



Setting up secure e-mail communication with Ericsson

Guideline for Ericsson partners

In this presentation

- Introduction
- Technical prerequisites
- Getting started
 - Exchanging Public Keys
 - Sending a signed e-mail
 - Adding contact to e-mail contacts
- Sending an encrypted e-mail
- Example of Certificate installation (VeriSign)
- Instructions for PGP users

Introduction

Ericsson demands secure communication of sensitive information. Sending encrypted e-mails is a solution for protecting sensitive information.

- E-mail 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 e-mail is unaltered. Your own IT department should instruct you how to share encryption keys and send encrypted e-mails. This presentation states the Ericsson guidelines.
- Confidential information should always be protected using e-mail encryption.

Disclaimer:

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information may be subject to change without notice. Ericsson shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from Ericsson (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of Ericsson products.

Technical prerequisites (1/2)

- Ericsson follows the international S/MIME standard for e-mail encryption.
- Everyone who wishes to communicate securely with Ericsson should use a solution compatible with the S/MIME standard.
- In order to send secure e-mail to Ericsson you need:
 - A X.509 standard compliant certificate.
- The following software needs to be pre-installed with the certificate.
 - S/MIME Compatible e-mail Software
 - Microsoft Office Outlook 2000, 2003, 2007, Express
 - Mozilla Thunderbird
 - Other equivalent e-mail software
 - Web browser
 - Internet Explorer
 - Mozilla (Firefox, Netscape, Apple Safari)
- If the IT department needs guidance they can contact Ericsson Extranet Support at exactextranet.support@ericsson.com or by calling +46 10 7133085.

Technical prerequisites (2/2)

Obtaining a Digital ID - A X.509 compliant certificate

If there is no valid e-mail encryption certificate, you should obtain a certificate from the relevant certification authority. If the company or organization does not have the possibility to get a certificate, it can be downloaded from a trusted source on the Internet.

Below you will find companies that provides certificates:

- [Comodo](#) (From \$7.20 per certificate per year)
 - [Geotrust](#) (From \$19.95 per certificate per year)
 - [VeriSign](#) (From \$19.95 per certificate per year)
-
- An example of certificate installation; see [detailed instructions on how to install a VeriSign certificate](#)
 - If the company or organization already has a valid e-mail encryption certificate, the person that will send encrypted e-mails, must share the Public Key with the Ericsson contact to exchange encrypted e-mail. (See instructions on following pages)

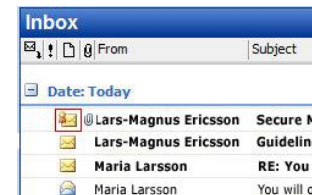
Getting started

Exchanging Public Keys and sending a signed e-mail

To be able to send and receive encrypted e-mails, you must exchange signed e-mails with your Ericsson contact so he/she can get your Public Key.

1. Send a signed e-mail to your Ericsson contact.

This will indicate to your Ericsson contact that you have a certificate that you are ready to receive his/her signed mail.



Symbol for signed e-mail in the inbox.

2. When you get a signed e-mail from your Ericsson contact you must save him/her in your e-mail contact list.

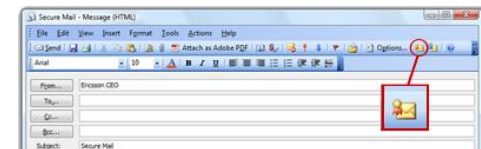
If the contact is already in your e-mail contacts, be sure to re-save it from the signed e-mail.



Save/re-save to contact list.

3. If the Ericsson contact sent the first signed e-mail, you must send a signed e-mail back to the Ericsson contact as well in order for him/her to get your Public Key. This is done by:

- Write your message as usual
- Select the Digitally Sign Message icon at the top of the message toolbar.
- Click send (your Public Key will now be sent along with the e-mail)



Send a signed e-mail back to Ericsson contact.

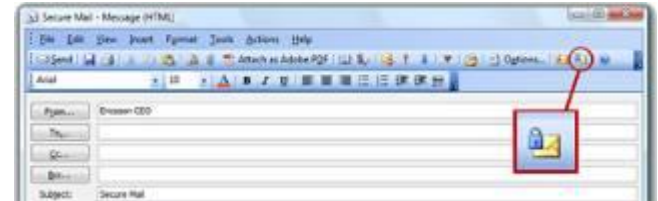
4. Now you can send encrypted e-mails to your Ericsson contact.

Note! The signed e-mail function is mostly used to exchange Public Keys; this will not protect the content!

Sending encrypted e-mails

It is important to encrypt the message before sending it.

