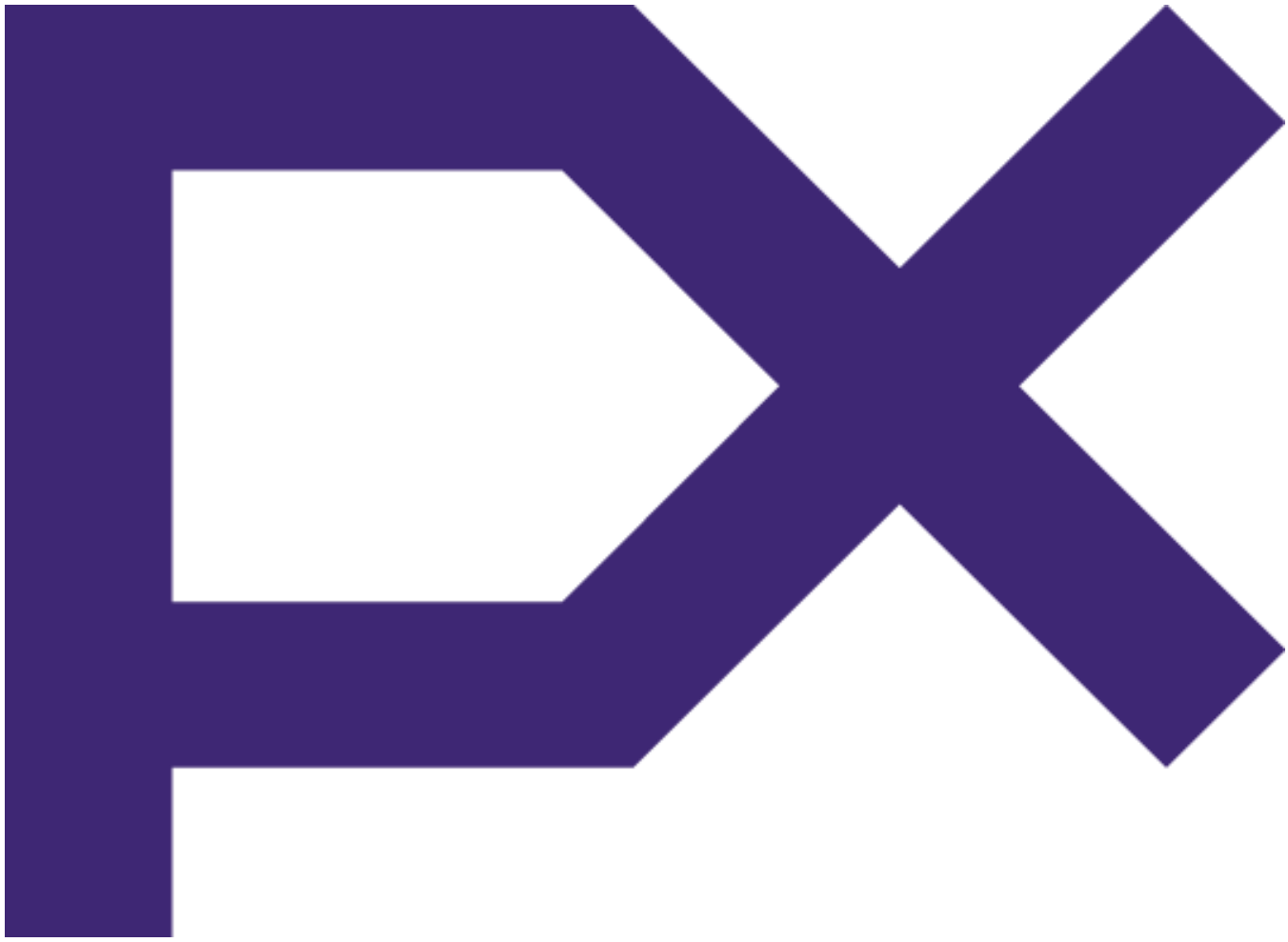
CENTRAL SECURITIES DEPOSITORY PRAGUE



COMMUNICATION CONNECTION OF PARTICIPANTS TO THE CENTRAL SECURITIES DEPOSITORY

Version effective as of 1st July 2021

CENTRAL SECURITIES DEPOSITORY PRAGUE

Contents

CENTRAL SECURITIES DEPOSITORY PRAGUE

COMMUNICATION CONNECTION OF PARTICIPANTS TO THE CENTRAL SECURITIES DEPOSITORY

Article 1
Subject Matter

1. This Regulation deals with the terms and conditions of on-line data communication between the Central Securities Depository (hereinafter the "**Central Depository**") and Central Depository participants, resp. other subjects using communication system of CSD Prague (hereinafter the "**Participant**" or "**Participants**").

2. The provisions of this Regulation shall apply unless otherwise stipulated in another specific regulation issued by the Central Depository or a decision of the competent Central Depository body.

Article 2
Definition of Expressions and Abbreviations Used

1. **Participant Data Communication** - electronic data communication for the submission of instructions, data and information relating to the registration of investment instruments and the settlement of trades involving investment instruments, to the extent of the authorization set out in the Operating Manual of the Central Depository, the Settlement System Rules or the Central Depository Participation Agreement. Data communication is carried out via the communication system and the Participant programme modules.

2. **Communication System** - the set of hardware and software instruments serving the purpose of data communication. The Prague Stock Exchange manages the Communication System for the Central Depository and its Participants (hereinafter the "**Exchange**"). The Communication System is divided into a central Communication System, the Communication Environment and the Participant Communication System.

3. **Central Communication System** - part of the Communication System situated within the Exchange's headquarters or individual sites. The Central Communication System is connected to the Exchange central computer servers (hereinafter the "**ATS**").

4. **Communication Environment** - part of the Communication System serving for the connection of the Central Communication System with the Participant Communication System.

