SIP -- IETF 68

Chairs:
Keith Drage
Dean Willis

Jabber rooms:
   Debate: sip@jabber.ietf.org
   Transcript: sipscribe@jabber.ietf.org

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,
- any IETF working group or portion thereof,
- the IESG, or any member thereof on behalf of the IESG,
- the IAB or any member thereof on behalf of the IAB,
- any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,
- the RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 3978 (updated by RFC 4748) and RFC 3979.

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 3978 (and RFC 4748) for details.

Agenda, Session 1

Time	Topic	Discussion Leader
1740	Agenda Bash	Chairs
1745	ICE Option Tag	Jonathan Rosenberg
1800	GRUU Changes	Jonathan Rosenberg
1820	3261 Revision Process	Robert Sparks
1840	Break	

Agenda, Session 2

Time	Topic	Discussion Leader
1300	SIPS Guidelines	Francois Audet
1325	Outbound	Cullen Jennins
1410	Request Fragmentation	Marc Petit-Huguenin
1420	SIP URI Service Discovery using DNS-SD	Jae Woo Lee Henning Schulzrinne
1430	Clarification of Privacy	Mayumi Munakata
1440	Record Route Management	Thomas Froment
1450	Domain Certificates	Vijay Gurbani

Announcements

draft-dotson-sip-certificate-auth-sol

- *What?*
  - Certificate based authentication in SIP networks
- *Why?*
  - Certificates offer strong authentication credentials; can enable authentication without pre-configuration of individual certificates (via the Public Key Infrastructure)
  - Many existing and planned deployments rely on certificates
- *Key Features*
  - Solution architecture is based on RFC2617
  - The private key is used to sign a string of data from the SIP dialog to create a challenge response; identity authentication is achieved using the public key
- ***Feedback is requested on the I-D***

SPITSTOP Discussions

- Spam over Internet Telephony (SPIT) has potential to become a serious problem when IP Telephony is massively used
  - similar to email spam today
- Some I-Ds address the issue already
  - draft-ietf-sipping-spam-04
  - draft-froment-sipping-spit-authz-policies-02
  - draft-tschofenig-sipping-spit-policy-00
  - draft-jung-sipping-authentication-spit-00
  - draft-niccolini-sipping-feedback-spit-03
  - draft-niccolini-sipping-spitstop-00
- We should discuss what actions of the IETF are needed to deal with the issue
- There is a mailing list for this discussion:
  - https://listserv.netlab.nec.de/mailman/listinfo/spitstop