

How to setup Outlook for encryption emails

Windows Users

Table of Contents

What is email encryption?

Page 3 Restricted | © Siemens 2022 | April 2022

SIEMENS

Page 3-4

Encryption for Siemens internal with existing SCD entry

Page 5 Restricted | © Siemens 2022 | April 2022

SIEMENS

Page 5-14

Encryption certificates for communication with externals without SCD-Entry
S/Mime certificates from Entrust

Page 15 Restricted | © Siemens 2022 | April 2022

SIEMENS

Page 15-20



What is email encryption?

What is email encryption?

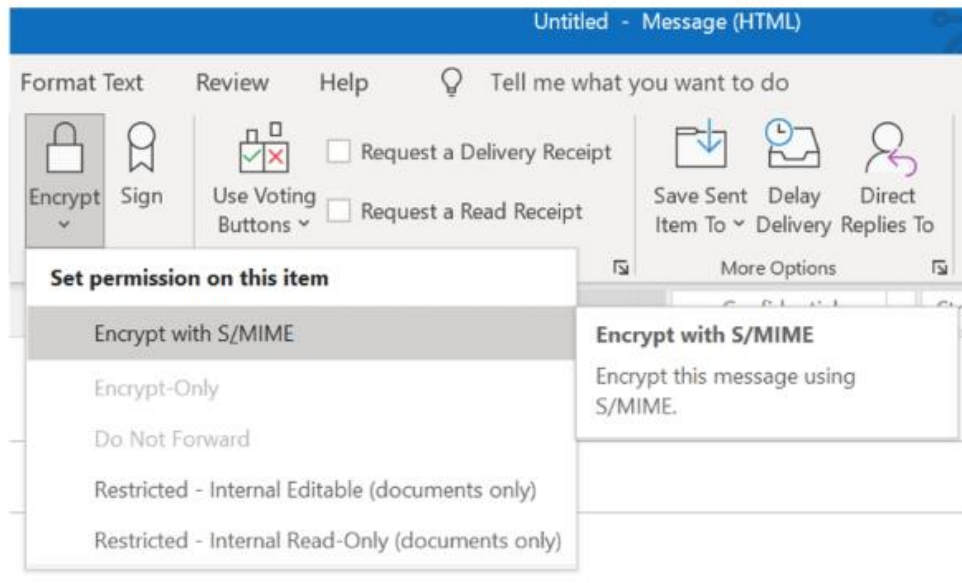
Encryption emails are used when you need to protect the confidentiality of an email message with sensitive content or/and files.

Encrypting an email message in Outlook means it's converted from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Any recipient without the corresponding private key, however, sees indecipherable text.

At Siemens, Outlook supports the following encryption option:

- **S/MIME encryption** - S/MIME is a certificate-based encryption solution that allows you to encrypt a message.

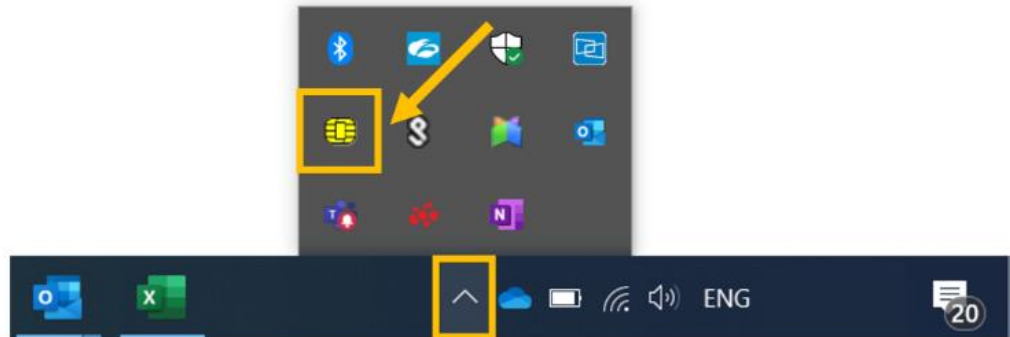
If you want to know more about encryption options from Microsoft, consult the [MS Documentation Page](#).





Encryption for Siemens internal with existing SCD entry

1. Check if your Smartcard is properly working



1.1 On your task bar, click on the arrow button to see the hidden icons (see picture).

1.2 Look for the PKI Basic Client symbol (if you use a smart card) or for the NSC Basic Client symbol (if you use a Network Smartcard) and check if it looks like the picture on the left (with no error sign).

