Strategies to Protect Your Organization

Mastering Mailflow

22 februari 2026

Rubicon

Agenda

- Mail authentication
- Security
- Delegation
- Tips

Who am I?

Dave Stork
Cloud Architect @ Rubicon BV The Netherlands
Microsoft MVP M365 Apps & Services since 2014
Microsoft Certified Trainer since 2015

d.stork@rubicon.nl
https://bsky.app/profile/davestork.nl
@dmstork@mastodon.social

https://about.me/dmstork

Microsoft Partner

Rubicon

Mail authentication

But first…

Note the difference

Inbound mail

From external sources “the evil internet”

Your environment needs to check mail

Outbound mail

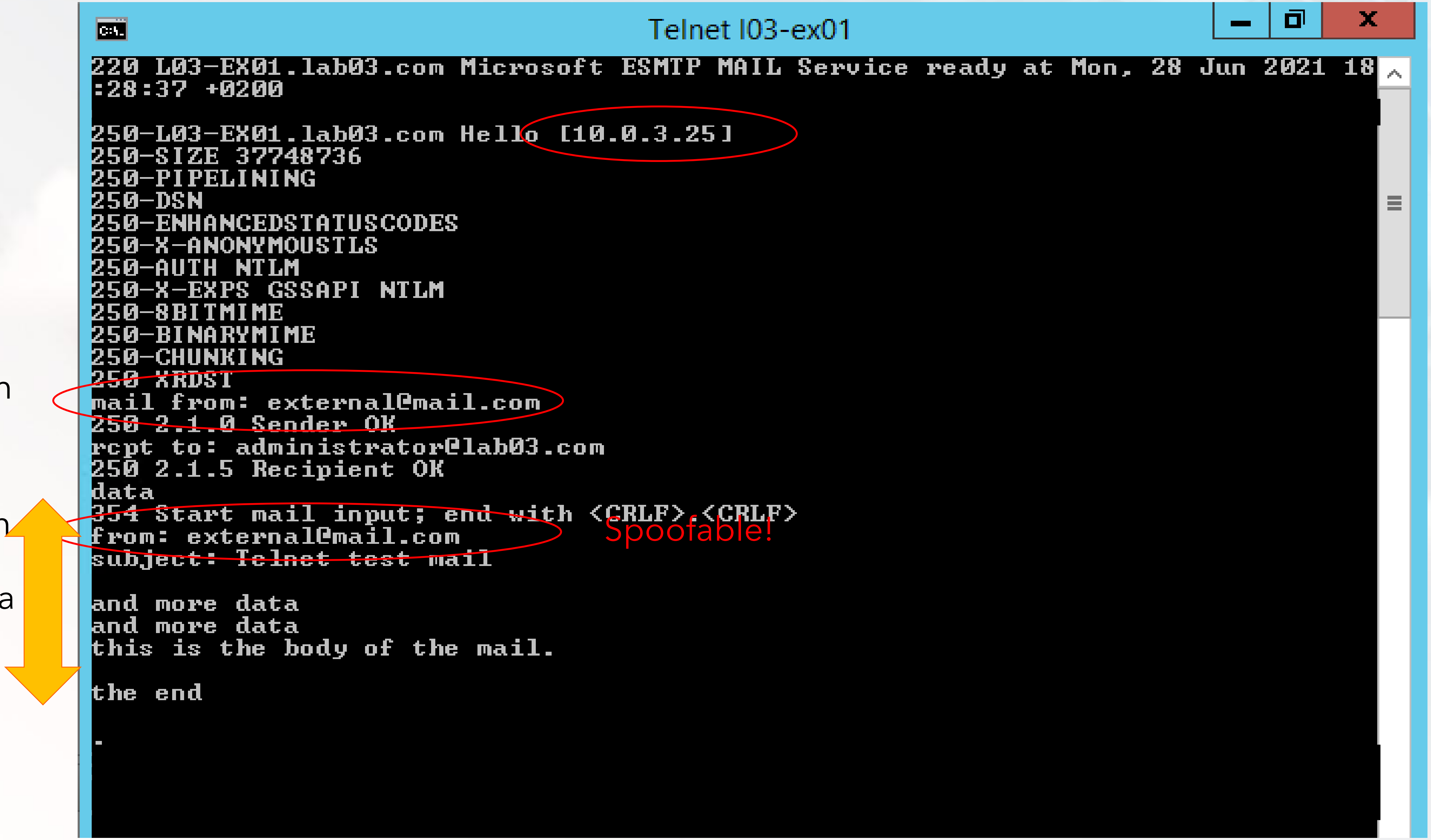
Mail sent from your organization to external recipients

