External User's Guide for S/MIME usage within the Novartis Secure Mail Service

This guide is intended to help non-Novartis users to request, understand and setup S/MIME-certificates to achieve full mail client integration with Secure Mail.

Document history:

Revision	Date	Author	Comments
1.0	May 31st 2012	Nicolas Buser (Ext), Novartis	First Version

Table of Contents

1 Document Purpose and Introduction

Novartis provides a service for secure e-mail communication called Secure Mail. This service involves standardized state-of-the-art encryption and signature features for internal e-mail communication and between Novartis associates and external partners.

This 'External User's Guide' has been written and published in order to help non-Novartis users to request an own S/MIME certificate and use it in conjunction with the **Novartis Secure Mail Service**. In this guide it doesn't matter if you are already using the Secure Mail Service or just planned to use it. Both scenarios are supported within this guide, e.g. the registration process is explained explicitly.

As S/MIME is a standard for secure e-mail exchange, most of this guide is a summary of commonly available knowledge and does not exclude further usage of the personal S/MIME-certificate to securely communicate with other non-Novartis recipients.

The main goal of the usage of S/MIME-certificates in conjunction with the Secure Mail Service is to improve the communication experience. For external partners the default interfaces are SecurePDF and the Secure Mail Web-Portal. A SecurePDF is delivered via e-mail once you receive an encrypted e-mail message via the Secure Mail Service. It is basically a PDF-form where a login has to occur before the decrypted e-mail message is downloaded over a secured channel. For sending an encrypted e-mail message the Secure Mail Web-Portal must be used.

As those interfaces might not fit expectations an alternative delivery method is available within the Secure Mail Service. The usage of an own **Personal Digital Identity** that could be either a **S/MIME-certificate** or a **PGP key-pair.** Unfortunately, none of those can be provided by Novartis to external partners.

The advantage of using an own S/MIME-certificate is the full integration of the Secure Mail Service into your e-mail client software. This allows sending and reading encrypted e-mail right within in your mail client – even when you are offline. As already mentioned you could as well start communicate securely with other non-Novartis recipients that have an own S/MIME-certificate.

2 Prerequisites

- You need to have an own, trustworthy computer (or USB-Security-Token) where you can install and protect[1] your personal S/MIME-certificate (Web Mail e.g. on public computers cannot be supported).
- Your internal IT responsible (and/or your Management) might need to approve the usage of S/MIME-certificates (for internal and commercial certificates)
- Your e-mail client software need to support S/MIME
- Budget of approximately $20 per year (for commercial certificates)
- In this guide only Microsoft Windows operating systems (XP/Vista/7) are fully supported
- In this guide only the following browser types are covered: Internet Explorer, Mozilla Firefox and Safari (not fully tested and documented).
- Setup time approx. 1-4 hours

3 Getting Started

In order to get to the point where you can just use your mail client to securely communicate to Novartis associates you will need to carry out quite a lot of steps. An overview of the suggested steps and proceeding can be found in the following sub-chapter 'Checklist'.

Most important as a first step is to figure out if you meet the prerequisites (see previous chapter).

Then we suggest checking out if the internal IT Service Desk (of the company you are working for) is capable to issue a personal S/MIME-certificate for you. If so, go ahead and trigger the internal process intended for that and proceed with step 9 of the checklist when you have the S/MIME-certificate installed.

In case the internal IT cannot issue such a S/MIME-certificate for you, we suggest that you make sure the usage of commercial S/MIME-certificates is allowed within the company. You want to make sure you don't break any rules (corporate policies, litigation, governance, etc.).

After that you can find information on how to request your own commercial S/MIME-certificate in chapter 5. Before proceeding we recommend to read the chapter of basic certificate handling and knowledge in chapter 4.

When you have installed your personal S/MIME-certificate you can proceed with the following chapters 6, 7, 8 to be able to fully use your certificate to communicate securely with Novartis associates.

[1] About protection see chapter 4.1

3.1 Checklist

With this checklist you'll get a detailed overview of all suggested tasks in the suggested order of processing:

No.	Task	Refer to chapter #	Done
1	Check if the S/MIME-approach is appropriate for you (e.g. not mainly depending on Web-Mail) and you fulfill the prerequisites	**1, 2**	
2	Ask your IT responsible (IT department or/and management) about S/MIME-certificates usage (own internal/commercial certificate)	**3**	
3	Check the S/MIME compatibility of your e-mail client (MS Outlook, Notes, Thunderbird, etc. usually are capable with no problem)	**2**	
4	Decide certificate registration mode (PKCS#12)	**5.1**	
5	Choose certificate vendor (depends on item above)		
6	Walk through the necessary registration procedure of chosen certificate vendor (certificate authority)	**5**	
7	Make sure you have the login for the service site of your certificate vendor noted, so you could easily extend your certificate once validity ends (usually after 1-3 years)		
8	Make sure you have a backup of your certificate (PKCS#12-file/*.pfx) at a safe location with a secret passphrase only you know (and only you have access to)	**4.1, 4.2**	
9	Make sure you have your Secure Mail login credentials or the registration message ready (the registration message is sent to you upon the first encrypted e-mail to you from a Novartis associate)	**7**	
10	Setup your mail client to use your S/MIME-certificate	**6**	
11	Register your S/MIME-certificate for the Secure Mail Service	**7**	
12	Accept the Novartis root certificate	**8.2**	
13	Distribute and collect certificates of your communication partners	**8.1**	

4 Basic S/MIME-certificate Handling and Knowledge

A S/MIME-certificate used for e-mail security is a personal X.509 certificate with the right to sign and encrypt e-mails. The X.509 certificates depend on ***asymmetric*** key encryption, which basically means, that your certificate consists of a **private key** and a **public key.** The certificate that is delivered to others is the certificate with only the public key. Only if you have the private key of your certificate, you will be able to sign e-mails and decrypt e-mails that you received or have sent earlier.

