GOV.UK

1. Home (https://www.gov.uk/)

Guidance

Set up government email services securely

Configure email services securely using encryption and anti-spoofing.

Published 24 August 2016
Last updated 27 April 2020 — see all updates

From:
Government Digital Service (https://www.gov.uk/government/organisations/government-digital-service)

Contents

Print this page

Government email administrators should follow this guidance to implement encryption and anti-spoofing. This will help to make sure your email service is configured and runs in a secure way.

This is a generic guide. If you need specific information about an email provider or application contact the PSN team (https://emailassurance.zendesk.com/hc/en-us/requests/new?ticket_form_id=130185) or contact the vendor for advice.

All gsi-family domain names (https://www.gov.uk/government/publications/changing-government-email-migrating-from-gsi/changing-government-email-migrating-from-gsi) (gsi.gov.uk, gse.gov.uk, gcsx.gov.uk or gsx.gov.uk) must now be replaced with a government domain like gov.uk, gov.scot, llyw.cymru or gov.wales.

Prepare to secure your email service

An email service describes any system sending emails on behalf of an organisation. This includes:

- the service providing users with mailbox access
- internal relays and gateways
- email filtering services
- third party services that send email on your behalf, like transactional email services

To implement this guidance you need to configure your email service to:

- support Transport Layer Security (https://www.gov.uk/government/publications/email-security-standards/transport-layer-security-tls) version 1.2 (TLS v1.2) or later for sending and receiving email securely
- apply DomainKeys Identified Mail (https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim) (DKIM) signatures to outbound messages
- check Domain-based Message Authentication, Reporting and Conformance (https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc) (DMARC) on inbound email

You'll also need:

- to be able to make administrative changes throughout the email service
- a public domain name system (DNS) record you can edit for each email domain

Configure cloud or internet-based email services

Encrypt email in transit

TLS is an encryption protocol (https://www.gov.uk/government/publications/email-security-standards/transport-layer-security-tls) used to protect data in transit between computers. To encrypt email services use TLS version 1.2 or later, and preferred cryptographic profiles (https://www.ncsc.gov.uk/guidance/tls-external-facing-services) for secure email transport between UK government departments.

A small number of domains in the gov.uk namespace do not yet support TLS. If you choose to create a rule to require TLS for *.gov.uk you should create an exceptions list for those domains if you need to.

Create rules to require TLS for sending to *.gov.uk. A small number of .gov.uk domains do not yet support TLS. Create an exceptions list for those domains if you need to.

If you operate a .gov.uk domain that does not support TLS you should ask any government organisations you work closely with to add you to their exceptions list.

You can choose to require valid certificates for domains you exchange email with, although not all domains have implemented this yet.

Avoid creating rules to require TLS on inbound email as this can lead to messages being rejected. Ask the sending organisation to set up rules if you require it.

Follow NCSC guidance on TLS (https://www.ncsc.gov.uk/guidance/tls-external-facing-services) to make sure you are using a strong TLS cipher suite and an appropriate certificate authority (CA). Your certificates must use a common name (CN) or subject alternative name (SAN) that matches the relay hostnames.

Cloud-based email services include managed TLS certificates. If you operate an internet-facing email service, you must buy and manage appropriate TLS certificates from the Digital Marketplace (https://www.digitalmarketplace.service.gov.uk/).

You must enable opportunistic TLS by default for domains not included in the mandatory TLS rules. You can use self-signed certificates for opportunistic TLS.

Set up TLS Reporting (TLS-RPT) (https://www.hardenize.com/blog/smtp-tls-reporting-tls-rpt) - this sends you a report if someone tries to connect using TLS but fails. You can direct the reports to the NCSC Mail Check (https://www.ncsc.gov.uk/mailcheck) service at tls-rua@mailcheck.service.ncsc.gov.uk. In the future you'll be able to see a dashboard to show you what the reports mean. Create a record with:

Record type: TXT

Host or record name: `_smtp._tls`

Record value: `v=TLSRPTv1;rua=mailto:tls-rua@mailcheck.service.ncsc.gov.uk`

Authenticate email

To prevent email spoofing you must put policies in place to check inbound and outbound government email using DMARC.

Implement DMARC (https://www.gov.uk/guidance/set-up-government-email-services-securely#dmarc-record) by:

- publishing a DMARC record starting at p=none rising to p=quarantine or reject during implementation
- enabling inbound checking on your email service - this is usually the default setting

Implement Sender Policy Framework (SPF) by:

- publishing public DNS records for SPF, including all systems that send email, using a minimum soft fail (~all) qualifier

Implement DKIM by:

- publishing DKIM selector and policy records
- signing outgoing email following the DKIM standard
- disabling outbound email footers if you have an outbound email filtering service

Have matching forward and reverse (A and PTR) DNS records for the sending hostname.

Configure PSN-based email services

You should follow guidance on moving to modern network solutions (https://www.gov.uk/guidance/moving-away-from-legacy-networks) which are generally more flexible, current, cheaper and quicker to deploy than using bespoke services over dedicated networks.