You are responsible to enable external recipients to verify it

Internal mail

Can include external SaaS applications

Might depend on delivery method; the system might consider this inbound mail



```
220 L03-EX01.lab03.com Microsoft ESMTP MAIL Service ready at Mon, 28 Jun 2021 18
:28:37 +0200

250-L03-EX01.lab03.com Hello [10.0.3.25]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-X-ANONYMOUSTLS
250-AUTH NTLM
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
mail from: external@mail.com
250 2.1.0 Sender OK
rcpt to: administrator@lab03.com
250 2.1.5 Recipient OK
data
354 Start mail input; end with <CRLF>.<CRLF>
from: external@mail.com
subject: Telnet test mail

and more data
and more data
this is the body of the mail.

the end

.
```

Sender IP

RFC5221.From
P1

RFC5222.From
P2

Data

Spoofable!

Proving the mail is actually from your organization

Mail Authentication

SPF – Sender Policy Framework

List of FQDNs & IP Addresses containing allowed sending servers

DKIM – Domain Key Identified Mail

Signature of mail headers and body, including which selector

Public key in DNS in signing domain

DMARC - Domain-based Message Authentication, Reporting and Conformance

Signals to recipient on how to handle authentication failures

Are both From addresses similar, does SPF or DKIM fail

Mail address for sending (aggregate) reports (zipped & XML)

Forwarding mail breaks but has valid use cases (mailing lists)

Repairing forwarding

SRS – Sender Rewriting Scheme

Rewrites the RFC5221.From address (P1)

Corrects SPF failures

Does NOT correct DMARC failures

ARC – Authenticated Received Chain

Adds ARC signature based on authentication results when receive before forwarding

Receiving organization must trust ARC domain

This does account for DMARC failures due forwarding

Security

Encrypted transport between two organizations

Transport Security

Opportunistic TLS

Negotiations at connection and highest possible security will be used

Fallback to weaker or no encryption

Valid for each domain

Forced TLS

Same as opportunistic but no fallback to weak or no encryption

Not RFC compliant for receiving organizations. Outbound is your prerogative.

Mandatory or Partner TLS

No negotiations and no fallback

Often configuration per mail domain required

Encrypted transport between two organizations

Transport Security

MTA-STS – MTA Strict Transport Security

DNS record to signal MTA-STS use; hardcoded HTTPS site with policy file
Policy file contains FQDN of receiving server that must match CN certificate
Trust at first connect. Will not connect when server FQDN is not in policy file

DANE - DNS-based Authentication of Named Entities

Requires DNSSEC to ensure trust
Uses TLSA DNS record to validate transport certificate presented by receiving server
No per domain security required

Priority within Exchange Online is:

First attempt DANE, then MTA-STS and finally Opportunistic (or Forced) TLS
Mandatory TLS connection overrides all because it's domain specific

How do you protect messages themselves?

Message Security

Client S/MIME – Secure/Multipurpose internet Mail Extensions (similar PGP/GPG)
Message encryption at client and open standard
Requires certificate exchange between sender & receiver + config at each client
Breaks filtering
Gateway S/MIME
Message encryption at egress point/ mail gateway of organization
Dependency on gateway
Configuration on both organization required

Microsoft Purview Message Encryption & IRM
Does not break filtering
Manual or organization trigger
Can be used with any external recipient (ME) without preconfiguration
Provides granular usage restrictions (IRM)

Some basic and helpful facts and tips

Defender filtering

Defender for Office 365 Plan 1 vs Plan 2
Plan 1 is IMHO minimum with Safe Links, Impersonation protection etc.
Plan 2 is for more in-depth hunting and investigations

- Explorer as more flexible Message Trace

Configuration

Follow either standard or strict recommendations with your own customizations

Validate with ORCA or Configuration analyzer

Some gotcha's:

Users can be blocked if they cross outbound spam threshold

- send-as mail also count towards delegate not shared mailbox

Not all default quarantine policies notify of any quarantined mail

Shared Mailbox quarantine access requires filtering by user

When you have services in front of Exchange Online

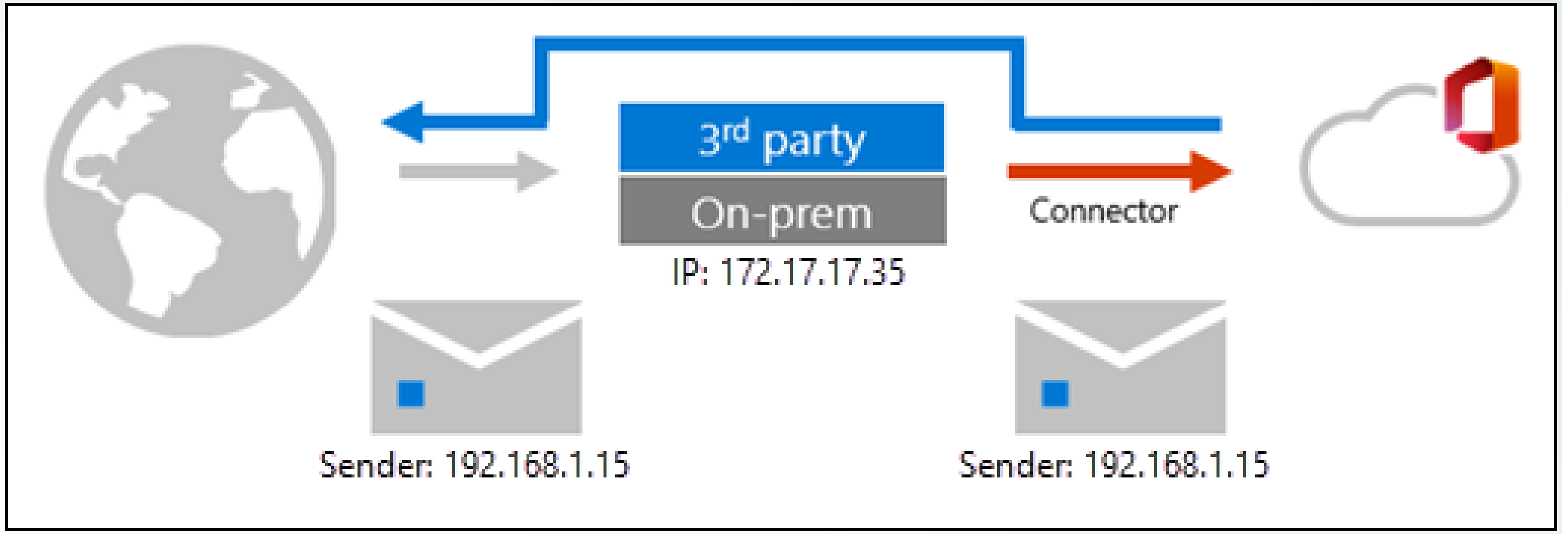
Enhanced filtering

Enhanced filtering or skip-listing

Used with hybrid on-prem Exchange, third party filtering services or appliances

Identify correct “Original Sender IP”

Crucial for increased correct assessment of mail authentication



Mail delegation

Rubicon

Sending mail from a third-party application

Mail delegation to Exchange Online

Client Submission

- User account authenticates and sends mail to internal and external recipients
- Uses Exchange Online configuration
- Note: Basic Authentication deprecated

SMTP Relay

- No user required, but sends mail to internal and external recipients
- Requires addition of static IP in SPF
- Inbound Connector accepting from sending IP

Direct Send

- Seen as if your device\app is external sender (e.g. anonymous mail)
- Requires addition of static IP in SPF
- No sending to external recipients (no open relay)

Sending mail from a third-party application

Relaxed vs Strict alignment

Relaxed alignment

- Default setting DMARC policy
- Any subdomain is equal to organization domain:
  - sub.contoso.com EQUALS contoso.com

Strict alignment

- Enforced for SPF and or DKIM
  - sub.contoso.com NOT EQUALS contoso.com

Be aware

- Strict alignment: many MTA services may prevent this. Use different domain
- If relaxed alignment is good enough, use subdomain.

Sending mail from a third-party application

Mail delegation with HVE

High Volume Email (HVE) – Public preview

- Client submission directly into Exchange Online
- Special account and license within Exchange Online
- Still supports Basic Authentication on smtp-hve.office365.com
- Can be used by third-party applications (Conditional Access policy!)
- Intended for internal bulk mailing

Sending mail from a third-party application

Mail delegation with ACS

Azure Communication Services (ACS)

- Mail relay service based in Azure and subscription based
- Requires configuration independent of Microsoft 365
- Does support both P1 & P2 from domain (e.g strict alignment possible!)
- Supports Client Submission Basic Auth on smtp.azurecomm.net
- Supports automation
- Intended for internal and external bulk mailing

Final and best tip

Rubicon

Do not use mail!

If there are any other solution to transport information, use it!

Mail is not designed with security in mind

Scan to mail features: additional software can drop scanned files directly in OneDrive.
APIs are more flexible and safer.

Push your software manufacturer to adopt more modern methods
MS Graph and NOT EWS!

Questions?

