BusinessNet Connect
Integration manual
UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky

March 2026

UniCredit Bank

Introduction

Dear Client,

The integration of corporate systems with banking systems is becoming an increasingly frequent topic not only for the largest companies with tens of thousands of payments every year but also for the small ones selling goods and services online.

We are pleased that you have chosen our BusinessNet Connect product for your solutions. This Manual will help you correctly set the interconnection of systems.

If you have questions do not hesitate to contact our technical support.

Email: eb@unicreditgroup.sk

Telephone number: +421 2 6920 2097 (working days, 8:00 – 16:30)

UniCredit Bank Czech Republic and Slovakia, a.s., pobočka zahraničnej banky

CONTENTS

GLOSSARY

BusinessNet Connect
BusinessNet Connect is a service of the bank for exchanging files between the client and the bank by means of the WebDAV protocol. It allows downloading statements and uploading payment instructions. Communication is secured, uses certificates, and enables automation, see Chapter 5.

WebDAV
The technology used for the BusinessNet Connect service. It is a standardized extension of the https protocol allowing remote file management on a web server. The advantage is native support for the protocol in operating systems.

Technical user
A user profile is intended only for the work with the BusinessNet Connect product. The user is not intended for common work in BusinessNet Professional internet banking.

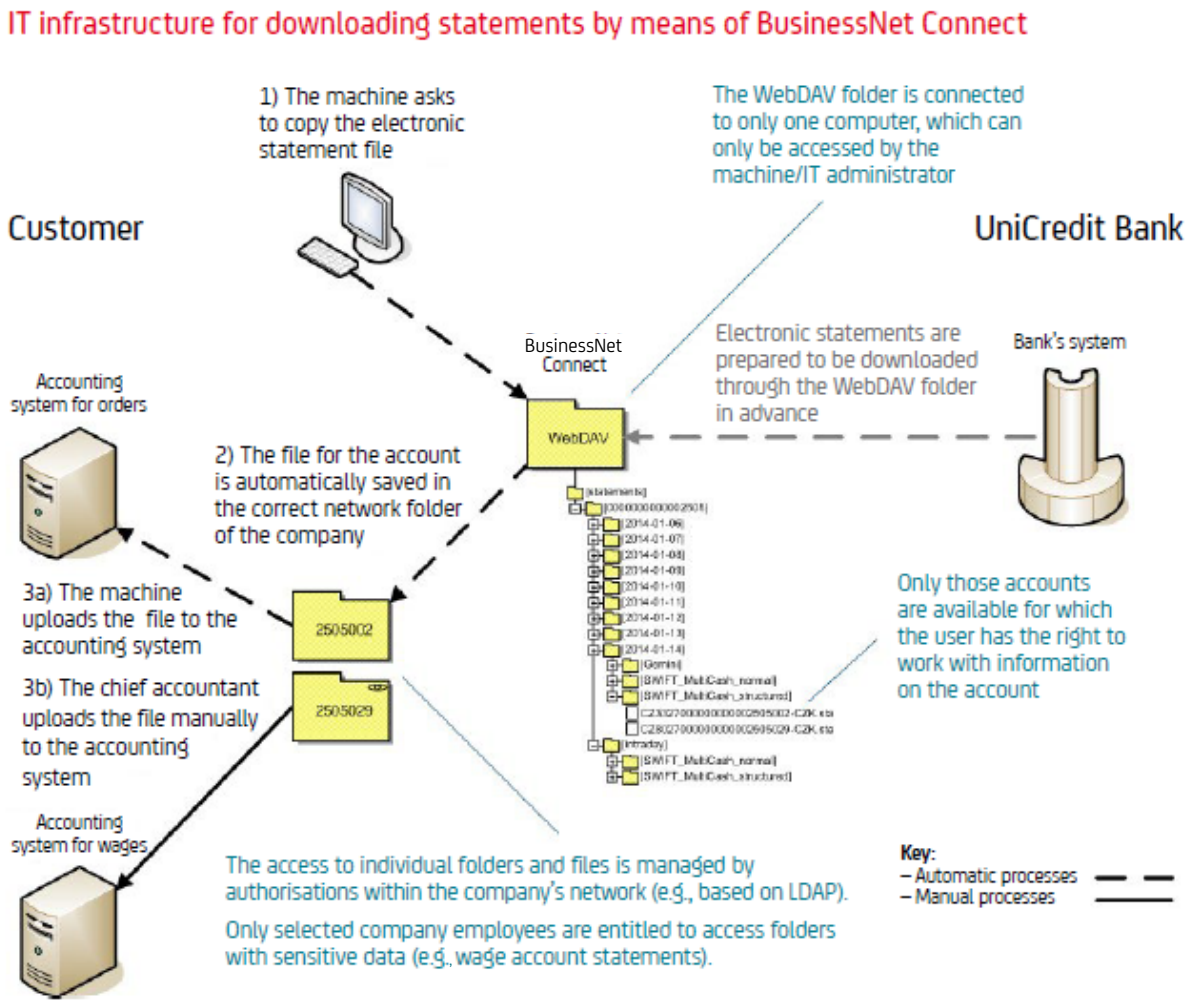
Password for telephone communication
This is a password serving as secondary identification of the client during telephone communication with the technical support for electronic banking (for example, to unblock a blocked userID). Modifications and setting of the password are supported by your banker.

