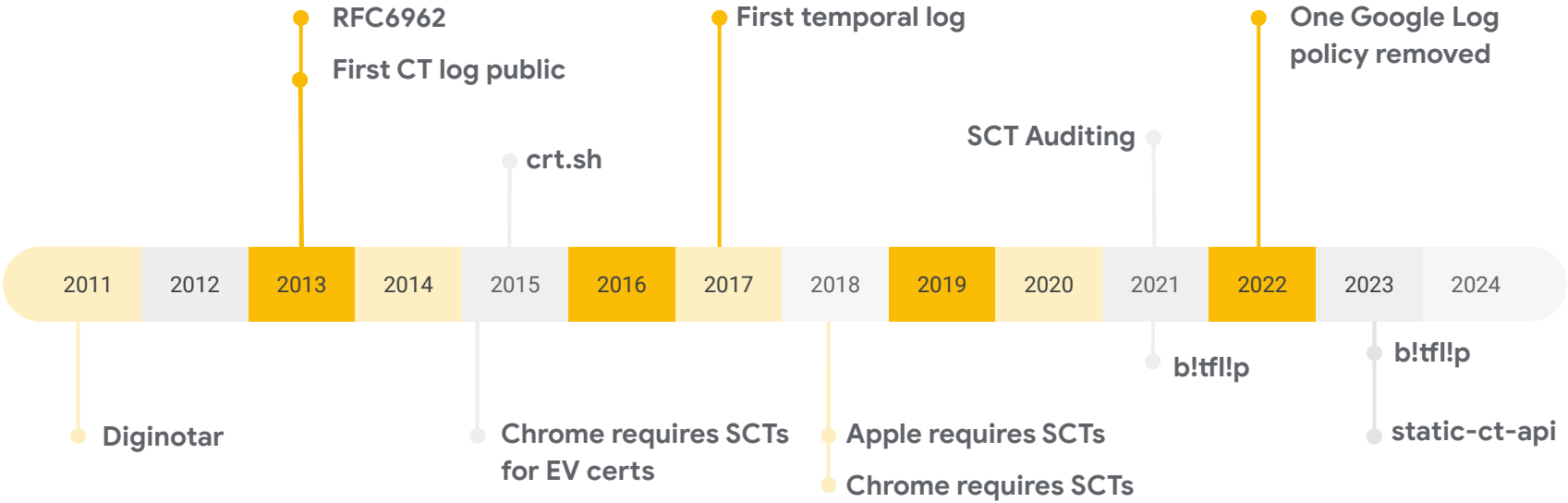
04 Verification

05 Coordination overhead

01

Introduction: CT

Evolution of CT



What happens if ***the*** log fails?

What happens if ***the*** log fails?

oops.

What happens if *a* log fails?