Rubicon

Please give your feedback

Mastering Mailflow: Strategies to Protect Your Organization

Solutions built on and born in the cloud

Security

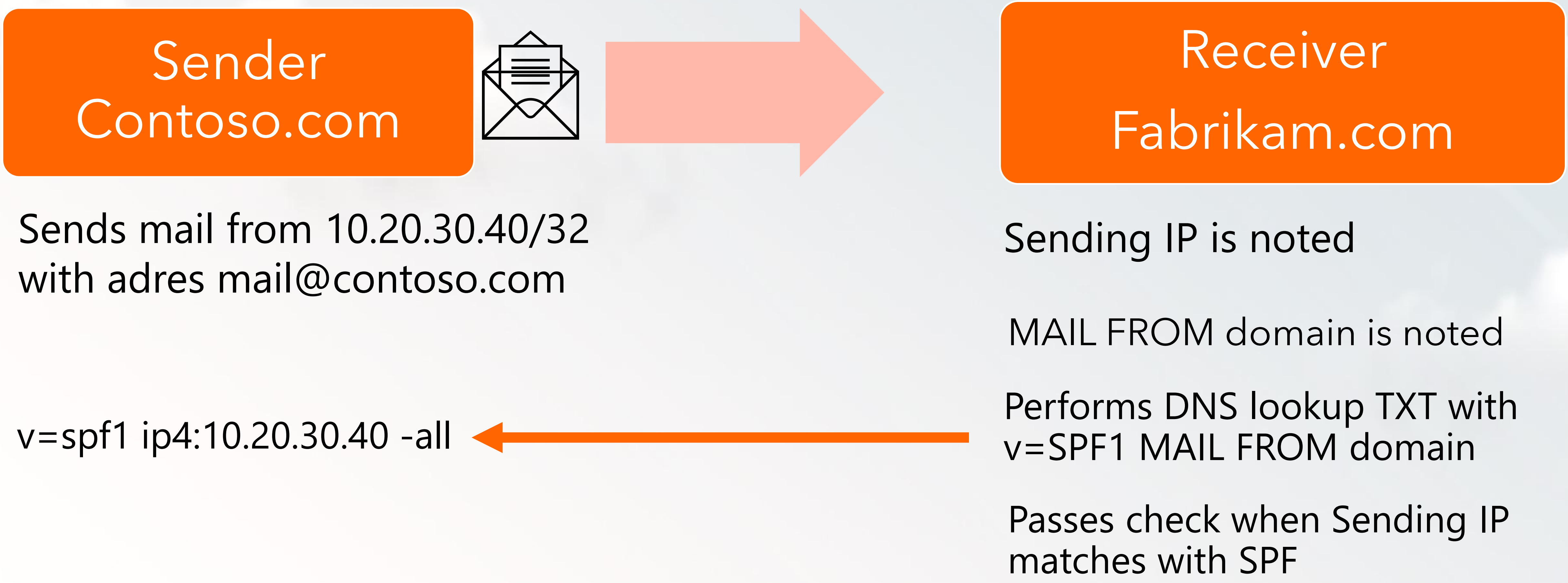
Applications

Integration

Data

Managed Cloud Services

SPF flow



Sender
Contoso.com

Receiver
Fabrikam.com

Sends mail from 10.20.30.40/32
with adres mail@contoso.com

v=spf1 ip4:10.20.30.40 -all

Sending IP is noted

MAIL FROM domain is noted

Performs DNS lookup TXT with
v=SPF1 MAIL FROM domain

Passes check when Sending IP
matches with SPF

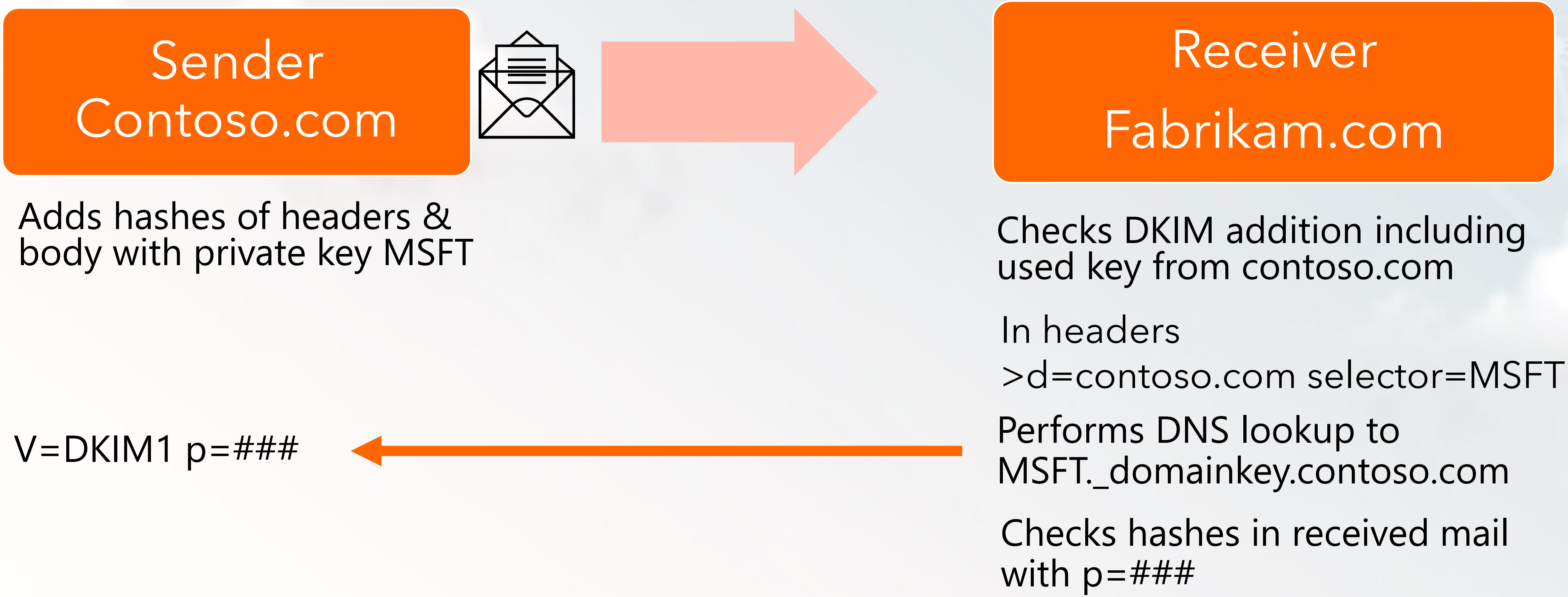
SPF TXT record syntax

v=spf1 a:mailserver.nl ip4:123.12.254.254 include:_spf.mail.nl –all

Match	
IP4	Ipv4 address or range
IP6	Ipv6 address or range
A	DNS A records for domain
MX	DNS MX records for domain
INCLUDE	Include spf of other domain
ALL	Always matches (catch all).

