

EXCHANGE REGULATION

COMMUNICATION CONNECTION OF PXE PARTICIPANTS

PART 1 – GENERAL PROVISIONS

Article 1

Subject of regulation

This part of the implementing regulation governs the conditions for on-line electronic data communication between POWER EXCHANGE CENTRAL EUROPE, a.s. (hereinafter “PXE” or “the Exchange”) and PXE participants and clearing participants. This part does not, however, concern communication in relation to trading on the Hours Auction with place of delivery registration in Hungary, if the PXE participant accesses this Auction through the internet interface managed by EXAA. This part of the implementing regulation also applies as appropriate to clearing participants’ communication connection. This part is also used for connection to the Trayport trading system, unless the nature of the issue indicates otherwise.

Article 2

Definitions

Data communication of PXE participants means electronic data communication used to transfer orders, data and information about exchange operations in the Trading System¹. Data communication takes place via PXE communication system and front-end module. The PXE communication system means a set of hardware and software resources used for data communication. The PXE communication system is divided into central communication system, communication environment and participant communication system.

Central communication system means a part of the PXE communication system located in the premises of PXE. The central communication system is connected to the central computer servers of PXE.

Communication environment means a part of the PXE communication system used for connection of the central communication system with the participant communication system.

Participant communication system means a part of the PXE communication system located in the office or premises of a PXE participant. Participant communication system is owned and fully managed by PXE participant.

Front-end module means a program module used by PXE participant for exchange trading or entering of instructions for settlement. The front-end module is installed and operated by PXE participant and located in his premises.

¹ As defined in the Trading Rules

Communication Connection

Communication server means software supplied by PXE that provides for exchange of data and information between the front-end module and central computer servers of PXE. The communication server is installed on the PC of the PXE participant.

Production environment means a separated logic area of the PXE central computer server storing actual trading data and current software versions and processing daily data in the Trading System. (E.g., testing environment storing data and software for the purpose of testing is different.)

Article 3

Technical description of the participant communication system

Basic technical description of supported types of participant communication system is provided in Appendix 2.

Participant communication system is connected to the central communication system via communication environment defined in Appendix 1 and also to LAN or to PC of the PXE participant.

Participant communication system is fully managed by PXE participant.

PXE communication system interface to the customer is defined (terminated) by the interface between the central communication system and the communication environment.

Article 4

Installation of the participant communication system

Interface for participant communication system in the central communication system is provided to PXE participant upon a written request addressed to PXE. Template of a request under paragraph 1 is provided in Appendix 3.

PXE participant is obliged to procure installation, configuration and management of participant communication system at its own cost.

For the purpose of the participant communication system of the “VPN standalone client” type PXE supplies to PXE participants software, installation instructions and hardware with access PIN for client authentication.

For the purpose of the participant communication system of the “Site to Site LL” type PXE shall provide basic requirements for parameters and configuration of the communication equipment in the participant communication system.

For the purpose of the participant communication system “Site to Site VPN” PXE shall provide basic requirements for parameters and configuration of the communication device in the participant communication system.

PXE participant is obliged to keep secret the provided authentication information for participant communication system. In case of a theft of the provided PIN of the hardware, PXE participant is obliged to change the PIN of the hardware using the supplied software. In case of a loss or theft of the hardware, the PXE participant is obliged to notify PXE and PXE shall immediately prevent its further use for client authentication. If the PIN is lost or forgotten, the entity is obliged to deliver hardware to PXE for generation of a new PIN.

PXE is not responsible for installation and is not liable for damage incurred by PXE participant due to incorrect installation of the participant communication system.

Prior to installation, PXE participant is obliged to obtain the communication environment according to its choice, at its cost from the respective operator of such environment.

Article 5

Conditions of communication system operation

PXE participant is obliged to pay to the Exchange the fee for connection to the PXE communication system according to the PXE Fee Schedule.

The communication system may only be operated in accordance with the rules defined by PXE.

Communication Connection

PXE is not authorised to make any changes in the communication system and to use it for purposes different from those stipulated in this part of the PXE rules. In case of damage or abuse of the communication system, the PXE participant is obliged to compensate the damage incurred by PXE.

