

How Let's Encrypt is Deploying MTCs

Matthew McPherrin



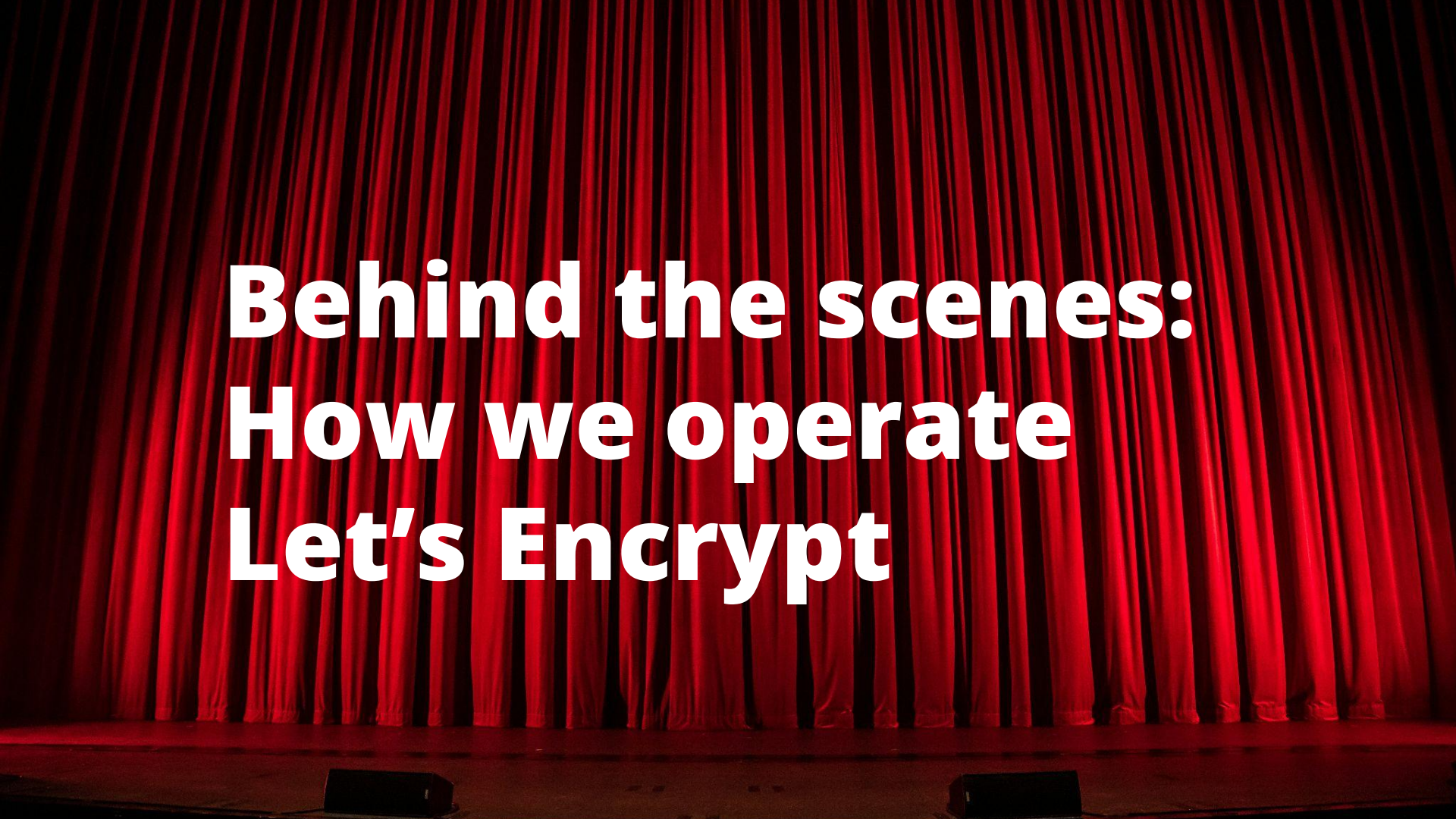


Let's  **Merkle ...?**

MTCA: Under Development

Staging: Soon!

