Securely Sending Email in 2024

OWASP NEW ZEALAND 2024

Richard Gray

SECURITY OPERATIONS MANAGER AT SMX

Thank You to Our Sponsors and Hosts!

AppSec NZ
appsec.org.nz

OWASP NEW ZEALAND
owasp.org.nz

AUT UNIVERSITY
TE WĀNANGA ARONUI O TAMAKI MAKAU RAU

BASTION SECURITY GROUP

DATACOM

aws

84.

PentesterLab

plexure

VERACODE

Without them, this Conference couldn't happen.

Introduction

SMX

Richard Gray

SECURITY OPERATIONS MANAGER

Content

INTRODUCTION

- Sender Spoofing - What's the problem?
- History of Email
- SMTP Basics
- Email Authentication Mechanisms
- Why does any of this matter?
- Recommendations
- Real World DMARC Usage

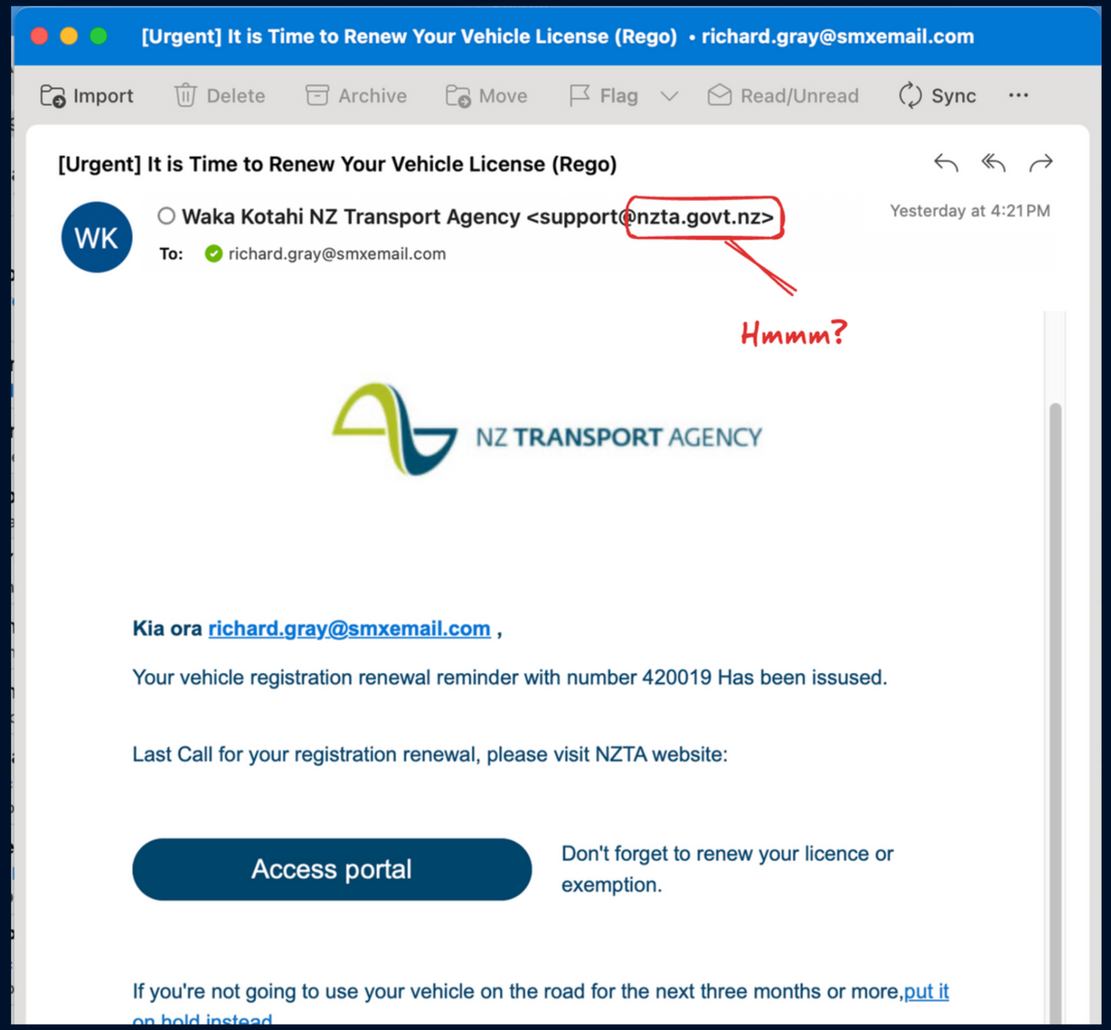
NZTA Notifications

THE PROBLEM

“Genuine vehicle licence reminder emails from Waka Kotahi NZ Transport Agency always come from @nzta.govt.nz” ...

NZTA - Phishing Example

THE PROBLEM



NZTA - DMARC Record

THE PROBLEM

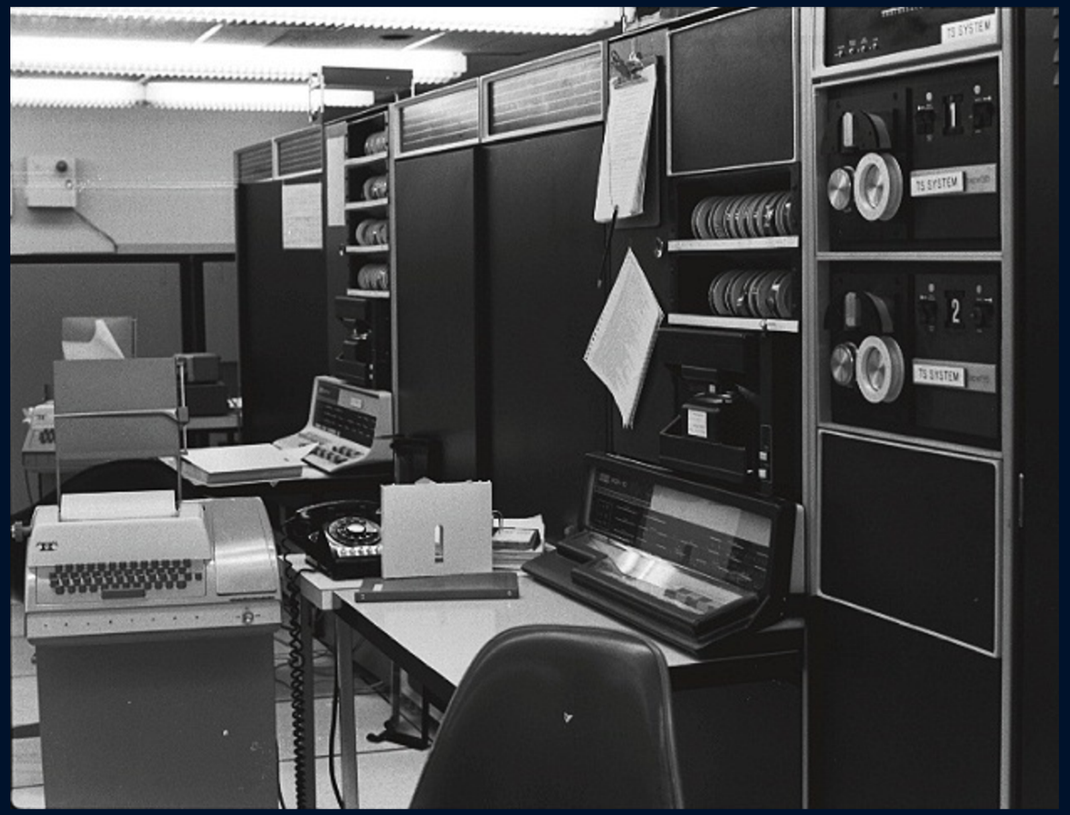
```
$ dig -t txt _dmarc.nzta.govt.nz +short
"v=DMARC1; p=none; rua=mailto:XXXX@nzta.govt.nz;"
```

NZTA's DMARC Record (with minor edits for brevity)