In case of an attempt of PXE participant for an unauthorised access to AOS or to the PXE system using other methods than profiles assigned by PXE, defined data interface, the trading day manager is authorised to disconnect the participant communication system of such PXE participant from the central communication system until further procedure is decided by the respective PXE authorities.

In case of suspension of PXE participation, the PXE participant's participation in the PXE communication system is suspended. PXE participant is obliged to continue paying the fee stipulated in paragraph 1.

In case of termination of PXE participation, PXE is authorised to cancel the interface for connection of participant communication system.

Article 6

Options of connection on the application layer

There are two potential ways of connecting the front-end module to AOS on the application level:

via PXE Communication Software and ODBC interface

via Web services based interface

Methods under item (1) are absolutely independent on the type of participant communication system (see Appendix 2)

In case of connection according to item (1a), the PXE participant provides for the Front-end module. PXE supplies only the Communication server. The participant is entitled to one application connection for the basic fee according to PXE Fee Schedule.

In case of connection under item (1b), the Front-end module (PXE Monitor) is provided by PXE, but the participant may acquire it itself. The participant is entitled to two parallel application connections for the basic fee according to PXE fee tariff.

In case of connection under item (1b), PXE supplies the hardware with the access PIN for client authentication. Use is similar to Article 4, paragraph 5.

PXE participant is obliged to arrange installation of PXE software (PXE Monitor or Communication server) on his own according to the instructions supplied by the Exchange. PXE supplies new versions to PXE participants and PXE participant is obliged to have proper installation arranged (installation is automatic in case of PXE Monitor).

PXE is not responsible for installation of the supplied software and its new versions. PXE is not liable for damage incurred by PXE participant due to incorrect installation.

PXE participant is obliged to report function defects of the supplied software to the Exchange.

Article 7

Additional connections of PXE participants

Participant may be simultaneously connected to PXE via multiple application or communication connections.

PXE offers several solutions of the need for additional connection of participants:

Possibility to use additional application connection. This means the participant may be connected to PXE simultaneously via two or more installations of communication server under article 6, paragraph 1a) or via three and more installations of the front-end module under article 6, paragraph 1b).

Possibility to use additional communication and application connection. This means the participant may be simultaneously connected to PXE via multiple communication connections and thus also application connections.

Communication Connection

Possibility of additional connection to AOS. The participant has the option to ask for another (second) access to the AOS trading system (new participant code). This solution is suitable for double access to AOS with separated data.

PXE participant is obliged to pay PXE fees for use of additional connection according to PXE Fee Schedule.

Participant files the application for additional connection using the attached forms (Appendix 3 – communication connection, Appendix 4 – application connection).

Provisions hereof shall apply to technical description, operation, installation and uninstallation, service and defect procedure of additional connection accordingly.

Article 8 **Service of the PXE communication system**

The responsibility of PXE for PXE communication system does not go beyond the interface of the central communication system and the communication environment.

PXE is not responsible for service of communication environment and does not provide for it.

PXE provides service only on the part of the PXE communication system it is responsible for.

PXE may provide service also via third party.

Service terms and conditions are publicised in the PXE Bulletin.

Article 9 **Procedure in case of a failure in the PXE communication system**

As regards the participant communication system, PXE provides to PXE participants service consultations to identify the cause and to diagnose the potential fault. The method of providing consultation is announced in the PXE Bulletin.

PXE may provide service also via third party.

In the event that a fault is identified on the communication environment, PXE participant is obliged to contact the respective provider of the environment and arrange for its remedy.

In the event that a fault is identified on the central communication system, PXE is obliged to remedy the fault without undue delay.

In the event that a fault is identified in the communication software, PXE is obliged to remove the fault without undue delay.

Article 10 **Liability for damage**

PXE is not liable for any damage incurred by PXE participant or other persons due to a fault of the participant's communication system or faults in the communication server or front-end module and the resulting loss or leakage of data,

an unauthorised manipulation of the communication system, communication server or front-end module or abuse by PXE participant or another person,

a breach of obligations stipulated by generally binding legal regulations, PXE regulations or PXE rules.

