JPAAWG
Japan Anti-Abuse Working Group

IETF Standards and Email Security

DMARC.org

Steven Jones

DMARC Update

DMARC RFC is 10 Years Old

- Charter approved in 2014 8月
- RFC 7489 DMARC published <u>2015</u> 3月
- New “DMARCbis” draft started in 2020 11月

- JPAAWG 7 – “There Is A Deadline”
  - Extended to 2025 3月

- Main specification and Aggregate Reporting met deadline
- Failure Reporting document did not meet deadline

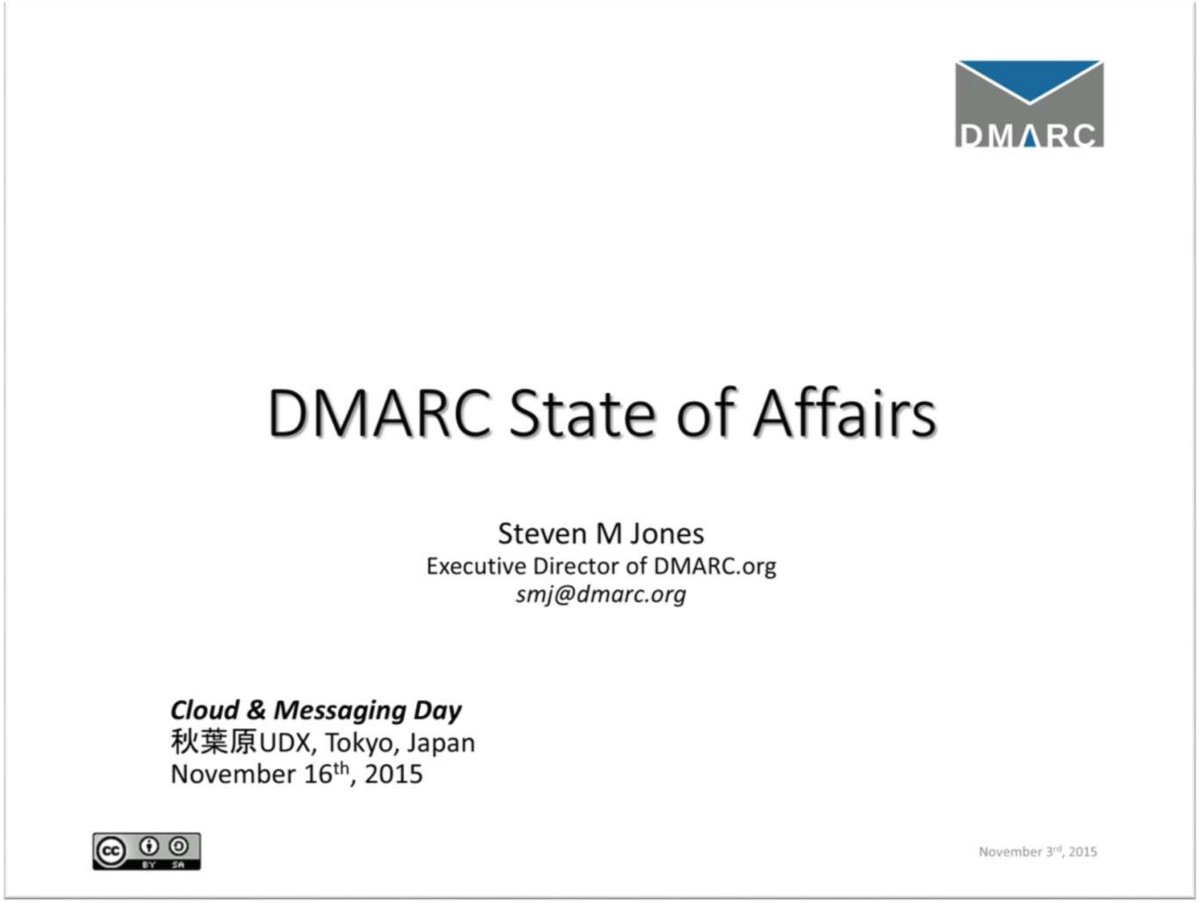
DMARC RFC is 10 Years Old

- Problem: DMARCbis and Aggregate Reporting reference the Failure Reporting document
  - Cannot proceed with “dangling references”
    1. Submit Failure Reporting and proceed, or
    2. Remove all references to Failure reporting
- Failure Reporting must be formally submitted to IESG
- Working Group Last Call scheduled to end 10月 23日
- Unclear if deadline is 11月 6日 or 12月 6日

Overview of DMARCbis Differences

- Informational ⇨ Standards Track (if approved)
- Public Suffix List replaced by DNS Tree Walk and PSD
- Several tags deprecated: `pct=`, `rf=`, `ri=`
- `np=` tag added for non-existent subdomain policy
- `psd=` tag brought from RFC 9091 (obsoleted)
- Report size limit notation removed from `rua=`
- DMARC SPF only uses `MAIL FROM:`, no fallback to `HELO`
- More guidance about PII/NPI risks in reporting

Final DMARC Update?



