ALLDISPATCH
@IETF121

DKIM2

draft-gondwana-dkim2-motivation-00

Bron Gondwana, Fastmail
Richard Clayton, Yahoo
Wei Chuang, Google

IETF

Motivation

The dkim-replay group didn't progress because it didn't solve enough problems, this work replaces ARC and has significant buy-in.

DKIM2 is designed to support/mitigate issues with:

- DKIM Replay
- Backscatter
- Asynchronous spam-scanning / bounces
- Reversible modification algebra
- Mailing lists
- Forwarding services
- Abuse reporting for intermediates

Background

This work grew out of:

- ARC-Seal is meaningless security theatre: (Aug 2017) https://mailarchive.ietf.org/arch/msg/dmarc/4Gu1EErK4iuo9pQnZ-uJ2tKpMDQ/
- Email Mailpath (one of the DKIM-Replay drafts): (Oct 2022) https://datatracker.ietf.org/doc/draft-gondwana-email-mailpath/
- The DKIM-Replay problem statement: (Jan 2024) https://datatracker.ietf.org/doc/draft-ietf-dkim-replay-problem/

IETF

Goals

1. It is intended that legacy mail systems constructed in the last century will be able to interoperate with this new specification. However, more recently developed systems will, after a period of parallel running, need to be upgraded in order to continue to be able to authenticate email.

2. We favor simplicity over obscure functionality.

3. We aim to keep the number of cryptographic operations required the same or less, for all the most common types of email flow.

4. We aim to make all parts of the specification mandatory to implement because experience shows that interworking is adversely affected by providing optional functionality.

Draft Charter

https://notes.ietf.org/YGynIPpYS7yqg5G7ZeSQeA

Design proposals will be tested during the development of specifications. The working group will favor designs that are tested at scale, and produce:

- A design overview describing the problem area and proposed mechanism https://datatracker.ietf.org/doc/draft-gondwana-dkim2-motivation/
- An algebra for describing how to reverse common changes to email content https://datatracker.ietf.org/doc/draft-gondwana-dkim2-modification-algebra/
- A specification for authenticated email flow through multiple sites.
- A specification for error and bounce handling with the authenticated email flow.
- A best practices guide for implementation during the changeover period, in which interoperability with existing standards needs to be maintained.
- An update to DMARC adding DKIM2 as an additional mechanism.

IETF

Hoped-for dispatching outcome

A new working group

This is too big for MAILMAINT.

EMAILCORE is busy with other work.

there's energy;
there's a draft charter;
there's a couple of drafts already;
there's some experimental code already

IETF