Go to https://www.ends2ends.com/ and follow link to test account (currently: https://www.ends2ends.com/email.cgi)

Enter a desired username like “naticka”

Enter a corresponding password for testing like “whatnot”. Don’t use anything special since these are only test accounts.

Enter the promo code supplied via another channel.

Click Create

Print the corresponding response page since it will not be offered again. Here is an example:

```
Email account naticka@testemail.ends2ends.com created!
incoming/outgoing server: testemail.ends2ends.com
IMAP SSL Port 993 naticka/pass
SMTP TLS Port 587 naticka/pass
SMIME certificate bundle (encrypted w/ your pass) has been emailed to you.
 (Test root CA Certificate here
    issuer/subject: ZX Communications Certificate Authority
    thumbprint: 14af4496d4ab4fd3633814ebb6c32a6b53511bd6 )
SMIMEA Record: naticka@testemail.ends2ends.com.smimea.txt
 .. submitting to DNSSEC servers. To check, do:
  dig -t type53
3354f0f7b62c3a65eea601f54f45ddfed61be95425384305c9f49530._smimecert.testemail
.ends2ends.com.
 Once you get a response (few minutes) you may send a S/MIME signed email
 to checkme@ends2ends.com to test.
..
..
```

Follow the instructions on your Outlook desktop client (restated below).

Adding the new email account to Outlook [NOTHING NEW]:

File->Account Settings

[for Office 2016 or Microsoft/Office 365: Manage Profiles->email accounts]

New->Manual setup or additional server types

Next->POP or IMAP->Next

Fill in

Your name: username (“naticka” in this example)

Email Address:username@testemail.ends2ends.com (naticka@testemail.ends2ends.com in this example)

Account Type: IMAP

Incoming mail server: testemail.ends2ends.com

Outgoing mail server (SMTP): testemail.ends2ends.com

Logon Information:

User Name: username (“naticka@testemail.ends2ends.com” in this example)

Password: the password you entered on creation (“whatnot” in this example)

Check the “Remember password” box

More Settings->Outgoing Server

Check “My outgoing server requires authentication”

Check “Use same settings as incoming mail server”

Click “Advanced” tab

Incoming server (IMAP): 993/SSL

Outgoing server (SMTP): 587/TLS or STARTTLS

OK

Next (causes Outlook to check settings)

Close the “Test Account Settings” pop-up

Finish

Close

You should now see customary Microsoft test email and email from this test system.

This test email will have your new SMIME certificate and private key attached to it.

Installing an SMIME and related certificates [NOTHING NEW]:

Double click on the attached .p12 file.

Click “Open” on the pop-up warning or, if you want to analyze first, “Save”.

The “Certificate Import Wizard” should pop-up.

Pick “Current User" then “Next”

“Yes” ON “User Account Control” pop-up if it appears.

“Next” on import wizard which leads to a Password prompt.

Enter the password used to create the account (“whatnot” in this example).

Check the box for “Mark this key as exportable” then “Next”.

Leave “Automatically select the certificate store…” checked and click “Next”

Windows may pop up a security warning regarding the installation of the test certificate authority. If you wish to verify the authenticity of the test root certificate, compare the thumbprint shown in this pop-up with that shown in the email you received for “ZX Communications Certificate Authority” (or go to https://www.zxcominc.com/ca/ to get thumbprint) before clicking “yes”

“Finish”

[You may use certmgr.exe to view the 3 new certificates - one in "Trusted Root Certification Authorities", "Intermediate Certification Authorities", and in "Personal".]

Now tell Outlook to use this S/MIME certificate[i] [NOTHING NEW]:

On Outlook client:

FILE->Options->Trust Center->Trust Center Settings->E-mail Security

Under "Encrypted e-mail" heading -> Settings

Click “New”

Fill in your new email address in "Security Settings Name" (naticka@@testemail.ends2ends.com in this example)

Under "Certificates and Algorithms" click top “Choose” button

Click "More choices" if it shows up.

Scroll and click on the new certificate corresponding to new email/.p12 file

Ok

Ok on Change Security Settings pop-up

OK on Trust Center

OK on Outlook Options

Check to see if things worked [NOTHING NEW]:

Send a SMIME SIGNED test email to checkme@ends2ends.com from this new account:

Click “New Email”

In pop-up click “OPTIONS” tab then click “Sign” (near “Encrypt”)

To: checkme@ends2ends.com

Subject: whatever

Body: 123 testing

Send

In a few seconds you should have a response from our test email server.

THE NEW PART:

Try to send encrypted email to checkme@ends2ends.com (clicking Encrypt instead of Sign above). This will fail since your Outlook client has no way of knowing what certificate/key to use for checkme@ends2ends.com or any other recipients that are not in your local enterprise database (e.g. GAL).

To overcome this you can install ES2ES (or, at reduced functionality, add ldap.ends2ends.com to your Outlook address book for testing*) for global, seamless end to end secure email exchange. See instructions on our main web page www.ends2ends.com.

After installing ES2ES, you should be able to send an encrypted email to checkme@ends2ends.com.

Note: All the steps prior to this labeled “NOTHING NEW” are already handled as part of any SMIME Outlook deployment. They are presented above as FYI.

***summary: File->Account Settings->Address Books->New->LDAP->Next->ldap.ends2ends.com->Next->Finish->Restart Outlook**

---

[i] Outlook sometimes performs this part automatically. So you may be able to skip this.