DMARC

DMARC State of Affairs

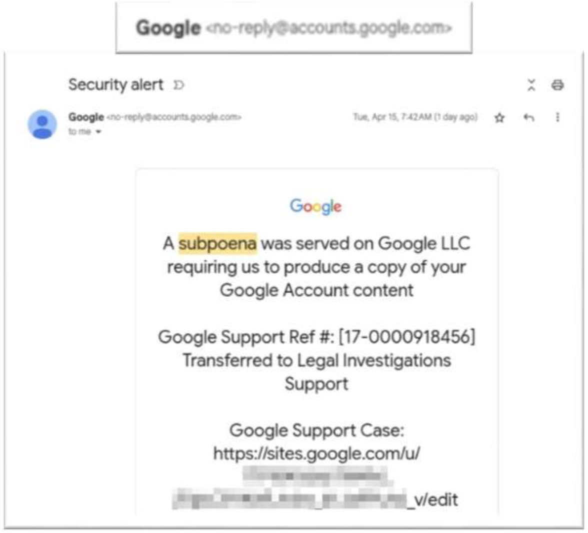
Steven M Jones
Executive Director of DMARC.org
smj@dmarc.org

Cloud & Messaging Day
秋葉原UDX, Tokyo, Japan
November 16th, 2015

DKIM Replay Attacks

DKIM Replay Attacks

- 2022: Proton Mail CTO blog post
  - Growing publicity about DKIM Replay
- 2023: DKIM Working Group reactivated
  - Google & Yahoo announcement
- 2024: Google & Yahoo enforcement
  - Attacks developing against Google
  - *Late 2024 – DKIM2 announced*
- 2025: PayPal Gift Address Campaign
  - Google Sites + OAuth App Campaign Publicized



Google <no-reply@accounts.google.com>

Security alert

Google <no-reply@accounts.google.com>
to me

Tue, Apr 15, 7:42 AM (1 day ago)

Google

A subpoena was served on Google LLC requiring us to produce a copy of your Google Account content

Google Support Ref #: [17-0000918456]
Transferred to Legal Investigations Support

Google Support Case:
https://sites.google.com/u/
[redacted]_v/edit

Source: X / @nicksdjohnson

What Is DKIM Replay?

Classic DKIM Replay:

- Take a message that was DKIM signed by the domain/company with good reputation
- Alter the message:
  - Change envelope recipient(s)
  - Alter unprotected header fields, body
    - Ex. Add body content if `l=` tag was used, or `Reply-To:` if header wasn't signed
- Resend the message to victims

DKIM Replay Evolved

- Setup/compromise sending account or domain
- Compose a message with spam/phishing content
- Send message to an account you control
- Change envelope addresses via forwarding or list
- Let forwarder/list re-send instead of renting botnet
  - Mailing list used in PayPal case
  - Microsoft Office 365 accounts are a popular vector
  - Combine multiple layers, final hop may pass simple SPF check

DKIM Replay Steps and Counters

Attack Steps

Access account/domain	Obtain signed message	Replay	Recipient Verifies
Multi-Factor Auth ATO detection Trial account limits	Time-limited signatures Unique key per service Rotate keys often	Track body hashes, duplicate Message-ID:	Monitor spikes in d= domain, selector or DKIM key used

Countermeasures

DKIM Replay Countermeasures

- Limit the time each DKIM key/signature is valid
  - More frequent DKIM key rotation
  - Use the `x=` tag (expiration time) in DKIM signatures
- Always sign `From:`, `To:` and `Cc:` headers even if empty
  - Sign as many headers as you reasonably can
  - Review all header signing – `Date:`, `Reply-To:`, `Subject:`, etc

DKIM Replay Countermeasures

- Content scan messages sent from new/trial accounts*
- Disallow pre-shortened links in messages, check for redirects
- Limit `To:` addresses for trial accounts
- Receivers: record DKIM body hash, signatures
  - Limit # of messages accepted using same hash or signature

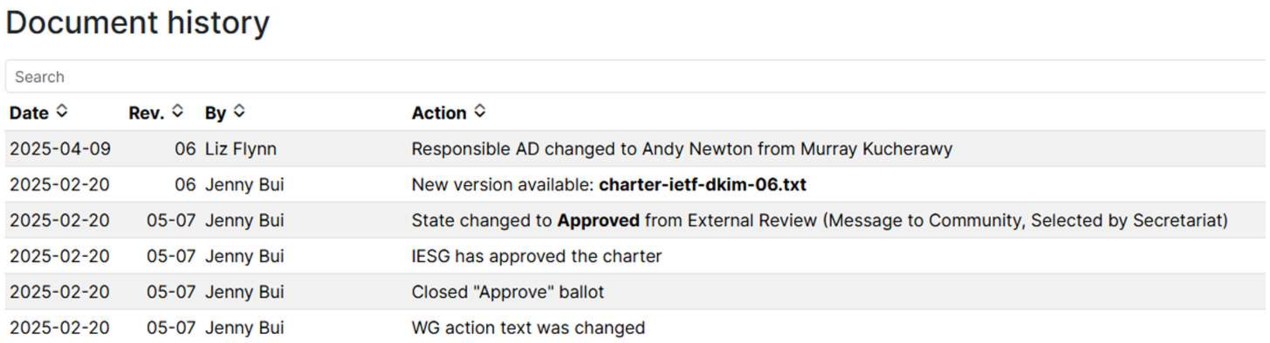
DKIM2 Since JPAAWG 7

Developments Since JPAAWG 7

- IETF Working Group Chartered
- Settled Scope And Direction
- Publishing Technical Documents
- Sessions At IETF Meetings

