

Corporate Netbank

Datasikkerhedsinstrukser

Sikker logon

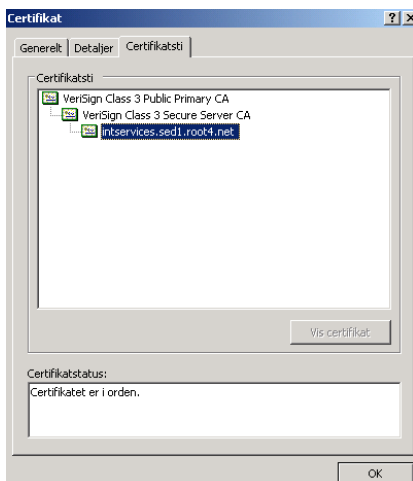
Brugeridentifikation

Brugerens identitet i Corporate Netbank verificeres ved brug af en identifikationsmetode:

- kortlæser med kabel
- kortlæser uden kabel

Logon-oplysningerne er personlige. Identifikationsmetoden må ikke overdrages til andre brugere.

Du bør kun indtaste logon-oplysningerne, når du starter en sikker session af Nordea's Corporate Netbank. Kontrollér, at der er en hængelås i browserens statuslinje eller til højre i browserens adresselinje. Hængelåsen bekræfter, at browseren har en krypteret forbindelse til Nordea. For at være helt sikker på, at forbindelsen er til Nordea, kan du klikke på hængelåsen, og så ser du dette skærm billede:



Sikker dataoverførsel via internettet

Den krypterede forbindelse (SSL-kryptering) sikrer, at data, der overføres mellem din browser og Nordea, hverken kan ses eller manipuleres af uautoriserede brugere.

Antivirusprogram

Virus og anden ondsindet software udgør en trussel for alle pc-brugere i dag. Virus kan stamme fra USB-nøgler (eller andre flytbare medier) eller e-mail eller kan downloades, mens du er på internettet.

- Sørg for altid at have et anerkendt antivirusprogram på din pc.
- Kontrollér, at antivirusprogrammet har de seneste virusdefinitioner.
- I tilfælde af et virusangreb skal du omgående kontakte din virksomheds it-ansvarlige og lade være med at bruge pc'en, før virussen er fjernet.

Billedet kan se forskelligt ud afhængigt af browser og browserversion.

INFORMATION

Ønsker du flere oplysninger om Corporate Netbank, kan du kontakte din lokale rådgiver i Nordea.

NORDEA.COM/CN

GENVEJE

Mere information om Nordea's cash management produkter finder du på:

NORDEA.COM/CASHMANAGEMENT

NORDEA.COM/CN

FAKTA

Corporate Netbank giver nem og sikker adgang til en bred vifte af banktjenester og giver et samlet overblik over likviditeten inklusive information om saldo- og transaktioner i realtid.

Internetbrowsere

Din browser og dens indstillinger har meget stor betydning for sikkerheden på din pc. Mens du er på internettet, kan din browser acceptere at afvikle eksterne programmer, men det bør ikke ske vilkårligt.

Vi anbefaler derfor, at du:

- bruger den seneste version af din internetbrowser
- indstiller browseren, så den beder dig om at acceptere overførsel af programmer fra pc'en til internettet eller omvendt
- kun downloader filer fra leverandører, som du kan stole på, når det gælder sikkerhed
- kun accepterer signerede applets, ActiveX-kontroller og andre eksekverbare programmer fra pålidelige leverandører eller blokerer fuldstændigt for import
- som minimum bruger browserens standard sikkerheds-indstillinger.

Firewall

- Du bør altid have en firewall som beskyttelse mod usikre netværk. Hvis din pc er koblet til virksomhedens lokale netværk, er der normalt en firewall mellem dette netværk og internettet. Denne firewall beskytter mod uautoriseret adgang til det lokale netværk fra internettet.
- Hvis du ikke har en firewall, fx hvis du bruger en stand-alone pc, anbefaler vi, at du installerer en personlig firewall på din pc og sikrer dig, at den kun tillader den nødvendige trafik.

For at få adgang til Corporate Netbank skal du åbne protokollen HTTPS på port 443 i din firewall. Du opnår det højeste sikkerhedsniveau ved kun at åbne for trafik UD gennem porten i din firewall og fx kun til Nordeas URL-adresse: <https://solo.nordea.com/nsc/engine>

Rapportere mistænkelige aktiviteter

Hvis du oplever unormal adfærd (fx lang logon proces eller pop op-vinduer) eller mistænker sikkerheden generelt, kontakt da straks din administrator eller Nordea.

Spærring af adgang til Corporate Netbank

Hvis du har mistet dine logon-oplysninger, eller du har mistanke om misbrug af andre grunde, skal du straks spærre kortet og få aktiveret et nyt.

Du kan spærre kortet og bede om at få aktiveret et nyt ved at kontakte en af dine kontaktpersoner i Nordea.