1. BEFORE YOU START

1.1 Access rights concept

Only an automated process or one person, who will download files from or upload files into a local folder, should be able to access the WebDAV folder. The access to local files should be managed at the level of corporate authorisations – for example, by means of Active Directory / LDAP, which is administered by the company's administrators based on internal processes of the company. Once a file has been saved locally, the bank has no means to help with control of access rights. Thus, **think twice who should have access to these local files** (e.g., to statements containing wage data or other sensitive data).

The direct access to the WebDAV folder **should never be shared!**



« back to content

1.2 Automation level

The level of automation is mostly determined by internal processes of the company. BusinessNet Connect offers a possibility of full automation of the processes. In such case, a command line interface along with automatically scheduled jobs should be used for file uploading and downloading, encryption, decryption, and file signatures. Before starting the integration, think about **which processes should be automated**.

E.g., BusinessNet Connect would be used for downloading MT942 statements (with intraday movements) which are then imported into the accounting system. To import a payment file with invoices on a monthly basis, the traditional BusinessNet Professional would be sufficient (manual import using an internet browser).

Condider the following aspects:

- Is the action needed frequently (e.g., statement should be downloaded every 5 minutes)? Use BusinessNet Connect...
- Is an early response decisive for the action (e.g., should payment be sent within 5 minutes after the invoice generation)? Use BusinessNet Connect...
- Does an internal company process forbid human operator to touch the payment file (e.g., payment file must be delivered to bank directly from ERP system)? Use BusinessNet Connect...

But:

- Do you need to authorise payments by several people and the accounting system does not support multilevel signature authorisations? Use BusinessNet Professional to sign transactions...

1.3 Non-standard situations handling

During the integration, we **recommend** setting up internal company processes for cases when the WebDAV folder is not available (e.g., due to a scheduled internet banking outage).

Within these measures, we recommend the following settings:

- service availability monitoring
- automatic messages on service unavailability – e.g., by e-mail to the IT system administrator
- a process (manual or automated) for reconnection to the WebDAV folder

1.4 Certificates

To increase the security of your connection to the BusinessNet Connect service, you can optionally use a certificate with which the bank will verify your login data. If you want to use a certificate to verify your login data please inform your banker.

Supported certificates and certification authorities

If you already use a certificate and you would like to only extend its use for UniCredit Bank, it must be supported by us. The following certification authorities are accepted for BusinessNet Connect:

- **Actalis** (https://www.actalis.com)
- **1. certifikační** (https://www.ica.cz/)
- **Česká pošta, s.p.** (https://www.postsignum.cz)
- **EIdentity** (https://www.eidentity.cz)

If you do not use similar certificates yet, we recommend using an S/MIME-type certificate from the Actalis certification authority (Italy) which provides certificates with a validity period of one year and with the possibility of subsequent extension FOR FREE. This certificate is suitable for certification when connecting to the WebDAV folder. See below how to download and install it.

Certificate expiry

The period of validity of certificates is limited to one year. A certificate which has expired cannot be used for secure login anymore. The check of certificate validity and timely extension is managed by the client.

« back to content

Certificate holder

If you do not use any electronic certificate yet, before obtaining it, think about who will be authorised to administer the certificate and distribute it to the bank's side. We recommend that the person responsible for the distribution of a public part of the certificate to the bank's side be the one already now administering BusinessNet Connect. This person included in the contact e-mail for Technical User administration is entitled to change and hold passwords for BusinessNet Connect.

