# Girolink Internet and other communication methods

# Table of contents

# 1 General

Nordea’s communication method enables you to exchange files with payments and payment information between PlusGirot, Nordea and Bankgirot. This means you can send and receive files to/from both giro systems.

You can also use the communication methods when you want to exchange information in files between different companies.

All communication methods meet the requirements placed by users for secure handling of payments and information.

# 2 Communication method

We can offer communication solutions for companies of all types. Here is a short presentation. More detailed information on every communication method is shown in the technical manuals.

## 2.1 Interactive communication method

- GiroLink Internet – interactive interface

GiroLink Internet is a web-based file-generating service with very high security that also includes functions for authorising files. Ready to use with access via home page.

GiroLink Internet also exists as a technical interface. The bank provides specifications to program companies who have agreed to the integration of GiroLink Internet in their accounting systems, so-called Internet-bank connection to Girolink Internet.

## 2.2 Other communication methods (non-interactive)

- SFTP
- VPN via Internet – FTP
- VPN via Internet – Connect Direct
- VPN via fixed connection – FTP
- VPN via fixed connection – Connect:Direct
- Fixed connection TCP/IP – FTP
- Fixed connection TCP/IP – Connect:Direct
- SNIX IP – FTP
- SNIX IP – Connect:Direct

**VPN**
VPN (Virtual Private Network) is a method for establishing a secure point-to-point communication over the Internet, a so-called VPN tunnel. In this encrypted tunnel information is provided in a secure way.

To establish a VPN tunnel necessitates that both end points use the same VPN protocol. PlusGirot uses IPsec VPN. File transfer protocol that is used via a VPN tunnel is FTP or Connect: Direct

**Fixed connection**
For the communication to be able to work over a fixed connection with point to point communication necessitates a link network that is provided by telephone operator. SNIX-IP is a trouble-free solution from TELE 2 that offers encryption and choice of bandwidth.

A fixed connection can also be enforded by a VPN for increased security.

File transfer protocol that is used over a fixed connection is FTP or Connect: Direct

For complete information read also the appendix for the respective communication method

# 3 Support

## 3.1 GiroLink Internet

Questions regarding GiroLink Internet and Internet bank connection to GiroLink Internet can by answered by Technical Support on weekdays 08.00 - 22.00 on telephone number 031-771 6992. Program providers can go to proglev@nordea.se

## 3.2 Other communication methods (non-interactive)

Questions regarding other communication methods can be addressed to File Transfer between the hours of 08.00 and 18.00 all banking days on telephone number 08-23 99 30 or via email gkddvlx@nordea.se

# 4 Accessibility

File Transfer is open 24/7. However, certain planned stoppages for maintenance may occur. As a rule these take place occasionally on a Sunday.

# 5 Connection and agreement

Connections to Girolink Internet and other communication methods are made via Customer Centres, branch offices or though an official contact (account manager).

The following may be established depending on which communication alternative the customer has chosen:

- Agreement on file transfer
- If required an agreement for the chosen security solution
- If required a seal agreement
- If required, power of attorney
- If required power of attorney for a third party (when a Service provider is used)

The customer will be sent a node identity together with user name and password.

# 6 Technical information

## 6.1 Conditions for using Girolink Internet

With GiroLink Internet communication is done via logging on to the home page. All data is encrypted. In order to be able to send files an interface called Webstart is used. In connection with transmission time Girolink Internet combines the items in question to be sent (%-item) using a selected security solution, and creates at the same time a check sum(seal sum) that is verified online.

In order to run Webstart the following is required:

- A Java Runtime installation for Windows with the lowest version 1.4.2 that can be downloaded from www.sun.com. Direct Link exists in GiroLink Internet.

For installation of Java Runtime there are instructions in an MS-Word document, which can be downloaded after logging on to GiroLink Internet.

**Security solution**
The user can choose between two security solutions, Nordea’s e-identification or SmartSec.

**Technical data**

- Internet Explorer 5.01-8.0, Mozilla from version 1.7
- Web browser needs support for Java and cookies must be accepted.
- 128-bits SSL (Security Socker Layer) encryption.
- Recommended screen resolution: 1024*768

Internet Explorer is the sole alternative for activation of Nordea’s e-identification in respect of cards

**Operating system:**
Windows 2000
Windows XP
Windows Vista
Windows 7

**Card reader:**
A card reader is required if e-identification on *cards* and SmartSec is going to be used. Nordea provides the card reader Todos Argos Mini II from Todos AB for e-identification. Argos Mini II is sold with a USB cable. Argos Mini II is useable with Windows 2000, Windows XP and Windows 7.

The smartsec card reader is ordered in connection with the agreement.

**Strengthened security**
Payment files that are created in the accounting system often lie unprotected in the internal network before they are signed and dispatched. The application software Safepax Giro protects files from the instant they are created in the accounting system until they are collected in GiroLink Internet.

Safepax Giro is useable together with all existing accounting systems and is certified by Riksgäldskontoret, the National Debt Office. More information about Safepax and its distributors is shown on på www.safepax.se.

**One solution for all files**
Girolink Internet enables you to handle files both to/from PlusGirot, Nordea and Bankgirot.

**Language**
There are four language versions of GiroLink Internet: Swedish, English, Norwegian and Danish.

**Demo**
Read more about Girolink Internet on www.plusgirot.se where there is also a Demo.

## 6.2 Conditions for using other communication methods (non-interactive)

The conditions vary depending on whether one is sending or receiving files; see also information for the respective communication method under Appendices.

## 6.3 Files to PlusGirot, Nordea, Bankgirot or other party.

Each file is assigned a unique file name using a generation index, which explains how several files of the same type can be sent on the same day.

