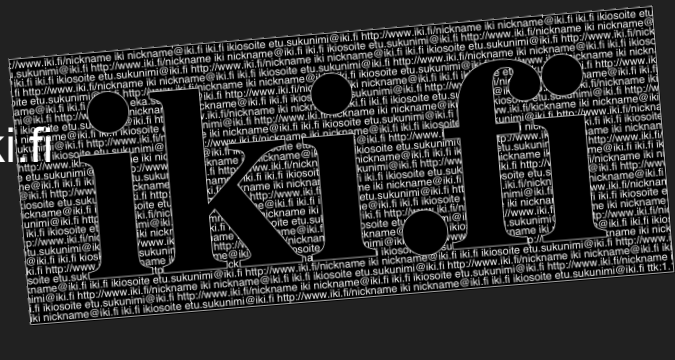
State of Email Today

nog.fi 2024-06-06

Hannu.Aronsson@iki.fi
Chair, Internet Users Forever iki.fi



iki.fi Internet Users Forever

The Internet Users Forever IKI is a non-profit society since 1995 which provides its 30.000 members, private individuals in mostly Finland, **permanent iki.fi-addresses** with e-mail and WWW forwarding (IKI **does not host** the web pages or offer internet services, it just forwards the addresses).

This allows our members to **keep the same personal identity** should the actual location or ISP of their e-mail or www homepages change.

Email “fun”

Good news

Spam, junk email filtering

- Spam volume not really growing
- Filtering tools work quite well
- Major issue today is spammy transactional emails (tickets, password resets) not getting to users

Bad news

Email is major entry point for malware, ransomware into organizations

Worse news

Phishing getting a lot “better”

- Spear phishing customized with AI
- BEC Business Email Compromise

Credential theft (session cookies)

- Insert emails directly into users inbox bypassing all email filtering

Bonus: Smishing, SMS phishing

SPF “Sender Policy Framework”

Sender

- List outgoing email server IP addresses in DNS
  - Cloud IP addresses could include spammer IPs
- Do not use -all but ~all

outlook.com. 300 IN TXT "v=spf1
include:spf-a.outlook.com ip4:157.55.9.128/25
include:spf.protection.outlook.com
include:spf-a.hotmail.com ~all"

Receiver

- Compare SMTP connection source IP address with DNS SPF record
- If match, pass
- If not match, use -all ~all ?all +all setting
- Not compatible with indirect email routes (forwarding, mailing lists, etc)
  - SRS (Sender Rewriting Scheme) hack doesn’t solve problem, breaks DMARC
- Some places block with SPF only (bad policy)

DKIM “DomainKeys Identified Mail”

Sending

- Sign key headers and content with your public key
  - Hint: oversign key headers to protect against replay attacks changing headers

```
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed; d=iki.fi; s=meesny; t=1716319820;
h=from:from:reply-to:subject:subject:date:date:messag
e-id:message-id:to:to:cc:mime-version:mime-version:c
ontent-type:content-type;bh=xq[...]zU8=;b=DIpi[...]kjo=
```

- Provide public key in DNS record

```
meesny._domainkey.iki.fi. 3600 IN TXT "v=DKIM1;
k=rsa; " "p=MIGf[...]QAB"
```

Receiver email server

- Verify signature with data from domain DNS
- If match, email confirmed to be from the specific domain

DMARC “Domain-based Message Authentication, Reporting and Conformance”

Sender

- Provide DMARC policy in DNS TXT

example.com 3600 IN TXT "v=DMARC1;p=none;sp=quarantine;rua=mailto:dmarcreports@example.com;"

- DKIM sign outgoing email
- Use reasonable SPF settings

Receiver email server

- Check DKIM and SPF
- If either passes, DMARC is pass
  - Expecially you should accept if DKIM passes but SPF fails
- If not pass, look at DMARC policy
  - What to do with message (none, quarantine, reject)
- Can report deliverability statistics back to sender

ARC “Authenticated Received Chain”

Forwarder

- Check DKIM and SPF from incoming connection, append ARC data

ARC-Seal: i=1; s=mail; d=iki.fi; t=1716320489; a=rsa-sha256; cv=none; b=mtF[...]Xg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=iki.fi; s=mail; t=1716320489; h=from:from:[...]:dkim-signature; bh=dvrH[...]Dw==
ARC-Authentication-Results: i=1; MTA-v6; dkim=pass header.d=gmail.com; dmarc=pass (policy=none) header.from=gmail.com; spf=pass (domain of REDACTED@gmail.com designates 2a00:1450:4864:20::233 as permitted sender)

mail._domainkey.iki.fi. 3600 IN TXT "v=DKIM1; k=rsa; "
"p=MIIB[...]QAB"

Receiver email server

- Check ARC headers
- Trust some ARC signers
  - Use your own allowlist
  - Allow your users to provide trusted ARC signer domains (their trusted forwarding services)
- Accept test results from trusted ARC chain

Moderate to hard

Email Best Practises: Sending Email

Follow best practises to get your email delivered reliably.

