A Next-Generation Approach to Email Authentication

DNS is a fundamental mechanism to route internet traffic built in the 1980s, prior to the cloud era. Because DNS also happens to be authenticated, easily discoverable, and globally accessible, it became a repository for the three basic elements of email authentication: DMARC, SPF, and DKIM. DNS however, was never built to be an email authentication mechanism and when used as such, is extremely hard to configure and maintain properly, causing over 70 percent of all email authentication projects to fail. A better approach is to build a DNS-based email authentication responder — Valimail Authenticator™ — that solves the many challenges of email authentication in a technically precise manner.

DNS as the source of truth

DNS emerged in the early days of the internet as a static routing mechanism. It is a fundamental part of how systems on the Internet route traffic, emails, data, and other communications from sender to recipient. But DNS can also be used in other useful ways completely detached from its routing functions. As cloud services proliferate, there’s a growing need to have a “source of truth.” Ideally, this source of truth is secure, easy to find, and globally reachable. DNS perfectly fits the bill, and is therefore increasingly being used in this way. In other words, though DNS began and still primarily serves as the internet's phone book (i.e. resolving alphanumeric addresses to IP addresses) its ability to serve as a globally distributed secure database makes it ideal as a source of truth.

One area in which DNS is used as the source of truth is in email authentication, where the email recipient gateway pings the sender’s DNS to ask, “Is this IP address/machine allowed to send as you?” Since the owner of the domain can securely update their DNS, it’s an ideal way to respond back to the recipient with a, “Yes, let that email through” or, “No, block that email, they are not allowed to send as us.” In today’s cloud services world, the ability to manage third-party email senders that send on behalf of an organization has become critical. Companies must be able to entrust best-of-breed third-party SaaS apps to run core business processes such as HR, payroll, finance, or CRM. These cloud services legitimately use the company's email address to drive workflows. Yet criminals also desire to send email impersonating the company's email address — these must clearly be blocked. Email authentication allows CIOs and CISOs to take advantage of DNS to lock down their email ecosystems to improve deliverability of legitimate cloud services and block fraudulent (phish) email. This ensures the integrity and security of the organization, using DNS as the source of truth and maintaining control over the use of email sent purporting to be the organization’s brand.
Leveraging DNS to automate email authentication

Email authentication is comprised of three standards — DMARC, SPF, and DKIM. They reside in a special area of DNS that is simply a group of assigned text fields in which DNS administrators can type any set of characters. Any machine on the internet can read these fields but only the domain owner can create and make changes to the fields. As such, it’s a convenient way to broadcast your list of approved email senders which a receiving server can query. It is important to note that this use of DNS is not connected to the traffic routing portion of DNS in any way. When configured and maintained correctly, these text fields form a global whitelist of approved email senders.

DNS was never built as an email authentication mechanism

DNS was built in the 1980’s and it shows. It is static, hard to work with, and finicky. As any company trying to implement email authentication realizes all too soon, DNS is unfortunately not optimized for today’s email authentication standards, especially in our modern cloud era. In fact, over 70 percent of companies trying to implement email authentication fail. Text fields are extremely fragile and require the precise typing of characters. Any extra spaces or just one wrong character can create serious misconfigurations and worse still, there is no method to validate the entry, because DNS doesn’t offer error handling. Changes are essentially made in a live production system — the global DNS. Worse, this is a never ending process — every addition or revocation of a SaaS app requires yet more DNS changes, resulting in continuous DNS work and the constant attention of scarce infrastructure resources.

The solution: a purpose-built email authentication responder

Valimail was created out of frustration with the current 70-plus percent email authentication failure rates. By pointing SPF, DKIM, and DMARC at a purpose-built DNS-based email authentication responder, most of the obstacles to getting email authentication to work are solved in a technically precise manner. As such, Valimail built Valimail Authenticator and hosted it in globally distributed AWS instances to service our growing list of multinational clients. The client’s DNS is never touched by our Authenticator — the client’s DNS simply refers the incoming authentication request to Valimail. Valimail validates or denies the authentication request based on the client’s global whitelist and provides the requesting server with a precise and accurate response.

“VALIMAIL’s system never touches nor affects client’s DNS, traffic routing, nor any other client system.”

RECEIVING SERVER

Your DNS

Valimail Authenticator™

Yes / No

1. "Ask Valimail.”

2. "Is this email allowed to send as your domain?"

3. "Is this email allowed to send as your domain?"
Impact of Valimail's service on DMARC, SPF, and, DKIM

DMARC
DMARC represents the explicit intent of the domain owner on two fronts: where should reporting be sent? And what is the policy enforcement desired should the email fail either SPF or DKIM? It requires infrequent updating. By pointing the DMARC record to our Valimail Authenticator, the client or Valimail Customer Success team can make error-free state changes without having to modify the client’s DNS nor deal with the static and antiquated text fields.

SPF
SPF already refers to other services’ IP rule sets. By pointing your SPF to Valimail’s system, the client is simply referring to one master rule set. Valimail’s Instant SPF™ technology creates on-demand instant SPF records in real time, resulting in perfectly formatted and precise responses. SPF changes are done through our modern and secure interface with 1-click ease, and no need to make changes in the company’s DNS systems. Instead of risky error-prone changes in a live-production DNS system, Valimail gives you a safe, error-free alternative to command-line changes. As with pointing DMARC at Valimail, our system never affects your DNS system nor can it make any changes. Since customers point only the SPF, DKIM, and DMARC at the Valimail cloud, the rest of their DNS remains in their control and unchanged (i.e. MX, A, C, PTR, and www records) — so there is no risk to the domain owner’s infrastructure. Your DNS is safe and locked down with no ability for Valimail to influence or make any changes.

DKIM
DKIM is a set of public keys meant to match the private keys of the allowed sending email servers. If the key matches, then the message is verified to have come from a specific email server and the message can be proven to be unchanged. Typically, 3rd party email services require the client to store these public keys in their DNS text files. They are stored as a string of characters, unreadable to humans and with no metadata indicating what the key is for, its age, and more. By copying and pasting the key into the Valimail system, the client can insert accompanying metadata in order to identify the key in the future, it can be validated, and its age can be tracked. This adds yet another large benefit to improving the operational management of DKIM keys. Administrators can manage key age and rotate keys more effectively with this increased visibility. Again, there is no interaction with the client’s DNS and no PII nor private data is exposed.