If it does, please continue to the next step.

If not, then please contact your [IT Service Desk](#).

> For more information on Network Smartcard on virtual clients, please consult its [Wikisphere](#) page.

2. How to setup S/MIME? | 1

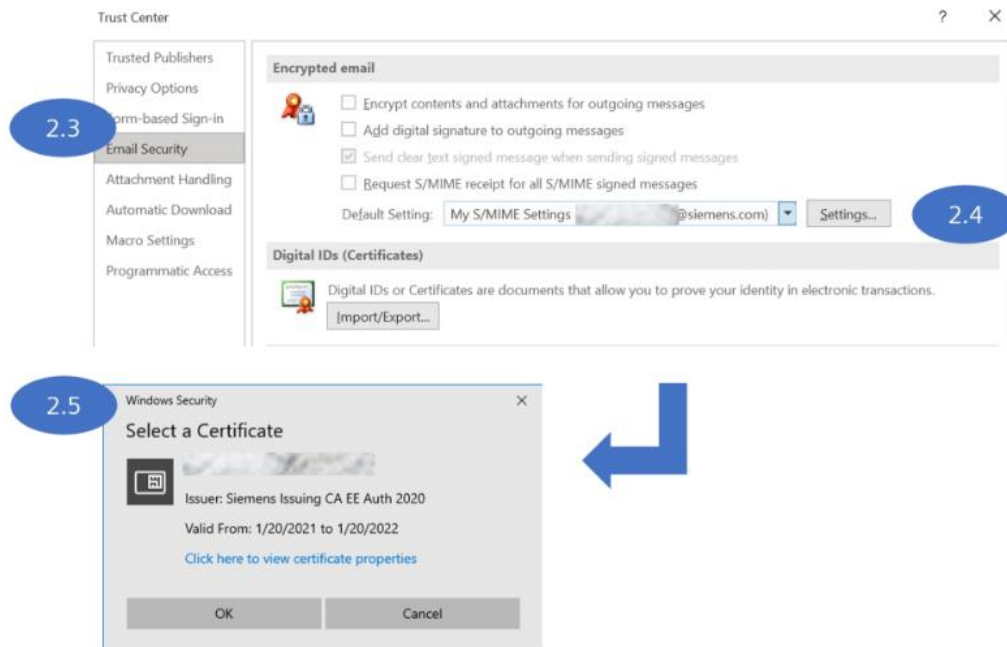
2.1 In Outlook, select the **File** tab and then **Options**.

2.2 Click on **Trust Center** and select **Trust Center Settings**.

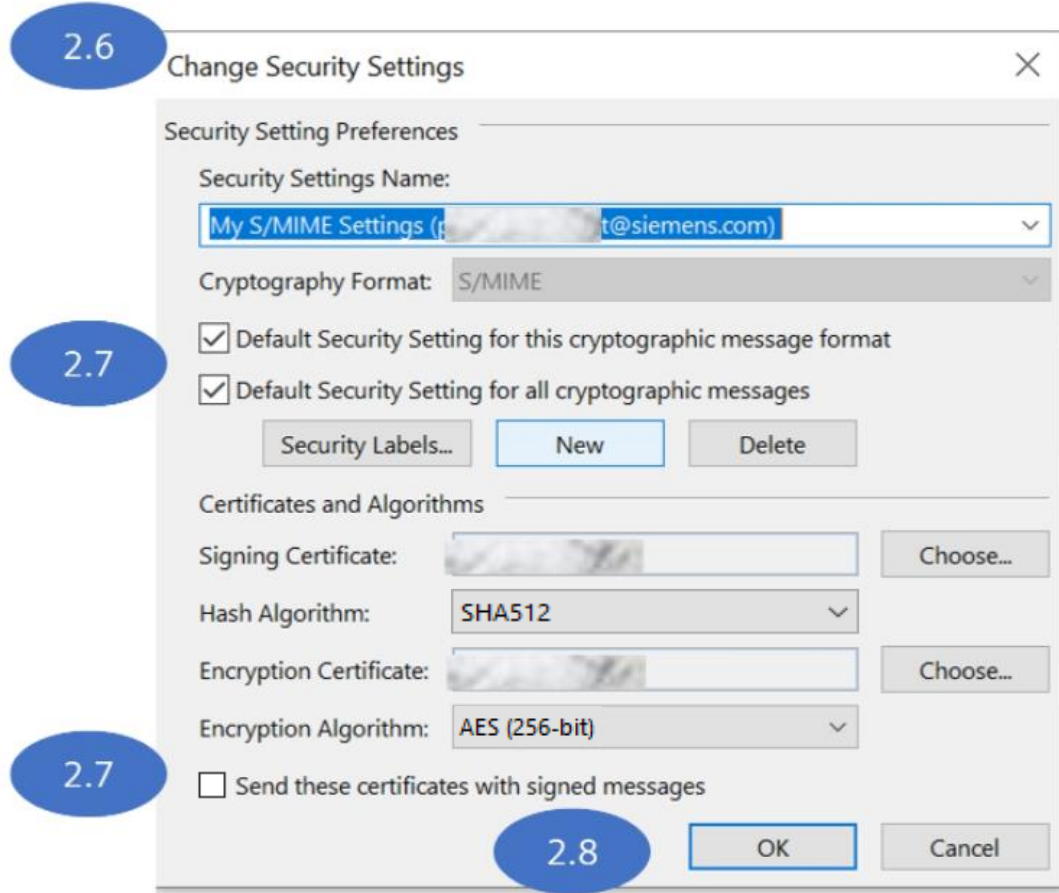
2.3 Select the **Email Security** tab.