Ray Tomlinson

HISTORY OF EMAIL

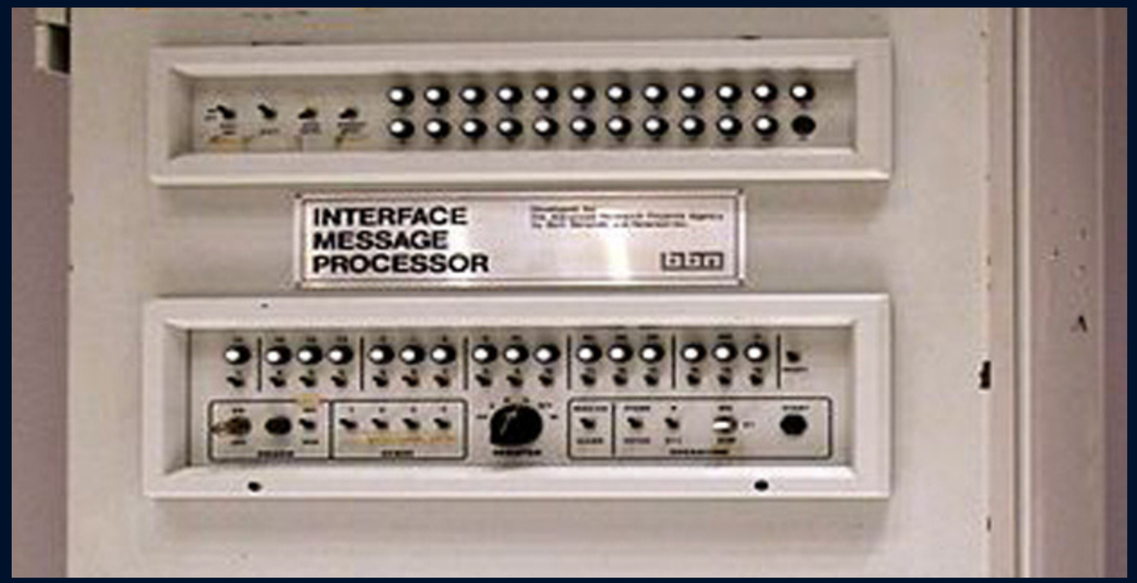
Ray Tomlinson

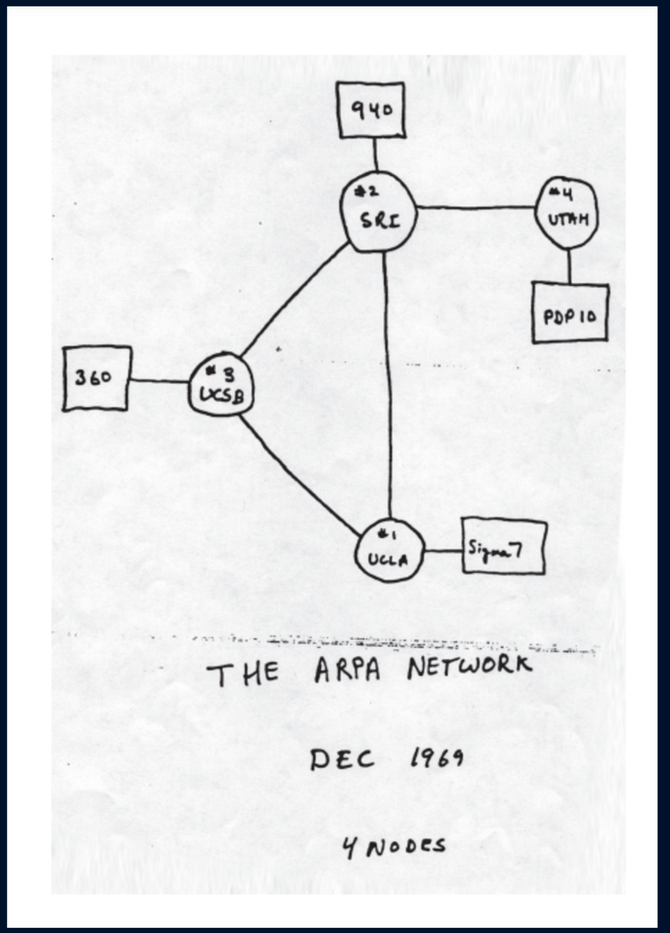


BBN-TENEXA & BBN-TENEXB

The ARPANET - 1969

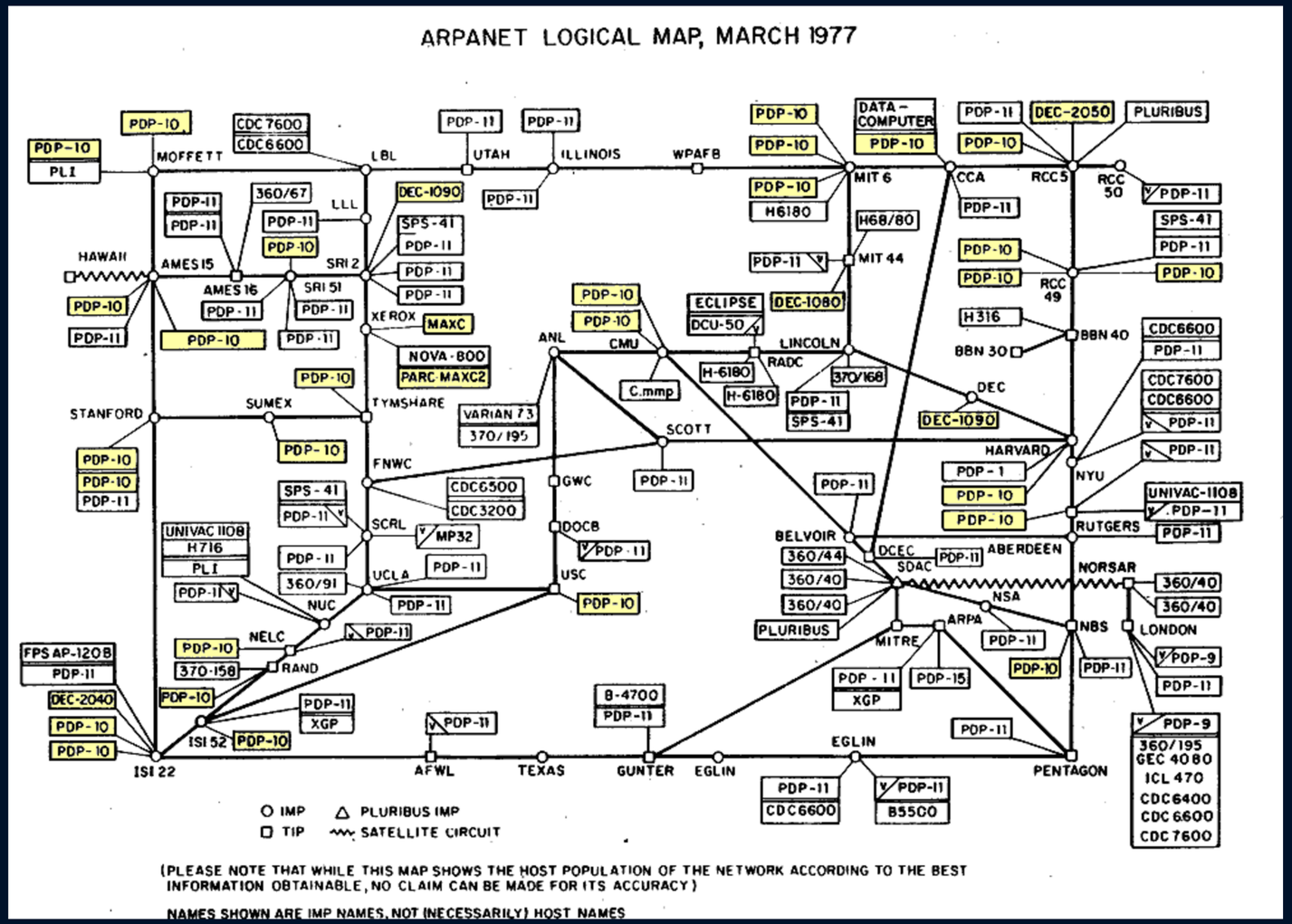
HISTORY OF EMAIL





The ARPANET - 1977

HISTORY OF EMAIL



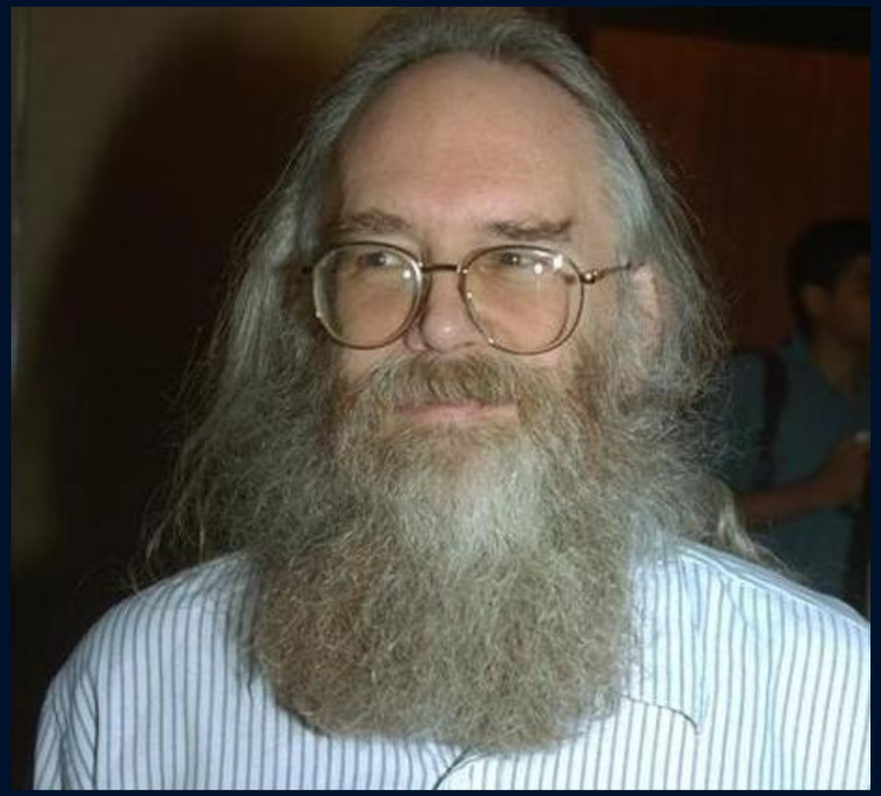
Setting the Scene

HISTORY OF EMAIL

- A relatively small network with high barriers to entry (you needed a $2M mainframe).
- Network participants largely known to each other.
- Government network not for commercial or personal use. Scope for abuse was not immediately apparent.
- Networking protocols under active development - priority of interoperability rather than security.

