Annex 2
to the CERTIS Rules

Conditions of use of the AMOS web portal

Version 7

effective from 1 December 2015

CONTENTS

1. Introduction

AMOS is a web application providing interactive access to data from the CERTIS system and the possibility to transmit and receive data. The AMOS system is operated by the Czech National Bank.

In particular, the AMOS system enables to display the participant's current position, administer items in a hold queue, search for items, display a daily statement, details and history of the account, insert and register a batch with input items, display an overview of batches and transmit a batch for processing, verify the electronic signature of a batch, create and register items, display the item archive, display a list of input and output files, download a protocol on input file processing, download an output file, administer the creation of output files, administer the participant's users, their roles and signature certificates, display an overview of fees, compliance with minimum reserves and a list of loro accounts, display documentation and messages for users, administer the participant's contacts and display the participant's log.

A detailed description of the individual web pages is available in the AMOS User Manual.

2. Access to AMOS

To use the AMOS system you need access to the CNB's communication gateway, operating system Windows 7 or higher and internet browser MS Internet Explorer 9 or higher. The AMOS application can be accessed at:

AMOS web	Host name	IP address	Production environment	Test environment
Primary	wsc.cnb.cz	193.84.144.151	https://wsc.cnb.cz/amos/	https://wsc.cnb.cz/amost/
	wsc2.cnb.cz	193.84.144.105		
Secondary	wsd.cnb.cz	193.84.144.152	https://wsd.cnb.cz/amos/	https://wsd.cnb.cz/amost/
	wsd2.cnb.cz	193.84.144.110		

Communication with the server (computer) on which the AMOS application is running at the CNB is secured using a certificate (server security certificate) issued specifically for the servers "wsc.cnb.cz" and "wsd.cnb.cz". This certificate was issued by VeriSign (Symantec) certification authority.

Where the user needs to sign batches when using AMOS, support for work with qualified certificates for batch signing shall be installed.

3. Users and roles

Specified employees of CERTIS participants shall be the users of the AMOS system. User administration shall be carried out by an authorised employee of the participant – user administrator.

3.1. User administrator

The user administrator shall administer the participant's users. In particular, he shall register new users, assign roles to users, change the login method (password/certificate), select the language version, remove users and register the participant's signature certificates. The user administrator shall log in the AMOS system using a commercial certificate.

The identification data of a user administrator (especially the unique name of his certificates) shall be transmitted by the participant in writing using the form "Identification of the CERTIS participant's user administrator" signed by an authorised person (see section 6.1). The form can be used to register a new administrator, change the data on a registered administrator or to cancel registration. User administrators shall be registered in the system by the operator.

3.2. Users

Each AMOS user shall be registered in the system. The user may choose whether to log in using a name (automatically assigned user code) and password or using a commercial certificate.

For AMOS login using a certificate, the operator shall only allow the use of commercial certificates issued by accredited providers of certification services: Česká pošta, s. p., První certifikační autorita, a. s., and e-Identity a.s. For use in the AMOS system, it is recommended that the certificate be designated as public.

3.3. Roles

Each user shall be assigned one or more roles, having access to certain data or rights to perform certain activities in the AMOS system depending on the roles assigned. The role shall determine whether the page will be displayed and which data will be visible to the user on the page.

AMOS roles shall be divided into active and passive. Passive roles shall only enable viewing of information. Active roles shall enable input of data and administration of processing. Passive roles shall be the first three roles in the table below (OBC, OPR and FIN).

