#### This is a slide

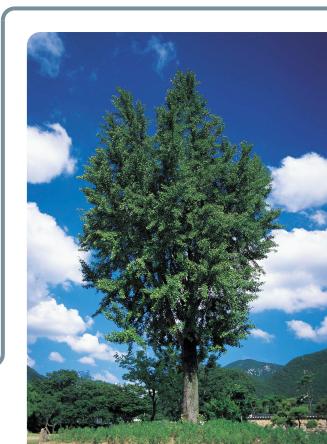


## Transparency.Dev

#### **Summit 2024**



Google



#### 



DigiNotar

#### 2011 1/2

### Someone should do something.



### draft-laurie-pki-sunlight



#### 2013

# **RFC6962**



### An ecosystem starts to form





#### 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 Al 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<sup>\*</sup> and commodity

#### **Evolution of protocols & formats**

- RFC6962 STH
- RPC, custom tiles
- CT Gossip
- ?

- $\rightarrow$  Generic Checkpoint <sup>[1]</sup>
- $\rightarrow$  Generic Tiles <sup>[2]</sup>
- $\rightarrow$  Generic Witnessing <sup>[3]</sup>

- [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**

- \${THING} (perhaps + MD5SUM)
- \${THING} + \${THING}.sig
- \${THING} is logged

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

#### Your ecosystems need you

#### Use the C2SP specs for formats & protocols

• An easy way to start is: use Tessera :)

#### Ensure your design is "closed"

- O Claims are falsifiable, verifiers exist, discoverability holds.
- $\bigcirc$  C2SP specs help with some of this:  $\rightarrow$  witnessing!

#### Demand transparency

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

#### Thank you

# **Enjoy your summit!**