Key Transparency

My friends have phone numbers, not public keys

Thibault Meunier
Cloudflare

Who am I

Research at Cloudflare

Discussion topics

1. Privacy, Signatures, Bot, Cache
2. Home automation
3. Butter croissant

Agenda

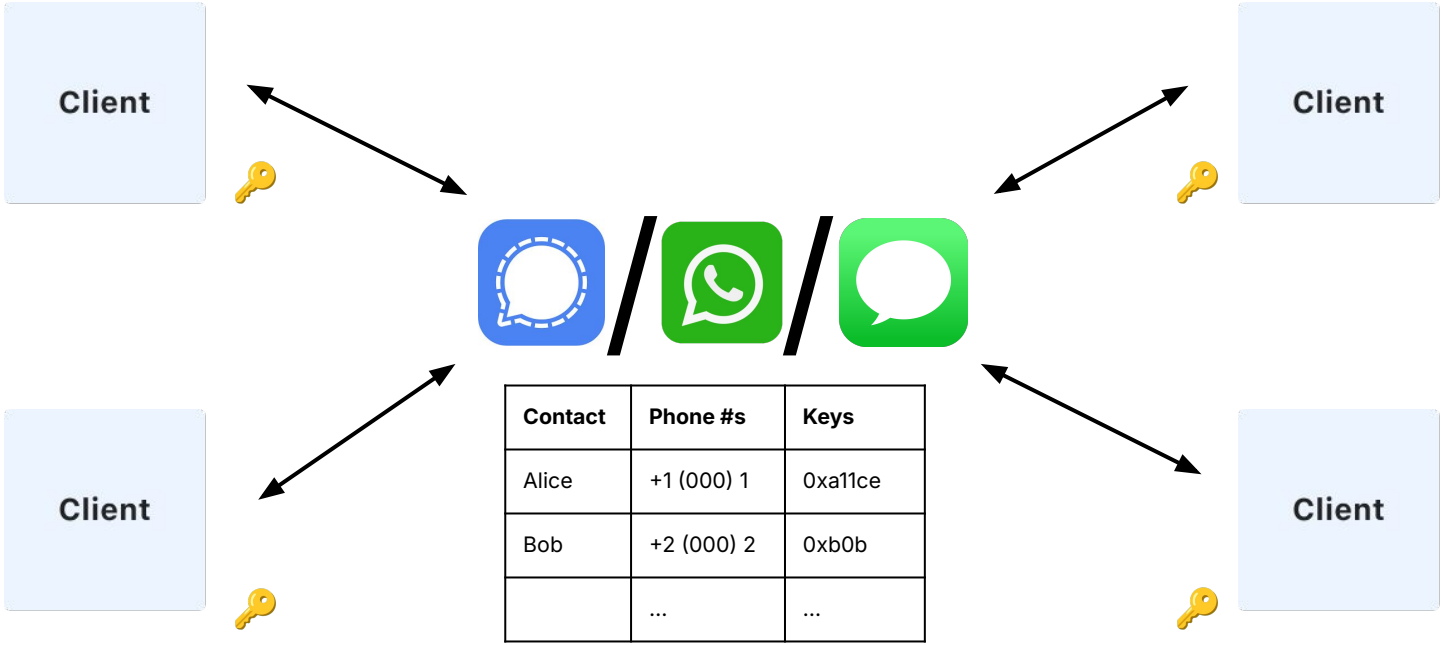
1. Introduction to Key Transparency
2. Auditor system design
3. Real-world deployment
4. What’s next

