Czech National Bank

Annex 2
to the CERTIS Rules

Conditions of use of the AMOS web portal and the AMOS/WS, XAMOS and RAMOS application interfaces

Version 15

effective from 19 May 2025

CONTENTS

1 Introduction 4
2 Access to AMOS 5
3 Users and roles 5
3.1 User administrator 6
3.2 Users 6
3.3 Roles 6
4 Signing, signature certificates 8
4.1 Signature certificates 8
4.2 Batches 9
4.2.1 Batches with input items 9
4.2.2 Batches with a certificate 9
4.2.3 Batches with checklists 10
4.3 Instructions to instant payments 10
4.4 Requests for the PaC Register 10
5 Protocols and output files 10
6 Overview of persons in AMOS 11
6.1 Authorised person 11
6.2 User administrator 12
6.3 User 13
7 Procedures 13
7.1 Procedures for ensuring access to AMOS 13
7.2 Procedure for transmitting a batch with a certificate 14
7.3 Procedure for creating and transmitting a batch with items 15
7.4 Procedure for transmitting an external batch with items 15
7.5 Procedure for transmitting an external batch with checklists 16
7.6 Procedure for transmitting files in the Mobility section 16
8 AMOS/WS application interface 17
9 XAMOS application interface and participants' application interface 18
9.1 Web service functions 18
9.2 Communication between XAMOS (CNB) and participants 19
9.2.1 Communication of participants with XAMOS 19
9.2.2 Communication of XAMOS with participants 19

10 RAMOS application interface 20
10.1 Web service functions 20
10.2 Communication between RAMOS (CNB) and participants 21
11 Security principles for AMOS users 22
11.1 User's obligations 22
11.2 Participant's obligations 23

1 Introduction

AMOS is a web portal providing users with interactive access to data from the CERTIS system, application interfaces AMOS/WS, XAMOS and RAMOS and the possibility to transmit and receive data.

In particular, AMOS enables the user to display the participant's current position, manage items in a hold queue, search for items, display the 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, 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, a list of loro accounts and cases of the mobility of the customers, monitor the processing of instant payments and their statistics, input instant payment scheme outages, change the X-limit, monitor profiles, requests and outages in the PaC Register, display documentation and messages for users, administer the participant's contacts and display the participant's log.

Information and procedures for using AMOS are given in Sections 2 to 7. A detailed description of the individual web pages is available in the AMOS User Manual.

AMOS/WS is an application interface enabling the user to transmit a batch with input items for processing, download a protocol on input file processing, download an output file and download information about a participant's current position. A description is given in Section 8.

XAMOS is an application interface enabling the user to transmit and receive instant payments and to enquire about instant payment processing status and system participants and their next unavailability. A description is given in Section 9.

RAMOS is an application interface that allows the use of web services to transmit data to the PaC Register, receive data from the PaC Register, submit queries regarding the status of data in the PaC Register and regarding interruptions of operation in the PaC Register. A description is given in Section 10.

2 Access to AMOS

To use AMOS, you need access to the CNB's communication gateway (signing the Agreement on access through the CNB's communication gateway), a supported version of the Windows operating system and the **Microsoft Edge** or **Google Chrome** internet browser in the latest version. The AMOS application can be accessed at:

AMOS web	Server name	IP address	Production environment
Primary	wsg.cnb.cz	193.84.144.108	https://wsg.cnb.cz/amos/
Secondary	wsh.cnb.cz	193.84.144.109	https://wsh.cnb.cz/amos/

The Wsg and wsh servers are used both for login by name and password and for login by certificate. A commercial certificate issued by an accredited certification authority must be used. The certificate must be registered in AMOS by a user administrator as an access (login) certificate, and its purpose of use must be for interactive access. Communication with the server on which AMOS is running at the CNB is secured using a certificate (server security certificate) issued specifically for a particular server. This certificate was issued by the DigiCert certification authority.

Where the user needs to sign batches or paste files in the Mobility section or sign these files when using AMOS, support for work with qualified certificates for batch signing shall be installed.

Test environment

The AMOS test environment is located on separate servers with similar architecture.

AMOS web	Server name	IP address	Test environment
Primary	wsctest.cnb.cz	193.84.144.122	https://wsctest.cnb.cz/amost/
Secondary	wsdtest.cnb.cz	193.84.144.125	https://wsdtest.cnb.cz/amost/

3 Users and roles

AMOS users shall be specified employees of CERTIS participants. 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/she 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 and manage the participant's contacts. The user administrator shall log into AMOS using a public certificate.

The user administrator is obliged to reconcile the participant's accounts, sign the certificates and review the roles of the operators and contact details of the participant at least on an annual basis.

The identification data of a user administrator (especially the unique name of his certificates) shall be transmitted by the participant in writing using the "Identification of the CERTIS participant's user administrator" form, 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 public certificate.

