JP AAWG Japan Anti-Abuse Working Group

# IETF Standards Update

**Keynote A1-2, 11月 5日**

DMARC.org

Steven Jones



# IETF Areas

- Domain Connect WG (dconn)
- DMARC WG (dmarc)
- Email Core Specifications WG (emailcore)
- Mail Maintenance WG (mailmaint)
- Structured Email WG (sml)
- TLS WG (tls)
- Using TLS in Applications WG (uta)
- SMTP Mailing List (smtp)

JPAAWG

2

Not covering the following:

- DKIM WG (dkim)
- JMAP WG (jmap)

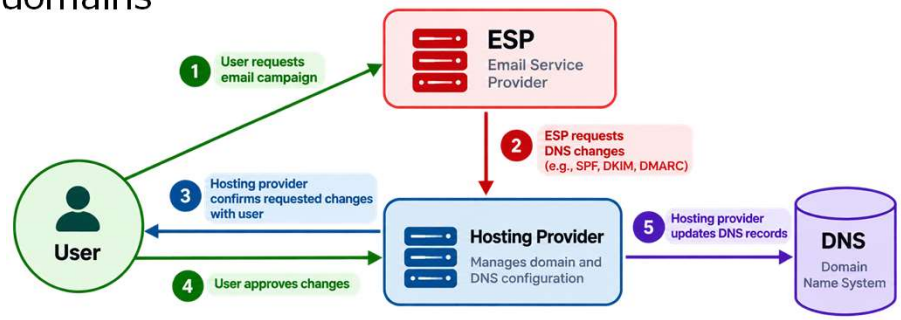



# Domain Connect Working Group

# Domain Connect WG

Standardize *Domain Connect Protocol* – enables service providers to request provisioning of DNS records by domain registrars and hosting providers on behalf of customers

- Reduce broken and mis-formatted DNS entries for small senders/domains




JPAAWG

# Domain Connect WG

- Domain Connect Protocol - DNS provisioning between Services and DNS Providers
  - `https://datatracker.ietf.org/doc/draft-ietf-dconn-domainconnect/`
- Domain Connect Protocol - Asynchronous Flow Extension
  - Splits the OAuth 2.0 flow from the base specification
  - `https://datatracker.ietf.org/doc/draft-ietf-dconn-domainconnect-async/`
- See also `https://domainconnect.org`

JPAAWG

5

Former M3AAWG initiative, “Simplifying DNS Management”




# DMARC Working Group

# DMARC WG

- Three core specifications have been published

- RFC 9989 – DMARC Base Specification
- RFC 9990 – DMARC Aggregate Reporting
- RFC 9991 – DMARC Failure Reporting




JPAAWG

8

- https://datatracker.ietf.org/doc/rfc9989/ - Core specification
- https://datatracker.ietf.org/doc/rfc9990/ - Aggregate reporting
- https://datatracker.ietf.org/doc/rfc9989/ - Failure reporting

# DMARC WG – ARC Status

- WG re-chartered to consider moving ARC to “historical” (currently “experimental”)
  - `https://datatracker.ietf.org/doc/draft-ietf-dmarc-arc-to-historic/`
  - Nobody collecting/publishing experimental data
- Proponents feel it should be “historical” to discourage new deployments
- Opponents feel it should be left alone until a replacement, like DKIM2, is ready to deploy

# DMARC WG: Section 7.4

- Certain mandates to go to “p=reject” policy
- RFC9989, Section 7.4 describes several ways that real-world mail usage is more complicated than “yes/no” rules
  - Example: Section 7.4 quotes RFC7960, saying you “SHOULD NOT” adopt “p=reject” if domain users submit messages to mailing lists
- An RFC must address the general case in limited space
- You must make implementation decisions based on your real-world use cases and adapt

JPAAWG

10

"Interoperability Issues between Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Indirect Email Flows" [RFC7960]
- https://datatracker.ietf.org/doc/rfc7960/

- Adapt:
  - Provide a sub-domain for users subscribing/posting to mailing lists
  - Limit mailing list participation to those lists that implement address rewriting, ARC, etc.
- Highlights the importance of having experienced staff, good vendors, attending JPAAWG/M3AAWG,  etc.

