JP AAWG Japan Anti-Abuse Working Group

Email Authentication and Related Standards

DMARC.org and LinkedIn

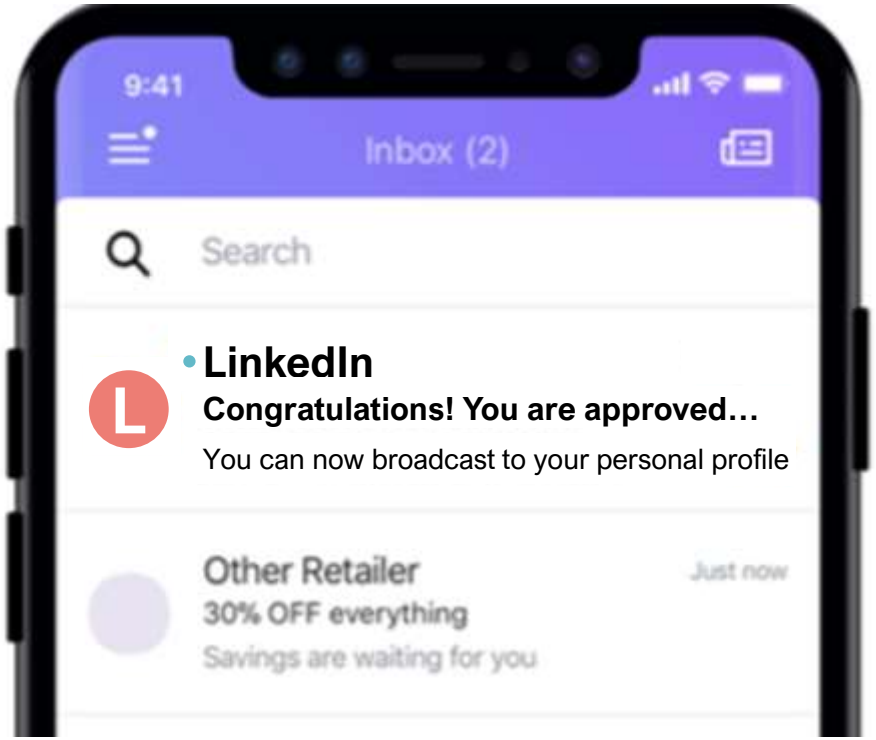
Steven M Jones

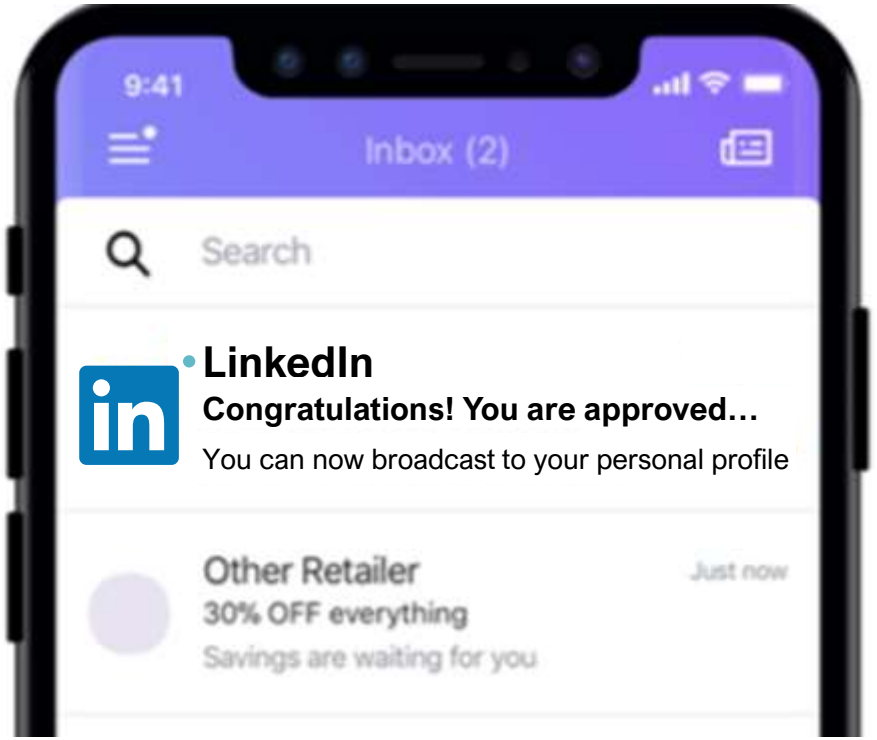
BIMI Background

JPAAWG

What Is BIMI?

