DKIM setup the easy way

How DKIM works

To put it in a nutshell, DomainKeys Identified Mail (DKIM) enables a receiving email server to authenticate the sender of an email. The sending email server digitally signs each sent email. These signatures are cryptographically created with a so-called private key. These digital signatures are placed in the email header, which the end user normally doesn't see. The receiving email server can, however, validate these signatures via the corresponding public key which needs to be placed in the Domain Name System (DNS), so the receiving email server can fetch it from there.

Basically DKIM requires two parts to work correctly:

- Sign outgoing emails with the private key on the sending email server
- Publish the corresponding public key in the DNS

The Problem? email servers managed by service providers, DNS managed internally

In practice, many companies (brands) use the tools and sending email servers of email service providers (ESPs). That's actually a very good idea, because ESPs have the know-how and the resources to handle newsletters and transactional emails in a professional way. But it also brings in some difficulties. In many cases, the brand keeps the control over the DNS setup. Let's assume the ESP generates the pair of public and private key. They set up the sending email server to use the private key to sign all outgoing emails and send the public key to the internal IT department of the brand, so they can publish it in the DNS. That would not be a problem, if DKIM setup were a one time thing. But for security reasons, DKIM keys should be changed (rotated) at least every six months to reduce the risk of compromised keys, either because the keys were cracked or stolen. To ensure a smooth transition to a new key, the usage of 3 keys in parallel is common (the first key is the old expired one, the second key the one in use right now, the third is the upcoming one). That's a considerable and ongoing effort to keep the emails properly signed. As a brand, wouldn't it be great to let the ESP do all the work? And for an ESP wouldn't it be perfect to be able to offer the brands the service to take care of DKIM completely?

Do not despair, because help is near

The good news is there are good working solutions for the problem:

- (sub)domain delegation:

  The brand can delegate a subdomain or a domain and give the control to the ESP. The ESP can manage the public key directly. The downside of that solution: brand owners normally don't like the idea of giving control over their domain into the hands of a third party. With subdomain delegation it is possible to hand over the control of only a certain subdomain (e.g. news.example.org instead of example.org). But that results in less attractive from addresses. e.g. info@news.example.org instead of news@example.org.

- Canonical Name record (CNAME):

  A CNAME defines that a domain name is an alias for another domain name. So the brand only once sets up the CNAME records for DKIM, basically telling the receiving email server which wants to fetch the public key to look it up at a different location, which is the DNS of the ESP.

  example:

  key1._domainkey.brand_domain.org → key1.brandname.esp_domain.com with "key1.brandname.esp_domain.com" being the actual position of the public key

  In that case, the brand only sets up where to find the actual key, which is in the DNS of the ESP. The ESP can now perform the key rotation.

Conclusion

Subdomain delegation is a good way to hand over the control for email authentication to the ESP. If there are concerns regarding losing control over the domain or if marketeers want "nice looking" from-addresses, CNAME records are the way to go.

Authors: Technical Team of the Certified Senders Alliance