draft-rieckers-radext-rfc6614bis
Making RADIUS/TLS a Proposed Standard

IETF 116 in Yokohama – radext | 28.03.2023

Jan-Frederik “Janfred”
Rieckers

Why RFC6614bis? (Changes since -01)

- Tasks:
  - Update TLS versions and MTI cipher suites
    - → Ref to RFC9325 for TLS guidance and cipher suites
    - → TLSv1.3 is included as RECOMMENDED, not MANDATORY. (See Discussion on ML/Github)
  - Add more text for TLS-PSK to use Radsec without PKI
    - → Most text should be in draft-dekok-radext-tls-psk
  - Add possibility for Raw Public Keys
    - → Basic text is there, needs to be expanded.

Why RFC6614bis? (Changes since -01)

- Tasks:
  - Add Server Name Indication
    - → No text yet, needs to be added
  - <insert your needed update here>
    - Are there any further updates?

Discussion items

- Credential Sharing
  - Is it OK that a number of clients share one certificate/PSK?
- RFC 2119 Modifier for
  - TLS-PSK
    - REQUIRED or RECOMMENDED
  - TLS-Raw Public Key
    - RECOMMENDED or OPTIONAL
    - Maybe even REQUIRED, now that OpenSSL has support for it?

Discussion items and next steps

- Handling certificate checks for Dynamic Peer Discovery
  - RFC7585 suggests using subjectAltName:naiRealm. Does anyone use it?
  - DNS Discovery may yield a hostname, use this if there is no naiRealm present in the certificate?
- RFC7585 is also still experimental, Downref or 7585bis?
  - 7585 also has 1 Erratum in status „Held for document update“
- Ready for WG adoption yet? (Maybe one more iteration as individual draft, adoption call in 1-2 months)

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