For AMOS login using a certificate, the operator shall only allow the use of public certificates issued by accredited providers of certification services: Česká pošta, s. p., První certifikační autorita, a. s., and eIdentity a.s. The use of certificates issued by other authorities shall be agreed in advance. For use in AMOS, 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 AMOS 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 information to be viewed. Active roles shall enable data input and administration of processing. Passive roles are OBC, OPR, FIN, XFI and XMR.

Overview of AMOS roles

Code	Role designation	Description
OBC	General information	displaying 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	displaying 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	displaying 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 and 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, with a certificate or with a checklist), 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 batches CPL, CPR and SP4, administration of external batches, transmission of external batches
MOB	Switching	the user has access to the administration of Mobility section cases

Code	Role designation	Description
XFI	Financial information of the IP	displaying information on the participant's status and position (current position, searching for instant payments, reporting of A-limit, maintenance of X-limit)
XMR	Monitoring and reporting of the IP	displaying information on instant payment monitoring and reporting, monitoring of availability of instant payment scheme
XLI	Maintenance of X-limit	maintenance of X-limit, reporting A-limit
XOD	Interruptions of operation of IP	reporting and monitoring instant payment scheme interruptions of operation
PNK	Pay a Contact	displaying and monitoring profiles, requests and interruption of operation status

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 Signing, signature certificates

4.1 Signature certificates

For signing batches, instruction to instant payments or the files in the Mobility section, and for inserting and deleting profiles in the PaC Register in AMOS, 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 eIdentity a.s. The use of certificates issued by other authorities shall be agreed in advance. For use in AMOS, it is recommended that the certificate be designated as public.

The signature certificate is registered in AMOS with a specific purpose. The specific purposes are divided into Certificates, Transactions, Checklists, Mobility and Pay a Contact. The signature certificate with the purpose "Certificates" is registered for an authorised person.

The participant's signature certificates shall be administered by a user administrator. The unique name of the signature certificate for the purposes of Certificates, Transactions, Checklists, Mobility and Pay a Contact 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 AMOS. The signature certificate shall be registered in the CERTIS system and assigned a unique code. The signature certificate may be revoked in AMOS at any time.

4.2 Batches

A batch shall consist of a file containing the data and one or two files containing the electronic signature of the former file. AMOS 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 provided with an advanced electronic signature (seal) based on the qualified certificate, which is in accordance with the ETSI TS 101 733 standard at the CADES BES level.[1] The signature shall be verified by the CERTIS system using the qualified certificate of the person signing. If the employee signing the data signs outside AMOS, he/she shall not be required to have access to AMOS.

4.2.1 Batches with input items

A batch with items shall contain the participant's input items in the CERTIS system and shall be provided with an advanced electronic signature (seal) based on the qualified certificate, which is registered with the purpose "Transaction". 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 or seals using the "Specification of the number of signatures of an input batch with items in the CERTIS system" form.

4.2.2 Batches with a certificate

A batch with a certificate registers the unique name of a qualified certificate for signing batches with items (purpose "Transactions"), for signing an instruction to conduct an instant payment (purpose "Transactions"), for signing batches with checklists (purpose "Checklists"), for signing files in the Mobility section (purpose "Mobility") or for signing the insertion or deletion of a profile (purpose "Pay a Contact"). The batch shall be signed in AMOS and will

[1] The rules can be found at http://webapp.etsi.org/WorkProgram/SimpleSearch/QueryForm.asp, with the possibility to search for keywords via http://pda.etsi.org/pda/queryform.asp.

be provided with an advanced electronic seal based on the qualified certificate, which is registered with the purpose “Certificates”. The unique name of such a certificate is registered by the operator after the “Specimen signature and specimen electronic signature of an authorised person of a participant in the CERTIS payment system” form is delivered.

4.2.3 Batches with checklists

A batch with a checklist shall either contain a checklist of beneficiaries or a checklist of payers. The batch shall be provided with an advanced electronic signature based on the qualified certificate, which is registered with the purpose “Checklists”. The unique name of such a certificate shall be transmitted to the operator in a batch with the certificate.

4.3 Instructions to instant payments

Instant payment orders have to be provided with an advanced electronic seal based on the qualified certificate, which is registered with the purpose “Transactions”. The unique name of such a certificate shall be transmitted to the operator in a batch with the certificate.

4.4 Requests for the PaC Register

Requests to insert or delete profiles in the PaC Register shall be provided with an advanced electronic seal based on the qualified certificate, which is registered with the purpose “Pay a Contact”. The unique name of such a certificate is transmitted to the operator in a batch with the certificate.

