

Amazon Trust Services - CABF 59

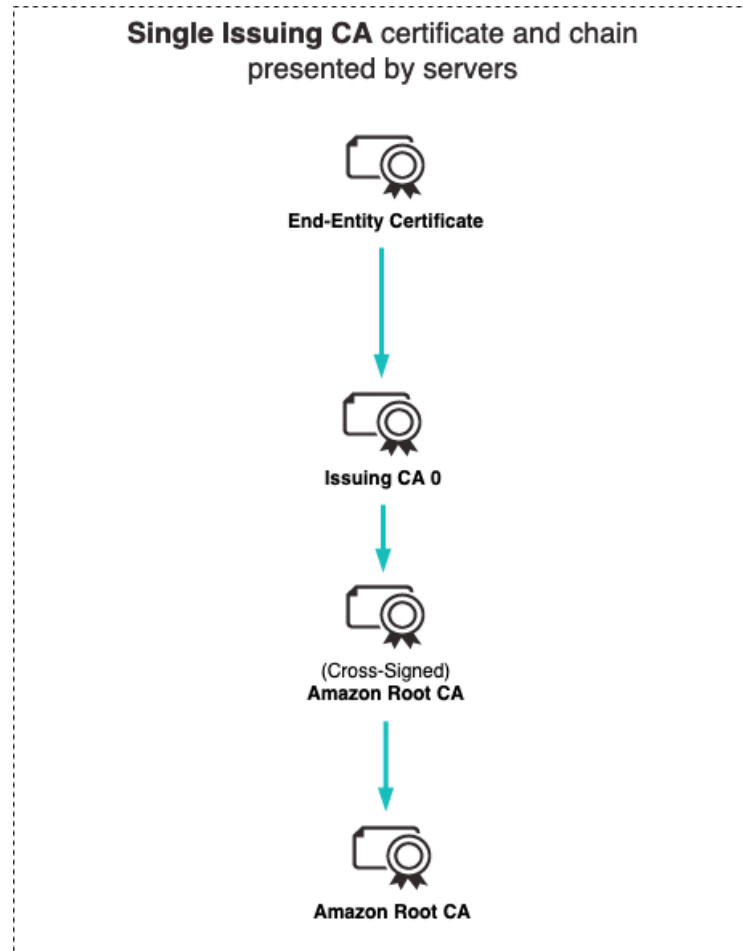
- **Amazon Trust Services (ATS)** is the public CA operated by Amazon.
- **AWS Certificate Manager (ACM)** is an AWS service that obtains publicly trusted certificates from ATS

Motivation

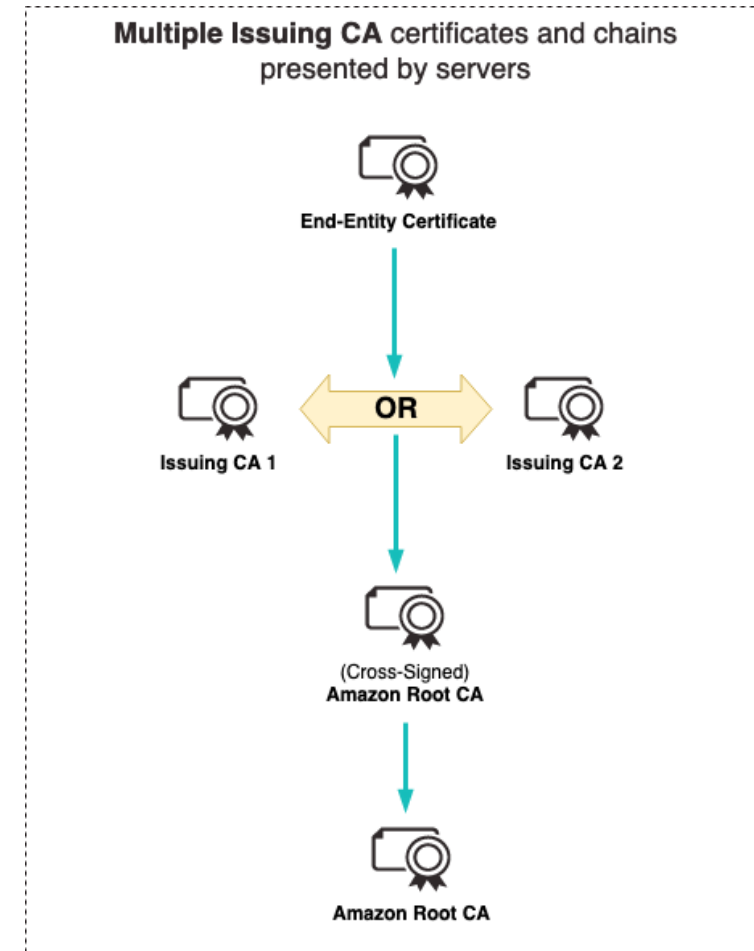
- Customers are looking for technical efficiency
- Existing documentation wasn't moving the needle
- Amazon wanted to create a more **resilient** and **agile** certificate infrastructure