IETF Working Group Chartered

- DKIM Working Group had been re-chartered in 2023 for DKIM Replay work
- Re-chartering for DKIM2 began in 2025 1月
- Completed before IETF 122



Document history

Search

Date	Rev.	By	Action
2025-04-09	06	Liz Flynn	Responsible AD changed to Andy Newton from Murray Kucherawy
2025-02-20	06	Jenny Bui	New version available: **charter-ietf-dkim-06.txt**
2025-02-20	05-07	Jenny Bui	State changed to **Approved** from External Review (Message to Community, Selected by Secretariat)
2025-02-20	05-07	Jenny Bui	IESG has approved the charter
2025-02-20	05-07	Jenny Bui	Closed "Approve" ballot
2025-02-20	05-07	Jenny Bui	WG action text was changed

Settled Scope and Direction

- DKIM2 will be a brand new, stand-alone protocol and not a modification of DKIM
- Must not interfere with existing uses of DKIM
- Maintain compatibility with DKIM keys and DNS records
- Will include changes in bounce handling
- Will include a modification algebra to record message changes made by an intermediary

Publishing Technical Documents

- DKOR – include envelope addresses in DKIM signatures
- DKIM Differential Changes

- DKIM2 Motivation (adopted by WG)
- Header Definitions (adopted by WG)
- Message Examples
- Bounce Processing Procedures
- Feedback Reports (FBL)
- Modification Algebra
- DNS Record Specification

See https://datatracker.ietf.org/wg/dkim/documents/

Sessions At IETF Meetings

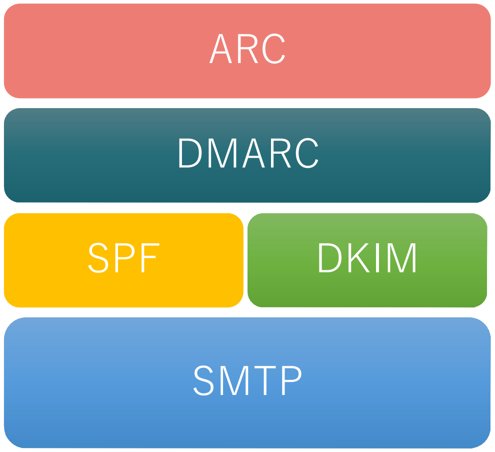
IETF 121	2024 11月	• Initial proposal
IETF 122	2025 3月	• Discussion of Motivations, Header Format, and Modification Algebra documents • Emphasis on producing a new protocol, but not disrupting existing ecosystem
IETF 123	2025 6月	• Activity on adopting Motivations and Header Format documents as WG documents • Debate of adoption/deployment timeline
IETF 124	2025 11月	• Hackathon: Building code to sign/validate samples • Whether to support multiple envelope recipients • Discuss Header Format and Modification Algebra documents

DKIM2

An Overview

Background for “DKIM2”

- Multiple protocols have been developed since 2002
- Each focused on a limited use case or scenario
- Patterns of use and abuse have changed over two decades
- Rather than add yet another layer, DKIM2 will try to cover the gaps with a new protocol



Goals for DKIM2

Three main goals for DKIM2:

- Prevent DKIM Replay-style attacks
- Prevent "back scatter" of bounce notifications
- Make message modifications reversible and auditable

Design Features of DKIM2

- Verifiable signatures at each hop that include all previous signatures (“chain of custody”)
- Include both envelope addresses in signatures
- (Cryptographic) “Algorithmic Dexterity”
  - Make it easy to change signing algorithms

Verifiable Signature At Each Hop

- Like ARC, all DKIM2 intermediaries will attach a cryptographic signature
- Each signature will include the envelope addresses (`MAIL FROM:`) and recipient (`RCPT TO:`)
- Captures where a message was redirected or forwarded at each step
- Include all non-trace headers in header hash, all body content in body hash – both hashes signed

Prevent DKIM Replay Attacks

- Because each signature includes the current envelope sender and recipient, it cannot be "replayed" by changing RCPT TO:
- Standardize which headers are signed, to eliminate opportunities to add/alter unsigned headers
- Verifiers encouraged to ignore signatures more than 14 days old

Prevent “Back Scatter” Bounces

- DSN/NDR will be sent back through the exact same sequence of hops that delivered it
- Relies on the envelope addresses included in each DKIM2 signature
- Remailers or forwarders could redact or hash addresses in DSN/NDR messages they send upstream, to protect privacy

Validate Modified Messages

- Each intermediary will record their changes to the message. This could include:
  - Header content (ex. “[External]” subject tag)
  - Body changes (ex. removed or added lines)
  - Entire removed MIME parts (ex. `b=` tag in the `DKIM2-Delta-Body:` header)
- Final recipient can validate the chain of signatures by reversing each modification

(Cryptographic) “Algorithmic Dexterity”

- DKIM2 allows for a second signature in the `DKIM2-Signature:` header
- Verifiers initially required to support RSA-SHA256 and Ed22519-SHA256
- Signers can include dual signatures during transitions
- Future updates can add/remove algorithms

