VALIMAIL

EMAIL AUTHENTICATION HANDBOOK

A Guide to SPF, DKIM, DMARC, ARC, and BIMI – by the Inventors of Automated DMARC



INTRODUCTION

This Guide Was Written By The Experts At Valimail

With deep expertise in Internet security and resilient infrastructure, the Valimail team regularly contributes to these standards and actively participates in threat detection communities — driving today's email authentication policies and tomorrow's cybersecurity advancements.

Table of Contents

01 **INTRODUCTION** **02**

It's Surprisingly Easy To Fake An Email 04

What Do These Five Standards Solve For? 05

02 **SPF** **06**

How It Works 07

Implementation Challenges 08

Limitations 08-09

03 **DKIM** **10**

How It Works 11

DKIM-Signature Header 12

Limitations 13

Implementation Challenges 14

04 **DMARC** **15**

Why Do We Need It? 16

Limitations 17

DMARC Records 17

DMARC Tags 18-20

6 Steps For Operationalizing Email Authentication With DMARC 21-28

05 **ARC** **29**

Why Do We Need It? 30

How It Works 30-31

06 **BIMI** **32**

How Does BIMI Work? 33

07 **CONCLUSION** **34**

Additional Resources 35

It's surprisingly easy to FAKE AN EMAIL

When the Internet and email were first created, they were only accessible to a handful of people, so there was no room for impersonation. Email's inventors didn't know how popular and central to business and transactions email would become, so they didn't include any way to verify an email sender's identity; email headers, including the "From:" and "Reply-to:" fields, are therefore remarkably easy to fake.

ENTER EMAIL AUTHENTICATION

By implementing email authentication, you enable only those senders that you explicitly authorize, thereby blocking everyone else who attempts to send in your name — spammers, phishers, and "shadow email" senders that may be legitimate but have not been vetted or authorized. This provides CIOs and CISOs with a significant new weapon to control shadow IT.

Email authentication collectively refers to the open Internet standards that validate email senders:

- **SPF** (Sender Policy Framework)
- **DKIM** (DomainKeys Identified Mail)
- **DMARC** (Domain-based Message Authentication, Reporting, and Conformance)
- **BIMI** (Brand Indicators for Message Identification)
- **ARC** (Authenticated Received Chain)

EMAIL AUTHENTICATION TIMELINE

NOW | ARC and BIMI
Extend reach of email authentication

2012 | DMARC
Builds on SPF and DKIM to prevent fraud

2007 | DKIM
Cryptographic and signature of message

2003 | SPF
Whitelist of authorized servers

What Do These Five Standards Solve For?

The five key standards solve the fundamental flaw of email: It can't be trusted. Each standard restores trust in a different way.

FIVE KEY STANDARDS OF EMAIL AUTHENTICATION



SPF

Validates if the sender is on the domain's allow list

DKIM

Validates the message and sender using PKI

DMARC

Ensure that the domain the user sees in the visible From: has been authenticated by SPF and/or DKIM

ARC

Allows authentication information to survive complex routing, so even forwarded messages and mailing list messages can be validated

BIMI

Lets domain owners specify which image appears alongside authenticated messages in recipients' inboxes



01 SPF

WHAT IS SPF?

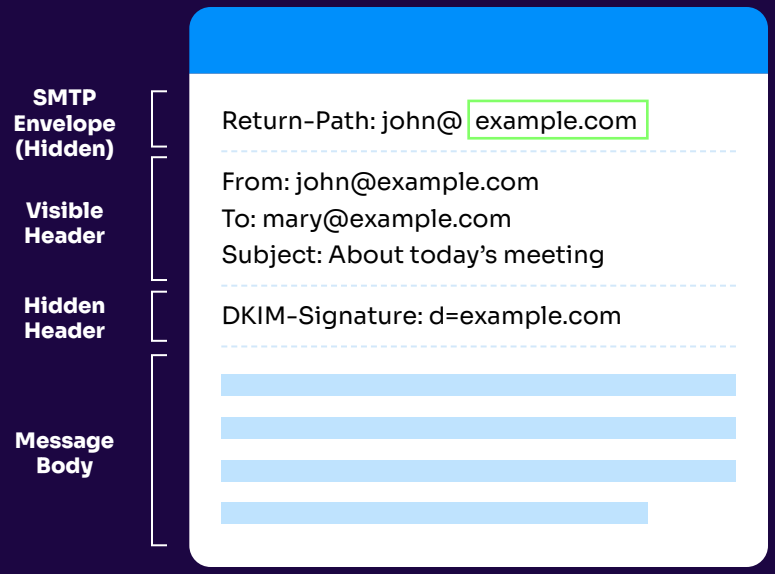
Sender Policy Framework is the standard that pioneered the concept of domain-based email authentication. SPF lets domain owners publish a list of approved IP addresses. If a mail server with an IP address that's not on the list tries to send email using that domain, it won't pass SPF authentication.

