Web PKI OPS (wpkops)

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- **The IETF plenary session**
- **The IESG, or any member thereof on behalf of the IESG**
- **Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices**
- **Any IETF working group or portion thereof**
- **Any Birds of a Feather (BOF) session**
- **The IAB or any member thereof on behalf of the IAB**
- **The RFC Editor or the Internet-Drafts function**

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

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. Introductory remarks (blue sheets, appointment of note taker, Jabber scribe, agenda bashing) - chairs - 5 mins

2. Project update - chairs - 5 mins

3. Status reports

3a. Trust models – Bruce Morton - 20 mins

3b. Cert/CRL/OCSP processing - Ben Wilson - 20 mins

3c. Revocation - Phill Hallam-Baker - 20 mins

3d. TLS stack - Paul Hoffman - 20 mins

4. PKI: State of the art and future trends – 20 mins

5. Open mic. - 20 mins

Objective

Record how the Web PKI actually operates today

Using the Security Considerations section, systematically catalog weaknesses

(Potentially) spawn IETF activities to address the weaknesses

(Potentially) spawn vendor development activities to address the weaknesses

Background

IETF 85 (November '12) - First BoF

IETF 86 (March '13) - First WG meeting

IETF 87 (July '13) - No meeting

September '13 - Area advisors met with chairs and authors to discuss progress

Set deadline of 16 Oct 2013 to demonstrate renewed commitment

Additional authors were appointed

Topics

Trust model - draft-ietf-wpkops-trustmodels-00

- Bruce Morton
- Inigo Barreira
- Karen O'Donoghue

Browser processing - draft-wilson-wpkops-browser-processing-00

- Ben Wilson
- Robin Alden
- Santosh Chokhani
- Wayne Thayer

Revocation - draft-hallambaker-pkixstatus-01

- Phill Hallam-Baker
- Gary Gapinski
- David Chadwick

TLS stack - www.ietf.org/proceedings/88/wpkops.html

- Adam Langley
- Paul Hoffman

Time line

Jun 2013 - First WG draft of 'trust model' document

Oct 2013 - First WG draft of 'certificate revocation' document

Oct 2013 - First WG draft of 'TLS stack operation' document

Feb 2014 - First WG draft of 'field and extension processing for certificates, CRLs, and OCSP responses' document

Jun 2014 - IESG submission of 'trust model' document

Jun 2014 - IESG submission of 'TLS stack operation' document

Oct 2014 - IESG submission of 'certificate revocation' document

Feb 2015 - IESG submission of 'field and extension processing for certificates, CRLs, and OCSP responses'

Charter issues

Reset time-line