4.1 Protect your private key from Theft

The private key of your certificate is the only sensitive data that gives other people trust in your digital identity. You have to prevent under any circumstances that your private key can be used by someone else:

- Never provide your PKCS#12-file (.pfx) to someone else; Use a safe backup location and never share your protection passphrase
- If you suspect your certificate with your private key could be stolen or your identity was already misused, you must immediately revoke your certificate with the appropriate process the CA (you were registering to) provides you.
- In order to prevent theft of misuse of your digital identity your workstation/notebook need to be protected appropriately. Please use malware and virus protection, update programs and operating systems timely and activate your firewall.
- Make sure nobody can use your computer with your login/profile as your password is the only protection of your private key

4.2 Protect your private key from Loss

If the private key of the certificate gets lost (e.g. hard disk crash or system gets staged freshly), you'll not be able to open your old encrypted e-mails anymore nor will you be able to sign new e-mails!

In order to prevent that, you will need to prepare a backup of the certificate with the private key (see chapter 4.6).

4.3 Certificate Expiration/Renewal

One thing about certificates you have to keep in mind is that every certificate expires sooner or later. This means that you have to request a new certificate or try to extend the validity through the Certificate Authority you ordered the certificate. Please find the necessary information on their web page. Personal S/MIME-certificates that currently can be bought have a validity period from 1-3 years.

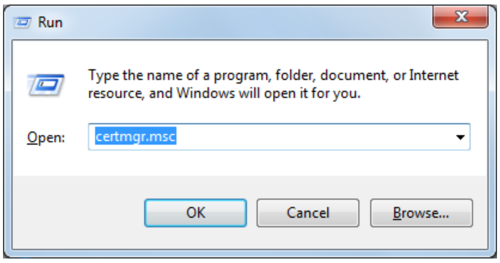
WARNING:

When your certificate has expired and you ordered a new one; **Don't delete the expired certificate! If you delete your expired certificate you won't be able to read old encrypted e-mails anymore!** See chapter 7.2.1 for information on how to register the renewed certificate.

4.4 Visual representation of a certificate in Microsoft Windows

Certificates on a Windows system are usually kept in the CAPI-Store. Some application like the Mozilla products (e.g. Firefox browser) and the Chrome browser are exceptions and hold their own certificate stores.

To open your personal CAPI-Store on Windows you need to run the certificate manager by executing the following command in the 'Run'-Mode (use Windows-Key + R): **certmgr.msc**

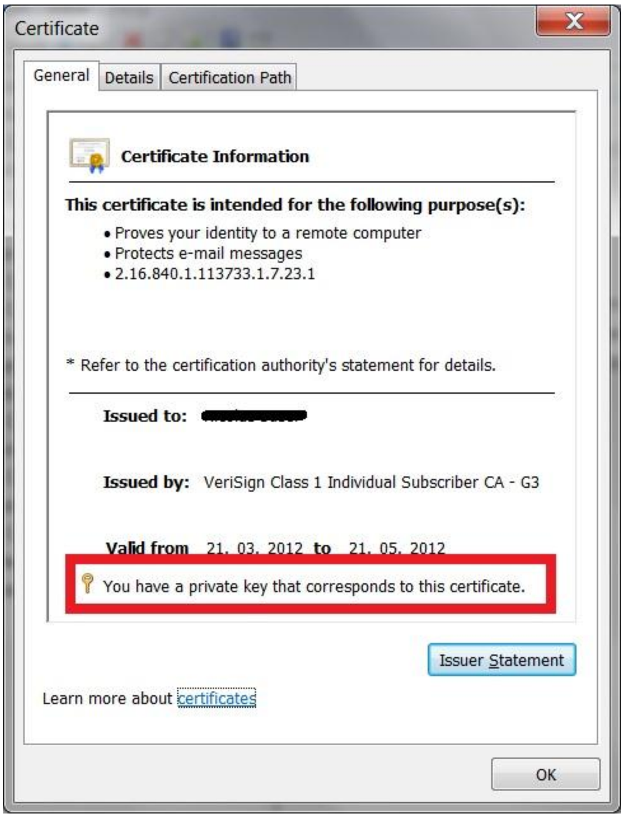


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

Filed under 'Personal' → 'Certificates' you will find your personal S/MIME-certificate. Double-click it to check if you have the corresponding private key installed (see red mark).

Figure 1: X509 S/MIME-certificate with private key



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Protects e-mail messages
- 2.16.840.1.113733.1.7.23.1

* Refer to the certification authority's statement for details.

Issued to: [redacted]

Issued by: VeriSign Class 1 Individual Subscriber CA - G3

Valid from 21. 03. 2012 to 21. 05. 2012

You have a private key that corresponds to this certificate.

Learn more about certificates

4.5 Installation of the S/MIME-certificate from a PKCS#12-file

Once you have a PKCS#12-file with your certificate, it usually contains your private key[2] as well. Therefore it is protected with a security sensitive passphrase. The extension for a PKCS#12-file usually is '**.pfx**' (e.g. 'MyPersonalCertificate.pfx'). Sometimes the extension '.p12' is used as well.

You can install your certificate on any number of systems/devices as long you have that passphrase. Generally you'd like to make sure that the system/device is trustworthy and the private key is protected accurately after installation.

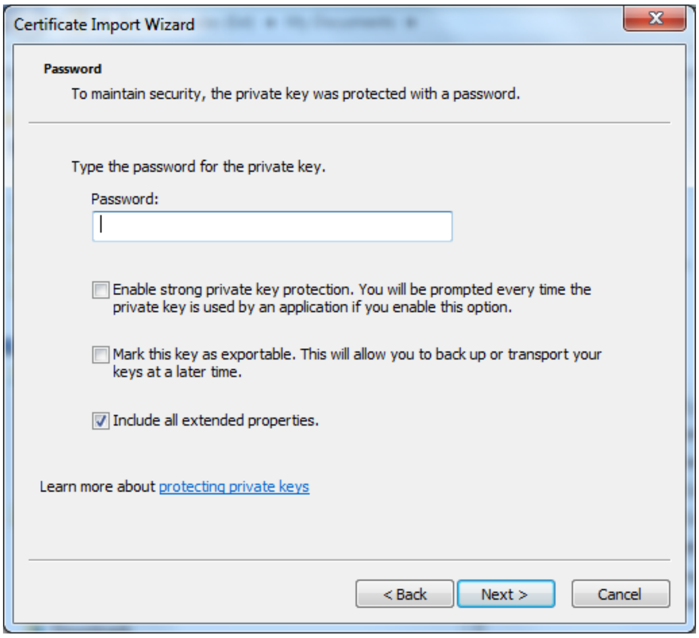
The installation procedure depends pretty much on the system/device. For Windows see next chapter.

