Security in knowledge

Alternatives and Enhancements to CAs for a Secure Web

Ben Wilson

Digicert, Inc. - CA/Browser Forum

Eran Messeri

Google

RSA CONFERENCE EUROPE 2013

Session ID: ARCH-R01

Session Classification: Intermediate

Current Web PKI System

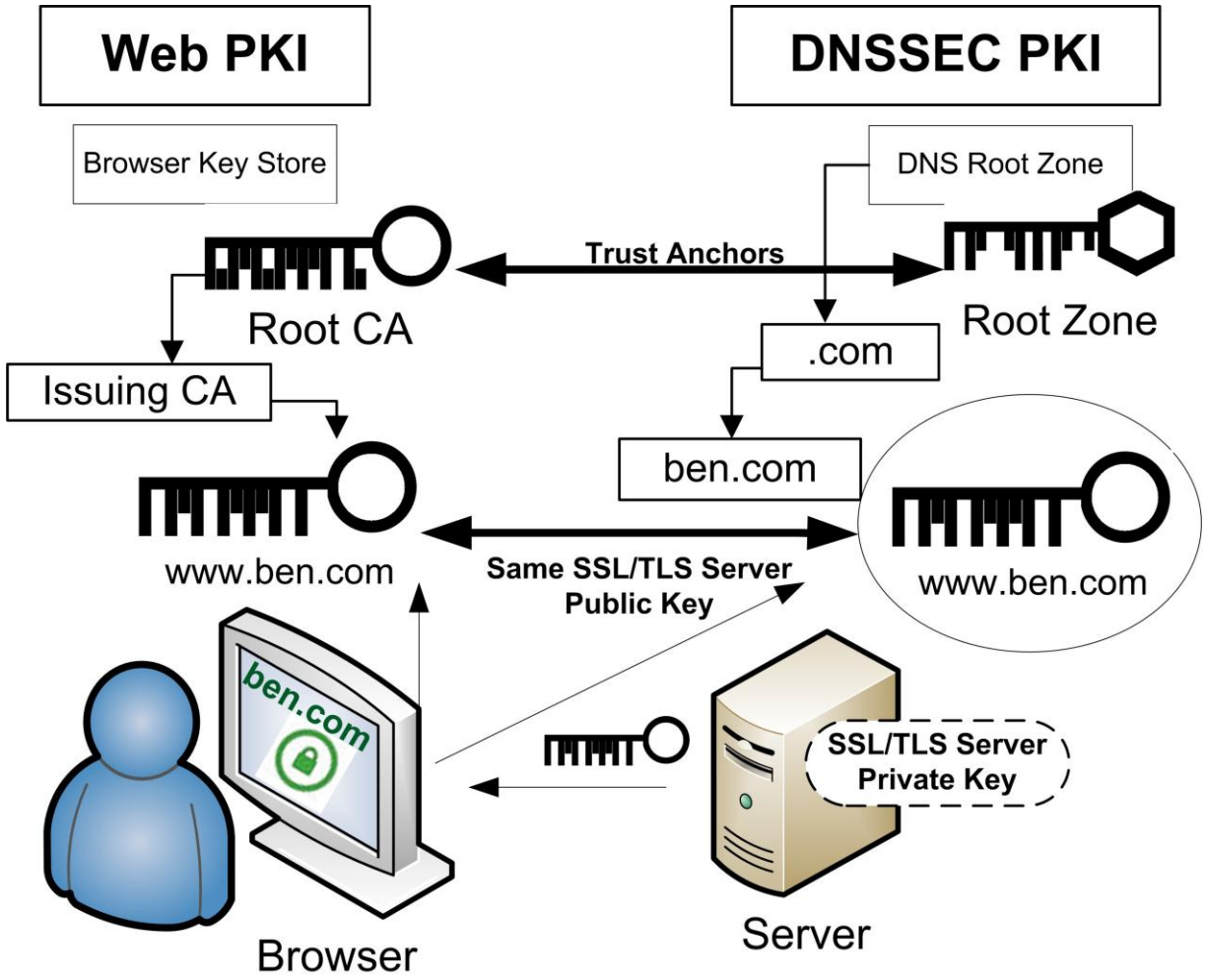
- OS / Browsers have Managed PKI Deployment for Almost 20 Years
- CAs expected to implement high-security practices
  - Trust model re-examined after CA operational security lapses in 2011
  - CA/Browser Forum continues to improve industry practices
- There are diverse opinions about “what’s best”
  - But industry self-regulating mechanisms are in place.