5 Protocols and output files

Protocols on the processing of input files, output files, instant payments, electronically transmitted dispatch notes[2] and replies of the (multiple) account number query function from the PaC Register are provided with an advanced electronic seal based on the qualified certificate of the CERTIS system. The certificate to verify the CNB’s electronic seal was issued by Czech Post’s certification authority PostSignum:

[2] Dispatch notes are transmitted with the data files in cases where an alternative means of transmitting and receiving of data files is used pursuant to Annex 4 to the CERTIS rules.

Subject serialNumber=S16676,CN=Systém CERTIS,OU=Sekce informatiky,O=Česká národní banka,OrganizationIdentifier=NTRCZ-48136450,C=CZ

Issuer PostSignum Qualified CA 4

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

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

Test environment

The certificate to verify the CNB's electronic seal was issued by Czech Post's certification authority PostSignum:

Subject serialNumber=S16676,CN=Systém CERTIS TEST,OU=Sekce informatiky,O=Česká národní banka,OrganizationIdentifier=NTRCZ-48136450,C=CZ

Issuer PostSignum Qualified CA 4

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 seal for signing batches with items, batches with checklists or for signing files in the Mobility section,
- persons authorised to sign written (fax) orders,
- number of signatures, seals of an input batch with items in AMOS,
- involvement of the participant in the instant payment scheme,
- registration of the participant in the PaC Register.

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

- name and contact information,
- unique name of the signature certificate (qualified certificate) used for the 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,
- updating the contact list in AMOS.

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

- name and contact information,
- unique name of the access certificate (public 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 AMOS according to assigned roles.

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

- name,
- login method,
- unique name of the access certificate (public 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 "Specimen signature and electronic specimen signature of the CERTIS participant's authorised person" form	
	Registration of authorised persons, especially the unique names of signature certificates
Specification of user administrators The "Identification of the CERTIS participant's user administrator" form signed by an authorised person	
	Registration of user administrators, especially the unique names of public 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.

7.5 Procedure for transmitting an external batch with checklists

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

The input data file shall be registered in CERTIS.

7.6 Procedure for transmitting files in the Mobility section

Action in AMOS	Performed by
Establishment/administration of the case in the Mobility section	Any user (role MOB)
Insert the file into the case	Any user (role MOB)
Signing of the file	Any user (role MOB)
Transfer of the case	Any user (role MOB)

Mobility cases are registered in AMOS.

8 AMOS/WS application interface

Web Services (AMOS/WS) as an extension of AMOS 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 the processing of INTOCC batches,
- function for downloading output FROMCC batches,
- function confirming download of FROMCC batches and
- function for downloading the current balance on the participant's account with information about the status of the X-limit and the A-limit of the instant payment scheme participants.

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

Access shall be conditional on user registration in AMOS with access using a public certificate with the purpose set to WebServices (the same purpose as for connection to XAMOS). 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 interface is secured via a server certificate issued exclusively for the "amoswstest.cnb.cz" and "amosws.cnb.cz" servers. These certificates were issued by the DigiCert certification authority.

Xsd and wsdl definition files and the "AMOS/WS – technical specification" technical documentation shall be available in AMOS.

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

9 XAMOS application interface and participants' application interface

Web services for the instant payment scheme provide an A2A (application-to-application) interface for transmitting and receiving instant payments and enquiring about the payment status and receiving information about scheme participants and their unavailability.

The operator informs participants about planned unavailability and outages of the XAMOS application interface by e-mail using the contacts in the "Instant payments – Technical matters" category.

9.1 Web service functions

The instant payment scheme contains two core web services, which contain the following functions:

- InstantPaymentXamosService – the CNB's web service
  - **initInstantPayment** – function for initialising instant payments,
  - **getStatusForDebtor** – function for the payer's bank to enquire about instant payment status,
  - **getStatusForCreditor** – function for the beneficiary's bank to enquire about instant payment status,
  - **getParticipants** – function for enquiring about system participants and their next unavailability,
- InstantPaymentParticipantService – the participant's web service,
  - **checkInstantPayment** – function for testing the feasibility of an instant payment in the case of the beneficiary's bank,
  - **informCreditor** – function for deciding to approve/reject an instant payment sent to the beneficiary's bank,
  - **informDebtor** – function for deciding to approve/reject an instant payment sent to the payer's bank,
  - **Ping** – function for checking a participant's availability.

The xsd and wsdl definition files for instant payments and the “Instant payments – technical specification” technical documentation are available in AMOS (in the “Various”, “Instant Payments” section).

9.2 Communication between XAMOS (CNB) and participants

Access to the CNB’s communication gateway is required for the use of XAMOS. The transport protocol is the https protocol with obligatory client authentication using commercial certificates issued by accredited certification authorities (1. CA, Czech Post’s PostSignum and eIdentity).

