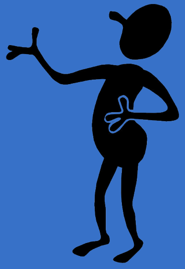
HRR400MCWBI

Aaron Gable
Let’s Encrypt

Pass the SALT
July 5, 2024

How to Revoke and Replace 400 Million Certificates Without Breaking the Internet

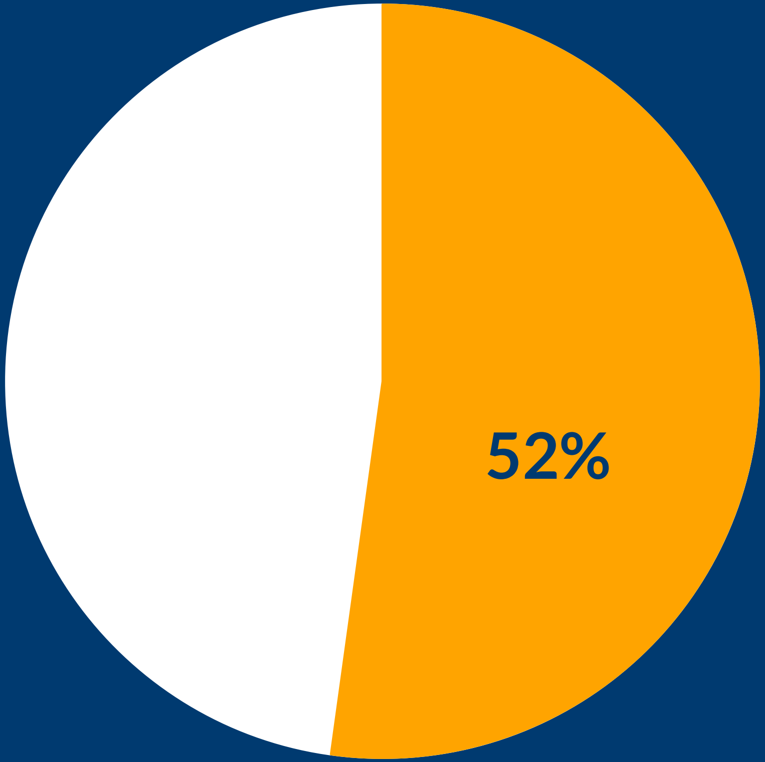


Aaron Gable
Let's Encrypt

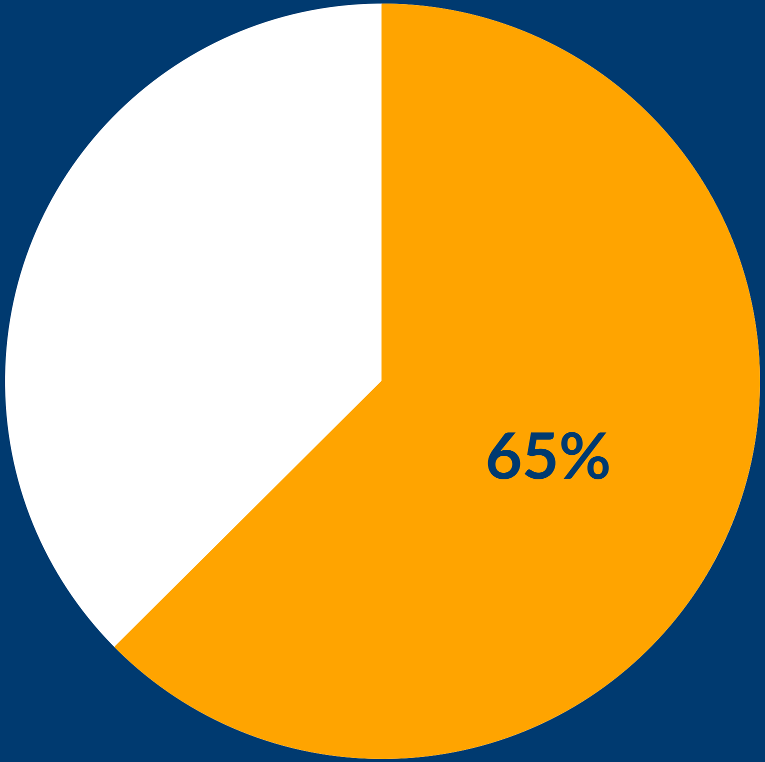
Pass the SALT
July 5, 2024

Let’s
Encrypt

The Web

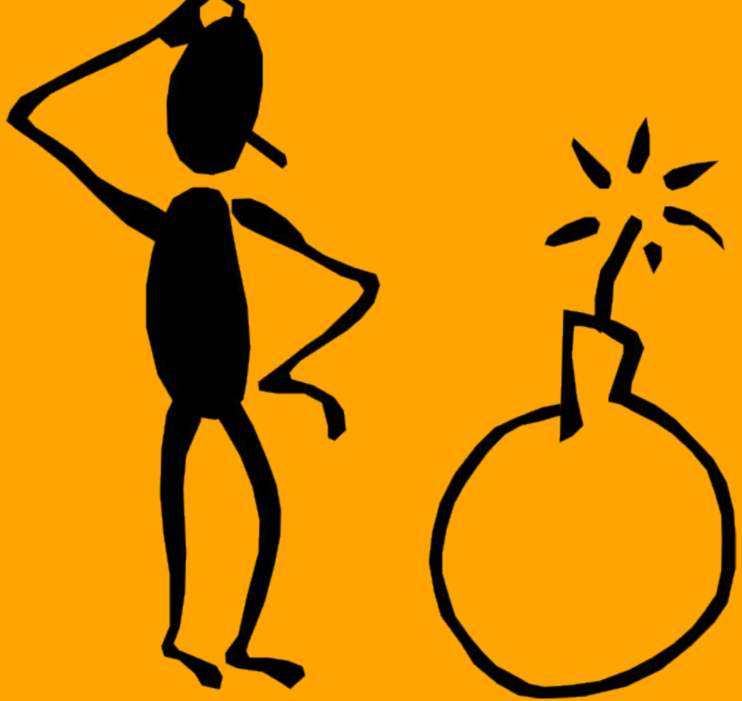


