User Manual: SuisseID Signing Service by QuoVadis

Content

1 Basics .................................................................................................................................................. 2
  1.1 Self-enrollment process .................................................................................................................. 2
  1.2 Strong authentication ...................................................................................................................... 3
  1.3 Important Abbreviations ................................................................................................................ 3

2 Requirements ....................................................................................................................................... 3
  2.1 Mobile Phone with internet access (Smartphone) ........................................................................ 3
  2.2 Email account ................................................................................................................................ 3
  2.3 Windows Computer with internet access ....................................................................................... 4
  2.4 QuoVadis PIN letter ....................................................................................................................... 4

3 SIDSS Self-enrollment ......................................................................................................................... 4
  3.1 Self-enrollment Email ..................................................................................................................... 4
  3.2 2 factor authentication App Installation ........................................................................................ 5

4 True-Sign V (Middleware) .................................................................................................................. 9
  4.1 Download true-Sign V ..................................................................................................................... 9
  4.2 Install the true-Sign V Client .......................................................................................................... 9
  4.3 Add your Account ........................................................................................................................... 9
  4.4 Change Certificate PIN .................................................................................................................. 11

5 Update True-Sign .................................................................................................................................. 13
  5.1 Delete Account .............................................................................................................................. 13
  5.2 Uninstall True-Sign ........................................................................................................................ 14
  5.3 Installation true-Sign ....................................................................................................................... 14
1 Basics

1.1 Self-enrollment process

This is the process which you are requested to follow to use the SuisseID Signing Service by QuoVadis:

Start
(Email from QuoVadis)

Email from
noreply@safenet-inc.com

"Self-Enrollment"
Website

2 factor authentication
App Installation

Add Account

True-Sign V
(Middleware)
Installation

Token-generation in
MobilePass App

Authentication via
2 factor authentication
App

Transport-Code
SMS
(delivered at beginning)

Change certificate
password

End
(Using SuisseID Signing
Service)
1.2 Strong authentication
Based on the strong authentication we use, several security queries are necessary. Specifically are these the following three:

- Transport PIN (TIN) from QuoVadis PIN letter
- OTP PIN from 2nd Level Authentication App
- Passcode from 2nd Level Authentication App

Please remember the secrets (passwords) because you need them later on.

1.3 Important Abbreviations

- SuisseID Signing Service by QuoVadis subsequent named as SIDSS
- SafeNet MobilePass App subsequent named as SMPA
- CRYPTOCard MP-1 Authentication Token named as MP1
- Transport PIN subsequent named as TIN

2 Requirements

2.1 Mobile Phone with internet access (Smartphone)
To get a Token, which is needed for the authentication, you have to install 2 factor authentication App. Therefore you need an App-compatible mobile phone with internet access and allowed cookies:

- **Apple**: Requires iOS 4.3 or higher
- **Android**: Requires Android-version 2.3 or higher
- **Windows Phone**: Works with Windows Phone 7.5, 8 and 8.1
- **BlackBerry**: BlackBerry 10

2.2 Email account
SIDSS sends you an activation email with the linked 2 factor authentication App. To get this email you need a valid email account to which you have access from your mobile device.
2.3 Windows Computer with internet access
You need a Windows Computer to use the middleware true-Sign V for the certificates.

Requirements:

- 1 GB RAM or higher
- Minimum 130 MB of free disc space
- Windows Vista 7, 8 or 8.1
- Local administrator permissions to install software and driver

2.4 QuoVadis PIN letter
Concurrently to the sent self-enrollment email, QuoVadis will send you a PIN letter per mail. This PIN letter contains the TIN, which you need to activate your SIDSS account (see chapter 4.4).

3 SIDSS Self-enrollment
3.1 Self-enrollment Email
Because of the self-enrollment, an email was sent to you from noreply@safenet-inc.com. Open this email with the subject “QuoVadis – SuisseID Signing Service Self-enrollment” on your mobile phone and click on the Link provided to enroll with QuoVadis – SuisseID Signing Service. The email looks like this:

Your self-enrollment account has been created.

If you are enrolling a hardware token and do not yet have your token, contact your system administrator.