HOW IT WORKS

- Domain owners publish SPF records to the Domain Name System (DNS) that spell out the rule sets for their domains. An SPF record is plain text, and it can be as simple as a single line listing the IP addresses that are allowed to send email on the domain's behalf.
- When an email server receives an incoming email, it examines the domain shown in the message's Return-Path.
- Using DNS, it checks to see if there is an SPF record for that domain.
- If there is a record, the receiving server then checks the IP address of the mail server that sent the message to figure out if it matches the SPF rules.
- If there's a match, the email passes the test and, in most cases, is delivered to the user's inbox.
- If not, the receiving server will typically reject the message or add a flag to it, to mark it as suspicious.

How SPF works

Receiver validates the sender against the IP whitelist associated with the "Return-Path:" domain from the SMTP envelope



IMPLEMENTATION CHALLENGES

SPF records are text, but the syntax is a little tricky and it can be easy to make typos or other errors that are hard to spot, rendering the SPF record useless.

The rules ("mechanisms" in the language of SPF) can be quite a bit more complicated than lists of IP addresses. For example, an SPF record can include:

- A list of specific permitted IP addresses or net blocks (ranges of IPs).
- Rules that point to other types of DNS records. For instance, "if the MX record or the A record for the sending server contains a specific IP address, let the message pass."
- "Include" mechanisms that reference SPF rules controlled by another entity. For example, if you are using Google's G Suite and you want to enable SPF for the mail sent by Gmail (as well as email notifications sent by Google Docs, Google Calendar, and so on) you would add "include:_spf. google.com"to your SPF record. This tells mail servers to do an additional DNS lookup for _spf. google.com to find additional SPF rules listed there.

There are no notification mechanisms in place: so if something goes wrong with your implementation of any of the above items, it's up to you to figure out when, why, and how it happened.

LIMITATIONS

- SPF contains a limit on the number of DNS lookups that mail servers will do when evaluating an SPF record, aka the 10-domain lookup limit. 10 lookups can go pretty quickly, particularly because one lookup might contain other lookups of its own. For instance, at the time this was published, "include _spf.google.com" actually comprises four different lookups, because the SPF record at _spf.google.com contains three more lookups of its own
- SPF only lets you know that a message came from an approved IP, but IPs do not always represent a one-to-one relationship. Shared systems could use the same IP address. Or if the IP identifies a service that you authorize, say MailChimp, then anyone using the same IP address on that system could send messages that authorize with your SPF record.

LIMITATIONS (CONT'D)

- SPF uses the domain shown in a message's Return-Path field for authentication, not the "From:" address that humans can actually read. This creates three issues:

1. The "From:" address can still be spoofed



2. The Return-Path is used to indicate where bounce messages should go, so the "From:" and Return-Path domains may differ. Most mail clients do not display the Return-Path address by default.

   - For example, if you're sending mail through a mailing list, the "From:" field might show your address, while the "Return-Path:" field shows the address of the email list.

3. Phishers can use the general invisibility of "Return-Path:" to set up their own domains with their own SPF records. Then they can send out phishing emails with a company's domain showing in the "From:" field but the phisher's own domain in Return-Path. Such messages are fake, but they will pass SPF authentication.

   - SPF does not inherently support email forwarding. Any SPF records from senders trying to reach you through a forwarding address won't validate, because to the receiving server, it looks like the message is coming from the forwarding server, not the source.

SPF is an essential part of email authentication, but it wasn't designed for the cloud era. In the absence of a DMARC record, how receiving servers handle a message that fails SPF is entirely up to them.



02 DKIM

WHAT IS DKIM?

DomainKeys Identified Mail uses public key cryptography to authenticate individual email messages. And unlike SPF, DKIM signatures can survive most forwarding:

If the contents of the signed headers and message are not altered, the DKIM signature will still work.

DKIM is a stronger method of authentication than SPF because it survives most forwarding and you can ensure the message has not been tampered with in transit.

HOW IT WORKS

- The domain owner creates a cryptographic public-privatekey pair, and places the public key in a DNS record at alocation specified by the message's DKIM header, whichincludes a domain name and a "selector."
- The server sending an email message digitally signs the message in a way that cryptographically combines a hash of the contents of the message (including its main headers) with a secret, private key that only the sender has access to.
- The result is a signature that the server attaches to the message, as part of a DKIM header field that tells recipientswhere to find the public key (by domain and selector)corresponding to the private key used to sign the message.
- Receiving servers use DNS to retrieve the public key found at the indicated domain and selector, then use that key to decrypt the signature and validate that the hash matches the locally computed hash of the message.
- If there's a match, then the message hasn't been tampered with since it was signed, and the recipient knows exactly which domain and selector it was signed by.
- Using DNS allows domain owners to authorize specific senders, by placing public keys in separate selector records (so a single domain could have many selectors, each one for a different sender). This allows for many different services to send on behalf of the domain without all needing to share the same private key.