All gsi-family domain names (gsi.gov.uk, gse.gov.uk, gcsx.gov.uk or gsx.gov.uk) must now be replaced with a government domain like gov.uk, gov.scot, llyw.cymru or gov.wales.

Encrypt email in transit

Providers of PSN-based email services should:

- use opportunistic TLS for secure email transport within the PSN - this does not require CA signed certificates
- publish mail exchanger (MX) records in their public DNS for all email domains classified Official, so people outside the PSN can email them securely

Authenticate email

Implement DMARC by:

- publishing a DMARC record in your public DNS record, starting at p=none rising to p=quarantine or reject during implementation
- enabling inbound DMARC checking in the PSN email filtering portal

Implement Sender Policy Framework (SPF) by:

- publishing an SPF record in your public DNS record, including all systems that send email, using a minimum soft fail (~all) qualifier
- enabling inbound SPF checking in the PSN email filtering portal
- including the MessageLabs email filtering service in your SPF records so that internet-based recipients can see the origin of incoming emails - to do this, add `include:spf.messagelabs.com` to your SPF record

Implement DKIM by:

- publishing DKIM selector and policy records
- signing outgoing email on all systems that send email - you can do this in the Symantec Email Security.Cloud portal
- disabling outbound email footers in the PSN email filtering portal - this is usually the default setting

Have matching forward and reverse (A and PTR) public DNS records for your sending hostname.

Configure other email sending services

Other email sending services may sit inside or outside your network, and use the same domain name as your users, or a subdomain. These email sending services include:

- email filtering services
- applications or scripts developed by or for your organisation
- cloud-based applications that send email like Salesforce or MailChimp
- line-of-business applications that send email like an HR or finance system

Encrypt email in transit

Use TLS (https://www.gov.uk/government/publications/email-security-standards/transport-layer-security-tls) version 1.2 or later for secure email transport between UK government departments. This is a requirement when purchasing any new email service for central government to comply with the Minimum Cyber Security Standard (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf).

Authenticate email

To authenticate email from other sending services do the following.

1. Include additional email sending services in your DMARC (https://www.gov.uk/guidance/set-up-government-email-services-securely#dmarc-record) and Sender Policy Framework (https://www.gov.uk/guidance/set-up-government-email-services-securely#spf-record) records.

2. Use DKIM signing (https://www.gov.uk/guidance/set-up-government-email-services-securely#DKIM-record). Cloud-based applications or email filtering services will provide their own DKIM signature. You will need to create an additional DKIM DNS record. For other services you may be able to use the same signature as your other email if you send them from the same domain.
3. Ask your service provider for information about applying DKIM signatures and including email sending services in your SPF record.
4. Consider using a separate subdomain for third party email services to simplify SPF and DKIM implementation.

Configure your DNS records

Create and iterate DMARC records

Read the DMARC guide (https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc) for more details on what it is and how it works.

Read NCSC on implementing DMARC (https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing) for more information.

You must also make sure digital services have a DMARC record (https://gdstechnology.blog.gov.uk/2016/06/28/updating-our-security-guidelines-for-digital-services/).

Create and manage DKIM

Read the DKIM guide (https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim) for more details on what it is and how it works.

Read the NCSC guidance on implementing DKIM (https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing) for more information.

It may be difficult to implement DKIM on legacy email services. In this case, you should upgrade to a compatible cloud-based service and email filtering service to apply DKIM instead of adding cost and complexity to your existing environment.

PSN-based email users can enable DKIM in the Symantec Email Security. Cloud portal (https://clients.messagelabs.com/). Make sure you have ‘Email Disclaimers’ disabled on inbound and outbound email and are using the ‘no disclaimer’ option on outbound emails. If disclaimers or other changes to the message are applied at this point invalidate the DKIM signature will be stripped.

Create and iterate SPF records

Read the SPF guide (https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf) for more details on what it is and how it works.

Read the NCSC guidance on implementing SPF (https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing).

Make DNS changes

DMARC, DKIM and SPF require you to make changes to the DNS records for your domains. The table below shows who to contact to make those changes.

Record type	DNS provider
*.gsi.gov.uk, *.gsx.gov.uk, *.gse.gov.uk, *.gcsx.gov.uk, *.x.gsi.gov.uk	Vodafone Contact GDS (https://emailassurance.zendesk.com/hc/en-us/requests/new?ticket_form_id=130185)
*.gov.uk or any other domains	Your registrar or DNS provider

Use the WHOIS search at the .gov.uk registry (https://community.jisc.ac.uk/janet-apps/whois) to find your registrar or DNS provider.

When requesting changes you must include specific information for each record. If given the option, set a short time to live (TTL) in DNS records so you can see changes quickly and fix issues.

DMARC

Record type: TXT

Host or record name: `_dmarc`

Record value: `v=DMARC1;p=none;fo=1;rua=mailto:dmarc-rua@dmarc.service.gov.uk,mailto:dmarc@<yourdomain.gov.uk>`

Create the email address and put your domain in place of `<yourdomain.gov.uk>`.