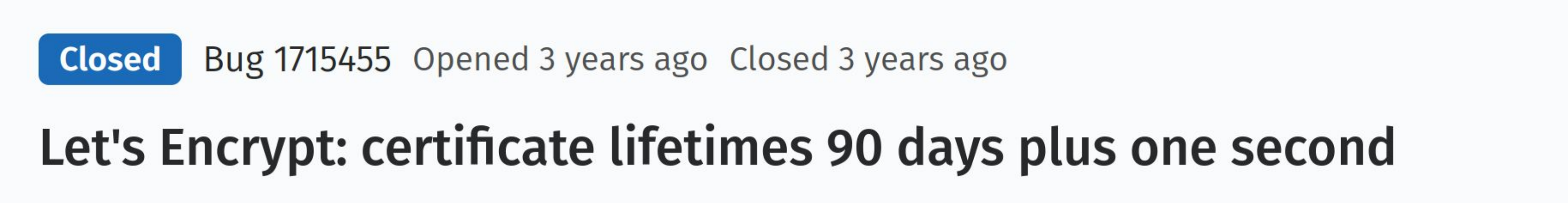
The WebPKI



375M Certificates

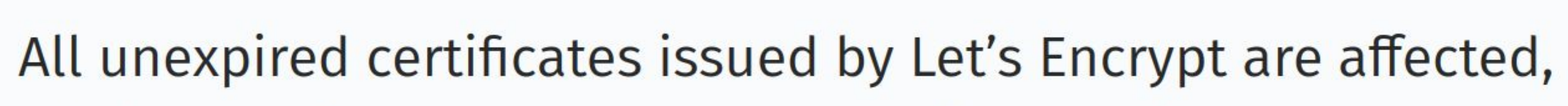
430M Domains





Closed Bug 1715455 Opened 3 years ago Closed 3 years ago

Let's Encrypt: certificate lifetimes 90 days plus one second



All unexpired certificates issued by Let’s Encrypt are affected,

What happens if you revoke everything?

What **breaks** if you revoke everything?

