WPKOPS

PKI for the Web

Steve Hanna
Tim Moses

IETF 85 BoF

Note well

http://www.ietf.org/about/note-well.html

Any statement made within the context of a BOF is considered an "IETF Contribution". All IETF Contributions are subject to the rules of RFC 5378 andRFC 3979 (updated by RFC 4879).

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

1. Introduction (Tim Moses) – 10 mins

2. The Web-app owner's perspective (Jeff Hodges/ Brad Hill) – 20 mins

3. The CA’s perspective (Ben Wilson) – 20 mins

4. Outstanding questions (chairs) – 10 mins

5. Comments and questions from the audience – 50 mins

6. Wrap-up (chairs) – 10 mins

Problem statement

Correct operation of the Web PKI depends upon coordination in the implementation, configuration, and deployment of its components (servers, clients, and certification authorities). These components are commonly developed and operated by unrelated organizations, yet important aspects of their functionality are not publicly well specified. This frequently leads to problems for the Web PKI's participants (application owners, infrastructure providers, and equipment vendors). Documenting these problems and their causes is required in order to have a basis for overcoming them.

Document editors

Trust model - Iñigo Barreira, Bruce Morton

Certificate, CRL, and OCSP field and extension processing - Ben Wilson, Robin Alden

Revocation - Phillip Hallam-Baker, Gary Gapinski

TLS stack operation - Adam Langley

Questions

1) Is the problem clear, well-scoped, solvable, and urgent?

2) Do we believe that product vendors will take notice?

3) Is the proposed charter (Draft 4) suitable?

4) Are there others willing to serve as editors?

5) Who is willing to review documents and/or comment on the mailing list?

6) Who feels that a working group should not be formed?

7) Who feels that a working group should be formed?