The following is needed for sending files:

- System that can create a file format for the service in question
- The ability to create sending items (%-items )
- The ability to create Seal for the file tampering protection
- Agreement as to service, communication method and seal
- Node identity, User name and password
- Agreement regarding file name
- Approved test of file content and Mac-code, see resp. User instruction
- File transfer protocol
- Possible VPN protocol

It is always the Customer who initiates a sending.

## 6.4 Files from PlusGirot, Nordea, Bankgirot or other party.

The following is required for receiving files:

- System that can receive a file format for the service in question
- Agreement regarding service, communication method

- Received Node identity
- Have submitted information on user name and password to PlusGirot
- Agreement regarding file name
- Tests, if any, are completed, see resp. User instruction per accounting service File transfer protocol
- Possible VPN protocol

It is always PlusGirot who initiates a sending.

# 7 File change protection for other communication methods

Security in PlusGirot's file transfer services is very high. The use of file change protection means that unauthorised changes cannot be made during the sending. When files are sent electronically it is highly important to ensure non-exposure to unauthorised changes. PlusGirot handles two different methods to ensure this. The methods area employed to ensure that the files come from the correct sender.

**Methods**

- HMAC
- Nexus Electronic Seal (SÄKData) protector code

### HMAC

HMAC is used as a file protection and make the files protected from unauthorized changes during the file transport to Nordea.

The file protection often called seal is used for all of the files that are sent to Nordea.

Nordea don't provide any software for creating HMAC seal and refer instead to open source and vendors of seal program. Technical specification, testing and information about HMAC is published on www.plusgirot.se/hmac.

### Nexus Electronic Seal

Nexus Electronic Seal (SÄK DATA) is a seal method that is provided by Technology Nexus and can also be used to Seal the files to Nordea. More information about Nexus seal by telephone 031-720 60 00.

## 7.1 Tests for other communication methods

Test must always be conducted before you can begin to send and receive files or when you make changes in for instance in changing the method of communication.
The tests that are compulsory are: test of communication, seal and service(file content).

## 7.2 Test of communication

Various test routines are applicable depending on the communication method that is to be tested. See Tests under the resp. communication method.

### 7.3 Test of service (application tests)

When communication is established the file content/layout is tested. The files are sent to the application's test node, which is specified at the place for the destination node in the per-cent items, see sector 13. The test varies according to the service in question. See the user instruction for the respective service at www.plusgirot.se /Företag.

### 7.4 Application Test support

You are welcome to contact the test group on banking days between 08.00-17.00 by telephone on 08-222202 or e-mail to pg.kundtester@nordea.se

## 8 Nordea's name standard for other communication methods

### 8.1 Files to Nordea

PDGSX.<user name>.F<file type>(+1)
For example: PDGSX.XTCPNET.FPO1(+1)

PDGSX is the first prefix in the file name. The second part consists of the user name and may be a maximum of 15 characters but is normally 7 characters. The third part is the file type's designation, see also the attached list of file types. (+1) after the file type is always a fixed value, a so-called generation index and is automatically calculated by Nordea when more than one file type is sent.

Name standard's third part, can as per agreement be fixed if there is a need and agreement has been reached.

### 8.2 Files from Nordea

The customer has the choice to decide on the file name according to the following standard XXXXXXX.XXXXXXX.XXXXXXX . Maximum seven characters between the points

## 9 Node identity

The key concept in PlusGirot's file transfer is based on nodes. A node is a logical representation of an application or a customer. The node that sends the files are called the Source node and is the node that **the file is to be sent to**, which is called the Destination node.

## 10 Sendning format

Sending format S2 facilitates standardised file identification. This is essential to a uniform standard for media management.

Sending format S2 also makes it possible to run several sub-files of the same type in a single sending. Each sub-file is to be surrounded by file items (%020 and %022) and the entire sending is to be surrounded by sending items (%001 and %002).

In other respects all per cent items have the same length as the application items. Letters must always be upper-case. All items are alfa-numerical and written left-aligned and blanks filled in (does not concern the number field in the File Trailer %022, which must be numerical and written right aligned and zero filled in. In connection with the seal the File Trailer also contains the Seal Sum, see below).

Compulsory information is in extra bold type. Other information is not essential but can if specified improve the handling related to file transmission.

A data forwarding agent must always specify the origin in the address fields (%020).

**Transmission header**

| Position | Content |
|---|---|
| 1–4 | **%001** |
| 5–14 | **Delivering node**. (Node ID.) |
| 15–20 | **Password.** (Is NOT specified for SNI or TCP/IP transfer.) |
| 21 | **0 (zero)**. Indicates delivery. |
| 22–24 | File type. |
| 25–30 | **External reference**. Dates must be specified as yymmdd. |
| 31 | Free field for e.g. sending number during the day. |
| 32 | **0** (zero). |
| 33–80 | Reserve/Blank. |

**File header**

An address post for each application file.

| Position | Content |
|---|---|
| 1–4 | **%020** |
| 5–14 | **Destination node**. |
| 15–24 | **Source node**. |
| 25–31 | **External reference 1**. Production date must always be stated. The date must always be stated in connection with Seal.) |
| 32–38 | **Number of items**. (Stated where possible for allocation of space.) |
| 39–48 | External reference 2. Free text field, e.g. where customer number is stated. |
| 49–80 | Reserve/Blank. |

**File trailer**

| | |
|---|---|
| 1–4 | **%022** |
| 5-11 | Number of records in file (Fantom records excluded), right justified “0” padded. |
| 12-43 | **KVV for key used, 128 bits, presented as 32 hexadecimal digits.** |
| 44-75 | **MAC for the file, 128 bits, presented as 32 hexadecimal digits.** |
| 76-80 | Blank/reserve |

