DMARC Architecture - Identifier Alignment

Contents

[Introduction](#)
[Terminology](#)
[DMARC - Identifier Alignment](#)
[Identifiers](#)
[Identifier Alignment](#)
[DKIM Alignment](#)
[SPF Alignment](#)
[Alignment Mode Tags](#)
[Reference](#)

Introduction

This document describes general Domain-based Message Authentication, Reporting and Conformance (DMARC) architecture concepts, along with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) alignment requirements in relation to DMARC.

Terminology

This section describes and provides definition to some of the key terms used within this document.

- **EHLO/HELO** - The commands that supply the identity of an SMTP client during the initialization of an SMTP session as defined in RFC 5321.
- **From header** - The From: field specifies the author(s) of a message. It will typically include the display name (what is shown to an end-user by the mail client), along with an email address that contains a local-part and domain name (For example, "John Doe" <johndoe@example.com>) as defined in RFC 5322.
- **MAIL FROM** - This is derived from the MAIL command at the start of an SMTP session and provides the sender identification as defined in RFC5321. It is also widely known as the envelope sender, return-path or bounce address.

DMARC - Identifier Alignment

DMARC ties what DKIM and SPF authenticate to what is listed in the From header. This is done by *alignment*. Alignment requires that the domain identity authenticated by SPF and DKIM match the domain in the email address visible to the end user.

Let's start with what an identifier is and why they are important in reference to DMARC.

Identifiers

Identifiers identify a domain name to be authenticated.

Identifiers in reference to DMARC:

- SPF:

  SPF authenticates the domain that appears either in the MAIL FROM or EHLO/HELO portion of the SMTP conversation, or both. These may be different domains, and they are typically not visible to the end user.

- DKIM:

  DKIM authenticates the signing domain that is affixed to a signature within the *d*= tag.

These (SPF and DKIM) identifiers are authenticated against the domain identifier derived in the From header. The From header domain is used because it is the most common Mail User Agent (MUA) field for the originator of the message and is the one used by end users to identify the source of the message (a sender), which also makes the From header a prime target for abuse.

> **Caution**: DMARC can protect abuse only against a valid From header.

DMARC can't operate on:

- Malformed, absent or repeated RFC 5322 headers
- Non-compliant headers, as they will not be validated
- When there is more than one domain identity in the header (*)

Therefore, a process in addition to DMARC should exist to identify messages with non-compliant malformed headers and implement a way to mark and make them visible as non-DMARC eligible headers.

(*) DMARC needs to extract a single domain identity from the header. If there is more than one email address in the header than this header will be skipped in most DMARC implementations. Processing headers with more than one domain identity are stated as out-of-scope in the DMARC specification.

When the Cisco ESA is able to detect more than one domain identity it leaves a proper message in the mail logs:

```
(Machine esa.lab.local) (SERVICE)> grep -i "verification skipped" mail_logs

Tue Oct 16 14:13:52 2018 Info: MID 2003 DMARC: Verification skipped (Sending domain could not be determined)
```

Identifier Alignment

Identifier alignment defines a relationship between the domain authenticated by SPF and/or DKIM and the From header. Alignment is a matching process which needs to be additionally met after successful verification of SPF and/or DKIM. The DMARC authentication process requires at least one of the identifiers (domain identity) used by SPF or DKIM to be aligned with the domain portion of the From header address.

DMARC introduces two alignment modes:

- **strict** mode requires an exact match (align) between domain names
- **relaxed** mode allows the subdomain of the same domain

Identifier Alignment is required because a message can bear a valid signature from any domain, including domains used by a mailing list or even a bad actor. Therefore, merely bearing a valid signature is not enough to infer the authenticity of the Author Domain.

DKIM Alignment

DKIM domain identifier is obtained by reviewing the *d*= tag in a DKIM signature, and it is compared with the From header domain to successfully verify a DKIM signature.

As an example, the message can be signed on behalf of domain d=blog.cisco.com, which identifies domain *blog.cisco.com* as a signer. DMARC uses this domain and compares it with the domain part of the From header (For example, noreply@cisco.com). The alignment between these identifiers will *fail* in strict mode but pass using relaxed mode.

> **Note**: A single email can contain multiple DKIM signatures, and it is considered to be a DMARC "pass" if any DKIM signature is aligned and verifies.

SPF Alignment

The SPF (spfv1) mechanism authenticates domain identifiers delivered from:

- MAIL FROM identity (MAIL FROM command)
- HELO/EHLO identity (HELO/EHLO command)

The MAIL FROM domain identity tries to be authenticated by default. The HELO domain identity is authenticated by DMARC only for messages with an empty MAIL FROM identity, like bounce messages.

A common example of this would be where a message is sent with a different MAIL FROM address (noreply@blog.cisco.com) compared to what's in the From header (noreply@cisco.com). The MAIL FROM domain identity part of noreply@**blog.cisco.com** will align with the From header domain of noreply@**cisco.com** in relaxed mode but *not* in strict mode.

Alignment Mode Tags

DMARC alignment modes can be defined on a DMARC policy record using **adkim** and **aspf** alignment mode tags. These tags indicate what mode is required for DKIM or SPF identifier alignment.

Modes can be set to relaxed or strict, with relaxed being the default if no tag is present. This can be set under the tag-value as:

- **r: relaxed mode**
- **s: strict mode**

Reference

- RFC5321 - Simple Mail Transfer Protocol
- RFC5322 - Internet Message Format
- RFC6376 - DomainKeys Identified Mail (DKIM) Signatures
- RFC7208 - Sender Policy Framework (SPF) for Authorizing Use of Domains in Email
- RFC7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)