PRINCETON
UNIVERSITY

Stephen Schultze
Associate Director
Center for Information Technology Policy

Sherrerd Hall, Room 304
Princeton, New Jersey 08544
609.258.2175
sjs@princeton.edu

Public Comments to the CA/Browser Forum Organizational Reform Working Group

March 30, 2012

I am pleased to respond to the CA/Browser Forum's request for comments on its plan to establish an Organizational Reform Working Group.[1] For more than a decade, Internet users have relied upon digital certificates to encrypt and authenticate their most valuable communications. Nevertheless, few users understand the technical intricacies of the Public Key Infrastructure (PKI) and the policies that govern it. Their expectations of secure communication with validated third-parties are set by the software that they use on a daily basis—typically web browsers—and by faith in the underlying certificates that are issued by Certificate Authorities (CAs). CAs and browser vendors have therefore been entrusted with critically important processes, and the public reasonably relies on them to observe current best practices and to relentlessly pursue even better practices in response to new threats.

The CA/B Forum emerged after the PKI system on the Internet was already established, but it has become one of the *de facto* venues for the industry to discuss and define policy standards. Although it began as a mechanism for creating the "Extended Validation" certificate policy standard, it has recently asserted a broader role in defining policy standards for the much larger set of certificates used throughout the industry.[2] The Forum is the industry's attempt to create a self-regulatory structure that can keep up with the rapid operational developments and security vulnerabilities in this area. It should be commended for its efforts.

Nevertheless, the current organizational structure suffers from at least two major shortcomings. First, the Forum includes no representatives from the public or from CAs' customers—these are commonly referred to by CAs as "Relying Parties" and "Subscribers," respectively. This is troubling, given that these are the entities that are most at risk from poor policies or practices. Second, the Forum conducts its business largely in secret, with little public transparency into the process by which policies are developed and implemented. While there may be benefits to keeping some security vulnerability information private for short amounts of time, there is no compelling reason to do most of the Forum's work in private.

Fortunately, there are indications that the Forum is open to change. The call for comments notes that CA/B Forum will consider, "wider membership and participation," and "a more open and public process." The Forum derives its legitimacy from its users and the others in the PKI ecosystem that choose to implement its guidance. A major change in posture in the two areas cited is necessary for it to secure and retain this legitimacy.

[1] The comments and opinions presented here are entirely my own, and do not necessarily reflect those of Princeton University, the Center for Information Technology Policy, or any other entity.
[2] "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0" at http://cabforum.org/Baseline_Requirements_V1.pdf

Wider membership should include representatives from all parts of the ecosystem, in proportions and with voting authority that allows them to meaningfully represent their interests. As a result of the industry structure, CAs dominate current membership. Some of this is inevitable given that there are simply far more CAs in existence than browsers, but the formal addition of relying parties, subscribers, and perhaps the auditor community would help promote a more diverse and healthy consideration of stakeholder interests. Likewise, the Forum should consider how to structure voting rights to ensure that these interests are appropriately represented the process, and how to encourage new entities that seek to take part.

The processes of the CA/B Forum should be made completely open to the public, absent some compelling reason in individual cases. Most of the rest of the PKI ecosystem, and indeed most policy processes related to the Internet as a whole, are conducted in public due to the broad set of stakeholders involved. The public posture of technical standards groups like the IETF and W3C should be guidance for opening the policy processes at the CA/B Forum. Email discussion lists, draft documents, and face-to-face meetings should all be made significantly more public.

The comments that PayPal has already submitted to the Forum succinctly summarize the need for an, "open, public, multi-stakeholder process."[3]

If the CA/B forum truly wishes to play a broader role in fostering industry best practices through proposed policies, it must be seen as representative, responsive, and transparent. If it cannot do this, it could fail not only to fulfill that mission but also to provide a dynamic industry-driven alternative to hands-on government intervention. The recent security breaches and revelations of troubling industry practices have not lent confidence to a process that is seen by many as being far too insular. Given the high likelihood of similar headline-grabbing developments in the future, CA/B Forum should change course while it still has that opportunity.

Regards,
Stephen Schultze

Associate Director
Center for Information Technology Policy
Princeton University

[3] "PayPal supports reform at the CA/Browser Forum" at http://www.thesecuritypractice.com/the_security_practice/2012/03/paypal-supports-reform-at-the-cabrowser-forum.html