All of Government

Secure Email Common Implementation Framework

Issued by

Digital Services branch

Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Contents

1 Purpose

The purpose of this All of Government Secure Email Common Implementation Framework is to provide guidance to New Zealand Government Agencies on industry practices for securing external email. This will:

- improve the overall security of external email services within the New Zealand Government;
- decrease the likelihood of successful spoofing of domains in phishing attacks; and
- enable the retirement of the SEEMail service.

2 Introduction

The Department of Internal Affairs (DIA) as the Lead Agency for ICT Common Capabilities has developed an email security framework, using email security controls available through the Domain Name System (DNS), to enable the retirement of the SEEMail service. These freely available security controls will deliver additional levels of protection as they can be applied to all email, not just emails specifically tagged to route via SEEMail. When reviewing the use of open standards to replace SEEMail, it was determined this could and should be extended out to all NZ Government Agencies.

Guidance to support this Secure Email Common Implementation Framework is provided by the Secure Government Email Architecture which was approved by the Government Chief Information Security Officer (GCISO) and the SEEMail Security Working Group (SSWG).

Goal

The goal of this Secure Email Common Implementation Framework is to provide technical settings for email security that meet industry standards. The settings will provide:

- transmission security through encryption;
- message integrity through digital signing;
- a basic level of nonrepudiation through permitting only authorised services to send email on behalf of each domain; and
- protection against domain spoofing.

3 Exclusions and Limitations

Classification up to IN-CONFIDENCE only

This document covers the use of email platforms for the transmission of unclassified email and email classified IN-CONFIDENCE and below.

Certification & Accreditation

All Certification and Accreditation (C&A) for email security services remains the responsibility of each Agency.

Protective Security Requirements (PSR) classification markings

This framework does not change the requirements under the PSR for protective markings. NZ Government information, including emails, requires protective marking.

Exceptions

As with any technology settings this Framework attempts to address most use cases, however it is accepted there will be some situations where specific services may not be able to confirm to the recommended settings. Exceptions to this framework remain the responsibility of the individual Agencies.

4 Technologies Being Used

The technologies required to be deployed are:

- **Transport Layer Security** (TLS) providing session level encryption with a minimum version of TLS1.2, including controls enforcing encryption for all email (Implicit TLS).
- **TLS Reporting** (TLS-RPT) to receive feedback on issues related to the encryption of email transmissions using TLS.
- **Sender Policy Framework** (SPF) to ensure only authorised servers & services can send messages from your domain.
- **Domain Keys Identified Mail** (DKIM) for message signing, providing limited nonrepudiation, and ensuring messages are not altered in transit.
- **Domain-based Message Authentication, Reporting, and Conformance** (DMARC) for tying SPF and DKIM together with policy and providing reporting (A DMARC reporting tool is required)
- **Mail Transfer Agent Strict Transport Security** (MTA-STS) for enforcing encryption on all inbound messages from supported sending domains.
- **Data Loss Prevention** (DLP) for ensuring messages marked with classifications higher than IN-CONFIDENCE are blocked.

5 Agency Implementation

Detailed configuration settings will be sent to all Agencies and can be obtained through emailing sge@dia.govt.nz.

Appropriately skilled suppliers will be invited to offer services in support of the Framework on Pae Hokohoko | Marketplace (marketplace.govt.nz). This will allow Agencies to select from a panel of suppliers to gain assistance with their implementation projects to enable SPF, DKIM, DMARC and MTA-STS, and assist with the iterative work required to move towards the enforcement of these security controls. Agencies will also be able to procure DMARC reporting and/or ongoing operational support for managing the security controls if needed. The Marketplace service scope will be flexible so it can adapt to any future changes to the guidance.

These services will include DMARC reporting tools which will most likely be 3rd Party Software as a Service (SaaS) providers like Valimail, OnDMARC, EasyDMARC, Proofpoint or others*. It is important for Agencies to use a DMARC reporting tool to ensure they can meet their expectations under NZISM section 15.2.36.

*These are only examples of DMARC reporting providers and this is not an endorsement of their services.

6 Deployment timeline

The following are the critical dates associated with deployment of this framework.

- **October 2025** - All Agencies should have lifted their email security standards to be in line with this Framework.