Here's an example of a DKIM-Signature header



HERE'S WHAT THIS HEADER INDICATES:

d= indicates the domain

s= indicates the selector that mail servers will use to find the appropriate DKIM key

h= shows the list of headers covered by the signature

bh= is the signature covering those headers

b= is the digital signature for the message body

LIMITATIONS

- DKIM was built as an anti-spoof tool, not an anti-fraud/phishing mechanism. To stop phishing, the most important address is the domain in the From field. This is what humans use to determine who or what a message is coming from. The domain used to sign a message could be completely different from the domain shown in the From field.
- The security of DKIM depends on the operational security of the private key used to sign messages. If a hacker were to get ahold of a domain's private key, he or she could start signing messages as that domain, and they would pass DKIM validation perfectly. Worse, the domain owner might have no idea that this is happening.
- DKIM signatures don't require any kind of connection to the mail servers controlled by the domain owner. Attacks could be executed from anywhere in the world with the domain owner remaining in the dark.

Simplify DKIM Management With Valimail

A single DNS change

Track the age of each DKIM key for easy rotation

No more IP addresses or net blocks

IMPLEMENTATION CHALLENGES

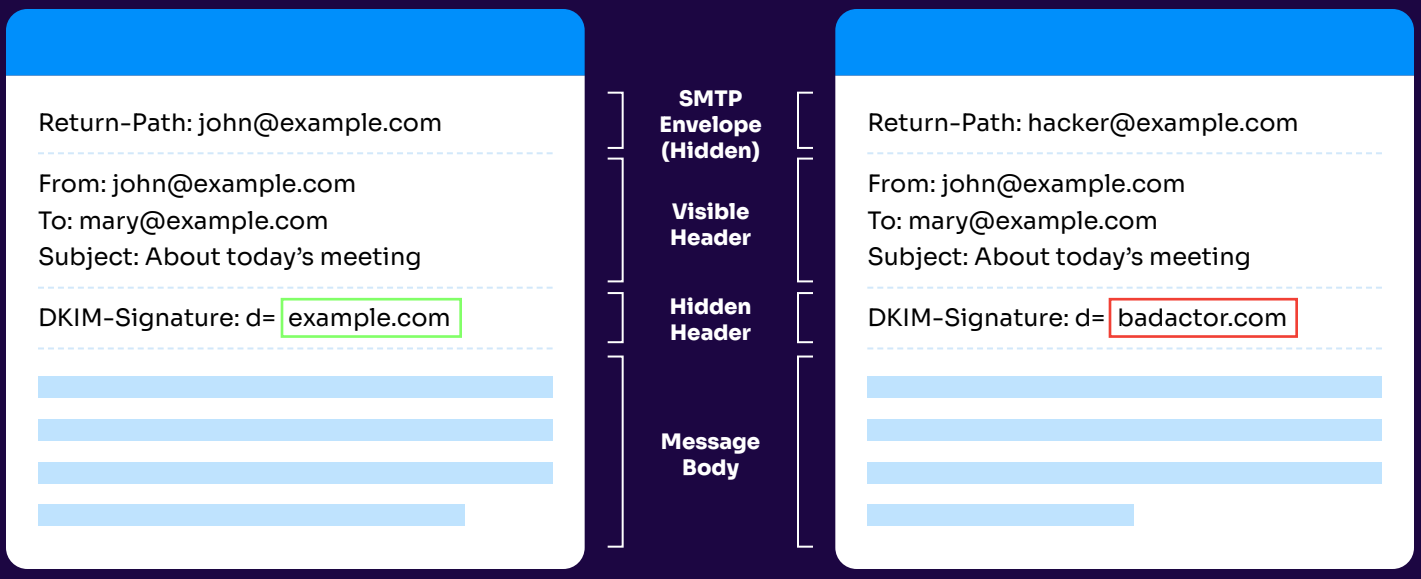
DKIM key management is vital for providing true security and protection. Email senders need to understand the significance of different DKIM key lengths (longer keys are more secure). They need to track the age of specific keys so they can rotate them regularly. In many cases, this is not happening. And while senders could manually create individual DKIM key records for each email service they use, they often don't, meaning all services use the same key, making tracking impossible.

How DKIM Works

Receiver validates the DKIM-Signature with a public key stored in DNS at the "d=domain" in the hidden header

But Messages Passing DKIM Can Still Be Spoofed

Receivers only check a hidden header that may not match the domain people see in the visible <From:> field as in the example below





03 DMARC

WHAT IS DMARC?

Domain-based Message Authentication, Reporting and Conformance builds on SPF and DKIM to stop exact-domain email spoofing by matching what is checked by SPF and DKIM with what the end user actually sees — The “From:” header field.

WHY DO WE NEED IT?