SPF

Record type: TXT or CNAME (check guidance for your service on which to use)

Host or record name: `@` (if required)

Record value: `v=spf1 include:<your email server domain> ip4:<your email service IP> ~all`

Put your email server domains and/or email sending IP ranges in place of the <> sections. You do not need to include both - in many cases you may only need `include:`.

DKIM

Record type: TXT

Host or record name: `selector._domainkey`

Put your selector, or the selector provider by your service provider, in place of selector in the host or record name.

Record value: `v=DKIM1; k=rsa; p=<your DKIM key>`

Paste your DKIM key from your key generator in place of `<your DKIM key>`

Some providers will use a CNAME record instead of a TXT record. Follow the guidance from your provider.

Check your email services are secure

Check your email certificates are valid and renewed

You must make sure your email certificates are valid and renewed, otherwise your organisation may not be able to send or receive emails securely.

Software as a Service email providers should manage your email certificates on your behalf. If you have issues with your certificates you should:

1. Check if you still need the domain.
2. Delete the domain if you do not use it anymore.
3. If you still use the domain, ask your certificate authority to replace your email certificates.
4. Register your domain with NCSC's Mail Check service (https://www.mailcheck.service.ncsc.gov.uk/) and make sure you set up notifications to receive security alerts.

There's more guidance about email certificates on the NCSC website (https://www.ncsc.gov.uk/guidance/provisioning-and-securing-security-certificates).

Check your email is authenticating

Your email may not work properly, be treated as spam or be susceptible to hijack if you have a:

- missing Sender Policy Framework (SPF) record
- misconfigured or poorly configured SPF record
- missing Domain-based Message Authentication, Reporting and Conformance (DMARC) policy
- weak DMARC policy

To check your email is authenticating, you should:

1. Implement the guidance on securing government email (https://www.gov.uk/guidance/securing-government-email) - including domains which do not send email.
2. Register your domain with NCSC's Mail Check service (https://www.mailcheck.service.ncsc.gov.uk/), and make sure you set up notifications to receive security alerts.

Check your email server is active and responsive

You must make sure your email server is active and responsive so that:

- your emails reach their destination
- there's a lower risk of emails being hijacked

To make sure your email server is active and responsive, you should:

1. Check your mail server (MX) records are correct (https://dnschecker.org/mx-lookup.php).
2. Fix any typos and remove inactive MX records.
3. Register your domain with NCSC's Mail Check service (https://www.mailcheck.service.ncsc.gov.uk/), and make sure you set up notifications to receive security alerts.

Check your email services are encrypting email

Make sure your email services are using TLS 1.2 or above to encrypt email in transit.

To make sure your email is encrypted in transit, you should:

- look at email logs in your email service
- register your domain with NCSC's Mail Check service (https://www.mailcheck.service.ncsc.gov.uk/)
- manually check your secondary email services also use TLS 1.2 or above

Communicate changes to your organisation

You should communicate email security changes to anyone in your organisation who is running:

- email filtering services
- applications or scripts developed by or for your organisation
- cloud-based applications that send email like Salesforce or MailChimp
- line-of-business applications that send email like an HR or finance system

You can also communicate these changes more widely across your organisation. It may be important to explain that this is a standard agreed across central government.

Published 24 August 2016
Last updated 27 April 2020 + show all updates

1. 27 April 2020
   Added information about checking email services and restructured document to make it clearer
2. 9 September 2019
   Clarifying information about encrypting email in transit and DNS changes.
3. 18 February 2019
   Added information to reflect updated guidance from NCSC and restructured content to increase clarity
4. 18 April 2018
   The approach to email security is changing and we have removed the need to pass an assessment.
5. 6 March 2018
   Updated to reflect that GDS is no longer performing the whitelist check as email assurance is being handed over the NCSC, which uses the MailCheck tool.
6. 5 March 2018
   Updated to reflect changes to PSN.
7. 25 August 2016
   In this update, CTS has: * changed and removed wording throughout the document to make it easier to understand * added steps to make it clearer what you need to do to implement the guidance * added technical detail previously included in 'securing government email' * changed the document title in line with GDS style * restructured the document around the three aspects of encryption, anti-spoofing, and assessment * removed references to ADSP as it is no longer used widely enough to be valuable Aside from ADSP these updates have not changed the guidance, only the presentation.
8. 24 August 2016
   First published.

Print this page

Brexit transition

39 days to go

Check you’re ready for 2021

(https://www.gov.uk/transition)

Related content

- Securing government email (https://www.gov.uk/guidance/securing-government-email)
- Protect domains that don’t send email (https://www.gov.uk/guidance/protect-domains-that-dont-send-email)
- How DFID migrated email from the PSN to the internet (https://www.gov.uk/government/case-studies/how-dfid-migrated-email-from-the-psn-to-the-internet)
- How Welsh public sector organisations migrated email from the PSN to the internet (https://www.gov.uk/government/case-studies/how-welsh-public-sector-organisations-migrated-email-from-the-psn-to-the-internet)
- Secure email guidance (https://www.gov.uk/government/collections/secure-email-guidance)

Collection

- Secure email guidance (https://www.gov.uk/government/collections/secure-email-guidance)