Sharing the public part of the certificate with the bank

Please send your certificate public key to bank's technical support email, eb@unicreditgroup.sk. Subsequently, you will receive information that the bank accepted your certificate. As soon as you receive the confirmation, the connection with the WebDAV folder has been set and you can start using it.

Example of certificate issued by Actalis certification authority download and installation

a) Obtaining the certificate

The certificate can be obtained for free for one year from the Actalis website:
https://www.actalis.com/s-mime-certificates

- Valid email is required to receive a verification code
- Use verification code to complete certificate issuing
- A password will be provided (for example, jy5b36w3xZ8a) and email with password-protected KPCS12 – S/MIME certificate will be sent

b) Certificate installation / certificate public part extraction

1) Install the certificate in Windows
- Confirm the installation and enter the password

2) Export certificate public part (public key)
- Open Internet Explorer
- Go to Tools -> Internet Options -> Content -> Certificates
- Select a certificate and choose „Export"
- Select „No, do not export private key"
- Select format „Der encoded Binary X.509"

3) The result is public certificate (key), Certificate File: xxx.cer

c) Sending the public part of the certificate to the bank

- Please send the public key by email to eb@unicreditgroup.sk
- Our technical support will confirm the certificate was delivered

2. UNICREDIT BANK CONNECTION SETUP

2.1 WebDAV agent

We recommend using a WebDAV agent to connect to the bank, which allows you to store information about previous connections (sessions), especially if you will be connecting to the bank repeatedly during the day. This makes communication with the bank and data transfer faster. Suitable WebDAV agents include (not a complete list):

- Syncovery,
- File manager Total Commander,
- Sardine Java WebDAV klient.

Note: The WinSCP application does not support saving information about previous connections and therefore cannot be recommended for frequent connections to the bank.

2.2 Technical user initial setup

Username and a one-time code (password) for the Technical User is delivered to the person responsible for the Technical User in email. The one-time code is valid for two days and needs to be changed:

- In your internet browser, enter the address https://www.unicreditbank.sk
- Select login to **BusinessNet** for corporate accounts
- Enter the username of the Technical User in the field “User number” on the login screen
- Enter the code provided in the e-mail (six digits) into the field “Security Code”
- Press the “Login” button
- In the next step, you will be prompted to enter the old code and select new one
- Once the new security code has been set, log out from the internet banking

2.3 WebDAV setup without a certificate to verify login data

There are several ways to work with a WebDAV folder. You can access it:

- As a network drive
  - you can then simply copy the file by dragging it with the mouse
  - or you can use the command line (this enables the full automation)
- using a file manager – e.g., Total Commander

Below you will find a description of several ways to connect to a WebDAV folder. However, the list of methods is not exhaustive, BusinessNet Connect has been successfully tested also for Linux with davfs or Cadaver clients.

The endpoint for connecting without a certificate to verify credentials is https://sk.unicreditbanking.net/webdav/.

Windows – setting up native WebDAV

For setting:
- run the following command in command line (X: stands for drive under which WebDAV will be mapped):
  net use X: https://cz.unicreditbanking.net/webdav/
- enter the username of the technical user
- enter the password of the technical user (see chapter 2.1.)

Windows – Total Commander file manager

To use WebDAV with Total Commander, you will need to install a plugin:

- install Total Commander – can be downloaded from
  http://www.ghisler.com
- install WebDAV plugin – can be downloaded from
  http://www.ghisler.com/dplugins.htm

To set a WebDAV connection:

- select Network places, select WebDAV folder and press F7 to create a new folder (connection)
- enter new folder name
- fill field Connect with
  https://sk.unicreditbanking.net/webdav/
- fill technical user userID into field „User name“
- fill technical user password into field „Password“ (see chapter 2.1.)
- activate check box „Secure server (via SSL)“
- deactivate checkbox „Use multi-step upload method“
- other fields remain unchecked

Linux – setting up native WebDAV

For example in Ubuntu, native WebDAV can be set as follows:

- select „File“ from the menu, then select „Connect to Server“ and „Secure WebDAV (HTTPS)“
- fill the field „Server“ with https://sk.unicreditbanking.net/
- fill „/webdav/” into field „Folder“
- fill technical user userID into field „User name“
- fill technical user password into field „Password“ (see chapter 2.1.)