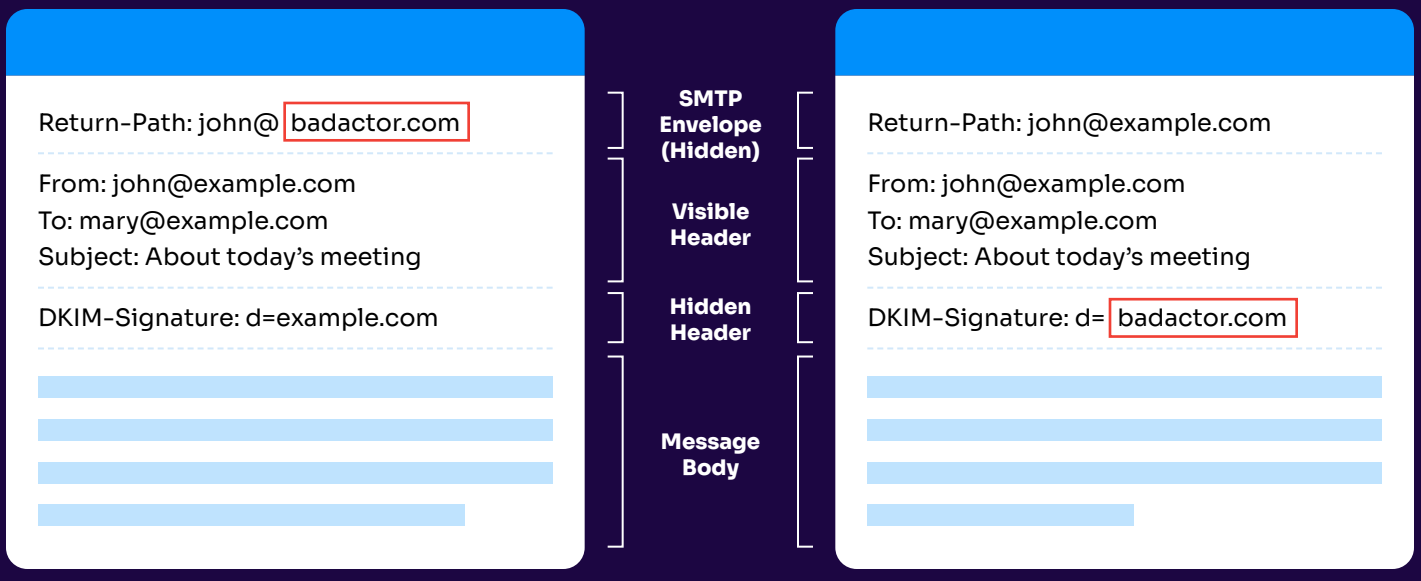
Neither SPF or DKIM authenticate the sender against the “From:” field that users see. The policy specified in a DMARC record will require that the DKIM key’s domain (or the SPF verified sender) and the domain shown in the “From:” address are “aligned,” i.e. that they match. This prevents phishers from using a bogus domain in the “From:” address while signing the message with an unrelated domain that they control. This simple check provides an enormous amount of protection that has not previously existed for email.

Email Messages Passing SPF Can Still Be Spoofed

Receiver only check the <Return-Path> domain and this may not match the domain people see in the visible “From:” field, as in the example below

Email Messages Passing DKIM Can Still Be Spoofed

Receivers only check a hidden header that may not match the domain people see in the visible <From:> field, as in the example below



DMARC provides global visibility into senders using your domain and their authentication status. It also allows domain owners to set a policy for what mail servers should do with unauthorized emails.

LIMITATIONS

There is a small percentage of messages that will still fail authentication after being forwarded or passed through a mailing list. This problem is addressed by implementing ARC.

How Does DMARC Work?