Senders may have logos they control displayed with their messages





Origins of BIMI

- 2015: Microsoft and GMail both start to display logos in (mobile) mail programs
- Logos taken from various internal sources
- Neither company wants to manage other people's logos

- Working group proposed under DMARC.org
- Just like a `FAVICON.ICO` for email (at first)
- First meeting held at the M3AAWG 34 in Dublin on June 11th
- Standalone group created at the end of 2016

Requirements To Use BIMI

- Deploy DMARC with “quarantine” or “reject” policy
- Publish an additional BIMI record in DNS
- Publish SVG logo image on a web server

- For Google you must obtain a special X.509 certificate
  - Verified Mark Certificate (VMC)
  - Two vendors, DigiCert and Entrust Datacard (MVA)
  - Must submit proof of trademark ownership
  - Include link to VMC in BIMI DNS record

Where Is BIMI Today?

Supports BIMI	Considering BIMI	Does not support BIMI
yahoo!	1&1	
Aol. Netscape	mail.com GMX	
Google	BT	Microsoft
Gmail Google Workspace		Outlook Office 365
Fastmail	COMCAST	YAHOO! JAPAN
Pobox		
	SEZNAM.CZ	

Source: bimigroup.org

More Information About BIMI

- JPAAWG 4 Sessions:
  - A1-4 これから始めるBIMI
  - A2-4 電子メール認証技術最先端領域
  - B2-5 あなたの組織をなりすましから保護するための技術を紹介

- Other Resources:
  - BIMI Group – www.bimigroup.org
  - Wikipedia - en.wikipedia.org/wiki/Brand_Indicators_for_Message_Identification
  - Many helpful pages and videos from vendors, check YouTube and bimigroup.org/videos/

Other Developments

JPAAWG

DMARC Reporting

- Microsoft stopped sending aggregate reports in 2017
- Microsoft **resumed** sending aggregate reports mid-2021
  - Limited to Hotmail, Live.com, MSN.com, Outlook.com
- Some formatting issues (main body encoding, too-long lines)

- No timeline for reporting from Office 365

What Is ARC?

Authenticated Received Chain (ARC)

- When a message is forwarded, email authentication is frequently broken
- ARC allows the forwarder to convey the authentication results as they received the message
- Recipients of forwarded messages with ARC headers can see if the message passed authentication when the forwarder received it
- If forwarder has good reputation, receiver may choose to accept their authentication results

Who Is Using ARC?

- ARC sealing messages
  - Google Groups
  - Outlook.com
  - Office 365
  - Fastmail
  - Strato.com (European hosting company)

- Two companies validating ARC on incoming messages
  - Large customer management (CRM) company
  - German company: About 10% of messages that failed normal authentication checks are “recovered” by validating ARC

What Happened To TLS 1.3?

- TLS 1.2 and earlier are vulnerable

- What are the advantages of TLS 1.3?
  - Much faster initial handshakes – half the time, milliseconds/connection
  - More secure encryption algorithms
  - More resistant to Man-In-The-Middle attacks

- Fairly good adoption due to CDNs, service providers
- Still need to fallback for consumers, small organizations

- Need to encourage adoption – see Open Round Table #1

IETF Activity

JPAAWG

DMARC Working Group News

- DMARC policies for Public Suffix Domains (PSD) published as RFC9091 in July 2021
  - United States published policy for **`.gov`** TLD in October
  - United Kingdom published policy for **`gov.uk`**
  - No data shared yet, maybe at M3AAWG 54 (February)

- No traction for `Author:` and `Sender:` drafts from 2020
  - Both addressed `From:` rewriting by mailing lists

Agenda for DMARC at IETF 112

- Methods to locate a domain's DMARC policy
  - How to find the Organizational Domain (OD)
  - RFC7489 references the Public Suffix List (PSL) from Mozilla
  - Proposal to move OD discovery to a separate document
  - Proposal to simplify OD discovery by doing more DNS lookups ("walk the tree")
- Some proposals related to indirect mail flows (mailing lists) and ARC may be discussed

EmailCore Working Group

- Developing updates to RFC5321 and RFC5322
- Proposal to make these features mandatory:
  - 8BITMIME [RFC 6152]
  - Enhanced Reply Codes [RFC 5248]
  - Delivery Status Notification (DSN) [RFC 3461]
- Proposal to make these features strongly recommended:
  - PIPELINING [RFC 2920]
  - SMTPUTF8 [RFC 6531]

