

# E-mail - SPF - DKIM - DMARC

## Cenário

Usamos correio eletrónico in-house, neste caso Exchange 2016 e pretendemos ter SPF, DMARC e DKIM ativos.

## SPF

*Sender Policy Framework* - ajuda a prevenir spoofing pois permite a verificação pelos destinatários de que e-mail recebido foi de facto enviado por quem está declarado.

Neste caso, foi colocada a seguinte linha, nos DNS's externos:

```
IN TXT "v=spf1 ip4:192.168.1.10 -all"
```

```
IN TXT "v=spf1 ip4: IP. IP. IP. IP -all"
```

**Notas:** A linha acima declara ser um registo SPF com o **v=spf1**, que todo o e-mail @vossodomínio.pt só pode ter origem no IP IP.IP.IP.IP e o **-all** define que o que não tiver essa origem é para ser considerado spam.

Para mais [info](#) e [aqui](#).

## DKIM

*DomainKeys Identified Mail* - assegura a integridade do e-mail enviado, apondo uma assinatura digital no cabeçalho de cada um, permitindo que a quem o recebe, verifique a sua autenticidade.

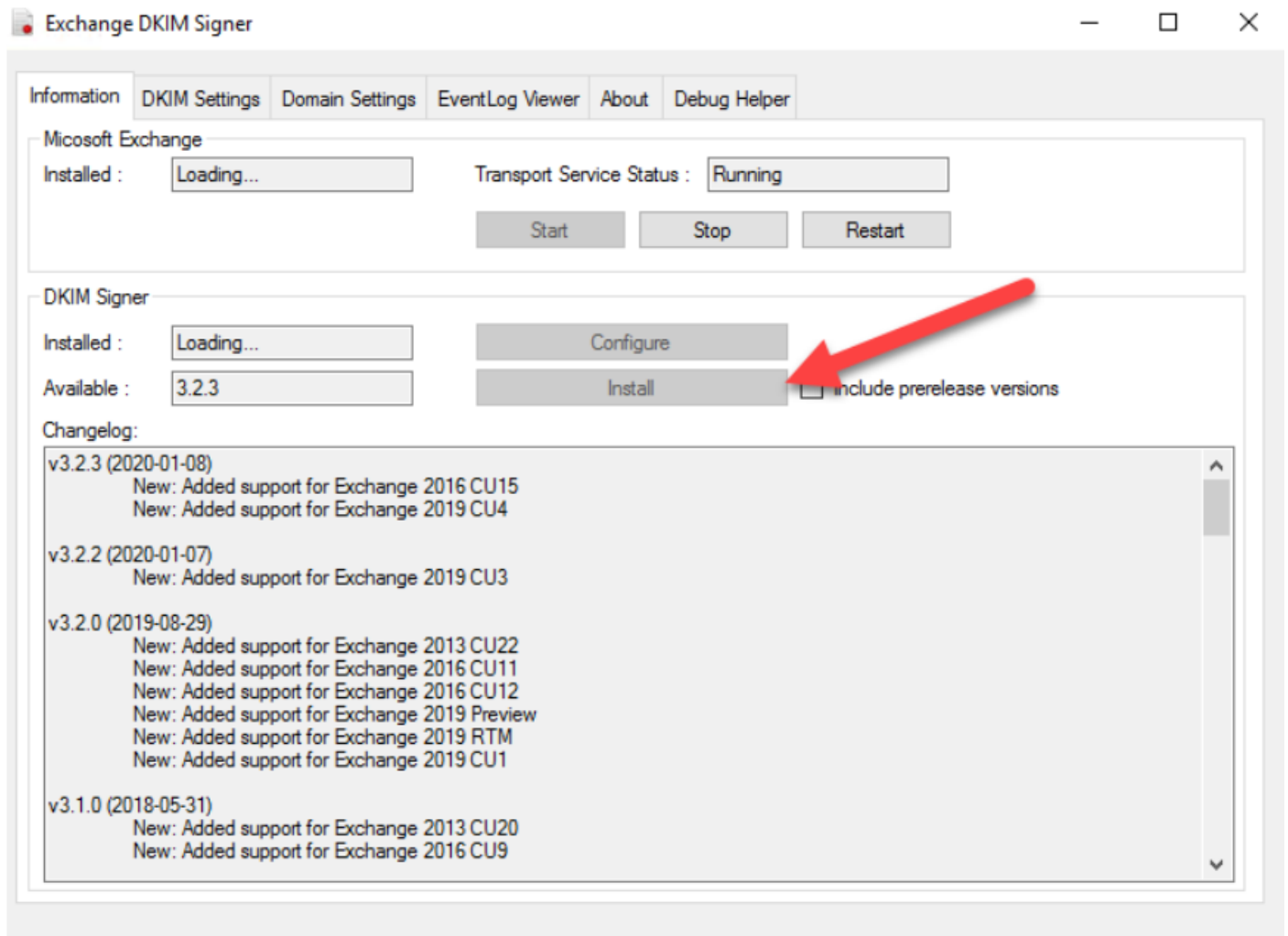
Resumidamente, o cabeçalho de cada e-mail que sai é cifrado usando a chave privada e quem o recebe usa a chave pública, que temos publicada no DNS externo, para assegurar que fomos nós que o enviamos.