2.4 On the field **Default Settings**, click on the button **“Settings...”**.

2.5 If you are using the Outlook for the first time, the “Select a Certificate” pop-up may appear. If it does, press **“OK”**.



2. How to setup S/MIME? | 2



2.6 In the Change Security Settings pop-up, the **Security Settings Name** will appear with your email.

2.7 Make sure the checked boxes are the same as in the image on the left.

2.8 Press **OK** button in the Change Security Settings, in the Trust Center and Outlook Options pop-ups.

You have now completed the setup of S/MIME.

3. Configure the LDAP directories



To encrypt an email, Outlook needs the recipient's encryption certificate.

You need to configure the certificates as LDAP (Lightweight Directory Access Protocol) address books. There are two directories available:

- Siemens Corporate Directory [SCD] (for communication with internal recipients)
- Directory Broker (for communication with Siemens business partners).

At Siemens, the LDAP is enabled for:

- an automatic installation and running, by downloading the Messaging LDAP Toolkit 1.0 from the Software Center (page 6 of this manual)
- or manually, by installing the directories manually (page 10 of this manual).

4. Install and execute Messaging LDAP Toolkit 1.0

4.1 Click on the **Start Button** on your Laptop Task Bar and open the **Software Center**.

4.2 Search for **Messaging LDAP Toolkit 1.0** and Install it.

4.3 When the App is installed, click on the **Start Button**, search for **Messaging LDAP Toolkit**, and select **"Add LDAP"**.

