



# Modern Transparency Logs

Filippo Valsorda



Obsoleted by: [9162](#)

Internet Engineering Task Force (IETF)

Request for Comments: 6962

Category: Experimental

ISSN: 2070-1721

**Levchin Prize  
Winner**

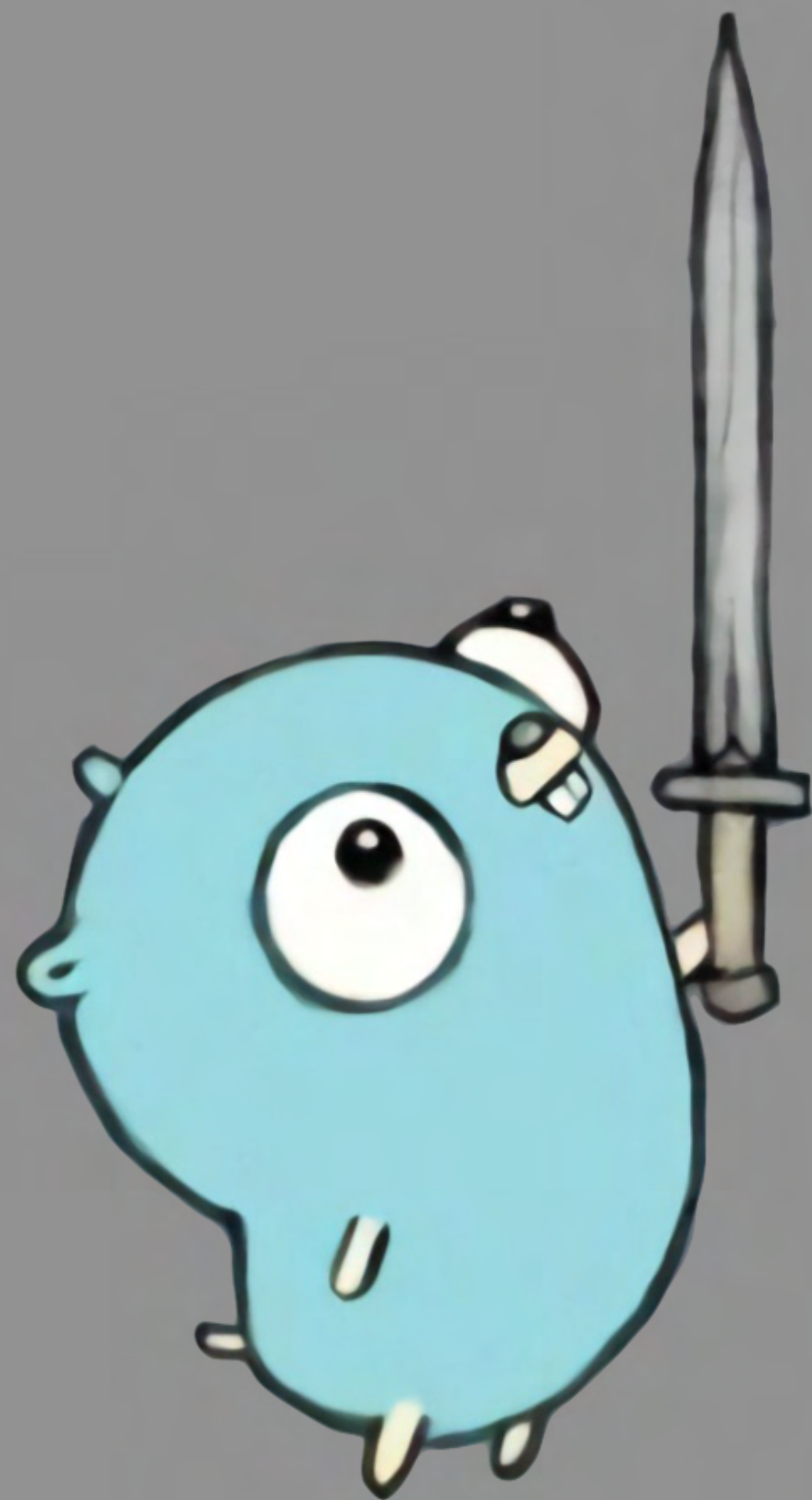
## Certificate Transparency

This document describes an experimental protocol for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed, in a manner that allows anyone to audit certificate authority (CA) activity and notice the issuance of suspect certificates as well as to audit the certificate logs themselves. The intent is that eventually clients would refuse to honor certificates that do not appear in a log, effectively forcing CAs to add all issued certificates to the logs.