2.4 WebDAV setup with a certificate to verify login data

Before connecting to the bank for the first time, it is necessary to deliver the public key of the certificate (see chapter 1.4), which is used to verify the login data to the bank. The key is set for the technical user and the person responsible for the technical user must send the public key to the bank by e-mail to eb@unicreditgroup.sk.

In the subject line, please state „Public Key Setup for Technical User Authentication“ and include the technical user‘s username.

In the body of the email, please state your company name.

This email will only be accepted if it is sent from the email address listed for the user in the Key Holder List section of the BusinessNet Connect contractual documentation.

After the key has been set for the technical user, the bank will confirm by email that the public key has been set.

The endpoint for connecting without a certificate to verify credentials is https://connect.unicreditbanking.net/sk/.

In other parameters, the WebDAV settings do not differ from the variant without a certificate for verifying login data.

3. DATA DOWNLOAD

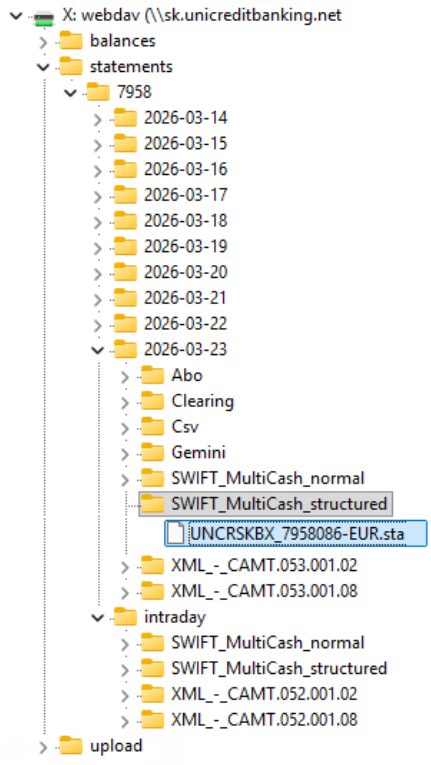
3.1 Electronic statements

The following types of electronic statements can be retrieved via BusinessNet Connect:

- Daily statements / MT940 – MultiCash structured, MultiCash unstructured, Gemini, ABO, Clearing, csv
- Daily statements / camt.053 v.2 – XML
- Daily statements / camt.053 v.8 – XML
- Intraday statements / MT942 – MultiCash structured, MultiCash unstructured
- Intraday statements / camt.052 v.2 - XML
- Intraday statements / camt.052 v.8 - XML

You can work with mounted WebDAV folder like any other folder. To automate file downloading, the directory structure and file naming convention are predefined.

3.1.1 Directory structure



In the **statements** directory, the subdirectory named by (technical) client number contains the following:

- 10 folders for daily MT940/camt.053 statements named by date
- one **intraday** folder with MT942/camt.052 statement

Each subdirectory is further divided into subdirectories by statement format types and they contain individual statements in files. Statements are also generated in all format types, thus, if you need a daily Gemini-format statement for one accounting system and MT940 MultiCash structured statement for another accounting system, just download the file from the correct directory.

The list of accounts available for BusinessNet Connect is governed by rights set for the Technical User based on the contractual documentation.

The Technical User has just the read-only right for these folders.

Note: Daily statements (MT940/camt.053) older than 10 calendar days can be downloaded manually in BusinessNet Professional – menu **Finances > Accounts > Electronic statements**.

3.1.2 File naming convention for electronic statements

File name always contains account number followed by hyphen and account currency code.

For the daily statement MT940 in both structured and unstructured MultiCash format, the filename extension is ".sta". For the Gemini format, the file extension is ".ace".

For statements with intraday movements MT942, for both structured and unstructured MultiCash formats, the filename extension is ".vml".

Example:
A file with an MT940 statement for the EUR account 7958086 held at UniCredit Bank will have the following name: UNCRSKBX_7958086-EUR.sta.

If BusinessNet Connect is set to encrypt the statements being downloaded, another filename extension ".esc" is added or all types and formats.

3.1.3 Statements format and paging

The up-to-date description for daily statement formats (MT940/camt.053) and statements with intraday movements (MT942/camt.052) can be downloaded from bank's website.

« back to content

The MT942/camt.052 statement downloaded via BusinessNet Connect contains **all MT942/camt.052 messages** generated on the respective day.

The newest message is always added at the end of the statement. Thus, in processing such statement the transactions contained in the previous messages that have already been processed need to be considered.

