DFN

draft-ietf-radext-radiusdtls-bis
Making RADIUS/(D)TLS a Proposed Standard

IETF 118 in Prague – radext | 10.11.2023

Janfred Rieckers | DFN-Verein

What happened since IETF117

▶ WG Adoption call finished, WG -00 version

▶ Changes, as discussed in San Francisco and thereafter on ML:

    – Trust model: PKIX+PSK mandatory for servers, clients can choose

    – Transport TLS+DTLS mandatory for servers, clients can choose

    – Updated text for Status-Server / Keepalive mechanism

    – Security considerations

    – Reference to TLS BCP

What is still needed?

▶ TLS Session Resumption (Request from Alan) – What should we say here?

▶ Implementation Considerations / Guidelines

– What should they say?

▶ Re-iterate Security considerations

– Is everything there that should be there?

– Can/should we remove some obvious sections?

– Should we move things to normative sections? (i.e. Migration UDP→(D)TLS has a few „MUST"s)

▶ Some small TODOs in the document, should be easy to fix

– CA indication for DTLS, Name „PSK Identifier", Port-Multiuse, Subnets

But wait – let's take a step back

▶ What problem do we want to solve?

▶ What we want to avoid: A ton of errata and a new -bis document in 2 years

▶ What we need for that:

– A list of all things that are wrong with RFC { 6613 | 6614 | 7360 }

  • That list we can tick off to know that we won't miss things

– A list of additional features that we need for RADIUS/(D)TLS

  • That list we can tick off to know that the new document is needed and we don't just need a bunch of errata and re-publish the original specs in standards track

Open issues and tasks

► What else is needed to publish this document?

– „Deprecating insecure Practices in RADIUS" somewhat depends on this

– WG schedule expects this in Jan 2024

► Open Dependency: Dynamic Discovery (RFC7585, Experimental)

– No normative ref? Downref? -bis?

► Re-iterate Normative References, there are some ref warnings from idnits

Discussion/Questions?

▶ Contact

▷ Jan-Frederik Rieckers

Mail: rieckers@dfn.de
Phone: 0049 30 884299-339
Fax: 0049 30 884299-370

Address:
DFN-Verein, Geschäftsstelle
Alexanderplatz1
10178 Berlin