

DNSSEC Experiments

draft-ietf-dnsext-dnssec-experiments-00

David Blacka, davidb@verisignlabs.com

IETF-62

Goals

- An attempt to formalize a general method for doing non-backwards compatible experiments in DNSSEC.
- Specifically, in public.
- Could apply to a number of proposals before the WG.

Method

- Uses the “Unknown Algorithm” transition mechanism.
- Encourages use of private algorithm numbers for experiments.
- Recommends a private algorithm naming scheme.

Caveats

- Slim chance this will not work (SHOULD vs MUST)
- Experimentally signed zones do not look secure to resolvers unaware of the experiment.
- Some more exotic experiments might not be effectively hidden by this technique.

Transition

- Discusses (briefly) how one might transition from an experiment to a standard
- None of the approaches are pretty.