Contents

1 Objectives ........................................................................................................................................... 2
  1.1 Document objectives .................................................................................................................... 2
  1.2 Terminology ................................................................................................................................... 2

2 Overview ............................................................................................................................................... 2
  2.1 Components .................................................................................................................................. 2
  2.2 Purpose .......................................................................................................................................... 2

3 Installation .............................................................................................................................................. 2

4 User interface ......................................................................................................................................... 3
  4.1 Configuration .................................................................................................................................. 3
    4.1.1 Certificate Service Address ....................................................................................................... 4
    4.1.2 User ID / Signer ID .................................................................................................................... 4
    4.1.3 Customer ID / Sender ID ........................................................................................................... 4
    4.1.4 Output Folder ............................................................................................................................ 4
    4.1.5 Reset To Defaults ..................................................................................................................... 4
  4.2 Certificate download ....................................................................................................................... 6
    4.2.1 Downloading a new certificate and installing it to the local Windows Certificate Store .......... 6
    4.2.2 Downloading a new certificate and exporting it to a file ......................................................... 7
  4.3 Certificate renewal .......................................................................................................................... 8
    4.3.1 Installing a new certificate locally ............................................................................................ 8
    4.3.2 Exporting a new certificate to a file ......................................................................................... 9
  4.4 Signing ........................................................................................................................................... 9
  4.5 User Guide ....................................................................................................................................... 10

5 Troubleshooting ..................................................................................................................................... 10
  5.1 Logs ............................................................................................................................................... 10
  5.2 Problem with installation .............................................................................................................. 11
    5.2.1 Missing root certificate .......................................................................................................... 11
    5.2.2 Unsupported platform ............................................................................................................ 11
  5.3 Cannot download new certificate ................................................................................................... 11
  5.4 Certificate is not found for signing or Certificate renewal ............................................................ 11
  5.5 Exporting certificate to file failed / Saving signed file failed ....................................................... 11
  5.6 Cannot open my file to sign ........................................................................................................... 11
1 Objectives

1.1 Document objectives
This is the User Guide for the Nordea Security Client 2. It is intended for end users and Nordea support staff.

1.2 Terminology
In the document, the following terms are used.
1. Nordea Security Client 2 – a PC Client used to sign files and download certificates
2. Nordea Certificate Service – A web service used to issue certificates

2 Overview

2.1 Components
The Nordea Security Client 2 is provided in a single installation package. It is a single application installed in a dedicated Windows application container. Please note that the installation folder is managed and protected by the Windows platform and might not be accessible without administrator privileges. Typically, the installation folder path should be as follows:
c:\Users\<user_name>\AppData\Local\Packages\NordeaSecureClientDEMO_2bnd5fqs75xpe\n
2.2 Purpose
The purpose of the Nordea Security Client 2 is to provide a way for the user to:
Sign files using a certificate stored in the Windows Certificate store.
Download a certificate from Nordea and either install it in a local Windows Certificate Store or export it in a .p12 file.

3 Installation
Start the installer from the provided MSIX package.

Note: Windows will automatically translate this screen to the local windows language.
Note: There is no option to choose an installation folder. The Nordea Security Client 2 is installed in a specific Windows application container that is fully managed by the Windows operating system.

4 User interface

The Main menu is launched when you start Nordea Security Client 2. To start it, click the application icon labelled Nordea Security Client 2 from the Windows Start Menu. The Main menu has 5 active buttons: Configuration, Certificate Download, Certificate Renewal, Signing and User Guide. There is also a version information label in the bottom right corner.

4.1 Configuration

The Configuration view enables users to customise Certificate Service Address, User ID/Signer ID, Customer ID/Sender ID and Output Folder. Note that values set here are applied in all other operations within the Nordea Security Client 2 application.
4.1.1 Certificate Service Address
Specify the **Certificate Service Address** that is used to obtain certificates.

4.1.2 User ID / Signer ID
The **User ID / Signer ID** value can be found in the Customer Agreement as “Signer ID” for Corporate Access and Corporate Access Lite customers, and as “Logon ID” for Finnish and Corporate eGateway Web Services customers. The stored value is pre-filled in all the respective fields in the **Certificate Download** and **Certificate Renewal** views. It is also used during the Sign operation.

4.1.3 Customer ID / Sender ID
The **Customer ID / Sender ID** value can be found in the Customer Agreement as "Sender ID" for Corporate Access and Corporate Access Lite customers. The "Customer ID / Sender ID” field in the Signing view will be pre-filled with this value.

4.1.4 Output Folder
The **Output** folder is the location where the Nordea Security client 2 will store all signed files and exported .p12 certificate files. Please make sure the Output folder defined should be existing in the PC.

4.1.5 Reset To Defaults
All four fields can be reset to their default values using the button in the upper right corner.
• Click on the icon in upper right corner.
• Click the **Reset To Defaults** pop-up button.

• Confirm the action by clicking **OK** in the pop-up dialog. You can also close this dialog if you do not want to reset to default.
4.2 Certificate download

The Certificate Download view is used to get a new certificate from Nordea. Please make sure that the Certificate Server Address is correctly set in Configuration View.

If you already have a valid Nordea certificate, you can alternatively use the Certificate Renewal view, which has less information to complete.

