Email Authentication

Email Authentication and Security

There are 3 authentication methods to verify email coming from a specific domain is authentic; [SPF](#), [DMARC](#) and [DKIM](#). This reduces or eliminates spammers and phishers from using a domain to falsely appear authentic.

How does SPF work?

Sender Policy Framework (SPF) is a way for a domain to list all the servers they send emails from. Think of it like a publicly available employee directory that helps someone to confirm if an employee works for an organization. SPF records list all the IP addresses of all the servers that are allowed to send emails from the domain, just as an employee directory lists the names of all employees for an organization. Mail servers that receive an email message can check it against the SPF record before passing it on to the recipient's inbox.

How does DKIM work?

DomainKeys Identified Mail (DKIM) enables domain owners to automatically "sign" emails from their domain, just as the signature on a check helps confirm who wrote the check. The DKIM "signature" is a digital signature that uses cryptography to mathematically verify that the email came from the domain.

Specifically, DKIM uses public key cryptography:

- A DKIM record stores the domain's *public key*, and mail servers receiving emails from the domain can check this record to obtain the public key
- The *private key* is kept secret by the sender, who signs the email's header with this key
- Mail servers receiving the email can verify that the sender's private key was used by applying the public key

How does DMARC work?

Domain-based Message Authentication Reporting and Conformance (DMARC) tells a receiving email server what to do given the results after checking SPF and DKIM. A domain's DMARC policy can be set in a variety of ways — it can instruct mail servers to quarantine emails that fail SPF or DKIM (or both), to reject such emails, or to deliver them. DMARC policies are stored in DMARC records. A DMARC record can also contain instructions to send reports to domain administrators about which emails are passing and failing these checks. DMARC reports give administrators the information they need to decide how to adjust their DMARC policies (for example, what to do if legitimate emails are erroneously getting marked as spam).

Source: https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/

NEXT STEPS

Configure SPF Policy

Configure DKIM Signature

Configure DMARC Reports

SPF Record Construction

At the beginning of the record, `v=spf1` identifies this as an SPF record. At the end of the record, `-all` defines the policy. Dash - for hard-fail, tilde ~ for soft-fail. In between the identity and policy, each `include:` defines the server domain names that are authorized to send as this domain. Each `+ip4:` defines the IP addresses that are authorized to send as this domain.

Example

```
v=spf1 +ip4:<IP Address> include:<FQDN> ~all
```

Microsoft 365

```
v=spf1 include:spf.protection.outlook.com ~all
```

Google Workspace

```
v=spf1 include:_spf.google.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
+	include	emailus.freshservice.com	Pass	The specified domain is searched for an 'allow'.

Prefix	Type	Value	PrefixDesc	Description
+	include	relay.mailchannels.net	Pass	The specified domain is searched for an 'allow'.
~	all		Fail	Always matches. It goes at the end of your record.

Further reading: a great explanation of SPF.

NEXT STEPS

Configure DKIM Signature

Configure DMARC Reports

DMARC Record Construction

At the beginning of the record, `v=DMARC1` identifies this as a DMARC record. The following components define the policy and action if failed. Create a TXT record with `_dmarc` as the host.

Example

```
v=DMARC1; p=quarantine; rua=mailto:<DMARC Report Address>; ruf=mailto:<DMARC Failure Report
Address>; adkim=r; aspf=r; fo=0; sp=reject; pct=100; ri=604800
```

Tag	TagValue	Name	Description
v	`DMARC1`	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	`quarantine`	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	`mailto:` <DMARC Report Address>	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	`mailto:` <DMARC Failure Report Address>	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.
adkim	`r`	Alignment Mode DKIM	Indicates whether strict or relaxed DKIM Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
aspf	`r`	Alignment Mode SPF	Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
fo	`0`	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.
sp	`reject`	Sub-domain Policy	Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.
pct	`100`	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.

Tag	TagValue	Name	Description
ri	604800	Reporting Interval	Indicates a request to Receivers to generate aggregate reports separated by no more than the requested number of seconds. Valid value is a 32-bit unsigned integer.

NEXT STEPS

Configure [SPF](#) Policy

Configure [DKIM](#) Signature

DKIM Record Construction

DKIM requires setup on the sending server. In the case of Microsoft 365, this is configured in [365 Defender](). To enable DKIM in Microsoft 365, the DNS record has to exist. The actual DKIM record is simple, but the server is queried for the key. Below are the actual record and the translated public record.

Microsoft 365 DKIM DNS Record (1) - Actual Record

```
selector1-example-com._domainkey.example.onmicrosoft.com.
```

Microsoft 365 DKIM DNS Record (2) - Actual Record

```
selector2-example-com._domainkey.example.onmicrosoft.com.
```

Microsoft 365 DKIM DNS Record - Public View

```
v=DKIM1; k=rsa;
p=MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgG2pFI5LpUou9yMvDDUZ0Sj1JvEqgUoBIta5Wuzo1sWXfOdkW
tPpAGKkFamhYRffR7Jag4MiHQY+PCAXFFSVxbMfiq4DoYWf6eLeDK7iyM1ZIgq5P2IrY5xWBkeuFLqaYbft+b7YiiyPAo
7Og7XVEps97P0MOvpowinJfTKZdb5BAgMBAAE=;
```

Tag	TagValue	Name	Description
v	`DKIM1`	Version	Identifies the record retrieved as a DKIM record. It must be the first tag in the record.

T a g	TagValue	Name	Description
k	`rsa (Length: 2048 bits)`	Key Type	The type of the key used by tag (p).

p	`MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgG2pFI5LpUou9yMvDDUZ0Sj1`
	`JvEqgUoBIta5Wuzo1sWXfOdkWtPpAGKkFamhYRffR7Jag4MiHQY+PCAXFFSV`
	`xbMfiq4DoYWf6eLeDK7iyM1ZIgq5P2IrY5xWBkeuFLqaYbft+b7YiiyPAo7O`
	`g7XVEps97P0MOvpowinJfTKZdb5BAgMBAAE=`
		Public Key	The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.

NEXT STEPS

Configure [SPF](#) Policy

Configure [DMARC](#) Reports