Section

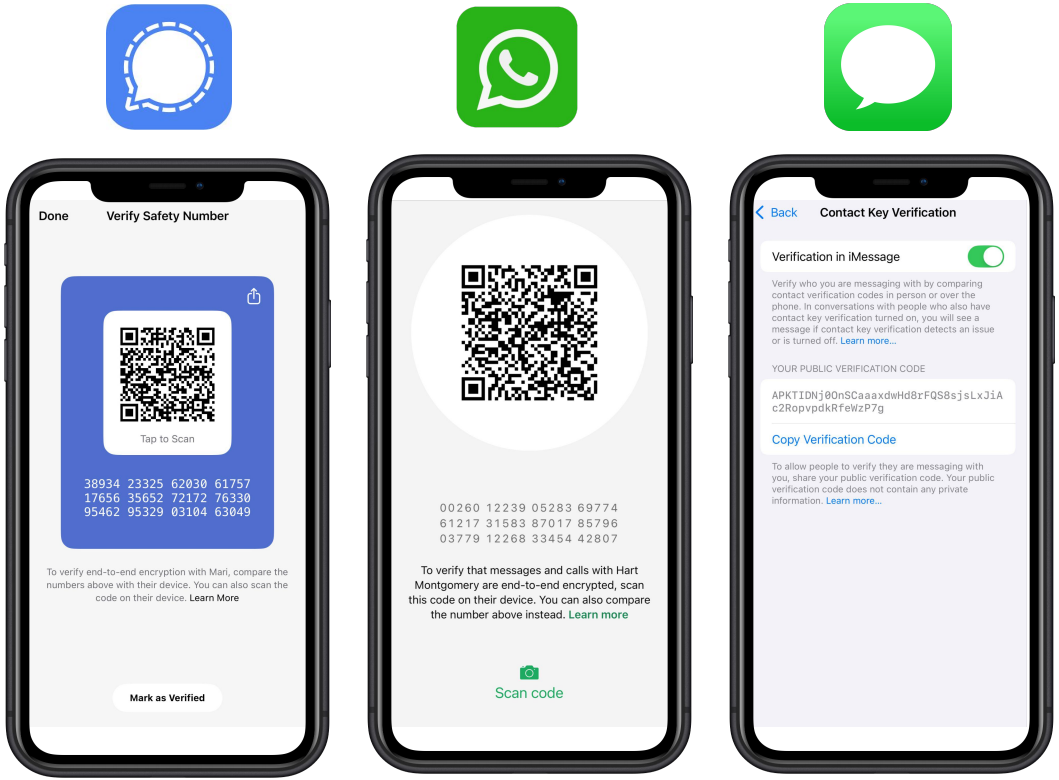
Introduction to Key Transparency

CLOUDFLARE

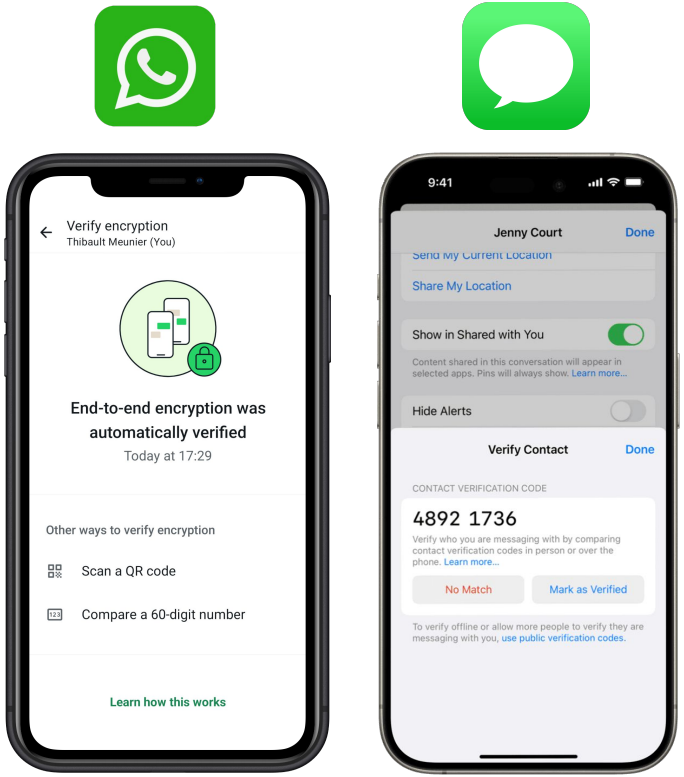
E2EE Messaging



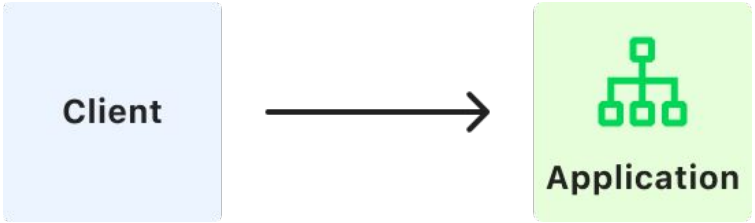
QR Codes


Done
Verify Safety Number
Tap to Scan
38934 23325 62030 61757
17656 35652 72172 76330
95462 95329 03104 63049
To verify end-to-end encryption with Mari, compare the numbers above with their device. You can also scan the code on their device. Learn More
Mark as Verified
00260 12239 05283 69774
61217 31583 87017 85796
03779 12268 33454 42807
To verify that messages and calls with Hart Montgomery are end-to-end encrypted, scan this code on their device. You can also compare the number above instead. Learn more
Scan code
Back
Contact Key Verification
Verification in iMessage
Verify who you are messaging with by comparing contact verification codes in person or over the phone. In conversations with people who also have contact key verification turned on, you will see a message if contact key verification detects an issue or is turned off. Learn more...
YOUR PUBLIC VERIFICATION CODE
APKTIDNj0OnSCaaaxdwHd8rFQS8sjsLxJiA
c2RopvpdkRfeWzP7g
Copy Verification Code
To allow people to verify they are messaging with you, share your public verification code. Your public verification code does not contain any private information. Learn more...

