Open Issues in RADIUS/(D)TLS to PS

radext WG Meeting
IETF 117 – San Francisco
Current implementations

- Desire to make combined RADIUS/(D)TLS specifications match current implementations wherever the text is ambiguous/unclear

- What implementations exist for RADIUS/TLS

- What implementations exist for RADIUS/DTLS
What is mandatory to implement?

• Having one document leaves us without two separate documents to reference for RADIUS/TLS and RADIUS/DTLS

• What is mandatory to implement for this specification?
  • RADIUS/TLS? RADIUS/DTLS? Both

• What is implemented today? (see previous slide)

• Resolution: Make whatever is more widely implemented today mandatory to implement (RADIUS/TLS?), make other optional
Single port for Auth and Accounting?

• Current specifications use a single IP Port for authentication and accounting packets
  • TLS uses TCP port 2083, DTLS uses UDP port 2083

• Do existing implementation match the current specification?
• Does this cause any issues?

• Proposed resolution: Leave as-is to match existing specifications
Deletion of MIB References

• The new document deletes the references to the MIBs

• Does anyone implement the MIBs or MIB counters for RADIUS/(D)TLS?

• If we remove the reference to the MIBs, should we add counters that a RADIUS server should maintain (similar to other RADIUS specs)?

• Proposed resolution: Ask the WG
Watchdogs

• Current text is ambiguous about requirement for watchdogs, because current RFCs contain conflicting text

• What do current implementations do?
  • Use Status-Server for RADIUS/TLS watchdog? Other?
  • Use Status-Server for RADIUS/DTLS watchdog? Use DTLS heartbeat? Other?

• Proposed resolution: Mandate Status-Server for RADIUS/TLS watchdogs, allow options of Status-Server of DTLS heartbeat for RADIUS/DTLS? Ask the WG
Use of ID 0 for all Status-Server requests

• The specification recommends using an ID of 0 for Status-Server requests, so that their use as watchdogs will not lead to exhaustion of the 256 bit ID space per connection.

• Do implementations do this today?
• If not, would it be worthwhile to reduce use of limited ID space?
• Would it be better to recommend the use of RADIUS/1.1? Instead, or in addition?

• Proposed resolution: Ask the WG
Add reference(s) to RFC 9325

• Provides guidelines on using TLS/DTLS in application protocols
• Should reference RFC 9325 and include references to specific sections where appropriate
  • Selecting cipher suites, etc.

• [https://datatracker.ietf.org/doc/rfc9325/](https://datatracker.ietf.org/doc/rfc9325/)

• Suggested resolution: Just do it!