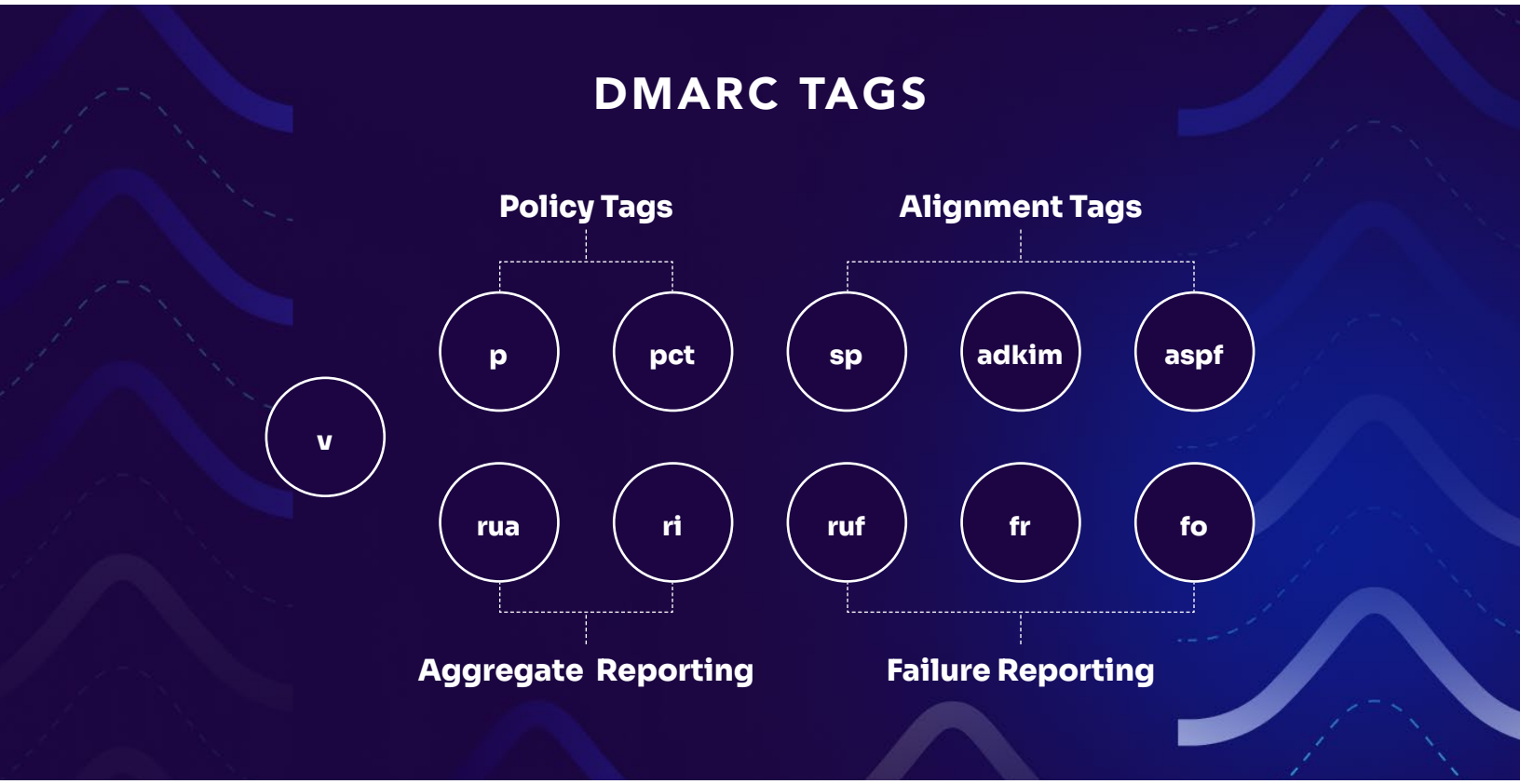
1. Email is received for delivery
2. Receiver checks authentication of the message using both SPF and DKIM, by:
   a. checking the sending IP of the message against the SPF record and/or
   b. validating the message using the sender's published DKIM key
3. Receiver validates DMARC alignment for the message:
   a. if SPF authentication passed, and the domain checked matches the domain in the visible From, then DMARC passes and/or
   b. if DKIM authentication passed, and the domain checked matches the domain in the visible From, then DMARC passes
   c. Otherwise, DMARC fails
4. If the email fails DMARC, receivers take action based on the policy specified in the domain owner's DMARC record:
   a. do nothing (p=none)
   b. send it to spam (p=quarantine)
   c. reject/delete it (p=reject)
5. Once a day, receiver sends a report to DMARC domain owner listing the authentication status for all senders using that domain

DMARC RECORDS

A DMARC record is inserted as a TXT record alongside your other DNS records.

Example Record:

```
_dmarc.example.com IN TXT
"v=DMARC; p=none;
rua=mailto:marc-@example.com
```



DMARC TAGS

- Only three tags are needed to effectively use DMARC ('v=', 'p=', and 'rua=')
- Only the 'v=DMARC1' tag is case sensitive
- Tags 'v=' and 'p=' must be set as the first and second position
- All other tags are optional and can be placed in any order
- Primary domain policies apply to subdomains unless a subdomain policy is explicitly defined
- You may have one and only one DMARC TXT record on a domain or subdomain; multiple records are treated as if there is no DMARC record at all.

REQUIRED TAGS

"v=DMARC1"

Identifier of a DMARC record. "I'm a DMARC record and you can use me to discover policy."

"p="

The "policy" tag tells the receiver what to do with a message that fails DMARC authentication. There are three values.

- **"p=none"** - receiver takes no action
- **"p=quarantine"** - receiver will treat the email as suspicious and send it to spam/junk folder
- **"p=reject"** - receiver rejects the email (does not deliver it)

OPTIONAL BUT RECOMMENDED TAGS

“rua=mailto:address@company.com”

Tells the receiver where to send the DMARC Aggregate reports.

Aggregate reports provide the most valuable information available through DMARC. They contain daily summaries of all the senders worldwide using your domain, and their authentication status.

Note: In order to get DMARC’s visibility benefit, you must define a reporting address. A p=none record with no reporting is the same as no record at all.

OPTIONAL TAGS

In most cases, a well-formed DMARC record only needs the previous three tags, while the remaining tags are not normally needed.

sp

Defines the policy for subdomains.

Subdomains will inherit the parent policy by default.

In general, you want your domains and subdomains to be covered by the same policy, so this tag isn’t needed unless you have subdomains that need different policies than the parent domain.

adkim

Indicates strict or relaxed DKIM identifier alignment.

The default is relaxed.

With a relaxed policy, DMARC alignment will pass if the organizational domains in the visible From and what is authenticated by DKIM. With strict alignment, a message that authenticates as email.example.com would fail DMARC alignment if the visible From was @example.com instead of @email.example.com.

aspf

Indicates strict or relaxed SPF identifier alignment.