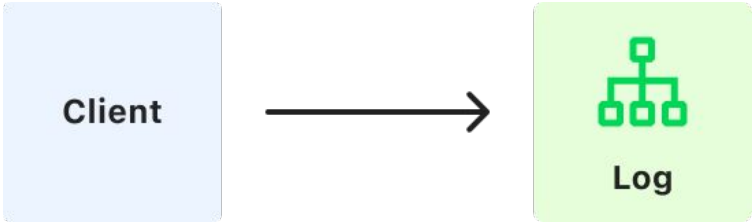
Key Transparency



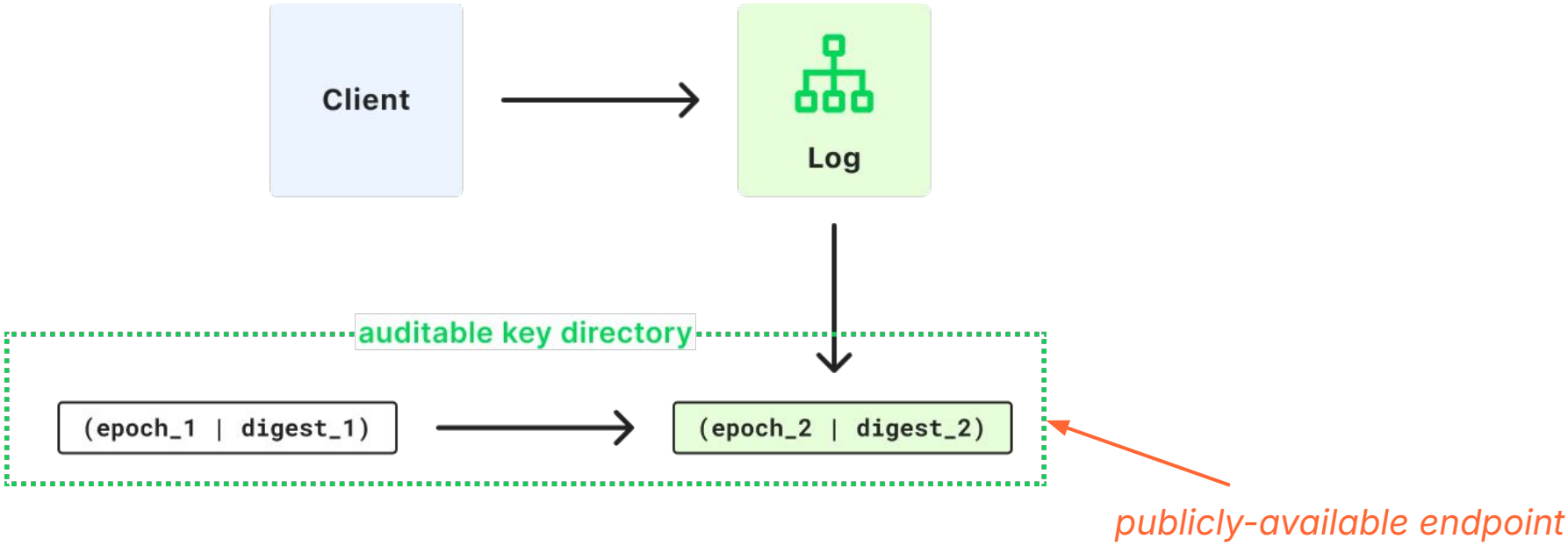
Key Transparency - Before



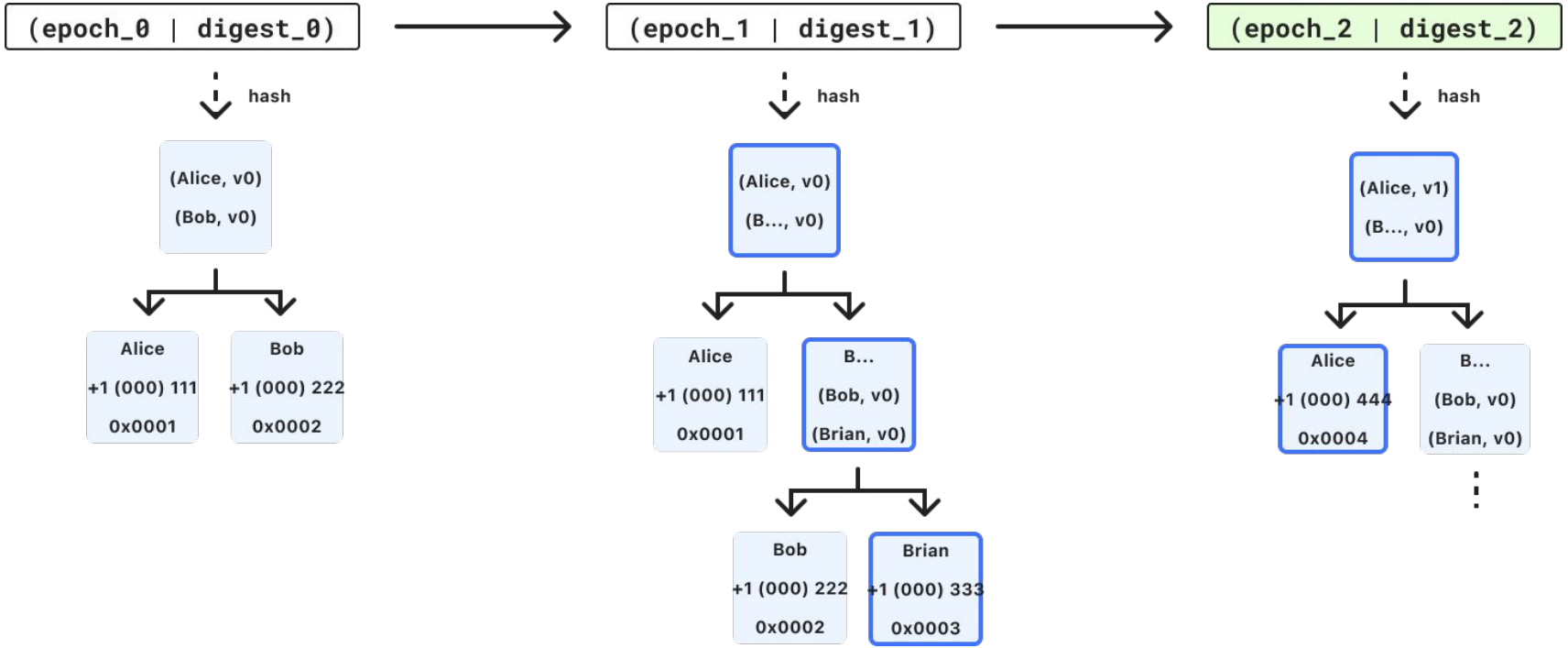
Key Transparency - Log



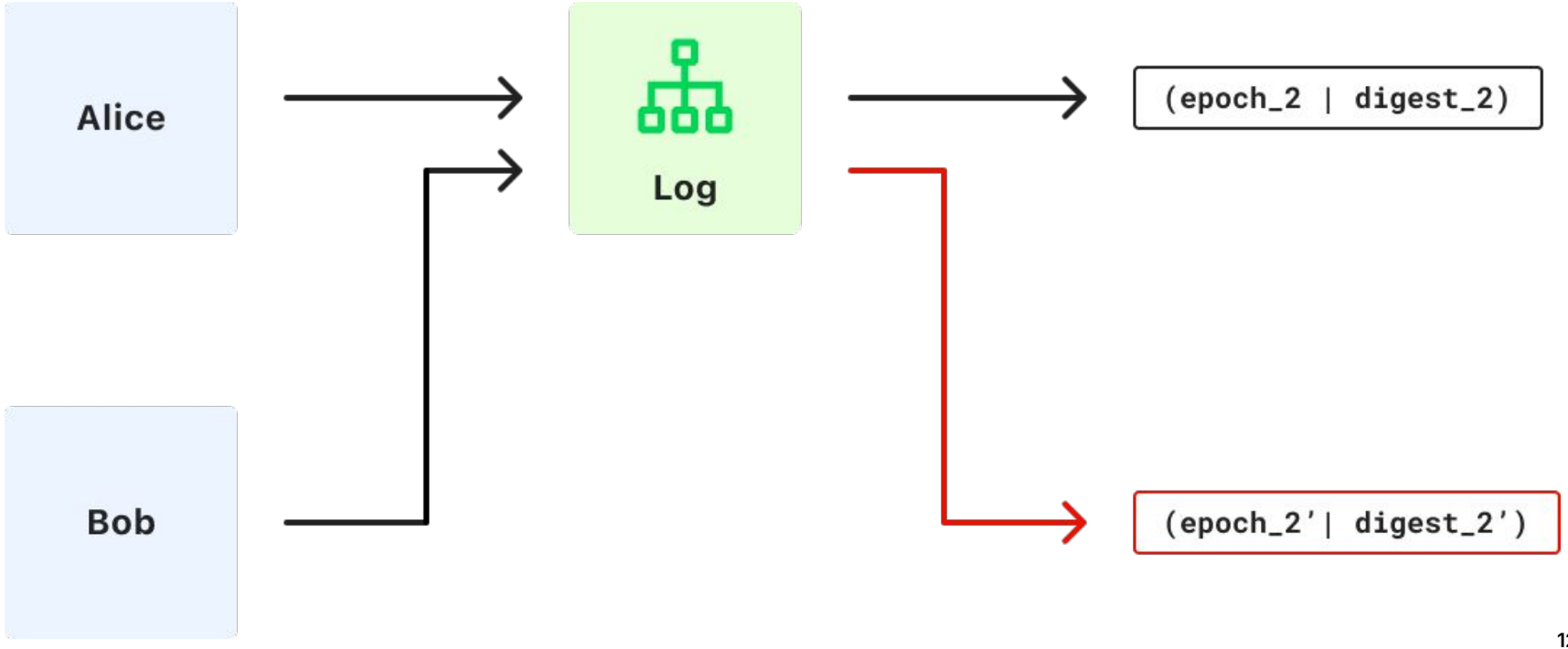
Key Transparency – Client and AKD



Key Transparency – Auditable Key Directory (AKD)