**Transmission Trailer**

| Position | Content |
|---|---|
| 1–4 | **%002** |
| 5–80 | Reserve/Blank. |

Nexus seal
This layout in the %22 record applies for the Nexus Seal.

| | |
|---|---|
| 1–4 | **%022** |
| 5–11 | Number of itemns (Right-aligned zero-filled in.) |
| 12–36 | **Seal sum**. (Nexus Electronic Seal) |
| 37–80 | Reserv/Blankt. |

## 10.1 Example of test file to Invoice payment service with Seal

```
%001TCP1234567 001P0082700
%020FS-T 0123456789090105 A9999
0A99990310231
2A9999 99999999 TESTBOLAGET AB TESTVÄGEN 1 TEL
08-123456 SEKSEK
53 SEK 11111FAKTURA1 00000010000031023VÅR
REFERENS 12345
53 SEK 222222FAKTURA2 00000020000031023VÅR
REFERENS 23456
53 SEK 3333333FAKTURA3 00000030000031023VÅR
REFERENS 33333
63 SEK 3333333KREDITFAKT3
000000500000031023041023VÅR REFERENS
43 444444MEDDELANDERAD1
MEDDELANDERAD2
43 444444MEDDELANDERAD3
MEDDELANDERAD4
53 SEK 444444FAKTURA4 00000040000031027VÅR
REFERENS 45678
34 1234567 TESTMOTTAGARE 1
5555555
54 SEK 1234567FAKTURA5 00000050000031024VÅR
REFERENS 56478
34 2345678 TESTMOTTAGARE 2 9960
2287240
54 SEK 2345678FAKTURA6 00000060000031024VÅR
```

```
REFERENS 67890
7A9999 99999999 000000160000+
SEKSEK
%022000001401234567890123456789012345678900123456789012345678901234567890
12
%002
```

(**NB!** The source node and delivery node are unique for each customer/Service office and is administered by PlusGirot. )

# 11 File types

## 11.1 PlusGiro service

| Plusgiro service | Send/Get | File type. | Destination node prod | Destination node test |
|---|---|---|---|---|
| Autogiro, in-delivery of payment instruction | Send | A05 | NAG | NAG-T |
| Autogiro, updating of payment information | Send and get/receive | A01 | NAG | NAG-T |
| Autogiro, booked payment instructions | Get/receive | A04 | | |
| Dok Tolk, IS format | Get/receive | 11P | | |
| Dok Tolk, TIPS format | Get/receive | 11T | | |
| Dok Tolk, picture format | Get/receive | 11B | | |
| e-invoice Company | Send | EFV | PFVXL | |
| Invoice payment service | Send | 01P | FS | FS-T |
| Invoice payment service foreign countries | Send | 01P | | |
| Invoice payment service, back reporting | Get/receive | 12P | | |
| Invoicing service | Send | 08P | FT | FT-T |
| GiroDirekt | Send | PO1 | GIRODIREKT | |
| GiroDirekt/GiroVision booked payments | Get/receive | DA1 | | |
| GiroDirekt/GiroVision preliminarily booked payments | Get/receive | DA2 | | |
| GiroDirekt error payments | Get/receive | POR | | |
| Inpayment service | Get/receive | 02P | | |
| Account statement in data media | Get/receive | FS1 | | |
| Crediting notification | Get/receive | CR1 | | |
| Nordic OCR Danmark | Get/receive | 11D | | |
| Nordic OCR Finland | Get/receive | 11F | | |
| Nordic OCR Norway | Get/receive | 11N | | |
| Nordic OCR Estonia | Get/receive | 11E | | |
| Nordic OCR Latvia | Get/receive | 11L | | |
| T.I.P.S | Get/receive | 24P | | |
| Exchange rates | Get/receive | VK1 | | |
| Out-payment service | Send | 03P | US | US-T |
| Total In | Get/receive | TI1 | | |

## 11.2 Nordea service

| **Nordea service** | **Send/Get** | **File type.** | **Destination node prod** | **Destination node test** |
|---|---|---|---|---|
| Electronic account statement | Get/receive | EKK | | |
| MT940 | Get/receive | 940 | | |
| e-invoice Company | Send and Get/receive | NSX | | |
| Interpay | Send | NBU | INTERPAY | INTERPAY-T |
| Interpay back reporting | Get/receive | | | |
| Salaries via personal account system (LON) | Send | LON | NBFSL | NBFSLTEST |
| Deduction receiver Salaries via personal account system (LON) | Get/receive | AVD | | |
| Salaries via personal account system (PKO format) | Send | 06P | PERSONK | PERSONK-T |
| Treasury files | Send | TF1 | PAYOUT | PAYOUT TEST |

## 11.3 Bankgiro service

| Bankgiro service | Send/Get | File type. | Destination node prod | Destination node test |
|---|---|---|---|---|
| Autogiro Corporate/Private | Send | BG4 | 8502000149 | AG TESTS |
| Autogiro accounting | Get/receive | BG4 | | |
| Autogiro consent, Private and Corporate | Send | BGM | 8502000149 | AG TESTS |
| Autogiro consent advice | Get/receive | BGM | | |
| Autogiro consent register | Get/receive | BMR | | |
| Autogiro electronic consent | Get/receive | BGE | | |
| Automatic ticking off LM | Get/receive | BGT | | |
| Bankgiro In-payments, text file | Get/receive | BGX | | |
| Bankgiro In-payment, picture file | Get/receive | BGB | | |
| GI+ | Get/receive | BGP | | |
| Suppliers’ payments | Send | LBR | 8502000149 | LBR TESTS |
| Supplier’ payments rejected | Get/receive | LBA | | |
| Supplier’ payments international | Send | LBU | 8502000149 | LBR TESTS |
| Supplier’ payments back reporting | Get/receive | LBR | | |
| Salaries CI/salary | Send | BGL | 8502000149 | LON TESTS |
| OCR | Get/receive | BGO | | |