Jon Postel

HISTORY OF EMAIL



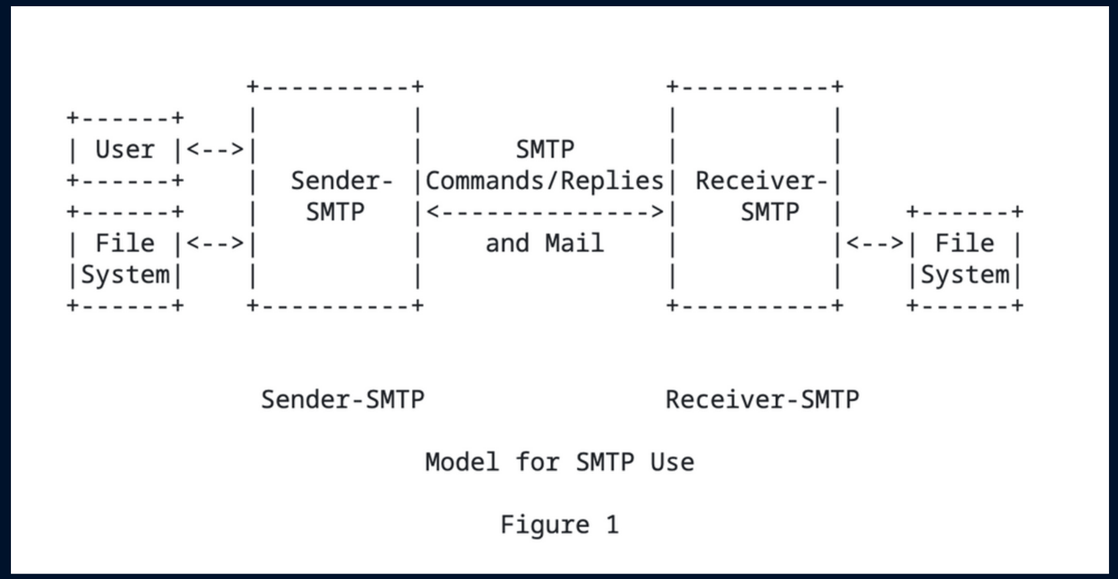
Postel’s Law (a.k.a the Robustness Principle)

"be conservative in what you send, be liberal in what you accept"

- Coined by Jon Postel in RFC 761 - Transmission Control Protocol
- Sounds good, but has resulted in a long tail of challenges and security problems.

SMTP - Simple Mail Transport Protocol

HISTORY OF EMAIL

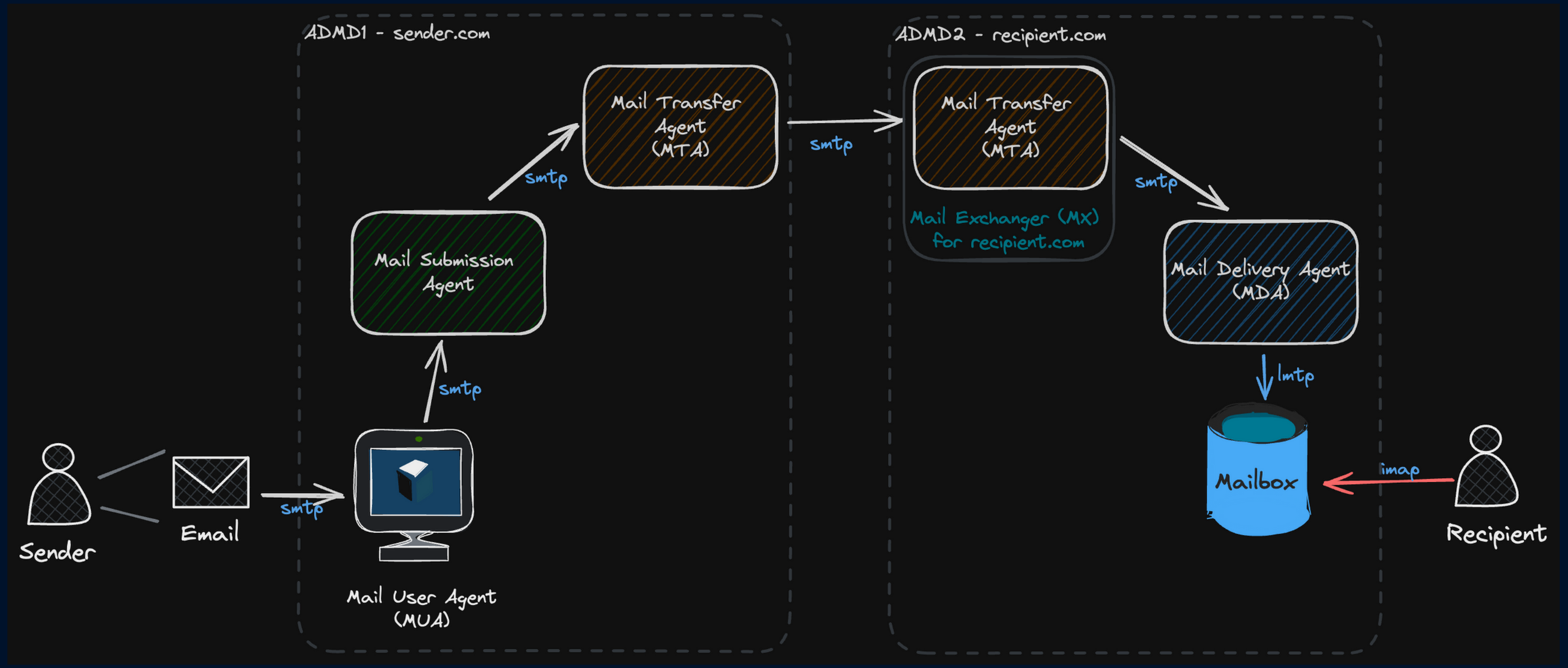


SMTP Model Diagram from RFC 788 (1981)

- First described in RFC 788, authored by Jon Postel and published in November 1981
- Grew from earlier mail protocols which relied on FTP as the underlying transport
- Although it has been developed and extended in subsequent RFCs, the basic protocol described in RFC 788 still closely resembles the SMTP we use today, 43 years later.