Action	
+	Pass (default, can be omitted)
-	Fail
~	Softfail
?	Neutral

DKIM flow



Sender

Contoso.com

Receiver

Fabrikam.com

Adds hashes of headers & body with private key MSFT

Checks DKIM addition including used key from contoso.com

In headers
>d=contoso.com selector=MSFT

Performs DNS lookup to MSFT._domainkey.contoso.com

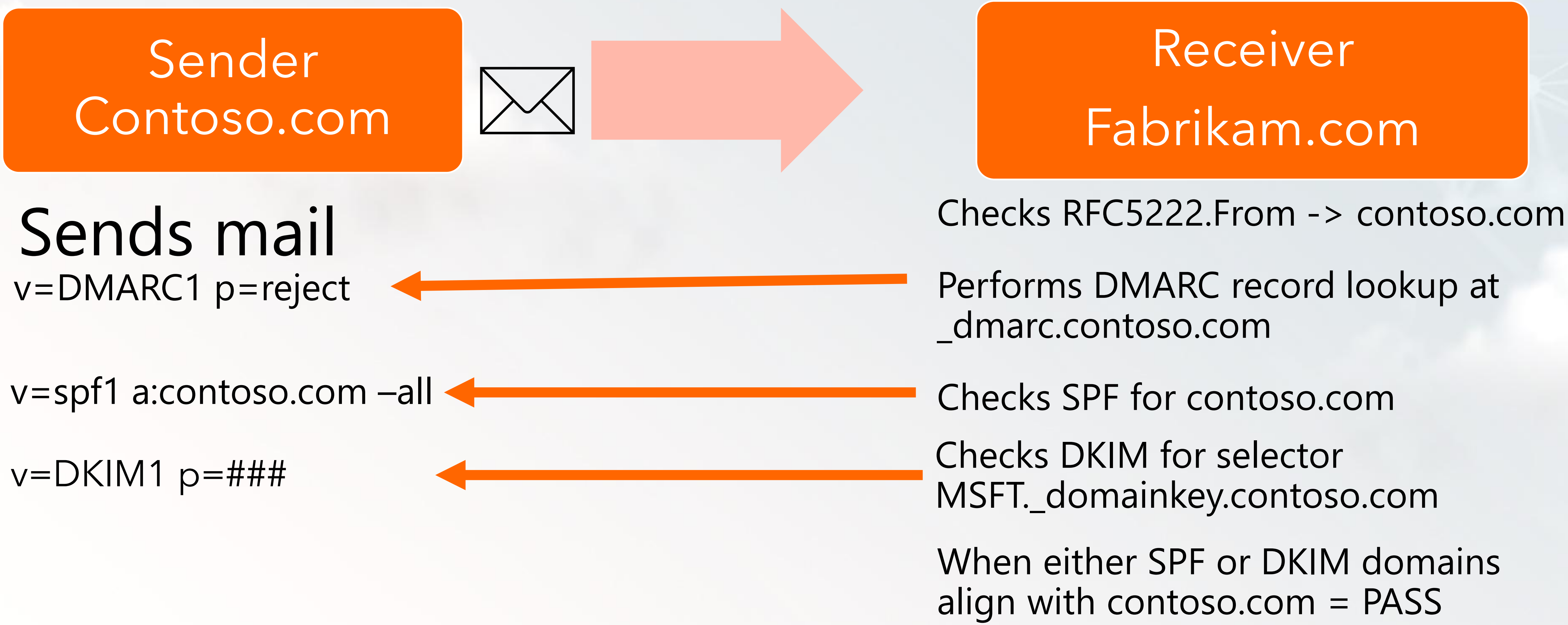
V=DKIM1 p=###

Checks hashes in received mail with p=###

FQDN	CNAME Value
selector1._domainkey.contoso.com	selector1-contoso-com._domainkey.contoso.onmicrosoft.com.

```
v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb2DQEBAQUAA4GNADCBiQKBgQDL1xw0fG6