4.5.1 Installing a S/MIME-certificate on Windows systems

On Windows systems you can only double click on the PKCS#12-file (*.pfx) in order to trigger the installation wizard. Using the default settings is recommended, but not necessary.

On the third wizard screen you have to enter your security sensitive passphrase.

Figure 2: Installation wizard for a PKCS#12-file



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

[2] See chapter 4 for explanation about private key of a certificate

4.6 Backup or Export of your S/MIME-certificate

In this guide a '**backup**' of a certificate refers to an export of a certificate with the private key included[3]. A simple '**export**' means that only the public parts of the certificate are exported, so no private key is exported.

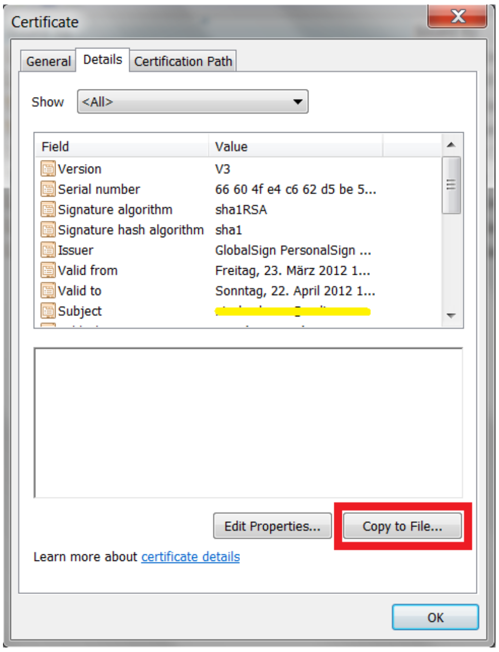
The backup of a certificate is important for you, as losing your certificate and private key means you cannot read the encrypted e-mails anymore (see chapter 4.1). Nonetheless, **never provide your PKCS#12-file (.pfx) to someone else!** Use a safe backup location and never share (or lose) your protection passphrase!

The exported public certificate enables others to send you encrypted e-mails. Therefore a precondition of secure e-mail communication is exchanging (public) certificates (see chapter 8.1).

4.6.1 Backup or Export your S/MIME-certificate from Windows

Open the visual representation of your certificate in the Windows CAPI-Store (see chapter 4.4). Change to the ribbon '**Details**' and open the export-wizard by clicking on the button '**Copy to File**' (see red box).

Figure 3: Certificate export entry point



Certificate

General | Details | Certification Path

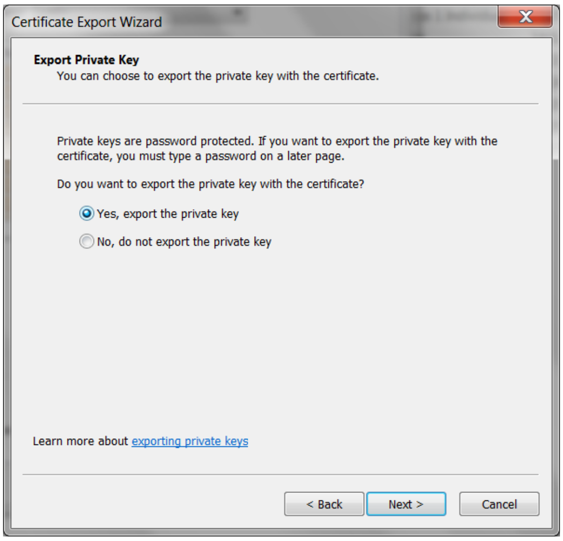
Show <All>

Field	Value
Version	V3
Serial number	66 60 4f e4 c6 62 d5 be 5...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	GlobalSign PersonalSign ...
Valid from	Freitag, 23. März 2012 1...
Valid to	Sonntag, 22. April 2012 1...
Subject	[redacted]

[3] See chapter 4 for explanation about private key of a certificate

Once **'Copy to File'** is pressed the export wizard is started with the following dialog.

Figure 4: Certificate backup with private key



Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

Choose whether to export the private key or not:

A. Please choose '**yes**, export the private key' if you wish to create a **backup** copy for yourself. (Protected with a secure passphrase)
B. Choose '**No**, do not export the private key' if you wish to only **export** the public parts of the certificate for sharing with others.

Note:

Once the private key option is grayed out (and therefore is not selectable), you are either not allowed to export the private key or just don't have it. The first scenario usually occurs if you have imported the certificate without the option 'Mark this key as exportable' (see Figure 2). As well some registration mechanisms don't allow you to export private key. In this case we recommend using the PKCS#12-option or a non-Internet Explorer browser for registration.

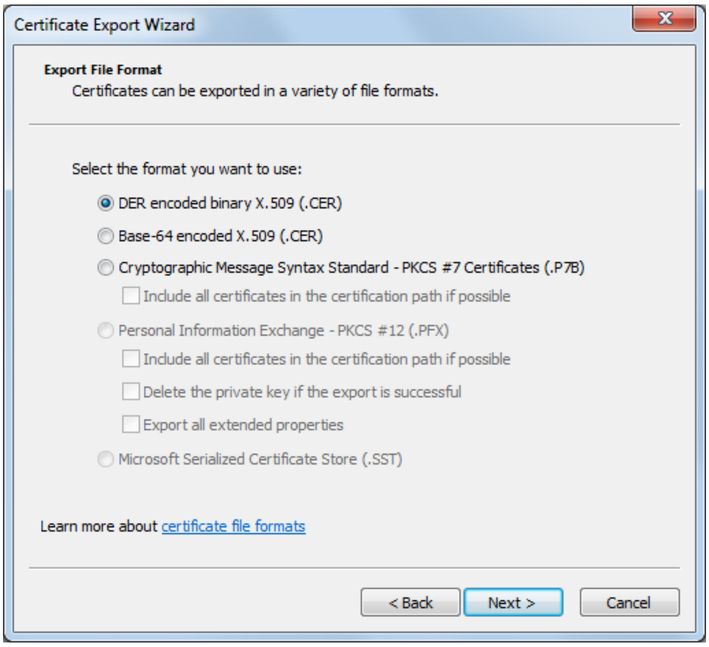
Option A - Backup:

Backup the certificate with private key means that you are about to create a PKCS#12-file that is protected by a secret passphrase you need to enter in the next wizard step. A secure passphrase should be long enough (> 10 characters), complex enough (use numbers, characters and special characters), should not be guessable, lost, shared and nor be accessible by someone else (in case you write it down). Please store the PKCS#12-file in a safe backed up location.

