

Beschrijving “Veilige informatie-uitwisseling via e-mail”

1 Begrippen

Beveiligingskanaal: Het verzenden van e-mail via een verbinding waarbij het TLS-SMTP-protocol wordt gebruikt en de instellingen van TLS-SMTP voldoen aan de in hoofdstuk 2 opgenomen vereisten.

Domeinnaam: De naam in het Domain Name System (DNS), het naamgevingssysteem op internet, waarmee de mailserver wordt geïdentificeerd.

Technische vereisten: In hoofdstuk 3 zijn de vereisten opgenomen waaronder bij gebruik van het TLS-SMTP-protocol uitwisseling van vertrouwelijke informatie via e-mail mag worden toegestaan.

2 Methode van uitwisseling van informatie

Beide partijen dienen, na ondertekening van de overeenkomst, technisch af te dwingen dat gedurende de looptijd, e-mail uitsluitend wordt verzonden als aan de technische vereisten is voldaan. Als niet aan deze technische vereisten wordt voldaan mag de email niet (meer) worden verzonden. Hiermee wordt voorkomen dat de email via een onbeveiligd kanaal wordt verzonden.

In hoofdstuk 3 zijn de technische vereisten, te weten de eigenschappen/parameters van het TLS-SMTP-protocol.

De leverancier in kwestie kan voor het operationaliseren van de veilige e-mail verbinding contact opnemen met de contractmanager van de Belastingdienst.

Beschrijving “Veilige informatie-uitwisseling via e-mail”

3 Technische vereisten

3.1 Algemeen

- De verzendende partij heeft ingesteld dat onderlinge e-mail alleen verzonden mag worden via dit beveiligingskanaal.
- De mailserver van de ontvanger dient (START)TLS te ondersteunen. SMTPS wordt niet door de Belastingdienst ondersteund.
- De gebruikte combinatie van symmetrisch en asymmetrische encryptie algoritmen dient voldoende sterk te zijn (zie 3.4.)
- End-to-end versleuteling van e-mail berichten (X509, PGP, etc) wordt niet toegepast. Alleen het transportkanaal tussen de mailservers is beveiligd.
- Versleuteling van het transportkanaal is alleen gegarandeerd als de mailserver van de Belastingdienst en de andere partij rechtstreeks met elkaar communiceren.
- De verzender heeft ingesteld dat de e-mail voor de andere partij alleen versleuteld en pas na geldige verificatie van het certificaat mag worden afgeleverd.
- Minimaal één actieve mailserver behorend bij een domein dient aan de technische vereisten te voldoen.

3.2 Authenticatie van de mailservers

- De mailserver van de ontvanger, dient van een geldig certificaat te zijn voorzien dat is uitgegeven door een bekende en vertrouwde CA. Dit certificaat dient door de verzender te worden geverifieerd. De door de Belastingdienst uit te voeren authenticatie van de mailserver slaagt als aan één van de certificaatvoorwaarden in paragraaf 3.3 wordt voldaan
- De verzendende partij dient de “intermediate-certificaten” bij het aangaan van de TLS-SMTP-sessie mee te sturen.

3.3 Certificaat vereisten

Voor correcte TLS communicatie, tussen de mailservers is het van belang dat de gebruikte certificaten aan een aantal voorwaarden voldoen. Indien dit niet het geval is functioneert de veilige emailuitwisseling niet.

De volgende twee velden van het certificaat op de mailserver van de ontvanger zijn erg belangrijk voor het opzetten van de TLS verbinding tussen twee mailservers. Dit zijn:

1. Common Name (CN);
2. Subject Alternative Names (SAN).

Bij de verificatie van het certificaat stelt de Belastingdienst allereerst de **Presented Identity** (verder PI) van de ontvangende mailserver vast. De PI is gelijk aan de SAN van het certificaat, als deze in het certificaat is opgenomen. Indien het certificaat geen SAN heeft of de SAN leeg is, dan is de PI gelijk aan de CN van het certificaat.

Vervolgens moet aan één van de volgende voorwaarden worden voldaan.

1. De domeinnaam die in de bestemming van de email staat is in de PI opgenomen. Dit hoeft geen exacte match te zijn (wildcards zijn toegestaan).
2. De Full Qualified Domain Name (FQDN) van de betreffende mailserver waarop de mail moet worden afgeleverd, is in de PI opgenomen. Dit hoeft geen exacte match te zijn (wildcards zijn toegestaan);

Bovenstaande verificatie-vereisten zijn hard geprogrammeerd in de hardware van de Belastingdienst.

Beschrijving “Veilige informatie-uitwisseling via e-mail”

3.4 TLS-SMTP-settings Mailserver

Onderstaand overzicht geeft de op het moment van afsluiten van de overeenkomst voor het TLS-SMTP-protocol toegestane algoritmen die volgens de Belastingdienst voldoende sterk zijn. De volgorde is van sterk naar zwak. De mailserver bevat steeds de op het moment van verzenden/ontvangen toelaatbare algoritmen. Deze kan dus afwijken van onderstaande lijst.

De combinatie van symmetrische en asymmetrische encryptie algoritmen die gebruikt mogen worden zijn:

ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AESGCM(256)	Mac=AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(256)	Mac=SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(256)	Mac=SHA384
DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
DHE-RSA-AES256-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(256)	Mac=SHA256
DHE-DSS-AES256-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(256)	Mac=SHA256
AES256-GCM-SHA384	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(256)	Mac=AEAD
AES256-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(256)	Mac=SHA256
ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AESGCM(128)	Mac=AEAD
ECDHE-RSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=RSA	Enc=AES(128)	Mac=SHA256
ECDHE-ECDSA-AES128-SHA256	TLSv1.2	Kx=ECDH	Au=ECDSA	Enc=AES(128)	Mac=SHA256
DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
DHE-RSA-AES128-SHA256	TLSv1.2	Kx=DH	Au=RSA	Enc=AES(128)	Mac=SHA256
DHE-DSS-AES128-SHA256	TLSv1.2	Kx=DH	Au=DSS	Enc=AES(128)	Mac=SHA256
AES128-GCM-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AESGCM(128)	Mac=AEAD
AES128-SHA256	TLSv1.2	Kx=RSA	Au=RSA	Enc=AES(128)	Mac=SHA256