Key Transparency – split view attack

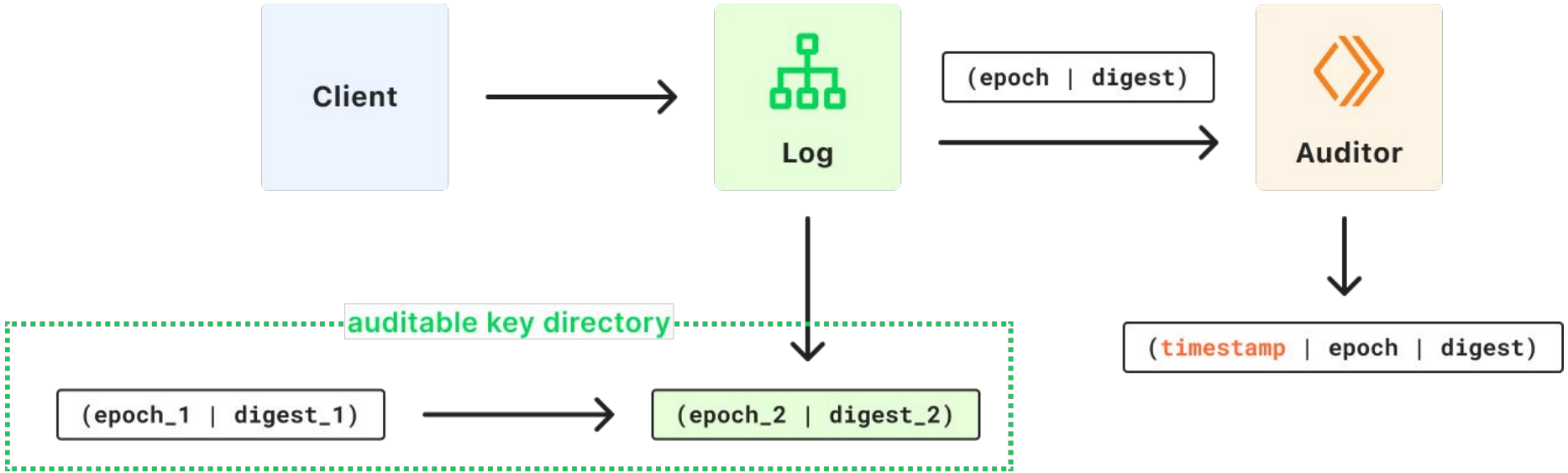


Section

Auditor system design

CLOUDFLARE

Introducing the Auditor



What is the Auditor responsible for?

Witnessing

Ensures epochs are unique and in sequential order.

Monitoring

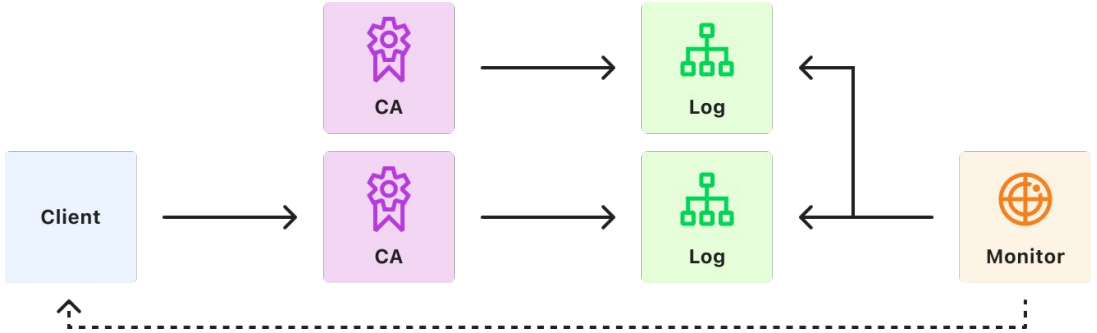
Making sure that the AKD is correctly constructed and that all epochs transitions are valids.

Privacy preserving

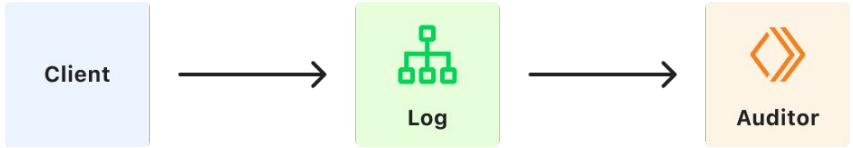
Does not see users' private information: no name, no phone number, no public key. It is a trusted third party.

