

- 1. Home (https://www.gov.uk/)
- 2. Email security standards (https://www.gov.uk/government/publications/email-security-standards)
- Government Digital Service (https://www.gov.uk/government/organisations/government-digital-service)

Guidance Using DomainKeys Identified Mail (DKIM) in your organisation

Published 19 February 2016

Contents

How DKIM works Further email security guidance

Print this page



© Crown copyright 2016

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 (https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/government/publications/email-securitystandards/domainkeys-identified-mail-dkim DomainKeys Identified Mail (<u>DKIM</u>) 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 <u>DKIM</u> check.

How **DKIM** works

<u>DKIM</u> 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 <u>DKIM</u> signature.

The receiving email service looks up the public key in the sender's <u>DKIM DNS</u> record then uses the public key to decrypt the <u>DKIM</u> 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 <u>DKIM</u> signature then the email passes the <u>DKIM</u> 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 <u>DKIM</u> on inbound email, but you should check to make sure it's enabled.

You need a separate <u>DKIM</u> key and <u>DNS</u> 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 <u>DKIM</u>. 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 <u>DKIM</u>.

Print this page