



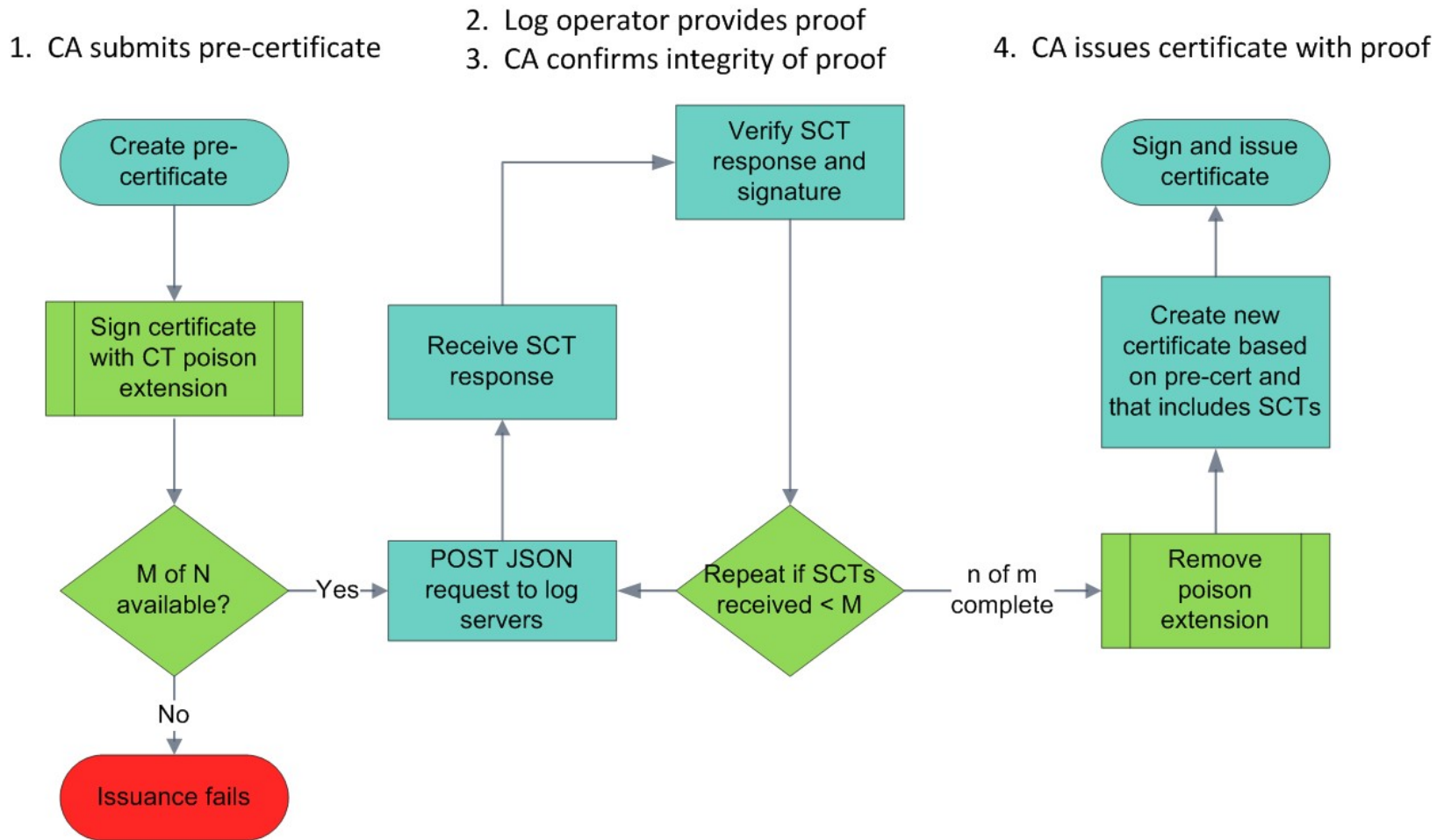
New Window of Opportunity:

Certificate Transparency -
A Certification Authority's Perspective
Ben Wilson, SVP DigiCert

Introduction

- Goals of Certificate Transparency:
 - Provide insight into issued SSL certificates
 - Provide better remediation services
 - Ensure CAs are aware of what they issue
- DigiCert supports the concept of transparent certificate practices and certificate logging:
 - Voiced our support of transparency early on
 - Already accessing Google's log server
- Some outstanding areas require discussion prior to advocating industry-wide implementation

Issuance Flow



Transparency

- Benefits
 - Fast detection = better mitigation
 - Greater visibility = better accountability for domain owners
 - Visible trust in operations = increased trust for CAs
 - Greater opportunity for discussion on certificates = improvement in Internet security
- Security
 - Enables detection of problem and mis-issued certificates
 - Necessary for adequate remediation

Public Logging

- Public logging was discussed previously in CA /B Forum
 - Action by a browser was needed to make it happen
- Public log shines a light on CAs
- Public log provides mitigation
 - All of the incidents could have been more quickly detected and remediated with CT
- Public log helps researchers
- Public log is detection in security
 - Baseline requirements is prevention
 - Revocation is remediation

Security Improvement

- Raises awareness of practices
 - Allows broader observation of a CA's practices
 - Allows domain owners to identify illegitimate use of domain names (Early Warning System)
- Exposes weak points/players in ecosystem
 - Enables research to identify improvement areas
- Enables trust decisions for domain owners
 - Self-regulating mechanism for the market

Other Benefits

- Backward compatible
- Driving towards implementation
- Expands the existing system
 - SSL has a proven track record
 - Lots of institutional knowledge
 - Increasingly stringent standards
- Avoids “unintended consequences” of new technology
- Deployed by CAs and Browsers
 - Web site operator participation is not required

Implementation

- Obtained REST JSON API from Google (URL reference)
- Identified log servers
 - No new infrastructure
- Updated our issuance code to communicate with log server
- Created code to verify signed proof on response before embedding into certificate
- Modified our certificate profile

Remaining Questions from CAs

- Number of Proofs
 - Each proof increases certificate size
 - Increased certificate size hampers performance
- Privacy, competitive business considerations
- Level playing field requirement for all CAs
- Exemptions for internal certificates
- Log accessibility and resiliency of deployment

Log Server Considerations

Model implementation provided by Google

- Uses SQL light for log tree storage
- Which CAs can add to a log?
- What will be considered a trusted log?

Security policy for trusted log operation is needed

- Identify desired uptime and performance objectives
- Scope broad enough to include entire system (e.g. mitigating disruption due to log compromises)
- Perform risk assessment and adopt controls
- Policy adoption process needs to be quick / efficient

Conclusion

DigiCert supports Certificate Transparency because it

- Addresses vulnerabilities in the current trust model
- Creates transparency and accountability that will lead to prevention and early detection of mis-issuances
- Is based on existing technologies that are easily supported with industry coordination
- Enhances existing self-regulating mechanisms by leveraging an existing, refined and time-tested CA trust-anchor system while avoiding the “unintended consequences” of new technology in unfamiliar space