**Czech National Bank**

**Annex 2**
to the CERTIS Rules

# Conditions of use of the AMOS web portal and the application interface of the AMOS/WS and the XAMOS

**Version 12**

**effective from 1 March 2020**

# CONTENTS

1 Introduction ..... 3
2 Access to AMOS ..... 3
3 Users and roles ..... 4
3.1 User administrator ..... 4
3.2 Users ..... 5
3.3 Roles ..... 5
4 Signing, signature certificates ..... 7
4.1 Signature certificates ..... 7
4.2 Batches ..... 7
4.2.1 Batches with input items ..... 8
4.2.2 Batches with a certificate ..... 8
4.2.3 Batches with checklists ..... 8
4.3 Instructions to instant payments ..... 9
5 Protocols and output files ..... 9
6 Overview of persons in AMOS ..... 10
6.1 Authorised person ..... 10
6.2 User administrator ..... 10
6.3 User ..... 11
7 Procedures ..... 11
7.1 Procedures for ensuring access to AMOS ..... 11
7.2 Procedure for transmitting a batch with a certificate ..... 12
7.3 Procedure for creating and transmitting a batch with items ..... 13
7.4 Procedure for transmitting an external batch with items ..... 13
7.5 Procedure for transmitting an external batch with check-list ..... 14
7.6 Procedure for transmitting files in the menu Mobility ..... 14
8 AMOS/WS application interface ..... 15
9 XAMOS application interface and participants' application interface ..... 16
9.1 Web service functions ..... 16
9.2 Communication between XAMOS (CNB) and participants ..... 17
9.2.1 Communication of participants with XAMOS ..... 17
9.2.2 Communication of XAMOS with participants ..... 18
10 Security principles for AMOS users ..... 18
10.1 User's obligations ..... 19
10.2 Participant's obligations ..... 20

# 1 Introduction

AMOS is a web application providing interactive access to data from the CERTIS system and the possibility to transmit and receive data.

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, cases of the mobility of the customers, to monitor the processing of instant payments and their statistics, input the interruption of operation of the instant payment scheme, change the X-limit, 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 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 to transmit and receive instant payments and to enquire about instant payment processing status and system participants and their nearest unavailability. A description is given in Section 9.

# 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 | 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/ |

Wsg server and wsh server 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 the AMOS application is running at the CNB is secured using a certificate (server security certificate) issued specifically for particular server. This certificate was issued by DigiCert certification authority.

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

**Test environment**

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

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 and manage the participant's contacts. The user administrator shall log in the AMOS system using a public certificate.

The user administrator is obliged to perform reconciliation of the participant´s accounts, signing of the certificates, review roles of the operators and contact details of the participant on annual basis at minimum.

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 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 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 are OBC, OPR, FIN, XFI and XMR.

**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, 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 batch CPL, CPR and SP4, entry of external batches, transmission of external batches |
| MOB | Switching | the user has access to the administration of menu Mobility |
| XFI | Financial information of the IP | viewing of 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 | viewing of information on instant payment monitoring and reporting, monitoring of availability of instant payment scheme |

| Code | Role designation | Description |
|---|---|---|
| XLI | Maintenance of X-limit | maintenance of X-limit, reporting of A-limit |
| XOD | Interruptions of operation of IP | reporting and monitoring of instant payment scheme interruptions of operation |

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 menu Mobility 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 signature certificate is registered in the AMOS System with the specific purpose. The specific purposes are devided to Certificates, Transactions, Check-lists, Mobility. Signature certificate with the purpose Certificates is registered for authorised person.

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.

## 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. 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, which is in accordance with the standard ETSI TS 101 733 in the level CADES BES. 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.

### 4.2.1 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 registered qualified certificate 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 using the form "Specification of the number of signatures of an input batch with items in the CERTIS system".

### 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 instruction to instant payment (purpose "Transactions"), for signing batches with checklists (purpose "Check-lists"), or for signing files in the menu Mobility (purpose "Mobility"). The batch shall be signed using a registered qualified certificate with the purpose "Certificates". The unique name of such a certificate is registered by the operator after the form "Specimen signature and specimen electronic signature of an authorised person of a participant in the CERTIS payment system" is delivered.

### 4.2.3 Batches with checklists

A batch with checklist shall contain either checklist of beneficiaries or checklist of payers. The batch shall be signed using a registered qualified certificate with the purpose "Check-lists". The unique name of such a certificate shall be transmitted to the operator within a batch with certificate.

### 4.3 Instructions to instant payments

Instant payment orders have to be mark by the guaranteed electronic seal with using 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 a certificate.

## 5 Protocols and output files

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

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

**Issuer** PostSignum Qualified CA 2

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 category Technical matters.

**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 [IČ 48136450],OrganizationIdentifier=NTRCZ-48136450,C=CZ

**Issuer** PostSignum Qualified CA 2

[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.

# 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 check-lists or for signing files in the menu Mobility,
- persons authorised to sign written (fax) orders,
- number of signatures of an input batch with items in AMOS,
- registration of the participant to the instant payment scheme.

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,
- actualisation of the contact list in the AMOS System.

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 (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 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 (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<br>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<br>The form “Identification of the CERTIS participant’s user administrator” signed by an authorised person | |
| | Registration of user administrators, especially the unique names of public certificates |
| Registration of users, assignment of roles<br>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 check-list

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

The input data file shall be registered in CERTIS.

## 7.6 Procedure for transmitting files in the menu Mobility

| Action in AMOS | Performed by |
|---|---|
| Estabilishment/administration of the case in the menu Mobility | 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) |

The case of the Mobility is registred in the AMOS system.

# 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 with the information about the high of the X-limit and the A-limit of the participant of the instant payment scheme.

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 the AMOS application.

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

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

# 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 downtime of the XAMOS scheme by e-mail using the contacts in the category Instant payments – Technical matters.

## 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 nearest unavailability,
- InstantPaymentParticipantService – the participant's web service,
    - **checkInstantPayment** – function for testing the feasibility of an instant payment with 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 technical documentation "Instant payments – technical specification" are available in AMOS (in the "Various" menu, "Instant Payments" section).

## 9.2 Communication between XAMOS (CNB) and participants

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 e-Identity).

### 9.2.1 Communication of participants with XAMOS

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 relevant IP addresses of the CNB'S servers for the InstantPaymentXamosService web service are listed in the following table:

| **Environment** | **IP address of ČNB 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 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** | **IP address of ČNB**<br>**Ports** |
|---|---|
| Test | 193.84.144.145<br>tcp/443, 1024-9999 |
| Production | 193.84.144.146<br>tcp/443, 1024-9999 |

# 10 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 seal 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.

## 10.1 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 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 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 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 Risk Management and Transactions Support Department of the CNB. Contact: certis@cnb.cz, tel.: +420 224 413 355.

## 10.2 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.