Go to the following URL to enroll with QuoVadis - SuisseID Signing Service:

https://se.safenet-inc.com/selfEnrollment/index.aspx?code=aSMEKqxbCxGT60NDYdfUD08r

If the above link does not work, copy and paste this URL to your web browser.
3.2 2 factor authentication App Installation

After clicking on the link provided in the previous email, a new page opens, based on the type of your mobile device:

<table>
<thead>
<tr>
<th>Mobile Device Operating System</th>
<th>SafeNet App</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>SafeNet Mobile Pass</td>
</tr>
<tr>
<td>Android</td>
<td>SafeNet Mobile Pass</td>
</tr>
<tr>
<td>Windows Phone</td>
<td>SafeNet Mobile Pass</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>CRYPTOCard MP-1 Authentication Token</td>
</tr>
</tbody>
</table>

3.3 Installation for iOS, Android or Windows Phone

Click on the SMPA-Icon to install the App. If you don’t see an icon as shown below, you have to allow cookies in your internet settings.

Enroll your MobilePass token

After you’ve installed the SMPA switch back to the website from the self-enrollment email and click on the Link “Enroll your MobilePass token”. Once you’ve clicked on the link, SMPA will be opened and you are in the process to create a new Token (Passcode and OTP PIN). Name your token “SIDSS” and click on “Activate”. 
Important notice: Please remember your OTP PIN which you define in the following step:

Now you have to create your OTP PIN, which should contain between 3 to 8 decimal or alphanumeric characters. The OTP PIN is a further protection which you need later on. Please remember your OTP PIN and confirm with “Continue”.

Passcode

After the self-enrollment you get the Passcode. You will need it to get your certificates with the true-Sign V Client and a new one for changing your SID Signing Account password. To create a new token, click on “Generate Passcode”.
3.4 Installation for BlackBerry:

Click on “Next” to start the process.

A new website will be loading with the information about the next steps. You will receive a new email with an initial PIN and an OTA installation link.
Follow the instructions shown in the email you receive with the subject “Over-The-Air (OTA) Installation for BlackBerry” from noreply@safenet-inc.com.

**Passcode**

After the self-enrollment you get the Passcode. You will need it to get your certificates with the true-Sign V Client and a new one for changing your SID Signing Account password.
4 True-Sign V (Middleware)

True-Sign V is the Middleware for SIDSS. It is required to manage your certificates.

4.1 Download true-Sign V

To get access to your certificates you need to install the true-Sign Client, which you can download here:

- Windows 64-Bit Version:  
  http://downloads.quovadisglobal.com/CH_SIDSS_TRUE_SIGN_V_CLIENT_WINx64.zip

- Windows 32-Bit Version:  
  http://downloads.quovadisglobal.com/CH_SIDSS_TRUE_SIGN_V_CLIENT_WINx86.zip

Open the downloaded ZIP file with a DoubleClick and extract the installation file with drag it on your Desktop.

4.2 Install the true-Sign V Client

Double-click the downloaded installation file and confirm the security message. After confirming the security message, the installation and program-start is automated. You can find the true-Sign Client it in the Windows info-area as shown below:

4.3 Add your Account

Right-click the true-Sign Client Icon and click on „Accounts...“. After the Client is opened click on “Add” to append a new account.
Fill in the following information and complete with “Next”:

E-Mail-Adresse analogue application form

OTP PIN from 2 factor authentication App

Passcode from 2 factor authentication App

After successful login you can click on “Finish”.
4.4 Change Certificate PIN

Choose your certificate by clicking on it and select „Change PIN“.

Authenticate the PIN-change-process while you enter your OTP PIN and MobilePass token. Confirm with “OK”: 

Your email address analogue certificate request
Password = OTP PIN
One Time Passcode = Passcode (MobilePass token)
Now you need your TIN from the QuoVadis PIN letter. Fill in the TIN in “Current PIN” and type a new PIN below twice. Confirm with “OK”:

![Image of QuoVadis PIN change interface]

Current PIN = Transport PIN from QuoVadis PIN letter
New PIN = Choose a new PIN
Confirm new PIN = Confirm the new PIN

After you changed the certificate PIN successful, the “keyon Virtual Smart Card”-driver will be installed and you can use your certificate:

![Image of keyon Virtual Smart Card installation]

![Image of certificate registration account]

Certificate Valid till Status
YOUR NAME (Qualified Signature) 18.08.2017 Ok
5 Update True-Sign

5.1 Delete Account

Open the true-Sign client. You can find the true-Sign Client it in the Windows info-area as shown below:

Choose your certificate by clicking on it and select „Delete“.

Accept the following message with „Yes/Ja“:
5.2 Uninstall True-Sign

Go to Windows Start and click on „control panel“:

Choose now „Programms and Features“ or in the category style „Uninstall Programm“.

Right click on „true-Sign V“ and choose deinstall. Accept the upcoming dialogue with „Yes/Ja“:

P.R.N. it will pop up a dialogue for data and service. Please accept it with “OK”:

5.3 Installation true-Sign

Follow point 4a.