Addressing The Goals

Prevent DKIM Replay-style attacks

- Substituting a different `RCPT TO:` will break signature
  - Cannot replay a captured message
  - If you sign to change `RCPT TO:`, your signature will fail or confirm your domain

Prevent "back scatter"

- Cannot use a domain you don’t control in `MAIL FROM:`, existing signature won’t validate

Make message modifications reversible and auditable

- Signature covers all message content and non-trace headers, so changes to content without a new signature invalidate message

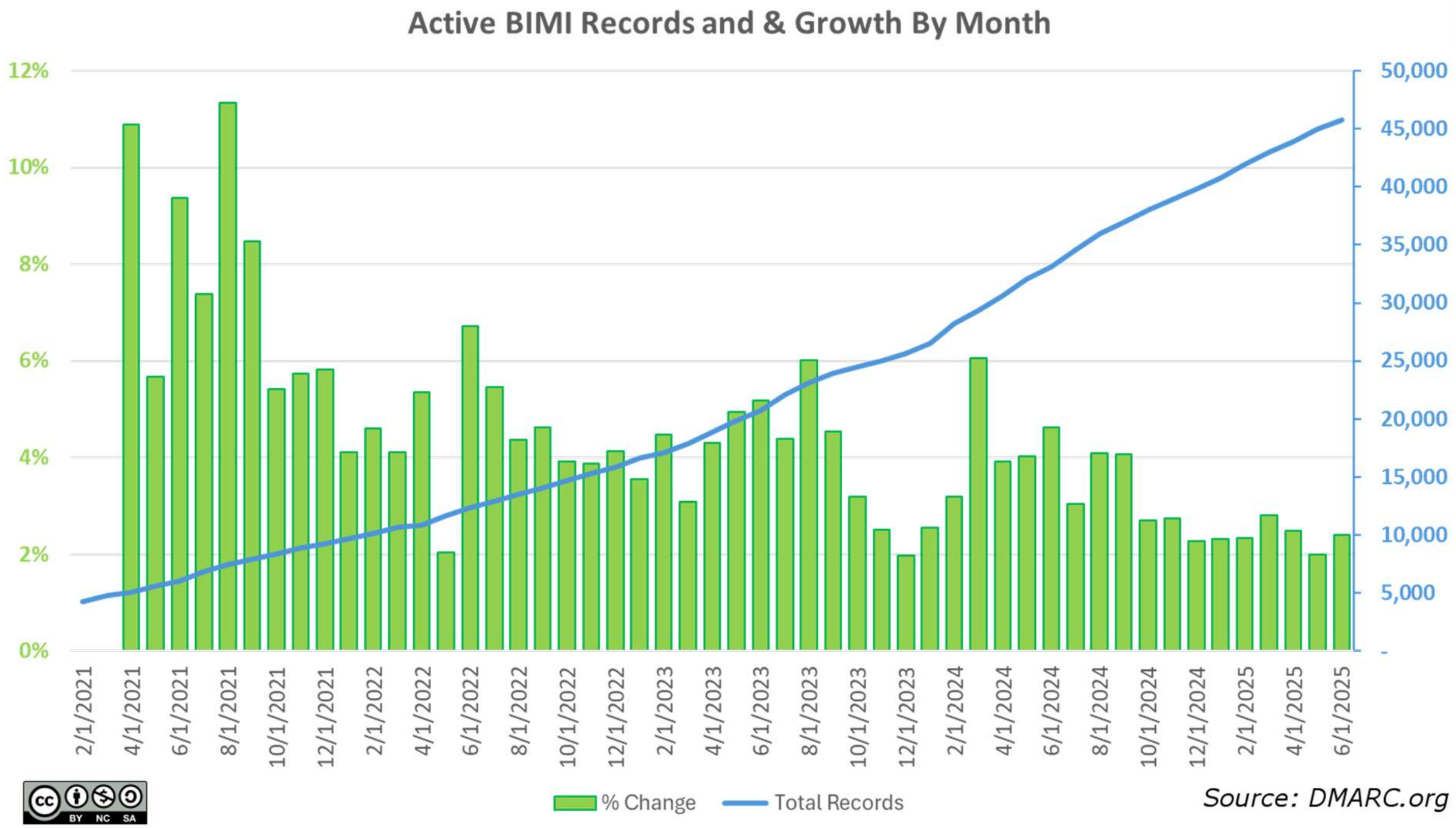
Impact And Implications

- Senders/intermediaries may need to “split the envelope”
  - Unclear if multiple RCPT TO: addresses will be supported
  - BCC and aliases/lists would create and sign individual messages
- Mailing lists and forwarders need to track changes made to each message and create a “MailVersion” header
- Likely to increase ATO activity, to access legitimate sending facilities/reputation