Logs are network services that implement the protocol operations for submissions and queries that are defined in this document.

Status of This Memo

**ata Exist**  
**B. Laurie**  
**A. Langley**  
**E. Kasper**  
**Google**  
**June 2013**



**Filippo Valsorda**

**Go cryptography  
maintainer since  
2018**

**At Google until 2022**

**The Go Checksum  
Database**

**Sunlight**

**TLS 1.3, Privacy Pass, age,  
mkcert**



L A T A C O R A

INTERCHAIN  
FOUNDATION



smallstep

Ava  
Labs.



Teleport

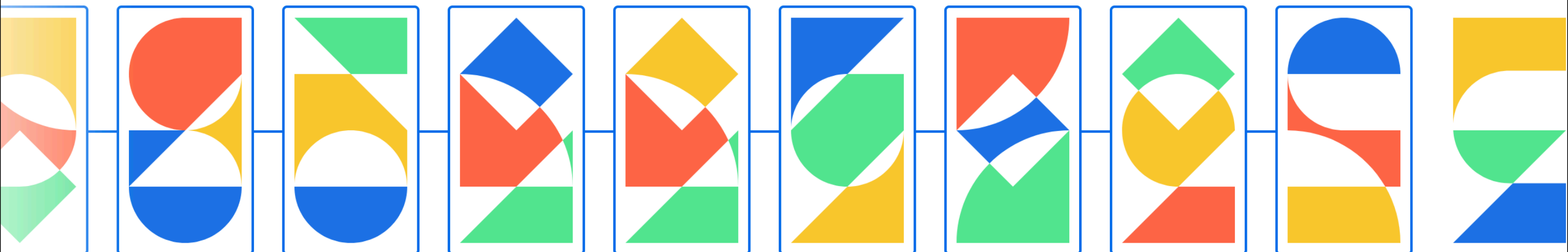


tailscale





# Trust your data with a tamper-evident log



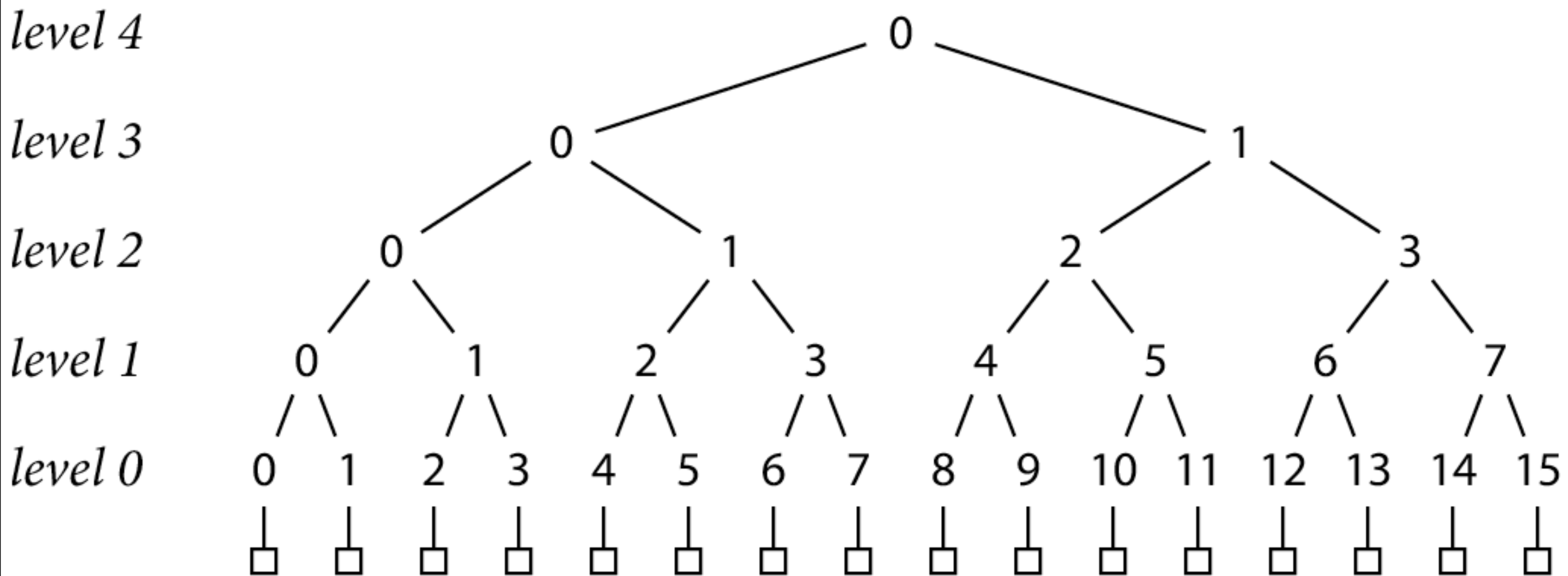
**You need to trust the data you rely on.** Your organisation handles more data every day, and the data helps you make critical decisions. But you need to know that it hasn't been modified or corrupted.