C0rqT14zUenYz4fbYC0JYq6SwyntswYUebqYfmo9zlGZp+tJo4sEFIl9oI
K3pH0xCN5dlIslYG5APhDsqNlelQ6VzX16uZxPKjd7EL11Z3ii/CxX1EtL
CF6CCOgQ1JmS0zps1+6/Xu+DonulN9pfJPk4V4iTSJaNMkwIDAQAB
;n=1024,1453500350,1
```

DMARC flow



Sender
Contoso.com

Receiver
Fabrikam.com

Sends mail

v=DMARC1 p=reject

v=spf1 a:contoso.com –all

v=DKIM1 p=###

Checks RFC5222.From -> contoso.com

Performs DMARC record lookup at _dmarc.contoso.com

Checks SPF for contoso.com

Checks DKIM for selector MSFT._domainkey.contoso.com

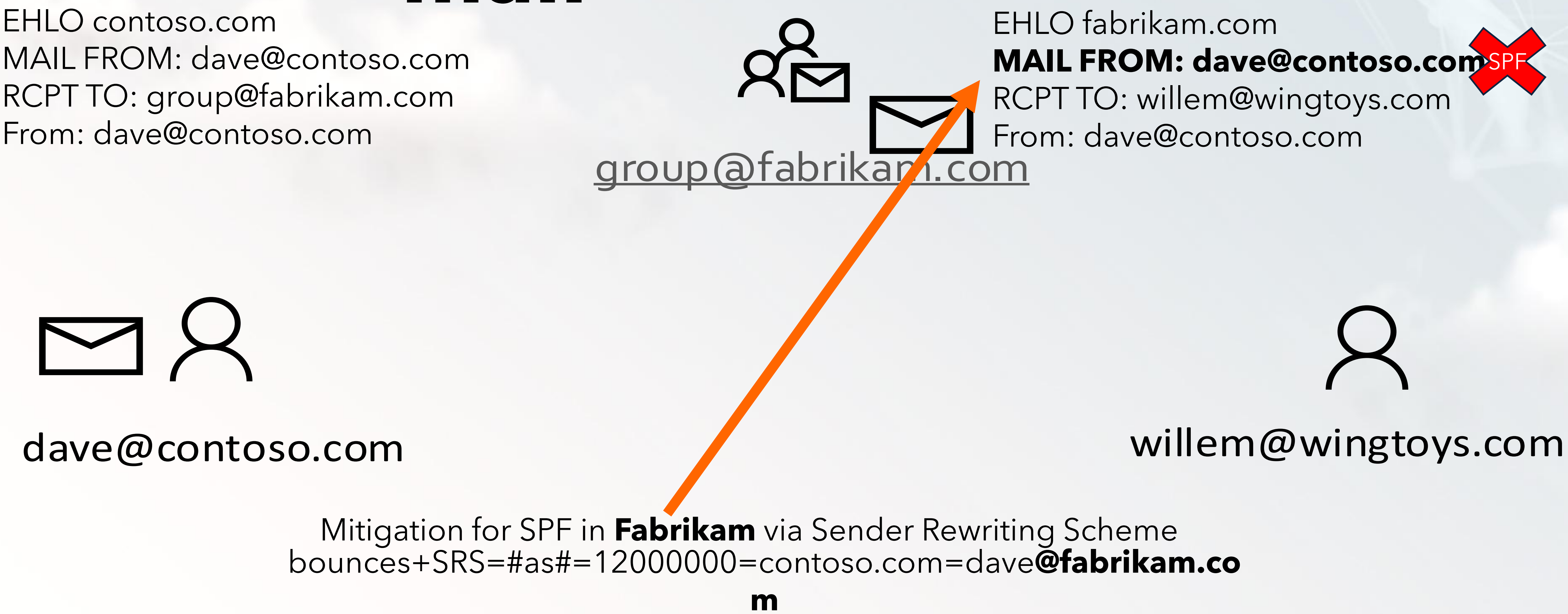
When either SPF or DKIM domains align with contoso.com = PASS

