# IT LOOKS RIGHT, BUT...

I’ve checked everything but my mail still isn’t authenticated.

Or not authenticated everywhere. Or not authenticated all the time.

# THINGS THAT BREAK

# WHAT IS THIS?

- Authentication failure epics
- DKIM was broken
- SPF was broken

# HOW DO WE KNOW?

# HOW DO WE KNOW?

- Sometimes it’s obvious
- Often it isn’t

# AUTHENTICATION-RESULTS

**Authentication-Results: mx.google.com;**
**dkim=pass header.i=@blighty.com header.s=blueberry header.b=gc24D4ut;**
**spf=pass (google.com: domain of steve@blighty.com designates 2a00:1098:88:f6::1 as permitted sender) smtp.mailfrom=steve@blighty.com**

spf=pass
spf=none
spf=fail

dkim=pass
dkim=neutral
dkim=fail
dkim=permerror

# DMARC REPORTS

- DMARC overview reports
  - Ten thousand foot view
  - Only if DKIM and SPF fail
- DMARC forensic reports
  - “fo=1” reports SPF or DKIM fails
  - Less widely supported

# HOW DOES DKIM FAIL?

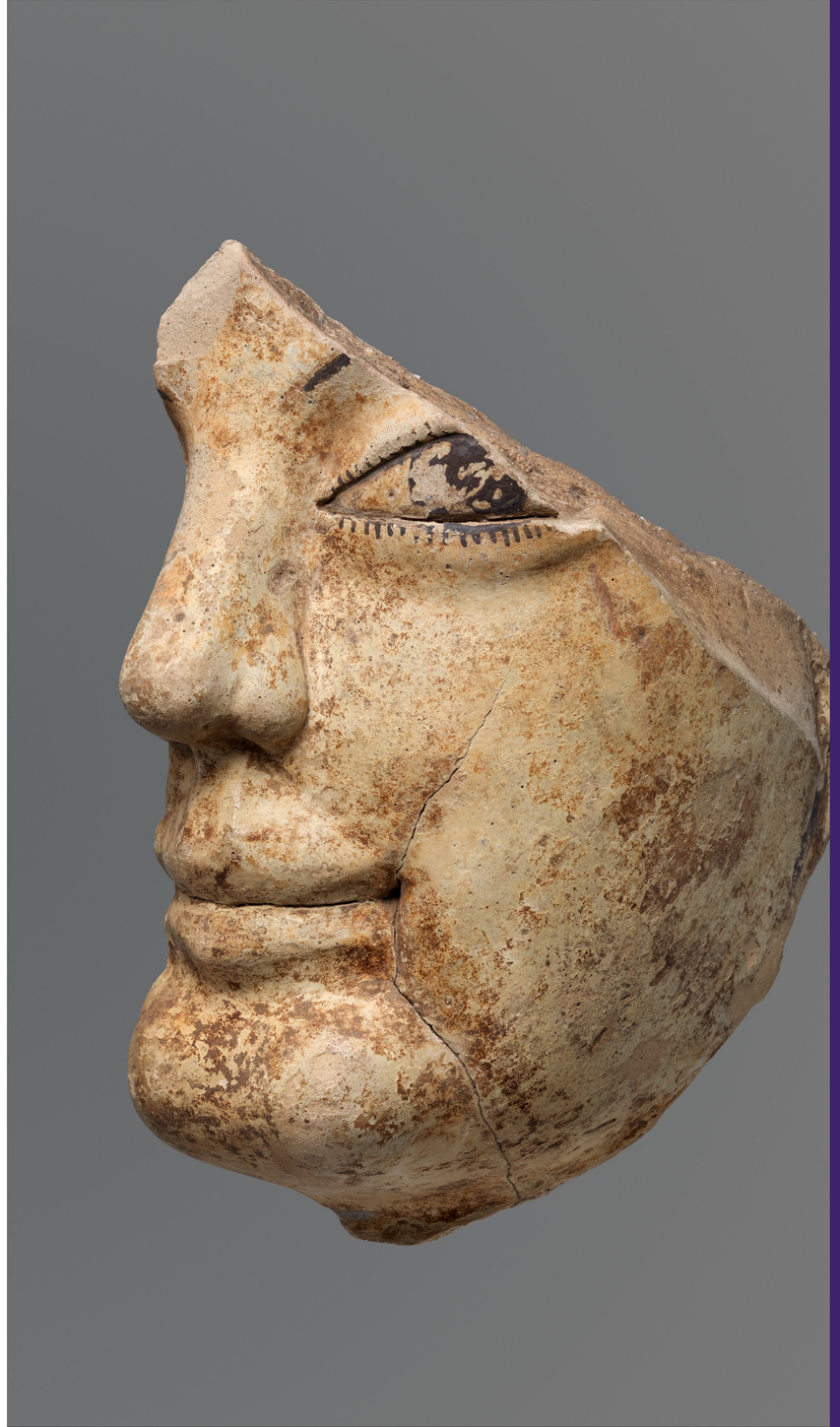
# HOW DOES DKIM WORK?