`nothing`

02

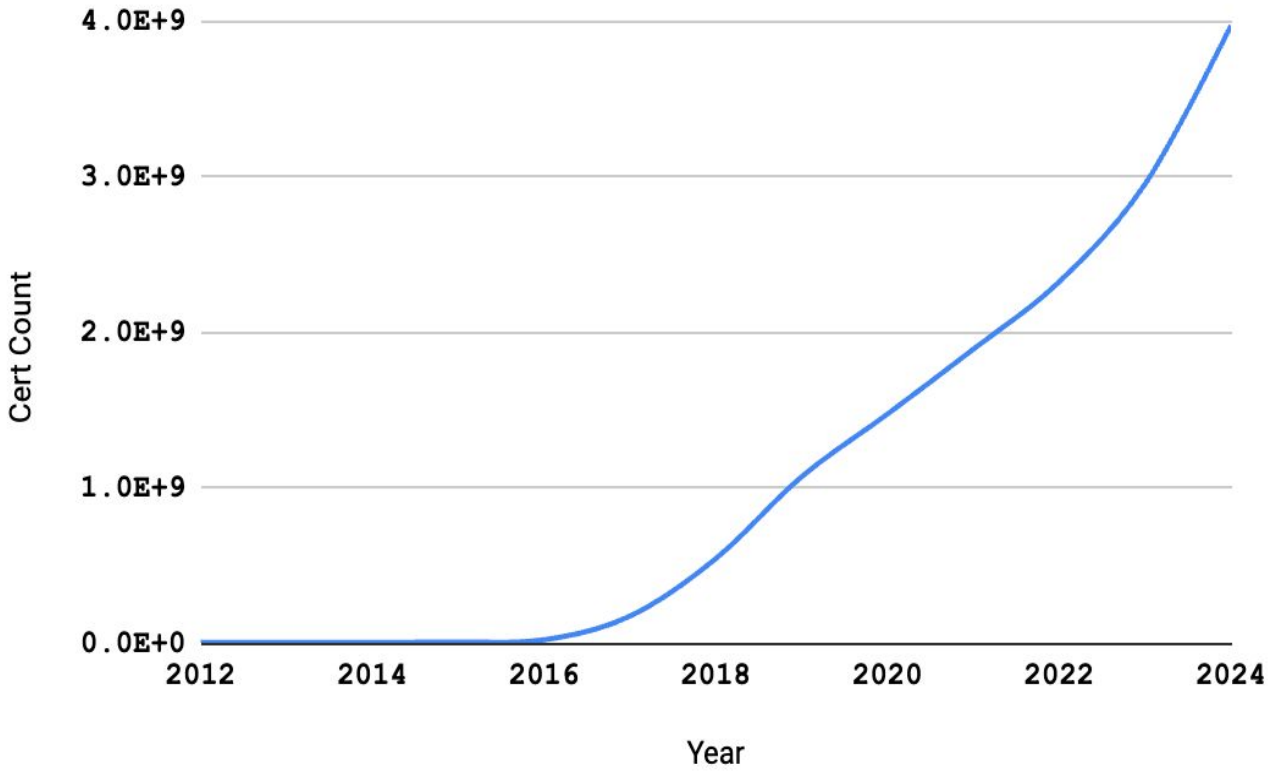
From one log to multiple logs

Why logs fail?

Integrity loss	Bitflips
	An entry is never included in the log
Availability	Can’t write to the log
	Can’t read from the log
Scalability	Logs grow fast
	Make sure you don’t run out of disk!
Compromise?	Unwanted data
	Split view

...

Number of certificates expiring every year*



How to configure clients with multiple logs?

How to configure clients with multiple logs?

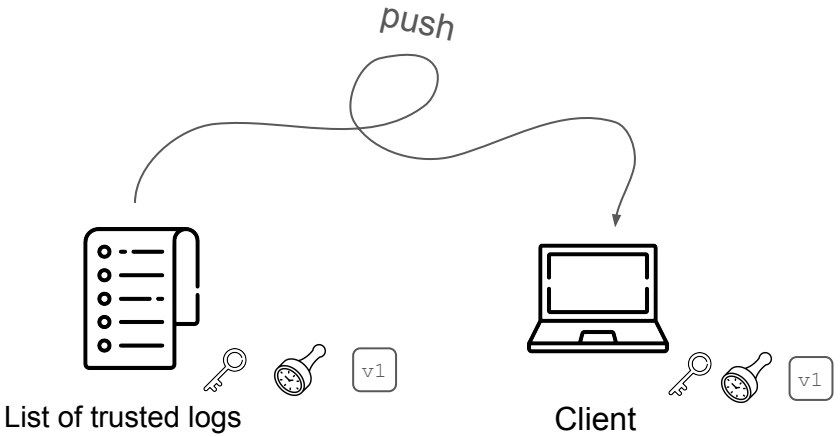
Push a log list with your binary!

How to configure clients with multiple logs?

Wait, how often do you update your binary?

How to configure clients with multiple logs?

- Dynamic push mechanism
- Signing
- Timestamping:
  - When do you start trusting a log?
  - When do you stop trusting a log?
  - How do you communicate this?
- How do you update your schema?



images: Flaticon.com

What happens if your entire *company* is compromised?