JMAP Working Group

- JSON Meta Application Protocol (JMAP)
- Access and synchronize email, calendar, contacts

- A number of RFCs published since 2019
  - RFC 8620 JMAP core
  - RFC 8621 JMAP for mail
  - RFC 8887 and RFC 9007

- Working on multiple documents at IETF 112
  - S/MIME (encrypted/signed message) support
  - Calendar, Task, and Contact objects

Adoption and Usage

JPAAWG

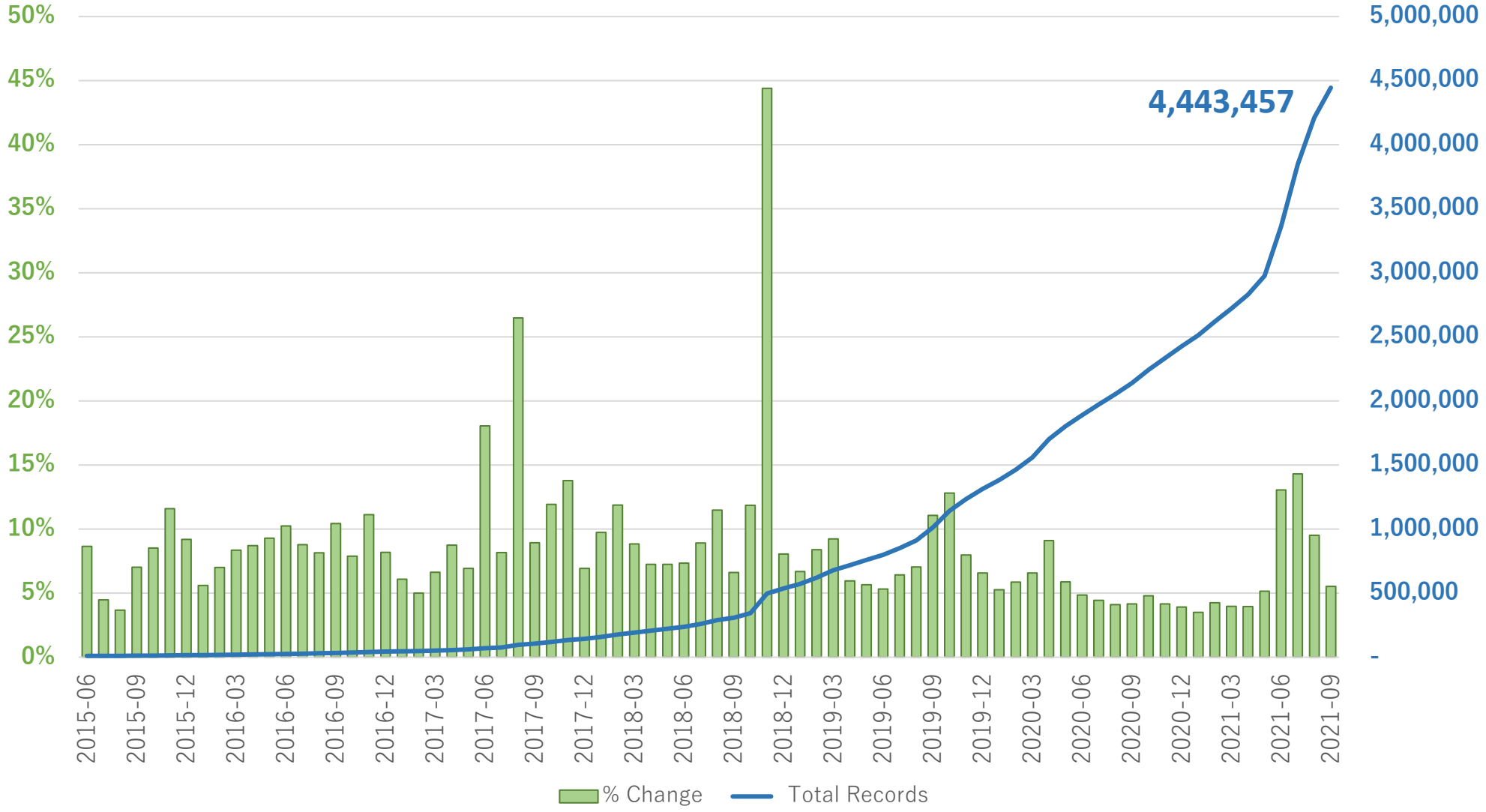
About This Data

- Raw data supplied by Farsight Security
- DNS request/response data captured from sensors widely deployed across the Internet
- Not 100% coverage of Internet, but a stable sensor network useful for comparisons over time
- DMARC.org thanks Farsight for their continuing support