Option B - Export:

Export the certificate without private key can be done into several formats. Please use the default one and specify a meaningful name. The public certificate can be provided to anybody interested in.

Figure 5: Export certificate



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
  □ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  □ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

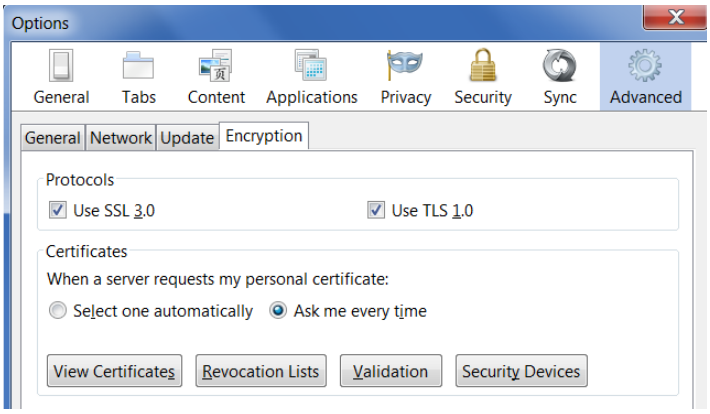
Learn more about certificate file formats

4.6.2 Backup or Export your S/MIME-certificate from Mozilla/Netscape-Store

If you walked through the registration process with a Mozilla Firefox or Safari browser the certificate generated for you will end up in the - so called - Netscape-Store.

In order to export or backup, open the '**Properties**' of the Firefox or Safari browser you need to find the following section.

Figure 6: Open Netscape-Store



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

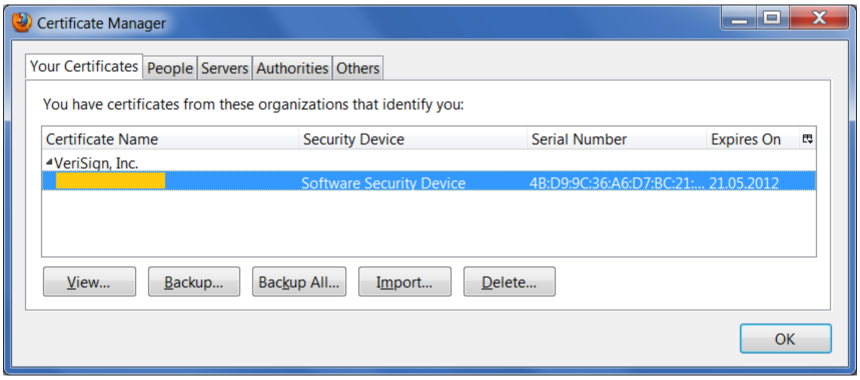
Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

Click on 'Show certificates'.

Figure 7: Certificates in Netscape Store



You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
◢VeriSign, Inc.			
[redacted]	Software Security Device	4B:D9:9C:36:A6:D7:BC:21:...	21.05.2012

In order to **backup** your certificate with private key, please mark it and use the '**Backup**' button. Usually a PKCS#12-file with the extension '.p12' will be created. Provide a secure passphrase for that file. A secure passphrase should be long enough (> 10 characters), complex enough (use numbers, characters and special characters), should not be guessable, lost, shared and nor be accessible by someone else (in case you write it down). Please store the PKCS#12-file in a safe backed up location.

In order to **export** your certificate without private key, please use the '**View**' button, go to the '**Details**' ribbon and press '**Export**'. The public certificate can be provided to anybody interested in.

5 Get your own S/MIME-certificate from a commercial CA

In order to get your own S/MIME-certificate as your personal digital identity you need to register with your e-mail address at a trustworthy certificate authority. There are many certificate authorities (CA's) available on the world and every single one has different levels of trust, registration processes, terms of conditions and prices. In order to make life easier for you, we will suggest some of them later.

This guide does not lead you through the registration process in detail, but tries to give you some hints and advices. The registration usually is a multi-step procedure where your e-mail address is validated by letting you click a link in an e-mail you received from the CA.

Before we get to that point you should decide on the certificate request method described in the next sub-chapter.

5.1 Two different approaches for the S/MIME-certificate request

There are two basic approaches to get your own S/MIME-certificate:

a) Register at the certificate authority (CA) and let the CA generate your private and public key of your certificate. Once your e-mail address is confirmed you only need to import the provided PKCS#12-file on your system. Backup the PKCS#12-file and the provided passphrase[4].

b) Register at the certificate authority (CA) and let your client computer generate the private key for your certificate[5]. This is usually done in a background browser process (e.g. plugin or script). Once done this process sends your certificate request to the CA. The CA creates your certificate that corresponds to your private key and provides you a link in order to download and install it (again script based). The download must be made on the requesting system, so the joint of your private key and the public key of the certificate will be successfully. For backup purposes you will need to export the certificate with the private key in a PKCS#12-file, protected with a passphrase.

Option a) is the easiest and most error prone way to request your own certificate. As well backup is very easy as you already got your PKCS#12-file with the private key included. The disadvantage of this approach is the fact that the certificate authority obviously has the private key of your certificate[6].

Option b) doesn't have the disadvantage mentioned above, but is quite an effort and not very error prone in terms of browser compatibility. As well you need to remember that you need to backup your certificate once the registration is complete. In case you are **not** using Internet Explorer for certificate generation the certificate is installed in an alternative certificate store (ev. in the Netscape Store), so you need to export it from there and import it to the Microsoft CAPI-Store (refer to chapter 'Installing a S/MIME-certificate on Windows systems') before you can configure it on an e-mail client (e.g. a Microsoft Outlook).

[4] Importance of a certificate backup with private key -> see chapter 4.1

[5] What is a private key? See chapter 4

[6] This imposes a security risk. See chapter 4.1

5.2 GlobalSign

GlobalSign is one of the longest serving and a very successful certificate authority (CA). It offers various digital ID's with different trust levels. In order to communicate with Novartis employees via Secure Mail, we are confident that the lowest trust level offered with the product **PersonalSign 1** is sufficient. The request can be done very quickly and involves only e-mail address validation (and a valid payment method).