How does that relate to Certificate Transparency

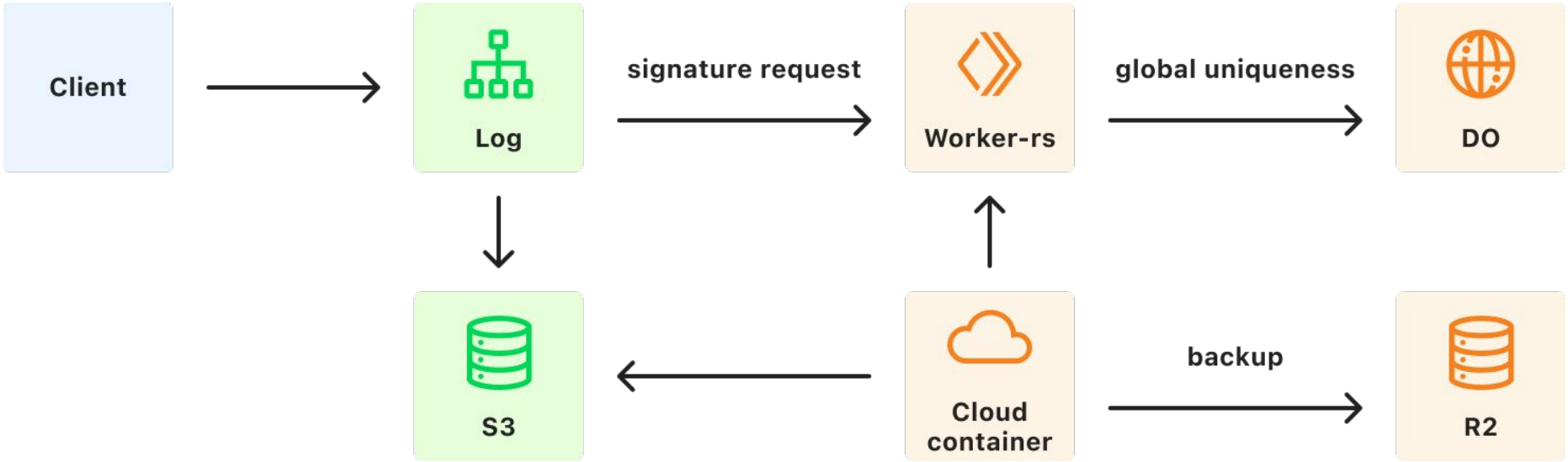
Certificate Transparency



Key Transparency



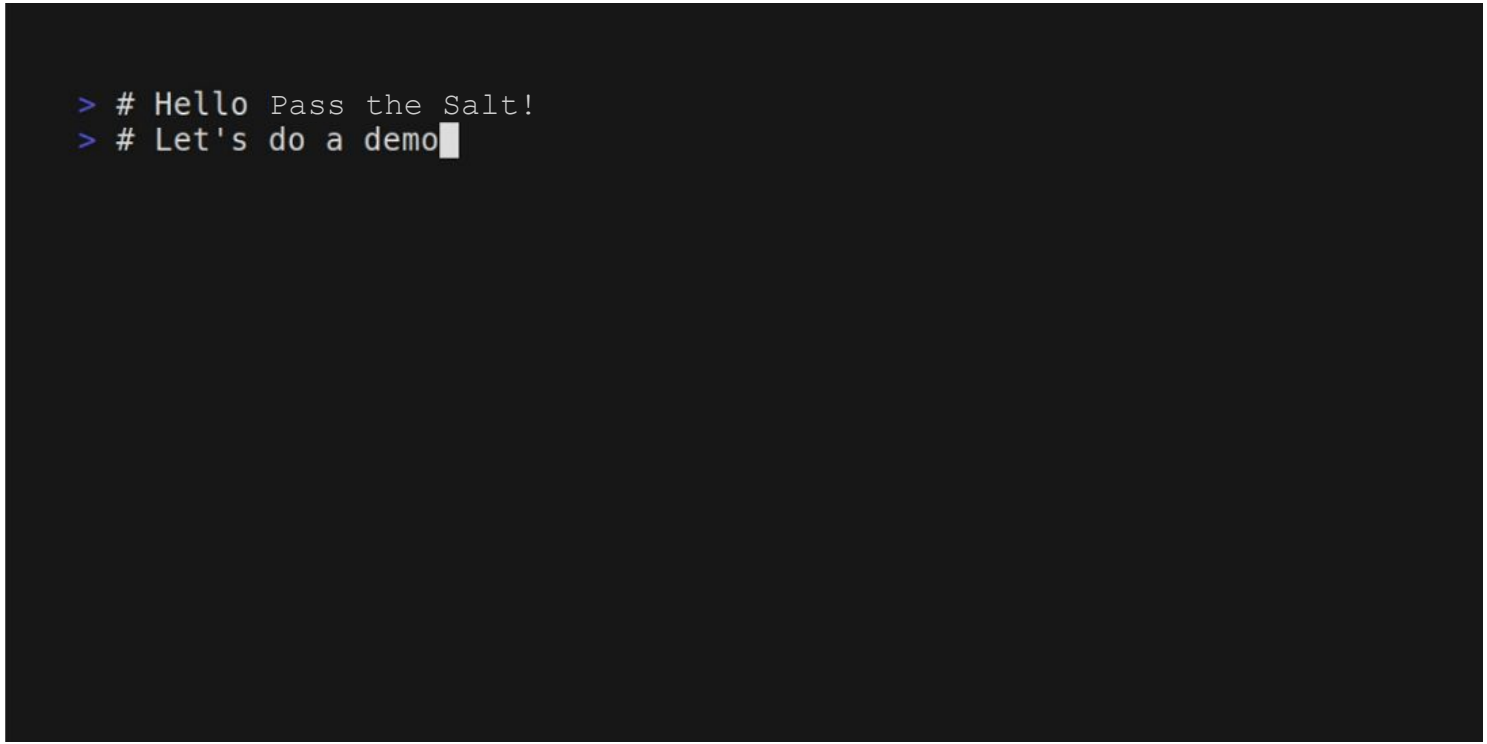
Validating epoch uniqueness and transitions



