GOV.UK

Guidance

Using DomainKeys Identified Mail (DKIM) in your organisation

Published 19 February 2016

Contents

Print this page

This publication is available at https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim

DomainKeys Identified Mail (DKIM) verifies an email's domain and helps show that the email has not been tampered with in transit. The receiving email service can then filter or reject email that fails the DKIM check.

How DKIM works

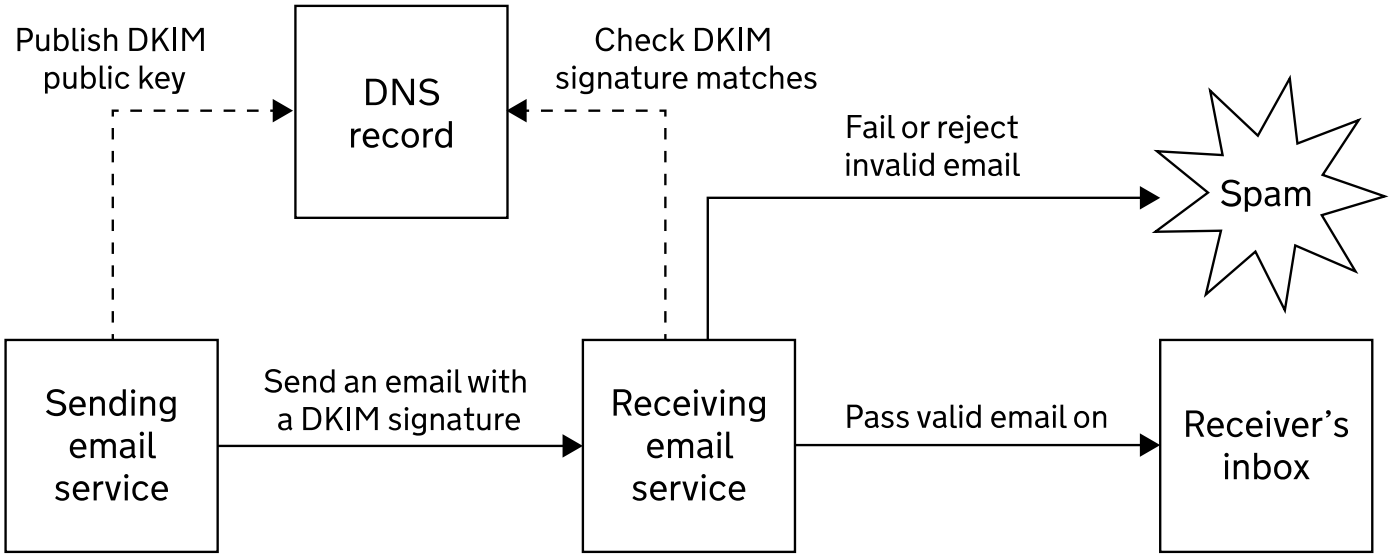
DKIM uses public key encryption to check email. The sending email service generates a string of characters known as a hash using the content of each outbound email. The sending service then encrypts the hash with its private key and adds it to the email header. This is the DKIM signature.

The receiving email service looks up the public key in the sender's DKIM DNS record then uses the public key to decrypt the DKIM signature on the email. It also generates a hash of the email in the same way the sending email service did.

If the hash matches the decrypted DKIM signature then the email passes the DKIM check. This means the email came from where it says it came from and has not changed in transit.

Most email services will automatically check DKIM on inbound email, but you should check to make sure it's enabled.

You need a separate DKIM key and DNS entry for each service you send email from. In addition to your own mail servers, you might also need to consider third-party applications and services that send mail on your behalf.



Further email security guidance

All public sector organisations must follow guidance on how to set up email services securely (https://www.gov.uk/guidance/set-up-government-email-services-securely).

Dkim.org (http://www.dkim.org/) has more information on DKIM. You can also read a simple explanation (https://postmarkapp.com/blog/explaining-dkim) and a more detailed video explanation (https://space.dmarcian.com/video-dkim-overview/) on DKIM.

Print this page