# 12 Appendices

Constitutes appendix **to Girolink Internet and other communication methods**

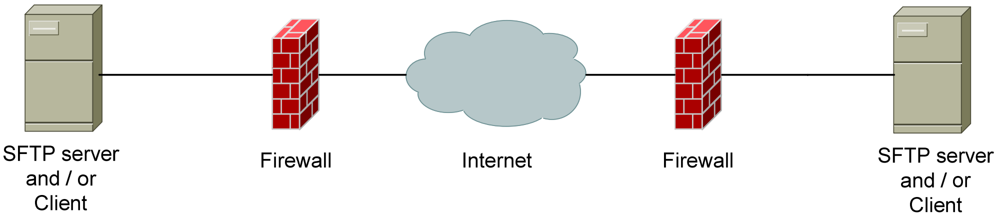
## SFTP

**SFTP (SSH File Transfer Protocol** ) is a network protocol that provides secure file transfers.

SFTP is based on the SSH protocol and is not the same as FTPS which is based on FTP and SSL. Nordea does not currently support FTPS.

**What is needed?**
No hardware is required but the sender needs a SFTP client and the receiver a SFTP Server. The sender must generate a SSH2/DSA key pair for authentication of the connection.

**Technical information**
The SFTP communication is routed over public Internet using static public IP address on both sides. No addresses from the private address space (RFC 1918) can be used.



Outline showing point-to-point communication with SFTP.

During the setup IP addresses, filenames and public DSA keys are exchanged.

**File to Nordea**
Each file is assigned a unique file name with a unique timestamp for each new file.

- The user creates a file in the local system
- The file can be sealed using HMAC
- File is transferred to Nordea with SFTP by specifying user name, authentication key and destination file name.
- Nordea processes the file.

**File from Nordea**
Nordea logs on to the SFTP server at the customer side using user name and authentication key, and sends the file to the SFTP server with the agreed filename.

**Characters**
All files are sent as binary files. In order to avoid character problems the files must be represented according to ISO 8859-1 before sending. If another Character table is used that should be specified to Nordea.

**File size**
Maximum file size that can be received is 200 MB. If more space is required this should be specified to Nordea.

**Record format /Record length**
Depending on the service/file type this must be checked by the customer when creating the file.

**SFTP commands**
PUT [local filename] [Nordea filename.<TIMESTAMP>] . – Sends the file
MPUT [*]. – Sending multiple files.
DIR – List the files within the directory.

Note: GET is not allowed. It is always the sending part that initiates a file transfer.

**Filenames**
The filename syntax for files to Nordea is normally built in four parts and look like this:
PDGSX.USERID.FILTYPE.<TIMESTAMP>
Timestamp is not done by command. The timestamp is a part of the filename and the default syntax is “YYYY-MM-DD-HH.MM.SS.NNNNNN”. The timestamp must be unique for each new transfer and may consist of any sequence of digits, dashes and dots up to 26 characters.

Ex PDGSX.XTCPXXX.F01P.2009-09-25-13.30.45.141516

**Example of SFTP script**
CD in
PUT [local filename] [Nordea filename.<TIMESTAMP>]

**Tests**
The following tests must be conducted once the connection are established:

- **SFTP**
  The customer and/or Nordea verify that it is possible to log on to the receiving side with the authentication key.

- **Files headers and trailers**
  A test file is sent to Nordea and in this way the file headers and trailers are also tested.

- The files are sent to a test node, which is specified as a destination node in the file headers and trailers, see chapter 10 – 11 in “GiroLink and other communication methods”. The test varies according to the service in question.

## VPN via Internet – FTP

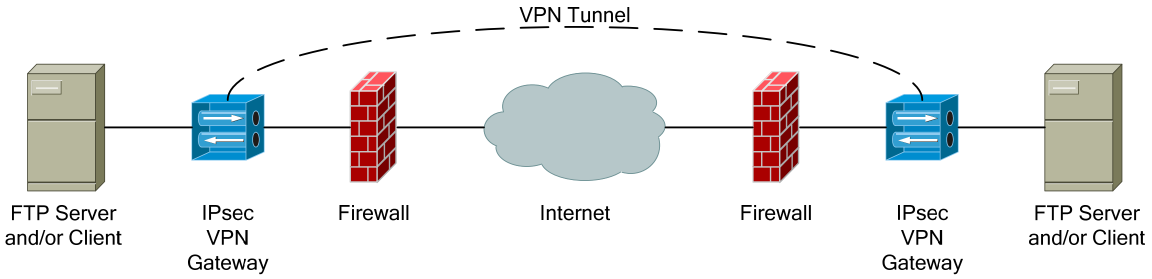
VPN (Virtual Private Network) is a method for establishing a secure point-to-point communication over the Internet. A so-called VPN tunnel is established between the end points and this tunnel transfers encrypted information.

### What is needed?

To establish a VPN tunnel necessitates that both end points use the same VPN protocol. PlusGirot uses IPsec VPN. There are solutions for establishing VPN in both hardware and software. Many suppliers offer firewalls with a built-in VPN function.

### Technical information

For the communication to be able to function it is required that each VPN Gateway has a public IP address that is routed over the Internet and also that the file server has a registered public address. This is to prevent the risk of IP conflicts. *This means that no addresses from the private address space (RFC 1918) may be used!*



Outline showing point-to-point communication with IPsec VPN.

The settings required to establish VPN are agreed between the parties in a way that ensures that the equipment at both ends of the tunnel uses the same methods for encryption, authentication etc.

