CA Self-Governance:
CA / Browser Forum Guidelines and Other Industry Developments

Ben Wilson, Chair,
CA / Browser Forum

Chronology of Frameworks

1995 - 1996 – PKIX chartered, BS 7799 published, EU Recommendation - Information Technology Security Evaluation Criteria (ITSEC), X.509v.3, ABA's Digital Signature Guidelines

1997-1999 – ETSI Guide on Requirements for Trusted Third Parties, Certificate Policy and Certification Practices framework (ISO/TC68/SC 2 and RFC 2527), Gatekeeper Criteria for Accreditation of CAs, NIST Common Criteria, CS2/CSPP for COTS Protection Profile

2000 -2003 – ANSI X9.79, WebTrust for CAs, ETSI TS 101 456, ISO 17799, ABA's PKI Assessment Guidelines, RFC 3647, ETSI TS 102 042, Certificate Issuing and Management Components (CIMCs) Protection Profile

2005 - 2007 – Meetings of the CA / Browser Forum to work on guidelines for EV SSL certificates, ISO 27001 adopted and ISO 17799 revised into ISO 27002

2011-2013 – ISO 27007/27008; ETSI TS 119 403 (EN 319 411-3), Baseline Requirements, Security Requirements, WebTrust 2.0 and ETSI updates, WPKOPS, CA Security Council, OTA's CA Best Practices, NIST Workshop on Improving Trust in the Online Marketplace

WebTrust Program for CAs

Audit of Management's Assertion that it has:

- assessed the controls over its CA operations
- maintained effective controls providing reasonable assurance that
- CA systems development, maintenance and operations were
  - properly authorized and
  - performed to maintain CA systems integrity.

http://www.webtrust.org/homepage-documents/item27839.aspx

Audit Coordination for Baselines

- Catch-22 for Browser Audit Report Requirements
- Final draft of 1.0 ready in Q2-2011 for public comment
- Effective date of July 1, 2012, but 2011 CA hacker
- SSL Baseline Requirements Audit Criteria v1.1
  - Effective January 1, 2013
  - Added nearly 60 new checklist items to WebTrust 2.0
- ETSI TS 102 042 v.2.2.3 and ETSI TR 103 123 v.1.1.1 (2012-11) - *Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates*

CA / B Forum Baseline Requirements

Rationale: Common security concerns exist for SSL/TLS and PKI for the Web.

Various stakeholders should not create (and then have to maintain) multiple, conflicting criteria that Certification Authorities have to meet.

If common baselines and reference points exist, then the number of variations will be reduced in root trust programs and audit schemes.

More about Baseline Requirements

CAs must assert that they comply with the Baseline Requirements and identify which certificates they issue and manage comply.

Profiles are specified, as well as time periods for validity of certificates and certificate information, and there are sunsetting / grandfathering provisions to effectuate change.

A foundation is in place among key participants that will facilitate ecosystem improvements over time.

Working with Mozilla and others on CA Practices

OTA's CA Best Practices

- CA checks reliable third party records, operates a quality control program, and screens and trains its employees.
- CA audited for compliance with Baseline Requirements and other CA / Browser Forum guidelines, and auditors are competent in computer security auditing.
- CA logs computer activity, reviews those logs, and conducts vulnerability scans and penetration tests. Roots are offline / air-gapped and protected by multiple layers of controls.
- CA maintains and regularly reviews practice statements, including business continuity, disaster recovery, and security incident response plans.
- CA stays current with developments by participating in industry-related organizations and events.

https://otalliance.org/resources/SSL/CABestPractices.html

CA Security Council

Group of commercial CAs formed in February 2013- *to advance internet security by promoting deployments and enhancements to publicly trusted certificates* [and to address SSL security awareness] *through public education, collaboration, and advocacy. The CASC strives for the adoption of digital certificate best practices and the proper issuance and use of digital certificates by CAs, browsers, and other interested parties* [and their potential impact on the internet infrastructure].

https://casecurity.org/mission/

CA / Browser Forum Transparency

- April – May 2011 – draft Baseline Requirements published and public comments solicited on Mozilla list (and over 100 comments were received and addressed or logged for resolution)
- May 2012 – public discussion email list created
- June 2012 – draft Network and Certificate System Security Requirements published for public comment on Mozilla list (no comments received)
- February 2013 – member votes are fully public

Path Ahead for CAs / Browsers

- Address SSL/TLS vulnerabilities by gathering information and following up after workshop
- Improve coordination with WebTrust, ETSI, and other key stakeholders
- Code Signing Working Group to identify and address weaknesses in code signing PKI
- Increased public outreach and education on secure implementation of SSL/TLS