Here a short summary of the facts for the **PersonalSign 1** product of GlobalSign:

- Low cost, $20 per year
- PKCS#12-Option
- Issued immediately
- Secure e-mail (S/MIME) certificate
- Trusted by the majority of operating systems
- Free Test-certificates available that are valid for 30 days
- Signing of Microsoft Office documents

5.2.1 Register for a PersonalSign 1 certificate

In order to start the registration-process please open the following link in your browser (Firefox recommended):

www.globalsign.com/authentication-secure-e-mail/digital-id

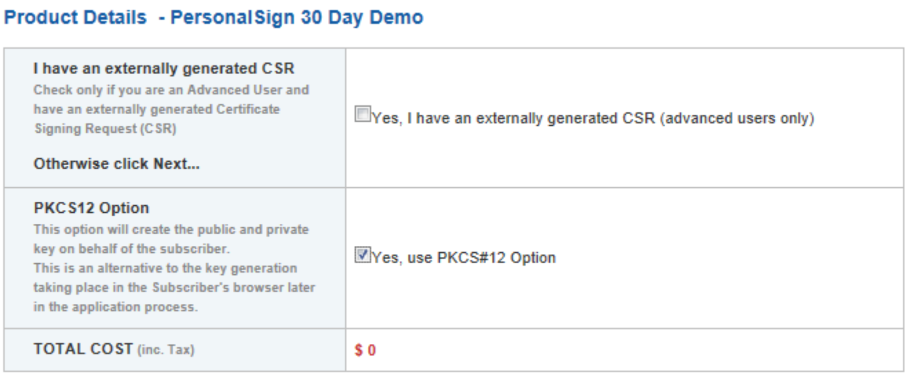
In the section **PersonalSign 1** click on the link for **‚Buy/Renew'** or **'FreeTrial'**. After an intermediate page the registration form should be visible. Please fill in all the necessary information and proceed the suggested way. Please make sure you remember your 'GlobalSign Certificate Center (GCC) Login Details' or write all down into this helping section:

Login name	
Password	
Pickup Password	
GCC User ID	
Order number	

GlobalSign offers you both certificate generation approaches as explained before[7]. In order to use the PKCS#12-Option check the appropriate checkbox on the second form (see Figure 8). If you decide to not use the PKCS#12-option you need to make sure you create a backup of your certificate (with private key) after the installation (see chapter 4.2).

[7] See chapter 5.1

Figure 8: PKCS#12-Option



Product Details - PersonalSign 30 Day Demo

I have an externally generated CSR Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR) **Otherwise click Next...**	□Yes, I have an externally generated CSR (advanced users only)
PKCS12 Option This option will create the public and private key on behalf of the subscriber. This is an alternative to the key generation taking place in the Subscriber's browser later in the application process.	☑Yes, use PKCS#12 Option
TOTAL COST (inc. Tax)	$ 0

Please follow all the instructions on the webpage or on the e-mails sent by Globalsign – make sure your spam filter did not hinder you.

5.3 VeriSign (Symantec)

VeriSign was bought by Symantec, but still issues certificates with the trust root of the VeriSign Certificate Authority. For the purpose of Novartis' Secure Mail service you can register for a personal digital ID.

Summary for the personal digital ID of Symantec:

- Low cost, $20 per year
- Issued immediately
- Secure e-mail (S/MIME) certificate
- Trusted by the majority of operating systems
- Free Test-certificates available that are valid for 60 days
- General Signature & Encryption

5.3.1 Register for a personal digital ID

In order to start the registration-process please open the following link:

http://www.symantec.com/verisign/digital-id/

Once the site has loaded click the **'Buy now'** button and choose the internet browser you are using for the registration. Depending on the browser used additional steps might be required. Please make sure that the same browser is used to finish the registration (eventually by opening the link in an e-mail).

Please follow all the instructions on the webpage or on the e-mails sent by VeriSign – make sure your spam filter did not hinder you.

As VeriSign does not support the generation of a PKCS#12-file don't forget to create a certificate backup (with private key) at the end of the registration (see 4.6).

6 Setup your mail client to use your S/MIME-certificate

In order to use your S/MIME-certificate for Secure Mail communication your mail client needs to have knowledge about your S/MIME-certificate. In this guide only the Microsoft Outlook setting is explained explicitly. For other mail clients please refer to the appropriate documentation available.

Note:

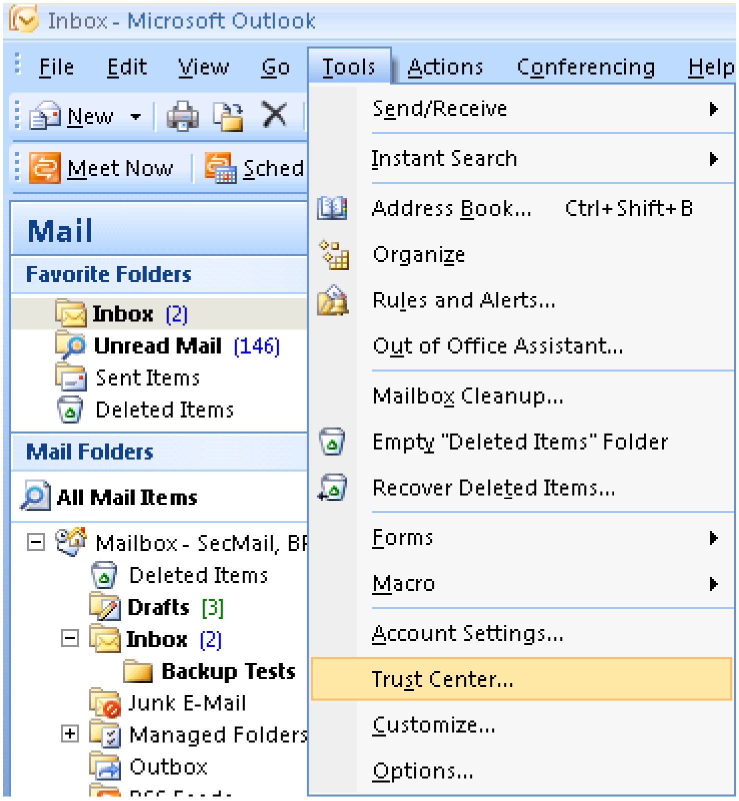
Before you proceed please make sure you have the certificate installed with private key available (see section 4.4) and have a backup available (see section 4.6).