What We Did: Random Issuing CAs

2015 - 2022



2022 - Present



How We Did It

- Automated closed-loop system
- Minimize impact through communication and outreach
 - Proactive blog posts, emails and direct contacts
 - Event notifications
- Customer were still impacted, so we worked with them
 - Hundreds of conversations, video calls and meetings

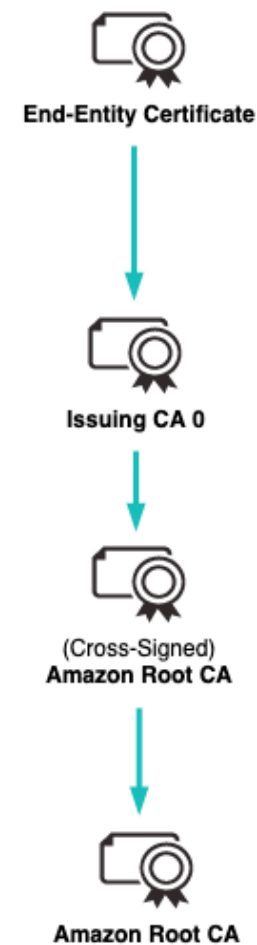
What We Learned

1. Customers are pinning
2. Communication gaps exist
3. Current “Best Practices” are conflicting

Observation 1: Customers are Pinning

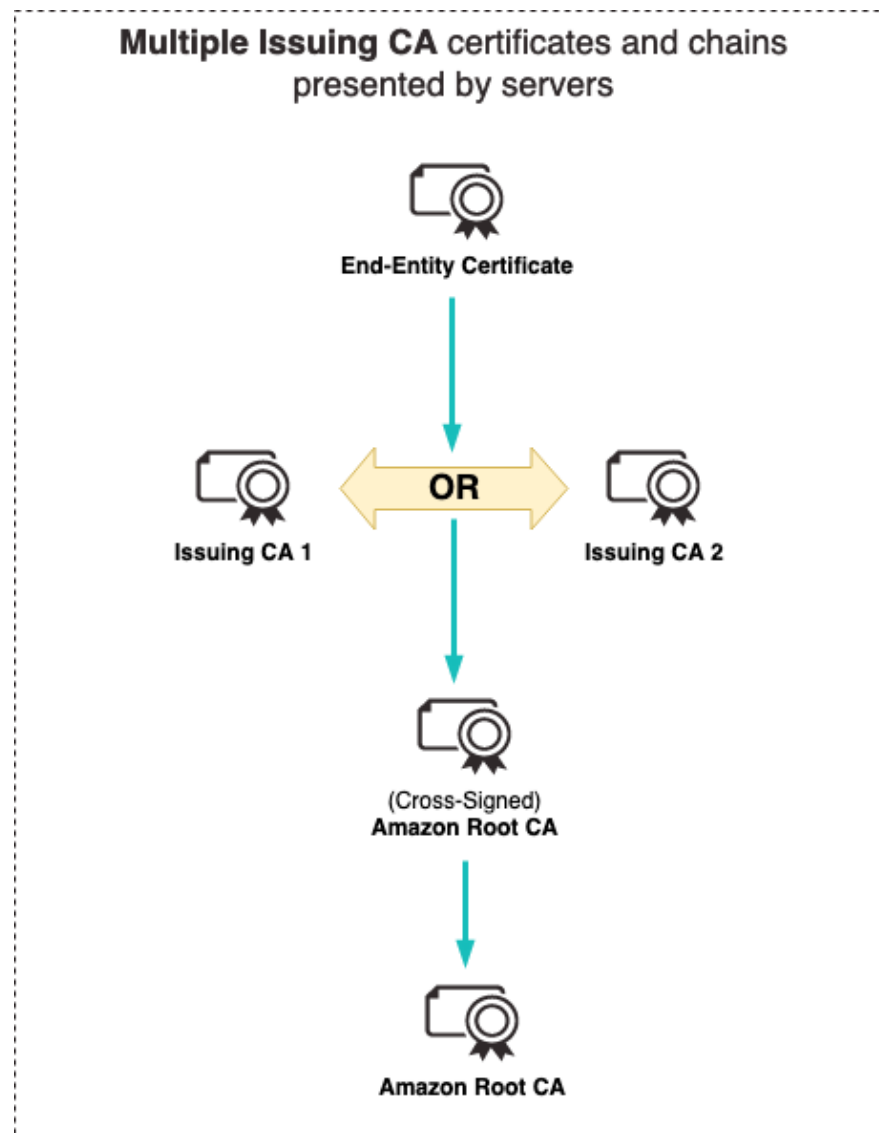
- Customers are pinning to....
 - End-entity certificates they control
 - End-entity certificates they **do not** control
 - ex... s3.amazonaws.com
 - Issuing certificate authorities
 - Specific root certificates (not keys)
 - self-signed / cross-signed
- Customers are hard-coding URIs
- Custom trust stores

Single Issuing CA certificate and chain presented by servers



Observation 2: Communication Gaps Exist

- Automated closed-loop system
- Customers of customers
- Wide variety of use cases
- Misunderstandings



Observation 3: Current “Best Practices” are conflicting

- **OWASP** guidelines
- Apple and Google Android documentation
- Industry alignment is key

OWASP / [www-community](#) Public
generated from [OWASP/www-projectchapter-example](#)

<> Code Issues 9 Pull requests Actions Security Insights

Add pinning cautions #744

Merged kingthorin merged 1 commit into [OWASP:master](#) from [heymarcel:master](#) on Mar 13

Conversation 1 Commits 1 Checks 0 Files changed 1

Changes from all commits File filter Conversations Jump to

```
47 pages/controls/Certificate_and_Public_Key_Pinning.md
... @@ -190,6 +190,18 @@ validating its certificate or public key. While pinning does
190 190 occur in an `OnConnect` callback, it's often most convenient because the
191 191 underlying connection information is readily available.
192 192
193 + ### When Do You Not Pin?
194 +
195 + Pinning requires control of upcoming certificate attributes. If the
196 + certificate key pair cannot be predicted in advance before it is put
197 + into service, then pinning will lead to an outage when the endpoint
198 + presents a new certificate. For instance, if a certificate provider
199 + generates random key pairs whenever a certificate is rotated, and you
200 + cannot control when this certificate is put into use, then you will
201 + not be able to update your clients until they have already experienced
202 + an outage. You should not pin using attributes of a certificate
203 + presented by an endpoint outside of your control.
204 +
```


Lessons Learned

- Fully understanding the impact of PKI changes is difficult and takes time so we must be thoughtful about timelines
- There is a lack of mechanisms to effectively communicate with everyone potentially impacted by a change
- We must work together on cohesive industry guidance to further PKI agility and clarify recommendations.