Cipher Suite Proliferation

Tim Polk
Sean Turner

IETF 78
29 July 2010
Standardizing Cipher Suites

• What we do now:
  – Algorithm is specified in Informational I-D/RFC.
  – How you use the algorithm with a particular protocol is specified in a different I-D/RFC and usually it’s Standard Track – but not always.

• The IANA registry often guides the choice for the I-D/RFC on the how you use the algorithm with a particular protocol.
  • E.g., SRTP requires Standard Track but TLS allows S/I/E.
Changing the Status Quo?

• Recently, some WGs have declined to work on cipher suite documents and they’re coming to the ADs:
  – Every author wants Standards track.

• Tim and I have discussed whether we should change to target more cipher-suite IDs to Informational.
Choices, Choices

• To summarize the steps, we think there are two ways to get a standards track cipher suite RFC:
  – Rule 1 - If the I-D came from a WG.
  – Rule 2 - If the cipher suite has broad international support and there’s a need and implementation(s).