🖋 OCSP to revoke

🖋 Replacement certificate

+ 🖋 OCSP for new cert

---

3 🖋/ 📜

× 400M 📜

1.2 Billion 🖋

÷ 750 🖋/ second

18.5 Days

🖋 OCSP to revoke

🖋 Replacement certificate

+ 🖋 OCSP for new cert

---

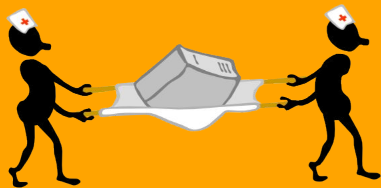
3 🖋/ 📃

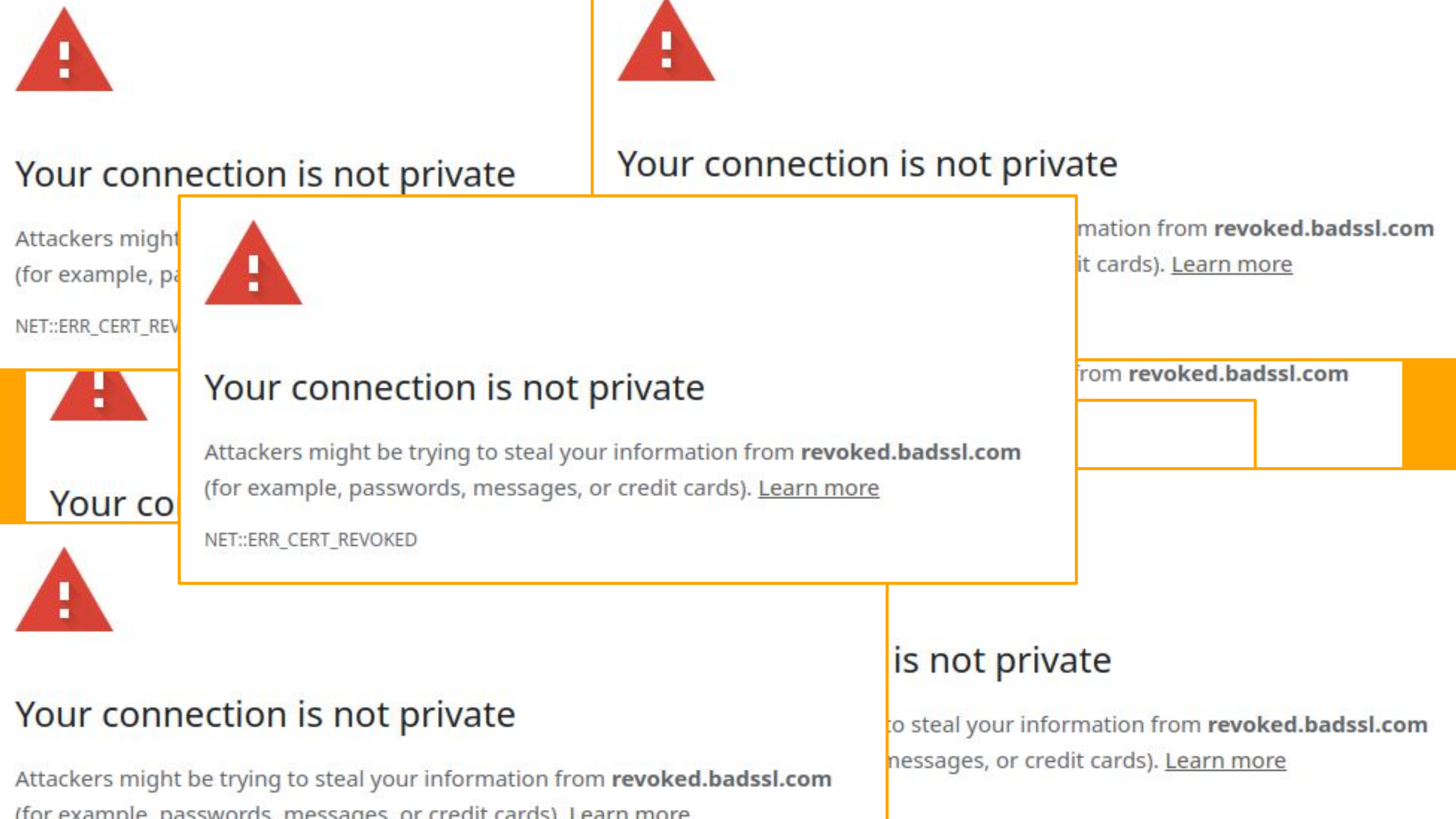
× 400M 📃

1.2 Billion 🖋

÷ 10,000 🖋/ second

1.4 Days





Your connection is not private

Attackers might be trying to steal your information from **revoked.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_REVOKED

