

DKIM (DomainKeys Identified Mail)

Introduction

“ DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in emails (email spoofing), a technique often used in phishing and email spam. [source](#)

Description

DKIM is a more advanced method than [SPF \(Sender Policy Framework\)](#) for combating email spoofing. It uses [Public-Key cryptography](#) to digitally sign each email. A mail server generates a keypair and the public key is then added as a DNS record for that domain. Using the private key the mail server affixes a digital signature to each email. The receiving [Mail Transfer Agent \(MTA\)](#) can then lookup the public key using the DNS record matching the sending domain and validate the signature.

Example

As an example, the host `mail.swigg.net` is used for sending emails. It has the following DNS record.

Domain	Type	Value
--------	------	-------

mail._domainkey	TXT	v=DKIM1; h=sha256; k=rsa; p=MIICljANBgqhkiG9w0BAQEFAAOCAg8AMIICGgKCAgEA0SF9I7b0bMcB3ptHM6LbV+rZ/rz1SmHyNCKzBrB6rs433avNHFO4bbs//NG9ZvrCqeEIC4NIXPO0VLI8Vbor9dA7HVcSct5aH9/qRWUMfE3LEH9cBVytVAm3/ICgHN6qhWKbnPxK//zh5tmzgdCTKuWyiqlSECbX63q3gWyuXYMJKqr/BzEq0fzLjymHCfaWkG3MI02pRp68HgpVcpvx2G/t3BKz50BrZVOISS E9Gi7wbb9jrdeGLwBYIBD4LR+QkVlr8z+ptCMfg+XOfjzLDsBNBUHnBFT/7N3/Ub9BNxsLBltZX3mAWNQQY/n31SC7ik9qs3t6lt22er1jo3WZqjWxBM4xseynUvfn4Lgcp+XQAZCWRQIHr2hwrX4KO1mK/vvvb/dS+NmCNXmWkDvzerVPBCXd fBn+1nbnAsv0vzBuf2yELfRkAluQRE/P RpeETXAjoayYsVePpOtJn5co0tuiOwbjUf+9hkNO1a3aN/jrK41BDJrGoNjvul3k WZX1Tz42ICQ168x6tuR5ImB5jJFlgGjz+dC5wY8Gmt4hCf1GPW6g7RjpaGUXTEFAEAE0iECsMjg2/Tm2Sb/H4phN/F2A nF4bkju548Yg73X37tVCkLejMgWH7TTgyQvZ/nXhsE4q31YrNZSNnWZMV+9z/yJyQvVmTXsOoDAIfkqxfCawEAAQ==
-----------------	-----	---

Revision #3

Created 29 October 2020 17:20:06 by dustin@swigg.net

Updated 2 April 2021 14:04:16 by dustin@swigg.net