Individual messages can be distinguished by the statement number and page number.

Paging applies to all statements (similar to paper statements). Depending on the volume of information in individual transactions, a statement page contains 6–7 transactions. Paging is used for both MT940/camt.053 and MT942/camt.052 statements.

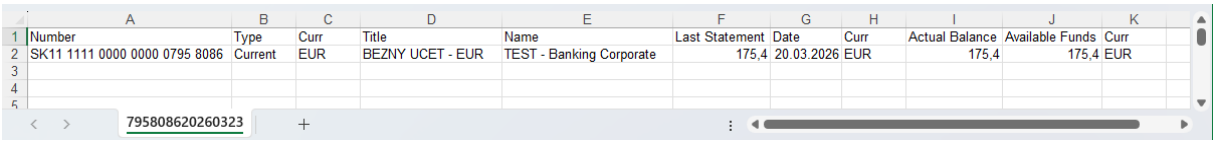
3.2 Balances

A special CSV file with account balances can be downloaded via BusinessNet Connect. It is the same information as is available in BusinessNet Professional at the „Overview of Balances" (Finances > Accounts menu).

It contains information on the balance from the latest statement, both the current accounting and available balance.

Current balances are balances at the time of Technical User login to BusinessNet Connect.

CSV file example:



	A	B	C	D	E	F	G	H	I	J	K
1	Number	Type	Curr	Title	Name	Last Statement	Date	Curr	Actual Balance	Available Funds	Curr
2	SK11 1111 0000 0000 0795 8086	Current	EUR	BEZNY UCET - EUR	TEST - Banking Corporate	175,4	20.03.2026	EUR	175,4	175,4	EUR
3											
4											
5											

795808620260323

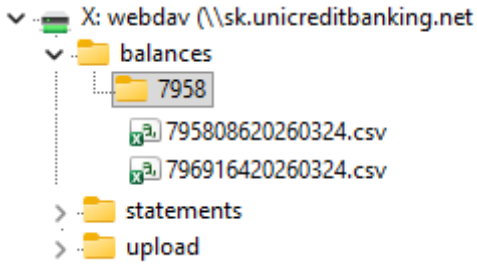
The meaning of CSV file columns is as follows:

- Number – account number
- Type – account type
- Curr – account currency
- Title – more detailed account type description, truncated to 20 characters
- Name – account name
- Last Statement – last statement balance
- Date – last statement date
- Actual Balance – current account balance
- Available Funds – account available balance

Note: The **balances** directory does not contain any history of files with balances. Only the current file for each of the accounts is available. To save a complete history of balances, files need to be downloaded on a regular basis.

You can work with a mounted WebDAV folder like any other folder. To automate file downloading, the directory structure and file naming convention are predefined.

3.2.1 Directory structure



The **balances** folder contains a separate file with balances for each connected account in the directory with the (technical) number of the client.

The Technical User has just the read-only right for this folder.

« back to content

3.2.2 File naming convention for balances

The filename always contains the account number and date of document generation.

Example: *The name of the file with data on balances for account No. 7958086 generated on 24 March 2026 will be 795808620260324.csv.*

If BusinessNet Connect is set to encrypt the files with balances being downloaded, another filename extension ".esc" is added for all files.

4. FILE UPLOAD

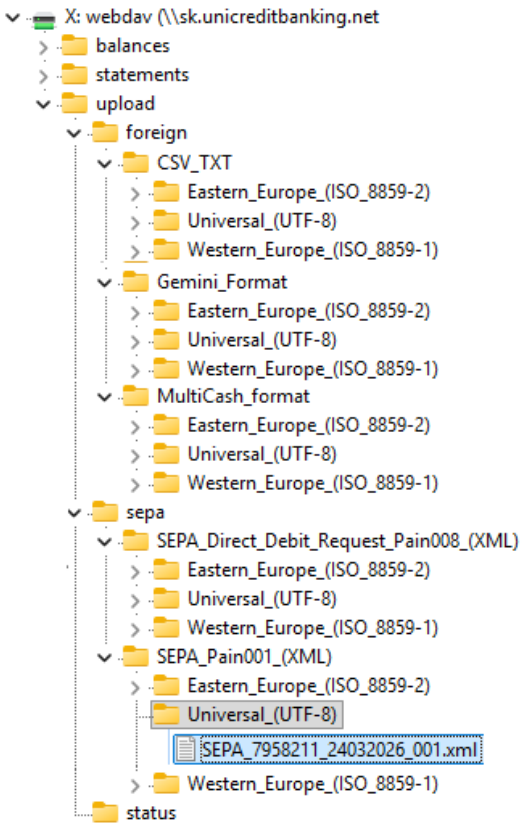
BusinessNet Connect supports the following payment files formats:

- Foreign payments – Gemini, MultiCash, CSV
- SEPA payments – pain.001 and pain.008

The up-to-date description for payment files formats can be downloaded from the bank's website.