4.2.1 Downloading a new certificate and installing it to the local Windows Certificate Store

- Specify Name / Certificate Receiver as stated in your agreement with Nordea. It is important that you use the exact spelling as in the Customer Agreement as this will be verified during the process.
- Specify User ID / Signer ID as stated in the Customer Agreement.
- Provide the one-time use SMS Activation code, received from Nordea during registration of the service. The SMS code was previously sent to your mobile phone. If you do not have an SMS code, please contact Nordea to receive a new one.
- Select a Country Code, depending on which country you use the service from.
- Select required Certificate Key Length and Certificate Hash Algorithm values from the lists.
- In Action, choose Install locally.
- Click on Request Certificate.
- If the installation is successful a confirmation message appears and you are returned to the Main menu.
• The new certificate is stored in Certificates-Current User / Personal / Certificates as shown in the following figure:

4.2.2 Downloading a new certificate and exporting it to a file

• Specify **Name / Certificate Receiver** as stated in your agreement with Nordea. It is important that you use the exact spelling as in the Customer Agreement as this will be verified during the process.
• Specify **User ID / Signer ID** as stated in the Customer Agreement.
- Provide one time use **SMS Activation code**, received from Nordea during registration of the service. The SMS code was previously sent to your mobile phone. If you don’t have an SMS code, please contact Nordea to receive a new one.
- Select a **Country Code**, depending on which country you use the service from.
- Select required **Certificate Key Length** and **Certificate Hash Algorithm** values from the list.
- In **Action**, choose **Export to File**.
- Enter the **Password** to protect the certificate file, again in **Confirm Password**.
- Click **Request Certificate**.
- If the export is successful a confirmation message appears and you are returned to the **Main menu**.
- The new certificate is stored in a .p12 file in the **Output Folder** specified in the **Configuration** view.

### 4.3 Certificate renewal

Certificate Renewal is used to replace an existing valid Nordea certificate with a more recent one. Please note that after downloading a new Nordea certificate, the previous one is no longer valid even if it has not yet expired.

#### 4.3.1 Installing a new certificate locally

- Specify **User ID / Signer ID** as stated in the Customer Agreement.
- Click **Request Certificate**.
- If the installation is successful a confirmation message appears and you are returned to the **Main menu**.
- The new certificate is stored in **Certificates-Current User / Personal / Certificates** as shown in the following figure:
User interface

Note: The old certificate is not removed from the Windows Certificate Store.

4.3.2 Exporting a new certificate to a file

1. Specify User ID / Signer ID as stated in in the Customer Agreement.
2. In Action, choose Export to file.
3. Enter the Password to protect the certificate file, again in Confirm Password.
4. Click Request Certificate.
5. If the export is successful a confirmation message appears and you are returned to the Main menu.
6. The new certificate is stored in a .p12 file in the Output Folder specified in the Configuration view.

4.4 Signing

To sign and produce Corporate Access Secure Envelope files, you need to have a valid certificate installed in Certificates-Current User / Personal / Certificates. If you do not, please consult the Certificate Download chapter of this User Guide.
4.5 User Guide

The User Guide view is dedicated to present this User Guide document. You can either view it directly in the application or export it as a PDF file via the Save as PDF button.

5 Troubleshooting

5.1 Logs

To start collecting application logs, the following log folder must be created on the local drive:

- Fill in the Signer ID as stated in the Customer Agreement. If you have filled the Signer ID in the Configuration view, this field will be pre-filled when you open the Signing view.
- Fill in the Sender ID as stated in the Customer Agreement. If you have filled the Sender ID in the Configuration view, this field will be pre-filled when you open the Signing view.
- In Select File To Sign, click Browse and select the file you want to sign.
- Select a Hash Algorithm to use in the signing process.
- The signed file can be found in the Output Folder specified in the Configuration view.

The User Guide view is dedicated to present this User Guide document. You can either view it directly in the application or export it as a PDF file via the Save as PDF button.

5 Troubleshooting

5.1 Logs

To start collecting application logs, the following log folder must be created on the local drive:
C:\Nordea2Logs\

A separate log file is created for each application run. These logs can be used by Nordea Support to solve issues. When logging is no longer needed, the log folder can be deleted and no more logs will be created.

5.2 Problem with installation

5.2.1 Missing root certificate
Make sure that the following certificate is installed and trusted in your system:
DigiCert Trusted G4

5.2.2 Unsupported platform
Check the Supported Platforms chapter to see if your system is compliant.

5.3 Cannot download new certificate
There are several possible reasons why a certificate many fail to download. In each case, the error pop-up dialog will provide the specific reason for failure.

5.4 Certificate is not found for signing or Certificate renewal
The Nordea Security Client 2 requires the user certificate to be stored in Certificates-Current User / Personal / Certificates.
Certificates that are not issued by Nordea, are expired or do not have matching User ID identification are ignored.
To check if the certificate is present, open the Windows Certificate Manager by running certmgr.csc from the Start menu.

5.5 Exporting certificate to file failed / Saving signed file failed
Check that the Output Folder set in the Configuration view is accessible and you have sufficient access rights to save files in this folder.

5.6 Cannot open my file to sign
Check if the file is accessible and you have sufficient access rights.
Check the size of the selected file. Despite no explicit file size limit, signing files larger than 600 MB can result in unexpected behaviour.

6 Supported platforms
The Nordea Security Client 2 can run on the following Operating Systems:
7 System setting of Reginal format

The Reginal format defined in Setting of Operating System needs to have time-separator of colon (:) instead of period (.). Otherwise the timestamp produced by Nordea Security Client 2 will be considered not valid by Nordea Certificate Service.

Example of correct Reginal format:

```
Region

Country or region
Finland

Regional format

Current format: English (United States)

Regional format data

Select Change data formats to switch among calendars, date, and time formats supported by the region.

Calendar: Gregorian Calendar
First day of week: Sunday
Short date: 2/9/2023
Long date: Thursday, February 9, 2023
Short time: 11:05 AM
Long time: 11:05:08 AM

Change data formats
```