Secure Mail to and from Ericsson

Directions for Use

Ericsson demands secure communication of sensitive information. Sending encrypted emails is a solution for protecting sensitive information.

There are two options allowing external parties who wish to communicate securely with Ericsson:

- S/MIME
- Office 365 Message Encryption (OME)

Contact your IT department or support to see if you have a solution and process for email encryption in place.

Contents

1 S/MIME

Email encryption protects the information being sent and ensures that only the intended recipients can read message content. It also ensures that the content of the email is not altered.

Your own IT department should instruct you how to share encryption keys and send encrypted emails. Below you will find Ericsson guidelines.

1.1 Before you get started

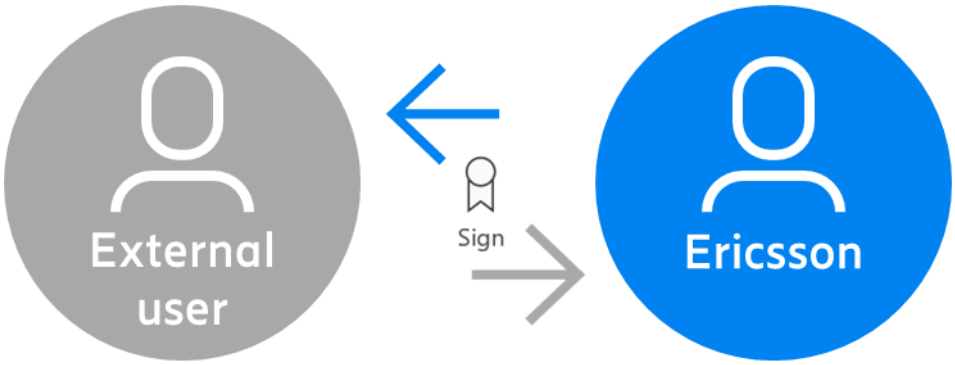
Before you can start sending encrypted emails, you must have a certificate with a Private and Public key. Your IT department should provide you with this. If you have not received a certificate, please contact your IT department.

Note: *Only S/MIME certificates provided by globally trusted Certificate Authority can be used to exchange S/MIME emails with Ericsson. The trusted CA list is the same that most of the browser providers use.*

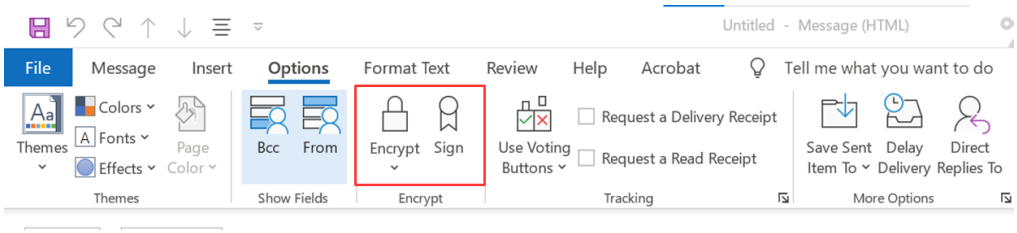
If you already have an S/MIME certificate please reach out to the Secure mail Support Team to check if it is accepted in Ericsson.

1.2 Getting started – Exchanging Public Keys

To be able to send and receive encrypted emails, you must exchange signed emails with your Ericsson contact so that they can get your Public Key and you get theirs.



This is how Encrypt and Sign message icons look like in Outlook M365:



