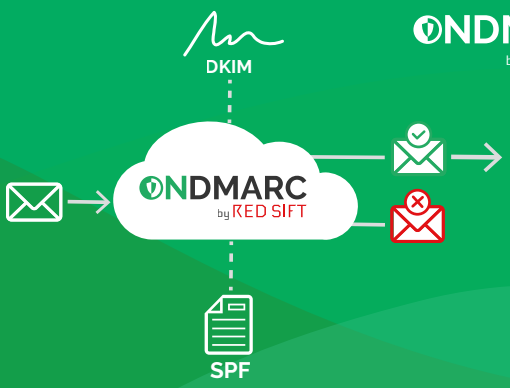
DKIM

DomainKeys Identified Mail



What does your DKIM record do?

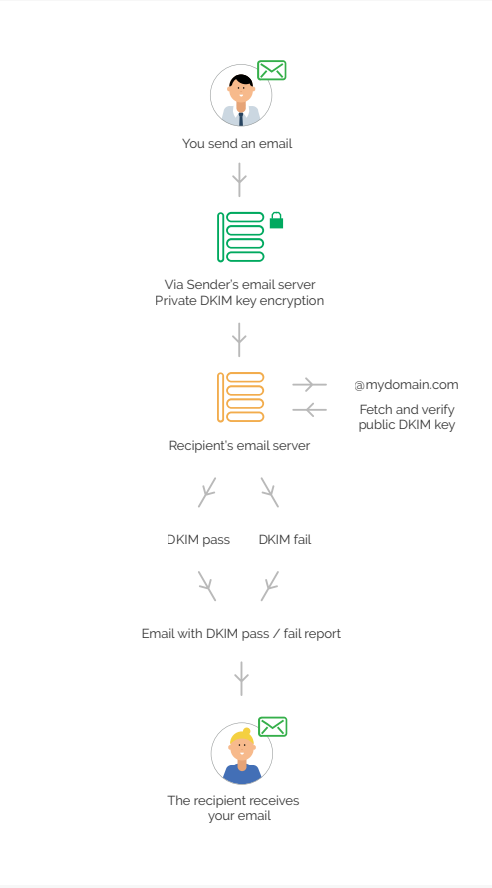
DKIM stands for DomainKeys Identified Mail, which is an email authentication protocol designed to prevent message modification in transit, a method often used in phishing and email scams.

How does your DKIM record work?

DKIM is a more recent standard and more complex than SPF. Its functionality is based on using asymmetric cryptography in the signature parts of the email. There is a private key stored on the server that sent the email, a place where it could never be read by the end-user, and a public key which is published in the DNS record of the sender's domain and is used to decrypted email signatures.

In other words...

When an email is composed, its headers and body are signed using the private key of the sender to create a digital signature, which is also sent as a header field along with the email. On the receiver's side (if DKIM enabled), the server retrieves the public key and verifies if the email was indeed signed by the sending domain. If the signature is successfully validated, that proves that the sending domain sent the message and also that the headers and body of the message have not been modified during transmission.



Member CyberExchange

Member of Microsoft Intelligent Security Association

UK CLOUD AWARDS 2019 WINNER

2017 Computing Security Awards WINNER Anti Phishing Solution of the Year

bsi. ISO/IEC 27001 Information Security Management IS 672913

GLOBAL CYBER ALLIANCE

How do you set up your DKIM record?

When you want to set up your DKIM record properly, follow these steps:

1. Generate an inventory list of all sending services you use to send emails

Tracking the domains is an important step that often gets overlooked by companies. Your organization may use different vendors for sending marketing messages, customer service messages, and corporate emails on their behalf.

2. Add DKIM record to your email server

Get in touch with all the sending services you use and request DKIM be configured and that you require a copy of the public key.

3. Publish your public key

You will be sent the public key, this will need to be added to your DNS. This will now become publicly available to any server that queries that name on your DNS.

4. Store your private key

When you start sending an email through this service from now on, it will be DKIM signed (using the private key) and specify the domain where the public key is located.

5. Test the process

If you have successfully configured everything on the your system, then the receiving server will query your DNS to locate the Public Key, use this to decrypt the signature and then verify that the email has not been tampered with.

Download the free DMARC digest eBook

Learn about the DKIM protocol and how, working with DMARC, you can begin to block phishing and impersonation attempts for good.

Find out more

RED SIFT

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. By harnessing the power of AI we can securely collate, compute & visualize data from thousands of individual signals to help organizations to optimize their cybersecurity.

Products on the platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence.

www.ondmarc.redsift.com
contact@redsift.com
@redsift