7 Compliance Monitoring and Reporting

The AoGSD team will be monitoring compliance to the framework. Monitoring will initially cover SPF, DMARC and MTA-STS settings and will be expanded to include DKIM. Changes to these settings will be monitored, enabling reporting on email security compliance across All of Government.

Ongoing monitoring will highlight changes to domains, ensure new domains are set up with security in place, and to monitor implementations of future email security technologies.

Where compliance changes, for example an Agency has a domain with an SPF record ending with -all, which is changed to ~all, this will be captured, to facilitate Agency communication by the AoGSD Security Team to determine if there is an issue or if an error has been made. This will be reviewed on a case-by-case basis and agencies will be communicated with by the AoGSD.

8 Securing all Email Enabled Domains

Purpose

This section defines the required settings for securing all enabled domains.

Transport Layer Security – TLS

TLS has become the default standard for providing encryption at the session layer between messaging servers. For most mail services TLS is enabled by default, however there are specific steps required to ensure TLS is always used.

TLS Requirement:

A minimum of TLS1.2 must be used.

TLS1.1, 1.0, SSL, no-TLS, or sending unencrypted must not be used.

Microsoft Office 365 Configuration

If an Agency uses Microsoft Office 365, then TLS1.2 (minimum) with strong cyphers is enabled by default. However, if the recipient's server does not support TLS or the TLS handshake fails, the email can revert to sending in the clear. To address this risk requires the configuration of an Outbound Connector requiring TLS, and a mail flow rule rejecting non-TLS connections inbound.

Configuring a Connector to Require TLS for All Outbound Mail

This forces Office 365 to only send mail via an encrypted connection. If the receiving mail server does not support TLS, the email will be rejected and not sent.

1. Log in to Exchange Admin Centre (EAC):
    - Go to the Microsoft 365 admin centre, then navigate to the Exchange Admin Centre.
2. Go to Mail Flow > Connectors:
    - In the left-hand panel, click Mail flow, then select Connectors.
3. Create a New Outbound Connector:
    - Click the + (plus) sign to add a new connector.
    - Choose From: Office 365 and To: Partner Organization. This will cover external outbound mail.
4. Set Domain Scope to All Domains:
    - In the domain settings, choose the Any domain option. This ensures the connector applies to all emails sent outside your organization.
5. Require TLS Encryption:
    - In the Security Restrictions section, select Force TLS.
6. Test and Save:
    - Review the configuration, test it, and click Save to enable the connector.

Creating a Mail Flow Rule to Reject Non-TLS Connections

This forces Office 365 to reject any incoming connection requests where the sending server does not support TLS.

1. Log in to Exchange Admin Centre (EAC):
    - Go to Mail flow and select Rules.
2. Create a New Rule:
    - Click the + sign to create a new rule and select Create a new rule.
3. Configure Conditions:
    - In the Apply this rule if... section, select "The recipient domain is external."
    - Alternatively, you can use Any recipient if you want the rule to apply to all emails.
4. Block Non-TLS Emails:
    - Under Do the following, select Reject the message with the explanation.
    - Customize the rejection message to indicate that TLS encryption is required.
5. Exception Handling (Optional):
    - If there are specific trusted domains that do not support TLS but are allowed, add those domains as exceptions.
6. Save the Rule:
    - Review the rule configuration and click Save to enforce it.

Google Cloud Platform

If an Agency uses Google Cloud Platform (GCP), they will need to manually disable TLS1.0 and 1.1. https://cloud.google.com/assured-workloads/docs/restrict-tls-versions By default all outbound email from GCP is encrypted and if TLS fails outbound email will not be sent unencrypted and will instead queue for delivery once TLS is restored.

TLS Reporting (TLS-RPT)

TLS reporting is a mechanism that allows domain owners to receive feedback on issues related to the encryption of email transmissions using Transport Layer Security (TLS). Specifically, it provides reports on the status of email message delivery over TLS, such as failures to establish secure connections due to misconfigurations, certificate issues, or downgrades.

TLS-RPT works by allowing mail exchange servers to send reports to the domain owner whenever there's a failure in TLS negotiation. These reports help organizations monitor their email traffic and ensure their messages are delivered securely.

Microsoft 365 offers TLS reporting capabilities within its suite of security and compliance tools to monitor secure email delivery and TLS encryption health. Various managed DMARC providers can also provide this service.

