Sunlight is the best disinfectant…

Sunlight is the best disinfectant...

... actually, it's really not;

polyhexamethylene biguanide is much better, but not nearly as catchy...

What's the point?!

- Remember the IANA transition discussions?!
    - Fun, weren't they?
- One of the refrains was: "The IANA functions have to stay in the US; if it goes to Elbonia, IANA might be compelled to remove Belka from the root zone".
    - Well, the IANA functions stayed in the US...
    - ... did this actually remove the threat?
- Wouldn't it be nice if we could address this threat?
    - We can!

A brief detour into certs...

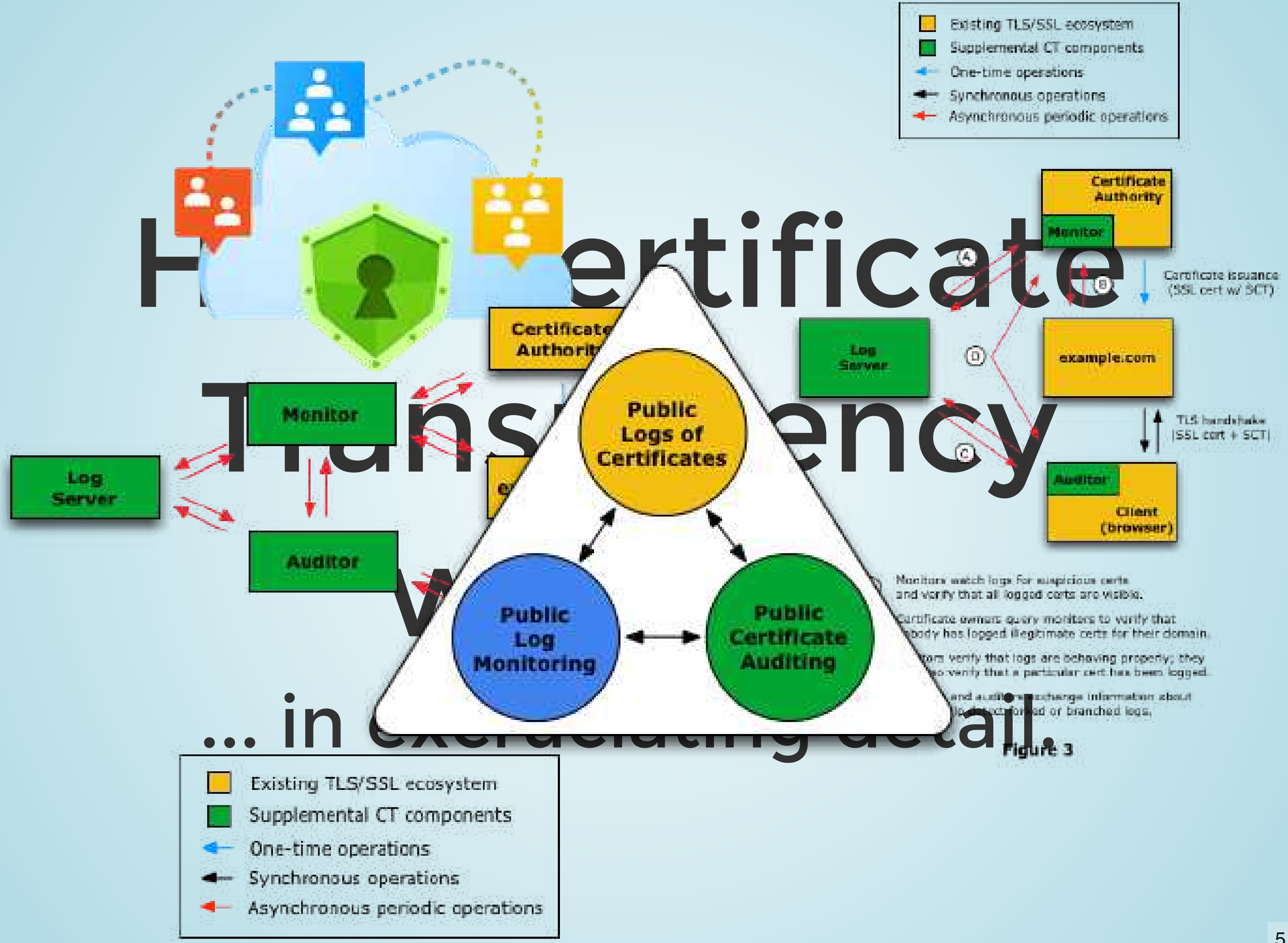
- The CA model sucks
  - I have a great soapbox rant....
    - ... but I'll spare you it.

