RADIUS Standards

As of End of 2023, there are several changes going on in the RADIUS specifications brought to us from the IETF. This page will document the different RADIUS standards.

(Disclaimer: This page is still Work In Progress)

RADIUS/UDP

This is the original RADIUS specification in RFC 2865 and RFC 2866.

RADIUS/(D)TLS

RADIUS/TLS is specified in RFC 6614, RADIUS/DTLS in RFC 7360. Both standards are in the "experimental" status, but are already heavily in use, especially for connecting NROs to the eTLRs.

RADIUS/(D)TLS-bis

With the 10 year anniversary of RFC 6614, the IETF is now working on making RADIUS/(D)TLS a proposed standard, the new standard is currently in draft status.

The main changes to RFC 6614 and RFC 7360 are the mandatory-to-implement features on the server side.

RADIUS/1.1

RADIUS/1.1 is a new way of calculating RADIUS packets that does not rely on the legacy cryptographic methods based on the RADIUS shared secret. Instead, RADIUS/1.1 relies completely on the confidentiality and integrity provided by (D)TLS, so RADIUS/1.1 can only be used over RADIUS/(D)TLS.

The migration to RADIUS/1.1 is fairly easy, since it is negotiated using ALPN (Application Layer Protocol Negotiation) within the RADIUS/(D)TLS handshake. Whenever both ends of the (D)TLS connection are running a software capable of RADIUS/1.1, the connection will be upgraded to RADIUS/1.1.

Apart from the calculation of RADIUS attribute obfuscation and cryptographic elements of the RADIUS protocol, the RADIUS messages are not altered, so RADIUS/1.1 is just another transport profile and should not affect any RADIUS operations.

Mutual authentication in RADIUS/(D)TLS (Certificates or TLS-PSK)

With RADIUS/(D)TLS, the use of the RADIUS shared secret, as used in RADIUS/UDP, is no longer necessary, instead the peers do mutual authentication within the (D)TLS layer.

This mutual authentication can be done via different means, the two main methods are certificates or Pre-Shared Keys.

IMPORTANT: When upgrading from RADIUS/UDP to RADIUS/(D)TLS with PSK, the PSK MUST NOT be identical to the RADIUS shared secret used before.

RADIUS feature matrix

For more information please check out the RADIUS slide deck with a feature matrix provided for WLPC EU 2023 by Herr Nilsson.