5. **Participant Communication System** - part of the Communication System situated within the Participant's headquarters or individual sites. Programme modules are connected to the Participant Communication System, via the Participant's LAN. The Participant Communication System shall remain the property of the Exchange.

6. **Participant's LAN** - Local Area Network operated and managed by the Participant, situated within the Participant's headquarters or individual sites.

7. **Programme Modules** - programme modules assisting Participants in placing orders for the registration of securities and the Settlement System. Programme Modules are provided by the Participant and are located within its workplaces.

8. **Communication Server** - software used for the exchange of data and information between the Programme Module and the Exchange's central computer servers. The Communication Server is installed on PCs on the Participant's premises.

9. **Production Environment** - separated logical space in the Exchange's central computer server where real data are kept, together with the current versions of programmes, and where data are processed on a daily basis (different from testing environment, for example, where data and programmes for testing purposes are kept).
10. **CDCP Enter** – a web application provided by Central Depository to participants and other subjects upon a contractual agreement. It is possible to give all types of instructions via CDCP Enter as is possible via data interface.
11. **Backup Communication Environment** - communication environment serving for the data connection of the Exchange's backup Central Communication System with the Participant Communication System in the event of the breakdown of the Central Communication System or of the Communication Environment.

Article 3
Technical Description of Participants Communication System

1. The Participant Communication System is connected via the Communication Environment defined in Annex 1 to the Central Communication System and to the Participant's LAN. The interface of the Participant Communication System and subsequently of the Communication System towards the Participant is defined by the specified data connection point (data outlet) to the Participant's LAN.
2. The brief technical description of the Participant Communication System is specified in Annex 2 attached to this Regulation.