Message Delivery

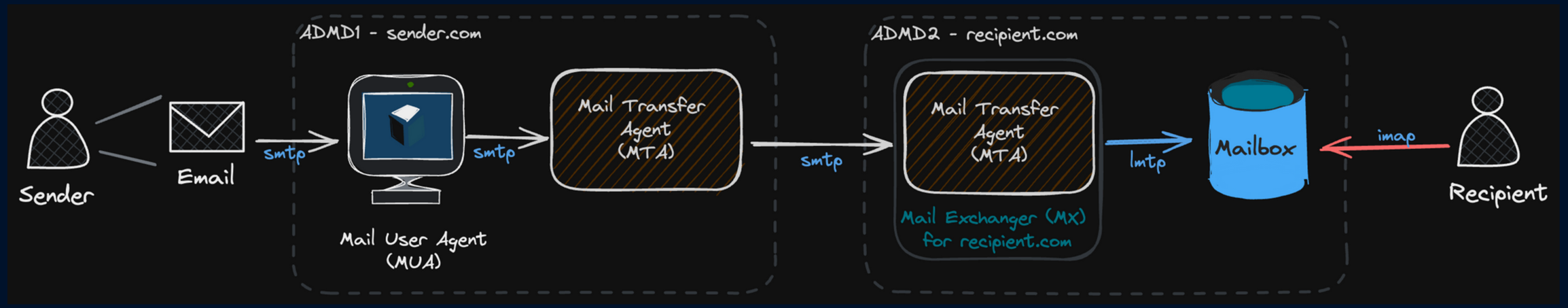
SMTP



SMTP Delivery Model

Message Delivery - Simplified

SMTP



SMTP Delivery Model

Open Relays

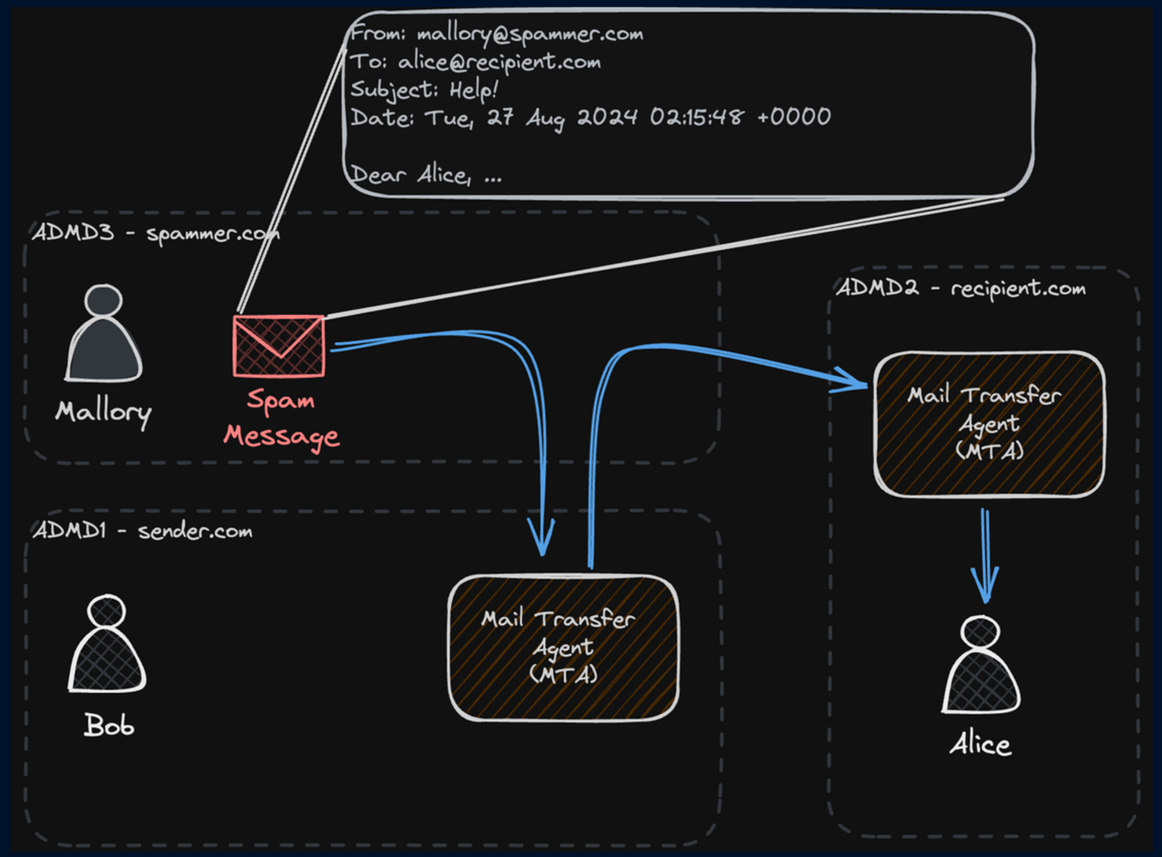
SMTP PROBLEMS

An SMTP server that allows anyone to deliver mail through it, not just mail to or from known users.

- ✅ Local Source, Local Destination
- ✅ Local Source, Remote Destination
- ✅ Remote Source, Local Destination
- ❌ Remote Source, Remote Destination

To avoid being an open relay, mail servers must only accept mail from authenticated and authorized clients.

- Authenticated users (e.g. user/password authentication)
- Authorized IPs (local network)



Message and Envelope

SMTP BASICS

Envelope

A wrapper around the email message containing routing information to support delivery of the message. The envelope identifies:

- The sender address
- The recipient address

Message

Actual message content visible to the user, defined by RFC 2822 and containing:

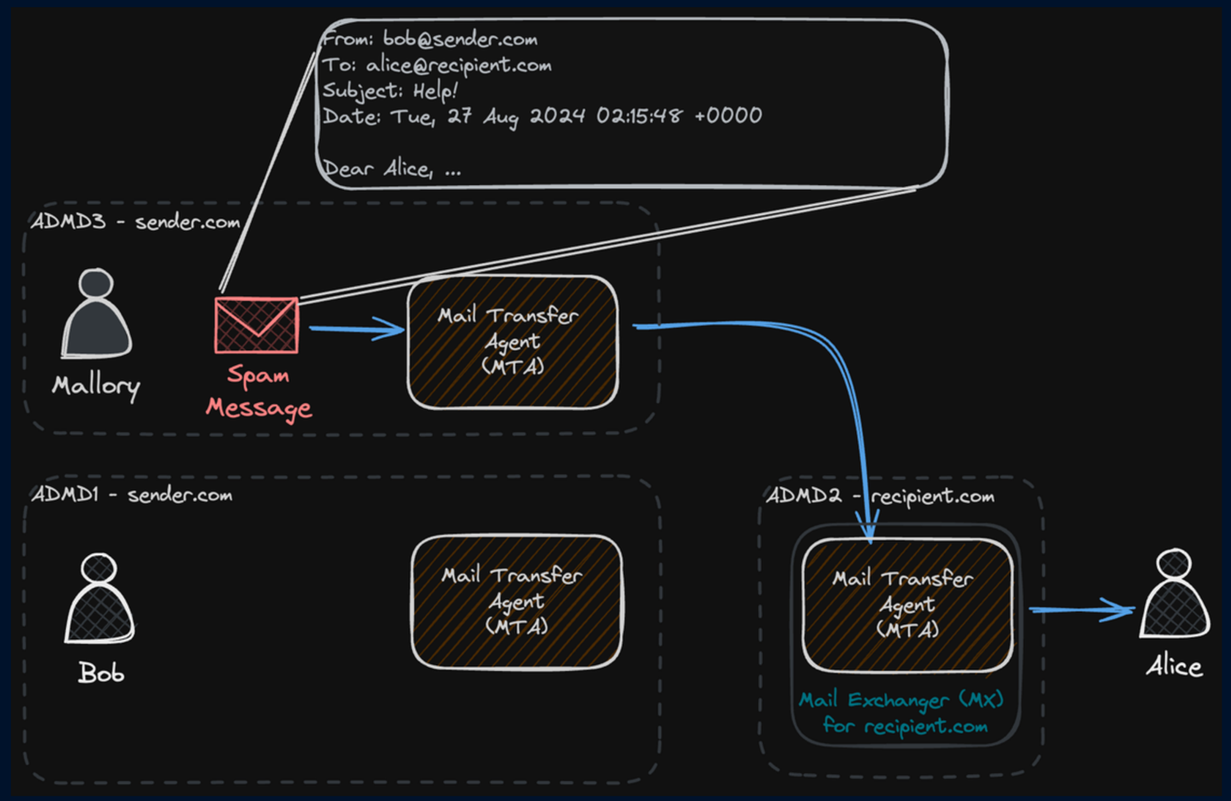
Headers - Metadata about the message including:

- From: the sender's email address as seen by the recipient.
- To: the recipient's email address
- Subject
- Date
- Message-ID
- Content-Type
- Various other headers

Body - the actual content of the message, which might be plain text, HTML, or both, and can include attachments.