6.1 Outlook Setup

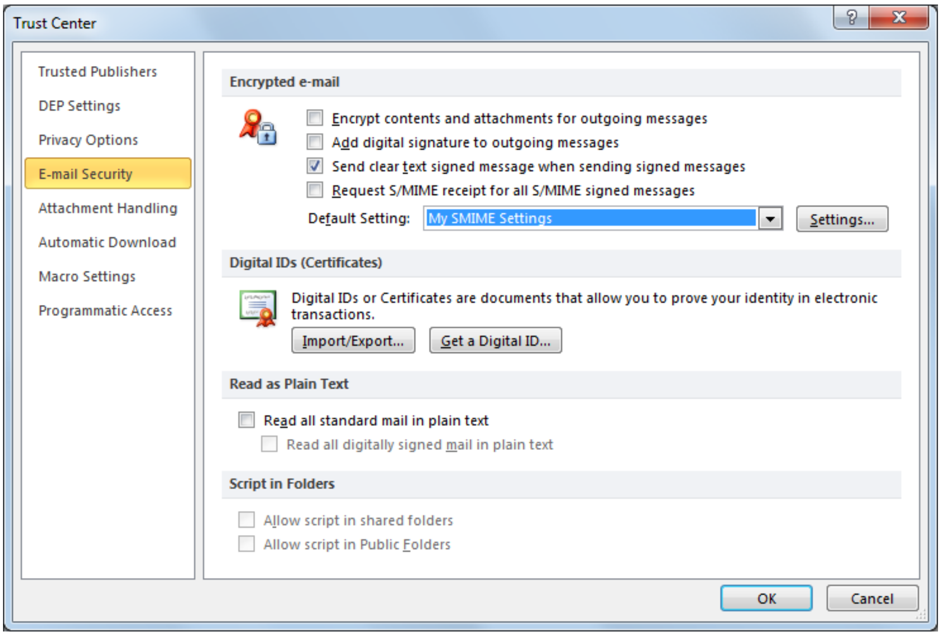
The following installation step might happen automatically in Outlook, but a quick check is recommended anyway.

Open Trust Center settings in Microsoft Outlook the following way:

- For Outlook 2007 click on Tools > Trust Center > E-mail Security > Settings



- For Outlook 2010 click on File > Options > Trust Center > Trust Center Settings > E-mail Security > Settings



Trust Center

Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages
□ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: My SMIME Settings

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

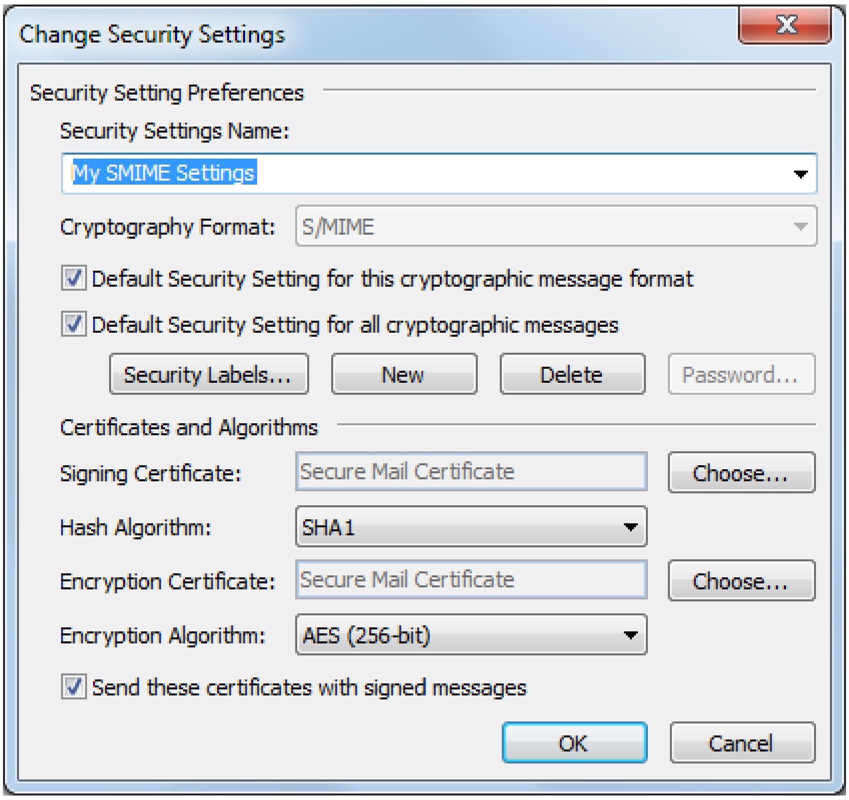
Read as Plain Text

□ Read all standard mail in plain text
□ Read all digitally signed mail in plain text

Script in Folders

□ Allow script in shared folders
□ Allow script in Public Folders

If there is no default setting already, clicking on the 'Settings'-button creates a new configuration that proposes the settings like in the following dialog:



Change Security Settings

Security Setting Preferences

Security Settings Name: My SMIME Settings

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format
☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: Secure Mail Certificate

Hash Algorithm: SHA1

Encryption Certificate: Secure Mail Certificate

Encryption Algorithm: AES (256-bit)

☑ Send these certificates with signed messages

In the sections '**Singing Certificate**' and '**Encryption Certificate**' your certificate must be listed. In many cases you only see the 'friendly name' of your certificate; this could be your e-mail address, your name or simply some description like we have in our screenshot above.

Once you can confirm that, you can just confirm the configuration by clicking 'OK' and you are ready to use your Outlook with full S/MIME capability.

Note:
If your no appropriate certificate is listed, your certificate is either not installed with the private keys available or is not valid to use for S/MIME (no item 'Secure Mail' in the certificate's Enhanced Key Usage property). If the latter case is true, there is no further way to troubleshoot. You need to start the registration process with another Certificate Authority that allows you use your certificate for S/MIME.

7 Secure Mail Service Registration

When you are not already registered for Secure Mail you need to ask a Novartis associate to send you an encrypted e-mail. This would then trigger a registration message that will be sent to you. This is the only registration method for external partners of Novartis.

