Corporate Netbank
- Data security instructions

Secure logon

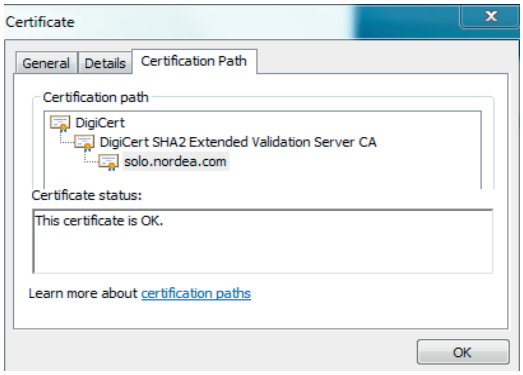
User authentication
The user's identity towards Corporate Netbank is verified by logging on using a:

- card reader without cable
- card reader with cable
- Nordea Codes

This logon information is personal. The code card, chip card or mobile device must never be handed over to any other user.

The logon information should only be entered when you are in a secure session to Nordea Corporate Netbank. Look for a padlock in the lower bar of the browser screen or to the right of the address bar in the browser. The padlock confirms that the browser has an encrypted tunnel to Nordea.

To be completely sure that the tunnel goes to Nordea, click on the padlock and you should see the screen below.



Secure data transport via the Internet
Due to the encrypted tunnel (SSL encryption) data can neither be seen nor manipulated by any unauthorised party when transferred between your browser and Nordea.

Antivirus program
Virus and other malicious software are a threat to all PC users today. Virus may come from USB memory sticks (or other removable media), from e-mails or material downloaded from the Internet. There are fake programs in the market so make sure that you always run an acknowledged antivirus program on your PC.

- Make sure the antivirus program contains the latest virus signature files.
- If a virus attack is detected, immediately contact the persons in your company responsible for IT or IT security and avoid using the PC until the virus has been removed.

The exact look of the screen may vary between different browsers and browser versions.

Internet browsers

Your browser and its configuration have a strong influence on your PC security. While you are on the Internet, your browser may accept running external programs, but it should not be done indiscriminately.

You are advised to:

- Use the latest version of your Internet browser.
- Configure the browser so you are requested to accept transfer of programs from the PC to the Internet or vice versa.
- Only download files from vendors that you can trust in terms of security.
- Only accept signed applets, ActiveX controls and other executables from trustworthy vendors or do not import programs at all.
- Use the browser's standard security configuration as a minimum.

Firewall

You should always have firewall protection against insecure networks. If your PC is connected to the company's local network, a firewall usually exists between this local network and the Internet. The firewall prevents unauthorised access to the local network from the Internet. If you do not have firewall protection and you use a stand-alone PC, we recommend that you install a personal firewall on your PC and ensure that only neccesary traffic is allowed.

To get access to Nordea Corporate Netbank, open the protocol HTTPS on port 443 in the firewall. A high security level is obtained by only opening for traffic OUT through the port in the firewall and for example only to Nordea's URL address:
https://solo.nordea.com/nsc/engine.

Report suspicious activities

If you experience abnormal netbank behaviour (delayed logon process or pop-up windows) or suspect your netbank session security in general, contact your administrator or Nordea immediately.

Blocking access to Corporate Netbank

If you have lost your logon information or you suspect misuse for other reasons, the card and/or Nordea Codes app must be blocked immediately. If the card is blocked, a new one must be activated. You can block the card, ask for a new card to be activated and block the Nordea Codes app by contacting either your administrator or one of your support contact persons in Nordea.