You can work with a mounted WebDAV folder like any other folder. To automate file downloading, the directory structure and file naming convention are predefined.

4.1 Directory structure



The **upload** folder contains 3 folders:

- foreign
- sepa
- status

« back to content

Foreign / SEPA are divided into subfolders by payment file format and by file coding. The payment file is simply copied into a correct folder – which is identical with using the Upload function in BusinessNet Professional.

The result of file upload can be checked in the **status** folder (see below).

The list of accounts, which can be used in the payment file, is governed by the list of accounts assigned within the contractual documentation to the Technical User holding the right to upload.

Each uploaded file must have a unique filename. We recommend that date and time be part of the filename. A maximum length of filename is 64 characters including its extension.

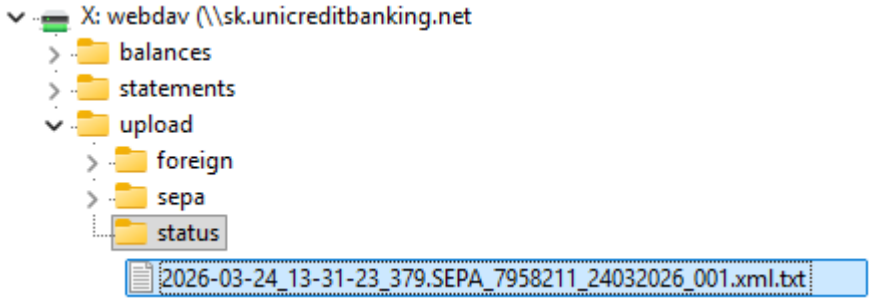
The Technical User has just the write-only right for these directories. For security reasons, uploaded files cannot be read from the WebDAV folder.

4.2 Error handling using status file

For each uploaded file a status file is created in the **status** folder. This file contains information on the result of the upload and summary data on the payment package (similar to the summary data from package details in BusinessNet Professional).

The filename always starts with the date and time of the upload followed by the uploaded file name. The file extension is ".txt".

Example: *The payment file " SEPA_7958211_24032026_001.xml " uploaded on 24. 3. 2026 at 13:31:23,379, will have the status file with the following filename: 2026-03-24_13-31-23_379. SEPA_7958211_24032026_001.xml .txt.*



Following fields of the status file should be checked once the file has been uploaded:

- Status – uploaded file status:
  - If the file ended in "306 (Error)"status, such package cannot be uploaded, nor it will be displayed in the files overview in BusinessNet Professional. Before the file is reloaded, it needs to be corrected. Individual error codes are described below.
  - Successfully loaded packages, ready for signature, will have the "302 (To sign)" status.
  - Partially signed packages (if automatic processing applies) will have the "303 (P. signed)" status. Signature process of such package should be completed in BusinessNet Professional.
  - If package is finally signed (automatic processing applies) the status will be empty.

Note: The signature process can take up to 5 minutes if automatic processing applies. Afterwards, the status file is updated. The signature result should be rechecked later.

We also recommend checking these fields:

- # Orders – the number of orders in payment file.
- Checksum – the sum of all payments amounts regardless the currency and sign (absolute values sum).
- # To sign – zero if all orders were automatically signed (automatic processing applies). Non-zero means that package contains orders which should be signed in BusinessNet Professional.