A shared key is currently used for authentication (pre-shared secret). A certification requirement for authentication will however be introduced.

### File to PlusGirot

Each file is assigned a unique file name using a generation index (+1)a, which explains how several files of the same type can be sent on the same day.

- The user creates a pay file in his/her system
- The pay file is Mac-code protected
- The VPN tunnel is set up at PlusGirot
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

### File from PlusGirot

PlusGirot can assign a unique file name in the customer’s system through the command ’store unique’ or add date and time variables ’timestamp’. Store unique requires the function to be activated at the customer’s end.

**Character conversion**
All characters are presented in upper-case (EBCDIC) irrespective of whether lower-case letters are used. In cases where character translation becomes a problem e.g. if national characters such as åä and ö are erroneous the following site command is used:

```
SITE SBD=(IBM-278,ISO8859-1)
```

In these cases files are sent from an EBCDIC environment and the file will go as a binary file:

```
SITE TYPE=IMAGE or SITE TYPE=BINARY
```

**File size**
Max. file size that can be received is 300 cyl, approx. 210 MB. If more space is required this should be specified with site command:

```
SITE PRI=nnnn                          nnnn=file size in cylinders
```

**Record format /Record length**
Depending on the service/file type this must be specified from the customer in the file transfer with SITE command:

```
SITE RECFM=FB LRECL=80
```

If the customer' ftp client does not support the site command the quote command can be used:

```
QUOTE SITE
```

**Example of ftp script**

```
FTP Nordea
USER ID
PASSWORD
QUOTE SITE recfm=fb lrecl=80 pri=500 sbd=(ibm-278,iso8859-1)
PUT <lokalt filnamn> ’Nordea filnamn’
```

**NB!** PlusGirot’s file name must normally be enclosed by ’. Depedning on OS and character translation it is sometimes required to replace ’ with ”.

**Tests**
The following tests must be conducted once the tunnel is established:

- **VPN**
  The customer or PlusGirot can by using its equipment test that the tunnel has the correct configuration and that it functions.

- **FTP**
  The customer or PlusGirot logs on with the user name, password and tests in this way that there is access to the respective server. This ensures that both the tunnel and FTP is tested.

- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See user instruction for the respective service: www.plusgirot.se /Företag

.Constitutes appendix **to Girolink Internet and other communication methods**

## VPN via Internet – Connect:Direct

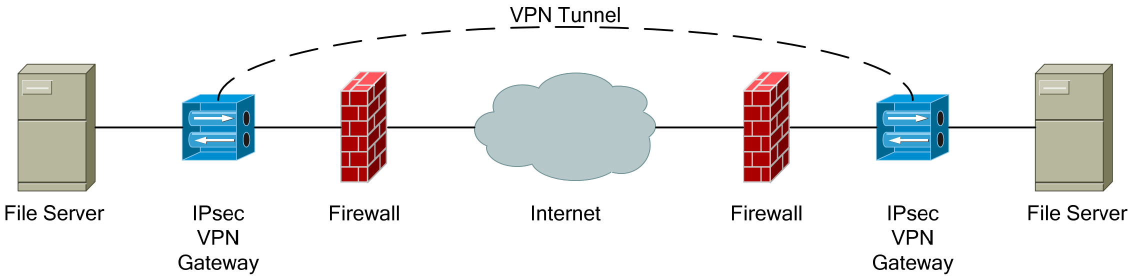
VPN (Virtual Private Network) is a method for establishing a secure point-to-point communication over the Internet. A so-called VPN tunnel is established between the end points and this tunnel transfers encrypted information.

### What is needed?

To establish a VPN tunnel necessitates that both end points use the same VPN protocol. PlusGirot uses IPsec VPN. There are solutions for establishing VPN in both hardware or software. Many suppliers offer firewalls with a built-in VPN function.

### Technical information

For the communication to be able to function it is required that each VPN Gateway has a public IP address that is routed over the Internet and also that the file server has a registered public address. This is to prevent the risk of IP conflicts. *This means that no addresses from the private address space (RFC 1918) may be used!*



Outline showing point-to-point communication with IPsec VPN over the Internet.

The settings required to establish VPN are agreed between the parties in a way that ensures that the equipment at both ends of the tunnel uses the same methods for encryption, authentication etc.

A shared key is currently used for authentication (pre-shared secret). A certification requirement for authentication will however be introduced.

**File to PlusGirot**

- The user creates a  file in his/her system
- The pay file is protected with a seal
- The VPN tunnel is set up at PlusGirot
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

**A requirement for receiving files from PlusGirot once the tunnel is established**

- Your Connect:Direct node name
- User name and password in your Connect:Direct environment
- File name

**File to PlusGirot - example**

```
SUBMIT PROC=COPYPG
SNODE=CDFW(Plusgiro node name)
SNODEID=(user name, password)
&NODE=PNODE
&DSNLOC = local file name
&DSNPG=(PDGSX.user name.F>filtyp>(+1)
&DISP=(,CATLG)
```

Control block information or DCB information that is to be sent is dependent on the service in question and must be sent by Connect:Direct transfer

Example

```
&DCB=(BLKSIZE=23440,LRECL=100,RECFM=FB)
```

**Tests**

The following tests must be conducted once the tunnel is established:

- **VPN**
  The customer or PlusGirot can by using its equipment test that the tunnel has the correct configuration and that it functions.

- **Connect:Direct**
  The customer or PlusGirot logs on with the user name, password and tests in this way that there is access to the respective server. This ensures that both the tunnel and Connect:Direct is tested.

- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- **Seal**
  A test file is sent to PlusGirot that is protected with test key. See the technical specification for HMAC.  The Seal sum must be specified in %022 post.