The only configuration required if using either Microsoft 365 or Google Cloud Platforms is for a DNS record to be created. Once the DNS record propagates, you'll start receiving reports from other email servers that encountered issues delivering emails to your domain using TLS.

Example TLS-RPT DNS record:

Name	TTL	Type	Data	Comment
_smtp._tls.yourdomain.com	3600	txt	"v=TLSRPTv1; rua=mailto:<tls-report@yourdomain.com>"	Enables TLS reporting on your domain.

TLS-RPT Requirement:

All email sending domains must have TLS Reporting enabled.

Sender Policy Framework – SPF

When correctly configured, SPF provides protection to domains by only permitting delivery of email which have been sent from valid source servers.

Most domains already have a SPF records enabled; however, DNS scanning has shown many SPF records end with a softfail ~all instead of a hardfail -all. This is a weak posture as ~all limits any protection afforded by SPF.

If an SPF record has ~all at the end, a malicious email sender can use any SMTP capable server to send on behalf of the domain, and the message will not be dropped by DMARC checks. While it will not 'pass' checks as being specifically listed as an authorised source, it will also not fail checks as the ~all permits unknown sending servers.

SPF Requirement:

All email sending domains must have an SPF record and it must end with a hardfail **-all** to prevent spoofing of messages via untrusted sources.

Example SPF Record:

The following is an example SPF record from the domain nsw.gov.au. This domain permits messages outbound only from the Microsoft Office online IP address ranges and denies all other addresses.

Name	TTL	Type	Data	Comment
spf:nsw.gov.au	3600	txt	"v=spf1 include:spf.protection.outlook.com -all"	Permits outbound email from the Microsoft Office online IP address ranges only & denies all others

When configuring SPF records consideration must be given to all servers and services which may send email on behalf of the domain. If the ONLY source is Microsoft Office 365 for sending all email then "v=spf1 include:spf.protection.outlook.com -all" will cover all email. However, if for example, bulk mail senders such as Sendgrid or Mailchimp or other external systems (such as Finance, HR/Payroll or CRM platforms) are used to send email their SPF entries will also need to be included. Agency's bulk sending services will be able to supply their requirements for SPF.

Moving from ~all (softfail) to -all (hardfail)

Moving from ~all to -all can have a severe impact on email flows. All valid source servers must be identified and included within the SPF statements before making the switch change.

DMARC reports should be reviewed looking for messages which are hitting the softfail controls. This will highlight source servers which are not explicitly permitted to send on behalf of an Agency's domain(s).

Once all source servers have been explicitly defined the suffix should be changed from ~all to -all.

Domain Keys Identified Mail – DKIM

DKIM is used to cryptographically sign messages as they leave an organisation. The cryptographic signature can be verified by the recipient server ensuring the message has not been altered in transit. DKIM signing needs to be provided on the exit points of all systems sending email on behalf of the organisation.

DKIM Requirement

All outbound email from all sending services must be DKIM signed. *NB: This needs to be applied at the last MX server in the sending email flow.*

Domain-based Message Authentication, Reporting, and Conformance – DMARC

DMARC ties the above SPF and DKIM settings together, advising recipient servers how to handle non-compliant messages from your domain. Most Agencies have DMARC policies in place however most also have the compliance is set to p=none. There are 3 options available for DMARC compliance: none, quarantine or reject.

When a receiving server receives an email purporting to be from an Agency's domain, it will look up their DMARC policy for instructions on how it should be applied. If the message passes the associated DKIM and SPF checks the message it will be delivered, or at least continue for further processing by other security measures, e.g. spam filters. If DKIM and / or SPF checks fail, it is the DMARC controls which advise the recipient server on how to proceed.

If the flag is set to p=none, any DKIM & SPF failures may be ignored, and the message delivered to the recipient's inbox. The exact way the message is handled may be determined by the recipient server's internal policies.

If the flag is set to p=quarantine any DKIM or SPF failures should result in the message being sent to quarantine, again depending on how the receiving server is configured – e.g. there may not be a quarantine service configured so the message might be delivered to the junk-mail folder instead. This is not considered a good approach as it has been well proven end users frequently get email released from quarantine and will read messages in their junk mail folder, including clicking on links.