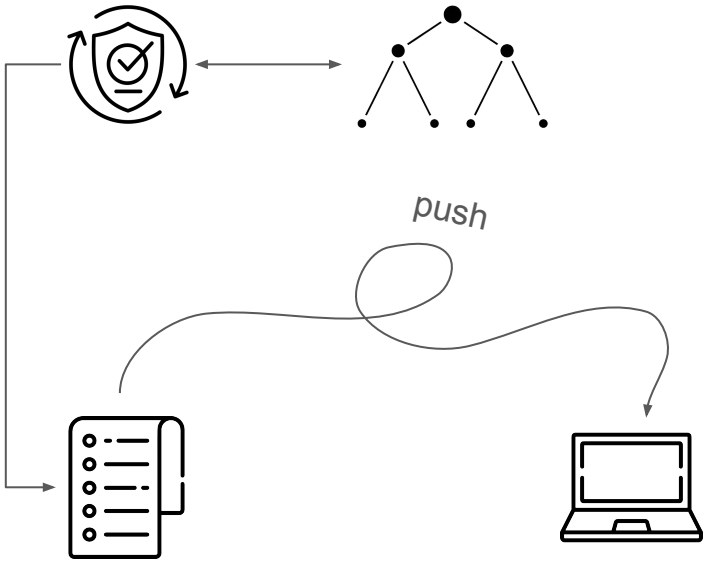
What happens if ***one*** *entire* company is compromised?

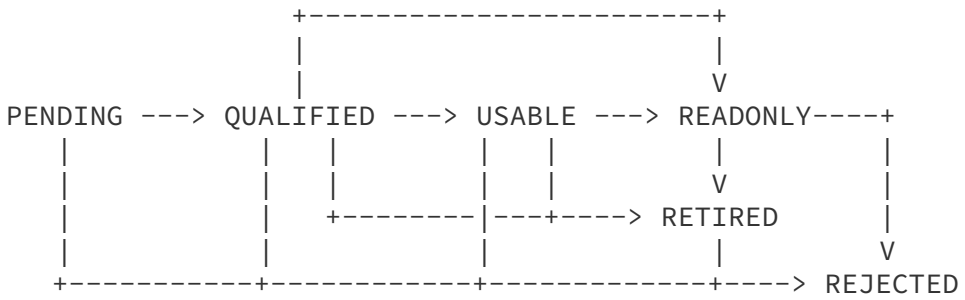
03

Multiple operators

What logs should you trust, and when?

Compliance monitoring





images: Flaticon.com

Chrome's policy

SCTs from two+ log operators,
with one+ still trusted.

Running a log can be ***hard***

Big responsibility

Append only, publicly writable, publicly visible, signed

System and human resources commitment

Business opportunity

Critical for the internet

We are taking steps to make it easier

Thank you

SECTIGO®

digicert®

CLOUDFLARE®

Let's Encrypt

亞洲誠信® TRUSTAsia

Google

04

Verification

CT doesn't help when **you don't look for misissuance**

CT

Only site owners can ID misissuance

- Nearly infinite site owners must opt-in
- Competes with cognitive burden of securing a site (e.g. CSP)
- No turn-key and free options

Centralize and automate detection

- Scaling *people* is *really* hard
- Avoid opt-in models
- Ensure end-to-end value

CT doesn't help when **you don't/can't act on alerts**

CT

How to detect mis-issuances?

Big orgs

- difficult to route
- false positives
- may be ignored

Small orgs

- how do I investigate?
- How do I report?

Be extremely clear about what happens when violations are detected

No SCTs

05

Coordination overhead

CT ecosystem in 2024

many

g00.gl

xyz.com

abc.co.uk

Domain owners

Google, BBC, usa.gov

plenty

CAs

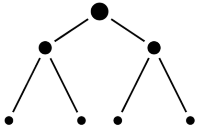
Google, Let's Encrypt, DigiCert

2+

User Agents

Apple platforms
Chrome
Chromium browsers
Android libraries
(More soon!)