The default is relaxed.

With a relaxed policy, DMARC alignment will pass if only the organizational domains in the visible From and what is authenticated by SPF match. With strict alignment, the subdomains also need to match: For example, a message that authenticates as email.example.com would fail DMARC alignment if the visible From was @example.com instead of @email.example.com.

OPTIONAL TAGS (CONT'D)

pct

The percentage of messages to which the DMARC policy is to be applied.

The default value is 100 so all messages are subject to the policy.

Changing the percentage to anything less than 100 gives imposters the opportunity to bypass your specified policy. For instance, at 80 percent, you'll have no control over which 80 percent of the messages will be subject to the policy.

ruf=mailto:address@company.com

Tells receivers where to send DMARC failure reports.

If not specified, receivers will not send failure reports.

Failure reports, aka forensic reports, are generated each time a message fails authentication. They may include the full contents of the failing email, and therefore may include PII. Because of the risk of PII exposure, none of the major mailbox providers (e.g. Google, Microsoft, Yahoo, etc.) generate these reports any more.

Fo

Failure reporting options: specifies which failed messages will trigger a failure report.

By default, failure reports are generated if all underlying authentication mechanisms fail.

None of the major mailbox providers (e.g. Google, Microsoft, Yahoo, etc.) generate these reports.

rf

Format for message failure reports.

Currently, only one format is available: AFRF

None of the major mailbox providers (e.g. Google, Microsoft, Yahoo, etc.) generate these reports. And if an ruf address is specified, failure reports will be sent in the AFRF format.

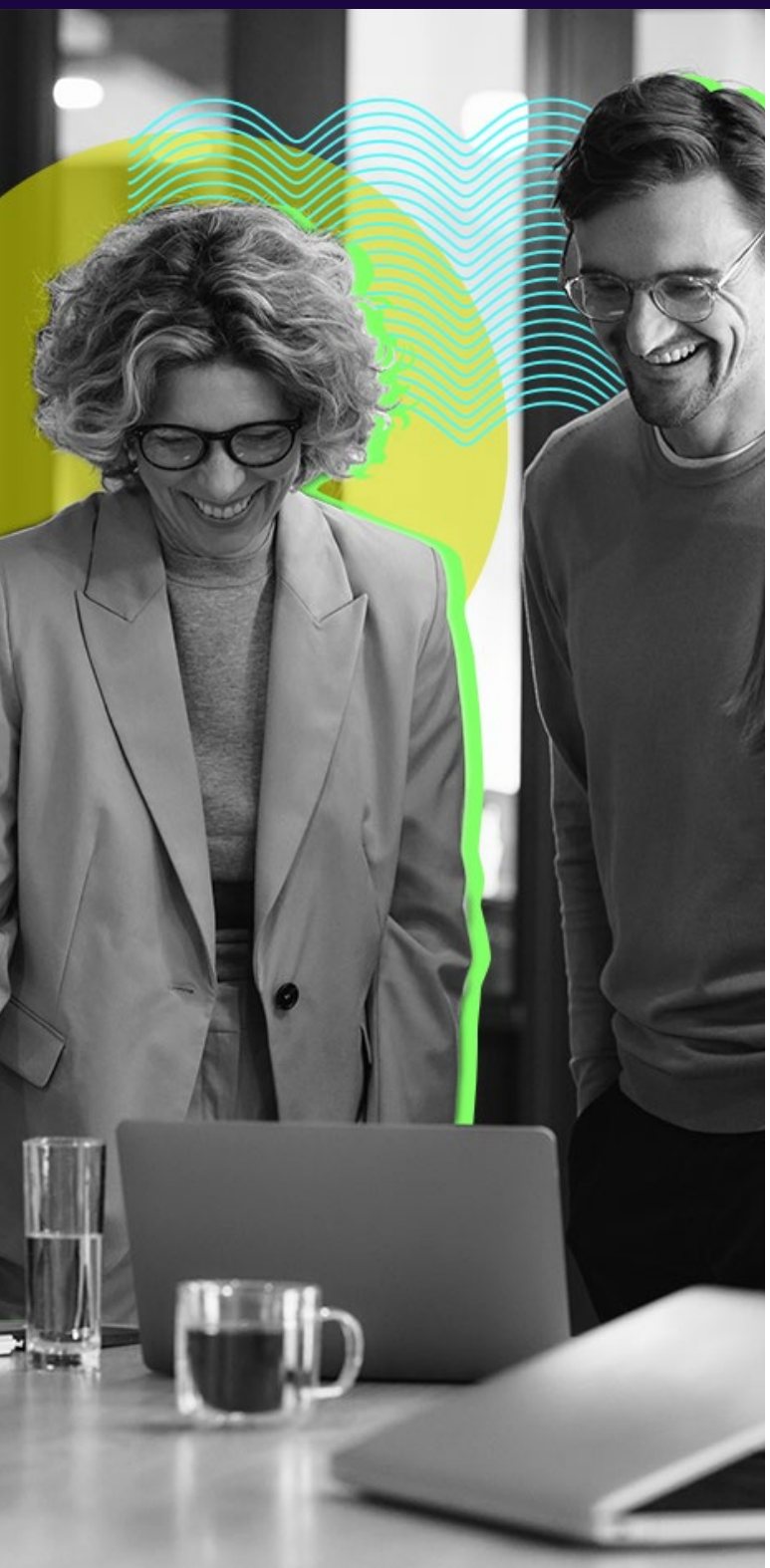
ri

The number of seconds elapsed between sending aggregate reports.