Section

Real world deployment

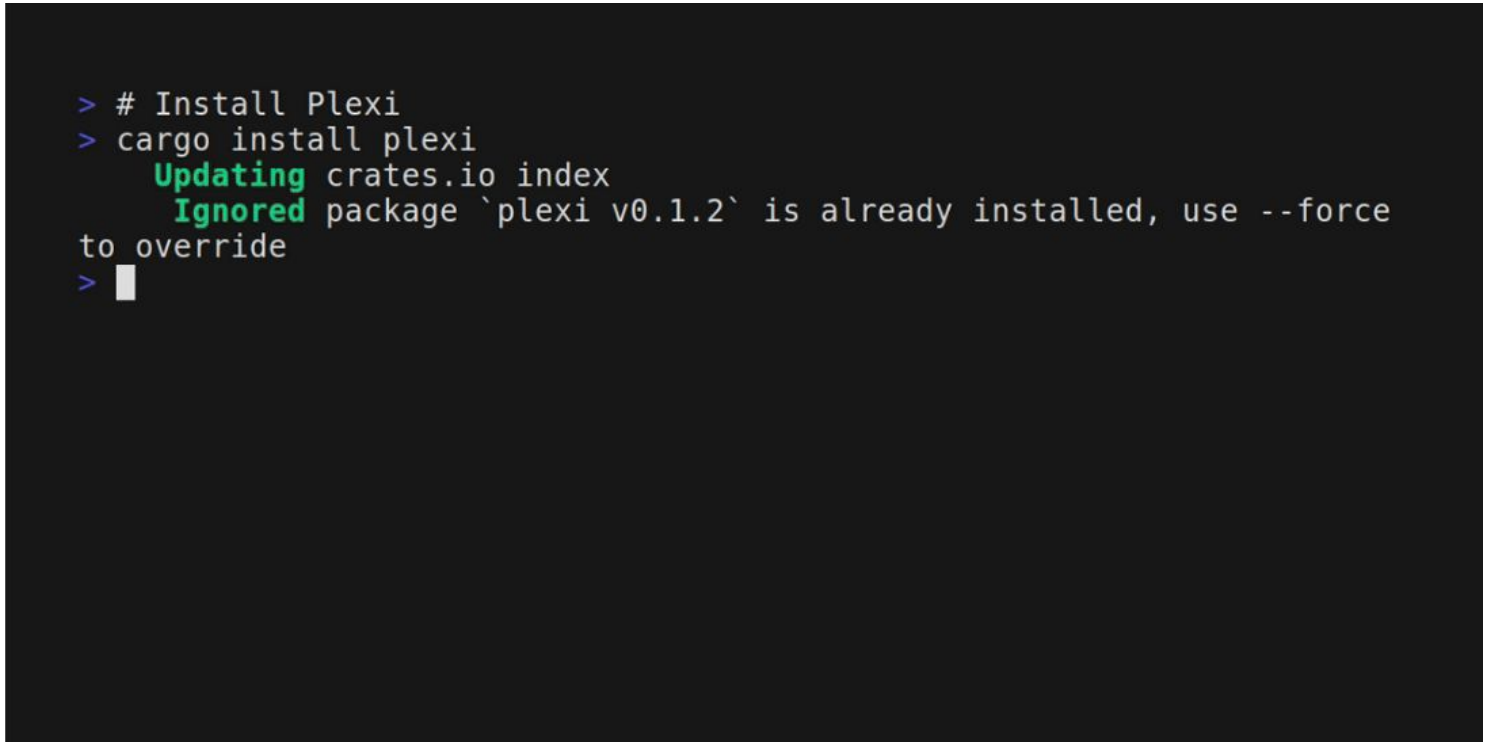
A command line interface



Recorded with
charmbracelet/vhs

Code on
cloudflare/plexi

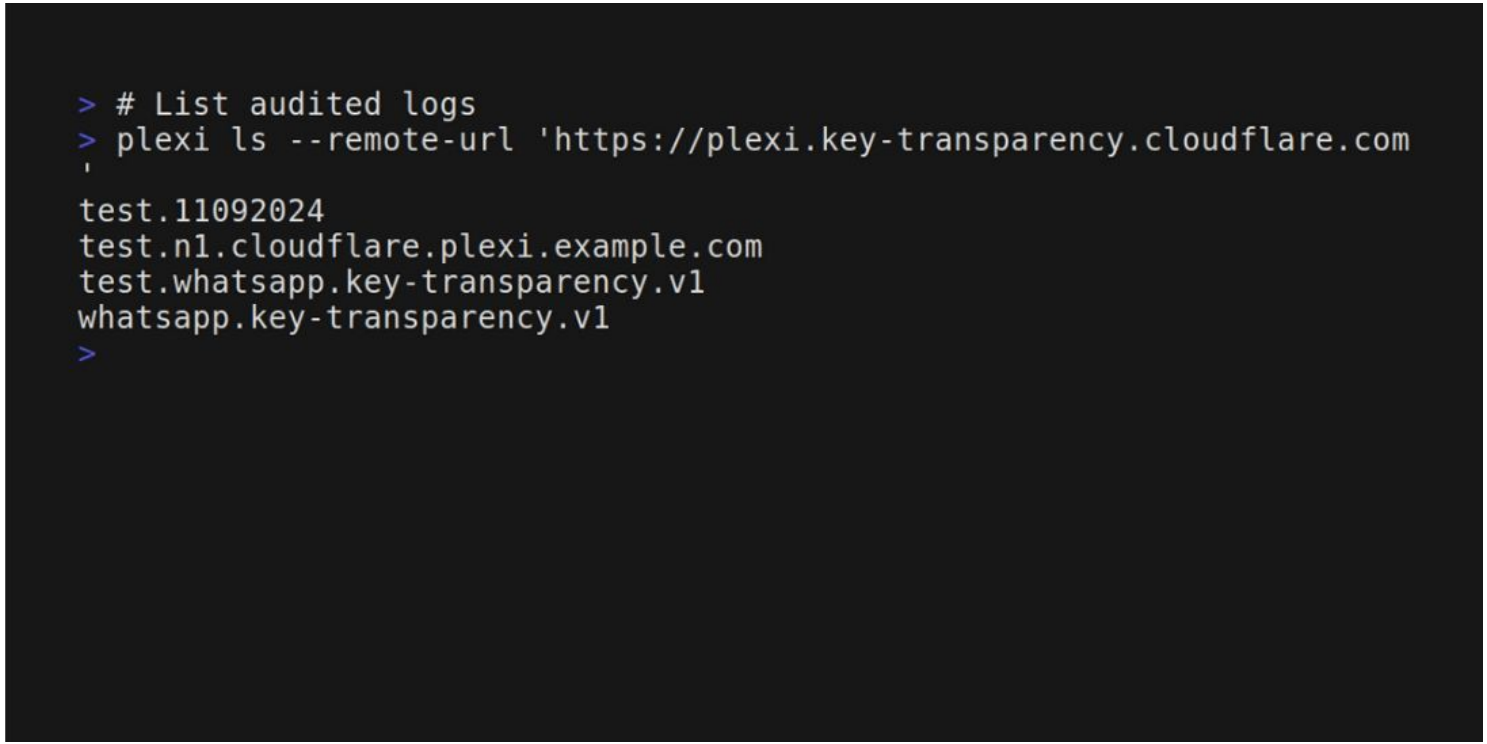
A command line interface



Recorded with
charmbracelet/vhs

Code on
cloudflare/plexi

A command line interface



Recorded with
charmbracelet/vhs

Code on
cloudflare/plexi

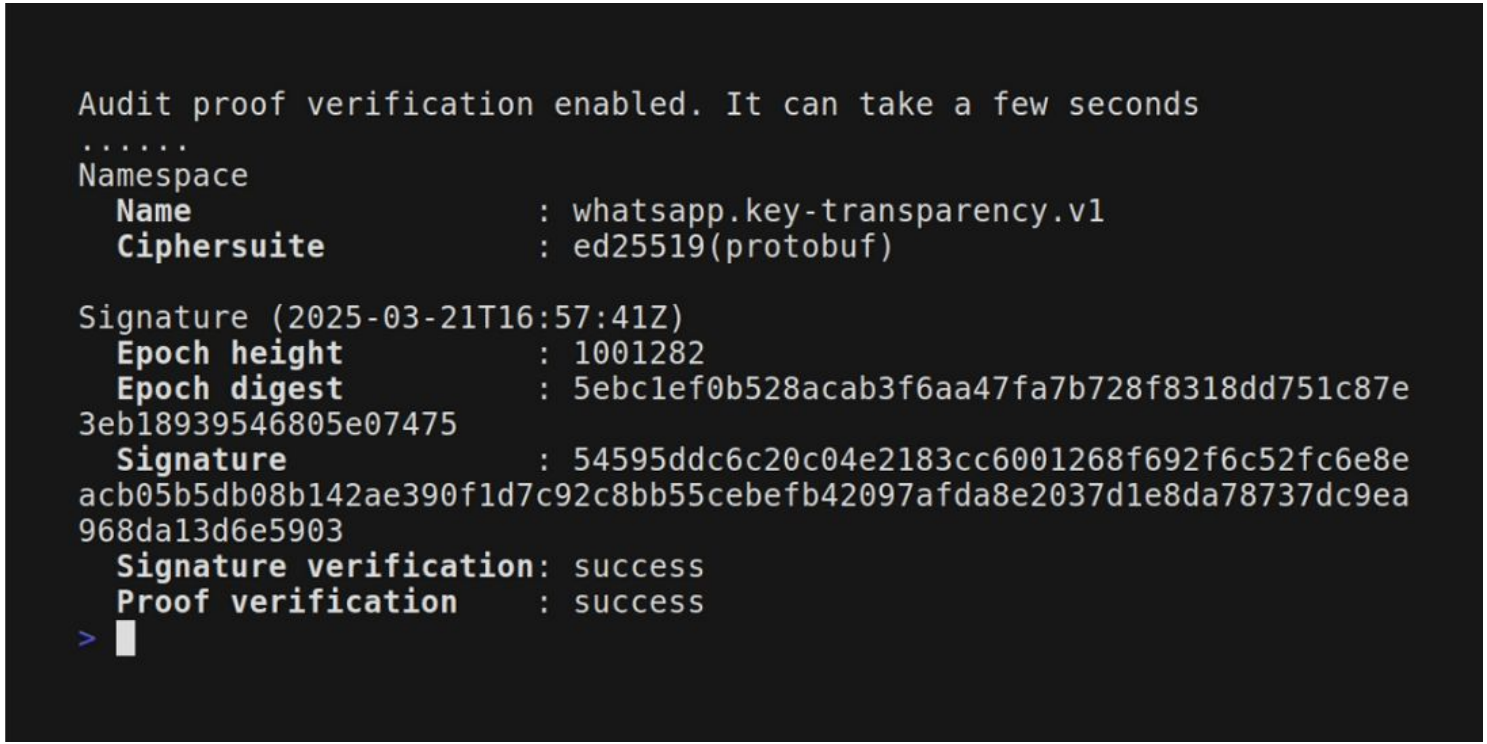
A command line interface

```
> # Audit the latest epoch
> plexi audit \
      --remote-url 'https://akd-auditor.cloudflare.com' \
      --namespace 'whatsapp.key-transparency.v1' \
       --long
Audit proof verification enabled. It can take a few seconds
.....
```