PART 2 – SPECIAL PROVISIONS FOR TRADING UNDER AN HOURS AUCTION

Article 11

Subject of regulation

This part of the implementing regulation governs the conditions of on-line electronic data communication between PXE and trading participants in relation to trading on the Hours Auction with place of delivery registration in Hungary, if the trading participant accesses this Auction through the internet interface managed by EXAA.

Article 12

Technical description of the participants communication system

1. Access to AOS is provided through the internet and an internet browser. AOS is understood to be the trading system operated by EXAA, which is located outside the Exchange's registered office and within which exchange trades can be concluded on the Hours Auction with place of delivery registration in Hungary.
2. For the authentication of the connection, participants are given an RSA key. Should a trading participant so request, the Exchange will assign the trading participant multiple RSA keys.
3. Internet connection is secured by each trading participant at its own expense.
4. The minimum required configuration on the part of the trading participant is:
MS Internet Explorer 5.0

or Netscape 6.0.
5. A PXE participant is obliged to keep secret the delivered authentication data for access to AOS. In case of theft of a delivered PIN on a hardware medium, the PXE participant is obliged to change the PIN on the HW medium by means of the delivered software. In case of theft or loss of the HW medium itself, the PXE participant is obliged to inform PXE of such fact and PXE shall immediately disable its further use for client authentication. Should the participant lose or forget the PIN, the entity is obliged to deliver the HW medium to PXE, which shall generate a new PIN.
6. PXE is not responsible for damage incurred by a trading participant due to incorrect use of AOS, the internet interface for access to AOS, or the issued RSA key (hereinafter for the purposes of this part referred to as the "communication system").

Article 13

Conditions of the participants communication system operation

1. The trading participant is obliged to pay the Exchange a fee for connection to the system for the Hours Auction with place of delivery in Hungary according to the PXE Fee Schedule.
2. The communication system may be used only in accordance with the rules set by the Exchange. Trading participants are not entitled to use the communication system for purposes other than those listed in the Exchange regulations. If the participant damages any part of the communication system, the participant is obliged to compensate the Exchange for the damage incurred.
3. If the trading participant attempts to access the Trading System without authorization or in a manner other than that established, the exchange day manager is entitled to block such participant's access to the Trading System until such time as the relevant PXE authorities decide on further steps to take.
4. In case of suspension of participation at the Exchange, the trading participant's participation in the communication system also is suspended. The trading participant remains liable during such time to pay the fee referred to in paragraph 1.

5. In case of termination of participation at the Exchange, the Exchange deactivates the trading participant's access to AOS and the participant is obliged to return to the Exchange the RSA keys with which it was entrusted.

Article 14

Procedure in case of a failure in the PXE communication system

1. The Exchange provides trading participants with service consultancy as regards the communication system to determine the cause and diagnosis of a possible failure. The manner in which the consultancy is provided is announced in the PXE Bulletin.
2. PXE also provides service through an authorised company.
3. If a failure is detected in the communication environment, the PXE participant is obliged to contact the respective provider of this environment and secure its repair.
4. If a failure is detected in the central communication system, PXE is obliged to remove the failure without undue delay.
5. If a failure is detected in the communication software, PXE is obliged to remove the failure without undue delay.

Article 15

Liability for damage

1. PXE is not liable for any damage incurred by the PXE participant or other entities due to unqualified handling of the communication system or misuse of the trading participant's access by another person or entity.

PART 3 – SPECIAL PROVISIONS FOR TRADING IN THE TRAYPORT SYSTEM

Article 16

Subject of regulation

This part of the implementing regulation governs the conditions of on-line electronic data communication between PXE and trading participants in relation to the Trayport system.