Overview of AMOS roles

Code	Role designation	Description
OBC	General information	viewing of general information (balance for the accounting day, overview of messages, access to documentation, list of participants, file types, fee bands, etc.), signature verification
OPR	Operational information	viewing of information on file processing (overview of batches, input files, output files, protocols), times of creation of output files, download of protocol on input file processing
FIN	Financial information	viewing information on the participant's balance and position (current position, searching for items, information on accounts, fees, statistical data)
POL	Entry of items	entry of items 01, 21, 37, 45, administration of items, creation and registration of batches, item archive, transmission of a batch with manually entered items
DAV	Entry of batches	entry of external batches SPP a SPN, administration of external batches, transmission of external batches
RVS	Administration of output files	setting the time of creation of output files, ad hoc creation of output files, download of output files
RHQ	Removal of orders from hold queue	entry of requirement to remove an order (accounting item) from hold queue – refusal of payment
LOR	Loro accounts	administration of loro accounts
PDA	Signing of batches	signing of batches (with items or with a certificate), transmission of batches
SUZ	User administration	user administration – user registration, role assignment, preparation of batches with a signature certificate
SBP	Administration of blocked items	entry of request for settlement or refusal of blocked item, administration of checklists of beneficiaries and payers and administration of parameters of blocked items, entry of item 44, entry and registration of RP4 batch, archive of items, entry of batch with manually entered items, entry of external batch CPL, CPR and SP4, entry of external batches, transmission of external batches

The "General information" role shall be assigned automatically upon user creation.

The "Signing of batches" role shall only provide access to the icon for signing a batch within AMOS. The batch shall be signed using a qualified certificate registered by the user in AMOS.

4. Batches and signature certificates

4.1. Batches

A batch shall consist of a file containing the data and one or two files containing the electronic signature of the former file. The AMOS system shall use following types of batches – batches with input items, batches with a certificate, batches with checklist of beneficiaries or payers. Each transmitted batch shall be signed using a secured electronic signature. The signature shall be verified by the CERTIS system using the qualified certificate of the signing person. If the employee signing the data signs outside the AMOS system, he shall not be required to have access to AMOS.

4.1.1. Batches with input items

A batch with items shall contain the participant's input items in the CERTIS system and shall be signed using a qualified certificate for signing batches with items. The unique name of such a certificate shall be transmitted to the operator in a batch with a certificate. A batch with items shall contain one or two files with signatures according to the participant's requirements. The participant shall specify the number of signatures using the form "Specification of the number of signatures of an input batch with items in the CERTIS system".

4.1.2. Batches with a certificate

A batch with a certificate shall contain the unique name of a qualified certificate for signing batches with items or checklists. The batch shall be signed using a qualified certificate for signing batches with a certificate. The unique name of such a certificate shall be transmitted using the form "Specimen signature and specimen electronic signature of an authorised person of a participant in the CERTIS payment system".

4.1.3. Batches with checklists

A batch with checklist shall contain either checklist of beneficiaries or checklist of payers. The batch shall be signed using a qualified certificate for signing batches with checklists. The unique name of such a certificate shall be transmitted to the operator within a batch with certificate.

4.2. Signature certificates

For signing batches in the AMOS system, the operator shall only allow the use of qualified certificates issued by accredited providers of certification services: Česká pošta, s. p., První certifikační autorita, a. s., and e-Identity a.s. For use in the AMOS system, it is recommended that the certificate be designated as public.

The participant's signature certificates shall be administered by a user administrator. The unique name of the signature certificate shall be transmitted to the CERTIS system in a batch which shall be electronically signed using an authorised person's certificate. The signature shall be performed in the AMOS system. The signature certificate shall be registered in the CERTIS system and assigned a unique code. The signature certificate may be revoked in the AMOS system at any time.

5. Protocols and output files

Protocols on processing of input files, output files and electronically transmitted dispatch notes[1] shall bear the electronic mark of the CERTIS system. The certificate to verify the CNB's electronic mark was issued by Czech Post's certification authority PostSignum:

Subject serialNumber=S16676,CN=Systém CERTIS,O=Česká národní banka [IČ 48136450],C=CZ

Issuer PostSignum QCA2

Certificate revocation lists (CRLs) are issued by the PostSignum certification authority (see the website www.postsignum.cz).

[1] Dispatch notes are transmitted with the data files in case of using the alternative means of transmitting and receiving of data files according to the Annex 4 to the CERTIS rules.

The participant shall be obliged to verify the authenticity of the protocols and output files by verifying the electronic mark of the CERTIS system. The operator shall inform participants about introducing a new CERTIS system electronic mark by e-mail using the contacts in the category Technical matters.