Recorded with
charmbracelet/vhs

Code on
cloudflare/plexi

A command line interface



Recorded with
charmbracelet/vhs

Code on
cloudflare/plexi

Section

Real world deployment

… in reality

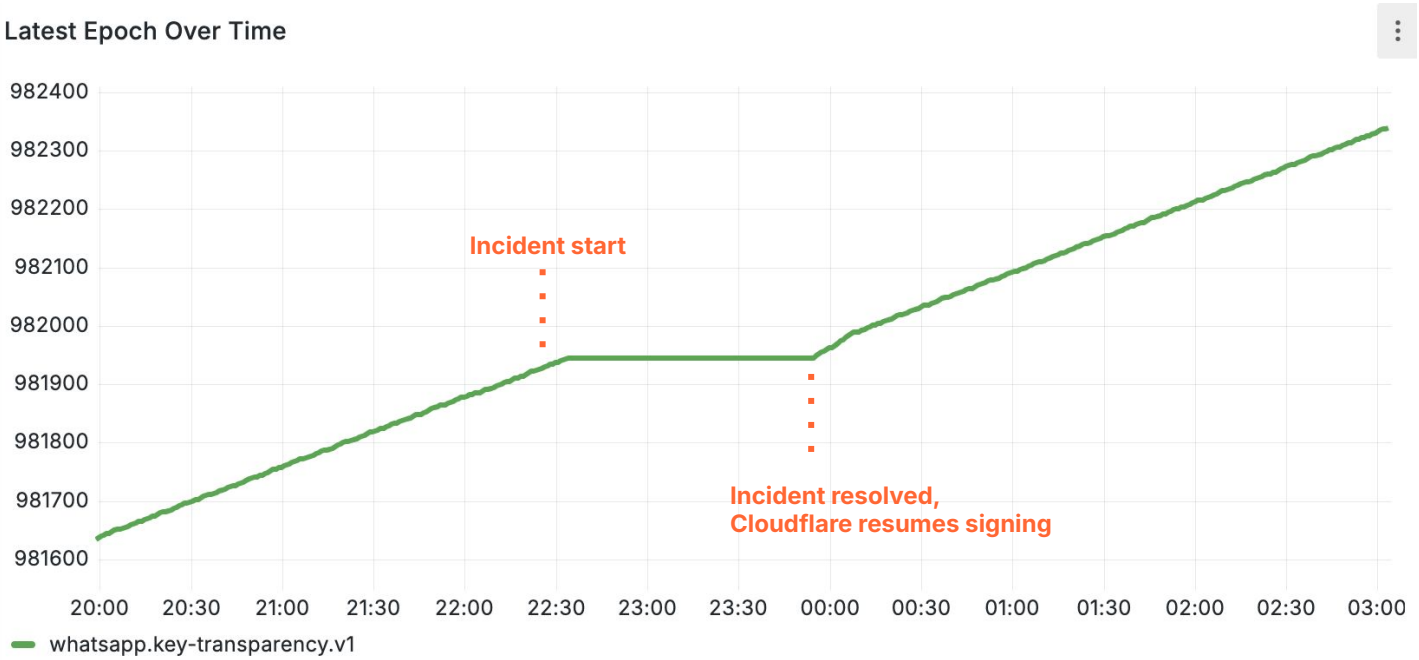
Incidents

Privacy Eng Pages App Fri 11:41 PM

Incident 1466211 triggered by Privacy Eng: 1 alert for Plexi Worker Production Epoch Not Increasing

38 replies Mon 11:04 AM

During an incident, epochs fail to progress



When epochs get bigger, verification latency increases

More incidents

Publishes every 30s

Theory

The Log publishes new heads.

Practice

When that failed, the backlog of updates grew, increasing the proof size 6x, going beyond our initial provisioning threshold.

Global ordering

Theory

Global ordering scales easily.

Practice

In practice, the auditor signs a timestamp. This means that it’s hard to replay signatures.

Integrity

Theory

No party gets corrupted.

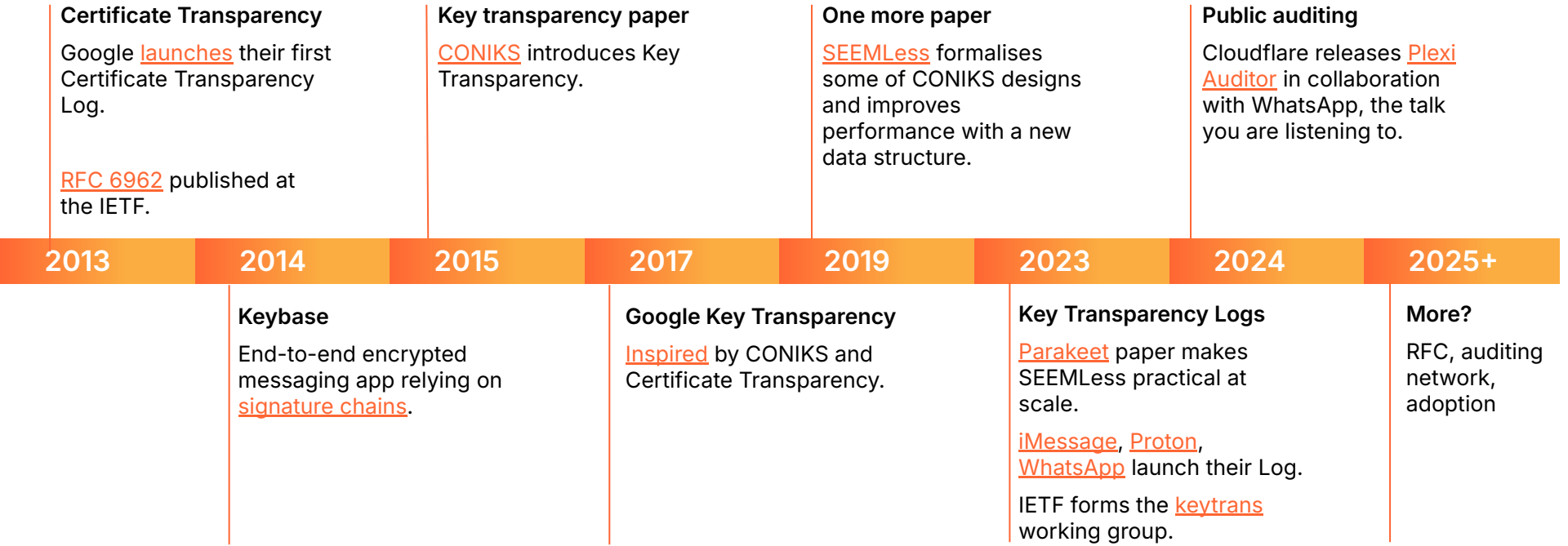
Practice

This is true! So far, both the Log and the Auditor managed to remain in a non-corrupted state, despite hiccups.