Article 17

Article 18 TRAYPORT trading system

1. For connection to the Trayport trading system the trading participant will obtain the special front-end trading module "GlobalVision Exchange Trading System" (hereinafter referred to as the "Trayport client"), which the trading participant installs on the computers within its computer network at its own expense.
2. For the Trayport client's data connection, the trading participant will use the communication environment under Article 2 of Appendix 1 and exclusively the participant's communication system under Article 4 of Appendix 2.
3. The Trayport client is supplied to the trading participant, and data connection is enabled for the trading participant on the basis of its request submitted to PXE in the format of its choice. The trading participant shall inform PXE in particular of the IP address referred to in Article 2 of Appendix 1.
4. The trading participant is entitled to use the Trayport client only if it has previously concluded a licence agreement (Electronic Clickwrap Licence – End User Agreement) with the company Trayport Limited, Company ID No. 02769279, with registered office at 4th Floor Rose Court, 2 Southwark Bridge Road, London, SE1 9HS, and then under the conditions stipulated in this

licence agreement. The trading participant is obliged to bar access to the Trayport client by unauthorised persons or entities and to ensure that its employees or persons having a similar relationship to the trading participant adhere to the conditions of this licence agreement.

5. The Exchange has the right to conduct an inspection as to whether the trading participant is using the Trayport client properly in accordance with the conditions of the licence agreement. The trading participant is obliged to provide the Exchange the co-operation necessary for this purpose.

PART 4 – FINAL PROVISIONS

Article 19

Effectiveness

This Regulation was approved by the Exchange Chamber on 15 September 2011 and shall come into effect on 1 October 2011.

Appendix 1

Communication environment

PXE participant has the option of the following communication environment.

1. Digital line

This communication environment is used for participant communication system of the type “Site to Site LL”.

Participant’s digital line is added as “timeslot” to the central structured circuit E1 on the PXE side. In order to increase availability, the Participant may use two access lines which may be separated to two independent E1 circuits to two separate central locations on the PXE side.

Operator of central data lines E1 : TELEFONICA O2 CZECH REPUBLIC

(Local operator of digital lines of the participant should agree with Telefonica O2 on termination of digital circuits in those E1)

| | |
|-----------------------------------------------------------|-------------------------------------------------|
| Recommended access speed | 128 kb/s – 256 kb/s |
| Modem interface | V.35 or X.21 – by type of router interface |
| Location of opposite end station | BCPP, a.s, merged circuit 2 Mbps (E1) |
| Identification of merged line (E1) of the Exchange | Praha 1, Rybná 14 PH-PH30N737, or PH-PH30N728 |
| Identification of backup merged line (E1) of the Exchange | Praha 1, Václavské náměstí 42 PH-PH30N730053 |

2. Internet

This communication environment is used for participant communication system of the type “VPN Standalone Client”, “Site to site VPN”, or “Internet Direct”.

In case of Internet communication environment, a part of the participant communication system connected to the Internet must have assigned a permanent IP address in the Internet network. The IP address must be provided to PXE prior to installation or its potential change. PXE shall notify the participant of the IP address of the PXE communication gate in the Internet network after application for installation has been filed.

| | |
|--------------------------|---------------|
| Recommended access speed | min. 512 kb/s |
|--------------------------|---------------|

Considering the character of the communication environment, availability and response time is not guaranteed.

Potential exceptions are approved by PXE general secretary.

Appendix 2

Basic technical description of the supported types of participant communication system

1. Site to Site LL

The transfer channel is realised by data connection between private networks of PXE and PXE participant. This is secured by PXE central router and participant router. Central routers are connected to the PXE central network with exchange servers AOS. Participant router is connected to the participant's network to which computers with front-end module are also connected.

Central routers are interconnected with the participant router by a digital line (Communication environment according to Appendix 1, article 1).

TCP/IP is the network protocol. Application connection is secured via TCP/IP protocol.

Network IP address of the participant's computer is assigned by PXE. IP address transfer (NAT/PAT) is possible, but participant computers must present themselves with the assigned IP address to the network towards PXE. Participant IP addresses are assigned from IP address ranges not used in the Internet (RFC 1918).

In normal situations, both central AOS servers are accessible for the participant via all IP line connections of the communication environment, but only the main AOS server is active for generation of data in normal situation. The server application is activated on the backup server only in case of failure of the main server and the participant is notified of that.

