

HTTP-Auth

IETF 90 – Toronto

Chair Slides
chaise glisse

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

- 10:00-10:05 – Blue sheets, Agenda bashing
 - Also finding a jabber scribe and reading the note well
- 10:05-10:10 – Status
- 10:10-10:20 – Basic & Digest enhancements (chairs)
- 10:20-10:35 – Digest (Rifaat)
- 10:35-10:50 – Basic (Julian)
- 10:50-11:10 – SCRAM (Alexey)
- 11:10-11:20 – Other documents
- 11:20-11:30 – Open Mic

Status

- New versions of Basic & Digest
- New version of Mutual
 - First version of Mutual-Algo
- New version of SCRAM
- New version of HOBA

- Rest-Auth has been allowed to expire.
- Also “Extension”, but that is likely a mistake, right?

Basic & Digest Enhancements

- The charter requires us to update Basic & Digest:
 - I18N for both
 - New algorithms for Digest
- The group has considered further changes:
 - Hashed username in Digest (in the draft)
 - Username parameter in the challenge for Basic (M. Sweet)
- None of these changes are going to make either of these protocols an example of modern security.
- They're likely to generate DISCUSSEs when they reach the IESG.
- That doesn't mean we can't do them.
 - But let's DISCUSS this now.
- Do we want to make changes to Basic & Digest other than I18N and new hash algorithms.

Presentations by Rifaat, Julian,
and Alexey go here.

Other Documents

- We now have the complete set of Mutual-Auth, Extensions and Algorithm.
- HOBA hasn't changed much.
- Do people think HOBA is ready for WGLC?