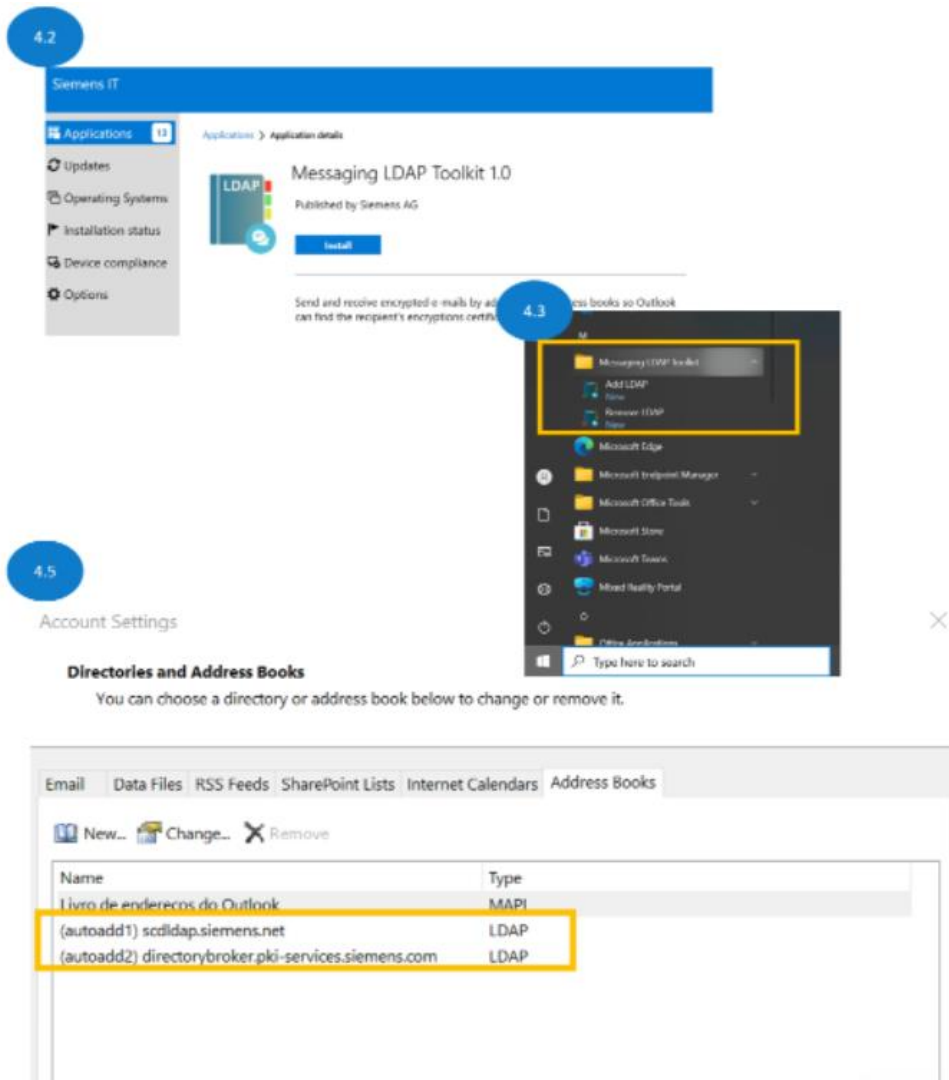
It will start adding the LDAP Directories automatically. When it is finished, you will be shown a message to restart your Outlook.

4.4 Restart the Outlook.

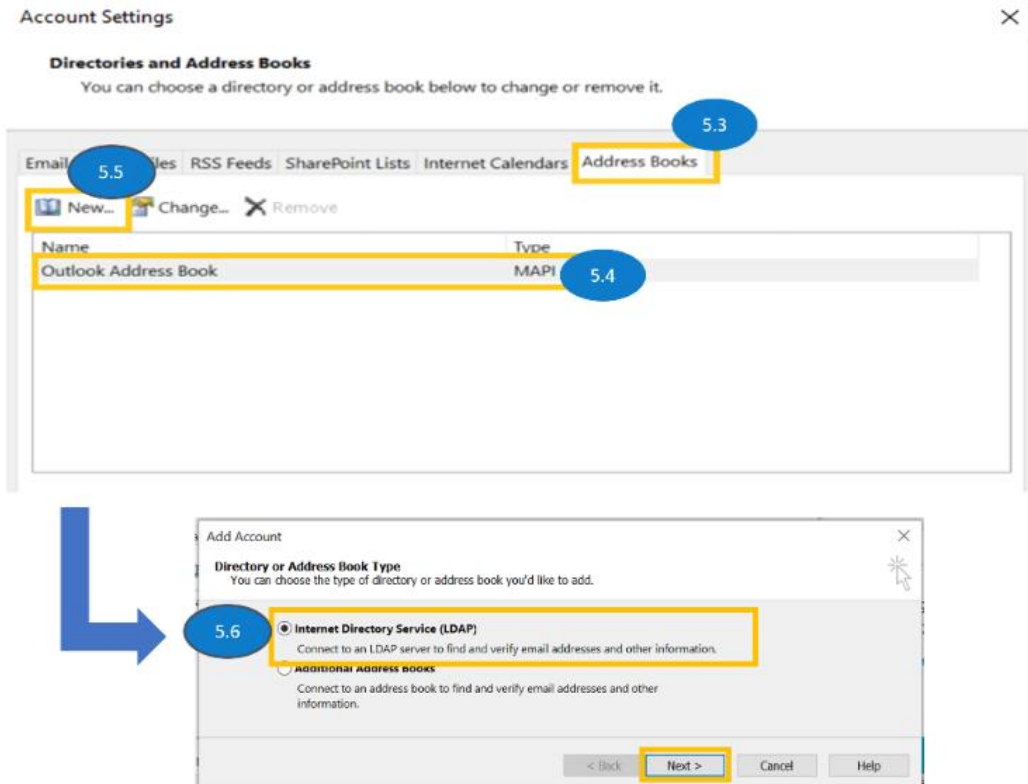
Now, you should be able to send encrypted e-mails.

