EPSILON

Minimally Covering NSEC Records and DNSSEC On-line Signing

draft-weiler-dnsext-online-signing-01.txt

Sam Weiler, weiler@tislabs.com
Johan Ihren, johani@autonomica.se

March 2005

General Idea

- To prevent zone-walking, use minimally-covering NSEC records
- No resolver changes needed (no “real” protocol changes)
- For existing names:

```
OwnerName NSEC OwnerName+ε (RRSIG NSEC A ...)
```

- Example:

```
 example.net NSEC example-.net (RRSIG NSEC
   DS NS)
```

Negative Answers

- On-demand generation of minimally-covering NSEC & RRSIG records (on-line signing)

  QNAME-ε NSEC QNAME+ε (RRSIG NSEC)

- Example, QNAME= example.com (non-existing)

```
exampld.com NSEC example-.com (RRSIG NSEC)
).com NSEC +.com (RRSIG NSEC)
```

Innovation

- Any ε function may be used, so long as the NSEC doesn't cover existing records
- Test for covered names; substitute real NSEC or real 'next name'
- Previous example:

```
exampld.com NSEC example-.com (RRSIG NSEC)
```

- If exampdd.com exists (as an unsecured delegation):

```
exampldd.com NSEC example-.com (NS RRSIG
  NSEC)
```

- If a.example.com exists (example.com is an empty non-terminal):

```
exampld.com NSEC a.example.com (RRSIG NSEC)
```

Status

- Suggested change: update dnssec-protocol section 2.3, which prohibits NSEC bitmaps of (NSEC RRSIG) – prohibit validators from rejecting NSEC's with only (NSEC RRSIG)

Questions

- Would the WG like to adopt this as a work item?
- Is the doc ready for WG last call?