Application TCP ports and target IP addresses of AOS servers shall be provided by PXE. IP addresses of AOS servers are from ranges not used in the Internet.

IPSec protocol is used on the lines between participant routers and central routers to secure confidentiality and authentication of data transferred via the transfer channel.

Basic technical specifications of "Site to Site LL":

Participant's communication equipment

Router. CISCO Systems type router, line 1800 and higher, with 1 Port Serial WAN Interface Card, operation system IOS IP PLUS 3 DES ver. 12.2 and LAN interface according to the type of local network of the participant is recommended.

Communication environment

Digital line according to Appendix 1, paragraph 1, terminated by an interface according to the router interface type on the side of the participant.

Line protocol

HDLC

Network protocol

IP (TCP/IP)

IP address of the line connection

Unnumbered is recommended for WAN IP. Otherwise, the range according to RFC with 30 bit mask for two-point connection must be agreed.

IP address of the participant part of the network

Allocated to participant by exchange from the range of private IP addresses non-routable in the Internet according to RFC 1918.

This address range shall be routed in the central communication system to the interface of the communication environment towards the participant communication device. The potential transfer of IP addresses (NAT) to another address space shall be provided for by the Participant on his side.

IP address of the central part of the network:

The address range from private IP addresses non-routable in the Internet according to RFC 1918.

The range must be routed on the participant communication device to the range of communication environment towards the central communication system. The potential necessary transfer of IP addresses (NAT) to the address space of the Exchange shall be provided for by the Participant.

Routing:

Static, no routing protocol for exchange of routing information is used between the participant communication equipment and the central communication system.

Security of communication line:

Access Control Lists (ACL), IPSec

Specific assigned IP range of participant and central part of the network, IP addresses and TCP ports of the servers on the side of PXE, IPSec parameters and informative example of CISCO IOS setting shall be provided to participant by PXE upon filing an application for installation of the communication device.

2. VPN Standalone Client

Communication environment of the Internet network (according to Appendix 1, article 2) is used for this type. The technical platform is Virtual Private Network (VPN) using security protocols IPSec for client authentication and confidentiality of transferred data. A hardware device is used for storing certificates and cryptographic keys. PXE provides client VPN software, hardware device for storing the certificate and installation instructions for Internet VPN connection.

The instructions assume installation of VPN client on the Windows type operation system and PC computer with a USB port. Connection of the computer to the Internet must be available and the computer must have a static IP address assigned in the Internet network. The computer receives the second (internal) IP address from the exchange VPN server. The IP address is assigned from the ranges according to RFC 1918. Front-end module is also installed on this computer.

Basic technical specifications of “VPN Standalone client”:

Installation of client VPN SW requires a computer with Pentium class processor or higher, at least one USB port, Windows XP Professional SP2 operation system (min. 256 MB RAM) and the user with administrator rights for this operation system. Installation on Windows Server 2003 SP1 is also possible. It is recommended no to use another cryptographic device than the below USB Token iKey and other active IPSec connections on the computer.

The computer must be connected to the Internet and the computer must have assigned a permanent IP address in the Internet network. The IP address must be communicated to PXE prior to installation and PXE must also be notified of its later change.

If the computer connected to the Internet is located behind a firewall, the firewall must allow outgoing communication to the Internet network on ports UDP of protocol udp/4500 and udp/500 for the target IP address of the access VPN gate BCPP. The firewall supports transfer (NAT or PAT) of the internal IP address of the computer to the registered IP address within the Internet network communicated to PXE.

Dial-up/DSL connection of the computer to the Internet network is possible, but the connection provider must provide for assignment of permanent IP address (see previous items). In this case, it is highly necessary to secure the computer system (current updates, anti-virus, etc.). The installed software CISCO VPN Client includes a simple internal personal firewall.