- Hash the sent email body
- Hash the sent email headers
- Sign hashes with a private key

- Get public key from DNS
- Hash the received email body
- Hash the received email headers
- Check the signature

# AND HOW DOES IT FAIL?

- Signing or public key misconfigured
- Body was modified
- Headers were modified
- DNS lookup of public key failed
- Something else



# A SERIES OF UNFORTUNATE EVENTS

Things going wrong. So many things.

# DON’T LET THEM TYPE IT IN

# DON’T LET THEM TYPE IT IN

**Authentication-Results: dkim=permerror (no key for signature)**

```
dig testing2._domainkey.blighty.com txt

testing2._domainkey.blighty.com. 3600 IN TXT “v=DKIM1; k=rsa; p=MIIBojANBgkqhkiG9w0BAQEFAAOCAY8
AMIIBigKCAYEArvXR29IqEb0HLXc4Zfgmt+bMyZwNC2PTuCjPqICG2ELeYZU6ooqVoC15IltwGB/rw2PVMta1JYY9
USD/s6VDuacnU2NpwFrPvVii1Vl6Ywf8Jyb/FVcyVLps2Tz8VRNpHVinqXzg1rSV787EW60iPsGPER9YNO
x4lUoQzC7xKyXwCgxTJziDdyvG8Yrtn7SN…
```

# DON’T LET THEM TYPE IT IN

**Public key as published in DNS:**

testing2._domainkey.blighty.com. 3600 IN TXT “v=DKIM1; k=rsa; p=MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEArvXR29IqEb0HLXc4Zfgmt+bMyZwNC2PTuCjPqICG2ELeYZU6ooqVoC15IltwGB/rw2PVMta1JYY9USD/s6VDuacnU2NpwFrPvVii1Vl6Ywf8Jyb/FVcyVLps2Tz8VRNpHVinqXzg1rSV787EW60iPsGPER9YNOx4lUoQzC7xKyXwCgxTJziDdyvG8Yrtn7SN…

**Public key as provided to the customer:**

testing2._domainkey.blighty.com. 3600 IN TXT “v=DKIM1; k=rsa; p=MIIBojANBgkqhkiG9wOBAQEFAAOCAY8AMIIBigKCAYEArvXR29IqEb0HLXc4Zfgmt+bMyZwNC2PTuCjPqICG2ELeYZU6ooqVoC15IltwGB/rw2PVMta1JYY9USD/s6VDuacnU2NpwFrPvVii1Vl6Ywf8Jyb/FVcyVLps2Tz8VRNpHVinqXzg1rSV787EW60iPsGPER9YNo x4lUoQzC7xKyXwCgxTJziDdyvG8Yrtn7SN…

# DON’T LET THEM TYPE IT IN

- DKIM public keys aren’t user-friendly
- Use CNAMEs rather than TXT records if you possibly can
- Describe the process of adding DNS with “copy and paste”
- Maybe use tools rather than eyeballs to compare things

# QUOTES ARE HARD

# QUOTES ARE HARD

- A TXT record holds multiple strings
- Each string can’t be bigger than 255 characters
- DKIM keys need several strings
- The standard format for a TXT record has each string surrounded by double quotes

"v=DKIM1; k=rsa; p=MIIBojANBgkqhkiG9w” “0BAQEFAAOCAY8AMIIBigKCAYEA” “rvXR29IqEb0HLXc4Zfgmt+bMy”

- Web interfaces to DNS servers don’t handle this format well

# QUOTES ARE HARD

Pasting this string into your hosting company or registrar DNS interface…

"v=DKIM1; k=rsa; p=MIIBojANBgkqhkiG9w” “0BAQEFAAOCAY8AMIIBigKCAYEA” “rvXR29IqEb0HLXc4Zfgmt+bMy”

…might put this record into DNS.