Prod: Next Year

A background of red stage curtains with vertical folds, illuminated from below, creating a warm, theatrical atmosphere. The curtains are a deep red color, and the lighting highlights the texture and folds.

**Behind the scenes:
How we operate
Let's Encrypt**

Physical Infrastructure

- 2 Datacenter Locations
- Two dozen servers
- Network, HSMs, etc
- Some AWS: CT Logs, etc
- Some Cloudflare: CDN



two of them



Our Forest of Trees



MTCA Log 1a:

6 Day Certs



MTCA Log 1b:

45 Day Certs

DC1



MTCA Log 2a:

6 Day Certs



MTCA Log 2b:

45 Day Certs

DC2

When a Datacenter is down:

- Those logs stop growing where they are
- Issuance continues in the other DC risk-free
- We can continue to serve publicly from cloud mirrors, etc, as required





Storing and Serving: It's all tiles!

Tile Storage

- **In our datacenters:**
 - **Object storage (eg, SeaweedFS)**
- **In our mirrors and backups:**
 - **AWS S3**
- **Served publicly via CDN**

Bonus Extra Tile Layer

- Merkle Tree CA logs don't store pubkeys - just hashes
- We need those internally still
- **Solution: An extra layer of tiles**

Measuring the tree

How much storage will we need for the CA log, and for the pubkey tiles?

How much storage will our and other MTCA mirrors need?



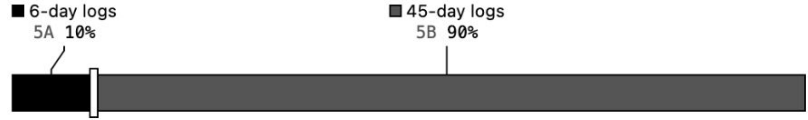
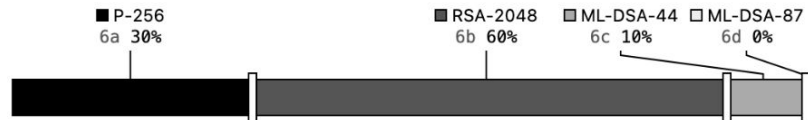
compressed (bytes)	$2 \times (\text{mix} \times (\text{key} + 3))$	307.0	
compressed (bytes)	$2 + 2 + 2 + L9$	306.0	
compressed (bytes)	$L16 \times L10 \div 100$	76.5	
	256×2	8,122.0	
		6-day logs (A)	45-day logs (B)
	$L4 \times 10^6 \times L5 \div 100$	68,200,000	613,800,000
	$L19 \div L3$	17,050,000	20,460,000
tes	$L20 \times L2$	102,300,000	920,700,000
per log	$L20 \div L1$	8,525,000	10,230,000
nd, per log	$L22 \div 86400$	98.67	118.40
(days)	$L2 + L11a$	41	80
er log	$L22 \times L24$	349,525,000	818,400,000
per log		6-day logs (A)	45-day logs (B)
	$\lfloor L25 \div 256 \rfloor$	1,365,332	3,196,875
	$L26$	1,365,332	3,196,875
(full)	$\lfloor L25 \div 256 \rfloor$	1,365,332	3,196,875

SPREADSHEETS

~~SPREADSHEETS~~

<https://mcpherrinm.github.io/mtsizecalc/>

<https://mcpherrinm.github.io/mtsizecalc/>

PART I — INPUTS		6-DAY LOGS (A)		45-DAY LOGS (B)		
1	Number of logs		2		2	
2	Certificate lifetime (days)		6		45	
3	Renewal at day		4		30	
4	Active certificates (millions)					682
5	Split of active certificates between lifetimes (%)					
6	Key mix (%)					
7	Avg TBSCertificateLogEntry size (bytes)		300			
8	Entry tile compression ratio (% of uncompressed)		25			
9a	Retention after expiry, CA (days)		35			
9b	Retention after expiry, mirror (days)		35			
10	Checkpoint interval (seconds)		2			
11	Let's Encrypt share of total issuance (%)					50

