THE PPSP PEER PROTOCOL (PPSPP)

Arno Bakker
Riccardo Petrocco (TU Delft)
Victor Grishchenko (Citrea LLC)

VU UNIVERSITY AMSTERDAM
LOOKING FURTHER

OVERVIEW

- Updates since IETF 89:
- -09:
  - Nits about e.g. newer references fixed
- -10:
  - LEDBAT was not in Normative references
- IESG telechat on July 10th
  - All Area Directors vote on draft

IESG TELECHAT

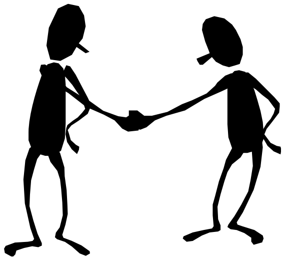
- IESG Evaluation: Revised I-D Needed
- Has 5 YES / NO OBJECTIONs
- Has 4 DISCUSSes.
- Needs 5 more YES or NO OBJECTION positions to pass

- Reviews from:
  - OpsDir
  - GenArt
  - SecDir

DISCUSS BARNES

“My DISCUSS here is based mainly on the readability of the document, which seems bad enough to be an impediment to interoperability.

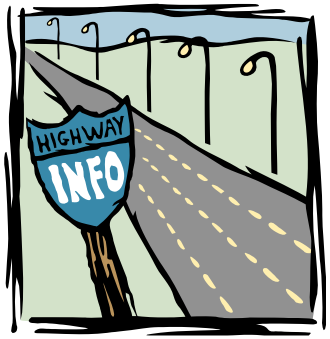
As far as I can tell, this document does not define a protocol, in the sense of a set of actions required to achieve a given objective.”



DISCUSS COOPER

“I'm a little surprised about the choice of LEDBAT for congestion control of live streams. It seems like LEDBAT is not what the receiver would want the sender to use for live-streamed content […]

will yield early, […] no […] acceptable level of quality”



DISCUSS MORIARTY

“I am still reading this draft, but don't see any response to the SecDir review that raised some very important points for discussion: […]

I'll amend this when I get further into my review and would appreciate a response to the SecDir review.”

DISCUSS FARRELL

“I have a number of discuss points (sorry;-), but most of 'em are pretty simple really.

(1) 3.10: What is a "benign" environment? I actually do understand what is meant, but how could a program evaluate that in order to decicde [sic] whether or not to send a PES_RESv4?”

“(2) 6.1.2.2: What exactly are the "munro" bytes that are the first input to the signature? […]”

DISCUSS FARRELL

“(3) 7.6 and 13.5: SHA1 as the MTI is wrong. Why is that ok, given the collision resistance is less that designed for?”

“(4) 7.7: Why RSASHA1 and not RSA with SHA256?”

“(5) 7.10: The message number is wrong in the figure.”

$$Q^{-1} \sum_{z} \sum_{y} |y\rangle\, |z\rangle \sum_{x:\, f(x)=z} \omega^{xy} .$$

DISCUSS FARRELL

“(6) 8.4: […] two questions:

a) where is the "chunk size used" option in section 7? and

b) do all the swarm metadata options have to be sent each time with no limit on ordering […]?”

“(7) 8.13: Don't you need to register the ppsp URI scheme?”

- ppsp://192.0.2.0:6778/e5a12c…

DISCUSS FARRELL

“(8) 13.4: Wouldn't DTLS change the chunk size considerations and also influence how messages map to datagrams?”

IANA STATUS

IANA Review State: IANA OK - Actions Needed

- Version 0 not defined :-(
- Question one single top-level registry [for] the six new registries defined in this draft?
- Hence: IESG Evaluation: Revised I-D Needed

Internet Assigned Numbers Authority

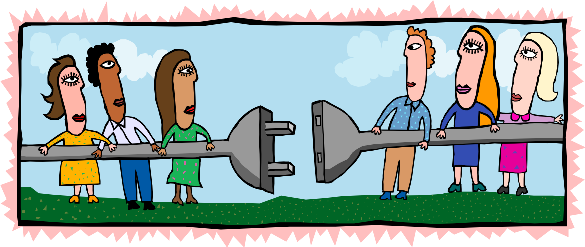
FUTURE

- Await other AD ballots
- Respond to DISCUSSes so far
- Process COMMENTs and reviews

- Moving forward!