6. Overview of persons in AMOS

6.1. Authorised person

Authorised person – the participant's employee entitled to specify:

- user administrators
- certificates to verify a guaranteed electronic signature/electronic mark for signing batches with items
- persons authorised to sign written (fax) orders
- number of signatures of an input batch with items in AMOS

The authorised person shall be registered in the CERTIS system using the form "Specimen signature and specimen electronic signature of an authorised person of a participant in the CERTIS payment system", which shall contain:

- name and contact information
- unique name of the signature certificate (qualified certificate) used for electronic signing of items with batches
- specimen signature

The form shall be signed by a person authorised to sign the payment system agreement.

6.2. User administrator

User administrator – the participant's employee administering access of the participant's users to AMOS. In particular, the user administrator shall be responsible for:

- registration and administration of the participant's users
- assignment of roles

The user administrator shall be registered in the CERTIS system using the form "Specification of the user administrator of a participant in the CERTIS payment system", which shall contain:

- name and contact information
- unique name of the access certificate (commercial certificate)

The form shall be signed by an authorised person.

6.3. User

User – the participant's employee who has access to the individual pages in the AMOS system according to assigned roles.

Users shall be registered in the AMOS system by the user administrator. The registration shall contain:

- name
- login method
- unique name of the access certificate (commercial certificate) or access password
- selection of the language version
- assigned roles

7. Procedures

7.1. Procedures for ensuring access to AMOS

Participant	Operator
Specification of authorised persons The form "Specimen signature and electronic specimen signature of the CERTIS participant's authorised person"	
	Registration of authorised persons, especially the unique names of signature certificates
Specification of user administrators The form "Identification of the CERTIS participant's user administrator" signed by an authorised person	
	Registration of user administrators, especially the unique names of commercial certificates
Registration of users, assignment of roles User administrator in AMOS	

7.2. Procedure for transmitting a batch with a certificate

Action in AMOS	Performed by
Creation of a batch with a certificate	User administrator (SUZ role)
Signing a batch with a certificate	Authorised person (PDA role)
Transmission of a batch with a certificate	Any user (SUZ or PDA role)

The unique name of the signature certificate shall be registered in CERTIS.

7.3. Procedure for creating and transmitting a batch with items

Action in AMOS	Performed by
Insertion of items, creation of a batch with items	Any user (POL role)
Signing a batch with items	Any user (PDA role)
Transmission of a batch with items	Any user (POL or PDA role)

The input data file shall be registered in CERTIS.

7.4. Procedure for transmitting an external batch with items

Action in AMOS	Performed by
Insertion of an external batch with items (with or without external signature)	Any user (DAV role)
Insertion and signing of an external batch with items	Any user (PDA role)
Signing of an external batch with items	Any user (PDA role)
Transmission of an external batch with items	Any user (DAV or PDA role)

The input data file shall be registered in CERTIS.

8. AMOS/WS application interface

Web Services (AMOS/WS) as an extension of the AMOS system provide an A2A (application-to-application) interface for transmitting INTOCC batches and receiving FROMCC batches.

AMOS/WS web services include five functions:

- function for transmitting INTOCC batches,
- function for downloading protocols on processing of INTOCC batches,
- function for downloading output FROMCC batches,
- function confirming download of FROMCC batches and
- function for downloading the current balance of the participant's account.

The transport protocol shall be the https protocol with obligatory client authentication using commercial certificates issued by public certification authorities (1. CA, Czech Post's PostSignum and eIdentity) and registered in the AMOS application.

Access shall be conditional on user registration in the AMOS system with access using a commercial certificate with the purpose set to WebServices. The URLs and relevant IP addresses of web services servers are listed in the following table:

Environment	IP address	URL
Test	193.84.144.136	https://amoswstest.cnb.cz/amosws/AmosWSPort
Production	193.84.144.135	https://amosws.cnb.cz/amosws/AmosWSPort

Network communication with the server operating the AMOS/WS application is secured via server certificate issued exclusively for "amoswstest.cnb.cz" and "amosws.cnb.cz" servers. These certificates were issued by the VeriSign (Symantec) certification authority.

