

This is a slide



Transparency.Dev

Summit 2024



AI Cutter (al@google.com)
9th October 2024

Google



2010

2011

DigiNotar

2011 ½

Someone should **do** something.

2012

draft-laurie-pki-sunlight



A large, spreading oak tree with Spanish moss hanging from its branches, set in a grassy field. The tree is the central focus, with its thick trunk and numerous large, horizontal branches extending across the frame. The leaves are a vibrant green, and the Spanish moss is a pale, silvery-white color. The background shows a dense forest of similar trees, and the foreground is a grassy area with dappled sunlight.

2013

RFC6962

2015

An ecosystem starts to form



2015 - now



The ecosystem develops & matures

2024

Certificate Transparency wins the Levchin Prize at Real World Crypto

For creating and deploying Certificate Transparency at scale

Certificate Transparency was a response to the 2011 attack on DigiNotar and other Certificate Authorities. These attacks showed that the lack of transparency in the way CAs operate was a significant risk to the Web Public Key Infrastructure (PKI). It led to the creation of the Certificate Transparency project to improve Internet security by bringing accountability to the system that protects HTTPS. Since 2013, the Certificate Transparency community has effectively monitored and fixed certificate anomalies. The award recognizes the enormous effort that it took to make Certificate Transparency a reality on the Web, and the tangible security benefits that it brings to all Web users.

Uncertain times

Supply chain attacks

Dependency confusion

Fake news & disinformation

Impersonation & identity theft

Phishing

Fraud

Malware

...

Other applications & ecosystems

Binary transparency

Key transparency

Signature transparency

Firmware transparency

AI model transparency



Evolution of tooling

Open source logs

- C++ in memory (CT-only) [2013]
- Trillian (Generic) [2016]
 - Used in: CT, GoSumDB, Sigstore, Prod change logging, Food supply chain, ...
- Serverless (Generic) [2021]
- **Sunlight, itko (CT-only) [2024]**
- **Tessera (Generic, but opinionated) [2024]**

Evolution of tooling

Logs are now ***boring**** and ***commodity***

Evolution of protocols & formats

- RFC6962 STH → Generic **Checkpoint** ^[1]
- RPC, custom tiles → Generic **Tiles** ^[2]
- CT Gossip → Generic **Witnessing** ^[3]
- ? → ?

[1] <https://c2sp.org/tlog-checkpoint>

[2] <https://c2sp.org/tlog-tiles>

[3] <https://c2sp.org/tlog-witness>, <https://c2sp.org/tlog-cosignature>

Evolution of protocols, & formats

We're starting to get **interoperability**

Evolution of the bar for trust

`${THING}` (*perhaps + MD5SUM*)

`${THING}` + `${THING}.sig`

`${THING}` is logged

Putting things in logs doesn't matter



Putting things in logs doesn't matter

Discoverability and **verifying claims** does!

<https://alexgaynor.net/2024/sep/09/signatures-are-like-backups/>

<https://transparency.dev/articles/logs-a-verifiable-transport-layer/>

Evolution of the bar for trust

$\{\text{THING}\}$ (perhaps + MD5SUM)

$\{\text{THING}\}$ + $\{\text{THING}\}.\text{sig}$

$\{\text{THING}\}$ is logged

$\{\text{THING}\}$ is *transparent* ⇒ **Someone is accountable** for $\{\text{THING}\}$,
⇒ **Claims** about $\{\text{THING}\}$ are **falsifiable**,
⇒ There exist **entities able to verify claims**,
⇒ $\{\text{THING}\}$ is **discoverable**.

Your ecosystems need you 🙌

- **Use the C2SP specs** for formats & protocols
 - An easy way to start is: use Tesseract :)
- **Ensure your design is "closed"**
 - Claims are falsifiable, verifiers exist, discoverability holds.
 - C2SP specs help with some of this: → **witnessing!**
- **Demand transparency**

<https://transparency.dev/how-to-design-a-verifiable-system/>

Thank you

Enjoy your summit!