1. Write your message as usual.
2. Select the ***Encrypt Message Contents and Attachments*** icon at the top of the message toolbar.
3. Click Send.
 - The message's content, and its potential attachments, are encrypted.
 - Only the sender and the recipients are able to read the encrypted e-mail.





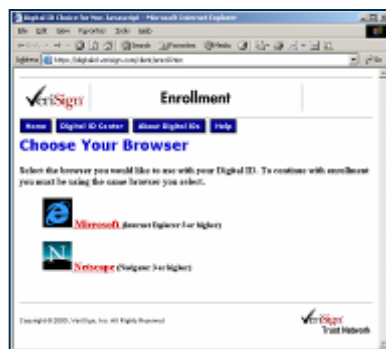
Certificate enrolment and setup using VeriSign

Example of Certificate installation

1.a Installation - Certificate enrolment

Guidelines for VeriSign

1. Go to the [VeriSign enrolment site](#)
2. Choose your browser type. Select Netscape if you have a Mozilla browser (Firefox, Netscape, Safari)
3. Complete the enrolment form:
 - Enter your details.
 - Select Cryptographic Service provider. If available, select “Microsoft Enhanced Cryptographic Provider v1.0”.
 - Make sure that you enable protection of your Private Key by checking the checkbox for additional security.



Contents of Your Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.

First Name: Nickname or middle initial allowed (example -- Jack B.)	<input type="text"/>
Last Name: (example -- Doe)	<input type="text"/>
Your E-mail Address: (example -- jdoe@verisign.com)	<input type="text"/>

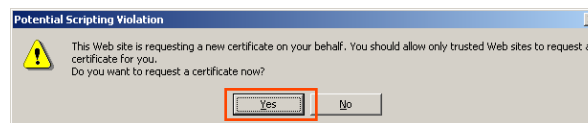
Cryptographic Service Provider Name Microsoft Enhanced Cryptographic Provider v1.0

Check this Box to Protect Your Private Key

1.b Installation - Certificate enrolment

Guidelines for VeriSign

4. Allow any potential scripting dialog that appears.

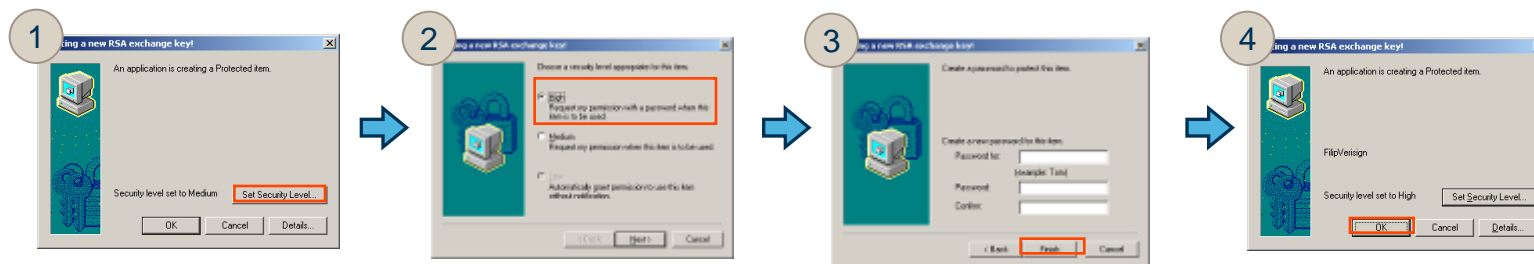


5. Select **Security Level** (1).

6. Set the security level to **High**, requiring a password when using the certificate (i.e. signing an e-mail) (2).

7. Choose a password. Use 8 characters, at least with one upper case and one number as a good password policy. Click **Finish** (3).

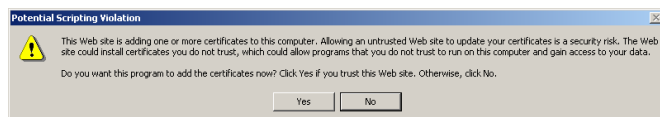
8. Click **OK** on the next dialog (4).