# DMARC WG: DMARCbis Differences

- Informational ⇨ Standards Track
- 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
- 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


JPAAWG
Emailcore
Working Group

# Emailcore WG

*Applicability Statement* for IETF Core Email Protocols

- An overview of extensions, protocols, and uses added or changed since 2008 publication of RFC 5321 and 5322
- Guidance for implementors to keep email useful and relevant on the modern Internet
  - Address syntax, encoding, and group syntax
  - Internationalization: addresses, domains, and content
  - Email authentication
  - Encryption
  - Privacy and confidentiality

JPAAWG

13

Applicability Statement – https://datatracker.ietf.org/doc/draft-ietf-emailcore-as/

# Emailcore WG

## Simple Mail Transfer Protocol – RFC 5321bis

- Publication pending Applicability Statement
- Clarified distinctions between Message Submission Agents (MSA) and Mail Transfer Agents (MTA)
- Corrections for reported errata
- Removed text related to source routing

JPAAWG

14

RFC 5321bis - https://datatracker.ietf.org/doc/draft-ietf-emailcore-rfc5321bis/
RFC 5322bis - https://datatracker.ietf.org/doc/draft-ietf-emailcore-rfc5322bis/

# Emailcore WG

Internet Message Format– RFC 5322bis

- Publication pending Applicability Statement
- Corrections for reported errata, many around ABNF
- Clarified “trace header” description
- Rewrote “Bcc:” description and security considerations

JPAAWG

15

RFC 5321bis - https://datatracker.ietf.org/doc/draft-ietf-emailcore-rfc5321bis/
RFC 5322bis - https://datatracker.ietf.org/doc/draft-ietf-emailcore-rfc5322bis/


MAILMAINT
Working Group
JPAAWG

# Mail Maintenance WG

## RFCs Published

- RFC 9979 – Further IMAP/JMAP Keywords and Mailbox Attributes
- RFC 10022 – IMAP UIDBATCHES Extension
- RFC 10080 – Updated use of `Expires:` Header In Email
  - Author says message “loses validity after” a date
  - MUA may choose not to display (or discard) message after this date

JPAAWG

17

RFC 9979 – Document certain message/mailbox attributes already in-use
- https://datatracker.ietf.org/doc/rfc9979

RFC 10022 – IMAP UIDBATCHES – client requests batches of N messages to operate on
- https://datatracker.ietf.org/doc/rfc10022

RFC 10080 – define/allow Expires: header to be used by author and MUA/recipient
- https://datatracker.ietf.org/doc/rfc10080/

Reminds me of RFC 7293 – Require Recipient Valid Since - https://www.rfc-editor.org/rfc/rfc7293.html

# Mail Maintenance WG

Discussions / Work Items

- Aggregate Performance Reporting (APRF)
  - Report up to four aggregated headers, given in DNS record in `d=` domain
  - Report target based on selector in DKIM signature
- MTA Hooks – A `milter` alternative for scanning, filtering, etc
  - `mtahooks` mailing list created, session scheduled for IETF 127
  - Will probably become a Working Group
- PACC – Automatic configuration of Email, Calendar, and Contacts
  - Pull configuration data from well-known addresses based on email domain

JPAAWG

18

APRF - https://datatracker.ietf.org/doc/draft-ietf-mailmaint-aprf/
MTA Hooks – https://datatracker.ietf.org/doc/html/draft-degennaro-mta-hooks
 - mailing list: https://mailarchive.ietf.org/arch/browse/mtahooks/
PACC - https://datatracker.ietf.org/doc/draft-ietf-mailmaint-pacc/
SMTPUTF8 - https://datatracker.ietf.org/doc/draft-ietf-mailmaint-smtputf8-syntax/


Structured Email
Working Group
JPAAWG

# Structured Email WG

- Mailbox and mail application providers automatically extract details from (transactional) email messages
- Schema.org started defining structured data formats for web and email content around 2011
- The Structured Email Working Group will produce a comprehensive, open, and extensible specification starting from the Schema.org formats

JP AAWG

20

This is how your iPhone or Android phone checks email and populates your calendar automatically

# Structured Email WG

- Multiple revisions to developing base specification
  - `draft-ietf-sml-structured-email-06`
- Added a trust/security document
  - `draft-ietf-sml-trust-01`
- Added a “quoted content” document to standardize quoted text from messages in a thread
  - `draft-ietf-sml-structured-quoted-content-00`

JPAAWG

21

Base spec - https://datatracker.ietf.org/doc/draft-ietf-sml-structured-email/
Trust/security - https://datatracker.ietf.org/doc/draft-ietf-sml-trust/
Quoted content - https://datatracker.ietf.org/doc/draft-ietf-sml-structured-quoted-content/


