DNS Key Distribution

Donald E. Eastlake 3rd

Member IETF

XXX Security Requirements

- include Authentication between previously unacquainted parties on the global Internet
- realistically, this means a public key system with some certification hierarchy

Public "KEY" Objectives

- Secure (signed Certificate)
- On Line / Highly Accessibility
- Variety of Key Types (RSA/DH)
- Use Natural Existing Names
- A system that will happen in our lifetimes...

Meeting the Needs

- DNS Security meets all these requirements:
- New KEY DNS resource record (RR) associates a public key of specified type with a natural DNS name
- New SIG DNS RR can authenticate any RR including a KEY RR. Such a signed named KEY is a certificate

Meeting the Needs (continued)

- DNS name zone hierarchy is the natural certification hierarchy
- DNS security extensions include provision for keys associated with users & hosts
- DNS security extensions include explicitly provision for indicating the protocol(s) that a key applies to
- DNS already widely deployed

DNS Security Deployment Status

- public alpha code to be made available soon by Trusted Information Systems (TIS)
- draft now incorporating implementation experience thus far: <ftp://ds.internic.net/internet-drafts/draft-ietf-dnssec-secext-04.txt> by D. Eastlake & C. Kaufman

Think About It...

KEY RR

```
                     1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             flags             |    protocol   |   algorithm   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               /
/                          public key                           /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
```

SIG RR

```
                     1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        type covered           |  algorithm    |     labels    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         original TTL                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      signature expiration                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         time signed                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         key footprint         |                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+         signer's name         /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               /
+-                          signature                           /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```