DMARC Playbook

Version: 0.1

ReBIT's Best Practices Whitepaper

Authors/Contributors

Vivek Srivastav	ReBIT
Chaitanya Rao	ProgIST Solutions LLP
Ambuj Bhalla	ReBIT

Revision History

Version	Date	Comments
0.1	21-06-2017	Initial Draft

ReBIT

Table of Content

1 Overview

DMARC, which stands for “Domain-based Message Authentication, Reporting & Conformance”, is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author (“From:”) domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

DMARC specifications when implemented appropriately would enable organizations to reduce spam and phishing emails sent to their customers and employees from unauthorized senders and domains. It would enable fraud protection, simplified email delivery and domain reputation. In addition it will also benefit the domain management and compliance functions of the organization.

This document provides a step by step process for implementing DMARC for an email sender. Configuration of the email receivers is not covered in this playbook.

2 Pre-requisite

Required	Access to the DNS registration account or management function of your organization.
Required	Implement SPF, DKIM and DMARC processing in the receiver/exchange server. Please refer to the email receiver’s/provider’s documentation for enabling DMARC, DKIM and SPF.
Optional	Partnership with value added vendors

3 General Outline of Procedure

The implementation should follow the following process to build the governance without risking the email operation.

- **Setup the observe mode**: This mode does not protect your organization’s email domain from phishing attack, but it will help identify the domains which are sending the emails on behalf of your organization. Out of this list of domains, you will need to identify the domains which are authorized to send emails on your organization’s behalf and create a whitelist.
- **Setup the quarantine mode**: The next step is to step up the security and change the policy so emails being sent from domain/IP not specified in your

whitelist are flagged by the receivers. Some receivers would start delivering such emails to the spam folder.

- **Setup the reject mode**: When this mode is turned on then the emails being sent from domains which are not in the whitelist starts getting rejected and are not delivered to the recipient.

3.1 Implementing SPF

Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators.

Compliance with SPF consists of three loosely related tasks:

- Publish a policy through the DNS record: Domains and hosts identify the machines authorized to send e-mail on their behalf. They do this by adding additional records to their existing DNS information: every domain name or host that has an A record or MX record should have an SPF record specifying the policy if it is used either in an email address or as HELO/EHLO argument. Hosts which do not send mail should have an SPF record published which indicate such ("v=spf1 -all"). It is highly recommended to validate the SPF record using record testing tools.
- Check and use SPF information on the email server: Receivers use ordinary DNS queries, which are typically cached to enhance performance. Receivers then interpret the SPF information as specified and act upon the result.
- Review and Revise mail forwarding on the MTA or exchange server.

Implement SPF policy in the following stages

1. Observe mode - “?all”
2. SOFTFAIL mode “~all” - messages which are not from the listed domain are tagged
3. FAIL model “-all” - messages that don’t match the domains listed in the SPF TXT record are rejected

A list of all IP addresses, domain addresses that send emails on behalf of the organizations is required for proper configuration of the SPF policy. There are eight mechanisms defined to configure these authorized list and SPF policy. The following table lists these policy reference mechanisms.

A	If the domain name has an address record (A or AAAA) that can be resolved to the sender's address, it will match
IP4	If the sender is in a given IPv4 address range, match.
IP6	If the sender is in a given IPv6 address range, match.
MX	If the domain name has an MX record resolving to the sender's address, it will match (i.e. the mail comes from one of the domain's incoming mail

	servers).
PTR	Deprecated
EXISTS	If the given domain name resolves to any address, match (no matter the address it resolves to). This is rarely used. Along with the SPF macro language it offers more complex matches like DNSBL-queries.
INCLUDE	References the policy of another domain. If that domain's policy passes, this mechanism passes. However, if the included policy fails, processing continues. To fully delegate to another domain's policy, the redirect extension must be used.
ALL	for all IPs not matched by prior mechanisms

If SPF is implemented by itself without DMARC, there is no feedback mechanism to determine if all domains and all IPs are covered. Without this feedback mechanism implementing a FAIL mechanism will be very difficult. The Aggregate Report feedback mechanism in DMARC enables comprehensive visibility of the domains and IP sending emails on behalf of the organization thus helps in building this whitelist required for the SPF configuration.