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See the user instruction for the respective service at www.plusgirot.se /Företag.

Constitutes appendix **to Girolink Internet and other communication methods**

## VPN via fixed connection – FTP

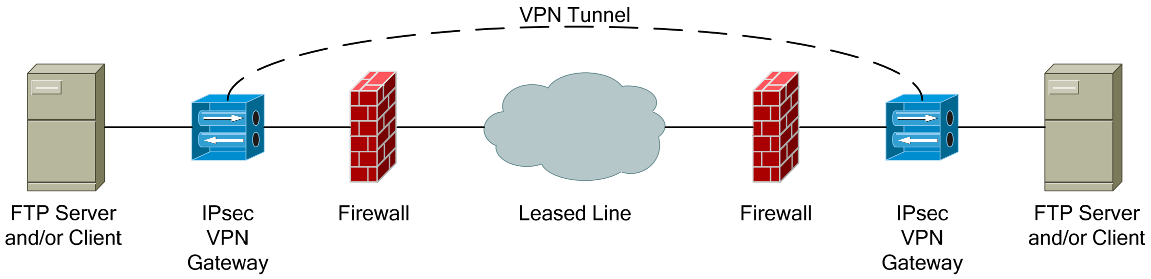
VPN (Virtual Private Network) is a method for establishing a secure point-to-point communication over the Internet. A so-called VPN tunnel is established between the end points and this tunnel transfers encrypted information.

### What is needed?

A link net is used in order for the communication to function over a fixed connection. Nordea can assign addresses to a link net from so-called RFC1918 addresses. If this in special circumstances is not suitable, it is possible for one of the customer's own registered public addresses to be used.

To establish a VPN tunnel necessitates that both end points use the same VPN protocol. PlusGirot uses IPsec VPN. There are solutions for establishing VPN in both hardware and software. Many suppliers offer firewalls with a built-in VPN function.

### Technical information



Outline showing point-to-point communication with IPsec VPN over a fixed connection.

The settings required to establish VPN are agreed between the parties in a way that ensures that the equipment at both ends of the tunnel uses the same methods for encryption, authentication etc.

A shared key is currently used for authentication (pre-shared secret). A certification requirement for authentication will however be introduced.

### File to PlusGirot

- The user creates a pay file in his/her system
- The file is protected with a Seal
- The VPN tunnel is set up at PlusGirot
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

PlusGirot can assign a unique file name in the customer's system through the command 'store unique' or add date and time variables 'timestamp'. Store unique requires the function to be activated at the customer's end.

### Character conversion

All names are presented in upper-case (EBCDIC) irrespective of whether lower-case letters are used. In cases where character translation becomes a problem e.g. if national characters such as åä and ö are erroneous the following site command is used:

```
SITE SBD=(IBM-278,ISO8859-1)
```

In these cases files are sent from an EBCDIC environment and the file will go as a binary file:

```
SITE TYPE=IMAGE or SITE TYPE=BINARY
```

### File size

Max. file size that can be received is 300 cyl, approx. 210 MB. If more space is required this should be specified with site command:

```
SITE PRI=nnnn                    nnnn=file size in cylinders
```

### Record format /Record length

Depending on the service/file type this must be specified from the customer in the file transfer with SITE command:

```
SITE RECFM=FB LRECL=80
```

If the customer' ftp client does not support the site command the quote command can be used:

```
QUOTE SITE
```

### Example of ftp script

```
FTP Nordea
USER ID
PASSWORD
QUOTE SITE recfm=fb lrecl=80 pri=500 sbd=(ibm-278,iso8859-1)
PUT <lokalt filnamn> 'Nordea filnamn'
```

**NB!** PlusGirot's file name must normally be enclosed by '. Depedning on OS and character translation it is sometimes required to replace ' with ".

### Tests

The following tests must be conducted once the tunnel is established:

- **VPN**
  The customer or PlusGirot can by using its equipment test that the tunnel has the correct configuration and that it functions.

- **FTP**
  The customer or PlusGirot logs on with user and password and in this way test that there is access to the respective server. This ensures that both the tunnel and FTP is tested.

- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- **Seal**
  A test file that is protected with  test key is sent to PlusGirot. See section 9.2. The Mac-code sum must be specified in %022 pos. 12-36. (Mac-code)

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See the user instruction for the respective service at www.plusgirot.se /Företag.

Constitutes appendix **to Girolink Internet and other communication methods**

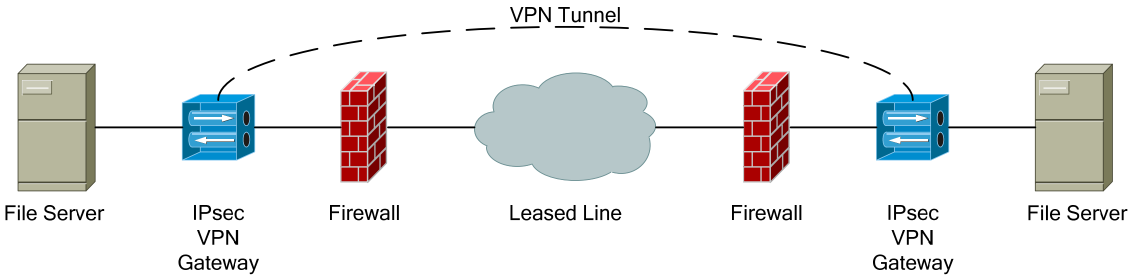
## VPN via fixed connection – Connect:Direct

VPN (Virtual Private Network) is a method for establishing a secure point-to-point communication over the Internet. A so-called VPN tunnel is established between the end points and this tunnel transfers encrypted information.