Impact And Implications

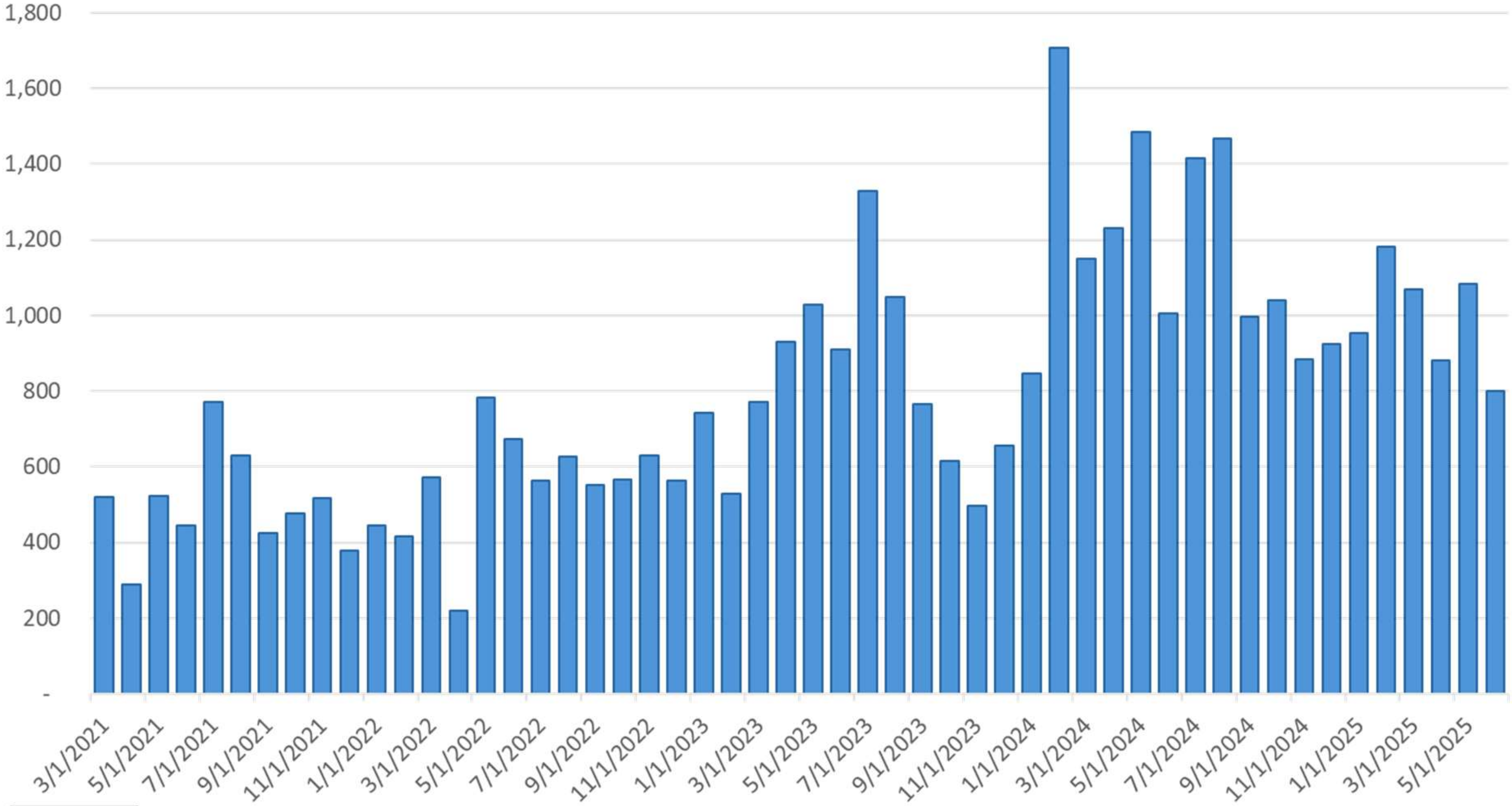
- Intermediaries will see bounced messages they handled
  - May request “feedback” about messages, but this feature has not yet been defined
- DKIM2 will co-exist with SPF, DKIM, DMARC, ARC
- “Large Operators” will “de-prioritize” message without valid DKIM2 signatures over time
- Implication that DKIM/ARC wouldn’t be needed