3.2 Implementing DKIM

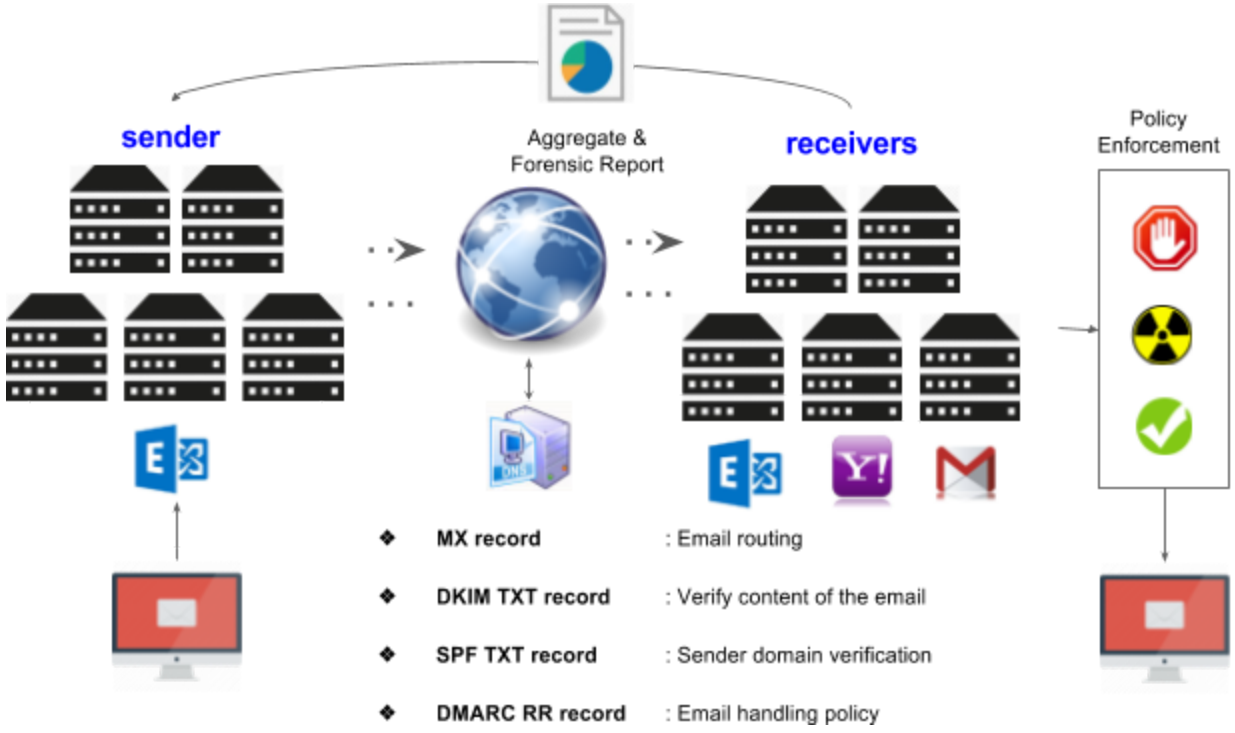
The DKIM configuration is more involved than SPF and DMARC because it requires a PKI infrastructure setup so an outgoing email server can sign the emails and the receiver email server can verify the signature. The public key for signing the outbound emails is maintained in the DNS DKIM TXT record.

The outgoing server uses the private key to sign the emails. DKIM supports multiple outgoing servers. For this DKIM uses a concept of selector. An email domain may define more than one selector. Each selector maps to a unique PKI. This enables multiple senders, each of which is sending emails on behalf of the organization to sign emails through different selector. Thus DKIM implementation may have more than one DNS DKIM TXT record.

DNS queries don’t support subdomain tree walking. Thus these selectors have to be known in advance if an external tool needs to validate whether DKIM is implemented for a domain or not.

3.3 Implementing DMARC

DMARC policies can similarly be implemented in the phased approach. The following diagram shows a complete configuration after DMARC implementation:



Once DMARC is implemented, any DMARC compliant receiver that receives emails from the sender domain will start generating aggregate and forensic reports and start sending to the email address specified in “RUA” and “RUF” DMARC configuration. This feedback is what provide proper deployment, governance and metrics.

4 DNS Records

DMARC implementation for the domain “**rebit.co.in**” is shown below in the example. The SPF, DKIM and DMARC are implemented as DNS TXT records. Once the setup is complete, these following records will be present in the DNS configuration of the organization.

SPF	**rebit.co.in**	v=spf1 mx a include:rebit.co.in include:mail.rebit.co.in ~all
DKIM	**mail**._domainkey.**rebit.co.in** Variables: **Selector**: mail **Domain**: rebit.co.in	v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDLgog6nmDTTj40GuIFRHzu2LzOON8rP07jq/XM3E6nuMBREGVqbQ7d9r3uImMLYjrNOZy1IJAo9TeZGYcUhrdFf6PaeHWEotHPu9YgEZfcsC1hqpb2tDE7RM1Cr/eDKGOe6HOJk/Yda/xwT4wxkEB2LLMwDH+5O29qOrfBuhTL9QIDAQAB
DMARC	_dmarc.**rebit.co.in**	v=DMARC1; p=none; rua=mailto:rua@rebit.co.in,mailto:rua.rebit@progist.in;ruf=mailto:ruf@rebit.co.in,mailto:ruf.rebit@progist.in;

In addition, the MX records defines the mailbox/exchange server to which the MTA (Mail Transfer Agents) forward the emails.

4.1 SPF DNS Configurations

The first portion of the policy is to define the incoming mail servers records (MX records) of the domain that are authorized to send mail for that domain.

In the example shown below we take the “rebit.co.in” domain for SPF implementation.