- Avoid using SPF only
  - Use reasonable SPF settings e.g. ~all not -all
- DKIM sign outgoing email
- Use DMARC
  - Use reasonable DMARC policy, not p=reject
- Use DNSSEC to secure domain-based email info (DNS TXT records)

Think about sending servers IP address space reputation management

- E.g. separate your own email from customer servers

Email Best Practises: Mailbox Provider (receiving)

- Do not block with SPF alone
  - Do not consider SPF -all a blocking failure
- Use DMARC and DKIM
- Use ARC information
- Prefer domain not IP address based reputation systems
- Help your users help you to receive their important transactional and time sensitive emails
  - Some transactional email is somewhat spammy (e.g. airline emails with EVERYTHING IN CAPITALS)
  - Prefer quarantine to blocking, so users can find their important messages
  - Provide user input to reputation system e.g. trusted ARC signers for their email

Email Best Practises: Intermediaries

A lot of real email is being forwarded

- University alumni
- Members of professional organisations
- Forwarding services
- User-configured forwarding
- Hosted domains email addresses
- … and more

Mailing lists (different case as they often want to change content)

Intermediaries need to be careful

- Do not break DKIM signatures
  - Don’t change email content or existing headers
- Add ARC signature
- Spam filter and tag forwarded email
- Use separate IP addresses for forwarding to preserve your originating email IP reputation
- SPF SRS (Sender Rewriting Scheme) doesn’t really help
  - it changes envelope sender which breaks DMARC address alignment

The BIG Players in Email

Google and Microsoft along with a few others manage a huge part of internet email today. Many individuals on Gmail. Many companies outsource to Microsoft services.

Works great most o the time, but senders need to adjust to what they seem to require. Recommended DMARC and DKIM and ARC does work well, additional reason to do it.

A lot of spam today comes from the big players' services and AWS etc. and has valid email signatures etc.

Email Security

Keeping email secure in transit: STARTTLS by default

- Has been great improvement against passive traffic capture on backbone networks

Fully securing email end-to-end (S-MIME, PGP)

- Not gaining popularity, too hard to use, problem getting keys for addresses easily

Verifying email is coming from the domain it claims

- Multiple solutions aim to prevent spoofing
  - But a lot of email is totally valid but from “nordae.com”
  - Many Mail apps only show name, not address/domain:
    Your Secure Bank <spammer@hijacked.domain>
- Does not prove email is or is not spam
  - Spammers send from their own domain, with all valid information for that domain

Maintaining Email Infrastructure

Linux default email servers are pretty OK

- Turn on DKIM and DMARC
- Enable a spam filter (e.g. rspamd)

Commercial email servers with support and fancy features available

Outsourcing organization/domain email to Google or Microsoft is easy, but

- Can be hard to get support
- Limited customization
- Free users are the product, not customers

You will need someone to manage email

- Set up stable solution and let it run
- Avoid daily tuning with “quick fixes” — lots of unintended consequences

Does create support load

- Help users help themselves, e.g. search quarantine for “lost emails” instead of blocked and lost
- Allow users to add their own trusted ARC domains

Email related organisations and groups

IETF (Internet Engineering Task Force)

- Main email standard RFCs, message formats, SMTP protocol, DMARC, ARC, DKIM, SPF, …
- Current example: DMARCbis group working on next version 2.0 of DMARC
- New Mail Maintenance group: https://datatracker.ietf.org/wg/mailmaint/about/
- Free to join and participate remotely or in (low cost) conferences
- Recommendation: Join the most relevant group email lists and follow them

M3AAWG (Messaging, Mobile, Malware Anti-Abuse Working Group)

- Sharing experiences, issues and solutions between email senders, mailbox and other messaging providers
- Best Current Practice documents
- 3 annual conferences, 2 US/Canada, 1 Europe
- Paid membership, worth considering if you work with email (or SMS or similar)

Not standards, proprietary

- SRS (hack for SPF)

Summary

Email is the ultimate example of open standards working for a long time

- With backwards compatibility all the way back — think old broken webcam picture emails

Email is still the base everything else falls back on

- Password resets, reach everyone, unique user identifier, all devices

Future features with growing support

- EAI (Email Address Internationalization) Ääkkösiä.Tässä@example.com
- BIMI (Brand Indicators for Message Identification) show logo next to your emails (DNS TXT point to CA signed SVG)
- DMARC 2.0 update ongoing in IETF

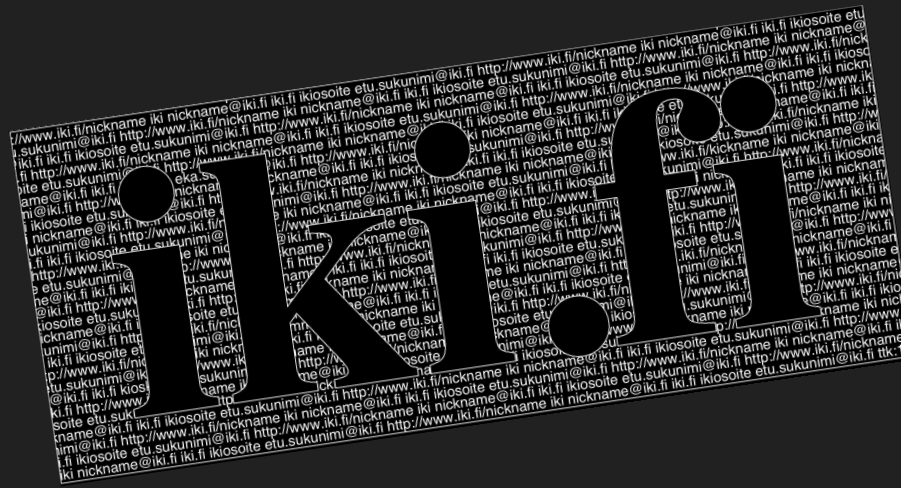
Email is here to stay … forever!

Thank you & Discussion

KEEP CALM
AND
USE EMAIL

Hannu.Aronsson@iki.fi
Mobile +358 40 500 6242
iki-hallitus@iki.fi
(remember iki is volunteers)

iki.fi Internet Users Forever



Started in 1995

Non-profit in Finland

Permanent internet identity = email address

- Email forwarding
- Web forwarding, iki domains, etc.

≈30.000 members, mostly from Finland

Active in internet advocacy and email standardisation

Only joining fee, no annual fee

See more at www.iki.fi and useful information at ikiwiki.iki.fi