bankgirot

SFTP (Secure Shell FTP using SSH2 protocol)

Technical Manual

March 2014

1. Table of contents

2. Introduction

This document

This document includes detailed technical information on the communication method SFTP (FTP SSH). This document has been devised for anyone wishing to adapt their system for SFTP.

This document is designed to be read on your PC and all terms mentioned in the factual section and the checklist are linked to chapter 6. Terms and definitions. There are also links to our website.

User help: Click the Previous view page navigation button – or use the Alt + Left Arrow keyboard shortcut – to return to the point in the document where you clicked a term.

What is Bankgirot?

Bankgirot is:
- An open system for both payers and creditors.
- The link between payers and creditors.

All banks operating in Sweden can participate in the bankgiro system. Bankgirot processes payments and information about incoming and outgoing payments for all parties. Payments and information always arrive on time.

Regardless of your bank connection:
- As a payer you can reach all creditors.
- As a creditor you can receive payments from all payers.

Customised payment solutions: Bankgirot offers everything from simple payment solutions for small businesses to automated electronic payment solutions for large enterprises with computerised accounting systems.

Bankgirot has established collaborations with several of the largest business, accounting and communication software companies. Together we create efficient business solutions for all payment needs, saving your business both time and money.

Continued on next page

, Continued

What is a communication method?

A *communication method* is the solution the company uses to send files to and retrieve files from Bankgirot.

Payment messages and reports are sent between your company and Bankgirot by file transfer.. There are several different solutions for communicating with Bankgirot. Information on available communication methods can be found at www.bgc.se, under Om våra tjänster/ Kommunikationslösningar och säkerhet/Bankgirots kommunikationslösningar.

What is SFTP (SSH)?

SFTP (SSH) is a communication method which involves

- secure file transfer between your accounting system and Bankgirot
- tamper protection in conjunction with your system sending a payment to Bankgirot.

SFTP is suitable for companies with large payment volumes and the need to adapt and automate the communication method to their internal payment procedures.

With SFTP files are transferred to Bankgirot over the Internet via an interception-protected channel (SSH between client and server).

What is SSH?

SSH is a technology for creating secure communication between two computers via the Internet using encryption. Nobody other than the people at the computers in question can access the files when they are transferred via the Internet.

The file transfer itself takes place according to FTP.

3. Criteria for SFTP

Agreement with bank

To be able to use and adapt your system for SFTP, your company has to have signed an agreement for a Bankgirot service with the bank. When your company concludes an agreement relating to a Bankgirot service, it also agrees on which communication method it wants to use.

When Bankgirot has registered the agreement, your company will be assigned a customer number at Bankgirot. Bankgirot will then help you to set up a communication link between your company and Bankgirot.

Technical criteria

The table shows which technical criteria are required to be able to connect to SFTP.

Technical criterion	Comment
Accounting information system	–
Internet connection	–
Software for SFTP	
Static and public IP address on an SFTP client or SFTP server	**Note:** It is not possible to use DHCP addresses.
Public key server (SSH)	Public keys are exchanged automatically on the server at the time of first connection
Protocol	SFTP with SSH version 2. Secure Copy (SCP) is not permitted
Software for tamper protection	**Cross-reference:** For more information, see *Tamper protection* below
Public keys, Clients	This is used without they being on the server; see Public key server (SSH) above.

Continued on next page

, continued

Tamper protection

For security reasons, the company must tamper-protect *all* files sent to Bankgirot.

To protect a file from tampering means that the file is protected from unauthorised alteration during transport. The file is assigned an encrypted check record (condensate) calculated based on the file's content and a unique code, before the file is sent to Bankgirot. Bankgirot checks the check record and can thereby confirm that the file has not been tampered with after the sender authenticated it. Tamper protection verifies that the instruction comes from the right sender.

In conjunction with your company signing an agreement with the bank on a Bankgirot service you will receive authentication keys for tamper protection from Bankgirot or your bank. You will also receive a password from Bankgirot.

Cross-reference: More information on tamper protection is available in the technical manual for Tamper protection. This is available to download from the Bankgirot website, www.bankgirot.se, under Om våra tjänster/Blanketter, manualer och trycksaker.

4. Preparations for connecting to SFTP

Technical information required by Bankgirot

When the company has signed an agreement with the bank, Bankgirot will contact the company's technical contact in order to get technical information. This information is needed so that Bankgirot can connect your company to FTPS.