Scenario 1: Current Let's Encrypt volume

Assuming about current volume:

- 700 million active certificates, mostly 45 day, some 6 day
- Mix of RSA and ECDSA, small fraction ML-DSA-44
- All other CAs roughly equal Let's Encrypt volume on MTCA mirrors
- Prune logs 35 days after expiry

Scenario 1: Current Let's Encrypt volume

SUMMARY	OBJECTS	STORED (COMPRESSED)
Let's Encrypt CA: standard log	15,027,478	194.21 GiB
Let's Encrypt CA: pubkey tiles	7,499,026	378.96 GiB
Let's Encrypt CA: total	22,526,504	573.18 GiB
Every MTCA Mirror	30,054,905	388.42 GiB

Scenario 2: A Scarier Further Future

Growth, everyone adopts ML-DSA-44 and short lived certs

- 1 billion active 6-day certs
- All ML-DSA-44
- Prune logs 35 days after expiry

Scenario 2: A Scarier Further Future

SUMMARY	OBJECTS	STORED (COMPRESSED)
Let's Encrypt CA: standard log	80,235,152	1,036.95 GiB
Let's Encrypt CA: pubkey tiles	40,039,064	12,553.06 GiB
Let's Encrypt CA: total	120,274,216	13,590.01 GiB
Every MTCA Mirror	160,470,280	2,073.89 GiB

Scenario 2b: CAs retain for 2 years after expiry

SUMMARY	OBJECTS	STORED (COMPRESSED)
Let's Encrypt CA: standard log	1,440,318,638	18,614.43 GiB
Let's Encrypt CA: pubkey tiles	718,750,002	225,342.81 GiB
Let's Encrypt CA: total	2,159,068,640	243,957.24 GiB
Every MTCA Mirror	160,470,280	2,073.89 GiB

(IE: Current CABF requirements)

245 TiB?

Two boxes of tapes.



245 TiB? One SSD.



micron

6600 ION

E3.L SSD | 245.76TB

So how do I get one?