Article 4
Installation of Participant Communication System

1. The Central Depository provides all the services set out in this Regulation and associated with the electronic data communication between the Central Depository and the Participants through the Exchange, on the basis of an agreement signed between the Central Depository and the Exchange. The Participants of the Central Depository who are also trading members are provided services associated with the communication connection to the Central Depository by the Exchange, in accordance with Exchange regulations.
2. Participants who are also trading members have the Participant Communication System installed via the Exchange based on a written application for the registration in the Communication System, and based on a written request for the installation of the Participant Communication System. The forms of the application are provided in the Exchange regulation dealing with the communication connection to the Exchange. Participants shall send the applications to the Exchange IT Division.
3. Participants who are not trading members get the Participant Communication System based on a written application for the registration in the Communication System and based on a written request for the installation of the Participant Communication System, the forms of which are provided in Annexes 3 and 4 of this Regulation. The installation may be carried out by the Exchange or a contractor appointed by the Central Depository.
4. Participants of the Central Depository are obliged to arrange for a proper Communication Environment and a Backup Communication Environment, according to their own choice and at their own expense, with an operator of such an environment.
5. For the Participant Communication System of the "**Site to Site LL/ETH**" type, the Exchange shall submit its essential requirements and parameters for the configuration of the Participant Communication System. Pursuant to the application, this type of Participant Communication System will be installed by

the Exchange within 3 weeks following the delivery of the application. In such a case, the Participant Communication System shall remain the property of the Exchange. Prior to the installation, the Participant is obliged to comply with the technical conditions for the installation. The conditions are provided in Annex 6.

6. For the Participant Communication System of the "**Site to Site VPN**" type, the Exchange shall submit its essential requirements and parameters for the configuration of the Participant Communication System.
7. For the Participant Communication System of the "**VPN Standalone Client**" type, the Exchange shall provide Participants with the necessary software for installation, together with an installation manual and an authentication hardware dongle with an access PIN.
8. As regards the Participant Communication System according to Articles 6) and 7), Participants shall arrange for the installation, configuration and maintenance of the Participant Communication System at their own expense. In such a case, the Participant Communication System shall remain the property of the Participant. The Exchange shall not be responsible for the installation and shall not be held liable for any damage incurred by the Participant in question from an incorrectly performed installation.
9. Participants of the Central Depository shall protect the submitted authentication data for the Participant Communication System as confidential. If the HW dongle PIN is stolen or lost, Participants shall make sure that a new HW dongle PIN is created, with the help of the supplied software. Participants shall notify the Exchange of any theft or loss of the hardware dongle, and the Exchange will in such a case immediately block the dongle for any further use for participant authentication. In the event of the theft or loss of a PIN, the Participant concerned shall deliver the HW dongle to the Exchange for the generation of a new PIN.

Article 5
Possible Connection via Application Layer

1. Programme Modules can be connected to ATS at an application level using two methods:
    a) With the use of the Exchange's Communication Server and ODBC interface; or
    b) Via a Web Service based interface.
2. The connection methods according to clause (1) are independent of the selection of the type of the Participant Communication System.
3. When connected in accordance with (1) (a) above, the Programme Module is provided by the Participant of the Central Depository. The Exchange only supplies the Communication Server.
4. If a connection is established according to (1)(b), the Exchange will only supply the Web Service interface; upon request, a standard client (open-source client) is also supplied, demonstrating the working method with such a data interface in Java.
5. If a connection is established according to (1)(b), the Exchange will supply a hardware dongle with a PIN for the members' authentication. The use is similar to the use set forth in Art. 4 (9).
6. Participants are obliged to arrange for the software installation according to the instructions provided by the Exchange.
7. Participants are obliged to notify the Exchange of any defects in the supplied software.

Article 6
Conditions for Operation of Participant Communication System

1. Participants shall pay the Central Depository fee for the use of the Participant Communication System, in accordance with the Central Depository Price List. Participants of the Central Depository who are also trading members shall pay the fee for the use of the Communication System to the Exchange, in accordance with the terms and conditions of the agreement signed with the Exchange.
2. The Participant Communication System may only be used in accordance with these rules.
3. Participants are not authorized to make any unauthorized interventions in the Communication System of the Exchange, and shall not use the Communication System for any other purposes than specified in the present Regulation. In the event of any damage or misuse of the Communication System, the Participant shall compensate the Central Depository or the Exchange for any damage incurred.
4. If a Participant makes an attempt at unauthorized access to the Programme Modules or the information system of the Central Depository and the Exchange other than through the profiles assigned by the Central Depository or the Exchange, defined in data interface[1], the Central Depository shall be entitled to disconnect the Communication System of this Participant from the Central Communication System, via the Exchange, until the respective bodies decide on further action.
5. If participation in the Central Depository is suspended, the Participant's participation in the Communication System will also be suspended. During such a period, the Participant shall continue to be obliged to pay the fee specified in paragraph 1.
6. Upon the termination of the participation in the Central Depository, the Participant is obliged to allow the Central Depository to uninstall the Participant Communication System. The uninstalling may also be carried out by the Exchange or a contractor appointed by the Central Depository.