Para habilitarmos DKIM usamos o script presente [aqui](#).

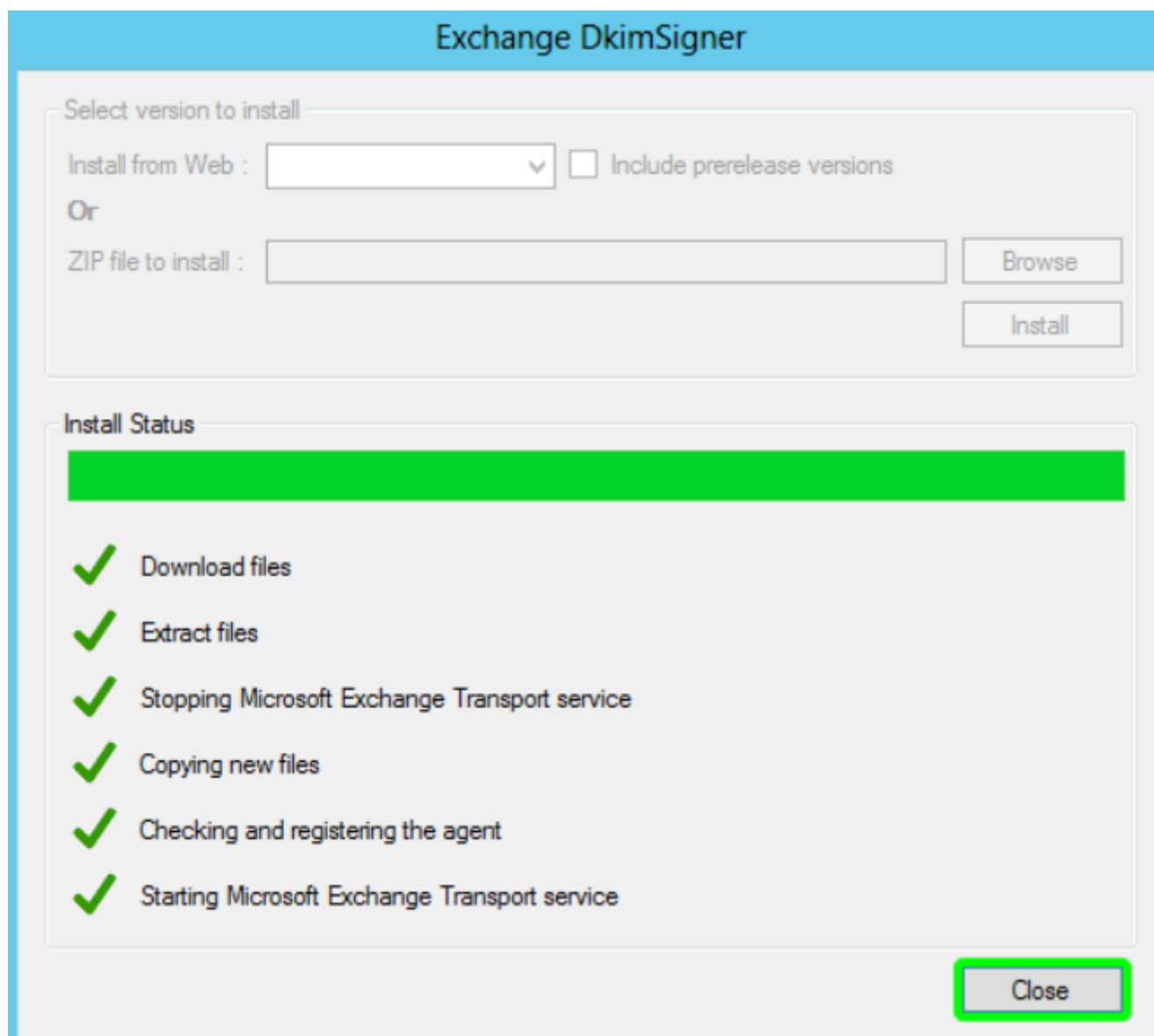
No servidor MX, [descarregamo-lo](#) e descompactamos.