Sender Spoofing

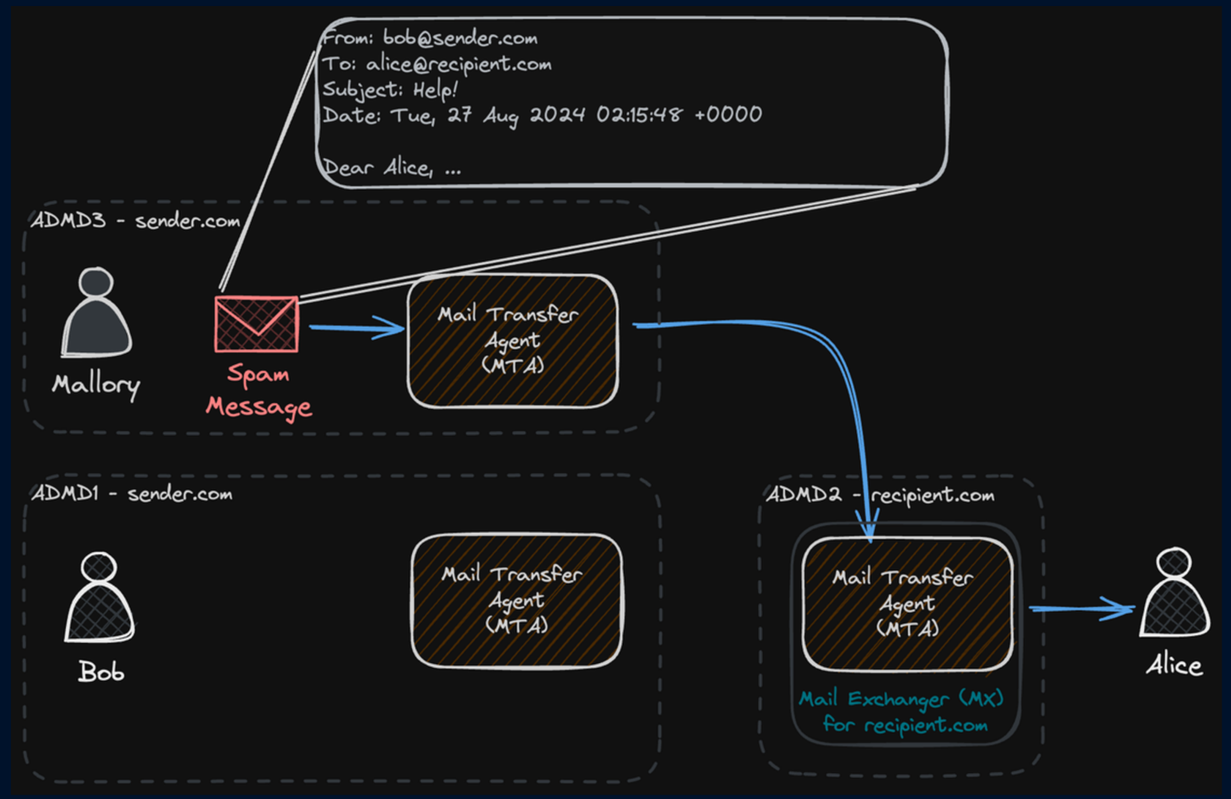
SMTP PROBLEMS



- Sender Spoofing is the creation of email messages with a forged sender address, typically intended to mislead the recipient.
- In this example, Mallory sends a message to Alice pretending to be Bob.
- How can Alice know that the received message is from Mallory and not Bob?

Email Authentication

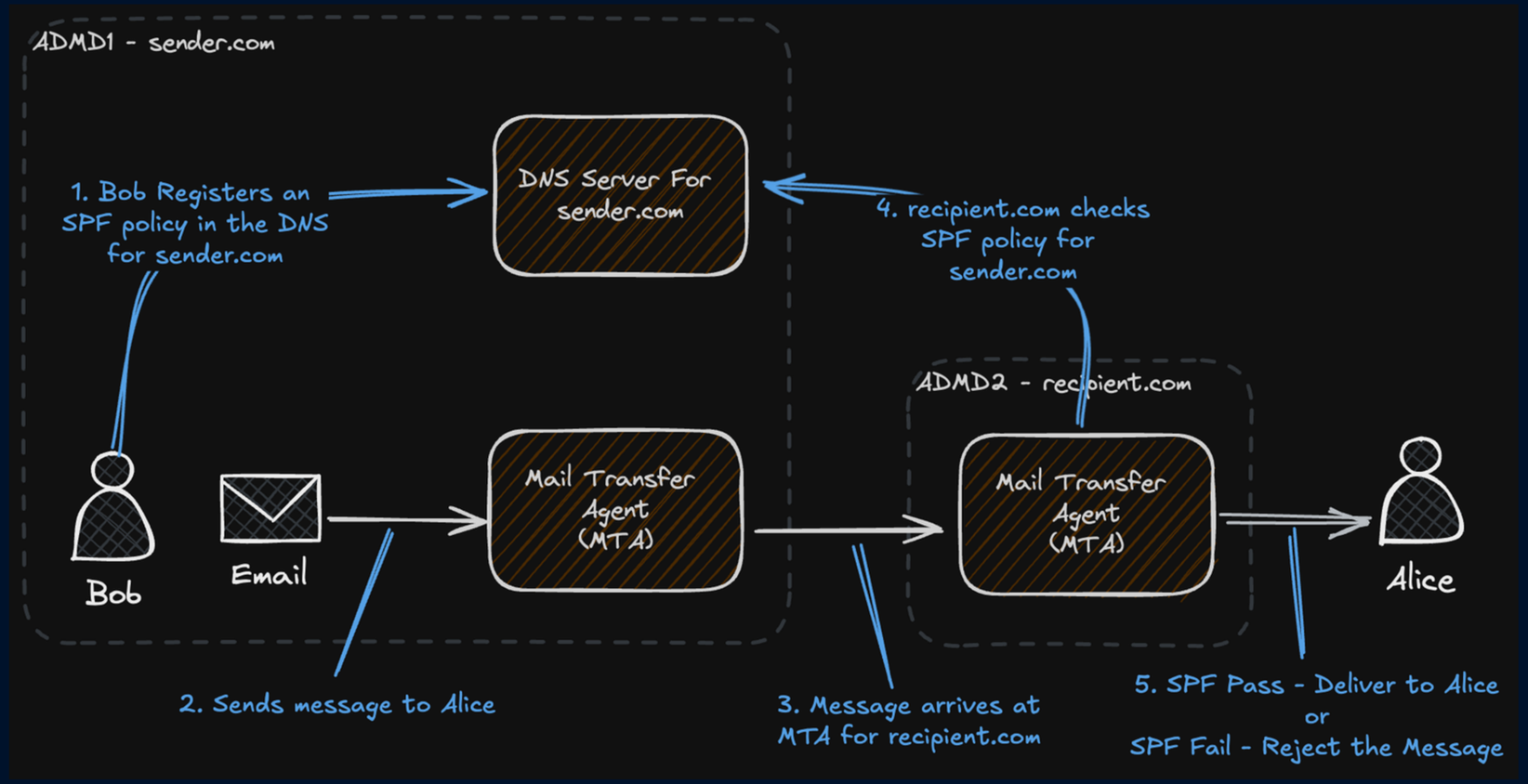
EMAIL AUTHENTICATION



- How do we verify the sender of a message?
- How can we be sure a message did originate from the apparent sender?

Sender Policy Framework (SPF)

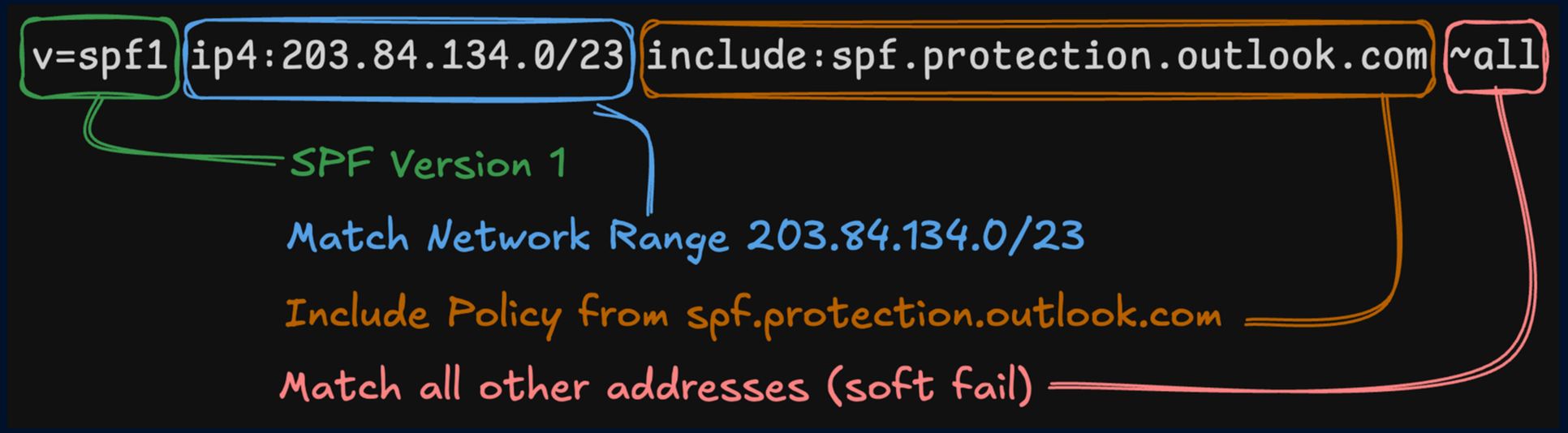
EMAIL AUTHENTICATION



- Allows domain owners to advertise which servers (IP addresses) are authorised to send mail for their domain
- Applies to the Envelope Sender address, not the From header address