FARSIGHT SECURITY

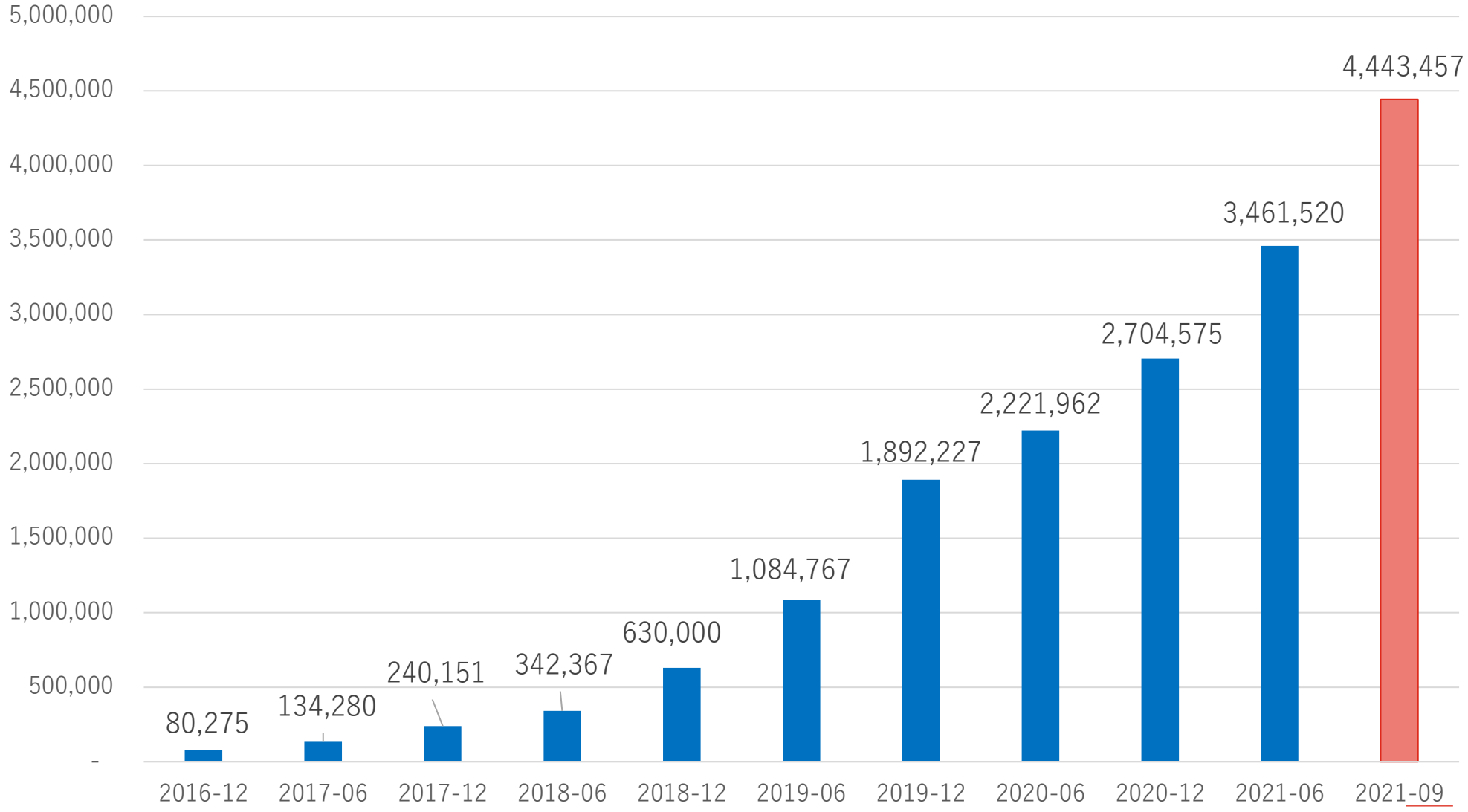
JP AAWG

Active DMARC Records and % Growth By Month



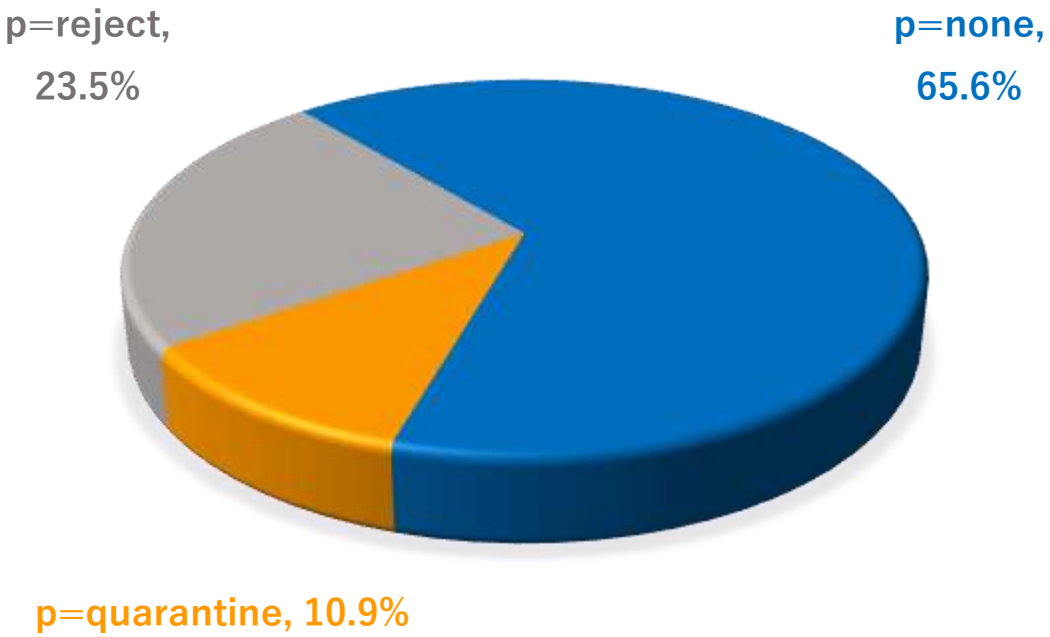
JPAAWG

Total Active DMARC Records By Period

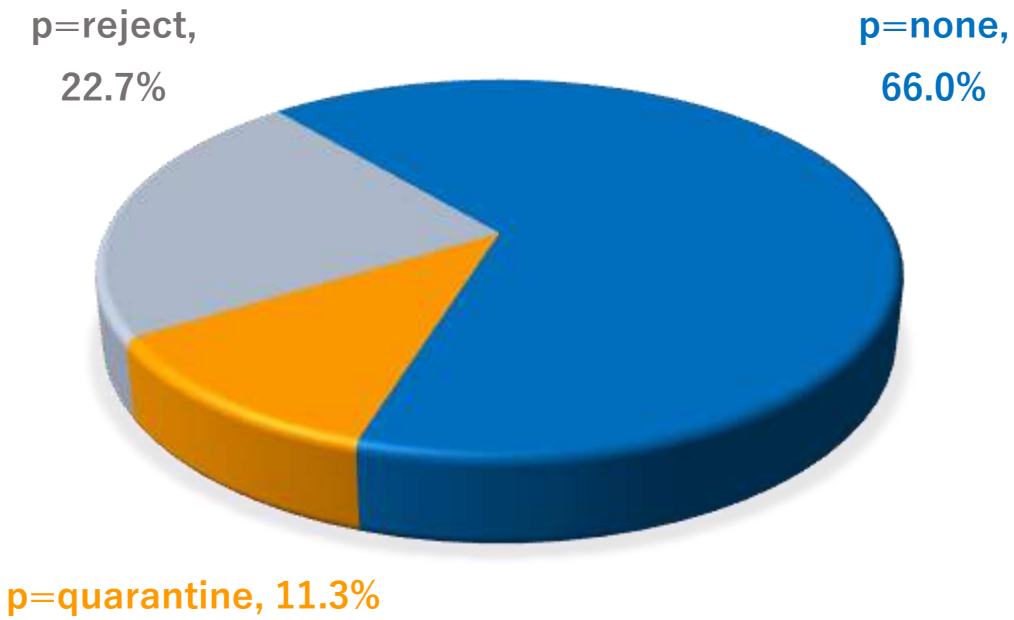


JPAAWG

DMARC Policies

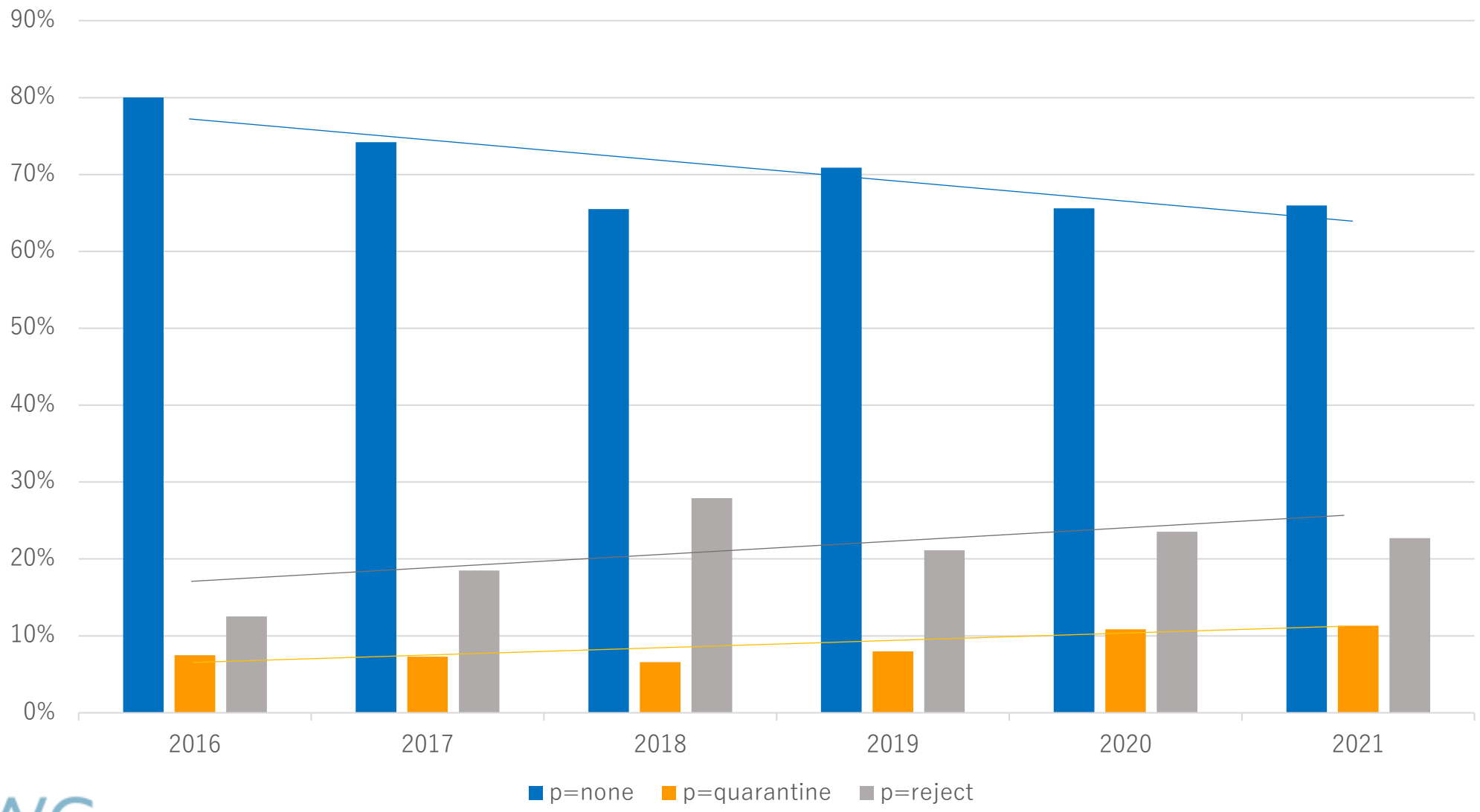


2020-12



2021-09