v=DMARC1; p=quarantine; sp=reject; rua=mailto:rua@contoso.com; ruf=mailto:ruf@contoso.com; fo=1; pct=50

TXT record on _dmarc.contoso.com

Tag	Short description	Value	Required?/default
V	Protocol version, for now its version 1	DMARC1	Required
P	Policy for organizational domain	None, Quarantine, Reject	Required
SP	Policy for subdomains of the organizational domain	None, Quarantine, Reject	Optional, if not explicitly defined SP is same as P
PCT	Percentage of messages subjected to filtering	0-100	Optional (default is 100)
FO	Reporting options	0,1,d,s	Optional
RUF	For reporting of forensic reports	Mail address	Optional (Required if FO= is used)
RUA	For reporting of aggregate reports	Mail address	Optional

Forwarding mail



EHLO contoso.com
MAIL FROM: dave@contoso.com
RCPT TO: group@fabrikam.com
From: dave@contoso.com

group@fabrikam.com

EHLO fabrikam.com
MAIL FROM: dave@contoso.com
RCPT TO: willem@wingtoys.com
From: dave@contoso.com

dave@contoso.com

willem@wingtoys.com

Mitigation for SPF in **Fabrikam** via Sender Rewriting Scheme
bounces+SRS=#as#=12000000=contoso.com=dave**@fabrikam.co
m**

Microsoft Partner

Rubicon

Forwarding mail

EHLO contoso.com
MAIL FROM: dave@contoso.com
RCPT TO: group@fabrikam.com
From: dave@contoso.com

group@fabrikam.com

Adds ARC-Seal to mails

EHLO fabrikam.com
MAIL FROM:
bounces+SRS ..
dave@fabrikam.com
RCPT TO: willem@wingtoys.com
From: dave@contoso.com ~~DMARC~~

