draft-timms-encrypt-naptr-01.txt

jim@telnic.org

Summary

- We've done the experiment and written it up

- Key points:

    - Cleartext Order and Preference fields makes sense:

        - Don't disrupt DDDS processing sequence

        - Optimisation: handle x-crypto NAPTRs as needed without having to decrypt all of them first

    - I-D requesting a new RRtype for keys is pending in the RFC2929-bis process

Why Experimental?

- Well it was an experiment....

  - The I-D just explains how to do it

  - Proposes x-crypto as Services field

    - Use x- to comply with established convention

    - Won't disrupt installed base

Next Steps

- Finalise the I-D and get it out

- Get real-world operational experience with interoperability/applicability of different crypto algorithms & key sizes, analysis of use cases, etc.

  - Possible standards-track ID once that's been done?

QUESTIONS?