Bankgirot needs the following information:

- IP address of the company's
  - SFTP client
  - SFTP server
- username and password for the company's SFTP server
- the required recipient filename for deliveries from Bankgirot.

Note: It is important for you to be prepared to give the above information to Bankgirot as soon as the agreement has been signed.

Technical information from Bankgirot

When Bankgirot has connected your company to SFTP, the company will receive the technical information required to allow you to adapt your system for SFTP.

The table shows which information the company will receive from Bankgirot.

Technical information	Comment
Username at Bankgirot	Used to log in to the Bankgirot SFTP server.
Bankgirot's IP addresses	Used to be able to link up to Bankgirot's SFTP server.
Data set names for testing and production	See the data set name principles in Section 5.2

5. Adapting your system for SFTP

5.1 Settings relating to encryption

Settings

The following settings are required for you to be able to use encryption:

- Encryption AES-256
- Hashing algorithm: SHA1
- Public key: SSH-RSA, key length 2048

Keys are exchanged automatically at the time of first connection

5.2 Settings relating to file format

Character encoding standard

Files to Bankgirot must be in ASCII format with the character set ISO8859-1 (Latin-1)

Files from Bankgirot in ASCII format with the character set ISO8859-1 (Latin-1) are terminated with Line Feed (LF=0x0A)

Principles for data set names

The data set name of files *from* Bankgirot includes the customer or service bureau number together with the time and date the file was created.

Files *to* Bankgirot must have a data set name according to the structure BFEP.Ixxxx.K0nnnnnn, where xxxx is replaced with a product code and nnnn is replaced with a customer number (right-justified and completed with zeroes).

Example: The table shows examples of product codes for some of the various Bankgirot services.

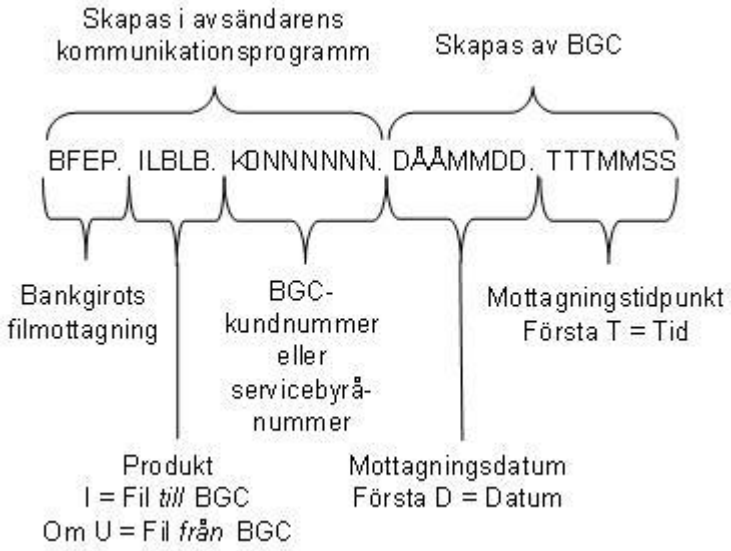
Bankgirot service	Code for production	Code for testing
Autogiro (direct debit)	IAGAG	IAGZZ
Supplier payments	ILBLB	ILBZZ
Salaries/Account deposits	IKIKI	IKIZZ

Continued on next page

, Continued

Data set name fields

This diagram presents the different fields in the data set name.



5.3 Settings relating to file transfer *to* Bankgirot

Bankgirot does *not* accept empty files

Bankgirot does *not* accept empty files, i.e. files which contain no transactions.

Several files can be sent on the same day

All files received or sent in Bankgirot's system are automatically given a unique file name with the help of a generation data set. This means that several files can be sent on the same day with no risk of date being overwritten.

Dialog when sending files

The Bankgirot SFTP server is set up with a special feature in order to enhance security for your data. You cannot connect to the server using any protocol other than SFTP (e.g. SCP or Telnet).

This is the structure of the dialog when sending files to Bankgirot:

SFTP <*login*>@sftp.bankgirot.se *(<login> = the company's user name at Bankgirot)*

Password: <*password*>

PUT local_filename //BFEP.Ixxxx.K0nnnnnn

Or

PUT local_filename /-/BFEP.Ixxxx.K0nnnnnn

QUIT

The file name at Bankgirot must begin with // or /-/ as the file is created in the system's directory, not the user's directory.

Commands for record length and file size

The table shows which commands are applicable depending on record length and file size when sending files to Bankgirot.