**What is needed?**
A link net is used in order for the communication to function over a fixed connection. Nordea can assign addresses to a link net from so-called RFC1918 addresses. If this in special circumstances is not suitable, it is possible for one of the customer's own registered public addresses to be used.

To establish a VPN tunnel necessitates that both end points use the same VPN protocol. PlusGirot uses IPsec VPN. There are solutions for establishing VPN in both hardware and software. Many suppliers offer firewalls with a built-in VPN function.

### Technical information



Outline showing point-to-point communication with IPsec VPN over a fixed connection.

The settings required to establish VPN are agreed between the parties in a way that ensures that the equipment at both ends of the tunnel uses the same methods for encryption, authentication etc.

A shared key is currently used for authentication (pre-shared secret). A certification requirement for authentication will however be introduced.

### File to PlusGirot

- The user creates a pay file in his/her system
- The pay file is Mac-code protected
- The VPN tunnel is set up at PlusGirot
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

**Requirements receiving files from PlusGirot**

- Your Connect:Direct node name
- User name and password in your Connect:Direct environment
- File name
- IP address

**File to PlusGirot - example**

```
SUBMIT PROC=COPYPG
SNODE=CDFW(Plusgiro node name)
SNODEID=(user name, password)
&NODE=PNODE
&DSNLOC = local file name
&DSNPG=(PDGSX.user name.F>filtyp>(+1)
&DISP=(,CATLG)
```

Control block information or DCB information that is to be sent is dependent on the service in question and must be sent by Connect:Direct transfer

Example

```
&DCB=(BLKSIZE=23440,LRECL=100,RECFM=FB)
```

**Tests**

The following tests must be done.

- **VPN**
  The customer or PlusGirot can by using its equipment test that the tunnel has the correct configuration and that it functions.

- **Connect:Direct**
  The customer or PlusGirot logs on with user and password and in this way test that there is access to the respective server. This ensures that both the tunnel and Connect:Direct is tested.

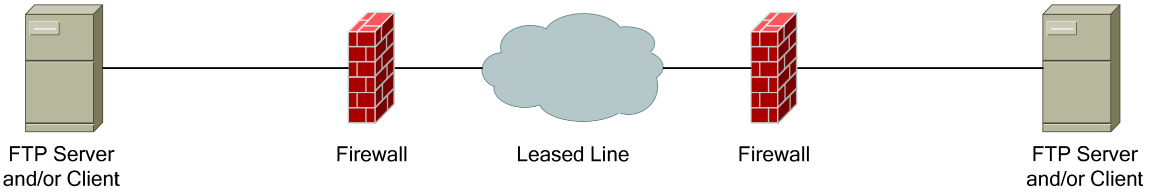
- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See the user instruction for the respective service at www.plusgirot.se /Företag.

Constitutes appendix **to Girolink Internet and other communication methods**

## Fixed connection TCP/IP – FTP

A link net is used in order for the communication to function over a fixed connection. Nordea can assign addresses to a link net from so-called RFC1918 addresses. If this in special circumstances is not suitable, it is possible for one of the customer's own registered public addresses to be used.



Outline showing point-to-point communication over fixed connection.

### File to PlusGirot

- The user creates a pay file in his/her system
- The pay file is Mac-code protected
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

### Files from PlusGirot

PlusGirot can assign a unique file name in the customer's system through the command 'store unique' or add date and time variables 'timestamp'. Store unique requires that the function is activated.

### Character conversion

All names in z/OS are presented in upper-case (EBCDIC) even if lower-case letters are used. In cases where character translation becomes a problem e.g. if national characters such as åä and ö are erroneous the following site command is used:

```
SITE SBD=(IBM-278,ISO8859-1)
```

In these cases files are sent from an EBCDIC environment and the file will go as a binary file:

```
SITE TYPE=IMAGE or SITE TYPE=BINARY
```

**File size**
Max. file size that can be received is 300 cyl, approx. 210 MB. If more space is required this should be specified with site command:

SITE PRI=nnnn nnnn=file size in cylinders

**Record format /Record length**
Depending on the service/file type this must be specified from the customer in the file transfer with SITE command:

SITE RECFM=FB LRECL=80

If the customer' ftp client does not support the site command the quote command can be used:

QUOTE SITE

**Example of ftp script**

```
FTP Nordea
USER ID
PASSWORD
QUOTE SITE recfm=fb lrecl=80 pri=500 sbd=(ibm-278,iso8859-1)
PUT <lokalt filnamn> 'Nordea filnamn'
```

**NB!** PlusGirot's file name must normally be enclosed by '. Depedning on OS and character translation it is sometimes required to replace ' with ".

**Tests**
The following tests must be done.

- **VPN**
  The customer or PlusGirot can by using its equipment test that the tunnel has the correct configuration and that it functions.

- **FTP**
  The customer or PlusGirot logs on with user and password and in this way test that there is access to the respective server. This ensures that both the tunnel and FTP is tested.

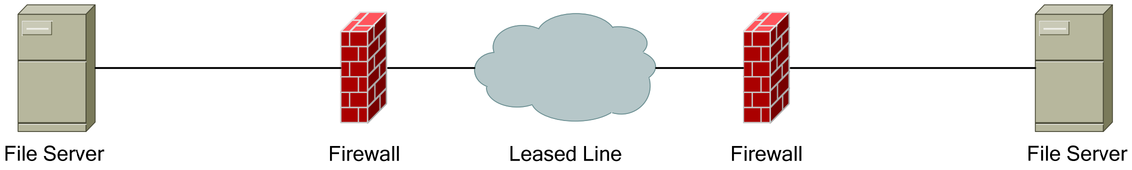
- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See user instruction for the respective service: www.plusgirot.se

Constitutes appendix **to Girolink Internet and other communication methods**

## Fixed connection TCP/IP – Connect:Direct

A link net is used in order for the communication to function over a fixed connection. Nordea can assign addresses to a link net from so-called RFC1918 addresses. If this in special circumstances is not suitable, it is possible for one of the customer's own registered public addresses to be used.



