Standards and Industry Regulations Applicable to Certification Authorities

By Kirk Hall, Trend Micro, Inc. (CA Security Council member)

From time to time observers of the Certification Authority (CA) industry have asked if additional rules and regulations applicable to CAs and the issuance of digital certificates would be beneficial to the internet security ecosystem.

To consider this question, it's first important to recognize the existing extensive standards and industry regulation of CAs that have been in place since 2000.

First, who are the CAs? It's been erroneously reported there are more than 600 publicly trusted CAs in the world – but that is incorrect. Instead, there are only about 65 publicly trusted CAs (including government CAs) with roots in the major browsers and applications. This includes CAs which own multiple roots in the browsers -- but all of these roots are subject to the same unitary performance audit standards and requirements discussed below. For more information on this issue, see https://casecurity.org/myths/.

1. WebTrust for CAs (2000)

The first requirement imposed specifically on CAs as a group was in 2000 when an annual security audit under the WebTrust for CAs standards was mandated by browsers and others with trusted root stores. See the original WebTrust audit standards available at http://www.webtrust.org/homepage-documents/item27839.aspx. These standards have been updated from time to time, so the current WebTrust audit standards are reflected in the detailed v.2.0 requirements found at the same link. Even before the first WebTrust for CAs standards in 2000, most CAs also underwent annual performance audits under SAS 70 standards (later replaced by SSAE 16 / SOC 2 / SOC 3) – and many still do in addition to WebTrust.

Nearly all CAs in North America follow the WebTrust standards, but CAs in other parts of the world may be audited to the equivalent ETSI (European Telecommunications Standards Institute) audit standards – see www.etsi.org. Government CAs must submit equivalent government performance audits on a periodic basis as well.

WebTrust for CAs requires annual performance audits by an independent third party auditor (usually from the world's major auditing firms) of a CA's operations and practices in each of the following substantive areas:

- Business practices disclosure
- Business practices management
- Environmental controls (especially security controls)
- Key life cycle management controls
- Subscriber key life cycle management controls

- Certificate life cycle management controls
- Subordinate CA certificate life cycle management controls

A successful audit results in an auditor report in prescribed form which is published on the CA's website and is also forwarded to each browser and application whose trusted root stores contains the CA's roots. Non-conformance with any material WebTrust or ETSI requirement will generally result in a "qualified" final audit report (rather than an "unqualified" report indicating full compliance), which will usually require remedial action by the CA.

Who enforces compliance with these audit standards and makes sure each CA successfully completes a WebTrust or ETSI audit every year? The major browsers and applications that include the CA's roots in their trusted root stores, including such browsers as Microsoft, Mozilla, Apple, Google, and Opera and mobile device or other applications such as Nokia, Android, Oracle, and Java. Without an annual WebTrust or ETSI audit report, the browsers and applications could remove a CA's trusted roots and the CA's end-entity certificates would no longer be trusted.

2. Raising the Bar – the CA/Browser Forum (2005)

To further raise the bar, CAs and the major browsers began meeting in 2005 to develop additional requirements to be met by all CAs through an informal group named the CA/Browser Forum. See www.cabforum.org.

The CA/Browser Forum's work currently includes bi-weekly teleconference calls and face-to-face meetings three to four times a year. Outside observers from the auditing standards bodies also participate, and information about Forum activities, including meeting minutes, are published on the Forum's public mailing list. There are increasing opportunities for interested third parties to participate in subject matter working groups, such as the Revocation Checking and Code Signing working groups.

3. Extended Validation (EV) Guidelines (2007)

The Forum's first major deliverable was the document *Guidelines for the Issuance and Management of Extended Validation Certificates* ("EV Guidelines") in 2007. The current version of the EV Guidelines is v.1.4, and creates uniform minimum standards for those CAs who issue EV certificates in the areas of security and training as well as the methods for authenticating organizations before issuance of EV certificates. These EV certs represent a higher trust level and so receive a special user interface treatment by the browsers, namely the "green bar" and the display of additional identity information for the website. See the current EV Guidelines at https://www.cabforum.org/documents.html.

The EV Guidelines were quickly incorporated into a ***second*** set of WebTrust audit requirements, named the *Certification Authorities – Extended Validation Audit Criteria* (the current version is v.1.3). CAs have been required to successfully complete a

second EV WebTrust annual audit (or ETSI equivalent) each year since 2008 in order to issue EV certificates that are recognized by the browsers with an EV user interface.