If the flag is set to p=reject, messages failing DKIM and SPF checks should be rejected and discarded by the recipient server. Many mail exchange (MX) servers in the sending path also check for DMARC compliance so non-compliant messages may be discarded before they even reach the destination server.

Moving to p=reject

Moving to p=reject is generally not a big move, and one which has been overestimated by many organisations. Safe migration is achieved through first ensuring all sending servers are covered within the SPF policy, then through monitoring DMARC reporting and following up on any identified issues. *The key is identifying these mail flow issues prior to switching over to reject.*

DKIM alignment within DMARC

Another important consideration in DMARC is the option to enforce strict alignment of the mailfrom and sender domain addresses within DKIM. This is set through adkim=s (for strict) or adkim=r (for relaxed) within the DMARC record. The default is relaxed. It is recommended that strict alignment be implemented, however this can cause issues if there are other services sending on behalf of a domain. For instance, if adkim=s on the domain for minties.govt.nz and a message is sent via a Mailchimp server with a source address of something@minties.govt.nz the DKIM alignment will fail, as the mailfrom address will show as it being from minties.govt.nz, yet the sender domain appears as being from Mailchimp. The message will therefore likely be dropped.

The recommended solution is to have bulk mail senders operating from a different subdomain to end users, though it is understood changing existing services to this could be disruptive.

For example, consider the domain minties.govt.nz. If there are users configured within the domain minties.govt.nz and we can set up external mail senders in the subdomain mail.minties.govt.nz, this allows the application of different policies to those domains. The DMARC record for the root domain minties.govt.nz would contain adkim=s while the DMARC record for the mail.minties.govt.nz subdomain would have adkim=r.

This option gives recipient servers the highest confidence the message is genuine and provides the sender with the greatest assurance the message will be delivered to the destination mailbox.

Inbound messages and DMARC

In both Microsoft 365 and Google GCP, you don't need to configure anything specific to handle incoming DMARC. Both platforms automatically check incoming emails against the sender's DMARC policy. If the DMARC check fails, they will act based on the policy defined in the DMARC record (e.g., none, quarantine, or reject).

For other email providers it is up to the Agency to check and ensure their email service performs DMARC checks and acts on the senders' policies.

Emails which fail DMARC (either reject or quarantine) should never make it to the users' mailboxes. Where the sending domain policy has p=quarantine these emails should not go to users' junk mail folders but should go to the email platform quarantine for release only by administrators (secops team) after review. The expectation is these will not be valid business emails. Sending them to users' junk mail folders may result in phishing links being clicked on and followed.

Where the sending domain policy rejects the email, the email should be rejected and dropped.

DMARC Reporting Services

Control 15.2.36.C.06 of the NZISM requires Agencies to review DMARC reports on a regular basis. To adhere to this requirement a DMARC reporting tool is required. There are many SaaS DMARC reporting providers. Some will be made available via the Marketplace (marketplace.govt.nz)

DMARC Requirements

DMARC needs to be set to p=reject on all email enabled domains.

adkim=s is recommended where domains are not involved with bulk mail sending.

Inbound emails must be checked for DMARC compliance and acted on based on the sending domains DMARC policy.

Enforce DLP in line with the PSR and NZISM requirements.

Agencies are required to review and apply their own DLP settings. **DLP Requirement**

Enforce DLP in line with the PSR and NZISM requirements.

MTA-STS

MTA-STS provides recipients with the ability to prevent incoming TLS sessions from downgrading to sending in the clear. This prevents adversary-in-the-middle attacks on the STARTTLS session commands where they attempt to force messages to default back to send unencrypted to intercept them. MTA-STS uses certificate verification to ensure the destination domain is valid and traffic is not being maliciously re-routed. This protection will be superseded by DANE.

MTA-STS Requirement

MTA-STS needs to be enabled and set to 'enforce' on all email enabled domains.

9 Securing Non-email Enabled Domains

Purpose

The purpose of deploying email security to non-email enabled domains is to prevent spoofed messages from that domain. This requirement remains even if the root level domain has SP=reject set within its DMARC record.

Example 1 – Root Domain with no SPF, DKIM or DMARC record.

If there was a non-email enabled domain called minties.govt.nz with no SPF, DKIM or DMARC records, this domain could easily be used for the sending of spoofed emails. An email sent by a threat actor from CEO@minties.govt.nz would not specifically fail DMARC checks as any queries would respond with none (or no record found). The message would, in many cases, be delivered to the destination mailbox.