Section

What’s next

Transparency – a timeline



Why there aren’t more auditors... yet!

Technical expertise

Key Transparency is new

There needs to be more expertise and understanding about the guarantees it provides with and without auditing.

Implementations

There are a lot

CONIKS, CT-based, AKD, tlog-based.

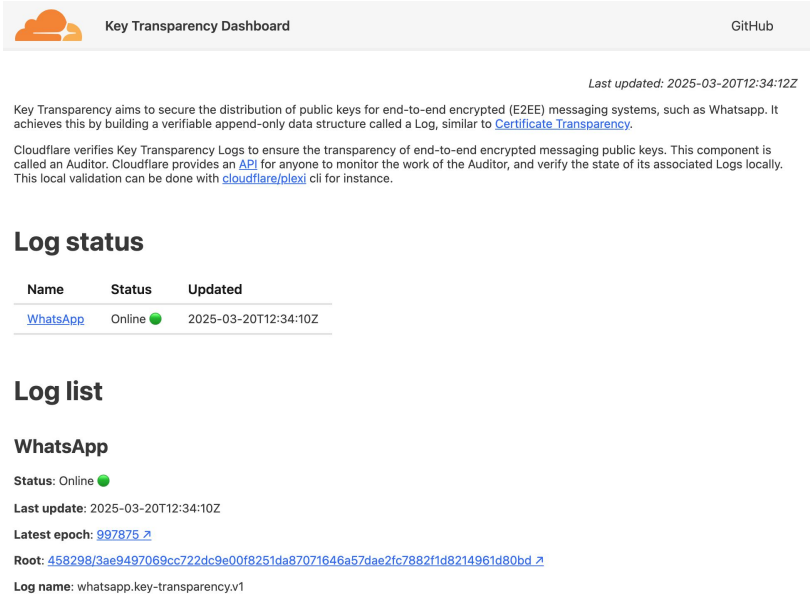
IETF keytrans is developing a standard.

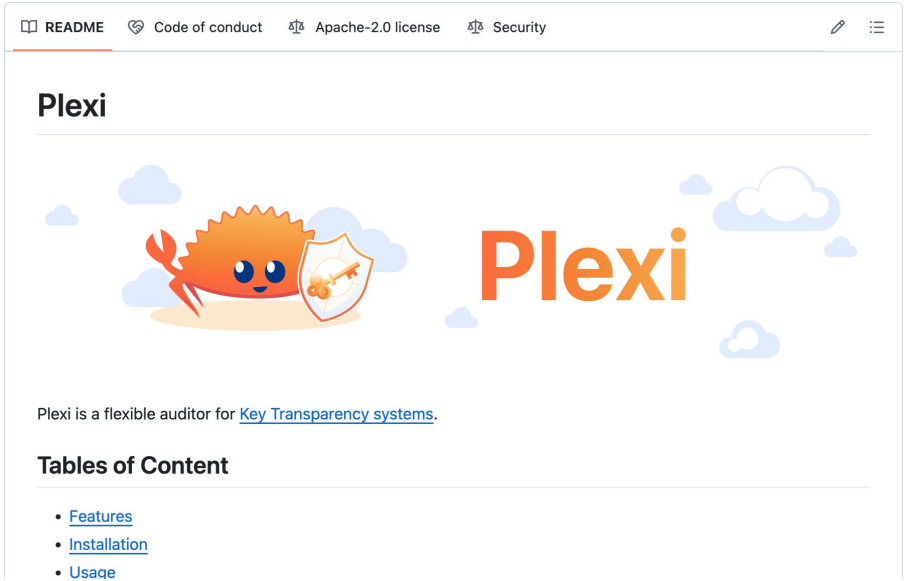
Performance at scale

Real world is big

Scale makes the system more expensive to audit, or less performant than on a off-the-shelf device.

Where can I see / use it?

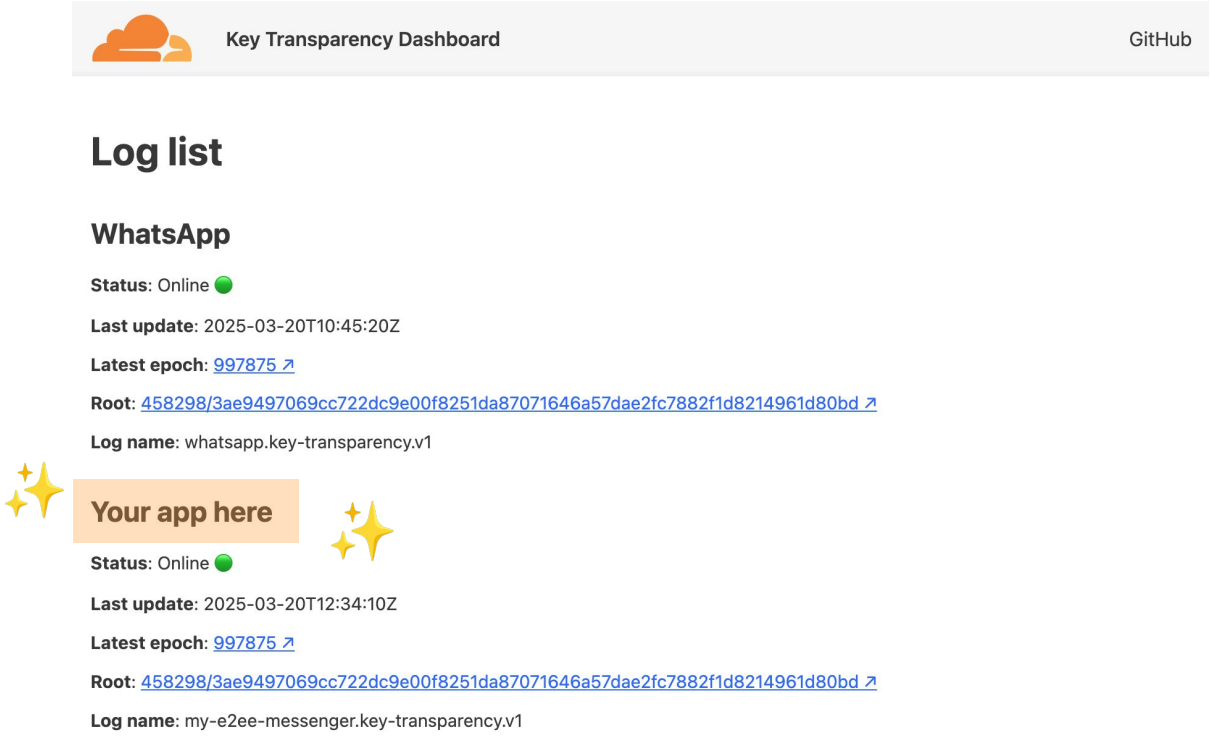




🔑dash.key-transparency.cloudflare.com

🦀 github.com/cloudflare/plexi

Towards a transparency ecosystem



Thank you

blog.cloudflare.com

engineering.fb.com