TLS Working Group
JPAAWG

# Transport Layer Security WG

Most activity around Post-Quantum Cryptography (PQC)

- Nothing specific to email and TLS
- However, all TLS use cases must be updated to meet PQC recommendations – including email

# Transport Layer Security WG

https://datatracker.ietf.org/wg/tls/documents/

Notable RFCs:

- RFC 9846 – Transport Layer Security (TLS) Version 1.3
- RFC 9849 – TLS Encrypted Client Hello
- RFC 9851 – TLS 1.2 is in Feature Freeze
- RFC 10015 – Deprecating Obsolete Key Exchange Methods in TLS 1.2 and DTLS 1.2
- RFC 10024 – Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3

JPAAWG

24

12 RFCs published in the last year!
RFC 9846 - Updated TLS 1.3 - https://datatracker.ietf.org/doc/rfc9846/
RFC 9849 - Encrypted Client Hello – encrypt the Server Name Indicator during initial handshake
- https://datatracker.ietf.org/doc/rfc9849/
RFC 9851 – TLS 1.2 feature freeze - https://datatracker.ietf.org/doc/rfc9851/
RFC 10015 – Deprecate KEM in TLS 1.2 - https://datatracker.ietf.org/doc/rfc10015/
RFC 10024 - PQ/T Hybrid Key - https://datatracker.ietf.org/doc/rfc10024/

# Transport Layer Security WG

Pending Publication:

- Use of ML-DSA in TLS 1.3
  - How to use post-quantum signature scheme ML-DSA (FIPS 204)
- ML-KEM Post-Quantum Key Agreement for TLS 1.3
  - Defines three ML-KEM NamedGroups for use in PQC key exchange
  - ML-KEM-512, ML-KEM-768, and ML-KEM-1024

JPAAWG

25

ML-DSA - https://datatracker.ietf.org/doc/draft-ietf-tls-mldsa/
ML-KEM - https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/


Using TLS in Apps
Working Group
JPAAWG

# Using TLS in Apps WG

Charter:

- Coordinate use of TLS to secure Internet communications
- Update minimums for existing applications using TLS
- Promote use of TLS by new applications and services

# Using TLS in Apps WG

Publications:

- RFC 9852 – New Protocols Must Require TLS 1.3
  - Best Current Practice document
- TLS/DTLS 1.3 Profiles for the Internet of Things (IoT)
  - Proposed Standard, awaiting publication as an RFC
- Post-Quantum Cryptography Recommendations for TLS-based Applications
  - Draft currently under development by WG
  - https://datatracker.ietf.org/doc/draft-ietf-uta-pqc-app/

JP AAWG

28

RFC 9852 - New Protocols Using TLS Must Require TLS 1.3 - https://datatracker.ietf.org/doc/rfc9852/
TLS 1.3 Profiles for IoT - https://datatracker.ietf.org/doc/draft-ietf-uta-tls13-iot-profile/
PQC Recommendations for TLS - https://datatracker.ietf.org/doc/draft-ietf-uta-pqc-app/


SMTP Mailing List
JPAAWG

# SMTP Mailing List

- SMTP “interest” mailing list without a working group
- Questions and suggestions are shared and discussed
- Sometimes suggestions become proposals for a specific WG, or lead to the creation of a new project or WG

JPAAWG

# SMTP Mailing List

- MTA Hooks – led to new mailing list, see MAILMAINT
- Consent Upon Recipient Engagement – CURE
  - Mechanism to allow mailbox providers to enforce recipient consent
  - Uses RFC 5322 headers, token shared when user replies
- SAMP – SMTP Address Migration Protocol
  - Proposed SMTP response code (“350 Address Migrated”)
  - Response code “251” exists, not really used

JPAAWG

31

MTA Hooks – https://datatracker.ietf.org/doc/html/draft-degennaro-mta-hooks
 - mailing list: https://mailarchive.ietf.org/arch/browse/mtahooks/
CURE, draft-cure-core - https://datatracker.ietf.org/doc/draft-cure-core/
SAMP – message thread https://mailarchive.ietf.org/arch/msg/ietf-smtp/9Cv40jGdNPN_zv9OoCYtN04aqlw/
 - draft: https://mailarchive.ietf.org/arch/msg/ietf-smtp/9Cv40jGdNPN_zv9OoCYtN04aqlw/4/


ありがとうございます
Thank you