RADIUS Crypto-Agility Requirements

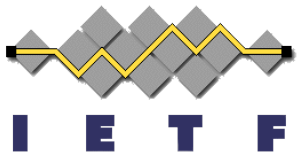
draft-ietf-radext-crypto-agility-requirements

March 30, 2011

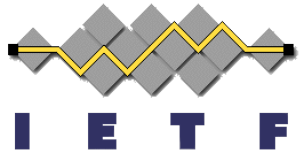
David B. Nelson

IETF 80

Prague, CZ



RADIUS Crypto-Agility Requirements - Status



- We have a RADEXT WG document to capture our consensus on the requirements.
- That consensus has developed over several IETF cycles since IETF-66.
- We will discuss remaining open issues at this meeting.
- The document will go to WGLC after IETF 80.
- Please read the document and file issues in TRAC ASAP!

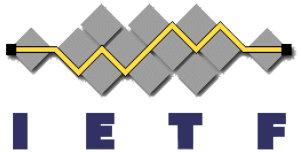
Open Issue #89

- Title: Keywrap and Password hiding requirements
  - The properties of a key and a password are different. Yet in several places, the document seems unclear about whether requirements for negotiation of Key-Wrap algorithms are distinct from requirements relating to hiding of passwords.
- Assuming that a proposal provides for confidentiality of entire RADIUS packets, is there a separate requirement for keywrap?

Open Issue #90

- Title: Process for publication and selection
  - Nowhere in the document is the approach to publication of crypto-agility solutions described, nor does the document describe how standards track crypto-agility mechanisms will be selected.
- Proposal is to describe the existing process:
  - Publication of proposals on Experimental track, and development of multiple interoperable implementations.
  - Evaluation for standards track based on requirements, experiment writeup and deployment experience.

RADIUS Crypto-Agility Requirements - Next Steps



- Final WGLC
- Address the comments received
- Issue a revised version
- Forward to the IESG?