Not just me / us who are unhappy
Browser vendors as well:

- LetsEncrypt
  - Complete the race to the bottom
- Certificate Transparency
  - Expose all certificates

How Certificate Transparency works

... in excruciating detail.



Existing TLS/SSL ecosystem
Supplemental CT components
One-time operations
Synchronous operations
Asynchronous periodic operations
Certificate Authority
Monitor
Certificate issuance (SSL cert w/ SCT)
Log Server
example.com
TLS handshake (SSL cert + SCT)
Auditor
Client (browser)
A
B
C
D
Monitors watch logs for suspicious certs and verify that all logged certs are visible.
Certificate owners query monitors to verify that nobody has logged illegitimate certs for their domain.
...ors verify that logs are behaving properly; they ...so verify that a particular cert has been logged.
...and auditors exchange information about ...to detect forked or branched logs.
Figure 3
Public Logs of Certificates
Public Log Monitoring
Public Certificate Auditing
Certificate Authority
Monitor
Log Server
Auditor
🟨 Existing TLS/SSL ecosystem
🟩 Supplemental CT components
One-time operations
Synchronous operations
Asynchronous periodic operations

Merkle Trees!

Like blockchains...

...but hipper

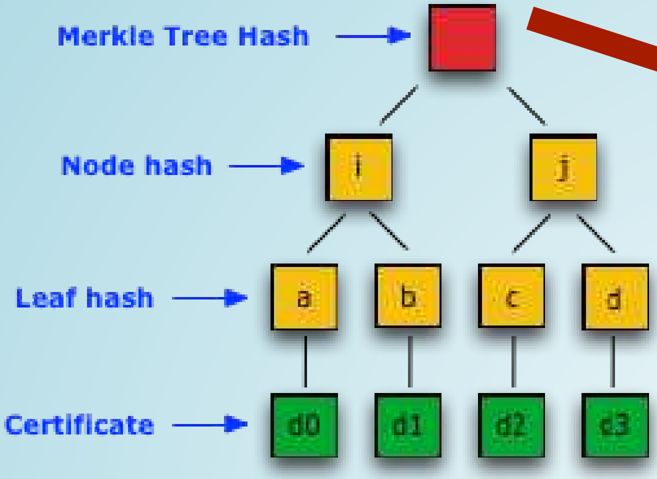


Figure 1