6+



Log operators

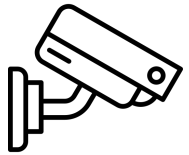
Cloudflare
Let's Encrypt
Google
Sectigo
TrustAsia
Digicert

12+

Log monitors

Censys
Cloudflare
crt.sh
Digicert
Entrust
Facebook
Keytos
Hardenize
Sslmate
Stellastra
Report-uri
Merklemap
...

3+

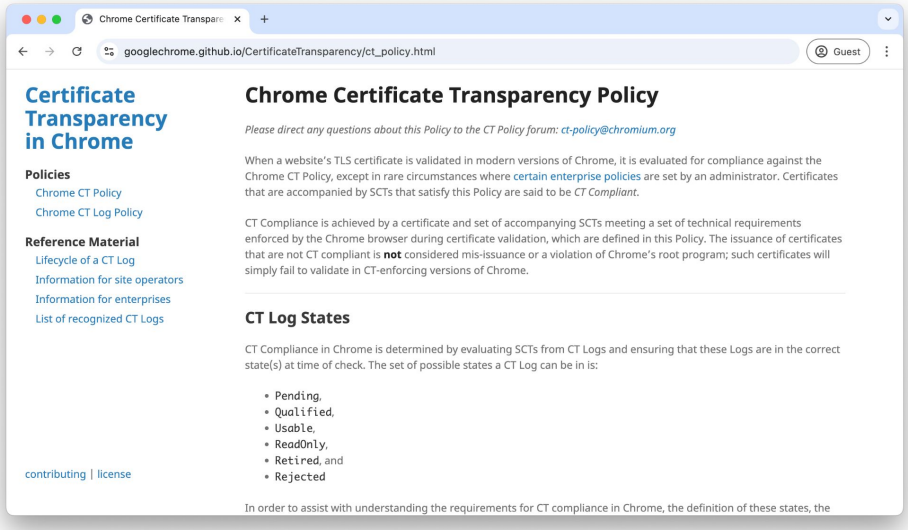


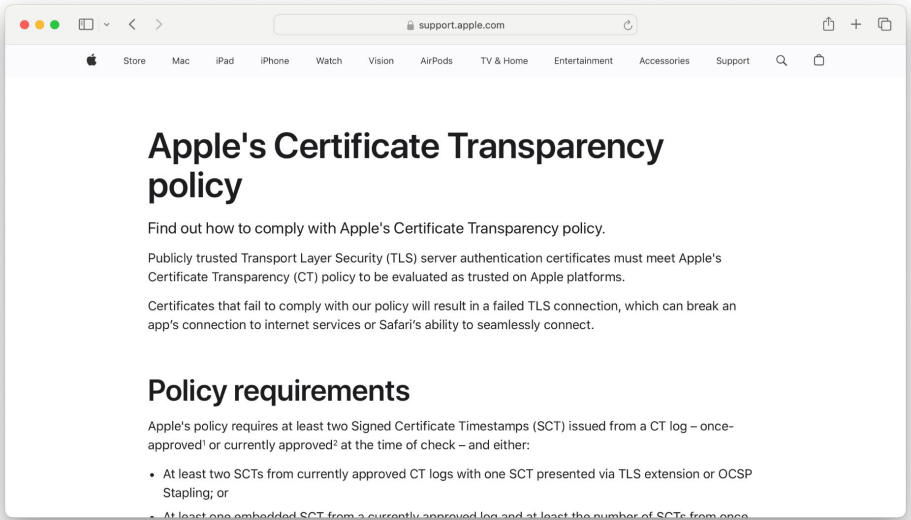
Log verifiers

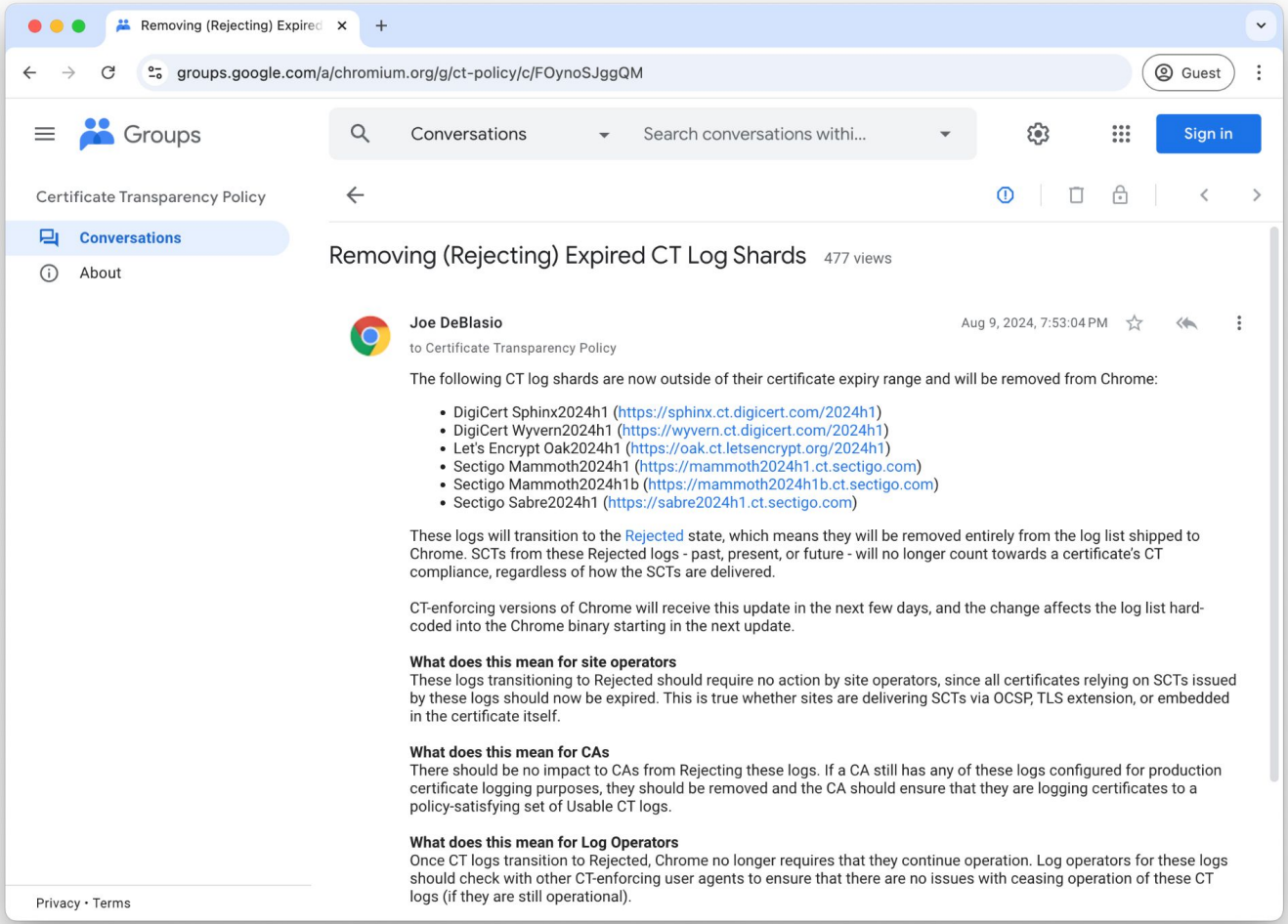
Cloudflare,
SSLMate
Sectigo
Google

images: Flaticon.com

Google


Chrome Certificate Transpare
googlechrome.github.io/CertificateTransparency/ct_policy.html
Guest
Certificate Transparency in Chrome
Policies
Chrome CT Policy
Chrome CT Log Policy
Reference Material
Lifecycle of a CT Log
Information for site operators
Information for enterprises
List of recognized CT Logs
contributing | license
Chrome Certificate Transparency Policy
Please direct any questions about this Policy to the CT Policy forum: ct-policy@chromium.org
When a website's TLS certificate is validated in modern versions of Chrome, it is evaluated for compliance against the Chrome CT Policy, except in rare circumstances where certain enterprise policies are set by an administrator. Certificates that are accompanied by SCTs that satisfy this Policy are said to be CT Compliant.
CT Compliance is achieved by a certificate and set of accompanying SCTs meeting a set of technical requirements enforced by the Chrome browser during certificate validation, which are defined in this Policy. The issuance of certificates that are not CT compliant is not considered mis-issuance or a violation of Chrome's root program; such certificates will simply fail to validate in CT-enforcing versions of Chrome.
CT Log States