SPF - Example Record

EMAIL AUTHENTICATION

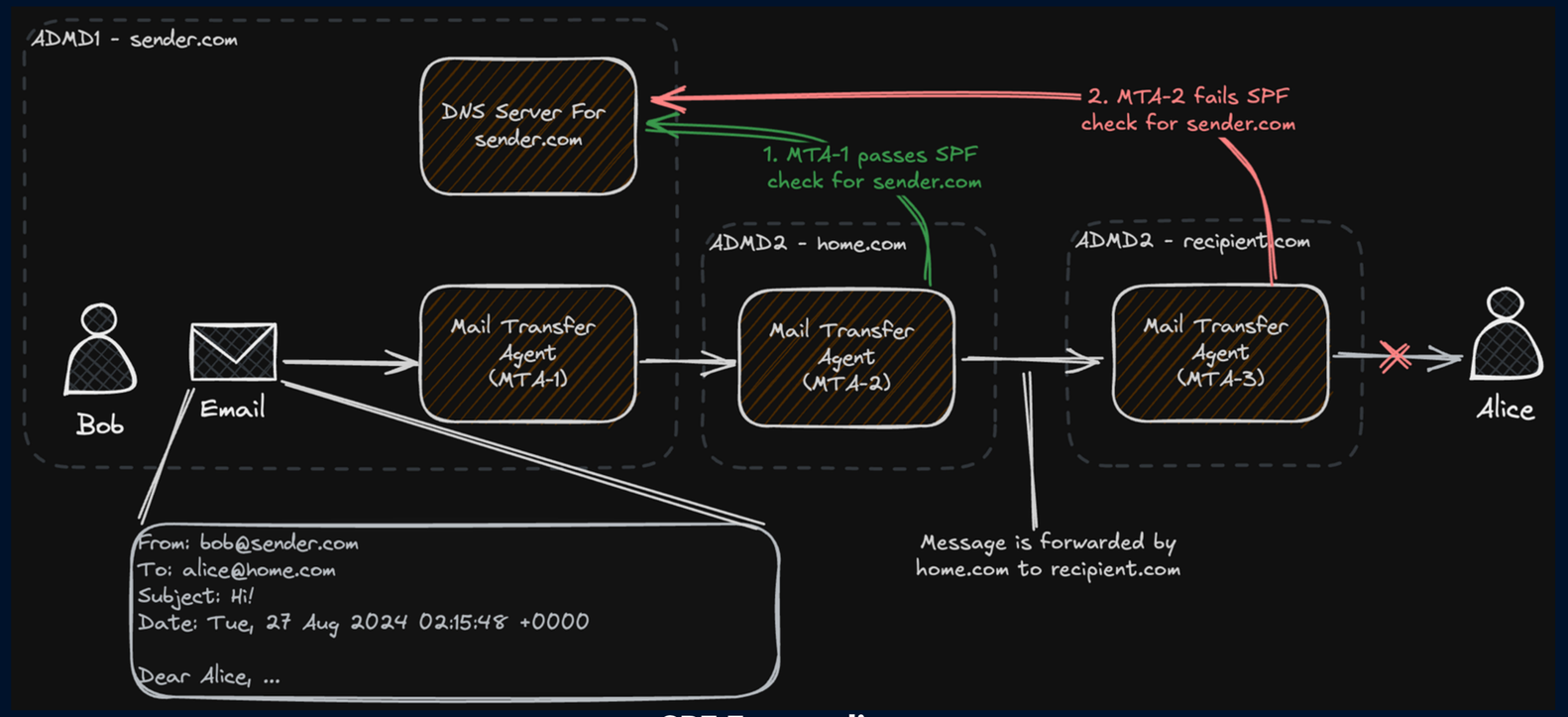


Record	Result	Description
-all	fail	Explicitly disallow all hosts
~all	softfail	Weak disapproval. Receivers should not reject mail on the basis of a softfail result alone.
?all	neutral	Neutral - Neither allowed nor disallowed
+all	pass	Pass all hosts

SPF - Weaknesses

EMAIL AUTHENTICATION

- Doesn't work well with forwarding and mailing lists. SPF checks fail at the onward destination.
- DNS size limits.
- Only protects the envelope sender, allowing for From header spoofing. I.e. the address the recipient sees.



SPF Forwarding

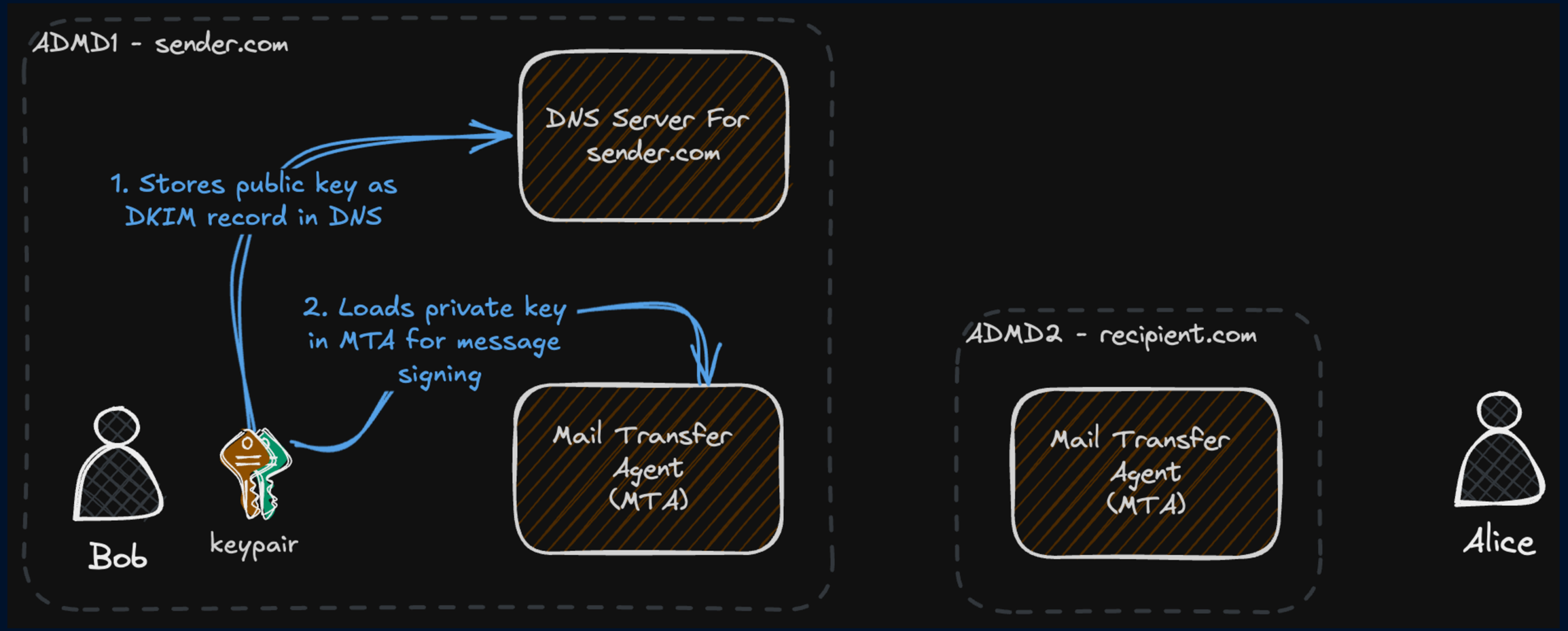
DomainKeys Identified Mail (DKIM)

EMAIL AUTHENTICATION

- An email authentication method based on digital signatures
- Verifies the sender's domain and ensures email integrity
- Adds a cryptographic signature to the email headers
- Receiving servers validate the signature using the sender's public key
- Addresses some of the deficiencies of SPF

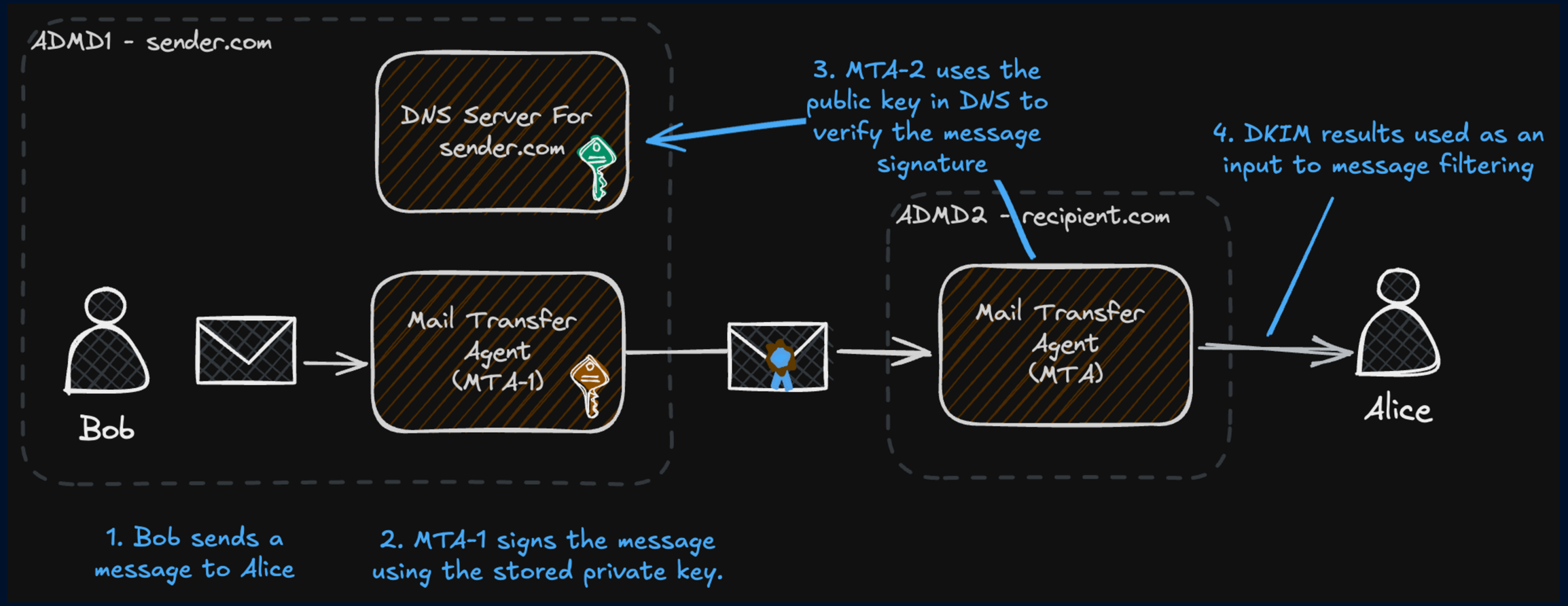
DKIM Setup

EMAIL AUTHENTICATION



DKIM Signing and Verification

EMAIL AUTHENTICATION



DKIM Strengths and Weaknesses

EMAIL AUTHENTICATION

Strengths

- Content integrity: DKIM verifies that the email content hasn't been altered in transit
- Forwarding compatibility: DKIM signatures remain valid when emails are forwarded
- Non-repudiation: Provides cryptographic proof of email origin, which SPF doesn't offer.