Record length/file size	Command	Comment
Files with a record length of max. 768 characters	–	If a longer record length is required, contact Bankgirot.
Files more than approx. 150 MB in size (the file size which can normally be sent)	SITE PRI=nnnn	nnnn = file size in MB x 20

Continued on next page

, continued

Character conversion when sending files	Files are saved at Bankgirot in EBCDIC format. Translation takes place between 8-bit ASCII (ISO8859-1) and EBCDIC Finnish/Swedish Code Page (1143).

5.4 File transfer *from* Bankgirot

Sending files

Bankgirot automatically sends files to the company when there is data ready to send in Bankgirot's system. The file is left in a preagreed location in your company's system. In other words, it is not possible to download files from Bankgirot.

Bankgirot uses Line Feed (LF) as a line break character when sending files from Bankgirot (LF =0X0A).

Note: For your company to be able to receive files, your business system has to be prepared for receipt.

Several files can be sent on the same day

All files received or sent in Bankgirot's system are automatically given a unique file name with the help of a generation data set. This means that several files can be sent on the same day with no risk of date being overwritten.

Company-unique file names with Store Unique

Bankgirot uses the Store Unique command to create a file name which is unique to your company. However, for this the function has to be enabled in your company's data system.

5.5 Testing

How it works

To check that the file transfer to Bankgirot is working and that the files you created in your business system or accounting system are correct, you can carry out a test at Bankgirot, which will notify you of the test results as soon as possible.

The table shows how a test works.

Step	Description
1	Your company creates a tamper-protected file containing authentic data.
2	Your company connects to Bankgirot according to an agreed communication method and sends the file to Bankgirot as a test file.
3	Bankgirot or the bank (if testing international payments) sends confirmation of a successful test.

Tip: To create your own files you can also use the sample files available at www.bankgirot.se, under Om våra tjänster and the relevant service.

Test file

The test file must include authentic data which you create in your company's payment software, i.e. payment jobs containing correct customer details (such as the real bankgiro number). The payments in the test file will not be actioned.

Note: Check that your company's details are recorded in your payment software before you create the test file, as these details will be checked during the test run.

Cross-reference: For more information on how to create test data in your business suite or accounting system, refer to the software documentation for your system or contact your software supplier.

Tamper protection during testing

The tamper protection must use a test key. When the test is passed, you can register a production key for tamper protection with a start date in your authentication software. **Note:** It is not possible to implement authentication for a file created with a date older than the date on which the authentication key is added.

6. Terms and definitions

Terms in this document This table lists Bankgirot's definitions of terms associated with the SFTP communication method.

Term	Definition
Bankgiro number	An address that points to a bank account. A bankgiro number can be associated with the bank and account number of your choice.
Payment instructions	The payments Bankgirot accepts and processes.
Data set name	The data set name is the technical name of all files sent to and from Bankgirot. It is generated from the customer number or service bureau number, the date and the time.
DHCP	Dynamic Host Configuration Protocol. A network protocol which permits automatic allocation of temporary IP addresses.
Tamper protection	To protect a file from tampering means that the file is protected from unauthorised alteration during transport. Tamper protection verifies that the instruction comes from the right sender.
SFTP	SFTP (Secure Shell File Transfer Protocol) A communication protocol which uses SSH to send encrypted files via the Internet.
SFTP client	Software on a sending computer which starts an SFTP session.
SFTP server	Software on a receiving computer which responds to calls from an SFTP client.
IP address	A numerical address used for computers.
Communication method	The method a company uses to send files to and retrieve files from Bankgirot.
Customer number	A customer number at Bankgirot used as the address for file deliveries. A company can have one or more bankgiro numbers linked to it. A customer number is always linked to a service.
Server certificate	A type of electronic identification.
Authentication key	A combination of digits and code which, together with an encryption algorithm, locks the check record for anyone without access to the key.
TCP/IP	Transmission Control Protocol/Internet Protocol. A general file transfer standard using different data networks, such as the Internet. TCP/IP is a collection of several different protocols. It is included in all Unix systems and is available for most computers (from PCs to IBM mainframes).
Technical Manual	A user guide with record and file descriptions. Mainly aimed at software companies and companies that develop proprietary software.
Testing	Conducted to verify that the information in the files complies with the specified layout.
Reporting	All companies receive reports on executed, unexecuted and monitored payments. Reporting comprises a number of reports that can be received on file and/or paper. The company can choose how often the reports are sent.