DMARC Policies By Year



JPAAWG

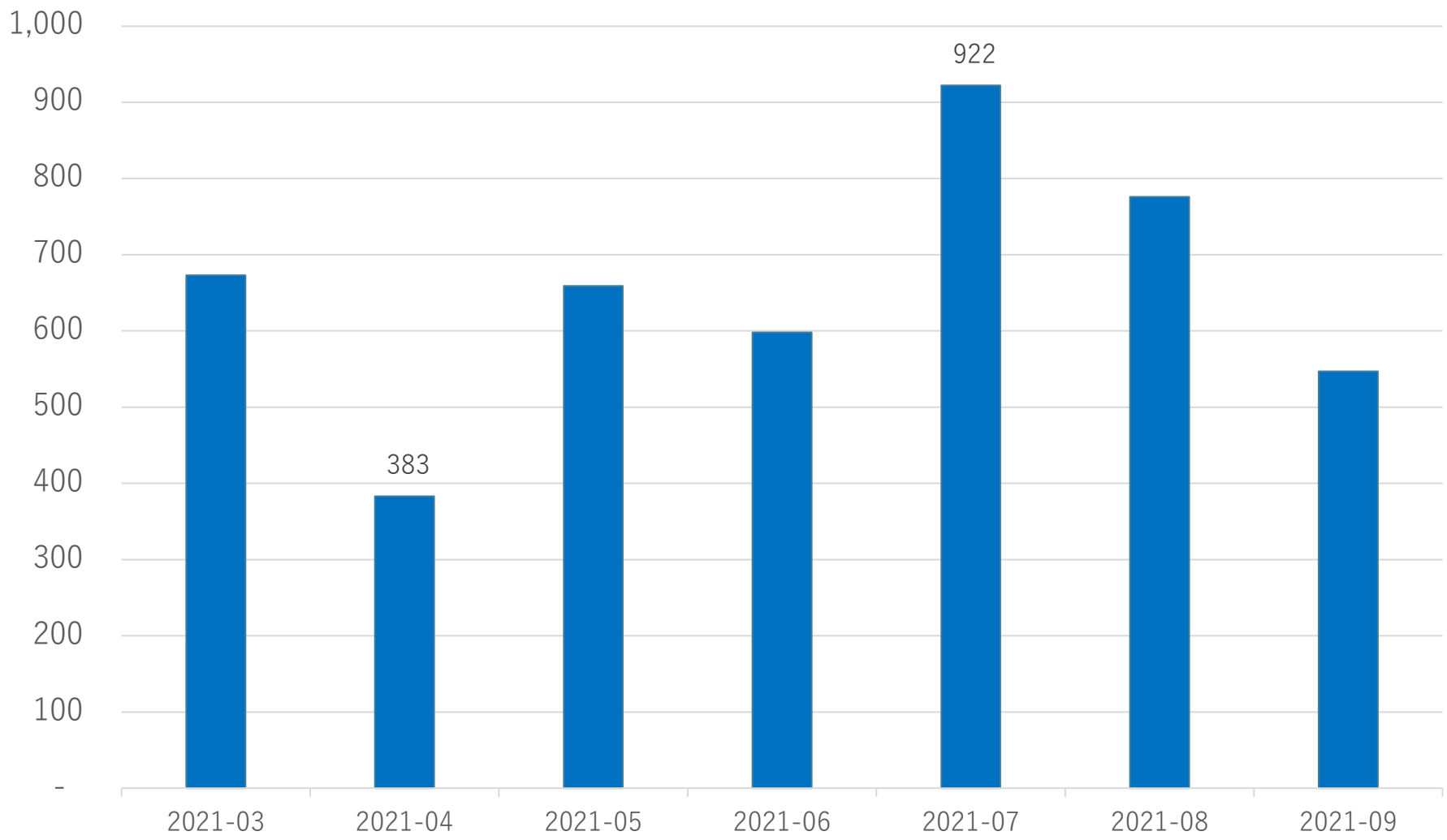
Active BIMI Records

- Total BIMI records observed: **9,860**
- Including link to a VMC: **179**
- Many large brands with a VMC:

JPMorgan Chase & Co.

18 records

Monthly New BIMI Records



JPAAWG

DKIM Signing Algorithms

- DKIM specified with RSA signature algorithm (2007)
- RFC 8463 (2018) describes Elliptic Curve algorithm for DKIM signatures (Ed25519-SHA256)
- Common problem with DKIM deployment:
  DNS TXT record too long for vendor's GUI
- Smaller keys provide equivalent strength against brute force attack
- Room to scale keys against quantum computing attacks

RSA Key vs. Ed25519 Key

- DKIM key record for 2,048 bit RSA key

```
test._domainkey.football.example.com. IN TXT (
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDkHlOQoBTzWR”
"iGs5V6NpP3idY6Wk08a5qhdR6wy5bdOKb2jLQiY/J16JYi0Qvx/byYzCNb3W91y3FutAC”
"DfzwQ/BC/e/8uBsCR+yz1Lxj+PL6lHvqMKrM3rG4hstT5QjvHO9PzoxZyVYLzBfO2EeC3”
"Ip3G+2kryOTIKT+l/K4w3QIDAQAB” )
```