Reception of the following components from PXE and their installation and use:

- ▶ Cisco VPN Client software with preset configuration
- ▶ HW device control software (SafeNet Borderless Security Client PK 6.1)
- ▶ hardware device (USB Token Rainbow iKey 2032) with generated pair of RSA keys and client certificate
- ▶ certificate of root certification authority issuing the client certificate (PSECA1)
- ▶ access PIN to HW device
- ▶ access UID and password for further authentication of the client

3. Site to Site VPN

Transfer channel is realised by data connection between private networks of PXE and of PXE participant. This is provided for by the central communication device of PXE and the participant communication device. The central communication device is connected to the central PXE network with AOS exchange servers. Participant communication equipment is connected to the network of the participant, to which computers with front-end module are also connected.

The central communication device is interconnected with participant communication device via the Internet (Communication environment according to Appendix 1, article 2). Internal communication between private networks is secured using the IPSec protocol.

IPSec parameters:

Phase1: certificate or pre-shared key, AES256, SHA1, Group 2

Phase 2: AES256, SHA HMAC (esp-aes-256 esp-shahmac), no PFS

The private IP addresses of the member part of the network (IP subnet) and of the central part of the network are assigned and established by the Exchange from the range of private IP addresses non-routable in the Internet according to RFC 1918. Possible transfer of IP addresses (NAT/PAT) to another IP address space is provided for by the member on its side.

The Exchange and the member will inform one another of public Internet IP addresses of the central communication device (central VPN gateway) and the member communication device (member VPN gateway). Likewise, they will inform one another via a secure channel of the pre-shared key, or the member will be issued a certificate for its communication device (based on an encrypted request generated in this device).

The technical specifications of "Site to Site VPN" may be specified based on an agreement between the participant and PXE.

4. Internet Direct

Communication Connection

This type of communication system uses the participant's communication device designated for direct connection to the Internet.

The central communication device is connected with the participant communication device via the Internet (the communication environment under Article 2 of Appendix 1).

This type of participant communication system may be used only for data connection to the Trayport system.

5. Mutual arrangements

Potential exceptions are approved by the PXE general secretary.

Appendix 3

Order Form Internet Comm. Connection “VPN client” or “Site to site VPN”

| | | |
|----------------------------------------------------------------------------------|-------------------------|--|
| Company (connected subject) | | |
| Address | | |
| Person responsible for communication connection | | |
| | Telephone number | |
| | e-mail | |
| Participant's code determined by PXE (if not determined yet, leave blank) | | |
| Registered Internet IP address (see Technical conditions) | | |

Order Form Communication Connection “Site to Site LL”

| | | |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|--|
| Company (connected subject) | | |
| Address | | |
| Person responsible for communication connection | | |
| | Telephone number | |
| | e-mail | |
| Participant's code determined by PXE (if not determined yet, please leave blank) | | |
| Parameters of the Participant's Digital Circuit (if not determined yet, please leave blank and send later) | Circuit's ID: | |
| | Timeslot in first central E1: | |
| | Circuit's ID and timeslot in backup central E1: | |

Communication Connection

| | |
|------------------------------------------------------|--------------------------------|
| | |
| Participant's IP subnet (172.16.xxx.0/24) | xxx = will be specified by PXE |
| PXE's IP subnet | will be specified by PXE |

Appendix 4

Participant Registration Form

| | | |
|----------------------------------------------------|--------------------------------|--|
| <p>Company (connected subject)</p> | | |
| <p>IČ</p> | | |
| <p>IN in OTE</p> | | |
| <p>Address front office -</p> | | |
| <p>Person responsible for communication</p> | | |
| | <p>Telephone number</p> | |
| | <p>e-mail</p> | |
| <p>Address back office -</p> | | |

| | | |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| | | |
| Person responsible for communication | | |
| | Telephone number | |
| | e-mail | |
| Application connection type (see Prováděcí předpis ... čl.6 odst.1) | Choose one of the following <input type="checkbox"/> PXE Communication server + ODBC <input type="checkbox"/> PXE web services interface (also PXE Monitor) | |

This form is basic for establishment of your company in the PXE trading system.

Choosing application connection type PXE web services interface represents 2 application connection. PXE Communication server +ODBC represents just 1 connection

If participant needs more application connections, it is not necessary to fill this form again. Send just simple request for another application connection and specify the application connection type.

Date

Signature