The first thing is to determine the email handling policy that the email receivers should use. There are four options that are available

- Fail or “-all” means only the domain’s mail servers (and those in the ‘a’ and ‘include’ sections) are allowed to send mail for the domain. All others are prohibited.
- Soft Fail or “~all” means only the domain’s mail servers (and those in the ‘a’ and ‘include’ sections) are allowed to send mail for the domain, but it is in transition. All other are prohibited.
- Neutral or “?all” means explicitly that nothing can be said about validity.
- Allow All or “+all” means that any host can send mail for the domain. This should never be used

If an organization has registered a domain that is not used for sending emails, it can implement the following SPF TXT record to prevent domain misuse.

TXT	rebit.co.in	v=SPF1 -all

This will prevent any emails from being sent using this domain.

If the domain is being used to send emails, the first thing is to add the MX record. The list below contains the DNS records for the mail servers (MX record) associated with Rebit.

MX	mail.rebit.co.in

For the authoritative mail servers your would need the tag ‘mx’ to be added to the SPF policy. If only your mail server is authorized to send emails for the domain, then this mx record can be included in the SPF configuration, for e.g.:

TXT	rebit.co.in	v=SPF1 mx -all

There is a possibility that not all the organization mail servers are defined in the organization's DNS records. For example, the test servers or applications with built-in mail systems. In this case, add the additional server domains or IP addresses. This should only be used if there are other internal systems, other than the mail servers, authorized to send mail for the domain. In our example below, we have added the IP address of RBI mail servers (125.18.33.229).

If systems are added, then your would need to add the 'a' tag to the SPF policy.

In case there are any external domains that may deliver or relay mail for your organization, then add the 'include 'tag of the SPF Policy. This should only be used if an external domain is trusted to send mail message for your organization's domain. For example, Customer Relations Management System, Cloud Mail Provider (Google, Office 365, Yahoo!), or Cloud Security Provider.

Please note: If you are using a Cloud Service Provider, you must work with them for the appropriate value for this setting. (in our example, Google IP address has been added)

It is recommended to use Soft Fail (~all). This will mark mail as non-compliant if it does not meet the defined criteria. Below is the SPF TXT record which must be created on the DNS server for the configuration specified previously.

rebit.co.in. IN TXT "v=spf1 mx a:125.18.33.229 include:64.233.168.27 ~all"

If you have your own DNS server, then please create TXT records for the above SPF policy. If you are using a third party DNS provider, then please follow their instructions for creating a TXT record.

There are some online tools that can be used to generate SPF records, such as:

- https://www.dynu.com/NetworkTools/SPFGenerator
- https://mxtoolbox.com/TXTLookup.aspx

4.2 DKIM DNS Configurations

Tag Name	Purpose	Sample
v	Protocol Version	DKIM1
t	t = flags (y means domain is testing DKIM)	t=y
k	k = cryptographic algorithm	k=rsa
p	p = public key	p=AAAAB3NzaC1yc2EAA AADAQABAAABAQDqUvun WmIt51xKx4TKSAwhHFh Q1wG2XUzU4OUzvSH46U

		zQ/yqDzXnKrTQnbFTTH NNsCZ5jagQz79qWpFC9 KQxz+o9D8bCHb6JsPjW mGDhb6ydiIgqD2EiWtt rv4P5WPIVZPx1UHQAXh NSFGG8GSPRU3nWkIqrl RfXo4pAscNr9aVoCv/b nykSkkdq2ywN8J5Qyvk dIH7iXbVgcEAwyR2Q+A X3yZqactXDkl7MhsVzX eUUZrZYXbC8fNQIwBLC 91lqix9DQGYs9mDXt43 ap0Gyj5m0ZsQpfPRv2s DItqYFj/jqMJyUrouj9 T5mYmNCnvg6dVyhJqTb O5PWEpmZ06B7b

4.3 DMARC DNS Configurations

Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r

4.4 Tools to investigate the DNS records

- DMARC Deployment Tools, https://dmarc.org/resources/deployment-tools/

- DMARC implementation status: https://dmarcguide.globalcyberalliance.org

5 Working with ReBIT

When your organization is ready to implement DMARC, kindly engage with ReBIT to participate in configuring the reporting URI for the aggregate and the forensic reports. ReBIT will set up a RUA and RUF email addresses that your organization should add to the DMARC configuration. This will enable ReBIT to track the spam across the financial sector and also work with other organization to bring down phishing websites. ReBIT would also maintain all DKIM selectors configured by the organization.

Please contact rirebit@rbi.org.in for engaging on this anti-phishing and DMARC implementation drive.

6 References

- ReBIT's webinar on DMARC, http://webinar.rebit.org.in
- Code and libraries, https://dmarc.org/resources/code-and-libraries/
- https://postmarkapp.com/blog/labs-a-free-tool-to-monitor-and-implement-dmarc
- SPF, DKIM, DMARC and Exchange Online, https://blogs.technet.microsoft.com/fasttracktips/2016/07/16/spf-dkim-dmarc-and-exchange-online/