CT Compliance in Chrome is determined by evaluating SCTs from CT Logs and ensuring that these Logs are in the correct state(s) at time of check. The set of possible states a CT Log can be in is:
Pending,
Qualified,
Usable,
ReadOnly,
Retired, and
Rejected
In order to assist with understanding the requirements for CT compliance in Chrome, the definition of these states, the


support.apple.com
Store
Mac
iPad
iPhone
Watch
Vision
AirPods
TV & Home
Entertainment
Accessories
Support
Apple's Certificate Transparency policy
Find out how to comply with Apple's Certificate Transparency policy.
Publicly trusted Transport Layer Security (TLS) server authentication certificates must meet Apple's Certificate Transparency (CT) policy to be evaluated as trusted on Apple platforms.
Certificates that fail to comply with our policy will result in a failed TLS connection, which can break an app's connection to internet services or Safari's ability to seamlessly connect.
Policy requirements
Apple's policy requires at least two Signed Certificate Timestamps (SCT) issued from a CT log – once-approved[1] or currently approved[2] at the time of check – and either:
At least two SCTs from currently approved CT logs with one SCT presented via TLS extension or OCSP Stapling; or


Removing (Rejecting) Expired
groups.google.com/a/chromium.org/g/ct-policy/c/FOynoSJggQM
Guest
Groups
Conversations
Search conversations withi...
Sign in
Certificate Transparency Policy
Conversations
About
Removing (Rejecting) Expired CT Log Shards 477 views
Joe DeBlasio
Aug 9, 2024, 7:53:04 PM
to Certificate Transparency Policy
The following CT log shards are now outside of their certificate expiry range and will be removed from Chrome:
DigiCert Sphinx2024h1 (https://sphinx.ct.digicert.com/2024h1)
DigiCert Wyvern2024h1 (https://wyvern.ct.digicert.com/2024h1)
