DKIM Policy Proposals
3 Proposals
‘A La Carte’

• Discovery Mechanism

• RISC Policy Description
  – Its (almost) all in the Key Records

• RISC Policy Description
  – Transitions

• Meets all of the requirements specified
  – [6.3 Req 7: MUST NOT provide]
Discovery Mechanism Proposal
‘Dialectic’

• Thesis: Use Prefixed TXT Record
  – 100% Compatible with legacy infrastructure
  – Simple
  – Not Wildcard friendly

• Antithesis: Use new RR
  – DKIM is made reliant on deployment of new DNS infrastructure
  – Transition management is problematic
  – Result: RR nobody uses and a graceless wildcard kludge

• Synthesis
  – Leave prefix policy record as is
  – Introduce new prefix pointer record to solve wildcard problem
  – Result: Compatibility but with incentive to upgrade DNS
How – an additional indirection layer

- **PPTR record**
  - Argument is a DNS node
  - Does not take a prefix → wildcard friendly

- **New resolution scheme for prefixed records**
  1. Look for TXT at _prefix.example.com
  2. If not found look for PPTR at example.com
  3. If found look for TXT at _prefix.pptr.example.com

- **Wildcards work**
  - But domains that do not need them can still use TXT
RISC Policy

- There is only one policy that matters
  - ‘I do DKIM on everything’
- The policy language must be extensible
  - But there are no DKIM policy extensions
  - Only extensions to describe non DKIM features
    - ‘I use this reporting mechanism’
    - ‘I do S/MIME’

- RISC policy language:
  - Tag [=value] sequence
- Example
  - DKIM
Why only one policy matters

• Key Records contain all the detail
  – The Key algorithms permitted
  – The C18N algorithms permitted
  – The sender addresses record applies to

• What if I want a partial policy?
  – Specify a Key Record for NULL algorithm
    • Probably a sender address restriction!
  – Add a static header to each message
RISC Policy - Transitions

• What is policy for?
  – Allow conclusion to be drawn from
    • Lack of a Signature header
    • No Signature header
    • Both **MUST** be treated the same – NVS
    • I always sign + NVS means not compliant with policy
  – **Signatures** do not encourage message rejection
    • **Policy does**

• 3 Outcomes
  1. Signed
  2. Compliant with policy but not authenticated
  3. Not compliant
What does recipient do?

• Signed
  – Check to see if purported sender qualifies for whitelist
  – If not standard spam filtering

• Compliant but not authenticated
  – Standard spam filtering

• Not Compliant
  – Standard spam filtering
  – Standard spam filter with higher suspicion
  – Reject
    • (Probably not a good gateway policy)
  – May apply third party attributes
    • (Sender is phishing target)
Navigating a Transition

• Sign messages twice
  – Sign (Old), Sign (New)
  – Some recipients only process Old [New]

• Key records for unsupported algorithm
  – MUST be treated as valid

• Policy must express fact we sign twice
  – DKIM=selector1  DKIM=selector2
Why

- Policy has 3 outcomes
  1. Signed
  2. Compliant with policy but not authenticated
  3. Not compliant

<table>
<thead>
<tr>
<th>Fake Sig</th>
<th>‘I sign’</th>
<th>‘I sign twice’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foo</td>
<td>3 ✓</td>
<td>3 ✓</td>
</tr>
<tr>
<td>Bar</td>
<td>2 x</td>
<td>3 ✓</td>
</tr>
<tr>
<td>Foo + Bar</td>
<td>2 x</td>
<td>3 ✓</td>
</tr>
</tbody>
</table>
Summary

• Significantly reduce complexity of SSP
• Meets all requirements
  – Fully wildcard compatible
    • Policy discovery always 3 steps or less
    • Fully compatible with legacy DNS, DKIM
    • But still has new RR
• Meets unstated requirements
  – Only means of navigating transition