Executamos como Administrador o "**ConfigurationDkimSigner.exe**".

Quando arranca, esperamos até que a função "**Install**" esteja disponível:



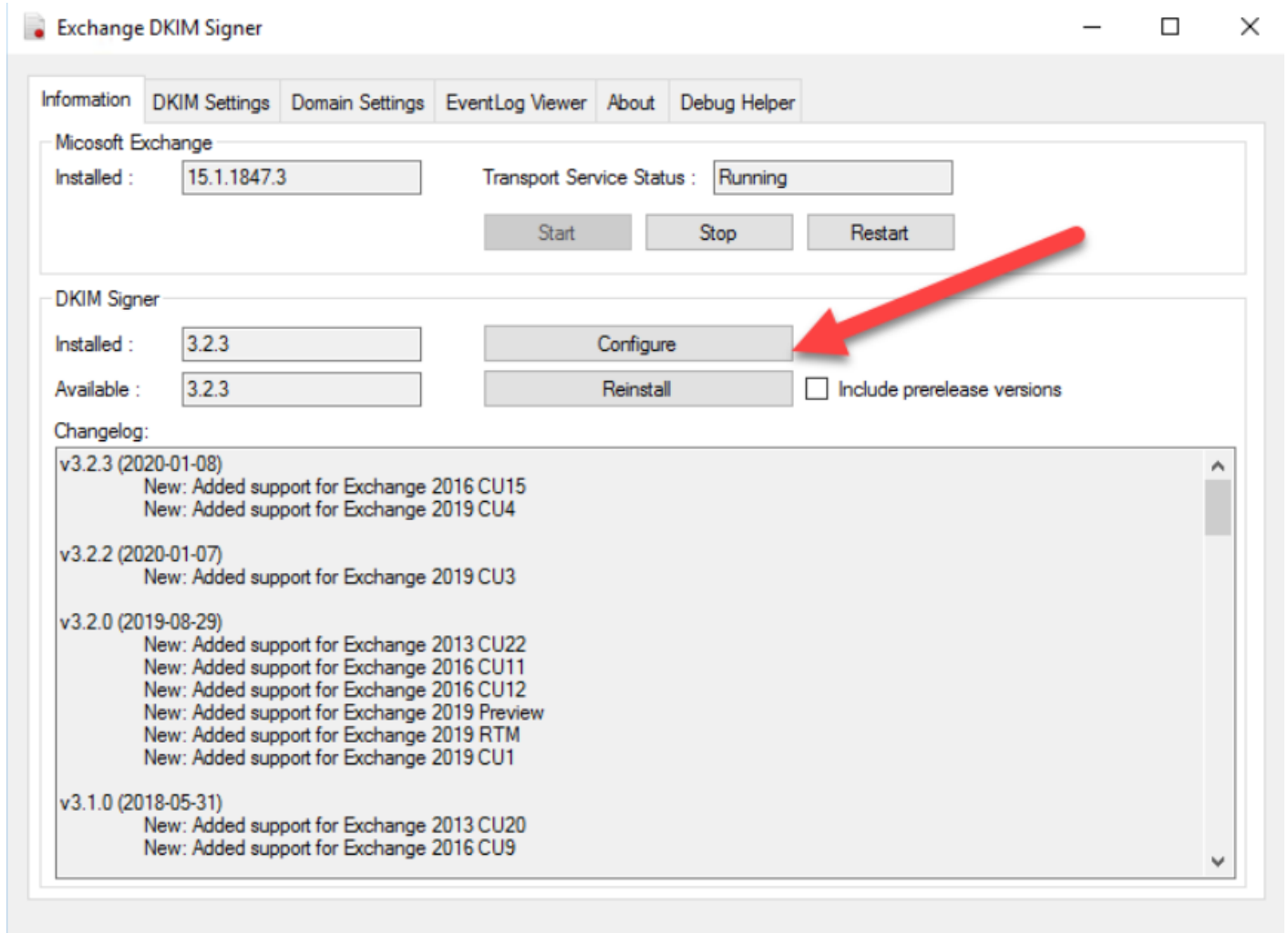
Instalamos e esperamos que o processo termine. Fechamos a janela em "**Close**":