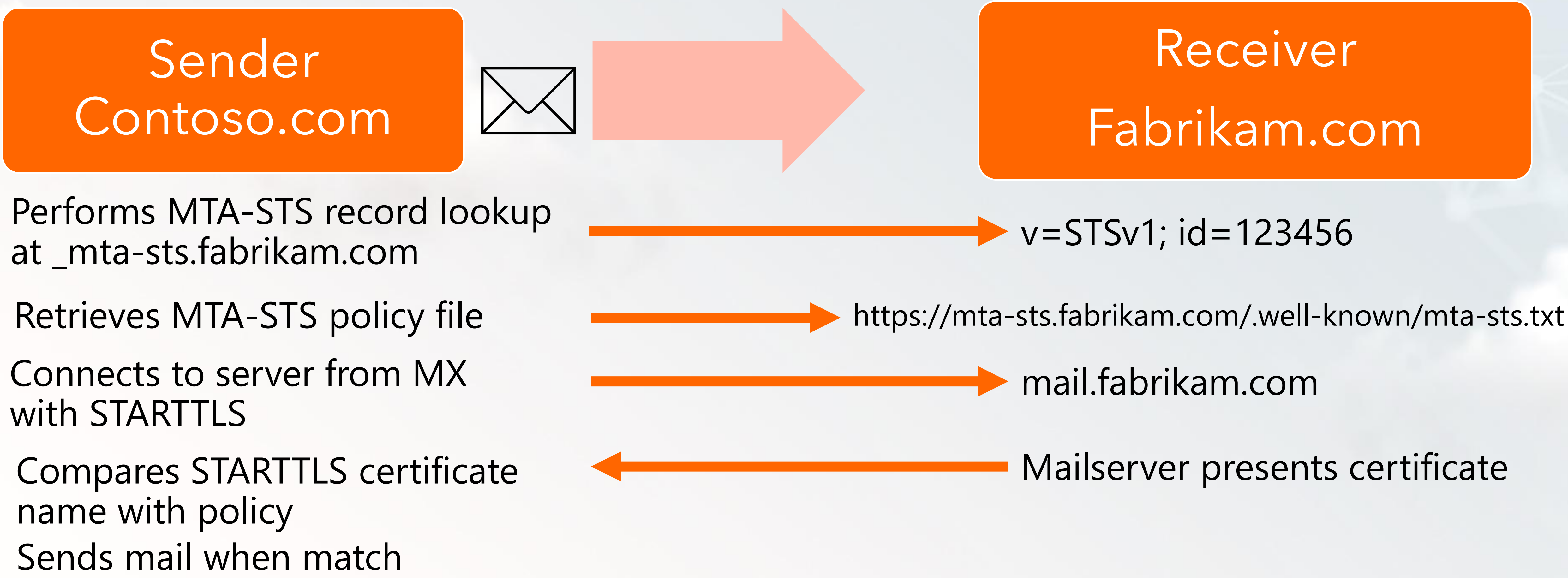
Trusts fabrikam as ARC intermediary

dave@contoso.com

willem@wingtoys.com

SRS fixes SPF checks, but still fails DKIM and DMARC checks

MTA-STS flow



Sender
Contoso.com

Receiver
Fabrikam.com

Performs MTA-STS record lookup at _mta-sts.fabrikam.com → v=STSv1; id=123456

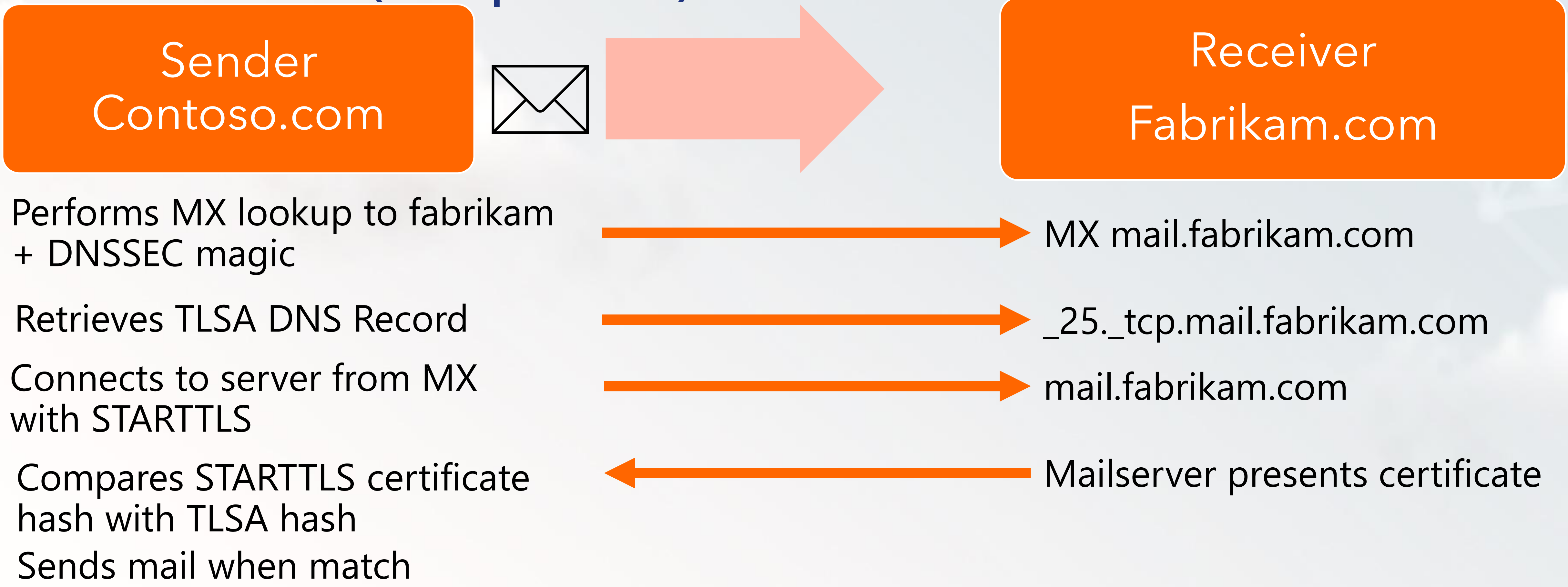
Retrieves MTA-STS policy file → https://mta-sts.fabrikam.com/.well-known/mta-sts.txt

Connects to server from MX with STARTTLS → mail.fabrikam.com

Compares STARTTLS certificate name with policy ← Mailserver presents certificate

Sends mail when match

DANE flow (simplified)



Sender
Contoso.com

Receiver
Fabrikam.com

Performs MX lookup to fabrikam + DNSSEC magic → MX mail.fabrikam.com

Retrieves TLSA DNS Record → _25._tcp.mail.fabrikam.com

Connects to server from MX with STARTTLS → mail.fabrikam.com

Compares STARTTLS certificate hash with TLSA hash ← Mailserver presents certificate

Sends mail when match