NIST Workshop in April 2013

“Improving Trust in the Online Marketplace”

- Reviewed current state and future of web PKI
  - DNS-based Authentication of Named Entities (DANE)
  - Certificate Transparency (CT)
  - Other solutions such as pinning, CAA, and OCSP Stapling
- NIST Workshop Conclusions:
  - No single solution is “best” because each is a different approach and addresses a different problem.
  - Eventually a combination may provide better security, usability, reliability, simplicity, and privacy/liberty.
  - Everyone keep working on these solutions, and we’ll continue the discussion on how to improve security of SSL/TLS.

Technology Overview



Technology Overview, Slide 2

Web PKI Hierarchy	DNSSEC PKI Hierarchy and DANE
• Multiple Trust Anchors • 65 Root CAs in Mozilla • Browsers require CA security audits and CAs screen against misleading names and provide additional identity checks • Revocation with OCSP • Fewer dependencies and PKI for the web making incremental progress with Pinning, Certificate Transparency, OCSP Stapling	• Single Root Zone CA • 300+TLDs & 1,000+ registrars • Variance in practice for security and vetting, potential “one stop shop” for an attacker, but scope of damage is limited • Revocation by DNS Update • Multiple dependencies – waiting until deployment of updates to BIND in stub resolvers, firewalls, routers, load balancers

Web PKI vs. DANE/DNSSEC

Field	Value
Issuer	DigiCert High Assurance EV CA…
Valid from	Tuesday, September 10, 2013…
Valid to	Tuesday, September 15, 2015…
Subject	www.digicert.com, DigiCert, I…
Public key	RSA (2048 Bits)
Authority Key Identifier	KeyID=4c 58 cb 25 f0 41 4f 5…
Subject Key Identifier	eb af 25 55 54 d1 56 b1 3f 87 …
Subject Alternative Name	DNS Name=www.digicert.com…
Enhanced Key Usage	Server Authentication (1.3.6.…
CRL Distribution Points	[1]CRL Distribution Point: Distr…
Certificate Policies	[1]Certificate Policy:Policy Ide…
Authority Information Access	[1]Authority Info Access: Acc…
Key Usage	Digital Signature, Key Encipher…
Basic Constraints	Subject Type=End Entity, Pat…

Certification Authority Authorization (CAA)
$ORIGIN ben.com.
. CAA 0 issue "digicert.com";

DANE
Authorized Public CA
_443._tcp.www.ben.com. IN TLSA 0 0 1
(7431e5f4c3c1ce4690774f0b61e05440883ba9a
01ed00ba6abd7806ed3b118cf)
Publicly Trusted SSL Certificate
_443._tcp.www.ben.com. IN TLSA 1 0 1
(1fcfef7b328e78a9d79a04531abe0fa7c66f34b1f
39bf41dd63ecb0be881a411)

Certificate Viewer

DNSSEC Record

What is Certificate Transparency (CT)?

CT requires public logging of TLS/SSL certificates

- Goals of Certificate Transparency:
  - Provide insight into issued SSL certificates
  - Provide better remediation services
  - Ensure CAs are aware of what they issue

How does CT work? Merkle hash tree has two proofs :

