# DKIM Sender Signing Practices
## July 2007 Update

**Jim Fenton <fenton@cisco.com>**

# What's new?

- Now a Working Group draft:
  - draft-ietf-dkim-ssp-00
- Removed user-level granularity
  - high overhead, little constituency for feature
- SSP published as prefixed TXT records
  - Based on mailing list consensus
- Name change of primary tag: "p" -> "dkim"
  - In the spirit of ssp-requirements section 4.6
- New lookup algorithm
  - (Another) attempt at compromise between wildcard and search
- New info on publication requirements
  - Required records for new algorithm to work reliably

# What's not new?

- Have not incorporated XPTR (but discussed in 4.1)
  - Discussed in draft-hallambaker-xptr-00
- No third-party authorization
  - Discussed in draft-otis-dkim-tpa-ssp-01
- Section 5 (Third-Party Signatures and Mailing Lists)
  - Is still there
  - Probably belongs in the Overview Document
- Still no "nomail" policy
  - In or out of scope for the WG?
  - Doesn't "strict" but not signing do the same thing?

# Wildcard problems

- Use of TXT records requires use of prefixes
- Wildcards just don't work with prefixes

  Can't publish _ssp._domainkey.*.example.com

- Wildcards in the domain (or any parent) prevent a NXDOMAIN error from being returned

  Can't distinguish between non-existent domains and existing domains without SSP record

# Lookup Algorithm - Goals

- Support publication/lookup of SSP for names within the domain

  Ref: “subdomain coverage”: SSP requirements sec. 4.2

- Minimize load on parent domains, especially TLDs and root
- Minimize need to publish additional “synthetic wildcard” domains in each domain
- Support selected method of publication

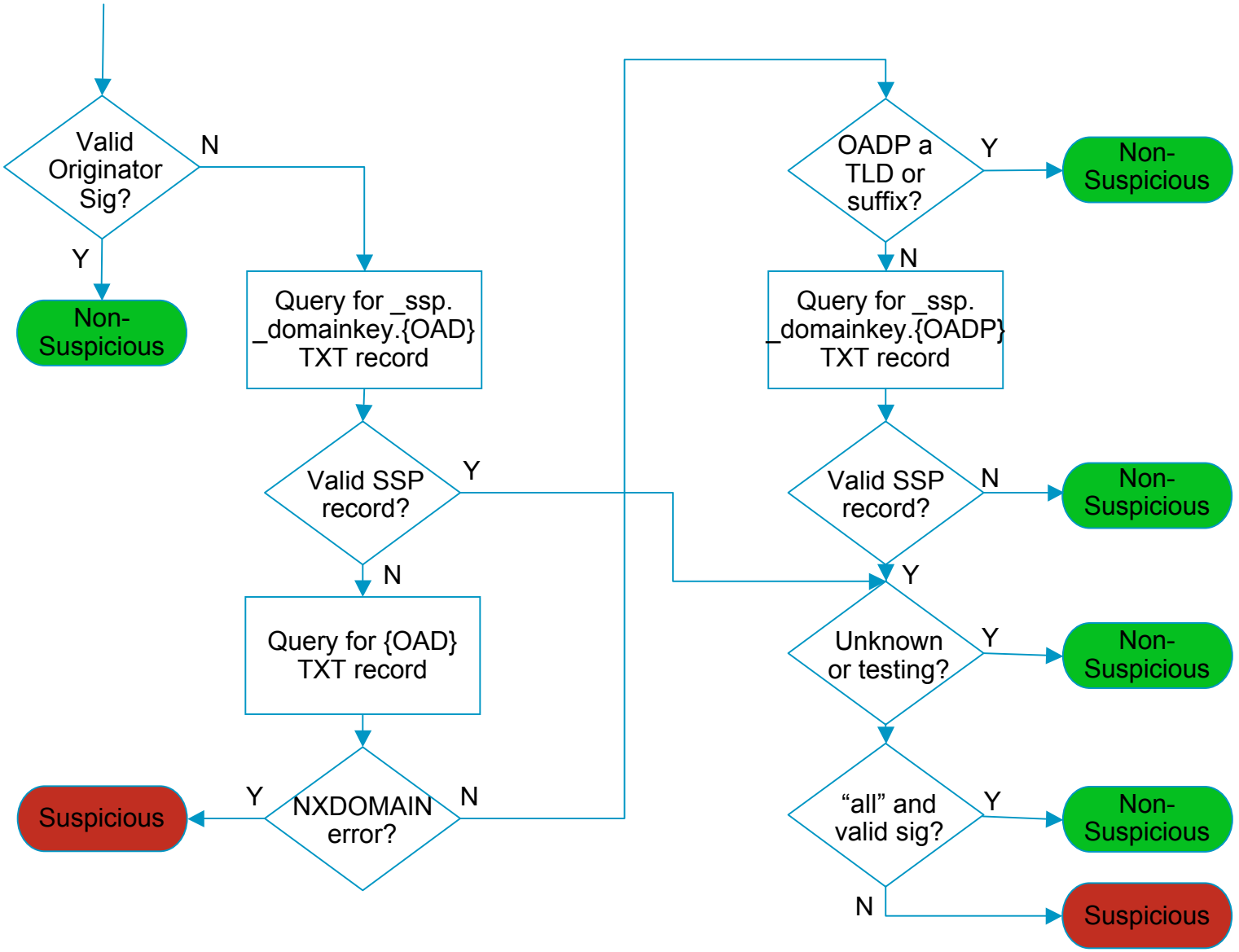
  WG consensus for prefixed TXT records rules out the use of wildcards

# Lookup Algorithm - Approaches

- If domain exists and SSP record doesn't, "climb the tree" looking for SSP
  - Unbounded and potentially excessive DNS lookups required
  - Concern about load on root and TLDs
- If domain exists and SSP record doesn't, assume no SSP
  - Requires publication of an SSP record alongside each name (A record, etc.) in the domain
  - Wildcards in domain problematic (a.example.com)
- If domain exists and SSP record doesn't, ascend one layer only
  - Requires publication of SSP only when more than one layer deep
  - Wildcards still problematic (a.b.example.com)

# SSP Lookup Algorithm

OAD = Originating Address Domain
OADP = Originating Address Domain's Parent



# Algorithm summary

- Maximum of 3 DNS lookups required
- Avoids need to publish SSP records at every other label in domain (A records, etc.)
- Interprets non-existent domains as suspicious
- Interprets existing but non-participating domains as non-suspicious

# Publication Requirements

- “Simple” names within SSP domains don’t require SSP records

  Resolved using parent lookup

- Two (or more) level names do:

  a.b IN A 10.10.10.10

  Subdomains as well, regardless if they’re in separate zones or the same zone as parent

- Avoid using wildcards (please)

# SSP “Strong” Option

- Some domains want to emphasize security over deliverability
  - Transactional domains from financial institutions
- They are making individual arrangements with consumer ISPs to drop unsigned mail
  - This doesn’t scale well!
- They would like to publish this request via SSP
  - Does not require verifiers to honor this request