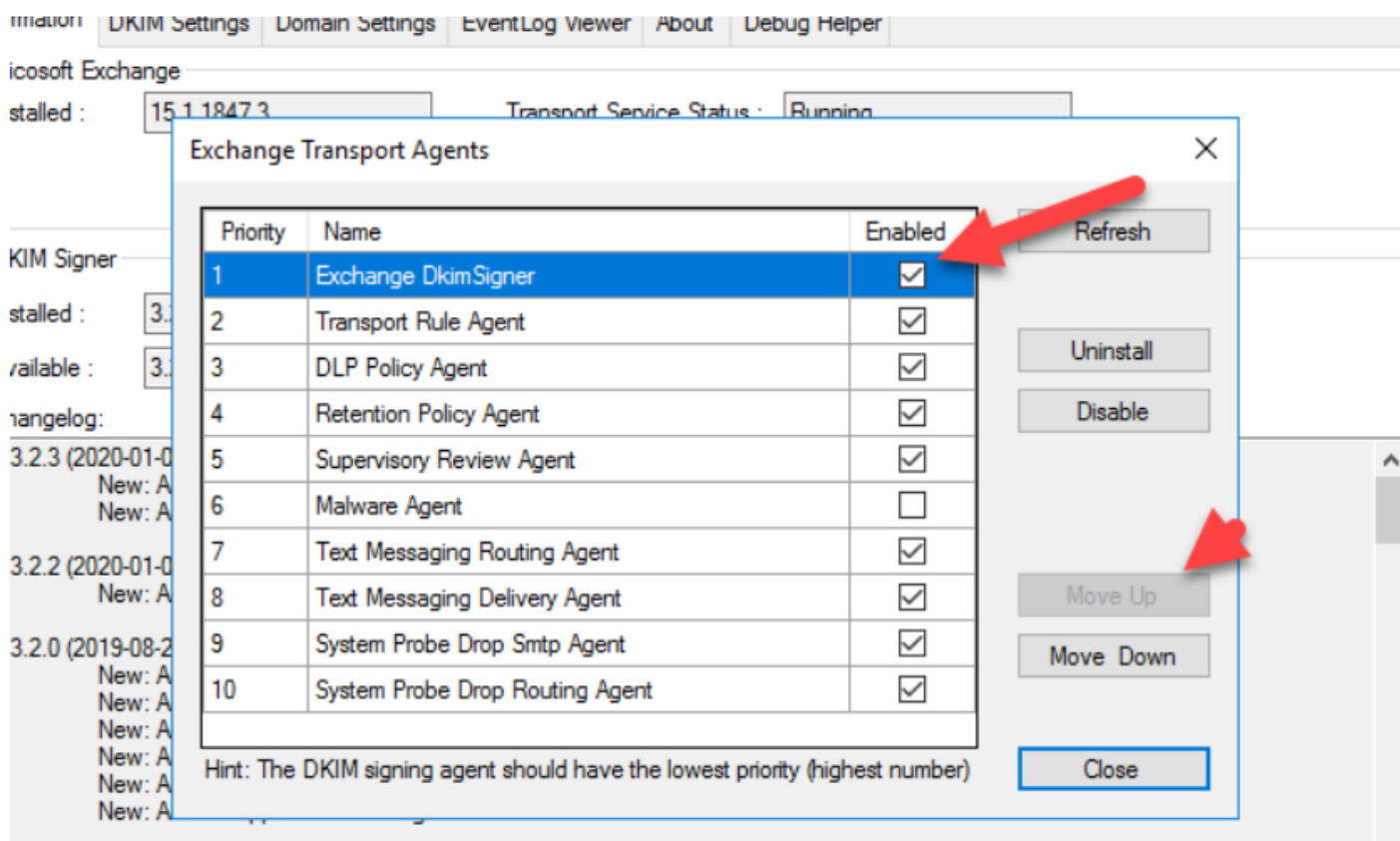
## Configuração

Arrancamos, com direitos de Administrador, com a aplicação "**Configuration.DkimSigner.exe**" presente em "**C:\Program Files\Exchange DkimSigner**".