Your connection is not private

Attackers might

(for example, pa

NET::ERR_CERT_REV

Your connection is not private

mation from **revoked.badssl.com**

it cards). Learn more

rom **revoked.badssl.com**

Your co

Your connection is not private

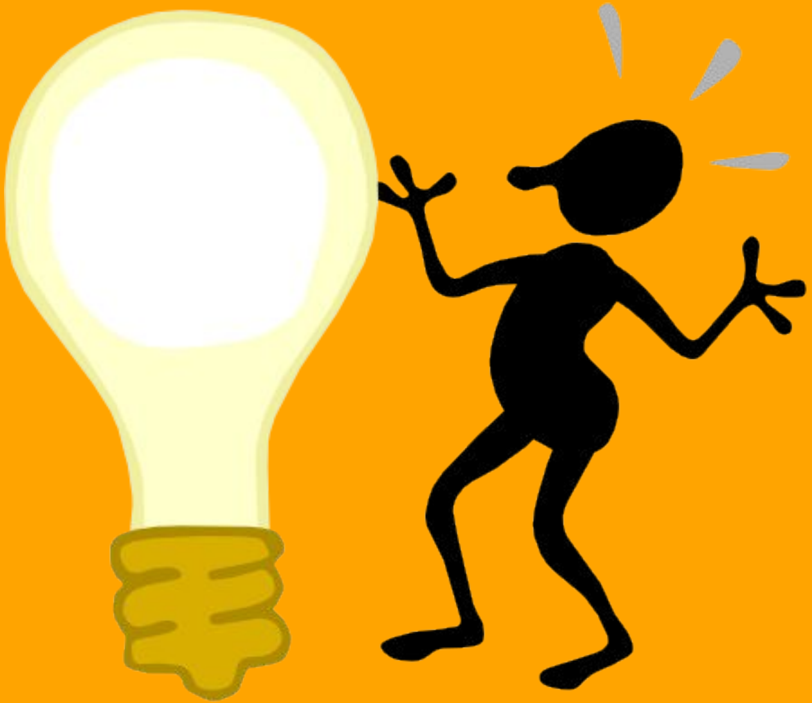
Attackers might be trying to steal your information from **revoked.badssl.com**

(for example, passwords, messages, or credit cards). Learn more

is not private

to steal your information from **revoked.badssl.com**

nessages, or credit cards). Learn more



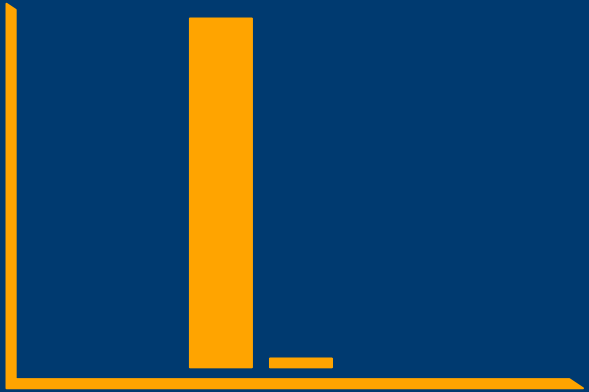
1. On-Demand OCSP ✅
2. ACME Renewal Info 🕘
3. Short-Lived Certificates 👀

1. On-Demand OCSP

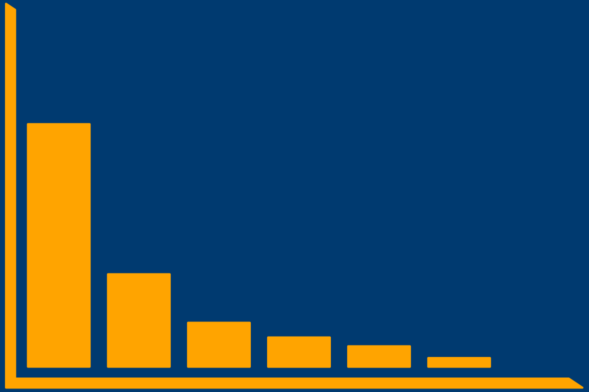
- OCSP to revoke
- Replacement certificate
- OCSP for new cert

Replacement certificate

OCSP Signatures per Certificate



Pre-Signing



Live-Signing

🖋️ Replacement certificate

+

1 🖋️/ 📃

× 400M 📃

400M 🖋️

÷ 10,000 🖋️/ second

0.45 Days

2. ACME Renewal Info

Q: When should I renew?

A:

```
GET /acme/renewal-info/aYhba4...IdlQyE
{
  "suggestedWindow": {
    "start": "2024-07-03 00:00:00",
    "end":   "2024-07-05 00:00:00"
  }
}
```

Q: Can this cert be revoked?