**What is a tlog**









**What are the entries?**  
**Who can add entries?**  
**Who monitors entries?**



A nighttime photograph of a river scene. In the foreground, a wide, paved walkway runs along the riverbank, illuminated by small, rectangular ground lights. To the right, a stone bridge with multiple arches spans the river. In the background, a large, multi-story building with a central tower and palm trees sits atop a hill. The scene is lit with warm, yellowish light, and the sky is dark.

**Do you need a “bulletin board”?**

**This is a “bulletin board”**





**What are the entries?**  
**Who can add entries?**  
**Who monitors entries?**



---

*Transparency tech provides  
accountability for data*

---





**Ultimately,  
transparency  
is about  
reputation  
staking**



# Split view attacks

| Present different versions of a log to hide data

**Local consistency and gossip  
don't work to protect against  
system  
compromise**





**Witness  
co signing**



# Witnesses are

1. Third-party cosigners
2. Reputational units
3. Part of a M-of-N policy
4. Lightweight
5. Reliable long-term





# The witness network



**The witness network is the  
part of a transparency  
system you can't build alone**

**Building an ecosystem is  
Hard, but we need to**



# Armored Witness<sup>1</sup>



1. <https://github.com/transparency-dev/armored-witness>

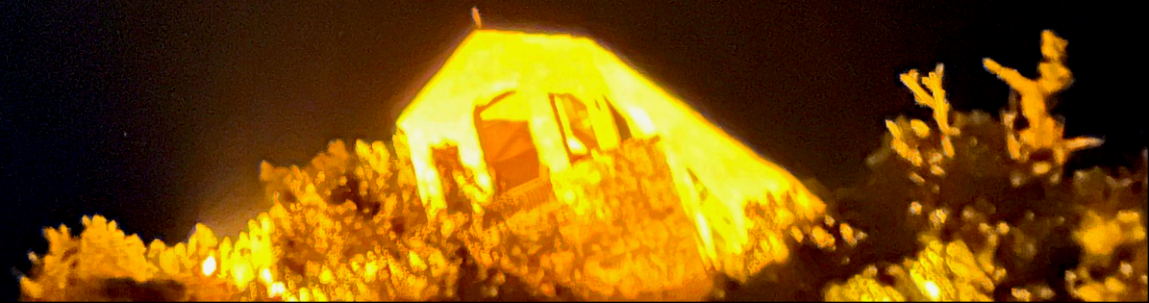




**Deploying tlogs**



SCTs





# Tiles

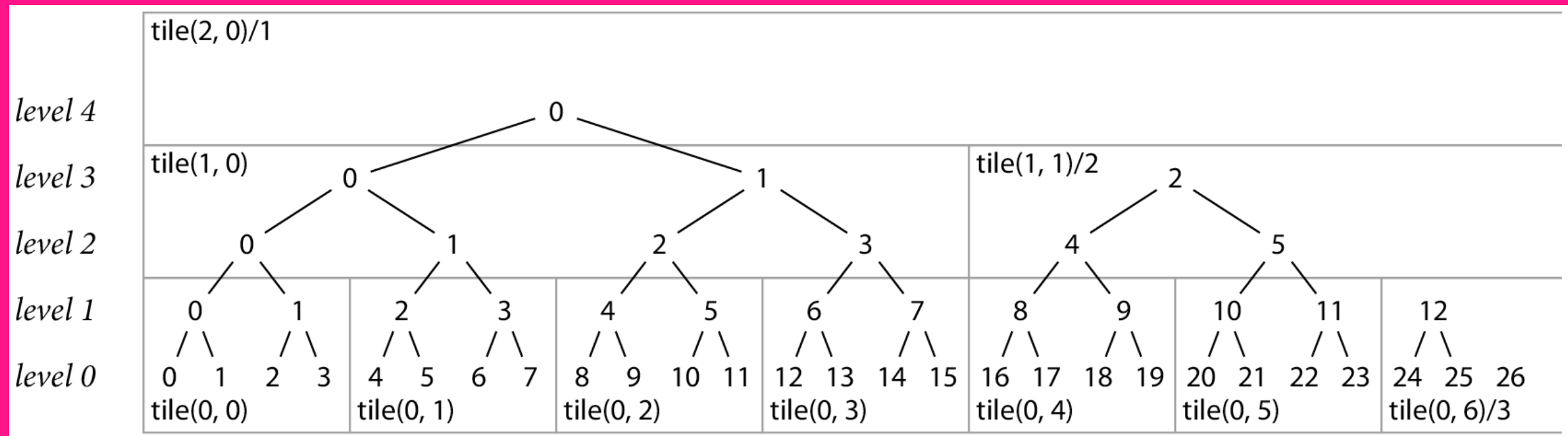


diagram by russ cox – <https://research.swtch.com/tlog>



# The checkpoint

<https://c2sp.org/tlog-checkpoint>

```
example.com/fancylog
```


```
109482
```

```
sFodV/vSp5O8n9a8QpW6PRY97tfOSW5bsc2X1/EQi08=
```

```
– example.com/fancylog hI2DwH[...]Q8MJloI=
```

```
– witness.example/winter 8w3N9V[...]5YZRDngg==
```





**Spicy  
signature =  
inclusion proof +  
signed checkpoint +  
m-of-n cosignatures**





# Spicy signature

```
index 73894
gSKyXoYZUgZ6jduWYrkDOARinOMGJveXjgMkBTcdPlQ=
B95lDa8R83lS8n0eG+o0buTxRKQTYFi//1U8anccXmA=
EKNzoDWG8LGC0Yp9o+sv3q1lpMP9uHQ9B20KNL+Q1zs=
RoopEkOdqkYqMB4MJXrbt/hMjOxsVn0IrWj pz1ZMMes=
