TLS FLAGS

YOAV NIR – IETF 112 – 9-NOV-2021
SINCE IETF 111

• Gone through WGLC
• Added requirement to drop malformed packets
• Published version -07
• Are we done?
  • Three Issues may be open
ISSUE 1/3 – GUIDANCE FOR IANA EXPERTS

- Section 4.1 contains guidance on how to assign numbers to flags.
- Martin Thomson opened Issue #11 and suggested to remove all the advice and leave it all to the discretion of the expert.
- I think giving the expert the rationale is important.
- So far, no changes have been made.
The RECOMMENDED field in the new registry is described as follows:

* Recommended, which is a Y/N value determined in the document defining the optional feature.

The text does not go into any further detail regarding what it means.

The assumption was that it meant the same as in other registries, as specified in section 5 of RFC 8447.

Do we need extra text to say so explicitly?
ISSUE 3/3 – DTLS 1.2

• Achim Kraus opened Issue #13, asking that the Flags extension be defined for DTLS 1.2 as well.

• Apparently, this could be useful for DTLS-RRC (Return Routability Check), which does address DTLS 1.2 as well as DTLS 1.3.

• Currently, the TLS-Flags draft is for TLS 1.3 and DTLS 1.3 only.

• Up to the WG…
ANY OTHER ISSUES?