Updates to the Cipher Suites in Secure Syslog

draft-ietf-uta-ciphersuites-in-sec-syslog

Chris Lonvick, Sean Turner, **Joe Salowey**

UTA@IETF114 - 20220727

Refresher

Status: Recently adopted as WG item

Abstract: Updates cipher suites in RFCs 5425 & 6012 and the transport protocol in RFC 6012

Motivation: Prompted by members of IEC 62351 TC 57 WG15; 5425/6012 algorithms are weak

-00 Text:

- Use TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 and not TLS_RSA_WITH_AES_128_CBC_SHA
- MUST use (D)TLS 1.2
- MAY use (D)TLS 1.3

Addressing 0-RTT in -01

Text [will be included/is included] that:

- Describes what 0-RTT is
- Notes RFC 8447 requires a profile to use 0-RTT
- Specifies the following:

  Because syslog does not support replay protection, see Section 8.4 of [RFC5424], and most implementations establish a long-lived connection, this document specifies that implementations MUST NOT use early data.

Next Steps

1. Publish/Review -01
2. Request WGLC end of August (?)
3. Profit!