If the Novartis associate is not able to send you an encrypted e-mail, he is probably not yet registered for Secure Mail. In that case the Novartis associate can find information about registering himself on the Secure Mail service site:

https://securemail.novartis.com/secure-mail/getting-started.shtml

Once you have the registration message in your mailbox you have two basic options:

1. Register at the Novartis Secure Mail Portal manually and receive SecurePDF's that allow computer independent communication with little effort. For sending e-mail the Secure Mail Portal must be used.
2. Auto-Register by replying with his own personal digital identification (S/MIME or PGP).

As this guide is about the usage of a S/MIME-certificate you want to use option #2. Nonetheless, if you were already registered to Secure Mail you already did the registration procedure from option #1. Please follow the S/MIME registration in the following sub-chapters based on your precondition.

7.1 Manually registered Secure Mail Portal users (SecurePDF)

If you had registered manually (sometime in the past) for receiving SecurePDF, you have been enabled to login to the Secure Mail web portal. In this web portal you have to upload your S/MIME certificate and change a preference setting in order to get your e-mails encrypted with it.

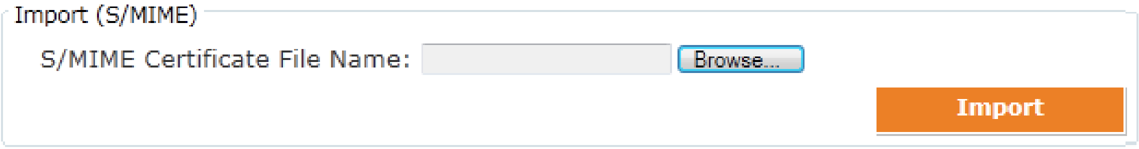
In order to prepare for the upload you need to export your public certificate (see 'Export' in chapter 4.6.1). The certificate file usually has one of the following file extensions:

- .pem
- .p7b
- .crt
- .cer

After that, please log in to https://secure-mail.novartis.net/SecMail/login.jsp with your e-mail-address and password.

- Navigate to 'Preferences' -> 'Certificates'
- Choose your certificate file and import it (see Figure 9)
- Change 'Preferred delivery method' to S/MIME-certificate
- Use the 'Logout' button

Figure 9: Import public certificate on Secure Mail service



Note:
If you have renewed your certificate, the above procedure must be repeated.

7.2 Auto-Registering your S/MIME-certificate

The Secure Mail Service allows you to auto-register with your S/MIME-certificate. The only precondition is that you have received the initial registration message from the Secure Mail Postmaster. The registration can be done by just replying to that e-mail with your S/MIME-signature (what happens when your mail client is setup accordingly). As the initial e-mail is already signed, you usually just need to reply and send it. A particular reply text is not needed. On Microsoft Outlook you can check if the reply will be signed by navigating to the **Option** ribbon where the **Sign**-button must be activated.

The replied e-mail with your signature also contains your public S/MIME-certificate. Your certificate will be captured by the Secure Mail Service and from now on be used for secure communication between you and Novartis associates (or other external registered partners).

The original e-mail initiating the registration message is now encrypted with your certificate and delivered to your mailbox. In your mail client you should now be able to open/read the e-mail message without further actions. As you will still get security warnings please proceed with the actions of chapter 8.

7.2.1 How to treat S/MIME-certificate renewals

When you used auto-registration you don't have a login for the Secure Mail Service Portal where you could upload your new certificate. In that case you can just install and use the new certificate on your client. Once you send secured e-mails to Novartis associates with your new certificate, the certificate change will be noticed by the Secure Mail Service personnel. After some short time (some business days) your new certificate will be approved and from then on the new certificate will be used to communication toward you as well. Before the approval e-mails sent from Novartis associates to you are still encrypted with your old (many even expired) certificate. As you should never delete your old, expired or even revoked S/MIME-certificates you shouldn't be impacted too much until the approval from the service personnel.

8 Start communicating securely with S/MIME-certificates

Once all the steps from the previous chapters were taken, you finally want to start communicate securely. In order to get to that point both communication partners must have the counterparty's public certificate. This is how asymmetric cryptography works and there is no way around that.

For that purpose you could send your exported certificate (not the backup certificate!) or simply send a signed e-mail - which is much easier most of the times. Your communication partner could then just reply (as well signed) and then you have his certificate as well. The exact steps can be taken from the sub-chapter below.

As well in special cases (like for Novartis) you will need to accept and import the root certificate first before you can get rid of security warnings (see chapter 8.2).

8.1 Exchanging public certificates is a precondition

As mentioned before you always need to have the recipient's public certificate before you can securely communicate with encrypted and signed e-mails. Therefore we recommend doing the following steps described here for **every new recipient**:

1. Send a signed e-mail to the recipient by using the button 'Sign' in the 'Options' tab within your e-mail draft. In this e-mail ask your partner to reply to it while keeping it signed.
2. Once you receive a singed e-mail from your communication partner, you can start communicating securely with the options 'Sign' and 'Encrypt'.
3. For later usage please add or update your partners contact in your address book because you want to make sure the public key is available when composing new e-mail messages.