"v=DKIM1; k=rsa; p=MIIBojANBgkqhkiG9w\” \“0BAQEFAAOCAY8AMIIBigKCAYEA\” \“rvXR29IqEb0HLXc4Zfgmt+bMy”

# QUOTES ARE HARD

- Use CNAMES pointing at ESP hosted TXT records. Really.
- If you see a backslash in a published DKIM key this is your problem

# FOLDING HEADERS

Part 1

# FOLDING HEADERS

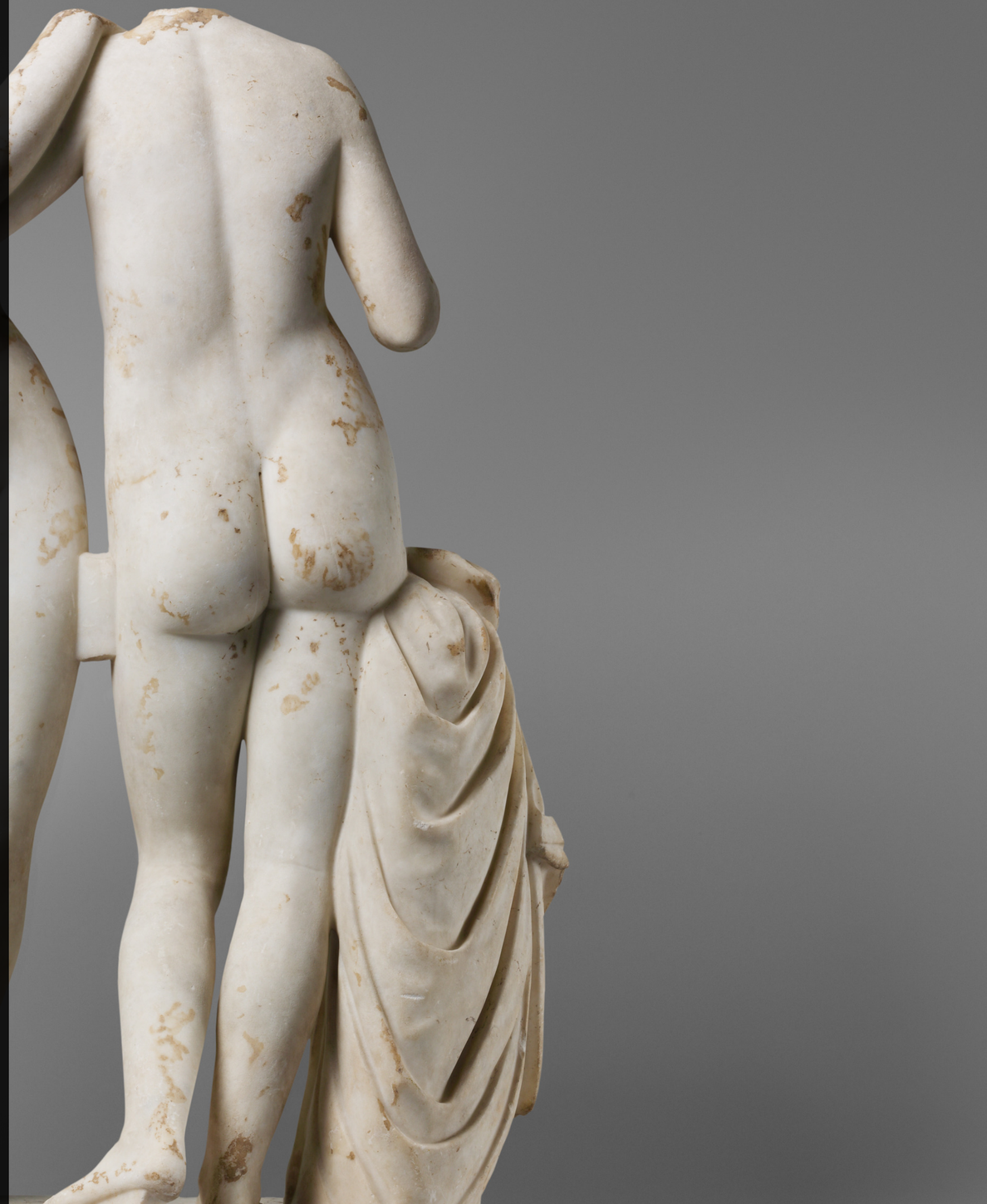
Received: from o4.m.fontawesome.com (o4.m.fontawesome.com [159.183.29.246]) by mx.turscar.ie (Postfix) with ESMTPS