4.5 Optional: You can confirm it by opening the **Account settings** and selecting the **Address books** tab. You will see the same directories as in the image on the left side.

In case of issues, get more information [here](#).



5. Install the LDAP directories manually | 1



5.1 In Outlook, select the **File** tab.

5.2 Click **Account settings** and select **Account settings**.

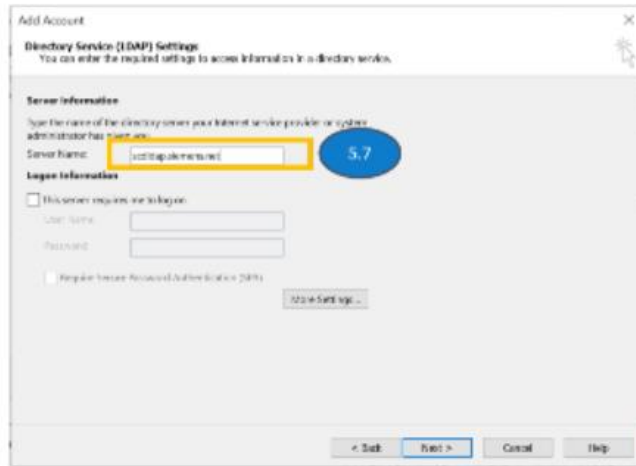
5.3 Select the **Address books** tab.

5.4 Outlook Address Book will (MAPI) appear in your list by default. If the two LDAP Directories are missing, then you should add them manually.

5.5 To add a missing directory, click **New**.

5.6 Select **Internet Directory Service (LDAP)** and click **Next**.

5. Install the LDAP directories manually | 2



5.7 Enter the missing directory (missing address book) in the server name field, by this order:

- scldap.siemens.net
- directorybroker.pki-services.siemens.com

5.8 Click **Next** and confirm the message by clicking **OK**.

5.9 Click **Finish**.

5.10 Restart your Outlook for the changes to take effect.



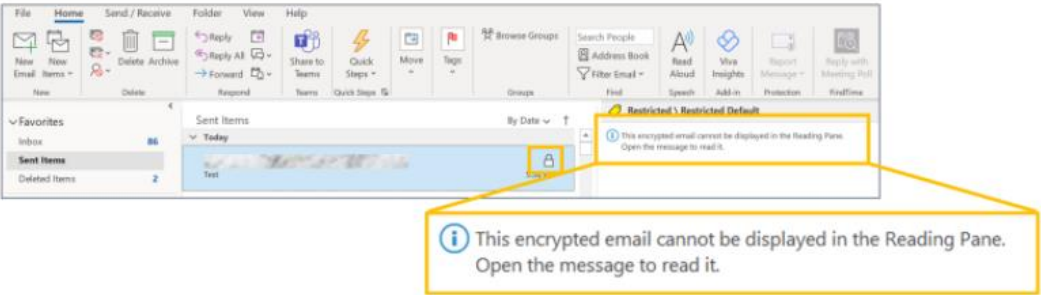
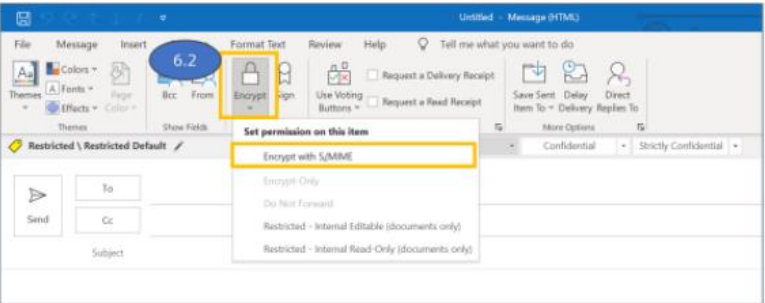
6. How to send an encrypted email

6.1 In Outlook, click on **New Email**.

6.2 In **Options**, click on **Encrypt** and select **Encrypt with S/MIME**.

6.3 Write your email message (with or without file attachments) and send it.

> You can see how an encrypted email is shown in your Inbox or Sent Items.