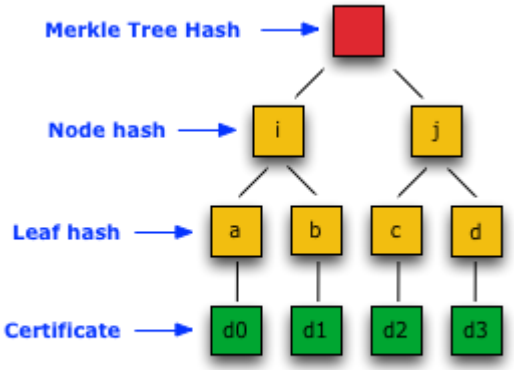
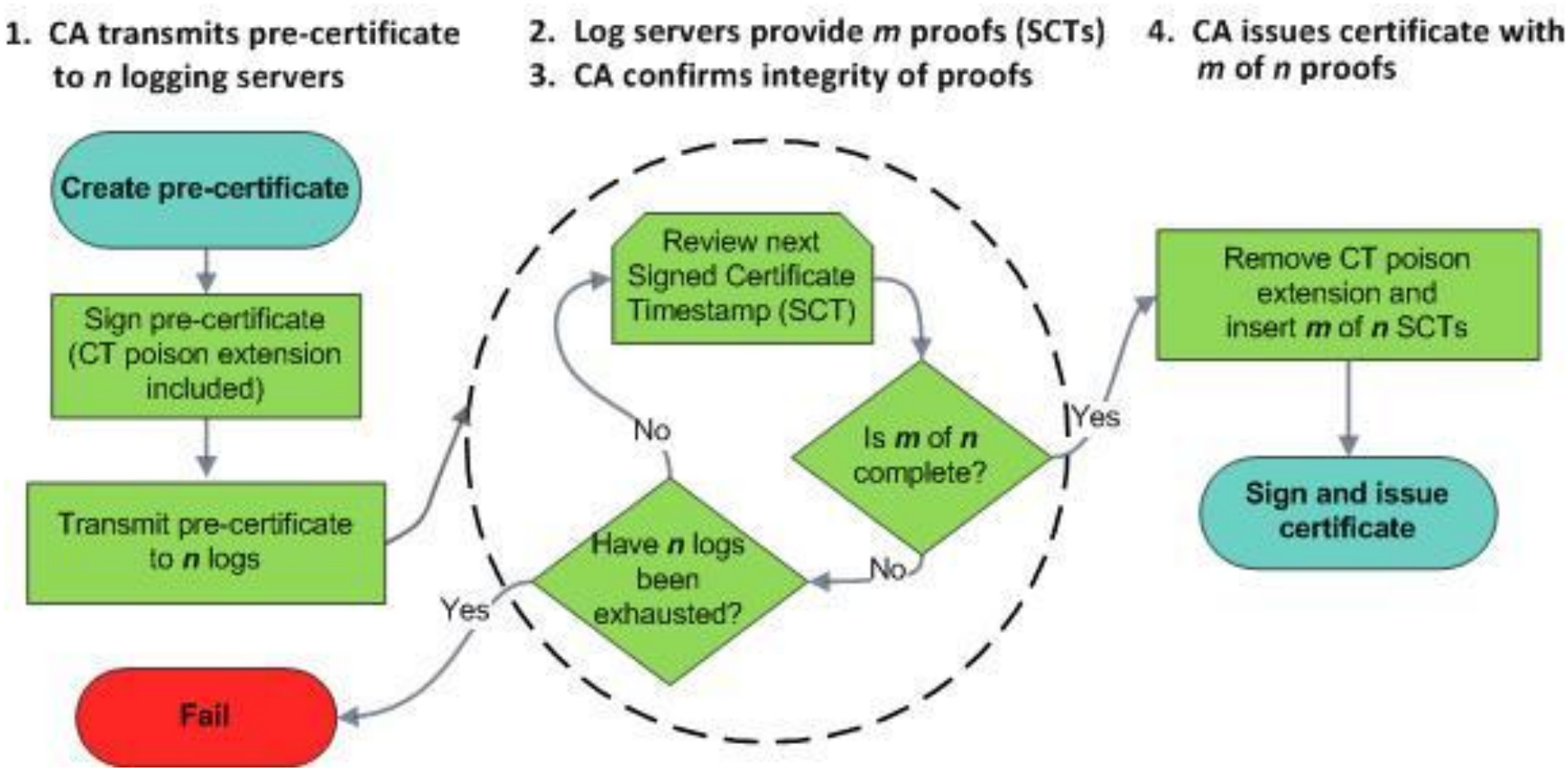


Figure 1

- **Consistency proof** verifies that a later log contains all certificates in previous log in same sequence.
- **Audit proof** any chosen certificate has been included in the log.

Process Flow



Key Points – Compatibility and Transparency

- **Compatible with current PKI implementations**
  - Supported by Google and Several CAs
  - Uses current specifications for SSL/TLS, path validation, and revocation checking
  - Expands the existing system with logging and log-checking
- **Public log shines broad light on CAs and Certificates**
  - Public log is “detection” in security
  - Early detection leads to better/faster mitigation
  - Info for researchers, domain owners, CAs, and browsers leading to greater public trust

Summary – Certificate Transparency:

- Addresses vulnerabilities in current trust model
- Creates transparency and accountability
- Uses easily supported existing technologies
  - Avoids “unintended consequences” of unfamiliar technology
- Enhances existing self-regulating industry mechanisms like CA/Browser Forum and Web PKI
- Is moving toward broader implementation

Take-Aways

- A secure, top-down chain of trust is integral to any web security solution.
- DANE requires end-to-end DNSSEC that doesn't exist.
- The Web PKI of CAs and Browsers has provided secure SSL/TLS communication for nearly twenty years.
- All stakeholders in the online ecosystem continue to improve the security of SSL/TLS with enhancements.
- CT logging systems will publicly monitor CAs.
- CT is the best new technology for the Web PKI.

Security in knowledge

Thank you!

Ben Wilson
DigiCert and CA/Browser Forum
@DigicertBen
ben@digicert.com
www.digicert.com

Eran Messeri
Google
eranm@google.com

http://www.certificate-transparency.org/