9.2.1 Communication of participants with XAMOS

Access is conditional on user registration in AMOS with access using a commercial certificate with the purpose set to WebServices (the same purpose as for access to AMOS/WS).

The URLs and relevant IP addresses of the CNB’s servers for the InstantPaymentXamosService web service are listed in the following table:

Environment	**CNB’s IP address Port**	**URL**
Test	193.84.144.116 tcp/4001	https://xamostest.cnb.cz:4001/Xamos/XamosPort
Production	193.84.144.117 tcp/4001	https://xamos.cnb.cz:4001/Xamos/XamosPort

Participants’ communications with the server on which the XAMOS application interface is running at the CNB are secured using a server security certificate issued specifically for the “xamostest.cnb.cz” and “xamos.cnb.cz” servers. These certificates were issued by the DigiCert certification authority.

Participants call the InstantPaymentXamosService web service from their IP address which falls within the range of addresses stipulated in the Agreement on access through the CNB’s communication gateway.

9.2.2 Communication of XAMOS with participants

The URL and IP address of the participant’s server on which the InstantPaymentParticipantService web service is available are specified by the participant on the “Registration of a direct participant of the CERTIS system in the instant payment

scheme" form. This IP address must fall within the range of addresses stipulated in the Agreement on access through the CNB's communication gateway.

XAMOS calls the InstantPaymentParticipantService from the IP addresses listed in the following table.

Environment	**CNB's IP address** **Ports**
Test	193.84.144.145 tcp/443, 1024-9999
Production	193.84.144.146 tcp/443, 1024-9999

10 RAMOS application interface

Web services for operating the PaC Register provide an A2A (application-to-application) interface for transmitting data to the PaC Register, receiving data from the PaC Register, enquiring about the status of data in the PaC Register and about the unavailability of the PaC Register services.

The operator usually informs participants about planned unavailability and outages of the PaC Register web services by e-mail using the contacts in the "Register – Technical matters" category.

10.1 Web service functions

The web services include the following functions for communication with the PaC Register:

- dotazCu (dotazCuMulti) – enquiring about an account number (or multiple account numbers)
- vlozeniProfilu – insert profile, renew profile
- seznamTc – list of telephone numbers
- odstraneniProfilu – delete profile
- ziskaniTc – obtaining telephone numbers
- dotazNaOdstavku – enquiring about planned unavailability
- dotazNaProfil – obtaining profile information
- dotazNaZmenuProfilu –request to change profile status

- dotazBanka – enquiring about the existence of a profile

The xsd and wsdl definition files for communication with the PaC Register and the "PaC Register – technical specification" technical documentation are available in AMOS (in the "Various", "Pay a Contact" section).

10.2 Communication between RAMOS (CNB) and participants

Access to the CNB's communication gateway is required for the use of RAMOS. The transport protocol is the https protocol with obligatory client authentication using commercial certificates issued by accredited certification authorities (1. CA, Czech Post's PostSignum and eIdentity).

Access is conditional on user registration in the AMOS system with access using a commercial certificate with the purpose set to WebServices (the same purpose as for access to AMOS/WS).

The URLs and the relevant IP addresses of the CNB's servers for the PnmImplService web service are listed in the following table:

Environment	**CNB's IP address Port**	**URL**
Test	193.84.144.148 tcp/5001	https://ramostest.cnb.cz:5001/Ramos/RamosPort
Production	193.84.144.149 tcp/5001	https://ramos.cnb.cz:5001/Ramos/RamosPort

Participants' communications with the server on which the RAMOS web service is running at the CNB are secured using a certificate (server security certificate) issued specifically for the "ramostest.cnb.cz" and "ramos.cnb.cz" servers. These certificates were issued by the DigiCert certification authority.

Participants call the PnmImplService web service from their IP address which falls within the range of addresses stipulated in the Agreement on access through the CNB's communication gateway.

11 Security principles for AMOS users

The Czech National Bank (CNB) pays constant attention to the above-average security of AMOS and has implemented modern technology to protect the confidentiality and integrity of its assets, as well as the availability and reliability of the entire system. A recognised electronic signature or electronic seal is used to ensure the non-repudiation of batches with items transmitted by the participant's user.

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 the 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.

11.1 User's obligations

A user of AMOS shall:

a) consistently protect the private key of the certificate for creating the electronic signature or electronic seal 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 seal, 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 AMOS 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 electronic seal or login certificate with the relevant certification authority, immediately invalidate the registration of the signature certificate in the CERTIS system, and immediately notify the CNB (see section 11.2 point d).

11.2 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.

d) if a possible security incident/event is suspected, contact the CNB immediately by e-mail at csirt@cnb.cz and certis@cnb.cz or by telephone at the contact numbers +420 224 418 135, +420 224 418 128 or +420 224 413 355 and provide the CNB with full cooperation in resolving the situation.