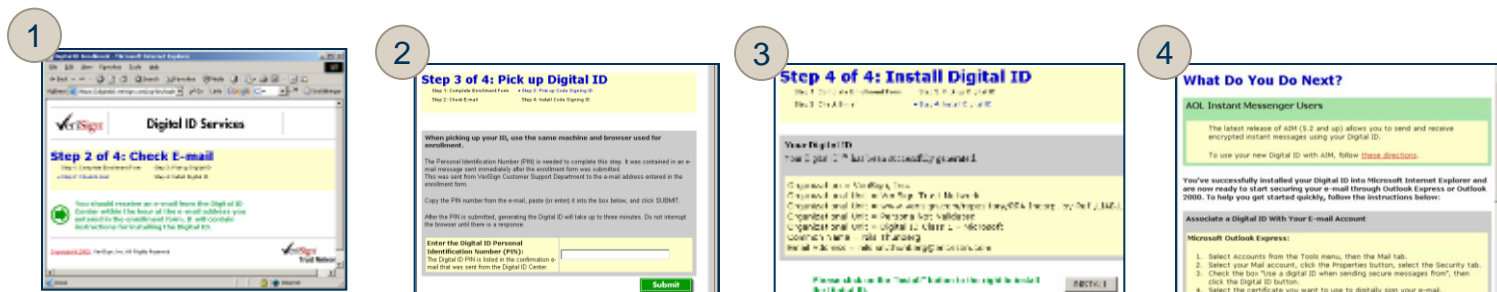
1.c Installation - Certificate enrolment

Guidelines for VeriSign

9. Check your e-mail and follow the instructions in the e-mail (1).
10. Enter the Digital ID **Personal Identification Number (PIN)** provided in the e-mail in the next step of the enrolment process (2).
11. Click **Install** to download and install the certificate (3).
12. Accept the Potential Scripting Violation dialog that appears two times.



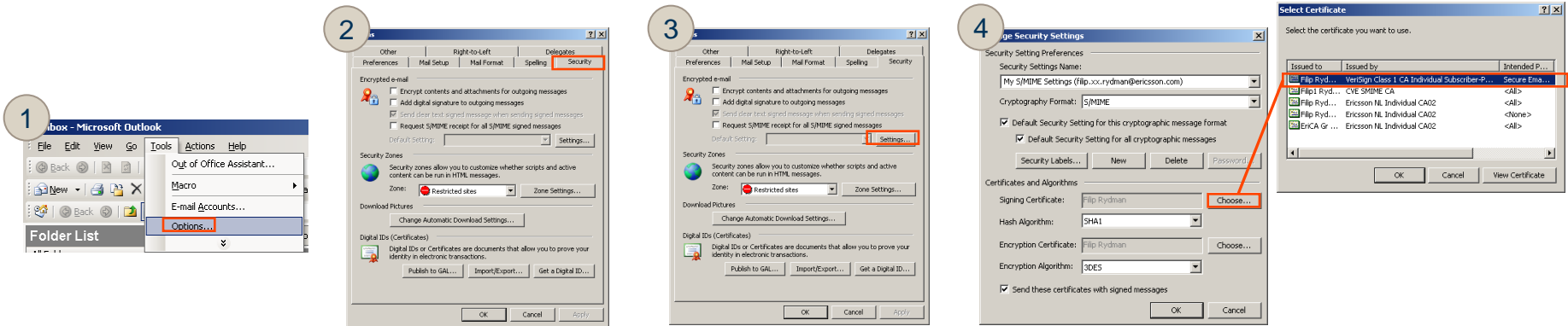
13. You have successfully installed a certificate when you see screen 4.



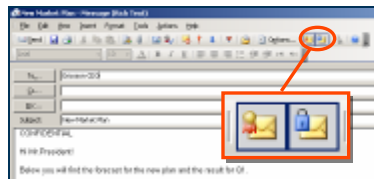
2 Installation - Certificate association with your e-mail account

Guidelines for Outlook 2000, 2003, 2007

Open Outlook → In the tools menu select **Options** (1) → Select the **Security** tab (2) → Click on **Settings** to change your Security Settings (3) → Click **Choose** on the next dialog and make sure you use the correct certificate (4).



You have now enabled the signing and encryption functionalities to be used for sending Secure e-mail to Ericsson users. These icons are displayed when creating a new e-mail.



Instructions for PGP users

Introduction



If you use PGP as your e-mail encryption software you must obtain a digital ID (certificate) in both cases. These instructions show how to use certificates with PGP.

1. PGP version 8.x or below (8.1 tested)

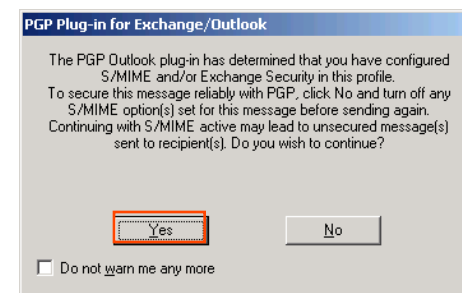
It is possible to use PGP version 8.x or below to encrypt or sign e-mails sent to Ericsson users. S/MIME options in Outlook interfere with PGP and may cause problems when encrypting or signing e-mail. Therefore S/MIME options must be turned off in Outlook.

