Announcement and Press Release

Release Date: 11 April 2011 - For immediate release

CONTACT:
Tim Moses
Entrust
+1 613-270-3183
tim.moses@entrust.com

PUBLIC COMMENT RELEASE OF "BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED CERTIFICATES"

Members of the CA/Browser Forum <http://www.cabforum.org> have been collaborating over the last two years to develop baseline requirements for the issuance of digital certificates that facilitate secure communication with public Web sites. The secure communications protocol that uses these kinds of certificates is known as Secure Sockets Layer or Transport Layer Security (SSL/TLS).

While the CAB Forum continues to develop and improve these "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates," it has decided to seek public review of the current draft. During the review period (ending at the end of May 2011), the CAB Forum is seeking constructive input on potential improvements to the document.

Once adopted, the Baseline Requirements will apply to the operation of all Certification Authorities that issue SSL/TLS certificates that chain up to any one of the root certificates embedded as trust anchors in publicly distributed browser software.

CA and browser members of the CAB Forum acknowledge that the current version lacks provisions in some key areas, and they anticipate working in the coming months to overcome these deficiencies. Nevertheless, they see great value in adopting and enforcing an initial version covering those areas where agreement has already been achieved. For this reason, the CAB Forum welcomes well-thought-out, constructive improvements to the current draft. Proposals for more far-reaching changes will be considered. However, proposals that may significantly hold-up the adoption of common requirements for the industry must await a future revision.

According to a spokesperson for the CAB Forum, "Representatives of the major browser suppliers and Internet certification authorities have long recognized the need to establish and enforce common standards for assurance across the industry. The current draft of the Baseline Requirements represents an initial step in that direction. We welcome input from others with expertise to share. And we expect to continue to enhance these requirements as the threat landscape evolves."

During the public comment period, the CAB Forum encourages discussion of the draft requirements on the Mozilla Dev-Security-Policy discussion list under a general topic of "Baseline Requirements," or more specifically by categorizing comments and discussion by section number and discussion topic as suggested below.

Additional information about enrolling on the Mozilla discussion mailing list can be found at: <https://lists.mozilla.org/listinfo/dev-security-policy>.

The discussion can also be followed without enrolling at:
<http://groups.google.com/group/mozilla.dev.security.policy/topics>.

Those desiring to comment directly to all members of the CAB Forum, but not specifically for purposes of open public discussion on the Mozilla list, may send email to questions@cabforum.com.

During the 45-day comment period, members of the CAB Forum will also participate in discussions on the Mozilla list and will gather, and to the extent possible, respond with clarifications or proposed revisions to the appropriate public or private channel based on whether the comment was received through the Mozilla list or the CAB Forum's questions email list. Both private and public comments received, and any resulting agreed-upon changes to the Baseline Requirements, will be posted to the CAB Forum Web site and/or to the Mozilla list.

Following the close of the open comment period, the CAB Forum will take under consideration and further discuss comments that could still not be resolved during the public comment period, and a final draft version of the Baseline Requirements that incorporates clarifications or improvements will be considered for adoption by the CAB Forum.

Following adoption of Version 1.0 of the Baseline Requirements, the CA/Browser Forum will request that all browser and relying party application software developers incorporate the Baseline Requirements into their accreditation and approval schemes as requirements for all applicants who request that a self-signed root certificate be embedded as a trust anchor in their software.

The CAB Forum also intends that the ETSI ESI Committee and AICPA/CICA Task Force on the WebTrust Program for CAs will coordinate revisions to their respective audit standards such that the Baseline Requirements will become auditable requirements starting in June 2011.

For existing subcategories found in the draft Baseline Requirements, please use the following framework, and, if necessary, extend the framework in order to accommodate your discussion topic:

BRi-Notices
BR1 -Scope
BR2 -Purpose
BR3 -References
BR4 -Definitions
BR5 -Abbreviations
BR6 -Conventions
BR7 -Warranties & Representations
BR8 -Community & Applicability
BR9 -Certificate Content & Profiles
BR10 -Certificate Application
BR11 -Validation Practices
BR12 -Certificate Status Checking & Revocation
BR13 -Employees & Third Parties
BR13.2 -Deleg. of Functions & Compliance Oblig
BR14 -Data Records
BR15 -Data Security -
BR15 -Data Security -Malware protection
BR15 -Data Security -Out-of-band confirmation
BR16 -Audit Requirements
BR17 -Liability & Indemnification
BR18 -Privacy & Confidentiality
BRA -Algorithm & Key Sizes
BRB -Certificate Extensions
BRC-User Agent Verification

For areas of discussion that you do not believe have been adequately accommodated in the existing outline, please use BR-New- followed by your specific discussion topic and please recommend an appropriate category or section heading.