DKIM beyond authentication – Protecting Brand identity and reputation

According to RFC 5863 the DKIM (DomainKeys Identified Mail) authentication allows an organization to claim responsibility for transmitting a message, in a way which can be validated by a recipient. The organization can be the author, the originating sending site, an intermediary, or one of their agents. An email message can contain multiple signatures, from the same or different organizations involved with the message.

This article evaluates the benefits of DKIM beyond the pure technical usage. It includes the evolution of further related standards that have been developed to improve email security as well as supporting email marketing success.

Technical authentication method

Additionally to SPF (Sender Policy Framework), DKIM is a domain-based digital signature authentication, using public key encryption utilizing the domain name service (DNS). It verifies the responsible organization as well as the integrity of the email message.
DKIM also provides a mechanism which permits potential email signers to publish information about their email signing practices; this will permit email receivers to make additional assessments about messages.

This authentication method is invisible to the email recipient as it is included in the email header and executed on DNS level. The email recipient only recognizes the from address in the inbox. Nevertheless, the from address does not need to match the signing DKIM domain to meet the pure technical requirements by definition. To confirm the technical integrity of an email message, it is signed by the email sender, who, when it comes to email marketing mass mailings, in most cases is an ESP (Email Service Provider).

Technical Short-thinking about DKIM

The biggest challenge nowadays is to fight against subjective spam classifications caused by subscriber feedback and spam clicks. This damages the sender reputation on sending IPs and domains. As the majority of sending email settings is built on shared IP pools and shared DKIM domains, the reputation has influence on multiple brands. From a technical standpoint, it is fully compliant to the RFC Standards, nevertheless it allows shady brands to cover themselves within that shared environment of the ESP and harm other brands

and the global reputation of the ESP. A domain is closely related to a brand. This could be the key element to build a dedicated domain-based reputation for a single brand within a shared ESP environment. Using the brand's domain in the DKIM signature and authentication will partly shift responsibility of the email content to the sending brand.

Domain Alignment and DMARC

DKIM's authentication of email identity also assists in the global control of "spam" and "phishing". In 2015 the DMARC protocol (Domain-based Message Authentication, Reporting & Conformance) has been developed. It is based on SPF and DKIM to fight email fraud such as phishing and spoofing. The fundamental idea is to secure a brand's domain. This is why Domain Alignment of FROM domain and DKIM domain is important.

Brands can only be protected, if they are going to be transparent about domain verification and integrity of their own practices and content. It is a logical chain for brands stick to their own brand identity and reputation. Accordingly, ESPs have to provide dedicated branded DKIM authentication to separate reputation on each single sending brand and to break up mingling of shared reputation.

Every ESP should enforce DMARC adoption by setting up Domain Alignment right from the beginning with a branded dedicated DKIM.

Added value for email marketing through BIMI

Up to this point DKIM and DMARC is a pure technical topic and hard to understand for marketers. In many cases marketers struggle to understand the importance of email security. This is the reason why DMARC adoption is still a tough fight and DKIM authentication is just a technical "thing" that the ESP should take care of – in the eyes of a marketer.

BIMI (Brand Indicators for Message Identification) is a good way of bridging the gap between tech nerds and marketers. The value of BIMI is obvious and easy to understand for marketers. It will still not enable the marketer's technical understanding of every single detail required for implementation. The chance to earn the benefits of BIMI for their brands success will help to get the support for dedicated DKIM domains, to implement Domain Alignment, and to adopt DMARC.

Final Conclusion

It has been a long journey from DKIM to BIMI. Finally, BIMI shouldn't be just the goal. Instead, BIMI should be the tool to explain to brands why it is important to provide their own sending domain for a dedicated email delivery setup.

DKIM is the very first puzzle piece for successfully implementing DMARC and finally BIMI. You will never start to climb the mountain from the top, but with the goal to reach the top everyone understands the need of a proper preparation and the right settings from the ground.

ESPs are the key player who are able to explain the benefits to the sending brand as well as providing the optimal technical infrastructure and technical guidance.

Once shared DKIM signatures are no longer an option for ESPs and dedicated branded domains are in use for DKIM authentication, it becomes an easier game to adopt DMARC, implement BIMI while fighting against email fraud and increase the benefits for email sending brands.

Author: Sebastian Kluth
Technical Lead CSA