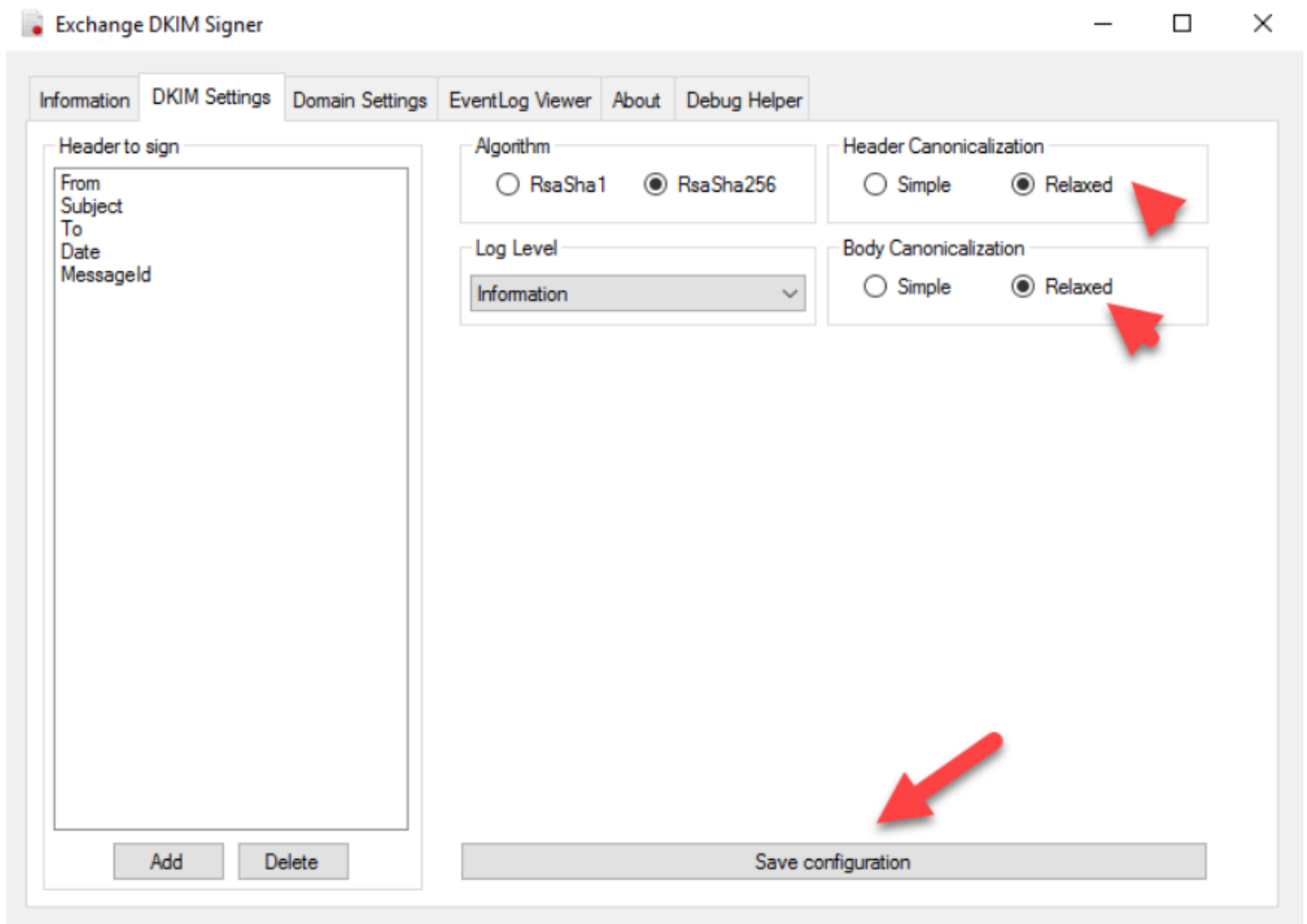
Tão logo abra e reporte que o "**Transport Service Status**" está "**Running**", clicamos em "**Configure**":



Movemos o agente "**Exchange DKIMSigner**" para o **topo**, se não estiver e clicamos em "**Close**".



Vamos ao separador "**DKIM Settings**" e definimos as opções "**Header Canonicalization**" & "**Body Canonicalization**" como "**Relaxed**" e guardamos a configuração em "**Save configuration**":



Vamos ao separador "**Domain Settings**", clicamos no botão "**Add**", definimos "**Domain name**" (no nosso caso xyz.pt apesar de na imagem estar rasurado e .com) e um **Selector** (no nosso caso escolhemos "**20200421**" mas é arbitrário) e pressionamos "**Generate new key**":

Information DKIM Settings Domain Settings EventLog Viewer About Debug Helper

## Domains

.com



Add

Delete

## Domain details

Domain name: .com

Selector: 20200421

Private key filename: .com.pem

Key length for generation: 2048

Generate new key

Select key file

Suggested DNS Name: 20200421.\_domainkey. .com.

