DKIM2 Header

IETF124

Open Questions

1. Single recipient per message, or multiple named recipients
2. Linkage between recipients and next domains:
    - nd=
    - pp=
    - CNAME selectors
3. Next hop DKIM2-support detection
    - Send DKIM2 header via SMTP extentions only
    - One signature per recipient
4. Sign all headers, or explicit list
    - Also oversign (all copies) or :name: × number of header fields

Single or Multiple Recipients

Problem statement: some sites (particularly Microsoft) want to send the same message to multiple recipients in a single SMTP transaction like they do now.

Options:

1. Ignore this request and force one signature per email (bad for adoption, extra signing cost, extra bandwidth use)
2. Include all the recipients in the one DKIM2-Signature (privacy concerns)
3. Include multiple DKIM2-Signatures, one per recipient, in the same email (extra signing cost, privacy concerns)
4. Send the signatures via SMTP and have the next system add them (complex)

Linkage between domains

Problem statement: some sites host domains for customers where they don’t control DNS, so may not be able to sign bounces.

Options:

1. Don’t allow sites to receive email for domains they can’t sign for
    a. Use existing DNS CNAME method used for sending as those domains
2. Have sending signer specify allowed next domains (`nd=`)
3. Have rt domain delegate to provider-owned domain via DNS (`pp=`)

DKIM2 support detection

Problem Statement: The sender doesn't know if the next hop supports DKIM2, which means you can't depend on it to verify, to sign bounces, or to strip anything that shouldn't be passed on.

Options:

1. DNS record for "I support DKIM2" to be published per-domain
2. SMTP extension to claim DKIM2 support per-connection
3. Design to not need next hop to reliably do anything

Sign All headers?

Problem Statement: Not all senders sign all the necessary headers for security, and new security issues with existing headers, or new security-critical headers, can be added later

Options:

1. Sign all headers except trace (Mail-Version will allow removing any changes)
2. Sign explicit list of headers as in DKIM
   a. All instances of each named header field (Mail-Version can remove)
   b. Explicitly list and oversign if wanted (same as DKIM)
3. Increase the “implicitly signed” headers to a large set or what’s known to be valuable to sign now; brittle but probably good for years.

NOTE: do we move most of this problem to Mail-Version and sign only the `Mail-Version` and `DKIM2-Signature` headers like ARC-Seal did.

Nit: Timestamp

Problem Statement: existing DKIM uses seconds since 1970-01-01T00:00:00Z, which is present in many standards. There's also RFC3339, and some other horrible formats used in various parts of email.

Options:

1. Use unix timestamp in DKIM2 as well
2. Use RFC3339 timestamp
3. Use one of the awful alternatives

Discussion topic: flags

Problem Statement: both the sender and intermediate sites may wish to make requests to later recipients.

Flags:

1. **donotmodify** This signer requests that this message not be further modified
2. **donotexplode** This signer requests that this message not be further exploded to multiple recipients
3. **donotforward** This signer requests that this message not be sent to any different recipient
4. **exploded** This signed wishes to state that it created multiple different copies of this same message
5. **feedback** This signer requests that this message be included in any feedback loop reports

Discussion topic: Multiple Algorithms

Problem Statement: we want to be agile with future algorithms, particularly post-quantum

Options:

1. Allow multiple separate signatures with different algorithms and same i=
2. Allow multiple signatures in the same header somehow
3. Something else?

Next steps for documents

Problem Statement: We have two drafts, dkim2-header and dkim2-spec, of which only header is adopted.

Options:

1. Pick one document and put everything in it
2. Make one the “how the mechanism works” and the other “how to use it”
3. Something else?