The following table should help you find the cause of unsuccessful package upload:

Status	Cause
Problems with the Technical User's right to accounts	
Status : 306 (Error) IBX00016 (USER HAS NOT IMPORT/UPLOAD RIGHTS FOR THE ACCOUNT Code[IBX00016])	The Technical user does not have upload rights for at least one of the accounts used in the payment file.
Status : 306 (Error) IBX00188 (Current account not existing Code[IBX00188])	At least one account used in the payment file is not assigned to the Technical user.
Problems with the payment file format	
Status : 306 (Error) IKC00022 (Parsing Impossible Code[IKC00022])	The payment file content cannot be parsed. This error type may occur, for example, in following situations: • A correctly structured file was uploaded into a wrong subfolder (e.g., a MultiCash file into a Gemini subfolder for foreign payments). • The uploaded file has a wrong format (e.g., a part of the file is corrupted).
Problems with encryption and signature	
Status : 306 (Error) JWB0524 (Uploaded file was not plain but the chosen transport profile accepts only plain files. (JWB0524))	A problem with file decryption on bank's side. This error type may occur, for example, in following situations: • Uploaded file was encrypted or signed but BusinessNet Connect is set to accept only plain files. • Uploaded file was plain (not encrypted) but BusinessNet Connect is set to accept only encrypted files. • Uploaded file was signed but BusinessNet Connect is set to accept only encrypted files. • Uploaded file was neither encrypted nor signed but BusinessNet Connect is set to accept only encrypted and signed files.
Status : 306 (Error) SG74107 (General public key error. (SG74107))	Problem with user signature key used for signature. Public key assigned to the user at the bank must be replaced by a correct type (the key should be re-created and registered again in the bank.)
Status : 306 (Error) SG74106 (General private key error. (SG74106))	Problem with bank's public key used to encrypt uploaded file. New key should be downloaded from bank's web site and set in the PGP program.

4.2.1 Example of successful upload status file

The status file after a successful upload via BusinessNet Connect (the package contains one order and is ready for signature in BusinessNet Professional):

Status : 302 (To sign)
Pay.Type : 3 (Sepa Payment)
Changed : false
Filename : SEPA_7958211_24032026_001.xml
Type : 1 (Upload)
Structure : 7 (SEPA Pain001 (XML))
Timestamp : 24.03.2026 13:31:23
Checksum : 1.02
Digest : BCA91A0381A0E9ADE29ECAFE22D7F837
Errors : 0
To sign : 1
Orders : 1

BNC7958|Technical User EST - BANKING CORP|Upload|24/03/2026 13:31:23|

4.2.2 Example of failed upload status file

A status file for failed upload via BusinessNet Connect (an account, for which the Technical User does not have the upload right, was used in the payment file):

Status : 306 (Error)
IBX00016 (USER HAS NOT IMPORT/UPLOAD RIGHTS FOR THE ACCOUNT Code[IBX00016])
Pay.Type : 1 (Foreign Payment)
Changed : false
Filename : 20260326_invoices_II.ska
Type : 1 (Upload)
Structure : 1 (MultiCash format)
Timestamp : 22.3.2026 10:01:24
Checksum : 0.00
Digest : 2d8837df68f388a8e24065ed90d62552
Errors : 0
To sign : 0
Orders : 0

25029752| CA Europa Test|Reservation|22/3/2026 10:01:24|
25029752||File imported|22/3/2026 10:02:12|

5. ENCRYPTION

BusinessNet Connect allows encrypting both the downloaded and uploaded files. It is another security feature with optional setting. For full automation of processing of payment files, it is mandatory to Encrypt and Sign uploaded files.

BusinessNet Connect supports only OpenPGP type RSA keys with validity less than one year.

For example, the **Gpg4win** programme and its graphic add-on **Kleopatra** can be used to work with keys and for encryption or decryption. Application can be downloaded for free, for example, from https://www.gpg4win.org.

5.1 Glossary

The pair of keys (to be created in Kleopatra application)

- **Public key**
  The bank uses the client's public key to encrypt the file content. The encrypted file can be decrypted using the client's private key.
- **Private key**
  The private key serves to decrypt the content of files encrypted using the public key.

Bank's public key (provided by the bank to a client)
The bank's public key serves to encrypt the file of payments on the client's side and is provided by the bank upon request.

Signature user (see the example of PGP creation in the chapter 5.2.)
A user intended only for the signature of payment files on the client's side. There can be several signature users. The user is not intended for common work in BusinessNet Professional. The private part of the user's key is used on the client's side to sign payment files sent to the bank. The public part of the key is used on the bank's side to verify the signature of a payment file sent to the bank by the client.

5.2 Example of new pair of keys creation in Kleopatra application

To create the pair of keys (public/private):

- Select menu **File** -> **New pair of keys**
- Select **Create a personal pair of keys OpenPGP** and fill optional data (will be used as the certificate identifiers)
  - Name (could be also company name)
  - Email
- Select **Advanced settings** and fill it according to the example
  - Key material: RSA
  - Certificate usage: Signing, valid for one year

After the pair of keys has been created, you can export its public part and save the public key in a file.

