

deutsches forschungsnetz



DFN

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

IETF 115 in London – radextra BoF | 07.11.2022

Jan-Frederik “Janfred” Rieckers

About RFC6614 (RADIUS/TLS / „Radsec“)

- ▶ Published May 2012 as Experimental
- ▶ Use TLS to encrypt RADIUS packets
- ▶ Mutual authentication via certificates, optional TLS-PSK (without further specification)
- ▶ Wide deployment in eduroam®
 - Connection between National Roaming Operators
 - Mandatory for connection between NRO and institutions in Germany

Why RFC6614bis?

- ▶ Bump the protocol from „Experimental“ to „Proposed Standard“
- ▶ Add additional specification from deployment experience
 - Update TLS versions and MTI cipher suites (Make TLS1.3 mandatory?)
 - Add more text for TLS-PSK to use Radsec without PKI
 - Add possibility for Raw Public Keys
 - Add Server Name Indication
 - <insert your needed update here>
- ▶ Authors/Editors/Reviewers welcome.

Discussion/Questions?

DFN

► 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