Xsd and wsdl definition files shall be available at the AMOS home page – https://wsc.cnb.cz/amos/.

The operator shall inform participants about planned unavailability and failures of the web services by e-mail using the contacts in the category Technical matters.

8.1. Data types of parameters with a batch, protocol and electronic signature

Batches, protocols and electronic signatures shall be transmitted either directly in an element of the type "base64Binary", or as an attachment (MTOM attachment).

The format of a batch shall conform to Annex 1 to the Rules. Protocol formats are described in section 8.4.

The electronic signature (apart from BASE64 coding for the purposes of the xml element of the type base64binary) shall be created in the signedData structure according to PKCS#7 in DER coding; the protocol shall not contain the signed data as such (the signature shall be external) and shall contain the signing certificate and always one signature.

8.2. Certificates, electronic signature and mark

A commercial certificate issued by a public certification authority shall be used for client authentication. The certificate shall be registered in the AMOS system by a user administrator as an access (login) certificate, and its purpose of use shall be WebServices. An access certificate with interactive access as the purpose of use shall not be allowed.

A qualified certificate or electronic mark issued by a public certification authority shall be used for signing batches. The certificate shall be registered in AMOS as a signature certificate (by transmitting a batch with a certificate).

A batch with items transmitted using AMOS/WS shall only have one electronic signature regardless of whether the participant specified one or two signatures for manual transmission of batches within interactive access.

To create an electronic mark (i.e. electronic signature), the AMOS system shall use a qualified certificate issued by Czech Post's certification authority PostSignum, see section 5.

8.3. putIntoCC function

The putIntoCC function shall be used to register and transmit an input batch with items in the AMOS system by the specified accounting day. The batch shall have the entry data file format pursuant to Annex 1 to the CERTIS Rules. The maximum data file size is stipulated in Annex 1 to the CERTIS Rules.

On the client's side, it shall be typically assumed that the client application transmits another INTOCC batch only after receiving the protocol for the previous batch. However, the system shall not prevent transmission of multiple batches in close succession without waiting for the protocol. Similarly, the system shall not prevent parallel access from multiple processes (e.g. one for high and another for low priority) or multiple applications of the same client.

Input parameters of the function

WS	Description
datum	Accounting day
ucastnik	Participant's numeric code
cislo	Batch number
priorita	Batch priority (H/L)
davka	Data pursuant to Annex 1 to the CERTIS Rules – see section 8.1
podpis	Data – electronic signature – see section 8.1

Output parameters of the function

WS	Description
stavKod	Numeric code of the result (0 = batch received for processing, other = error code, batch not received)
stavText	Description of the output state

Functionality

The function checks the entered parameters and returns the result code. It logs information about the processing of the order. If the input parameters are error-free, it enters the batch into AMOS and transmits it for processing.

Overview of output states

Check upon login:

10 Invalid certificate – the certificate is listed in the CRL

11 Invalid participant code – the participant code is not registered in CERTIS, or it is registered but the participant has yet to be activated

12 Participant blocked – the participant's activity in CERTIS has been suspended

13 Access certificate not registered in AMOS – the participant's commercial certificate is not registered in the AMOS system or is outside the boundaries of its validity registered in AMOS (before start of validity or after end of validity – see AMOS, the form "User maintenance / Users"), or the purpose of the certificate is not WebServices

Parameter syntax check:

51 Invalid batch number – batch number is zero or higher than 999,999

53 Mandatory parameter batch is empty

54 Mandatory parameter signature is empty

Accounting day check:

20 Batch date differs from current accounting day

22 Batches no longer received – accounting day has been closed

Participant check:

30 Participant's reception of input files has been blocked

Duplicity check:

40 Duplicate batch transmission – batch with the same designation has already been registered in AMOS or CERTIS

Unexpected situation:

99 Unexpected error – if an error other than the above occurs

Successful batch transmission:

0 Batch transmitted for processing – the function has entered the input file in AMOS. The batch is entered in state "Transmitted for processing" – it is shown in AMOS on the page "List of batches – Batch transmission".