Weaknesses

- Again, doesn't necessarily protect the From header.
- Vulnerable to replay attacks.

DMARC

EMAIL AUTHENTICATION

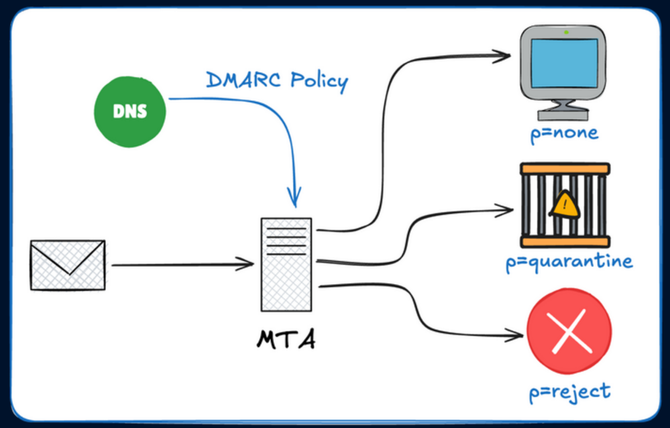
Authentication Alignment

Requires that the From header domain aligns to a domain verified by SPF or DKIM

Policy Enforcement

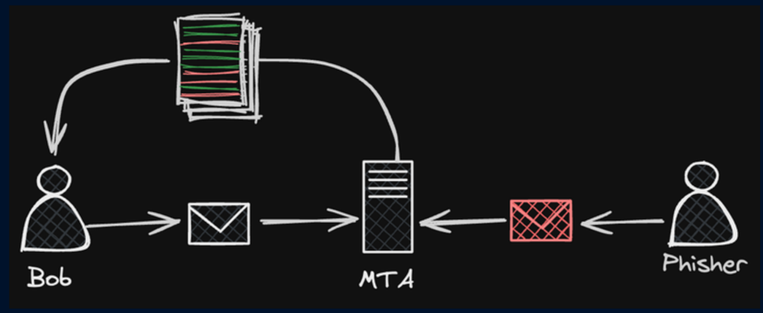
Allows domain owners specify how receiving mail servers should handle messages that fail authentication. Policies include:

- none - monitor only
- quarantine - treat as suspicious
- reject



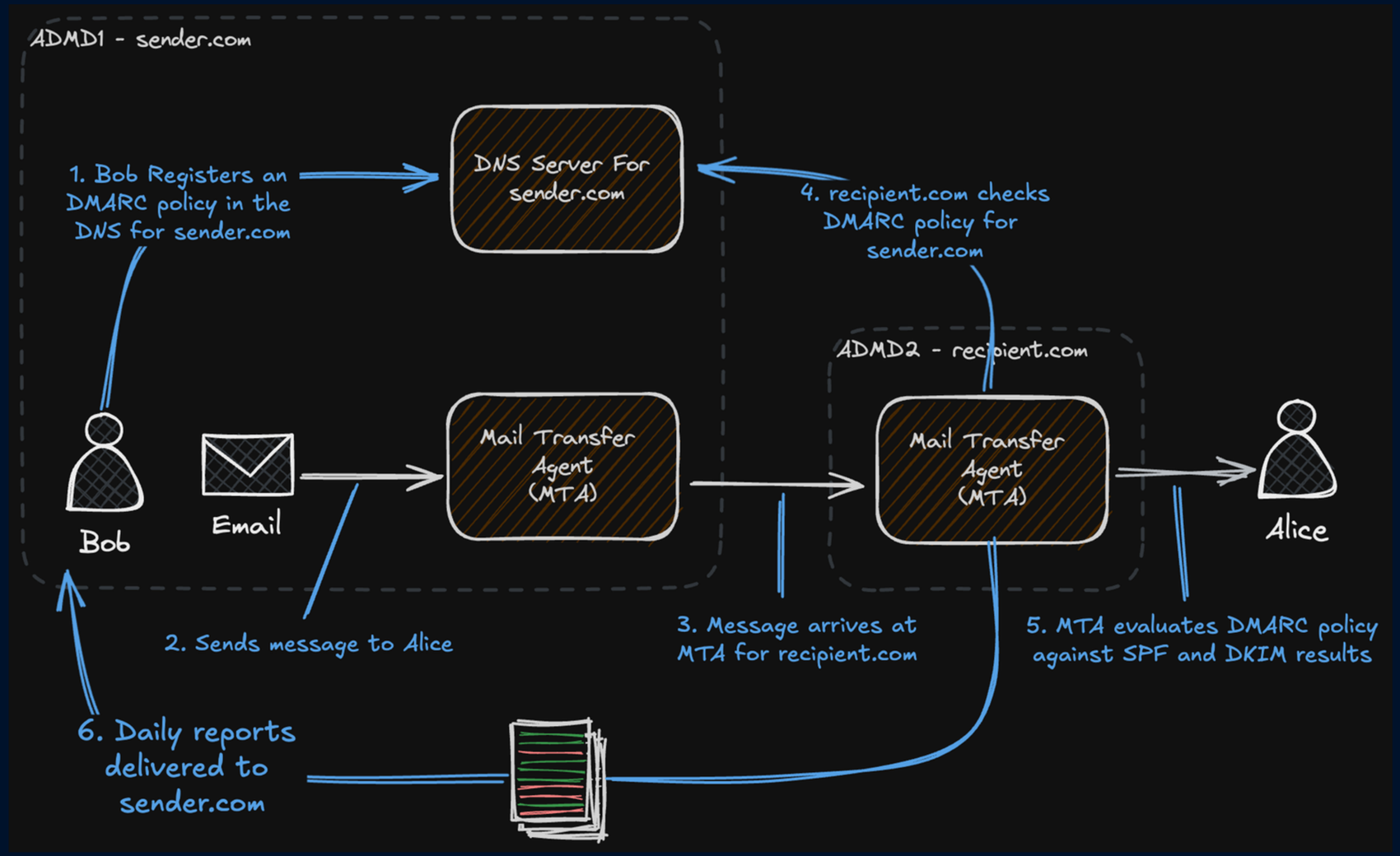
Reporting

Provides domain owners with detailed reports about emails sent using their domain



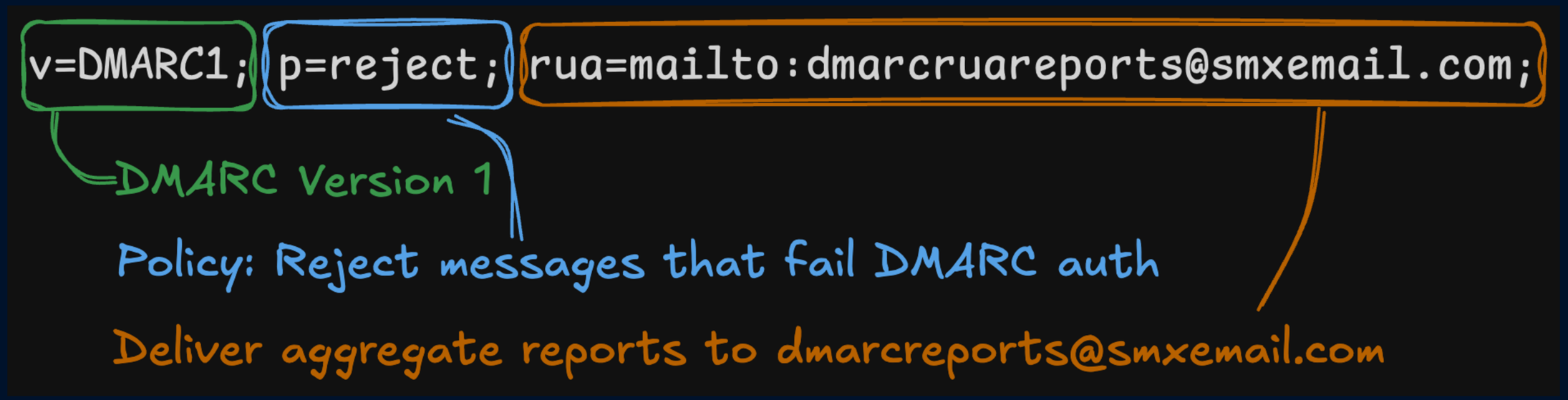
DMARC Process

EMAIL AUTHENTICATION



DMARC Record

EMAIL AUTHENTICATION



Why Should I Care?

