Domain Alignment for Email Authentication

Authentication is absolutely essential for professional email transmission. If you want to go further than SPF and DKIM and use DMARC, then alignment is obligatory. But even without DMARC, alignment is a correct and important step to implementing an authenticated email.

What is Domain Alignment?

To explain alignment, let's first of all take a step back. Emails always have two sender addresses. On the one hand, there is the sender address which is displayed to the user in his or her email program. This is called the RFC5322.From address, or more simply "header from" or "friendly from". On the other hand, there is RFC5321.MailFrom, which is used in SMTP communication. This address is often also called Envelope-From or MFROM and is saved in the header of the email as "Return-Path".
For the sake of simplicity, when we refer to "From" in the following, then we mean RFC5322.From, whilst when we refer to "Return-Path", then we mean RFC5321.MailFrom.

You can visualize this as being equivalent to a classic paper letter. The "From" is the author indicated on the actual letter. The "Return-Path" is the sender on the envelope in which the letter is sent.
This also makes it clear who will receive the letter back if it cannot be delivered. The email is no different. A notification that an email could not be delivered (also known as a bounce) is returned to the "Return-Path".

Alignment refers to the aligning of the domains used in the two techniques Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to the From address, so that they at least partially match. With a so-called "strict" policy, the domain must completely match, whilst with a "relaxed" policy, a match at the level of the organizational domain is sufficient.

In SPF alignment, the "Return-Path" and the "From" must match. In DKIM alignment, the match between the d-Parameter of the DKIM signature (put more simply: the DKIM domain) and the From is required.

Example:

DKIM d-Parameter: example.com
From: info@news.example.com
Return-Path:
20180816094418 43e6b1a4b6e54342ab2e11b9e290p0eu@bounces.news.example.com

In this example, with a relaxed policy complying with the standard, both SPF and DKIM alignment would be deemed to be present. All three values are based on the organizational domain "example.com". With a strict policy, alignment would not be deemed to be present, because rather than there being an exact match, subdomains are used.

Why is alignment important?

Especially if you do not send your emails yourself, but avail of a service provider such as an email service provider (ESP), an absence of alignment can initially seem quite legitimate. The "Return-Path" refers to the ESP infrastructure, with the "From" indicating the brand responsible for the content of the emails.

However, when you consider the reasons for introducing the email authentication techniques SPF, DKIM, and Domain-based Message Authentication, Reporting and Conformance (DMARC) in the first place, it is clear that the sender can only be considered authentic if the "From" and "Return-Path" and the DKIM domain match.
If we again take the example of a paper letter, things becomes even clearer: You probably would not consider a letter trustworthy if the sender on the envelope (the "Return-Path"), the sender/author in the letter (the "From"), and a final signature under the letter (the DKIM domain) all differed from each other.

DMARC is well known to be based on SPF and DKIM. However, for DMARC to pass, there must also be domain alignment. Even though it is sufficient for passing DMARC to have implemented either SPF or DKIM correctly, including alignment, it significantly reduces authentication errors to implement both.

Conclusion

At the very latest when you want to use DMARC, alignment is an absolute pre-requisite. If you do not want to conduct the technical mailing yourself and prefer to rely on a professional ESP as a service provider, this is unquestionably easiest to achieve if you, as the domain owner, perform a subdomain delegation to the ESP. The ESP can then fully control all authentication techniques and also ensure alignment.

Author: Alexander Zeh, Engineering Manager, Certified Senders Alliance