8.4. getProto function

The getProto function shall be used to download the protocol on input batch processing in text or csv format.

Therefore, it shall be typically assumed that if the client's application has transmitted an INTOCC batch and has not yet received the batch processing protocol, it will request reception of the protocol at regular intervals (roughly once a minute or at longer intervals) until the protocol is available. Parallel access of two processes, one for high and another for low priority, shall also be enabled. Parallel access of multiple processes from various applications of the same client shall not be ruled out either.

The delay between batch transmission and availability of the protocol shall depend on the batch size and potential concurrent transmission of large batches by multiple participants. Small priority batches are usually processed in 20 seconds at the earliest, in most cases within one minute. A batch with 10,000 items is usually processed in around one minute.

Input parameters of the function

WS	Description
datum	Accounting day
ucastnik	Participant's numeric code
cislo	Batch number
typ	Protocol type (CSV or TXT)

Output parameters of the function

WS	Description
proto	Data – protocol by type (existing ICP or CSV)
podpis	Data – electronic signature of protocol – see section 8.1
stavKod	Numeric code of the result (see below)
stavText	Description of the output state

Functionality

The function checks the entered parameters. It logs information about the processing of the order. The function returns the result code (output state); if the input parameters are error-free and the protocol exists, it also returns the protocol file and the protocol signature file.

Overview of output states

Check upon login:

10 Invalid certificate – the certificate is listed in the CRL

11 Invalid participant code – the participant code is not registered in CERTIS, or it is registered but the participant has yet to be activated

13 Access certificate not registered in AMOS – the participant's commercial certificate is not registered in the AMOS system or is outside the boundaries of its validity registered in AMOS (before start of validity or after end of validity – see AMOS, the form "User maintenance / Users"), or the purpose of the certificate is not WebServices

Parameter syntax check:

51 Invalid batch number – batch number is zero or higher than 999,999

Unexpected situation:

99 Unexpected error – if an error other than the above occurs

Non-existent batch

4 No batch corresponding to the requested protocol exists

Batch exists

7 Batch refused by AMOS (not inserted in input queue) – the stavText field contains the error description:

- The file with the first signature does not contain the digital signature of this batch
- Error verifying the certificate of the first signature of the batch – the certificate is not from the right CA, is invalid or has been revoked
- The batch is not signed (first signature) by the client's authorised person. The batch is signed by DN: #DN#
- The batch is signed (first signature) using an electronic signature which is not intended for signing batches.
- A batch with this number already exists.
- The batch date is earlier than the current accounting day.

3 Batch not yet processed, protocol is not yet available

2 Batch refused – batch is in state E – refused. The function will return the protocols.

1 Batch processed but some items refused – batch is in state Z – processed. The function will return the protocols.

0 Batch processed, all items received – batch is in state Z – processed. The function will return the protocols.

TXT protocol format

Format of the protocol sent by AMOS.

```
Organisation                 0100
Accounting day               09-04-2011
Number of input data file    000014
Type of input data file      33 AMOS input non-priority
Date of input                09-04-2011
Time of input                12:05:39
Fee band                     3
Number of transactions       000000005
Sum of CZK field amounts     00000100000000400
Error code                   000 - No fatal error
No. of refused transactions  000000000
```
…… followed by a list of errors, if any.

CSV protocol format

The protocol shall contain one or more lines separated by <CR LF> (hex(0D0A)) characters. The lines shall contain the individual parameters separated by semi-colon.

The first line shall contain information about the batch:

```
0100;20110409;14;33;20110409120539;3;5;100000000400;0;0<CR LF>
```

Meaning of individual parameters: Participant code; accounting day; batch number (see data file types in Annex 1 to the Rules); date and time of input in CERTIS; fee band; number of items in batch; sum of amounts in hellers; error code; number of transactions refused on account of formal error[2].

The following lines contain a list of errors, if any (each error on one line):

```
1;43;11;HD;A;110;Batch date is older than 10 days;20110103;Info<CR LF>
```

Meaning of individual parameters: Error serial number; input identification number of item (see Annex 1 to the Rules); item type; field; fatal error (Y/N); error code; error description; value; information

Number of errors in protocol

Unless the batch is refused (i.e. not contains a fatal error), it shall be processed and the protocol shall contain a list of all refused items and information about errors. The CERTIS system shall also return information about a refused item in data form as part of the output data in item of type HD:71 etc.