- Select **Send Public Key By Email**
- Or right-click in the list of certificates and select **Export**

5.3 The process of client's public key delivery to the bank

The key is set for the Technical User and the person responsible for the Technical User must send the public key to the bank by email to eb@unicreditgroup.sk.

In email subject mention „Setting a public key for the Technical User" followed by Technical user userID.

Mention company name in the email body.

The e-mail will be accepted if sent from the e-mail address provided for the user in the section of List of Key Holders of the contractual documentation for BusinessNet Connect.

The bank will confirm by email when the public key has been set.

« back to content

5.4 Import of bank's public key

- request the bank's public key by email at eb@unicreditgroup.sk
- in Kleopatra application, select File -> Import and select just downloaded bank's public key
- Kleopatra will prompt to certify the key -> confirm and choose your own password

5.5 Encrypting / Decrypting of downloaded files by the bank

Downloaded files can always be encrypted by the client's public key. Such setting must be agreed in the contractual documentation in advance with your banker.

Downloaded encrypted file must be decrypted otherwise it will be unreadable. The file can only be decrypted on the computer where the Technical User private key is stored.

- In Kleopatra application: menu File > Decrypt/Verify Files..., choose a file and select **Decrypt**.

5.6 Encrypting / Signing files

When uploading files via BusinessNet Connect, the following three options can be **optionally set**:

- **Encryption of uploaded files**
  Payment file is encrypted using the bank's public key before it is uploaded via BusinessNet Connect. Value can be set to No / Mandatory / Optional (bank will accept both encrypted and plain files).
- **Electronic signature of uploaded files**
  Payment file is signed by client's private key before it is uploaded via BusinessNet Connect. Additionally, payment file is encrypted by bank's public key. Bank will decrypt uploaded payment file using its private key and will validate the client's signature with client's public key. Value can be set to No / Mandatory / Optional (bank will accept both signed and unsigned files).
- **Automatic order processing**
  If set to **Yes**, all digital signatures are legally binding and all orders in the payment file are considered as if they were authorized in BusinessNet Professional. Loaded payment file is immediately sent to signature process and when completed orders are passed to bank's backend systems.
  If set to **No**, payment file is saved in BusinessNet Professional Signature folder in "To sign" status and must be manually signed in BusinessNet Professional.
  The pre-condition for activating automatic order processing is the use of a certificate to verify login data.

These settings must be agreed in the BusinessNet Connect contractual documentation.

5.6.1 Encryption of uploaded files

If encryption is set as mandatory for BusinessNet Connect, the payment file must be encrypted using the bank's public key before it is uploaded.

To encrypt a file:

- In Kleopatra application select **File > Sign/Encrypt...**
- Choose a file to be encrypted and set following parametres:
  - **Sign as:** leave this field empty (file is to be encrypted only)
  - **Encrypt for me:** leave this field empty
  - **Encrypt for others:** select bank's public key imported into Kleopatra
  - **Encrypt with password:** leave this field empty
- press **Encrypt** button
- save resulting file into **Upload** directory (see chapter 4).

5.6.2 Encryption and signature of uploaded files

If signature is set as mandatory for BusinessNet Connect: before being uploaded, the files must be encrypted using the bank's public key and signed by one of the users holding the **RSA key** (see chapter 5.2.). The user's public key must be registered with the bank.

To encrypt and sign a file:

- In Kleopatra application select **File > Sign/Encrypt...**
  Choose a file to be signed and encrypted and set the following parametres:
  - **Sign as:** select a user with the pair of RSA keys who has been set for signature
  - **Encrypt for me:** leave this field empty
  - **Encrypt for others:** select bank's public key imported into Kleopatra
  - **Encrypt with password:** leave this field empty
- Press **Sign/Encrypt** button
- Enter the password set during RSA key creation
- Save resulting file into **Upload** directory (see chapter 4)

Warning: If automatic file processing applies, loaded payment file is **immediately sent to signature process** and when completed orders are **passed to bank's backend systems**.

UniCredit Bank
Czech Republic and Slovakia, a.s.
Corporates

Contact
Payments & Cash Management
Šancová 1/A
813 33 Bratislava

Online
www.unicreditbank.sk

UniCredit Bank