The default value is 86400 seconds, which means reports are sent once per day.

6 STEPS

for Operationalizing Email Authentication with DMARC



IMPLEMENTING EMAIL AUTHENTICATION WITH DMARC (AND ITS CHALLENGES)

IT teams often underestimate the challenges of implementing DMARC, which leads to a lot of wasted effort — without actually achieving the protection that DMARC enforcement provides.

This six-step framework will help you understand what it takes to get to enforcement.

VALIMAIL

Step 1: Gain Visibility

IMPLEMENTATION

Create a p=none (monitoring mode) DMARC record and specify an aggregate reporting address

Translate and analyze DMARC aggregate reports

CHALLENGES

p=none provides great data but does NOT provide protection

THE BENEFIT

Inventory of all senders using your domain

CAUTION

Analysis is time-consuming

If you overlook or misidentify senders you can wind up blocking “good” emails when you move to enforcement

Step 2: Manage Shadow IT and Business Stakeholders



IMPLEMENTATION

Work with internal stakeholders to identify owners for each service

Categorize sending services: authorized, unauthorized, and malicious



RECOMMENDATION

Document an implementation policy that you can share with stakeholders using your domain

Step 3: Configure Services and their Authentication Records

With the information collected from step 2, for each authorized service sending as you, you're ready to configure each of them to work with DMARC.

IMPLEMENTATION

Work with the service to ensure they can send in an aligned manner

Acquire and publish appropriate SPF and/or DKIM records for each service

CHALLENGES

Not all vendors are equipped to support SPF and/or DKIM with alignment

DKIM is the stronger authentication method of the two

CAUTION

SPF and/or DKIM must be correct for DMARC to work

Each service must be authenticated via SPF or DKIM, but both are not required The SPF 10-lookup limit might be a problem

Even a small typo can render your configuration ineffective

Step 4: Broadcast the Program



IMPLEMENTATION

Publicize the intended results and benefits

Announce your implementation policy

Step 5: Move to Enforcement

IMPLEMENTATION

p=quarantine: unauthorized emails are marked as spam

p=reject: unauthorized emails are completely rejected by the receiving server

RECOMMENDATION

Start with p=quarantine and monitor DMARC aggregate reports for about thirty days. Once you're sure you're not blocking any good emails, move to p=reject

Step 6: Monitoring, Reporting, and Ongoing Configuration

The authentication program doesn't stop when you reach enforcement.

IMPLEMENTATION

Monitor for new or changing services

Update configurations as needed

Communicate with SIEM platforms for enhanced security intelligence

CHALLENGES

If you used a workaround for the SPF 10-lookup limit, you'll need to ensure your SPF record stays up to date with any third-party sender changes

CONCLUSION

If you use these steps as a framework for your authentication program, the outcome is well worth the effort.

DMARC at enforcement will help you:

- Stop exact-domain impersonation
- Identify and control shadow IT
- Protect your brand

Or With Valimail, You Could Be Done

A single DNS change

Identify authorized sending services

Authorize and deauthorize services with a single click

Achieve enforcement in 1/3 of the time



04 ARC

WHAT IS ARC?

The **Authenticated Received Chain** protocol provides an authenticated “chain of custody” for a message, allowing each entity that handles the message to see what entities handled it before, and to see what the message’s authentication assessment was at each step in the handling.

ARC allows receivers to make delivery decisions for email that has been routed in a complex way. These decisions can be based upon authentication seen along the chain instead of rejecting the message outright.

WHY DO WE NEED IT?

ARC solves one of the last remaining obstacles to widespread DMARC adoption: The difficulty that email authentication has when mail is sent via an intermediary, either through a forwarders or through a mailing list. Although this problem affects less than one percent of overall email volume, it can cause DMARC authentication to fail when it shouldn't.

HOW IT WORKS

ARC allows intermediaries to attach and sign authentication information they receive, creating a chain of signatures. Receivers can then validate every step of the chain, all the way back to the originating server. If the receiver trusts all of the intermediaries, all the signatures validate, and the mail was properly authenticated at the beginning of the chain, then the receiver can make a delivery decision.