If the batch is refused (i.e. contains a fatal error), the protocol shall terminate after reaching the 20th fatal error – no subsequent errors shall be listed in the protocol.

8.5. getFromCC function

The getFromCC function shall be used to download the oldest output batch that has not yet been downloaded, with specified priority within the specified accounting day, and the electronic signature of the batch.

In accordance with the combination of the entered parameters (date, priority), it shall download the file with the earliest creation time of those which have yet to be downloaded/received.

It shall be typically assumed that the client application will request receipt of a FROMCC batch at regular intervals (in the order of minutes) without specifying priority. Parallel access of two processes of the client application, one for high and another for low priority (at longer intervals), shall also be enabled.

[2] Formal error means error that does not result in the refusal of the entire batch, but only in the refusal of a single item.

Input parameters of the function

WS	Description
datum	Accounting day – optional. FromCC data for the last 10 calendar days are stored in AMOS.
ucastnik	Participant's numeric code
priorita	Batch priority – optional (H/L)

Output parameters of the function

WS	Description
datum	Accounting day
cislo	Batch serial number
priorita	Batch priority (H/L)
cas	FROMCC creation time
davka	Data pursuant to Annex 1 to the CERTIS Rules – see section 8.1
podpis	Data – electronic signature – see section 8.1
stavKod	Numeric code of the result (0 = FROMCC batch received, other = error code)
stavText	Description of the output state

Functionality

The function checks the entered parameters. It logs information about the processing of the order. The function returns the result code; if the input parameters are error-free and the requested batch exists, it also returns data with output items and the electronic signature. The participant shall verify the validity of the electronic signature of the batch before processing of output items.

Overview of output states
Check upon login:
10 Invalid certificate – the certificate is listed in the CRL
11 Invalid participant code – the participant code is not registered in CERTIS, or it is registered but the participant has yet to be activated
13 Access certificate not registered in AMOS – the participant's commercial certificate is not registered in the AMOS system or is outside the boundaries of its validity registered in AMOS (before start of validity or after end of validity – see AMOS, the form "User maintenance / Users"), or the purpose of the certificate is not WebServices
Accounting day check:
21 Date in future – the date is higher than the current accounting day
Unexpected situation:
99 Unexpected error – if an error other than the above occurs

No batch available:
5 No batch that has not been downloaded is available

A batch that has not been downloaded exists:
0 Batch downloaded

8.6. setFromCC function

This function shall be used to confirm download of an output batch. After the batch is downloaded, it is necessary to confirm that the batch has been downloaded successfully, so that the next batch can be downloaded.

Input parameters of the function

WS	Description
datum	Accounting day
ucastnik	Participant's numeric code
cislo	Batch number

Output parameters of the function

WS	Description
stavKod	Numeric code of the result
stavText	Description of the output state

Functionality

The function checks the entered parameters. It logs information about the processing of the order. The function returns the result code; if the input parameters are error-free and the batch has not yet been marked as downloaded in AMOS, it marks the batch as downloaded (the current system date and AMOS time are saved in the field Download time).

Overview of output states

Check upon login:

10 Invalid certificate – the certificate is listed in the CRL

11 Invalid participant code – the participant code is not registered in CERTIS, or it is registered but the participant has yet to be activated

13 Access certificate not registered in AMOS – the participant's commercial certificate is not registered in the AMOS system or is outside the boundaries of its validity registered in AMOS (before start of validity or after end of validity – see AMOS, the form "User maintenance / Users"), or the purpose of the certificate is not WebServices

Parameter syntax check:

51 Invalid batch number – batch number is zero or higher than 999,999

Unexpected situation:

99 Unexpected error – if a processing error occurs (e.g. a writing error in the table).

Non-existent batch

6 No batch corresponding to the request exists

Batch exists

0 Request processed – the specified output batch has been marked as downloaded where it had not been marked so earlier.

8.7. getBalance function

The getBalance function shall be used to download the current balance of the participant's account. The function returns the opening and current balance of the account and the debit and credit turnover from the start of the day for the specified accounting day.