Statistics

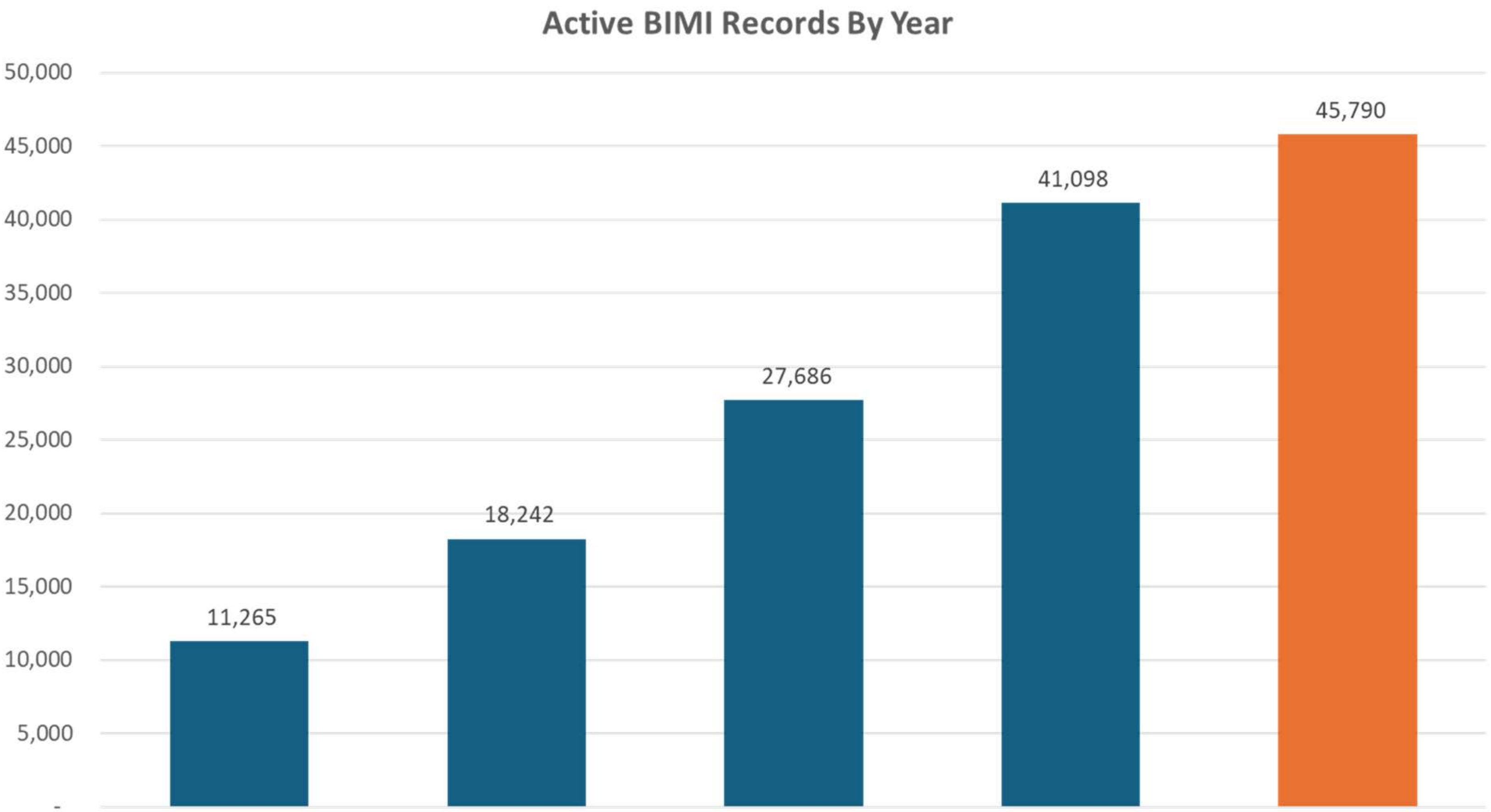


Source: DMARC.org

New BIMI Records By Month



Source: DMARC.org

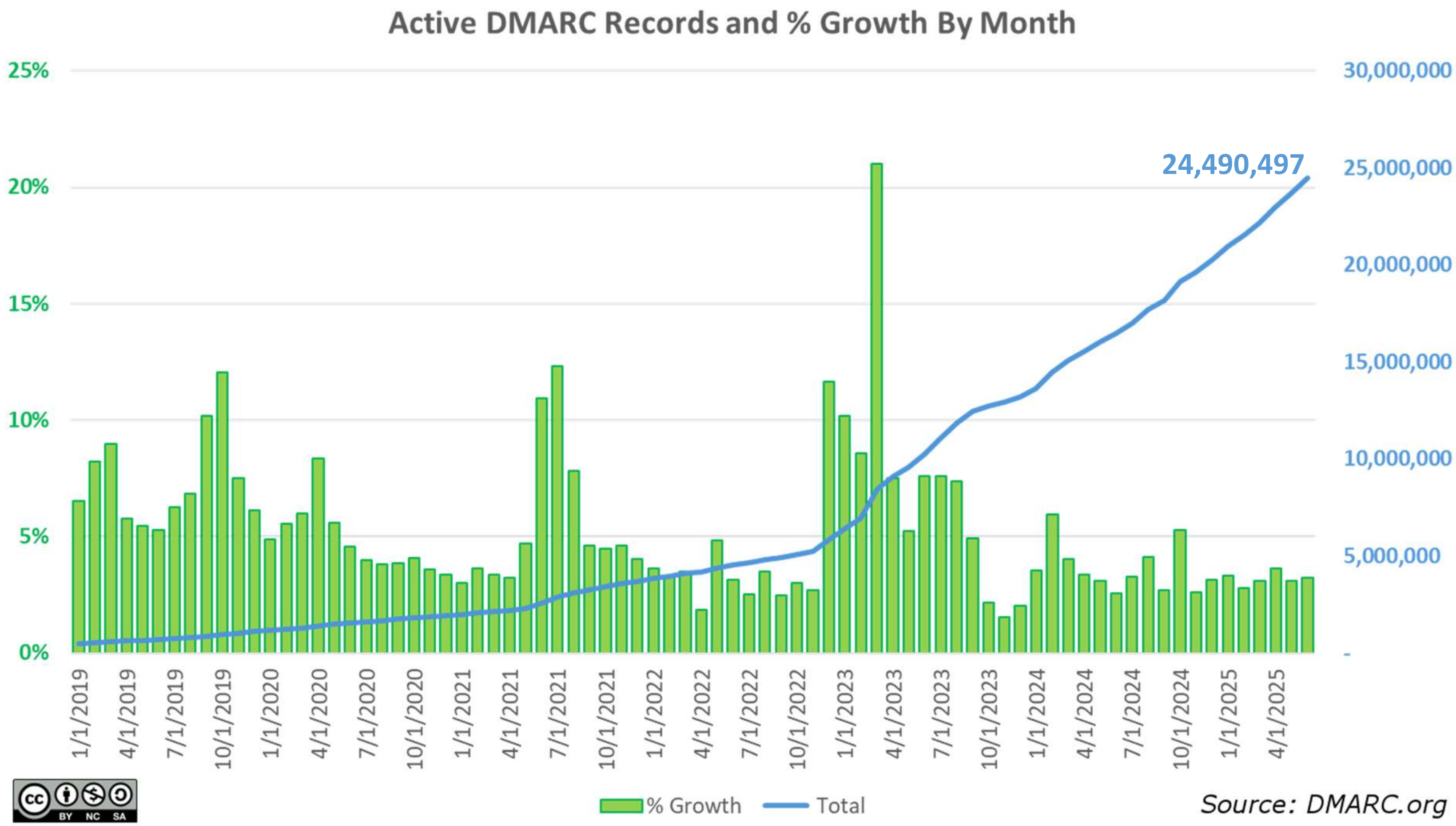