EMAIL AUTHENTICATION

Brand Protection

- DMARC safeguards your brand's reputation by preventing unauthorized use of your domain.
- Builds trust with your email recipients.
- Protects your staff, suppliers, and customers from phishing and other scams.

Deliverability

- From 2024, Google and Yahoo require that all senders implement SPF or DKIM, and that bulk senders also implement DMARC.
- Failure to comply with this requirement will result in messages being rejected or marked as Spam.

Compliance

- For government agencies, or organisations providing services to government, use of DMARC is now mandated by NZISM.

Recommendations - Summary

RECOMMENDATIONS

DMARC with an enforcing policy is essential

Start with p=none and consume reports into a DMARC report analyzer

Identify legitimate mail services and configure them for DKIM and SPF (both is best)

Transition to DMARC enforcement

Recommendations - SPF

RECOMMENDATIONS

Recommendations - DKIM

RECOMMENDATIONS

Configure DKIM signing on legitimate mail services

Make sure the DKIM signing domain aligns with your email sending domain

Validate your record

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=nz.smxemail.com;
     ... SNIP ...
From: SMX Limited <sales@comms.smxemail.com>
```

Organisational Domains are aligned

SMX DMARC STATS

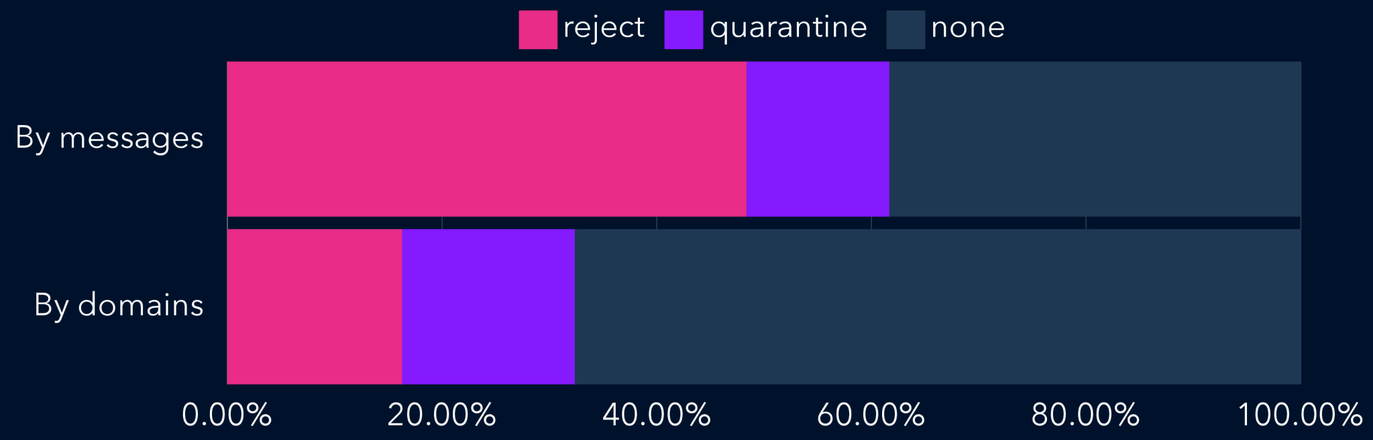
STATISTICS

37 million
messages in 1 week

34 million (92%)
messages protected by DMARC

184K
domains protected by DMARC

Message Count by DMARC Policy



Enforcing DMARC policies apply to 62% of messages, but only 32% of domains

The NZ DMARC Landscape

STATISTICS

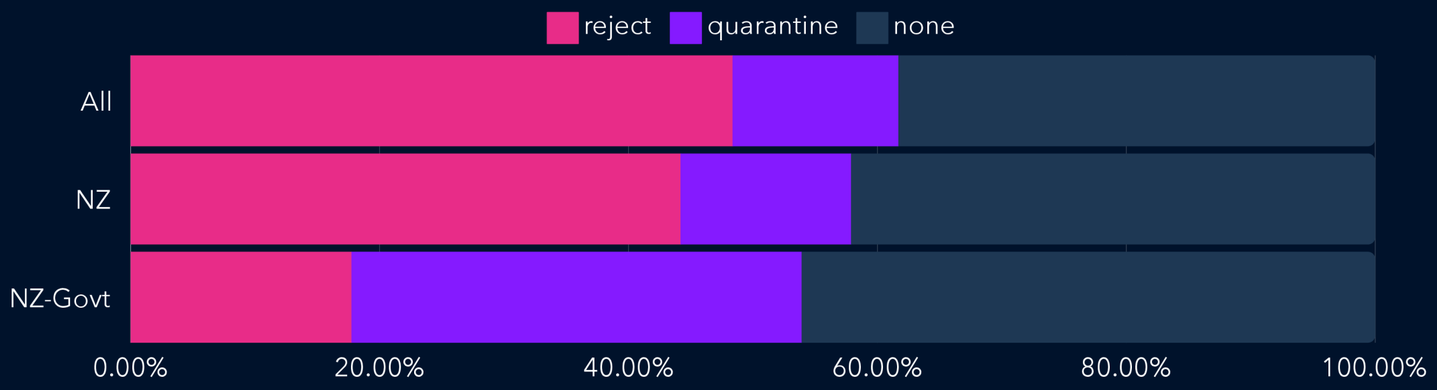
18 million

NZ messages protected by DMARC

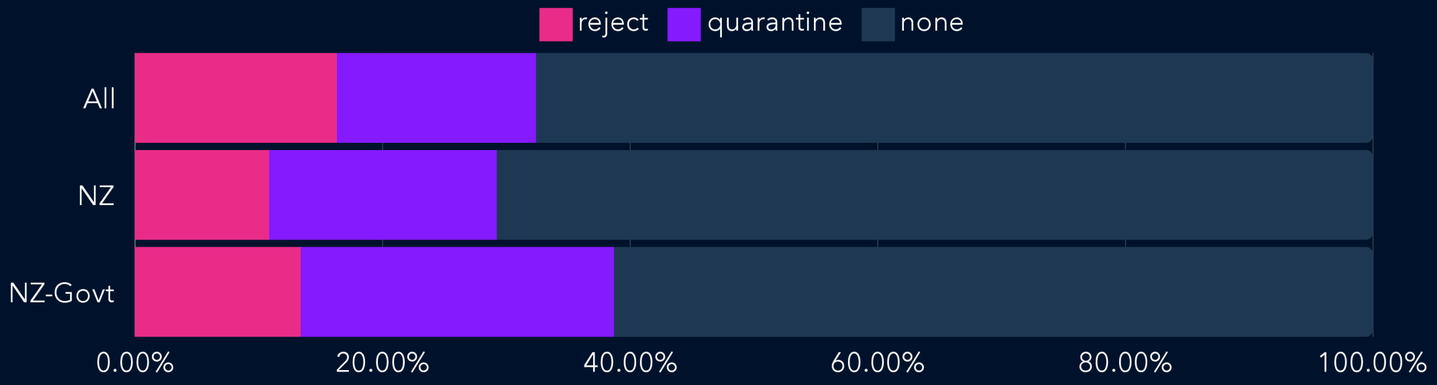
29K

NZ domains protected by DMARC

Message Count by DMARC Policy



Domain Count by DMARC Policy



NZ Top Senders

STATISTICS

NZ Top Senders - Overall

Rank	Domain	DMARC Policy
1	site.trademe.co.nz	reject
2	mail.ezibuy.co.nz	reject
3	edm.briscoes.co.nz	reject
4	comms.everydayrewards.co.nz	reject
5	mail-grabone.co.nz	none
6	digitalcomms.airnz.co.nz	reject
7	mail.trademe.co.nz	reject
8	flybuys.co.nz	quarantine
9	e.farmers.co.nz	none
10	neighbourly.co.nz	reject

NZ Top Senders - Government

Rank	Domain	DMARC Policy
1	msd.govt.nz	reject
2	ironline.ird.govt.nz	quarantine
3	nzta.govt.nz	none
4	aucklandcouncil.govt.nz	none
5	employment.govt.nz	none
6	companies.govt.nz	none
7	mail.aucklandlibraries.govt.nz	reject
8	qldc.govt.nz	none
9	news.aucklandcouncil.govt.nz	reject
10	doc.govt.nz	quarantine

Homework!

1. Check the DMARC record for your domain!
    a. Do you have one?
    b. Is it valid?
    c. What policy is being used? none, quarantine, or reject?
    d. Where are the reports going?

2. Check the SPF record for your domain!
    a. Do you have one?
    b. Is it valid?

Thank you!