Suggested DNS Record:

```
v=DKIM1; k=rsa;  
p=MIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApyopgaRuwFL  
Cb  
+14CcvtvhC5d9pUvpCLQdF4z0POvj72vYNoDcS/xMP1M9fT3RE/h7s/a  
HmR1+ai6othlcPOeF/NzRxm8T4YCMQGbDhVMjDnXSoNDXCThZS9ZoeIN  
09KNSp0Sn8PsacWu  
+QQbWPNrOw7iGUUnnu/hr1Nqpj6tdBfyRAqf7Ko3pxgLRFGjCKERjaxLKhrB  
+lDwVkwlrGc3+LyAntd93A5bQXvyNAb2MwS8kjq0XK5t5Jbt/gFdaXlcBG
```

Copy to clipboard

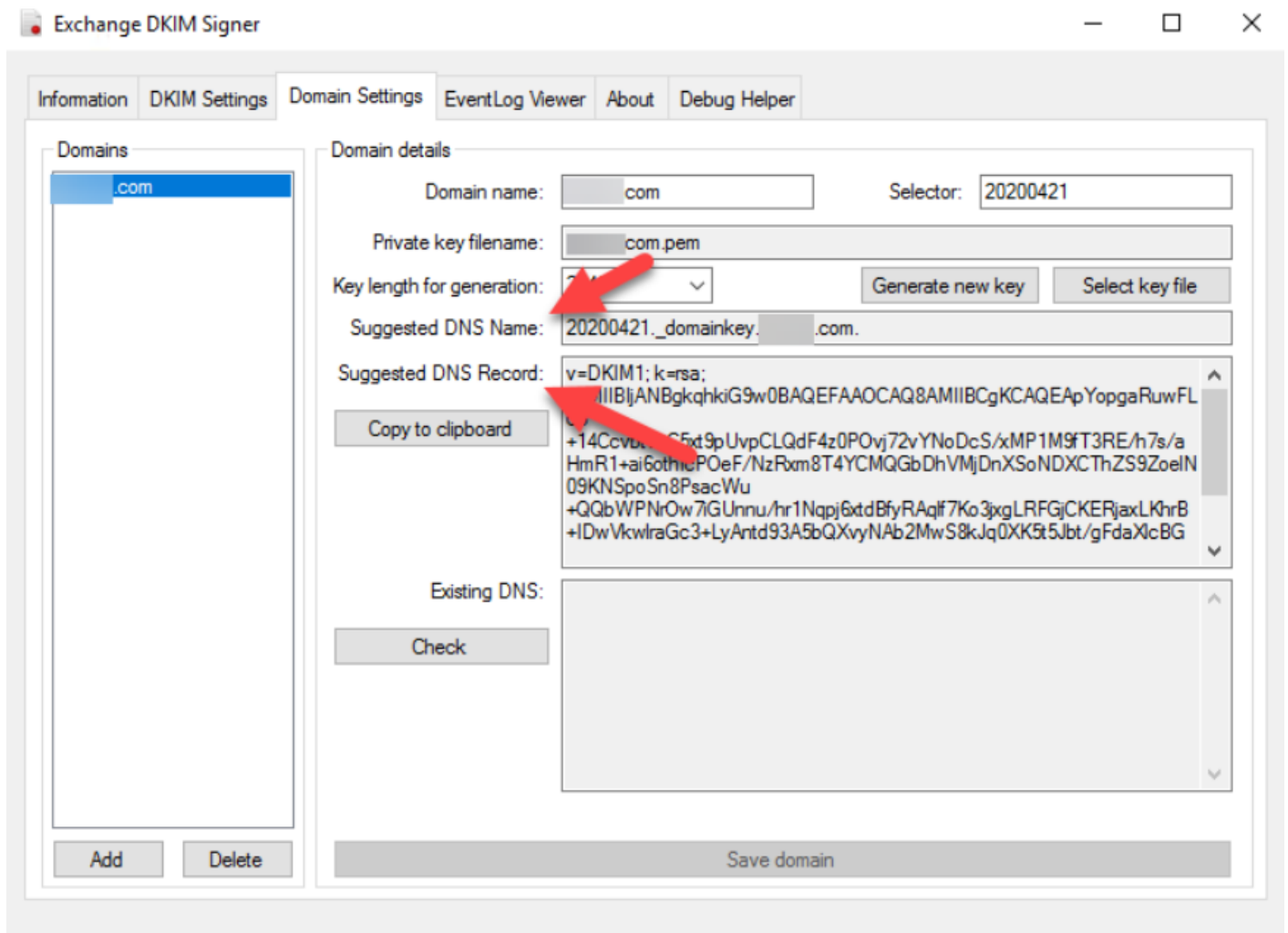
Existing DNS:

Check

Save domain







Após o que guardamos o domínio clicando em "**Save domain**":

Exchange DKIM Signer

Information DKIM Settings Domain Settings EventLog Viewer About Debug Helper

Domains

.com

Domain details

Domain name: com Selector: 20200421

Private key filename: com.pem

Key length for generation: 2048 Generate new key Select key file

Suggested DNS Name: 20200421.\_domainkey.com.


Suggested DNS Record: v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApyopgaRuwFLCb+14CcvbtvhC5xt9pUvpCLQdF4z0POvj72vYNoDcS/xMP1M9fT3RE/h7s/aHmR1+ai6othlcPOeF/NzRxm8T4YCMQGbDhVMjDnXSoNDXCThZS9ZoelN09KNSp0Sn8PscWu+QQbWPNrOw7iGUUnnu/hr1Nqpj6tdBfyRAqlf7Ko3xgLRFGjCKERjaxLKhrB+IDwVkwlrGc3+LyAntd93A5bQXvyNAb2MwS8kJq0XK5t5Jbt/gFdaXlcBG

Copy to clipboard

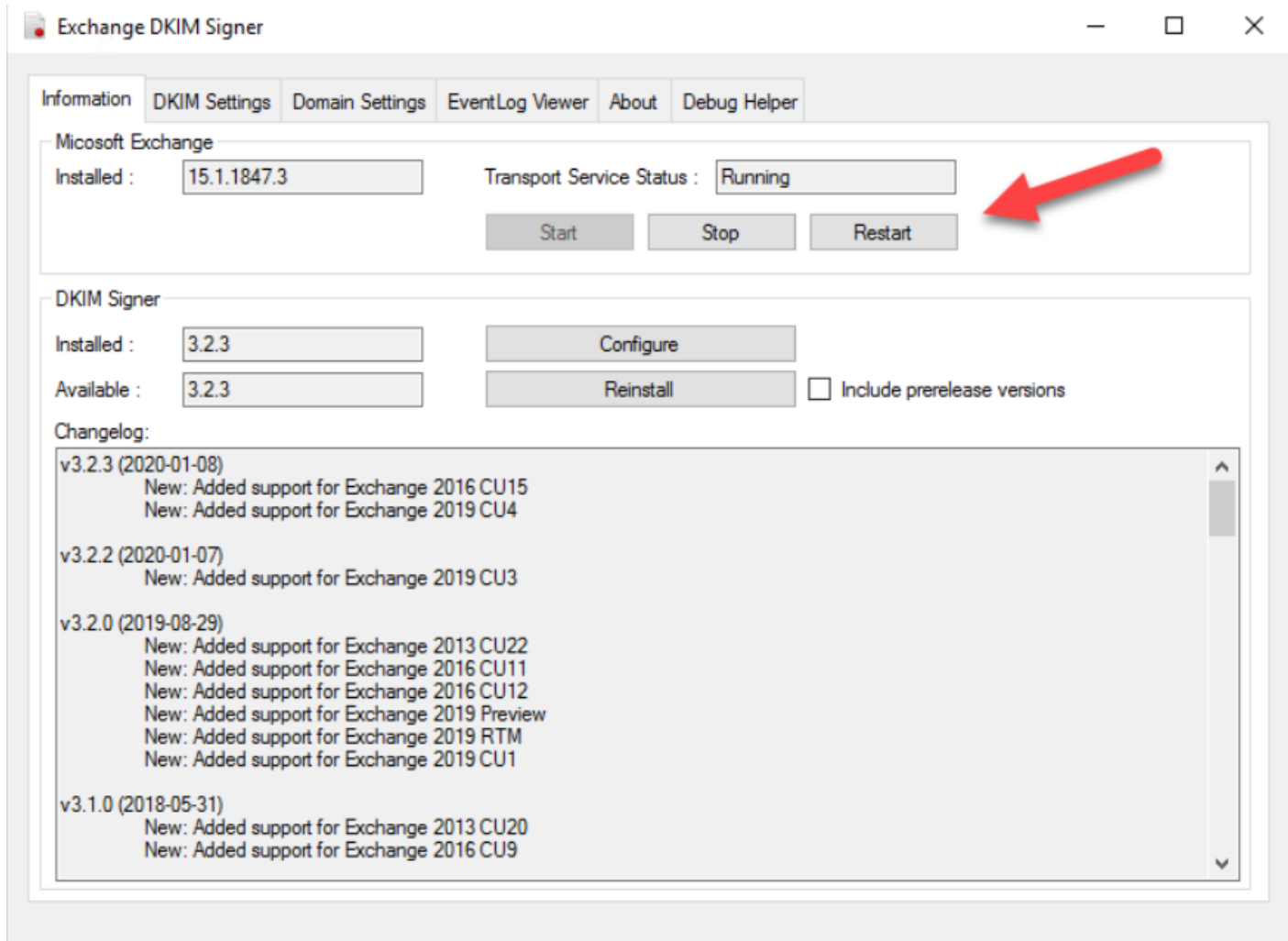
Existing DNS:

Check

Save domain



Vamos ao separador "**Information**" e reiniciamos o "**Transport Service**" (demora um bocado a reiniciar):



Neste cenário, a chave privada foi também colocada na **Sophos XGS** em:

## Email

Policies & exceptions

Data control list

SMTP quarantine

Mail spool

Mail logs

Encryption

**General settings**

Quarantine settings

Address group

\*\*\*

DKIM verification failed.

Accept

Invalid DKIM signature.

Accept

No DKIM signature found.

Accept

Apply

### DKIM signing



Domain



Key selector

Private RSA key

Manage



[Redacted]

dkim

[Redacted] RSA PRIVATE KEY-----

[Redacted]

Add

Delete

### Advanced SMTP settings

Reject invalid HELO or missing RDNS

☒ Enable [i](#)

Do strict RDNS checks

☒ Enable [i](#)

Scan outgoing mails

☒ Enable [i](#)

Route inbound mail through gateway

☐ Enable [i](#)

BATV secret

\*\*\*\*\*

[Show secret](#)

Apply

DKIM signing

Domain \*

Key selector \*

Private RSA key \*

```

-----BEGIN RSA PRIVATE KEY-----
[Redacted Key Content]
-----END RSA PRIVATE KEY-----

```

Save

Cancel

Para testar se o DKIM está a funcionar, podemos usar [este teste](#).

Para mais [info](#).

## DMARC

O *Domain-based Message Authentication, Reporting, and Conformance (DMARC)*, trabalha em conjunto com o *SPF* e o *DKIM* para assegurar a autenticidade dos originadores de correio eletrónico.

Assegura que os sistemas de correio eletrónico de destino confiam nos e-mails por nós enviados, ajudando os sistemas a decidir o que fazer com o correio eletrónico recebido.

Nos nossos DNS's externos colocamos a linha abaixo:

```
_dmarc IN TXT "v=DMARC1; p=reject; rua=mailto:a`m`n[s`r :0.0.0.0]
```

sendo que os valores são

```
v=DMARC1; p=reject; rua=mailto:vossoemail@vossodominio.pt;  
ruf=mailto:vossoemail@vossodominio.pt; sp=reject; adkim=s; aspf=s; ri=86400
```

A linha acima tem definido o seguinte:

**v=DMARC1;** - define a versão Dmarc e é obrigatório ser DMARC1;

**p=reject;** - é uma flag obrigatória e definida como p, rejeita e-mail não autenticado e envia relatório ao originador;

**rua=mailto:vossoemail@vossodominio.pt;** - para onde são enviados relatórios de ações tomadas;

**ruf=mailto:vossoemail@vossodominio.pt;** - endereço que receberá relatórios de erro;

**sp=reject;** - rejeita e-mail não conforme e envia relatório ao originador;

**adkim=s;** - define que o alinhamento com o DKIM é rigoroso ou seja, não está assinada é rejeitada;

**aspf=s;** - define que o alinhamento com o SPF é rigoroso ou seja, se não respeita definições SPF, é para ser descartado;

**ri=86400;** - intervalo de tempo em segundos, neste caso, 24 horas, para envio de relatório agregado.

**Nota:** Apesar deste cenário descrever implementação de SPF, DKIM e DMARC com Exchange in-house, podem usar a informação na [cloudflare](#), etc.

Para mais [info](#) e [aqui](#).

# Doação

**Se o acima te trouxe valor, aceito com gratidão uma doação**

[CoinRequest button](#)