Current Practice

SPF and DKIM break mailing lists making the email undeliverable

From: john@example.com
To: mailinglist@listserver.com
Subject: This Week's Mailing List

DKIM-Signature: d=example.com

Sent to Mailing List

From: mailinglist@listserver.com
To: recipients@whatever.com
Subject: This Week's Mailing List

DKIM-Signature: d=example.com

Verifies email passes authentication alignment before sending to list

From: mailinglist@listserver.com
To: recipients@whatever.com
Subject: This Week's Mailing List

DKIM-Signature: d=example.com

Authentication breaks alignment during forwarding process



Email cannot be authenticated

With ARC

Authentication information saved in a wrapper

From: john@example.com
To: mailinglist@listserver.com
Subject: This Week's Mailing List

DKIM-Signature: d=example.com

Sent to Mailing List

ARC Seal

From: john@example.com
To: mailinglist@listserver.com
Subject: This Week's Mailing List

DKIM-Signature: d=example.com

Verifies email passes authentication alignment and inserts ARC seal

ARC Seal

From: john@example.com
To: mailinglist@listserver.com
Subject: This Week's Mailing List

DKIM-Signature: d=example.com

Validates ARC set and determines if forwarder is trusted



If sealer is trusted, apply DMARC override and deliver email

This gives email services a flexible, robust way to handle email authentication even when messages pass through multiple systems that otherwise break authentication.



05 BIMI

WHAT IS BIMI?

Brand Indicators for Message Identification gives brands greater control over how their emails appear in consumer inboxes. Senders can provide brand-specific imagery that appears alongside messages they send. These images appear in place of the user photo or the initial letter that many email clients display next to the sender's name.

In order to use BIMI, senders must be using DMARC withan enforcement policy (quarantine or reject) on theirorganizational domain.

For brands, this is an opportunity to extend the reach andvisibility of their logos or other brand elements. For brands that send high volumes of email, this provides millions to billions offree brand impressions.

HOW DOES BIMI WORK?

Domain Owner:

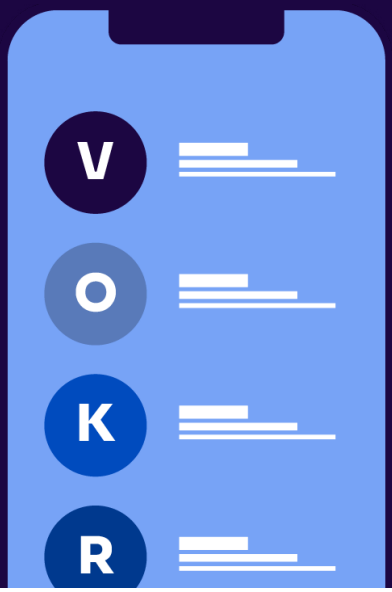
1. In order to use BIMI, senders must be using DMARC with an enforcement policy (quarantine or reject) on their organizational domain.
2. Publish a BIMI record in DNS
3. Publish a validated/trademarked logo

Once the domain owner completes these steps, the receiver will:

1. Check the authentication status of the incoming message
2. If the message passes authentication, the receiver will query DNS for a corresponding BIMI record
3. If a BIMI record and validating logo are present, the receiver can display the logo with the message in the inbox.

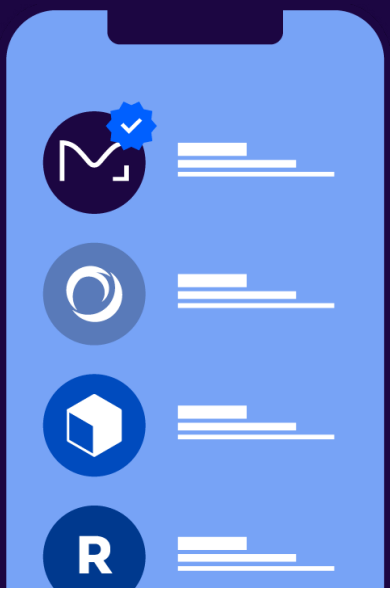
Without Enforcement and BIMI

Your messages are accompanied by suspicious markings and assumed identifiers



With Enforcement and BIMI

Your logo displays clearly in the inbox as mark of trust and authenticity





SPF

Validates if the sender is on the domain's allow list

DKIM

Validates the message and sender using PKI

DMARC

Ensure that the domain the user sees in the visible From: has been authenticated by SPF and/or DKIM

ARC

Allows authentication information to survive complex routing, so even forwarded messages and mailing list messages can be validated

BIMI

Lets domain owners specify which image appears alongside authenticated messages in recipients' inboxes

Together, these standards make email authentication extremely powerful and beneficial for organizations of all sizes.

However, they must be done right. Each standard requires careful configuration of DNS, intimate knowledge of email infrastructure, and constant monitoring and updating to stay current.

VALIMAIL'S SOLUTION

- Fixes built-in standards limitations.
- Auto-detects & classifies email-sending services.
- Authorizes/deauthorizes senders with one click.
- Eliminates iterative & manual DNS changes.
- Flags malicious activity.
- Manages all BIMI records and logos from one unified dashboard.

ADDITIONAL RESOURCES

Free DMARC Monitor account:
valimail.com/dmarc-monitor

Instantly check the status of your DMARC and SPF record:
domain-checker.valimail.com

Updates to the BIMI standard:
bimigroup.org

TRUST YOUR EMAIL

Valimail is the global leader in DMARC-as-a-service, and the inventor of hosted DMARC.