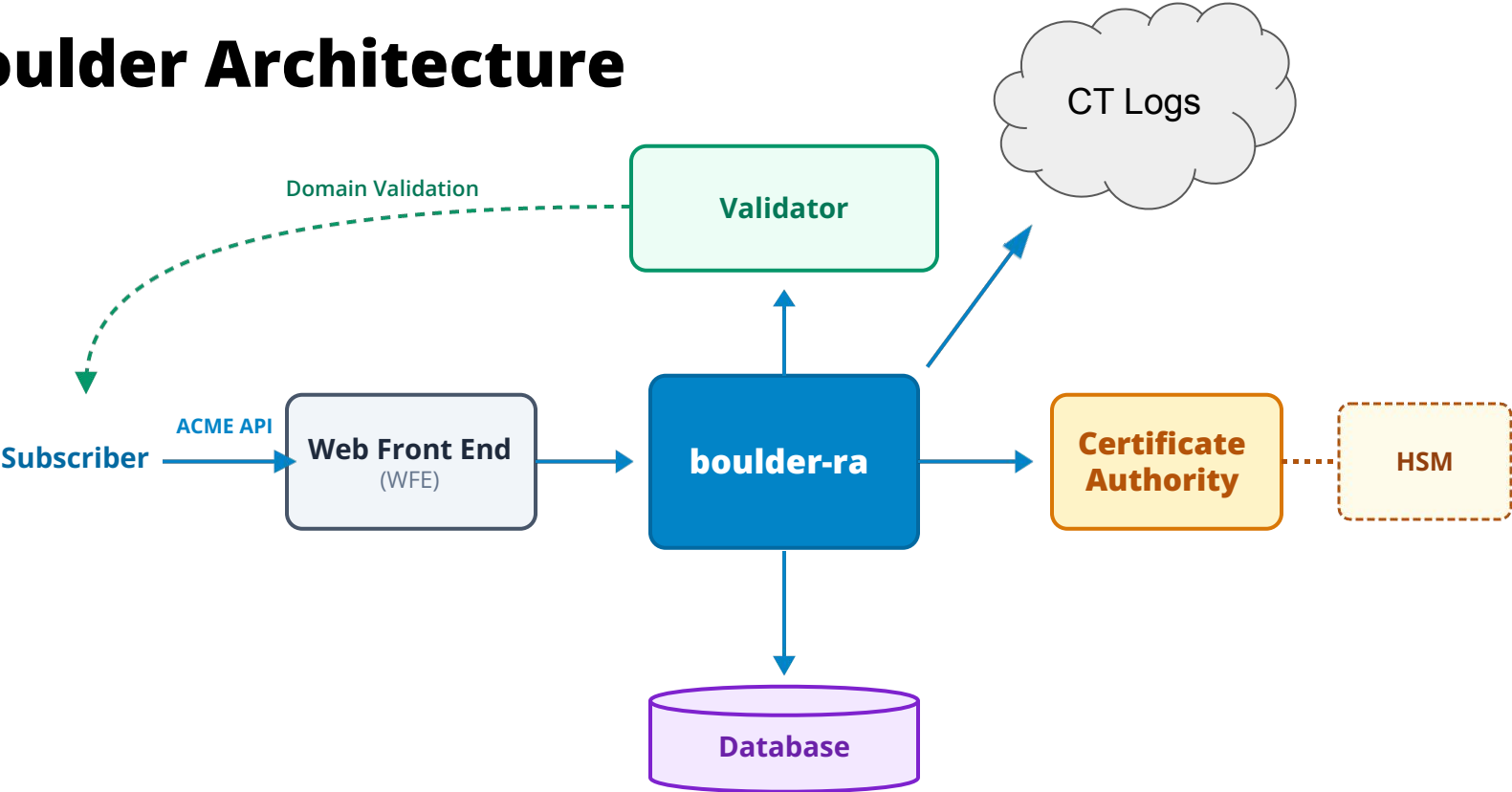
ACME

Boulder:
The Let's Encrypt
CA Software
- Now with MTCA!