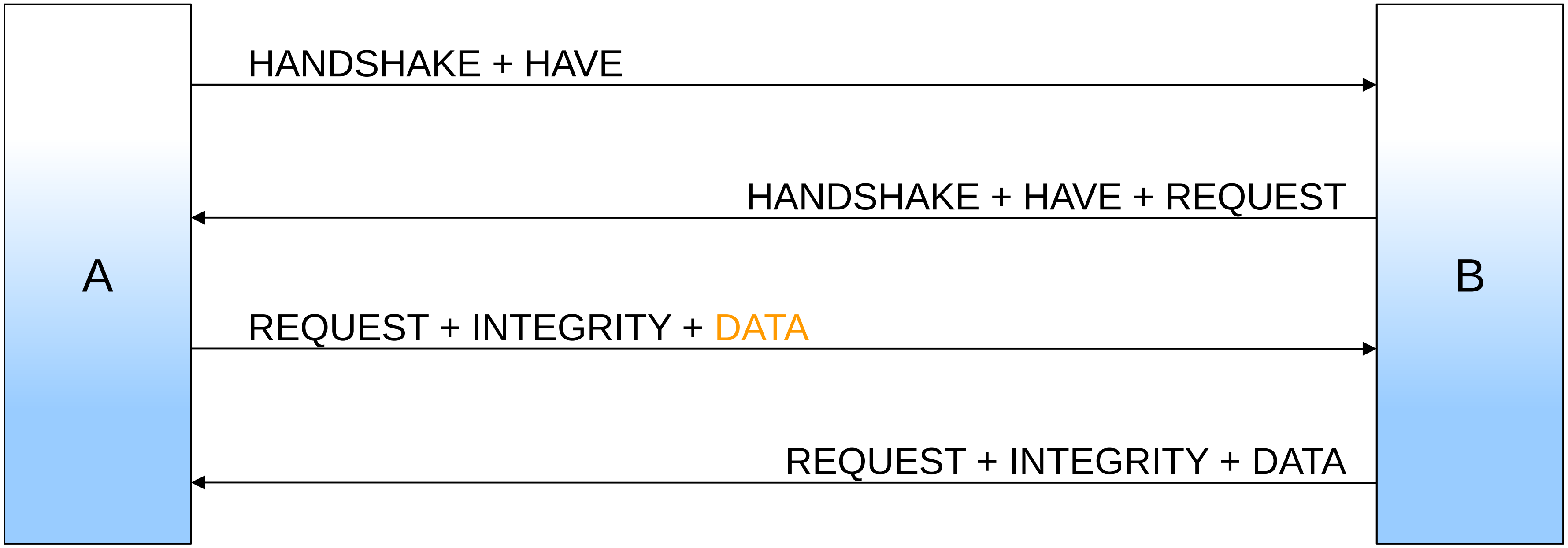
REFRESH: PPSPP MESSAGES

- Basic unit of communication: Message
  - HANDSHAKE
  - HAVE: convey chunk availability
  - REQUEST: request chunks
  - DATA: actual chunk
  - INTEGRITY: hashes to enable integrity verification
  - …
- Messages are multiplexed together when sent over the wire.



EXAMPLE PPSPP ON THE WIRE

- Peer A and B both have some chunks:


A
B
HANDSHAKE + HAVE
HANDSHAKE + HAVE + REQUEST
REQUEST + INTEGRITY + DATA
REQUEST + INTEGRITY + DATA

- Note: low latency, data transfer already in 3rd datagram.