Outline showing point-to-point communication over fixed connection.

### File to PlusGirot

- The user creates a pay file in his/her system
- The pay file is Mac-code protected
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

### Requirements receiving files from PlusGirot

- Your Connect:Direct node name
- User name and password in your Connect:Direct environment
- File name
- IP address

### File to PlusGirot - example

```
SUBMIT PROC=COPYPG
SNODE=CDFW(Plusgiro node name)
SNODEID=(user name, password)
&NODE=PNODE
&DSNLOC = local file name
&DSNPG=(PDGSX.user name.F>filtyp>(+1)
&DISP=(,CATLG)
```

Control block information or DCB information that is to be sent is dependent on the service in question and must be sent by Connect:Direct transfer

Example

```
&DCB=(BLKSIZE=23440,LRECL=100,RECFM=FB)
```

**Tests**
The following tests must be done.

- **Connect:Direct**
  The customer or PlusGirot logs on with user and password and in this way test that there is access to the respective server. This ensures that both the tunnel and Connect:Direct is tested.

- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See the user instruction for the respective service at www.plusgirot.se

Constitutes appendix **to Girolink Internet and other communication methods**

## Snix IP – FTP

SNIX is a ready solution from TELE 2 that involves:

- Customer-placed equipment
- Own dedicated fixed access line
- Installation and configuration
- Service, support and maintenance
- 24 hour running and monitoring

Encryption and choice of bandwidth is also offered for this service. With a SNIX connection all interested parties in the SNIX network can be reached. The connection therefore replaces the existing lines that previously went between the respective individual connected parties and this also offers the possibility to reach new partners.

### File to PlusGirot

- The user creates a pay file in his/her system
- The pay file is Mac-code protected
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

### Files from PlusGirot

PlusGirot can assign a unique file name in the customer's system through the command 'store unique' or add date and time variables 'timestamp'. Store unique requires that the function is activated.

### Character conversion

All names in z/OS are presented in upper-case (EBCDIC) even if lower-case letters are used. In cases where character translation becomes a problem e.g. if national characters such as åä and ö are erroneous the following site command is used:

```
SITE SBD=(IBM-278,ISO8859-1)
```

In these cases files are sent from an EBCDIC environment and the file will go as a binary file:

SITE TYPE=IMAGE or SITE TYPE=BINARY

**File size**
Max. file size that can be received is 300 cyl, approx. 210 MB. If more space is required this should be specified with site command:

SITE PRI=nnnn nnnn=file size in cylinders

**Record format /Record length**
Depending on the service/file type this must be specified from the customer in the file transfer with SITE command:

SITE RECFM=FB LRECL=80

If the customer' ftp client does not support the site command the quote command can be used:

QUOTE SITE

**Example of ftp script**

```
FTP Nordea
USER ID
PASSWORD
QUOTE SITE recfm=fb lrecl=80 pri=500 sbd=(ibm-278,iso8859-1)
PUT <lokalt filnamn> 'Nordea filnamn'
```

NB! PlusGirot's file name must normally be enclosed by '. Depending on OS and character translation it is sometimes required to replace ' with ".

**Tests**
The following tests must be done.

- **FTP**
  The customer or PlusGirot logs on with user and password and in this way test that there is access to the respective server. This ensures that both the tunnel and FTP is tested.

- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See the user instruction for the respective service at www.plusgirot.se

Constitutes appendix **to Girolink Internet and other communication methods**

## Technical Information - Snix IP – Connect:Direct

SNIX is a ready solution from TELE 2 that involves:

- Customer-placed equipment
- Own dedicated fixed access line
- Installation and configuration
- Service, support and maintenance
- 24 hour running and monitoring

Encryption and choice of bandwidth is also offered for this service. With a SNIX connection all interested parties in the SNIX network can be reached. The connection therefore replaces the existing lines that previously went between the respective individual connected parties and this also offers the possibility to reach new partners.

**File to PlusGirot**

- The user creates a pay file in his/her system
- The pay file is Mac-code protected
- File transfer takes place through the user specifying user name, password and sending the file
- PlusGirot confirms the customer

**Requirements for sending files to PlusGirot**

- Your Connect:Direct node name
- Your IP address
- User name and password set up in PlusGiro environment
- File name pre-allocated in PlusGiro environment
- Authorisations for user to allocate a given file name

**Requirements for receiving files from PlusGirot**

- Your Connect:Direct node name
- User name and password in your Connect:Direct environment
- File name
- IP address

**File to PlusGirot - example**

```
SUBMIT PROC=COPYPG
SNODE=CDFW(Plusgiro node name)
SNODEID=(user name, password)
&NODE=PNODE
&DSNLOC = local file name
&DSNPG=(PDGSX.user name.F>filtyp>(+1)
&DISP=(,CATLG)
```

Control block information or DCB information that is to be sent is dependent on the service in question and must be sent by Connect:Direct transfer

Example

```
&DCB=(BLKSIZE=23440,LRECL=100,RECFM=FB)
```

**Tests**
The following tests must be conducted.

- **Connect:Direct**
  The customer or PlusGirot logs on with user and password and in this way tests that there is access to the respective server. This ensures that both the tunnel and Connect:Direct is tested.

- **Files headers and trailers**
  A test file is sent to PlusGirot and in this way the Files headers and trailers are also tested.

- The files are sent to a test node, which is specified as a destination node in the Files headers and trailers, see sector 13. The test varies according to the service in question. See the user instruction for the respective service at www.plusgirot.se