2. PGP version 9.x or above (9.5 tested)

PGP version 9.0 and above support S/MIME and it is therefore possible to use S/MIME options and PGP at the same time.

■ Issues with PGP desktop

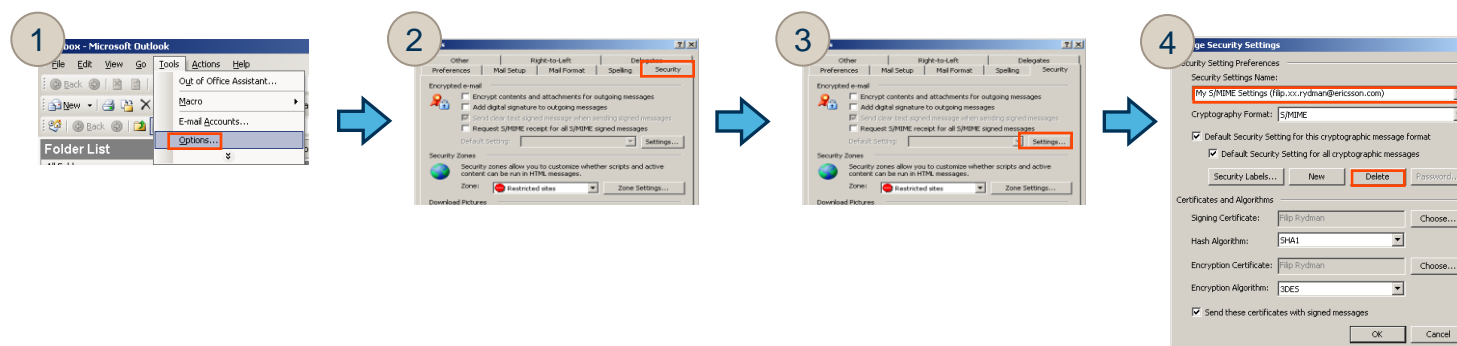
When you need to send signed or encrypted e-mails to other PGP users you will get this dialog warning. In most cases it is ok to click **Yes** and the message will be encrypted correctly.



Turning off S/MIME options in Outlook For PGP Desktop 8.x or below

You can switch between PGP and S/MIME in order to reliably send PGP encrypted e-mails to Non-Ericsson users

1. In Outlook select *Options* from the Tools menu.
2. Select the **Security** Tab.
3. Click on **Settings** to change your Security Settings.
4. Select each of your Security Setting Names and click **Delete**.*



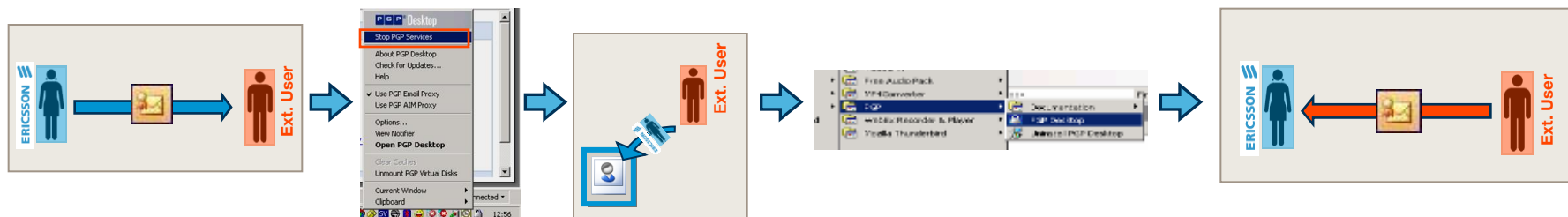
*Note that you don't delete your certificates permanently. They are only temporarily disabled in Outlook until you associate your certificates with your e-mail account again.

Exchanging Public Keys

For PGP Desktop 9.x and above

In order to be able to send an encrypted e-mail to a user within Ericsson, you must exchange Public Keys:

1. First, ask the Ericsson user to send you a signed e-mail.
2. Once you have received the e-mail, click on the PGP icon shortcut menu in the system tray and stop the PGP services.
3. You must then add the user to your **Outlook Contacts**.*
4. Next, you must restart your PGP services again in order to read your PGP encrypted e-mails. Do this from the start menu. You can now send encrypted e-mails to that Ericsson user.
5. Send a signed e-mail back to the Ericsson user as well in order for him/her to send encrypted e-mail to you.



* You may need to select another e-mail and then reselect the signed e-mail in order for the signature to be visible.

ERICSSON