Example 2 – Sub Domain with no SPF, DKIM or DMARC record, but where the root domain has SP=reject set

If the domain minties.govt.nz existed with a DMARC record including p=reject and the owner had a separate transactional service called payme, they may create an A record of payme.minties.govt.nz. That domain can be spoofed with messages sent appearing to be from accounts@payme.minties.govt.nz (or any other address) probably requesting the end users pay some form of fee.

The root domain minties.govt.nz will be checked for a DMARC record, looking for the existence of an SP entry, however having SP=Reject in the root record will only partially resolve the issue. SPF and DKIM record checks do not go up to the root record. Both will return a 'none' result, and will pass DMARC checks, though with a lower reputation. The end result is these messages are still likely to be delivered to the destination mailbox.

The following settings apply to all non-email domains, sub-domains and all new domains. Sub-domains can consist of as little as a single A record. They set blank records for SPF & DKIM and set DMARC to reject. After these are set, given the same spoofing examples above the messages would fail all DMARC checks and almost certainly be dropped.

Implementation

Implementation of these SPF, DKIM and DMARC records remains with each Agency through their normal DNS change processes.

SPF

The required SPF record needs to deny all senders. This is achieved through having no sending servers listed in the SPF record and using the hard deny -all option. Any message received by a recipient MX server performing SPF checks server will be rejected and dropped as the sending IP address will not match the blank SPF list.

Example SPF Record:

Name	TTL	Type	Data	Comment
<yourdomainname>	3600	txt	"v=spf1 -all"	Blank SPF record to deny all senders

DKIM

The purpose of a DKIM record on a non-email enabled domain is to force all messages to fail DKIM. This is achieved through providing a DKIM key with no public key.

Example DKIM Record:

Name	TTL	Type	Data	Comment
*._domainkey<yourdomainname>	3600	txt	"v=DKIM1; p="	DKIM record with no public key

DMARC

DMARC provides the protection through directing recipient domains to reject messages which fail the SPF and DKIM checks above. The purpose of setting RUA reports is to provide you the ability to check for any sources attempting to spoof messages from those domains. This is especially useful where those domains might be related to contentious public interest sites or events where people may seek to promote their own agenda through impersonated emails.

For instance, there could be groups who wish to influence the public for their own cause. Those groups may seek to exploit any possible domain impersonation through sending spoofed emails. With the above SPF and DKIM settings in place along with the DMARC below, almost all emails will be dropped before reaching the destination mailbox. The exception is if the recipient MX server does not support, or is configured to ignore SPF, DKIM, and DMARC checks.

These settings set the alignment to strict for both SPF and DKIM, rejecting 100% of messages which fail those checks on both the root level and subdomains.

Example DMARC Record:

Name	TTL	Type	Data	Comment
_dmarc.<yourdomainname>	3600	txt	"V=DMARC1;p=reject; adkim-s; aspf=s; rua=mailto:<your dmarc report RUA email address>;"	DMARC reject everything and report.

10 Agency Deployment Checklist

The following table is a checklist for Agencies to ensure they meet the requirements of this framework.

Setting	Requirement
All Email Enabled Domains	
TLS	Enforce a minimum version of TLS1.2.
TLS-RPT	Enable TLS Reporting on all email sending domains.
SPF	Ensure you have an SPF record which ends in -all.
DKIM	Ensure all outbound emails to Agencies or public destinations are DKIM signed.
DMARC (Outbound)	Ensure all domains have a valid DMARC record which ends in reject. Domains not used for bulk mailing should use the flag adkim=s.
DMARC (inbound)	Ensure Inbound emails are checked for DMARC compliance and acted on based on the sending domains DMARC policy.
MTA-STS	An MTA record must be defined and set to enforce.
Implicit TLS	Implicit TLS must be configured and enforced for all connections.
DLP	DLP must be enabled in line with your Agencies requirements under the NZISM
All Non-Email Enabled Domains	
SPF	Set every sub-domains' SPF record to "v=spf1 -all"
DKIM	Set every sub-domains' DKIM record to "v=DKIM1; p="
DMARC	Set every sub-domains' DMARC record to "V=DMARC1;p=reject; adkim-s; aspf=s; rua=mailto:<your dmarc report RUA email address>;"