Source: DMARC.org

DKIM Algorithms For New Keys

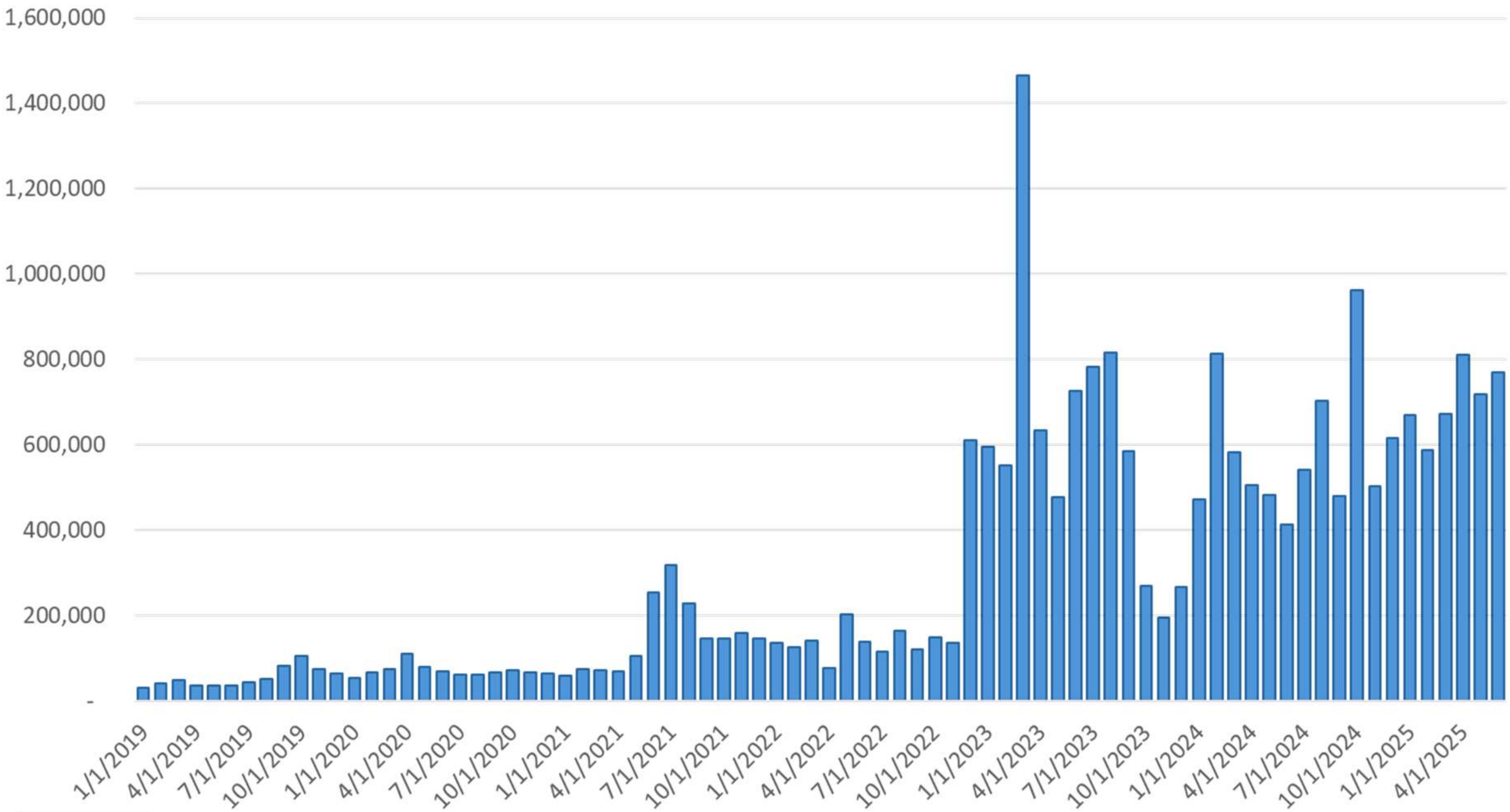
Are senders moving from RSA to elliptical curve (EC) algorithm for DKIM signing?