1.3 Adding contacts to email contacts

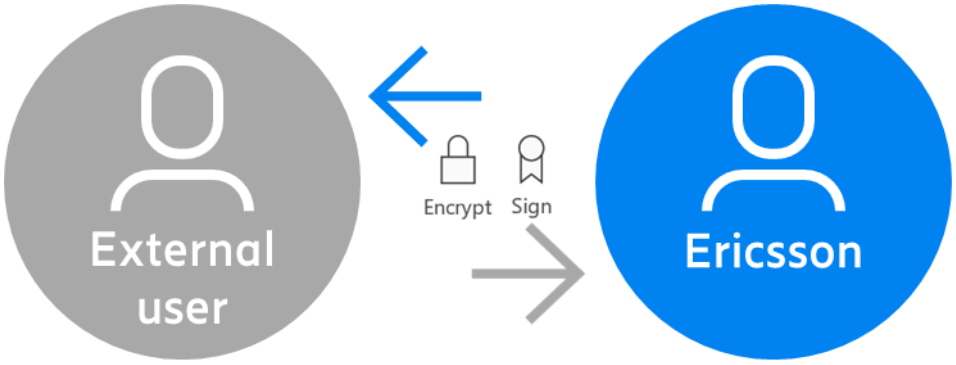
The Public Key can only be obtained by adding the contact from a signed email to your email contact list.

Note: *If the contact is already in your email contacts, be sure to re-save it from the signed email.*

You can now send and receive encrypted emails with this contact.

1.4 Sending an encrypted email

Emails we send often contain sensitive information, either in the body text or in an attachment, and if this information is compromised it can have severe impact on our business. That is why it is important to always encrypt an email containing sensitive information.



To encrypt an email:

1. Write your message as usual
2. Select the Encrypt icon at the top of the toolbar. The padlock and/or sign button will be highlighted when selected

3. Click send

Once the encrypt and/or sign button are selected, the email content, and its potential attachments, are encrypted. Only the sender and the recipients can read the encrypted email.

2 Office 365 Message Encryption (OME)

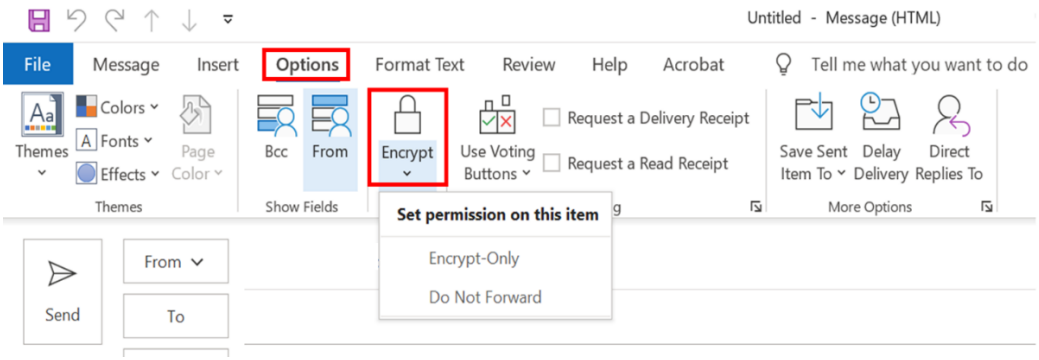
Office 365 Message Encryption service includes encryption, identity, and authorization policies to help secure your email.

Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content.

2.1 Sending messages encrypted with OME

Securing an email with OME via Outlook can be done under Options -> Encrypt and it comes with options to “Encrypt-Only” and "Do Not Forward".

If “Do Not Forward” is selected, the message is encrypted with additional protections to prevent the recipients from forwarding the email to others.



Note: Microsoft 365 Message Encryption is part of the Office 365 Enterprise E3 license. Additionally, the Encrypt-Only feature (the option under the Encrypt button) is only enabled for subscribers (Microsoft 365 Apps for enterprise users) that also use Exchange Online.

2.2 Receiving messages encrypted with OME

All Microsoft 365 end users that use Outlook clients to read mail, can read encrypted or rights-protected mail directly in Outlook even if they're not in the same organization as the sender. Supported Outlook clients include Outlook desktop, Outlook Mac, Outlook mobile on iOS and Android, and Outlook on the web (formerly known as Outlook Web App).

Recipients of encrypted messages who receive encrypted or rights-protected mail sent to their Outlook.com, Gmail, and Yahoo accounts receive a wrapper mail that directs them to the OME Portal where they can easily authenticate using a Microsoft account, Gmail, or Yahoo credentials.

3 Support

If you need support with encrypted emails (EriCA or OME), please contact: Secure mail Support Team.