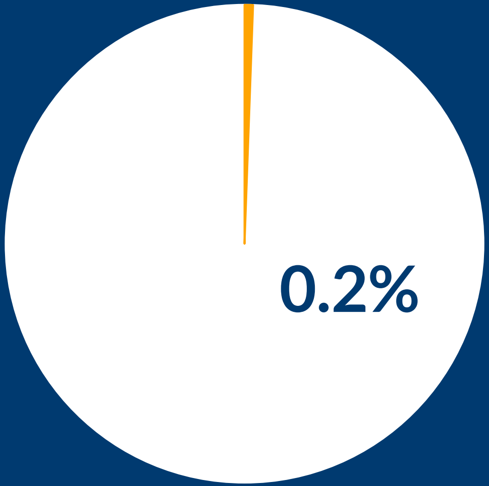
A:

```
POST /acme/new-order
{
  "identifiers": [
    "example.com", "www.example.com"
  ],
  "replaces": "aYhba4...IdlQyE"
}
```

draft-ietf-acme-ari-04

3+ ACME servers

10+ ACME clients



3. Short-Lived Certificates

Baseline Requirements, Section 4.9.1 “Circumstances for revocation”

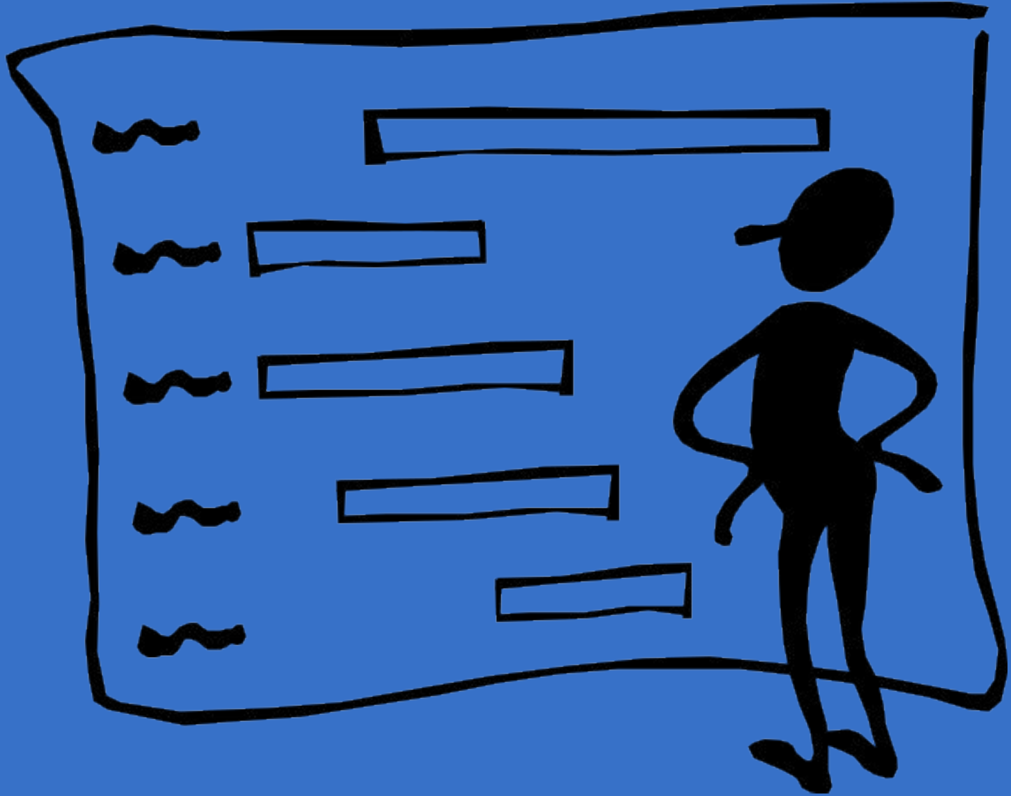
> ***With the exception of Short-lived Subscriber Certificates…***

Baseline Requirements, Section 1.6 “Short-Lived Subscriber Certificate”

> *…a Validity Period less than or equal to 10 days.*

```
notBefore:
    2024-07-03 01:02:03

notAfter:
    2024-07-10 01:02:03
```



Thank You!

Aaron Gable
aaron@letsencrypt.org