RFC 8301 says:

rsa-sha1 MUST NOT be used for signing or verifying.

Signers MUST use RSA keys of at least 1024 bits for all keys. Signers SHOULD use RSA keys of at least 2048 bits.

Generate keypair

```
openssl genrsa -out dkim.server.com.key 2048 -outform PEM
openssl rsa -in dkim.server.com.key -out dkim.server.com.pem -pubout -
outform PEM
```

Choose domain selector

Each key has assigned a label called domain selector. For domain **server.com**, selector will be i.e.: **20150726._domainkey.server.com**

Example DNS entry will be:

```
20150726._domainkey.server.com IN TXT "k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC30aRx6rlDA7LkhsM1AtuW8LoBrjo6RZH3yS
7nC9EgqV5ntFIzQyCo88hNBz72XwwFAAGKuCVIwcxV06lAHWnUTt+ZyjJlP/4XJo9JH76ZJu9vUT
aHw753IY3SZR+xEnJuyBr/LZknAEFqHuDP7V3+B6SWuBElSFFnImnP7oeMQQIDAQAB"
```

Configure exim4

In Debian, use **exim4-daemon-heavy** package. Change owner of private key file to be readable by exim4. In Debian exim4 user is **Debian-exim**. Put private key in */etc/exim4 directory*. In /etc/ssl exim4 cannot find file (chrooted?) remote_smtp transport is running under user 101 (Debian-exim) group 42 (shadow) In **exim4.conf** under **remote_smtp** transport add:

```
  dkim_canon = relaxed
  dkim_selector = 20180410
  dkim_domain = spox.org
  dkim_private_key = /etc/exim4/dkim.server.com.key
#  dkim_strict = true # optional - causes signing failures to defer
(requeue)
```

References

Setting up multi-domain DKIM with exim + Debian What is DKIM? Everything You Need to Know About Digital Signatures

Tools

https://protodave.com/tools/dkim-key-checker/