Received: from o4.m.fontawesome.com (o4.m.fontawesome.com [159.183.29.246])
by mx.turscar.ie (Postfix) with ESMTPS

# FOLDING HEADERS

- Use relaxed/relaxed or relaxed/simple canonicalization
- If DKIM fails and the c= in the signature starts with “simple” that’s where to start

# AUDIENCE PARTICIPATION BREAK



# WHO HERE LIKES TO HELP PEOPLE?

# WHO HERE LIKES ASKING FOR HELP?

# EMAILGEEKS SLACK #EMAIL-DELIVERABILITY

# FOLDING HEADERS

Part 2

# FOLDING HEADERS

- Relaxed DKIM canonicalization makes it safe to fold headers at any space between words
- A line must not be longer than 998 characters
- Headers must be folded so each line is less than 998 characters
- What if there’s a word that’s 1000 characters long, so it can’t be folded?

# ~~FOLDING~~ SMASHING HEADERS

List-Unsubscribe: <https://unsub.example.com/something?v=punAx5p70AFCWXi5OF43HLNr4xbWk…

List-Unsubscribe: <https://unsub.example.com/something?v=punAx5p70A
FCWXi5OF43HLNr4xbWk…

# ~~FOLDING~~ SMASHING HEADERS

- Smashing a header in the middle of a word rather than folding at a space will break DKIM
- A mailserver shortening lines will prefer folding
- A word in a header longer than a given limit will prevent folding to that limit and may force smashing the header
- The RFC mandated limit is 998 characters, but Microsoft at least may start smashing things before that, at 700-ish
- Keep headers a reasonable length, and don’t have any long words (such as URLs) longer than 500 characters between spaces

# VERY LONG LINES

# VERY LONG LINES

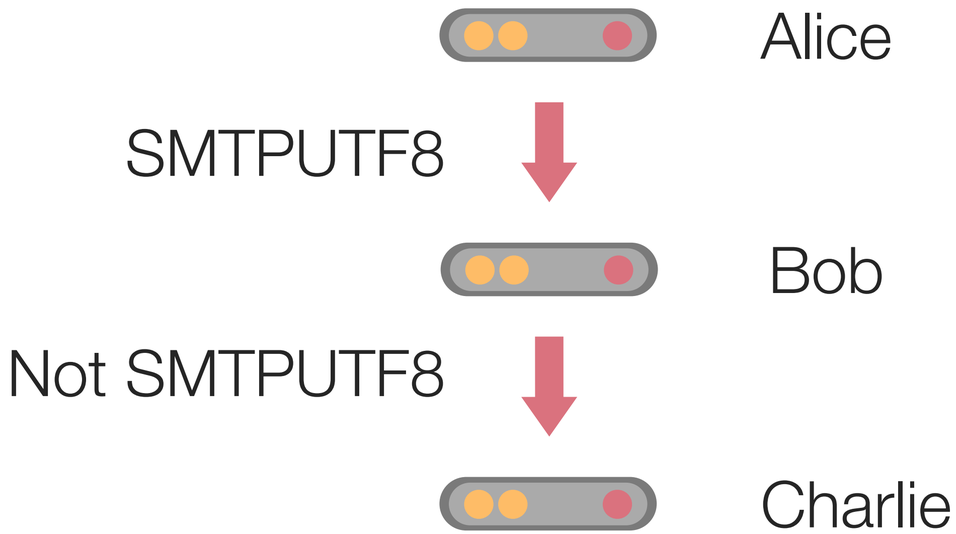
- Even with relaxed canonicalization breaking a line in the body will break a DKIM signature
- An email must not have lines longer than 998 characters
- HTML optimizers often create a single very long line
- An intermediate mailserver may break that into multiple lines, breaking the DKIM signature
- Encoding the body with base64 or quoted-printable encoding avoids the problem

# NON-ASCII AND SMTPUTF8

# NON-ASCII CHARACTERS

- Email historically is an ASCII only channel
- MIME encoding lets us convert non-ASCII content to ASCII and back
- SMTPUTF8 lets mailservers negotiate to send non-ASCII without any encoding needed
- SMTPUF8 is negotiated on each hop, not end to end

# NON-ASCII CHARACTERS



# NON-ASCII CHARACTERS

- Never put non-ASCII characters on the wire
- Using quoted-printable or base64 encoding avoids this issue as well as the problems with long body lines

