Czech National Bank

Annex 4
to the CERTIS Rules

Alternative means of transmitting and receiving of data files

Version 5

effective from 1 November 2018

CONTENTS

1 Introduction

Where the participant is unable to transmit and receive data via the AMOS system, the data may – after telephone agreement with the CERTIS operator – be transmitted/received by e-mail (see section 5) or in person in the CNB (see section 6).

In both cases the data shall be furnished with an electronic signature (electronic seal) and accompanied by a dispatch note (see section 2). The data shall be transmitted in an encrypted form (see section 3). If the data are submitted in person, the data need not be encrypted. The regulations for file names are provided in section 4.

2 Electronic signature (electronic seal), dispatch note

In both cases, data shall be signed using an electronic signature (electronic seal) similarly as the data transmitted via the AMOS system.

Signature certificates registered in the AMOS system shall be used. The number of signatures of input data shall be comunicated by the authorised person to the operator (see Article 16(2)(b) of the CERTIS Rules).

The output files from the CERTIS system shall bear the CERTIS's electronic seal based on the qualified certificate (see the Annex 2 to the CERTIS Rules).

Dispatch notes signed by a person specified in the CERTIS participant's specimen signatures shall be submitted together with the data files (see Article 16(2)(e) and (4) of the CERTIS Rules). It is possible to provide more data files on one form.

In case that CERTIS operator transmits the dispatch note in electronic form without the signature as described in the paragraph above, the dispatch note shall bear the electronic seal of the CERTIS system (see the Annex 2 to the CERTIS Rules).The electronic signature (electronic seal) ensures the authorisation of the data. The dispatch note is an instruction for the CNB to enter the data in the CERTIS system.

3 Data encryption, public certificates

3.1 Data encryption

Input files with items (INTOCC) and output files with items (FROMCC) shall be transmitted in an encrypted form.

To encrypt the files, the Signer module (Activex Signer.dll) can be used, which is available in the AMOS in “Miscellaneous / Help, documents, contacts” section under “AMOS technical conditions”.

The CNB provides a simple application (static website) to be downloaded, which allows to encrypt (and potentially also sign) data files using the Signer module. This application is also available in the AMOS “Miscellaneous / Help, documents, contacts” section under “Crypto library”.

The encrypted message can also be created by some other application. The message shall be created in the structure of the envelopedData under PKCS#7 in DER coding. Algorithm 3DES can be used for coding.

For encryption, public certificates issued by PostSignum, 1.CA or e-Identity certification authorities shall be used.

3.2 Public certificates

The CNB public certificate, which the CERTIS participant uses for encrypting INTOCC files can be downloaded in the AMOS “Miscellaneous / Help, documents, contacts” section under “Encryption certificate”.

For encryption of FROMCC files, the CNB shall use the participants’ public certificates issued by PostSignum, 1.CA or e-Identity certification authorities. The participants shall send their public certificates by e-mail to certis@cnb.cz. The e-mail subject shall consist of the participant’s code and the text “public certificates” (e.g. Subject: 0800 public certificates). The certificate should be in DER coding (suffix .cer). The suffix shall also include a chain .txt (e.g. cert10730772.cer.txt) to prevent the file from being blocked when it is sent by e-mail. The CERTIS participants are obliged to send updated public certificates.

4 Name convention

The data file name with items has the format YYYYMMDD_XXXX_NNNNNN, where:

YYYYMMDD is the date of the accounting day on which the input data file is to be processed or on which the output data file was created,

XXXX is the participant's numeric identity code,

NNNNNN is the data file number.

The suffix differs depending on the file's content:

- without suffix – the data file itself with items,
- .ep1 – file with the first signature,
- .ep2 – file with the second signature,
- .p7e – encrypted data file.

The CNB generates numbers of output files in the range from 501 to 899. It is therefore appropriate that participants do not use numbers from this range for input files.

5 Transmission of files by e-mail

5.1 INTOCC files

INTOCC files shall be sent to certis@cnb.cz. The e-mail subject shall consist of the participant's code and "INTOCC" (e.g. Subject: 0800 INTOCC). Participant shall sent e-mails in maximum once an hour in the case of non-priority files and in maximum twice an hour in the case of priority files. If the input file will have 10MB, participant should send INTOCC files more frequently.

The enclosed file (files) should be encrypted. However, the CNB accepts also unencrypted files from participants[1].

Simultaneously with data files, the participant shall submit a dispatch note signed by a person listed in specimen signatures. The CERTIS participant may also transmit

[1] Protection of the data held by the participant is its exclusive responsibility. If it sends unencrypted data, it risks a breach of data confidentiality and is fully responsible for potential consequences. However, the CNB has no reason not to process such data.

the dispatch note to the operator by e-mail or by fax; it shall immediately confirm the sending of the e-mail or the fax to the operator by telephone.

After processing all files from the e-mail, the CNB shall send back a confirming e-mail. In the event of errors, a protocol shall be annexed.

5.2 FROMCC files

The CNB shall send FROMCC files to e-mail addresses set by the participant. The CNB's e-mail shall include encrypted files with data, files with signatures and dispatch notes.

The e-mail subject shall consist of the participant's code and "FROMCC" (e.g. Subject: 0800 FROMCC).

The participants shall send their e-mail addresses to which the CNB will send FROMCC files by e-mail to certis@cnb.cz. The e-mail subject shall consist of the participant's code and the text "e-mail addresses" (e.g. Subject: 0800 e-mail addresses).

The CNB shall always send encrypted files to the participant by e-mail.

6 Submitting and receiving in person

6.1 INTOCC files

Where the INTOCC files are submitted in person, flash drives shall be used.

The encrypted files with data and files with signatures are stored on the medium. The files shall be encrypted according to the description in section 3.

The CNB accepts from the participant also unencrypted files with data[1].

Simultaneously with data files, the participant shall submit a dispatch note signed by a person listed in specimen signatures. The participant may also transmit the dispatch note to the operator by e-mail, by fax or on flash-disc; it shall immediately confirm the sending of the e-mail or the fax to the operator by telephone.

The CNB shall confirm the processing of files by telephone or send a confirmation e-mail.

6.2 FROMCC files

Where the FROMCC files are submitted in person, flash drives shall be used.

The encrypted files with data and files with signatures are stored on the medium. A dispatch note is attached to the medium.

At the participant's request signed by an authorised person the CNB may transmit to the participant also unencrypted files[2].

[2] Protection of the data held by the participant is its exclusive responsibility. After the data have been handed over to a person identified by the participant, the data are held by the participant. If the participant requests unencrypted data, it risks a breach of data confidentiality and is fully responsible for potential consequences. The CNB does not prefer this alternative, but is ready to satisfy the participant.