Let's Encrypt Oak2024h1 (https://oak.ct.letsencrypt.org/2024h1)
Sectigo Mammoth2024h1 (https://mammoth2024h1.ct.sectigo.com)
Sectigo Mammoth2024h1b (https://mammoth2024h1b.ct.sectigo.com)
Sectigo Sabre2024h1 (https://sabre2024h1.ct.sectigo.com)
These logs will transition to the Rejected state, which means they will be removed entirely from the log list shipped to Chrome. SCTs from these Rejected logs - past, present, or future - will no longer count towards a certificate's CT compliance, regardless of how the SCTs are delivered.
CT-enforcing versions of Chrome will receive this update in the next few days, and the change affects the log list hard-coded into the Chrome binary starting in the next update.
What does this mean for site operators
These logs transitioning to Rejected should require no action by site operators, since all certificates relying on SCTs issued by these logs should now be expired. This is true whether sites are delivering SCTs via OCSP, TLS extension, or embedded in the certificate itself.
What does this mean for CAs
There should be no impact to CAs from Rejecting these logs. If a CA still has any of these logs configured for production certificate logging purposes, they should be removed and the CA should ensure that they are logging certificates to a policy-satisfying set of Usable CT logs.
What does this mean for Log Operators
Once CT logs transition to Rejected, Chrome no longer requires that they continue operation. Log operators for these logs should check with other CT-enforcing user agents to ensure that there are no issues with ceasing operation of these CT logs (if they are still operational).
Privacy • Terms

All of this is **slow**...
...so we have to focus on what matters.