Article 7
Other Participant Connections

1. At any given moment a Participant may be connected to the Central Depository or the Exchange via more application or communication links, provided that all connections are equal. The Exchange offers the following possibilities for establishing Participant connections:
    a) Installation of the Communication Server or the Programme Module on one or more PCs; only one installation may be active within the Production Environment at a given time. This solution is free of charge.
    b) The possibility of making use of another application connection. This means that a Participant may at any given moment be connected to the Central Depository via two or more

[1] Data interfaces are sent to the participants via the Exchange Communication System

    installations of the Communication Server according to Art. 5. (1a) or via more installations of the Participant's Programme Module connected according to Art. 5 (1b).
    c) The possibility of making use of another communication and application connection. This means that the Participant may at any given moment be connected to the Central Depository via more communication and/or application links.
    d) The possibility of another connection to ATS. Participants are entitled to apply for another (second) access to the ATS Settlement System (a new participant's code). This solution is suitable for two Settlement System accesses with separated data.

2. Participants shall pay the Central Depository fees for the use of another connection under 1 (b), (c) or (d), according to the Central Depository Price List.
3. Participants shall file applications for another connection according to Article 7 (1) (b), (c) or (d) using the attached form (Annex 5).
4. The provisions of the present regulation shall apply accordingly for the technical description, operation, installing and uninstalling, service security and procedures in the event of a defect of an additional connection.

Article 8
Servicing of Communication System

1. The Central Depository is only responsible for the Communication System up to the interface of the Participant Communication System and the Participant's LAN.
2. The Central Depository will only ensure the servicing of the section of the Communication System for which the Central Depository is responsible, via the Exchange.
3. The Central Depository may also assign the servicing tasks to an authorized contractor.
4. The terms and conditions of the servicing are specified in the Central Depository's Newsletter (hereinafter the "**Newsletter**").

Article 9
Remedying Defects to Communication System

1. As regards the Participant Communication System, the Central Depository offers service consultations to Participants, via the Exchange, to identify the causes and diagnose any potential defects. The manner in which such consultations are offered is specified in the Newsletter.
2. If a defect is identified in a Participant Communication System, the Participant shall inform the Central Depository of the contact persons and the Central Depository shall be obliged to remedy the defect without unreasonable delay.
3. If a defect is identified in the Communication Environment, the Participant shall contact the respective provider of this environment and arrange for the respective repair thereof.
4. If a defect is identified in the Central Communication System, the Central Depository shall be obliged to remedy the defect without unreasonable delay.
5. If a defect is identified in the Communication Server, the Central Depository shall be obliged to remedy the defect without unreasonable delay.

Article 10
Liability for Damage

1. Neither the Central Depository nor the Exchange are liable for any damage incurred by Participants or other persons as a consequence of:
    a) Communication System failure or defects in the Communication Server, and subsequent loss or leakage of data;
    b) Unauthorized use of the Participant Communication System or a misuse thereof by a Participant or a third party;

c) Violation of the obligations stipulated in the generally binding legal regulations or the regulations of the Central Depository.

Article 11
Final Provisions

This Regulation was approved by the Central Depository's Board of Directors on 7 June 2021 and shall come into effect on 1 July 2021.This Regulation shall replace the document entitled "**Communication Connection of Univyc Participants in the Settlement System**".

Annex 1

Communication Environment

Participants of the Central Depository can choose one of the following Communication Environments:

1. Ethernet IP

- This Communication Environment is used for the communication system of the "**Site to Site LL/ETH**" type
- The Communication Environment is formed by the operator's data IP MPLS network
- Operator of the data network: T-Systems Czech Republic a.s.

