DKIM Setup for Send Mail from Visbo ReST Server

DKIM is used to sign an e-Mail and allow the recipient mail server to verify that this mail was generated on behalf of the sender organization.

This is done with a pair of public and private key, where the public key is published in the DNS Entry of the respective domain.

The private key is used for generating the signature on the server side, where the mail is generated. As long as the server has the private key, it can be any server and must not be part of the domain of the sender e-Mail.

I have configured this for newsletter2go, where the newsletter2go server generates mails on behalf of visbo.de. I am not sure if it is also required to configure this if the ReST Server uses the visbo.de e-Mail server to send the e-Mails. At least I have not found any DNS entry for DKIM beside newsletter2go, so it could be that it can be configured globally for all e-Mails from all addresses.

At the moment I try to configure it for the ReST server only. Here are some Documents I have used:

- DKIM HowTo: https://dkimcore.org/specification.html
- DKIM and nodemailer: https://nodemailer.com/dkim/
- Configure DNS at 1and1: https://mein.1und1.de/domain-dns-settings/visbo.de

Values I have used:

Name	Value	Description
Selector	visbo2019	name must be alphanumeric no capitals
Token	visbo.de	Domain of the Mail Sender

The Keys will be generated on the ReST server using openssl but instead of the proposal using keys with length 1024, not sure if we should increase key length to 4096.

The DNS entry for newletter2go is:

Name	Value	Description
Hostname	newsletter2go._domainkey	newsletter2go is the selector
Value/Wert	v=DKIM1; k=rsa; p=MIG...	p= contains the public key
TTL	1h	TimeToLive

The DNS entry for teh Visbo ReST Server is:

Name	Value	Description
Hostname	visbo2019._domainkey	visbo2019 is the selector
Value/Wert	v=DKIM1;t=s;n=core;p= MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMdnU4fbaUjkJM/2WH915WBgzi JYA4NkskN4NgsW4gYAcWYK7vSyn9o+bUGTgbtBGYSLCIaosrObypuKHkPKx30c38 3nRkqA3aJTUzSNbnzWV1I8hxTmVZOsaAuchJM3pYupihFAPdd40xMPokWdFIVZdV CdUrypzTKrO+D0SBnQIDAQAB	v=DKIM1 ist the version number t=s any domain name in the headers must be related to the same domain n= notes that might be of interest by human? p= contains the public key At the moment it is unclear how to handle the trailing equal signs
TTL	1h	TimeToLive

The Page https://dkimcore.org/c/keycheck delivers success for the DNS entry, so it seams to be correct.

On the ReST Server we need to extend the nodemailer configuration to use the DKIM Signing if the Keys are available.
The .env configuration that contains the SMTP Config has to be extended:

- SMTP Config add DKIM Properties
  "dkim": { "domainName": "visbo.de", "keySelector": "visbo2019" }

- Private Key & Public Key
  Store the PEM Format for Private and public key under /etc/visbo/visbo.de.priv and /etc/visbo/visbo.de.pub
- The Mail Component evaluates the SMTP Config value and either deletes the DKIM Property if the private key is not available or adds the private key to the SMTP Config value.

How to verify that the signature is appended and is valid?