# draft-ietf-mptcp-rfc6824bis IETF98 update

Alan Ford <alan.ford@gmail.com>
Costin Raiciu, Mark Handley, Olivier Bonaventure, Christoph Paasch

# Since IETF97

No changes, -08 draft (not currently published) currently has typo corrections from -07

Need to decide what if anything else is added to this base spec...

# SHA-256 in place of SHA-1

SHA-1 is deprecated everywhere, so we can’t really release 6824bis using it.

Propose just replacing SHA-1 with SHA-256 everywhere.

Although we truncate the hashes, this improves quality of hash data and removes any dependency on legacy code.

Consensus?

# Fabien’s Proposals

Proposal 1/5 - Flag “do not use this address for subflow establishment” for load balancers and for NATs. *Adopted*.

Proposal 2/5 - Reliability of ADD_ADDR. *Adopted*.

Proposal 3/5 - Differentiate between make-before-break (today’s ‘B’ flag in MP_PRIO) and break-before-make (a flag in ADD_ADDR). *Not yet adopted, limited support*.

Proposal 4/5 - More granular priorities. *Abandoned due to lack of clarity of definition.*

Proposal 5/5 - “Communities” to group address options on the same interface, e.g. IPv4/IPv6. *Limited support*.

# Application Layer Authentication

Presented in IETF96, would like to revisit.

Separate crypto scheme in the MP_CAPABLE negotiation. If chosen to be used:

- Decouple keys and tokens; only tokens exchanged in MP_CAPABLE
- MP_JOIN etc authenticated through query to application layer
- Allows arbitrary application-layer authentication; initial proposal is using TLS key exporter

Benefits:

- Encode arbitrary data in the token, for e.g. load balancing
- Remove keying material from the wire

Any interest in revisiting this?

# Anything else to add?