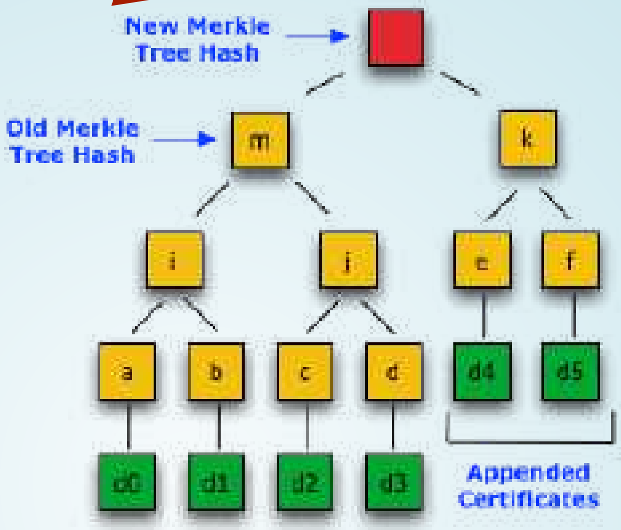


Figure 2

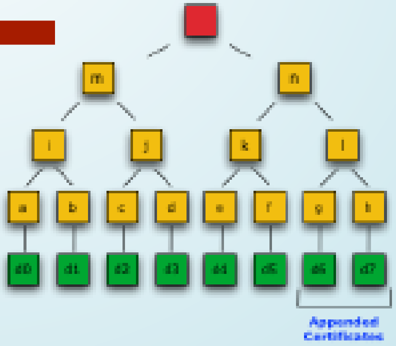


Figure 3

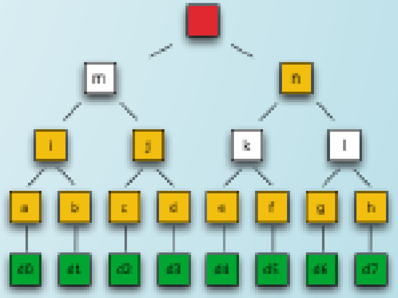


Figure 4

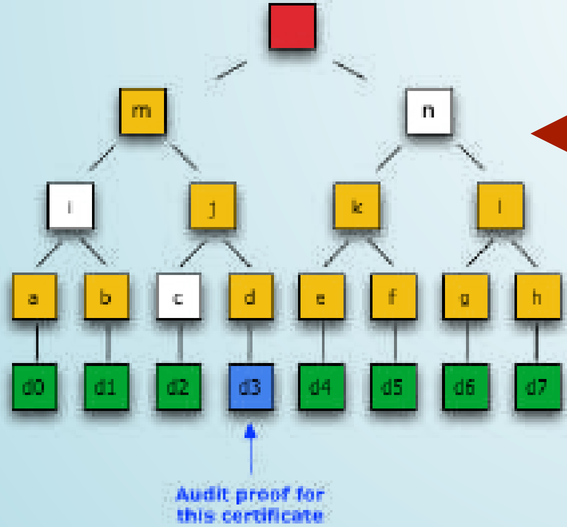


Figure 5

Gratuitous Kitten

Image: CC BY 2.0, "Red American kitten and baby duck"- Chief Trent

Certificate Transparency logs

- **Append-only**: certificates can only be added to a log; certificates can't be deleted, modified, or retroactively inserted into a log.

- **Cryptographically assured**: logs use a special cryptographic mechanism known as Merkle Tree Hashes to prevent tampering and misbehavior.

- **Publicly auditable**: anyone can query a log and verify that it's well behaved, or verify that an SSL certificate has been legitimately appended to the log.

Wow! Cool! Sexy! So what?!

- Don't want Elbonia to be able to remove Belka from the root zone.
  - Or the USA to be able to remove, well, anyone.

- Sorry, can't guarantee that.

  ...got you here under false pretenses.

- **Can** expose that this happened, which might be good enough.
  - If it is clear that the IANA was compelled to do something, then (hopefully) they won't be.

How?!

All changes to the root zone require a proof

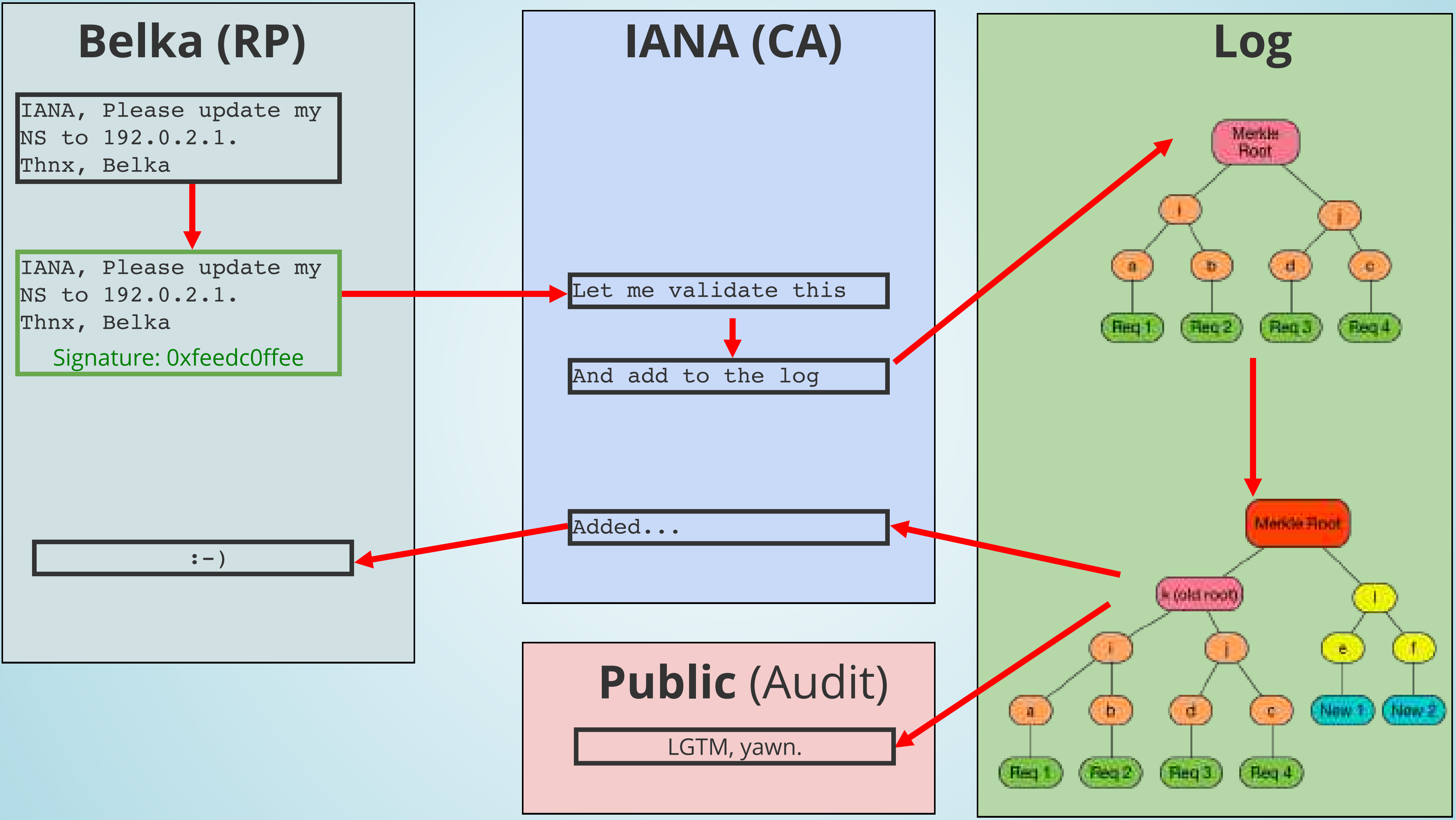
which is simply a cryptographic signature of the request,