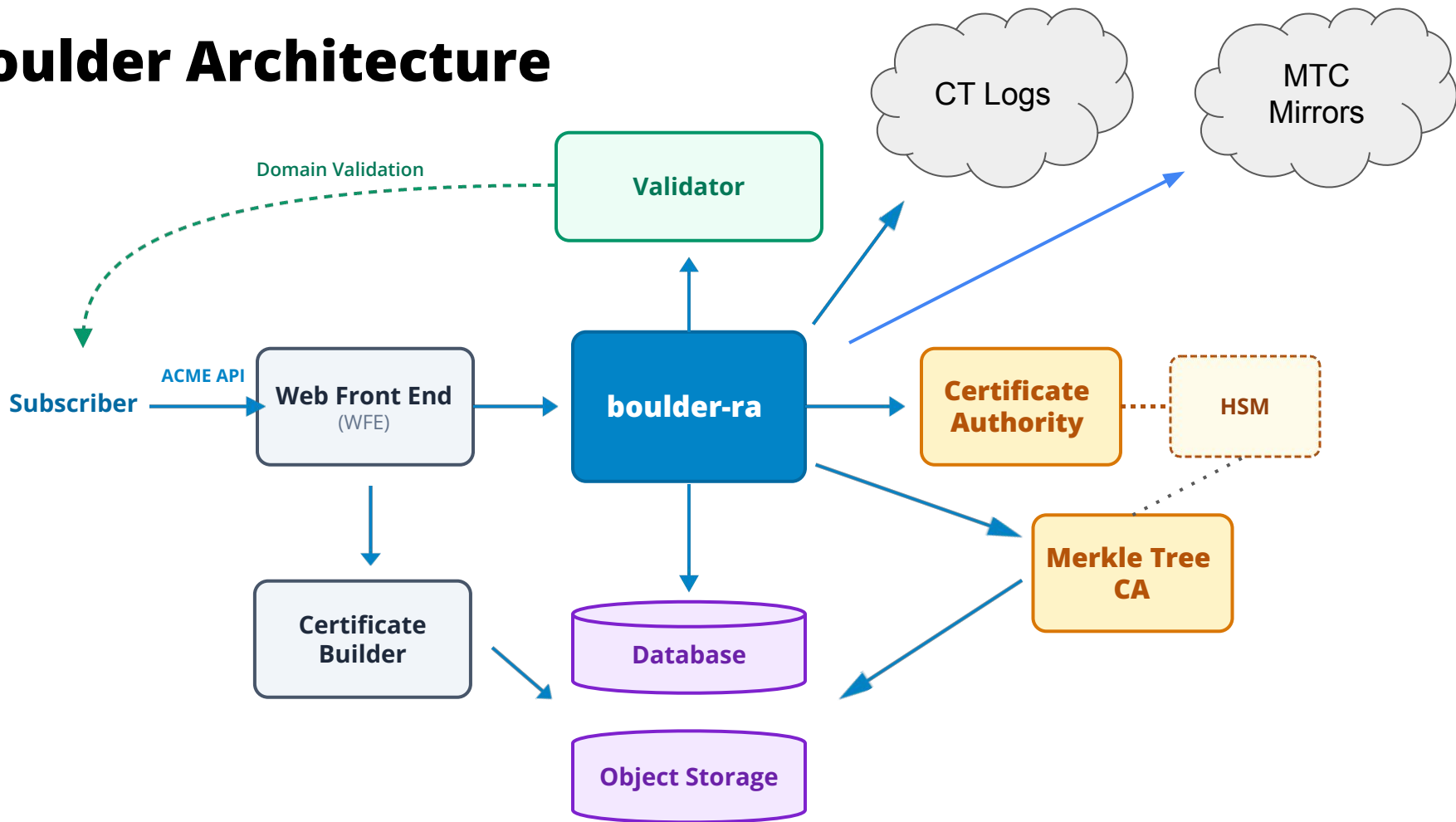
Boulder: The Let's Encrypt CA Software - ~~Now~~ with MTCA!

COMING SOON

Boulder Architecture



Boulder Architecture



Boulder MTCA Architecture

- ACME, Domain Validation, etc: Pretty much the same
 - Switch out some microservices:
 - Instead of a stateless x509 CAs: singleton MTCA per log, writing tiles
 - Instead of CT publisher: Merkle Tree publisher for mirrors
 - Add a new one for turning tiles into certificates
 - Need some new database tables
 - *So much for going all in on tiles*
 - Track Checkpoints, Landmarks
-
- Some invariants we need to break: Serials aren't globally unique

Singleton MTCA Per Log

Inspired by Sunlight:

- One instance runs per MTCA log
 - Pools requests
 - Writes data to storage
 - Talks to HSMs for signing
-
- We'll see how far we can get with this



Issuing MTCs to ACME Clients

- Opt-in with ACME Profiles (6 or 45 day certs)
 - *Assuming we can do 45 day certs...*
- Staging: Shadow testing initially, logging MTCs for all certs
 - Important to prove designs work at scale
- Soon! Under active development

How Let's Encrypt is Deploying MTCs

<https://mcpherrinm.github.io/mtsizecalc/>

<https://letsencrypt.org/>

<https://github.com/letsencrypt/boulder/>



Q&A?