Year	EC Keys	RSA Keys
2021	2,108	9,752,141
2022	2,454	10,817,441
2023	126,735	12,001,226
2024	167,791	11,364,848
2025 Q2	120,421	7,480,250



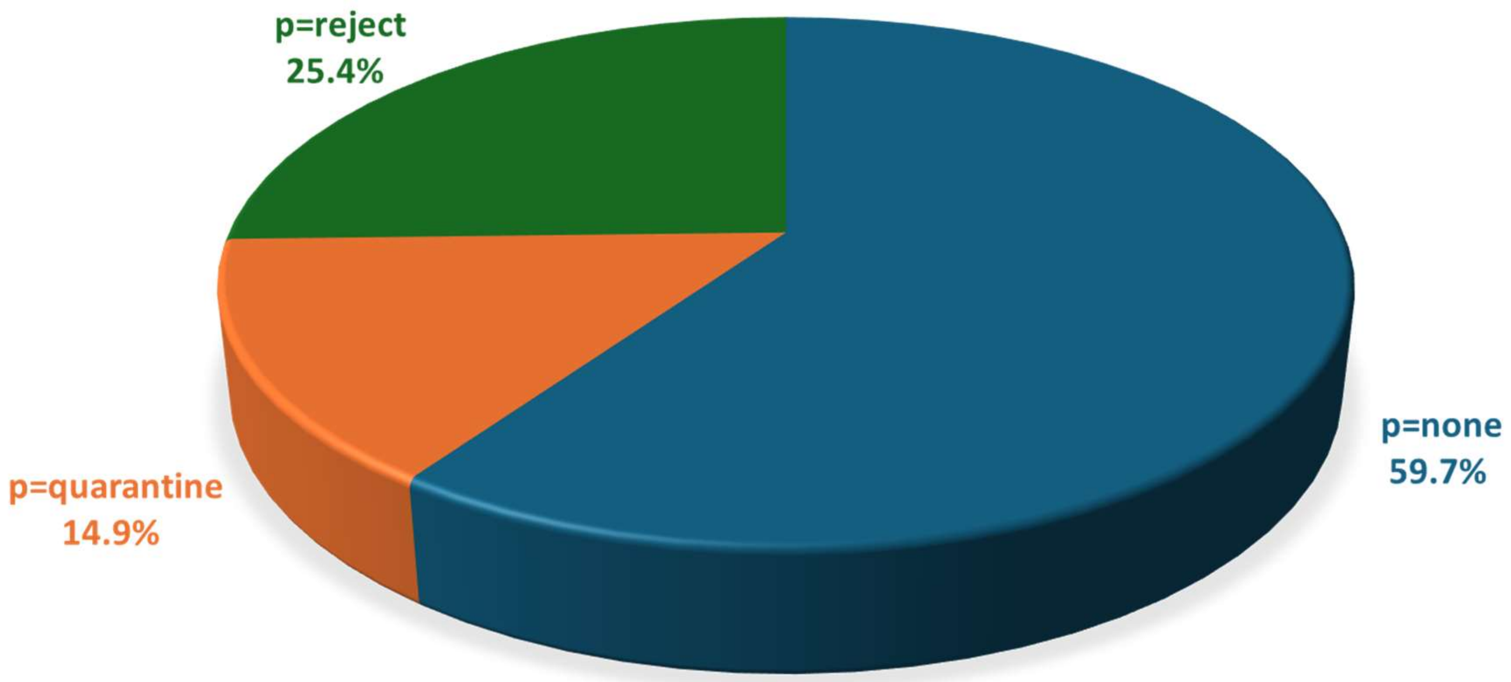
Source: DMARC.org

New DMARC Records By Month

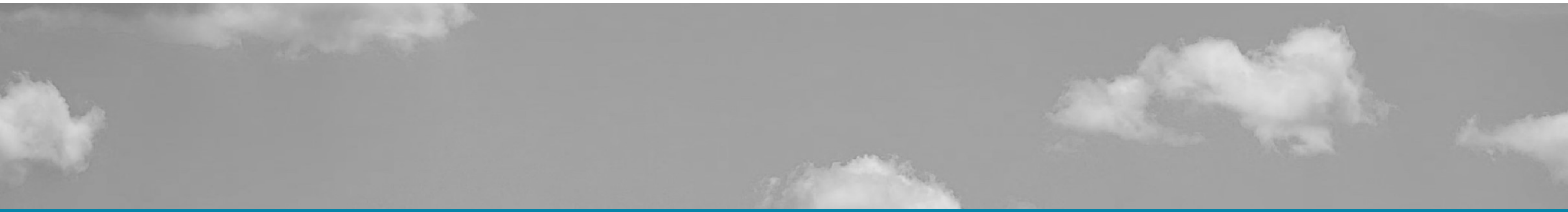


Source: DMARC.org

DMARC Policy Mix



Source: DMARC.org



ありがとうございます

Thank you