published in a Certificate Transparency style log

which anyone can verify (audit)

and the log operator / IANA cannot (be forced to) fake log entries

Example



Belka (RP)

```
IANA, Please update my
NS to 192.0.2.1.
Thnx, Belka
```

```
IANA, Please update my
NS to 192.0.2.1.
Thnx, Belka
```

Signature: 0xfeedc0ffee

```
:-)
```

IANA (CA)

```
Let me validate this
```

```
And add to the log
```

```
Added...
```

Log

Public (Audit)

LGTM, yawn.

Example

Elbonia (RP)

IANA, Ordering you to update Belka NS to 192.0.2.1.

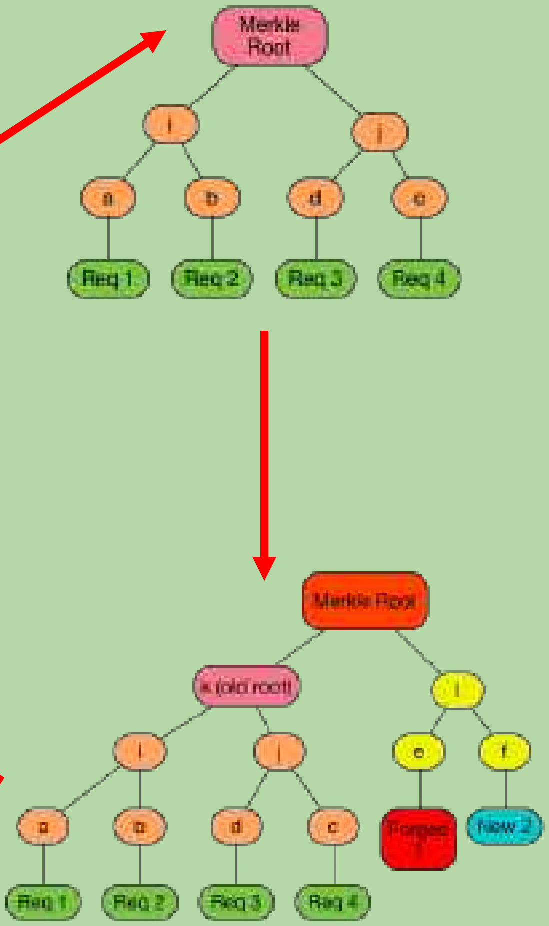
No. Just do it...

IANA (CA)

Please provide signature

Oh. Ok. Fair 'nuff...

Log



Public (Audit)

Oi! Shenanigans!

Bad Elbonia... or bad someone....

Questions?