More information



For mMac service (MacOS), please use the following manual:

[mMac Email Encryption](#)

If you are experience any issue with email encryption, consult the following manual:

[Solve email encryption issue due to missing or invalid certificate](#)

To know how to send encrypted emails in Outlook Mobile, consult the manuals:

- [Android](#)
- [iOS](#)

To have access to the Working Essentials Info Point about S/MIME, consult [here](#).

To know more about Outlook visit the [Microsoft 365 Hub page](#).

To stay updated about Outlook join the [Microsoft 365 at Siemens](#) Yammer group.

Encryption certificates for communication with externals without SCD-Entry

S/Mime certificates from Entrust

How to order a S/Mime certificate for Siemens Business Partners at ServerRA? | 1

My Certificates

- > Server SSL Certificates
- > Code Signing and Application Certificates
- > Secure Email Certificates
- > Certificate watchlists

Order Certificate

- > Trust Center Server Certificates
(internal trusted: TCID, SAID, WSID)
- > Trust Center Code Signing
(internal supplier: CSID)
- > QuoVadis Server Certificates
(external trusted: TLID, TLSID, TLWID)
- > QuoVadis Code Signing Certificates
(external supplier: TLC SXID)
- > Entrust Secure Email Certificates
(external supplier: ENSMIME)

Validated Domain Lists

- > Show top level domain list Siemens (TCID)
- > Show top level domain list QuoVadis (TLID)
- > Show top level domain list Siemens Healthineers (TCID)
- > Show top level domain list Siemens Energy (TCID)

Search Certificates

- > Server SSL Certificates
- > Code Signing and Application Certificates
- > Secure Email Certificates

Anyone inside Siemens can start the order from S/Mime certificates, for external employees the Content Owner/Sponsor must be an internal Siemens employee (ServerRA check's the SCD to confirm).

1. Please open a web browser (Chrome, Edge, Firefox) and navigate to [ServerRA](#).
2. Please select the certificate type "Entrust Secure Email Certificates (external supplier: ENSMIME)"

How to order a S/Mime certificate for Siemens Business Partners at ServerRA? | 2

> Home > Order Certificate

Please select a certificate type and then upload a valid CSR
You can also create an OpenSSL command based on the order. Click on "OpenSSL CSR Command Builder".

Certificate

Certificate Category: Entrust Secure Email Certificates (external supplier: ENSMIME)

Certificate Type:

E-Mail Address / Common Name:

Valid From: 27-Jan-2021 12:11

Valid To: 27-Jan-2024 12:11

Role	GID	Name	First Name	Search SCD
Certificate Sponsor				

Additional info:

Order

Order Type: New

Billing Info: [FAQ billing information](#)

OrgID:

Order ID or NRS:

HPOS:

Net Costs: 80,00 €

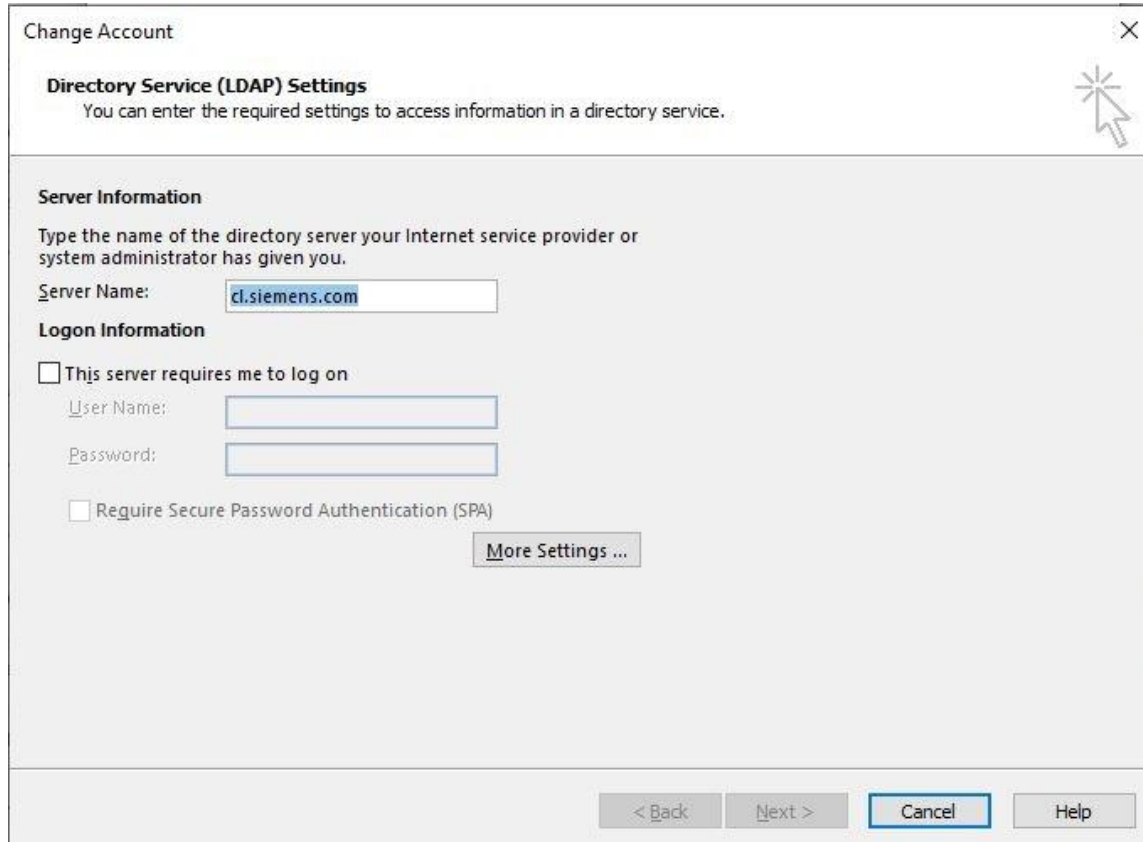
Creation date: 27-Jan-2021 12:11

Last change date: 27-Jan-2021 12:11

Requester:

- 3. Please fill in the Sponsor information by using the SCD search, the business partners external email address and the billing information.
- 4. Click on "Order Certificate" to complete the process.

The End User (Business Partner) must include the following configuration to the Outlook client:



The screenshot shows the 'Change Account' dialog box in Outlook. The title bar reads 'Change Account'. Below the title bar, there is a section titled 'Directory Service (LDAP) Settings' with a sub-header 'Directory Service (LDAP) Settings' and a description: 'You can enter the required settings to access information in a directory service.' Below this, there are two main sections: 'Server Information' and 'Logon Information'. In the 'Server Information' section, there is a text box for 'Server Name' containing the value 'cl.siemens.com'. In the 'Logon Information' section, there is a checkbox for 'This server requires me to log on' which is unchecked. Below this checkbox are two text boxes for 'User Name' and 'Password'. There is also a checkbox for 'Require Secure Password Authentication (SPA)' which is unchecked. At the bottom of the dialog box, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. A mouse cursor is pointing at the 'Cancel' button.

Change Account

Directory Service (LDAP) Settings
You can enter the required settings to access information in a directory service.

Server Information
Type the name of the directory server your Internet service provider or system administrator has given you.
Server Name:

Logon Information
 This server requires me to log on
User Name:
Password:
 Require Secure Password Authentication (SPA)
[More Settings ...](#)

< Back Next > **Cancel** Help

LDAP settings:
cl.siemens.com



Can I request certificate for any valid email?

You can order the certificate for any Business Partner email address with the exception for Siemens internal domains.

What will happen after the order is created?

The ServerRA will inform the Content Owner/Sponsor and End User that the order was accepted. The End User will receive an email from Entrust to continue the process.

Does the End User need to perform some steps?

Yes, the End User should open the email and follow the invitation to create the certificate.

Can ServerRA help the End User to recover the certificate or the PIN?

No, ServerRA does not have the certificate or private key. That information is only available for the End User (not even the Content Owner has that information). It is not possible to recover at Entrust or ServerRA.



For how many days the email invitation is valid?

The Entrust invitation is valid for 30 days, Entrust and ServerRA will only charge for issued certificates.

Does ServerRA cancel Entrust orders?

Yes, ServerRA will cancel automatically the order that was not processed.

What is the validity of this encryption certificate?

This certificate is valid for 3 years.

What will happen after the certificate creation?

The End User can install the certificate and exchange encrypted emails with Siemens, check FAQ from Entrust to find more details:

<https://www.entrust.com/knowledgebase/ssl/entrust-smime-faq>

The certificate from Entrust will be published inside the <https://directorybroker.pki-services.siemens.com/search/basic/>

For which users can these certificates be requested and what are they for "email encryption"?

Certificates can be ordered from business partners in general. For these users, no SCD input and no XGID are needed anymore. Certificates issued by Entrust can only be used to encrypt emails (S / MIME).