# NOT THAT ALGORITHM

# NOT THAT ALGORITHM

- DKIM supports RSA and Ed25519
- Ed25519 is great in almost every way
- Some mailbox providers only support RSA
- “dkim=neutral (no key)” is how they tell you

# INCONSISTENT DNS

# INCONSISTENT DNS

**.com root**

sausagemail.com NS nsone.net

**nsone.net**

sausagemail.com NS nsone.net
sausagemail.com NS nstwo.com

**nstwo.com**

sausagemail.com NS nsone.net
sausagemail.com NS nstwo.com

# INCONSISTENT DNS

**nsone.net**

s1._domainkey.sausagemail.com TXT <public key>

**nstwo.com**

s1._domainkey.sausagemail.com NXDOMAIN

# DNSSEC

# DNSSEC

- Secures DNS
- Some clients pay attention to it, some don’t
- If it’s misconfigured, some clients will get errors
- I rely on the Verisign Labs DNSSEC Analyzer

# WHY NOW?

And why Microsoft?

# WHY NOW?

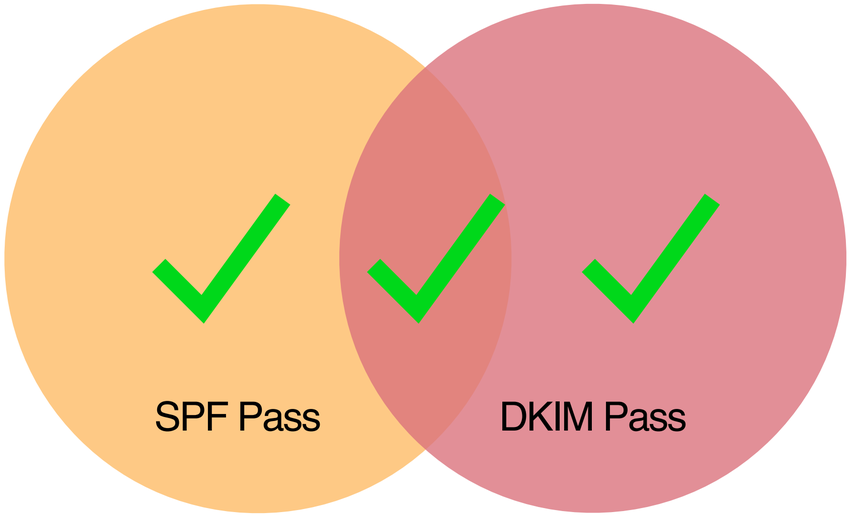
- Mailbox providers getting stricter
- Senders using enforcing DMARC
- Longer DKIM keys
- We’re better at the simple stuff

# WHY MICROSOFT?

- Not only Microsoft, but…
- Tend to rewrite invalid emails
- History of slightly inconsistent fleet

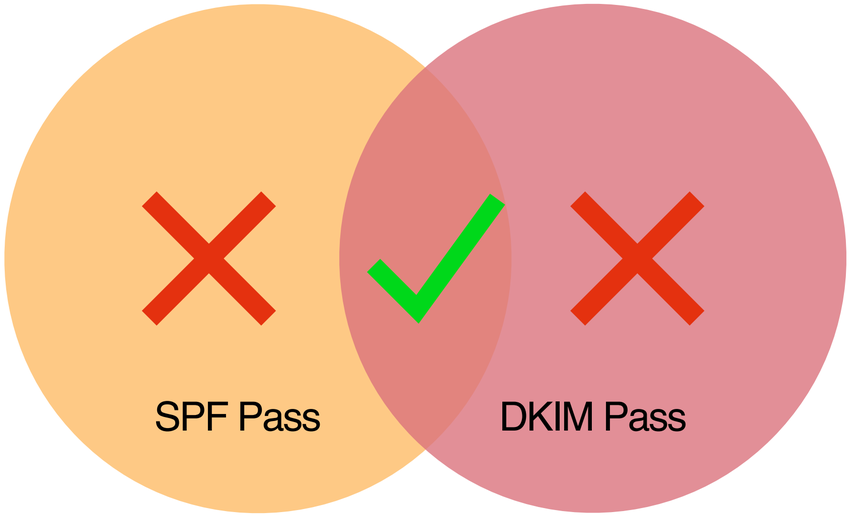
# WHY MICROSOFT?

## DMARC



# WHY MICROSOFT?

## MICROSOFT



# THAT'S ALL FOLKS

Any Questions?

# RESOURCES

wordtothewise.com/deliverabilitysummit2026

steve@wordtothewise.com