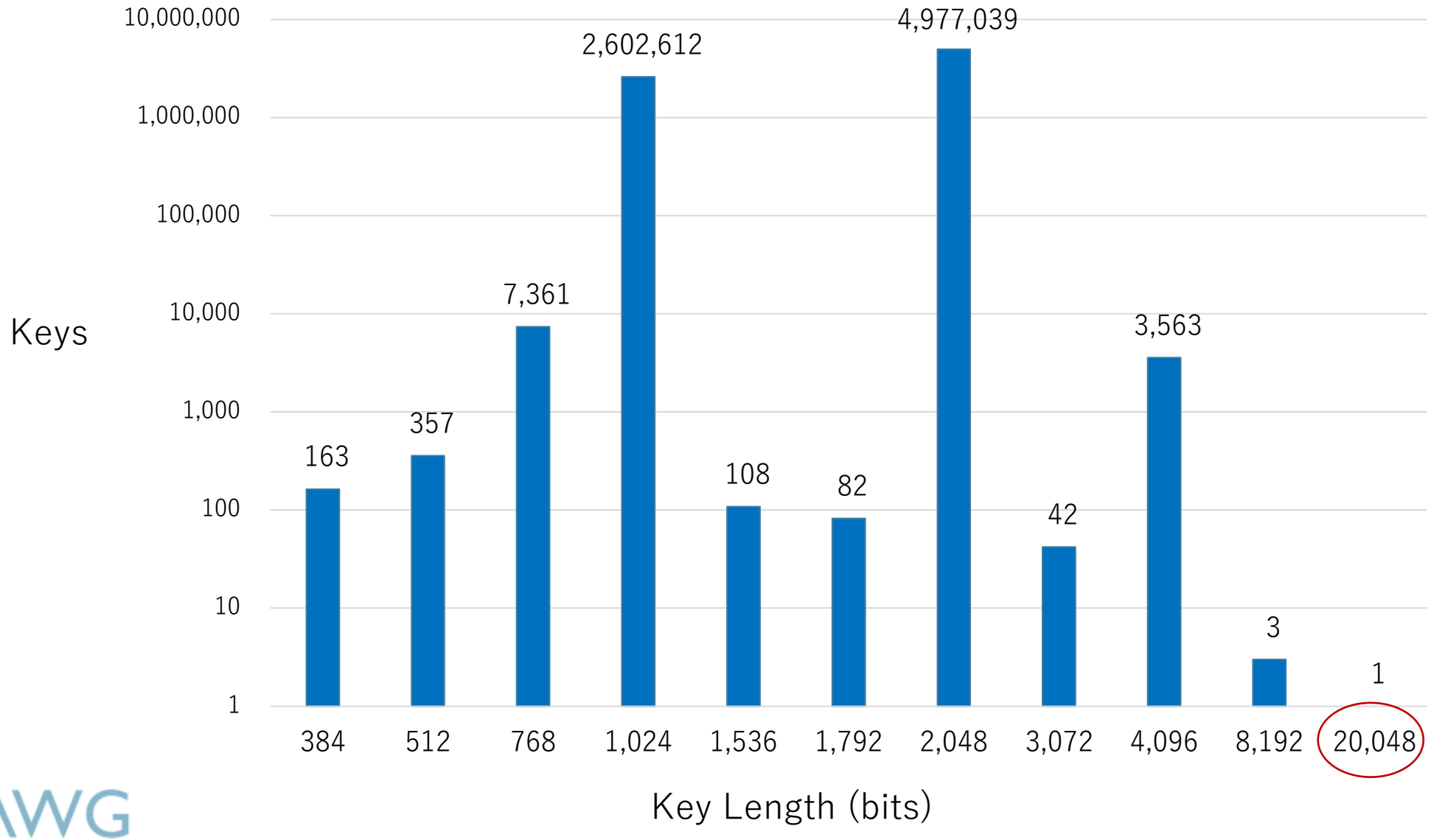
- DKIM key record for 256 bit Ed25519 key

```
brisbane._domainkey.football.example.com. IN TXT (
"v=DKIM1; k=ed25519; p=11qYAYKxCrfVS/7TyWQHOg7hcvPapiMlrwIaaPcHURo=” )
```

How Common Is Ed25519?

- Ed25519 keys: 1,775 (2,019 since 2018)
- RSA keys: 7,699,768 (38+MM since 2010)
- Answer: Not very common (yet)
- Why so few Ed25519 keys after three years?
  - Missing software support? Upgrades needed?
  - How many domains use an ESP's keys and software?
  - Perhaps promote Ed25519 with TLS 1.3 upgrade?

DKIM RSA Key Lengths (2021)



JPAAWG

Thank you