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

**Single Issuing CA** certificate and chain presented by servers

- End-Entity Certificate
- Issuing CA 0
- (Cross-Signed) Amazon Root CA
- Amazon Root CA

2022 - Present

**Multiple Issuing CA** certificates and chains presented by servers

- End-Entity Certificate
- Issuing CA 1
- (Cross-Signed) Amazon Root CA
- Amazon Root CA
- OR
- Issuing CA 2
- (Cross-Signed) Amazon Root CA
- Amazon Root CA
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
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
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.