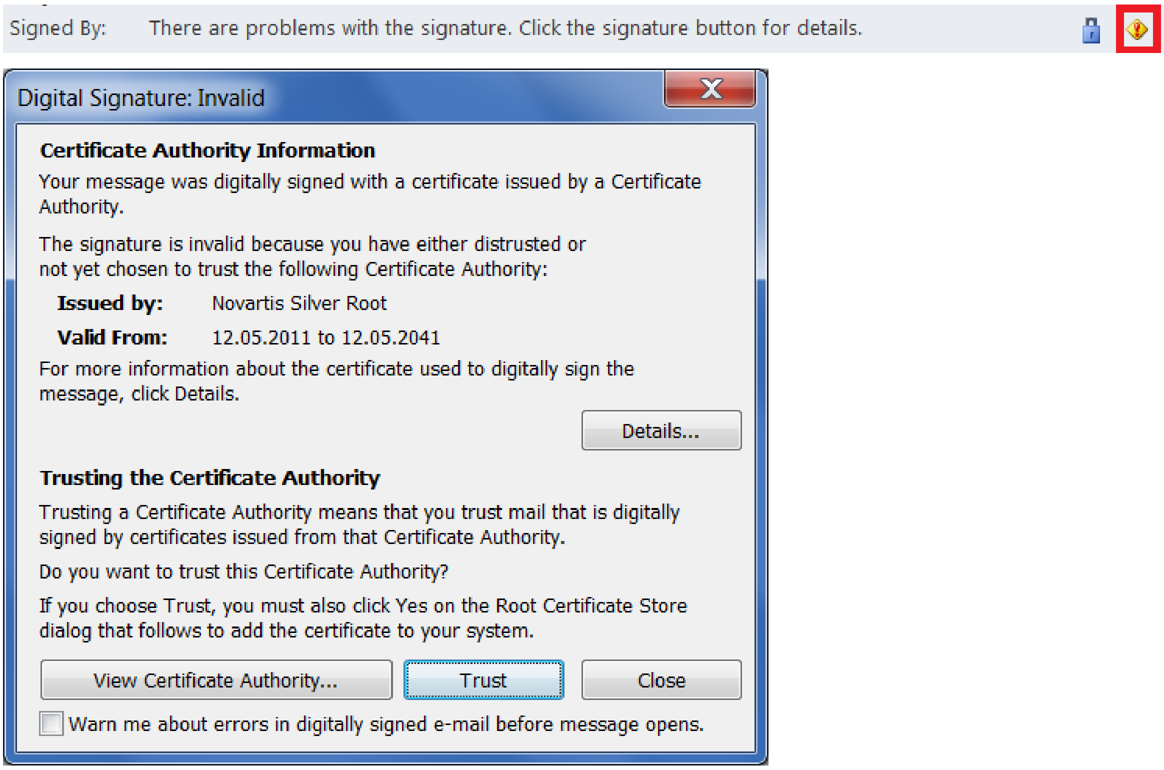
If you have installed and setup your S/MIME-certificate on more than one computer it is recommended to share the same address book or synchronize your entries manually (export/import). As well an export is suggested for backup reasons as the exchange of the public certificates is quite cumbersome.

It is quite possible that your communication partner's certificate will be renewed sometime, so updating the contact in your address book might be necessary more than once over the years.

8.2 Initial security warnings on e-mails from Novartis associates

When start communicating with Novartis associates you'll notice that you get security warnings in e-mails that could look like in the figure below. This is because Novartis is maintaining its own Public Key Infrastructure with an own root certificate that is not trusted by operating systems or browsers out-of-the-box.

Figure 10: Security warning and dialog



Signed By: There are problems with the signature. Click the signature button for details.

Digital Signature: Invalid

Certificate Authority Information

Your message was digitally signed with a certificate issued by a Certificate Authority.

The signature is invalid because you have either distrusted or not yet chosen to trust the following Certificate Authority:

Issued by: Novartis Silver Root

Valid From: 12.05.2011 to 12.05.2041

For more information about the certificate used to digitally sign the message, click Details.

Trusting the Certificate Authority

Trusting a Certificate Authority means that you trust mail that is digitally signed by certificates issued from that Certificate Authority.

Do you want to trust this Certificate Authority?

If you choose Trust, you must also click Yes on the Root Certificate Store dialog that follows to add the certificate to your system.

□ Warn me about errors in digitally signed e-mail before message opens.

We strongly recommend to import and trust the Novartis root certificate so the security warning disappears. Only that way you can easily determine if there is some fraud or not (e.g. if the sender is really the sender who he claims to be, etc.).

This can be done by clicking on the warning sign on your e-mail message (see red rectangle in the figure). In the popup dialog click 'Trust' and on a next dialog check if the fingerprint is equivalent with this:

36 94 b6 0c a9 17 b9 d7 e6 0f d2 a4 c4 e5 4e ae 48 04 5f a9

If this fingerprint matches the displayed fingerprint, you can allow the insertion into the trusted root store. After that (when the view is updated) the sign should disappear and there should not be any security warning anymore.

9 Support and Liability

As already mentioned in the chapter 'Document Purpose and Introduction' this document is intended to help external partners of Novartis. However, Novartis does not guarantee that the provided information in this guide helps you or is correct in under any circumstances. Novartis assumes no liability for actions that are recommended in this manual.

Please note that non-Novartis users cannot get any direct support from the Novartis IT Service Desk or from the Secure Mail Service personnel. External partners will have to contact a Novartis associate for any issue related to the Secure Mail Service.

More information and helpful troubleshooting advice can be found on the Secure Mail Service website https://securemail.novartis.com/secure-mail.

In general the Novartis Secure Mail Service Disclaimer is valid (see below).

9.1 Novartis Secure Mail Service Disclaimer

Users in the following countries are not allowed to use the Secure Mail system: Sudan, Syria, Iran, Iraq, North Korea, Rwanda and Cuba

By registering as an external user and creating a user account, you accept and agree that the use of Secure Mail to secure electronic information exchange is entirely at each individual user's own risk. To the maximum extent permitted by law, Novartis and its affiliates hereby disclaim any and all representations and warranties, whether express, implied or statutory, including, but not limited to, any representations or warranties related to title, non-infringement, performance, availability, confidentiality of information, security, fitness for a particular purpose, accuracy or completeness of the Secure Mail system. To the maximum extent permitted by law, in no event shall Novartis or any of its affiliates be liable for any losses, damages, claims or liabilities whatsoever arising out of or in any way related to the use, or inability to use, Secure Mail.

Further, you hereby agree to access and use your Secure Mail account only for purposes of securing electronic information exchange with other authorized and registered users and for no other purpose, and only in accordance with all applicable laws and regulations. You also undertake not to share your Secure Mail password or account details with any third party. Novartis reserves the right to, at its own discretion and without notice, change or terminate user access to Secure Mail and to deregister any external user and terminate any user account.

You hereby acknowledge and agree that the content of any electronic mail messages sent or received by you may be accessed, used or inspected by Novartis or any of its affiliates for any legitimate business reason and may be disclosed by Novartis or any of its affiliates to law enforcement officials or other third parties if Novartis or its relevant affiliate is legally compelled to do so in connection with any litigation, arbitration, investigation, audit or other legal proceeding.

The terms hereof shall be governed by the laws of Switzerland and any dispute shall be referred to the courts of Basel Stadt, Switzerland.