Input parameters of the function

WS	Description
datum	Accounting day
ucastnik	Participant's numeric code

Output parameters of the function

WS	Description
pocatek	Daily opening balance
debet	Daily debit turnover
kredit	Daily credit turnover
aktualni	Current balance of the account
stavKod	Numeric code of the result (0 = balance downloaded, other = error code)
stavText	Description of the output state

Functionality

The function checks the entered parameters. It logs information about the processing of the order. The function returns the result code; if the input parameters are error-free, it returns the opening balance, the debit turnover, the credit turnover and the current balance for the specified accounting day and participant.

Overview of output states
Check upon login:
10 Invalid certificate – the certificate is listed in the CRL
11 Invalid participant code – the participant code is not registered in CERTIS, or it is registered but the participant has yet to be activated
13 Access certificate not registered in AMOS – the participant's commercial certificate is not registered in the AMOS system or is outside the boundaries of its validity registered in AMOS (before start of validity or after end of validity – see AMOS, the form "User maintenance / Users"), or the purpose of the certificate is not WebServices
Unexpected situation:
99 Unexpected error – if an error other than the above occurs

Non-existent balance
23 Balance not found

Balance exists
0 Balance downloaded

9. Security principles for AMOS users

The Czech National Bank (CNB) pays constant attention to above-average security of the AMOS information system and has implemented modern technology to protect confidentiality and integrity of its assets, as well as the availability and reliability of the entire system. To ensure that batches with items transmitted by the participant's user are undeniable, a guaranteed electronic signature or electronic mark is used.

The CERTIS participant is obliged to pay appropriate attention to risks on the user's part, which stem from the manner of preparation and transmission of batches with items, as well as protection of signature certificates with a private key, the client station and the system environment.

These risks can be mitigated or even eliminated by following the security principles below.

9.1. User's obligations

A user of the AMOS system shall:

a) consistently protect the private key of the certificate for creating the electronic signature or electronic mark from access of persons other than the person to whom it was issued by the certification authority,

b) ensure systemic and physical protection of the private key of the certificate for creating the electronic signature or electronic mark, ideally using technical devices (token, chip card) on a "need-to-have" and "need-to-know" basis, or at least by setting a high level of security, i.e. access only via strong passwords, where the keys are located in secure software storage on the client station and in non-exportable format,

c) protect the client station with anti-virus safeguards, firewalls and other means of protection from malicious software, especially viruses, Trojans, spam, spyware etc.

d) ensure regular updates and maintenance of software, in particular the operating system, web browser and other installed applications,

e) ensure user login to the operating system using a standard user account without administrator rights and using a sufficiently complex password, or using a different mechanism with a corresponding or higher level of security,

f) prevent unauthorised persons from using the computer and above all the AMOS application using appropriate methods, e.g. by logging out or at least locking the computer when the user is absent,

g) not respond to requests by third persons to provide login details (spam, phishing); the login details are only meant for the given user and the CNB never requests them from users under any circumstances,

h) in the event of suspicion that a certificate has been abused, ensure immediate revocation of validity of the electronic signature certificate or login certificate with the relevant certification authority, immediately invalidate the registration of the signature certificate in the CERTIS system, and immediately notify the Cash and Payment Systems Department of the CNB. Contact: certis@cnb.cz, tel.:+420 224 413 355.

9.2. Participant's obligations

A participant of the CERTIS system shall:

a) prevent access of third persons to the private keys of AMOS user certificates,

b) ensure an appropriate level of security of the client computers of AMOS users, especially by using firewalls, anti-virus software and anti-spam software, by systematically seeking out known vulnerabilities, by updating the operating system and installed applications, as well as by restricting access of client stations to Internet addresses with harmful content.

c) ensure systemic and physical protection of the private keys of AMOS users, e.g. by acquiring tokens or chip cards with a secure storage for private keys and certificates.