AHCioX9nLjsrse6YhjRRmk1WUEirVOLLRoOQ6vfO5vk=
```

```
example.com/fancylog
109482
sFodV/vSp508n9a8QpW6PRY97tfOSW5bsc2Xl/EQi08=
```

```
- example.com/fancylog hI2DJw[...]1roIoI=
- witness1.example mJirIklj[...]qY9v2B/5bg==
- witness2.example TnKKVHLX[...]xwYwrSjgow==
- witness3.example S4X82uH5[...]3oEcROGLFQ==
```



**You don't have to  
call them 🌶️ spicy  
signatures**

**Offline-verifiable proofs is ok**



# **Spicy signatures**

**Like a digital  
signature, but  
"tlogged"**







# Implementations



```
$ spicy -assets ./log -key log42.key \  
    leafX.txt leafY.txt
```

Log loaded.

- Name: example.com/log42
- Current size: 0
- Assets directory: ./log
- + "leafX.txt" is now entry 0
- + "leafY.txt" is now entry 1
- New size: 2

Spicy signatures written! 🌶️



```
# cp apt-transport-tlog.py /usr/lib/apt/methods/tlog
```

```
# cat > /etc/apt/sources.list
```

```
deb tlog://deb.debian.org/debian stable main
```

```
deb tlog://deb.debian.org/debian stable-updates main
```

```
# apt update
```

```
Hit:1 tlog://deb.debian.org/debian stable InRelease
```

```
Get:2 tlog://deb.debian.org/debian stable-updates InRelease [55.4 kB]
```

```
 tlog://deb.debian.org/debian stable-updates InRelease.spicy
```

```
Get:3 tlog://deb.debian.org/debian stable-updates/main arm64 Packages [12.5 kB]
```

```
Fetched 67.9 kB in 11s (5946 B/s)
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
Reading state information... Done
```

```
All packages are up to date.
```





# Checksum Database

**Tiles and  
checkpoints**

**One hash per  
version**

**Low latency**





**Public log of signatures**

**Anti-spam and anti-poisoning**

**Offline proofs (🌶️!)**



**Cheap,  
simple CT log**

**Tiles and  
checkpoints**

**SCT extension**

**Single node, object  
storage backed**



**SUNLIGHT**






 <https://filippo.io/rwc2024>

 <https://filippo.io/newsletter>

 [@filippo.abyssdomain.expert](https://twitter.com/filippo.abyssdomain.expert)

 [@filippo@abyssdomain.expert](https://t.me/filippo@abyssdomain.expert)

 [filippo@golang.org](mailto:filippo@golang.org)

 [transparency-dev Slack](#)