Implementing DCB1596 Secure Email in Google Workspace

Configuration guidance for Google Workspace Administrators seeking compliance with the NHS Digital Secure Email Standard

Standards Documentation

DCB1596: Secure Email - NHS Digital

https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb1596-secure-email

This implementation guide is for version 2.3 (Amd 7/2019) of the standard.

This guidance document only includes sections of the standards where a Google Workspace Administrator is required to take action to ensure compliance. The remaining sections of the standard are covered under the standard compliance statement for Google Workspace.

Google Workspace Security Health Page

For domains with Google Workspace Enterprise, we recommend this guidance is followed in conjunction with a review of the Google Workspace Security Health Page. The latest best practice for security and compliance in Google Workspace is published on this page, with a status check of your domain.

Get started with the security health page: https://support.google.com/a/answer/7491656

Implementation

Encryption (DCB1596 §5.1)	Compliant By Default
Transport Layer Security (TLS) is a security protocol that encrypts email to protect its privacy. TLS is the successor to Secure Sockets Layer (SSL). **Gmail uses TLS by default** (opportunistic encryption), but when a secure connection isn't available (both sender and recipient need to use TLS to create a secure connection), Gmail will deliver messages over non-secure connections. Please also refer to the below section on configuring MTA-STS. The DCB1596 standard recommends that organisations use the NCSC Mail Check service to validate their TLS configuration.	

Anti-Spoofing (DCB1596 §5.2)	**Action Required**
The standard requires that DMARC, SPF and DKIM be enabled for the domain. Administrators are recommended to configure SPF and DKIM first, then configure DMARC.	
Sender Policy Framework (SPF) Configuration Configuration of SPF involves creating DNS TXT records for your domain - you should contact your domain registrar for details on how to complete this configuration. • Configuring SPF: https://support.google.com/a/answer/33786	
DomainKeys Identified Mail (DKIM) Configuration Gmail will sign all outbound email by default, using the DKIM domain key d=*.gappssmtp.com. We recommend that you configure your own DKIM key for all outgoing messages. Configuration of DKIM involves creating DNS TXT records for your domain - you should contact your domain registrar for details on how to complete this part of the configuration. • Configuring DKIM: https://support.google.com/a/answer/174124	
Domain-based Message Authentication, Reporting and Conformance (DMARC) Configuration	

Gmail supports Domain-based Message Authentication, Reporting, and Conformance (DMARC) as a way to prevent this type of spam. Use DMARC to define how Gmail handles messages that appear to be sent from your domain but that are actually spam.

Configuration of DMARC involves creating DNS TXT records for your domain - you should contact your domain registrar for details on how to complete this part of the configuration.

It is required that you deploy a DMARC policy of p=quarantine, rising to p=reject within 3 months of implementation. The NCSC have detailed guidance on iterating your DMARC configuration.

You may wish to configure a Google Group within your Google Workspace environment to receive DMARC activity reports - e.g. dmarc@example.com. If you are using the NCSC Mail Check service, you should add mailto:dmarc-rua@dmarc.service.gov.uk to your record. For the quarantine policy, this could look like:

```
v=DMARC1;p=quarantine;sp=quarantine;rua=mailto:dmarc@example.com,mailto:dmarc-rua@dmarc.service.gov.uk
```

We recommend that DMARC is deployed slowly - using the policy (p) and percent (pct) options - and checking the DMARC activity reports regularly. As per DCB1596, the domain should be at `p=reject;pct=100` within 3 months of accreditation.

- Configuring DMARC: https://support.google.com/a/answer/2466563

MTA-STS and TLS-RPT

By default, Gmail messages from your domain comply with MTA-STS when sent to external servers with an MTA-STS policy in enforced mode.

Configuration of MTA-STS and TLS-RPT for inbound emails involves creating DNS TXT records for your domain and serving of configuration file over HTTPS - you should contact your domain registrar for details on how to complete this part of the configuration.

You may wish to configure a Google Group within your Google Workspace environment to receive MTA-STS and TLS-RPT activity reports - e.g. mta-sts@example.com.

A public facing web server with a certificate signed by a trusted third-party root CA is required to publish your MTA-STS policy.

- Configuring MTA-STS and TLS-RPT: https://support.google.com/a/answer/9261504
- Check your domain MTS-STS configuration: https://support.google.com/a/answer/9276419

Interoperability (DCB1596 §6.3.6)	Compliant By Default

DCB1596 requires that systems should interoperate using one (or a combination of):

1. The Government Secure Networks (Not Applicable to Google Workspace)
2. Secure TLS point to point connections (Compliant by default, as per Encryption section above)
3. S/MIME or other email encryption

Optionally (as TLS is enabled by default), Google Workspace Enterprise administrators can configure hosted S/MIME within Gmail. This requires that users are provisioned with a valid certificate (in PKCS#12 format), which is then uploaded to Google Workspace either programmatically (via the S/MIME API) or by individual users via the Gmail UI.

- Enable hosted S/MIME: https://support.google.com/a/answer/6374496

Offshoring (DCB1596 §6.3.7)	Compliant By Default

Google Workspace is provided across two regions by default - the US and Europe.

NHS Digital guidance is that Data *"must be held in the UK - European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield."*

The Google Workspace US region is covered by Privacy Shield, meaning Google Workspace is compliant by default.

Optionally, Google Workspace Administrators can choose to configure a more restrictive Data Region policy.

- Choose a geographic location for your data: https://support.google.com/a/answer/7630496