4. Baseline Requirements (2012)

CAs and browsers next decided to extend some of the higher standards represented by the EV Guidelines to all other SSL server certificates through the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* in 2011 - the current version is v.1.1. See again https://www.cabforum.org/documents.html.

The new Baseline Requirements were embodied in a *third* set of WebTrust audit guidelines, the *SSL Baseline Requirements Audit Criteria (v1.1)* – see again the WebTrust documents available at http://www.webtrust.org/homepage-documents/item27839.aspx.

This means that those CAs who offer Extended Validation (EV) certificates will now have to complete a *third* annual performance audit starting in 2013.

5. Network and Certificate System Security Guidelines (2013)

Finally, in response to certain notable security breaches of CAs in 2011-12, including the Diginotar breach, CAs and browsers began work on heightened security infrastructure requirements for CAs (and for any external sub-CAs or Registration Authorities who have the ability to cause the issuance of a certificate from a publicly trusted root) through the new *Network and Certificate System Security Requirements*, which became effective January 1, 2013. See https://www.cabforum.org/documents.html. CAs have already agreed to voluntary compliance with these new and heightened security standards.

These new standards will be incorporated in the next version of the WebTrust for CAs audit requirements, probably later in 2013, and will increase the annual audit requirements applicable to all CAs to address recent security breaches.

6. Additional Browser Root Program Requirements

On top of the multiple WebTrust or ETSI audits each CA must successfully complete every year, the browsers have imposed additional trusted root program requirements that go beyond WebTrust and ETSI. These include the Microsoft Root Certificate Program, http://social.technet.microsoft.com/wiki/contents/articles/3281.introduction-to-the-microsoft-root-certificate-program.aspx, and the Mozilla CA Certificate Policy, http://www.mozilla.org/projects/security/certs/policy/.

Both browser root programs include extensive requirements and have been updated with new rules over the years. It is important to note that the Mozilla policy –frequently

updated - was developed with input from the entire Mozilla community via public comment and drafting over many years.

7. Summary: Existing CA Standards and Regulations are Extensive and Ongoing

In summary, it would be fair to say that CAs today are subject to considerable common security standards and industry regulations, imposed on CAs by the CAs themselves and by the browsers and applications as a condition to being included in trusted root stores. The standards and regulations are effectively enforced through three annual performance audits conducted by independent third party auditors under WebTrust, ETSI, or government audit requirements. The industry has been on a path of continuous self-improvement since 2000, and its work is continuing.

Consumers and interested parties can participate in ongoing improvement activities through the public mailing list of the CA/Browser Forum, www.cabforum.org, and through specific Forum working groups. In fact, many of the Forum's recent standards originated with suggestions from users and observers, such as the prohibition against end-entity certificates being issued directly from trusted roots and the phasing out of certificates from trusted roots for internal server (local host) names or IP addresses – see BR Sections 9.2.1 and 12.

The Forum welcomes all suggestions for improvement to SSL practices in the internet ecosystem, and will be responsive to new ideas that represent practical improvements that respond to real threats, that can be implemented by users, and that won't break the Internet. To submit suggestions, please contact questions@cabforum.org.

8. Role of the CA Security Council (2013)

The SSL ecosystem is also being improved through another CA organization – CASC.

In 2013, seven major CAs decided to do more to improve SSL practices on the Internet through their collective action and formed the CA Security Council (CASC) – see www.casecurity.org.

These seven CAs collectively represent over 95 percent of all SSL certificates issued worldwide today, and include the following companies:

Comodo
DigiCert
Entrust
GlobalSign
Go Daddy
Symantec
Trend Micro

The Council's mission is to advance Internet security by promoting deployments and enhancements to publicly trusted certificates and through public education, collaboration, and advocacy. 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.

CASC's first major initiative is to promote the widespread deployment of OCSP stapling to improve certificate revocation checking, which is essential to security on the Internet. CASC members also serve as a resource to the press, standards bodies, and the public for all questions relating to SSL and CA operations.

For more information about any aspect of CA standards and industry regulation, please contact the CA/Browser Forum, or contact CASC and its members through https://casecurity.org/contact-us/ or through our representatives at Connect Marketing:

Sherri Walkenhorst
sherriw@connectpr.com
801-373-7888

Emily Richards
emilyr@connectpr.com
801-373-7888