Access speed	1-2 Mbps
Interface	10BaseT /RJ 45

2. Internet

- This Communication Environment is used for the communication system of the "**VPN Standalone Client**" or "**Site to site VPN**" type.
- As regards an Internet Communication Environment, the Participant Communication System must have a fixed Internet IP address assigned. Such an IP address shall be communicated to the Exchange prior to the installation, together with any subsequent changes. The Exchange will communicate the Internet IP address of the Central Communication System to a Participant upon the filing of an application for the installation.

Recommended access speed	256 kbps

With respect to the character of this Communication Environment, permanent availability and response times - which in Communication Environment (1) are guaranteed by the operator - are not guaranteed. It is recommended that this Communication Environment be used as backup.

CENTRAL SECURITIES DEPOSITORY PRAGUE

Annex 2

Basic Technical Description of Supported Communication System Types

The communication channel is implemented via a data connection between Exchange's private networks and the private networks (or PCs) of individual Participants. IP is the network protocol. The application connection is operated via TCP/IP. The IP address of PCs or the network IP subnet are allocated by the Exchange. It is possible to make use of IP address translation (NAT/PAT); however, Participants' PCs in the network towards the Exchange must have assigned IP addresses. Participants' IP addresses/subnets are assigned by the Exchange from the ranges of IP addresses not used within the Internet (RFC 1918).

All central ATS servers are accessible from Participants via TCP/IP through all line connections and communication environments. Under standard conditions, only the main ATS server is active for Participants' applications. Server ATS applications are only activated within the backup server if the main server has a defect and the Participant is duly informed. In such a case, the Participant must route Participants' applications to the backup server. The TCP application ports and target IP addresses of the ATS servers will be provided by the Exchange. The IP addresses of ATS servers are assigned from ranges not used on the Internet.

IPSec protocol is used to ensure due confidentiality and authentication of data transferred via the communication channel.

1. Site to Site LL/ETH

The communication channel is implemented via a data connection between private networks of the Exchange and the Participant. This is secured by central Exchange routers and the Participants' routers. Central routers are connected to the central Exchange network featuring ATS Exchange servers. Participants' routers are connected to Participants' data networks in which PCs featuring Programme Modules are also connected. Central routers are connected with Participants' routers via the Communication Environment according to Annex 1.

IPSec protocol is used on the lines between Participants' and central routers to ensure due confidentiality and authentication of data transferred via the communication channel.

Basic Technical Specification of "Site to Site LL/ETH":

Participants communication device
Router. A router of the CISCO Systems type is used.

Communication Environment
According to Annex 1

Line protocol
Depending on the applied Communication Environment:
ETH - Ethernet

Network protocol
IP (TCP/IP)

Line connection IP address
ETH - the Exchange will determine the communications network addressing on the basis of an agreement with the network operator

IP address (IP subnet) of the participants' part of network
Range assigned by the Exchange to the Participant from private IP addresses routed within the Internet according to RFC 1918.This address range will be routed in the Central Communication System to the Communication Environment interface, towards the Participant Communication System. The translation of IP addresses (NAT) to another address space (if any) shall be arranged by the Participant.

IP address of the central part of network
Address range from private IP addresses routed within the Internet according to RFC 1918.
The range is routed in the Participant communication device to the Communication Environment interface, towards the Central Communication System. The translation of IP addresses (NAT) to another address space (if required) shall be arranged by the Participant.

Communication line security
Access Control Lists (ACL), IPSec

The Exchange supplies the Participant communication device for Site-to-Site LL/ETH - i.e. the router, and arrange for its installation, configuration and maintenance. The router is the property of the Exchange. Participants are not authorized to configure the communication device in any manner; they are only able to view the setup.

2. VPN Standalone Client

The Internet Communication Environment is used for this type (see Annex 1, Art. 2). Virtual Private Network (VPN) is the technical platform with the use of IPSec security protocols for client authentication and the security of transferred data. A hardware dongle is used for the storage of certificates and cryptographic keys. The Exchange provides VPN software for the Internet VPN connection, together with the hardware dongle for the storage of certificates and installation manuals. According to the instructions, the VPN client is designed for installation with Windows and on a PC with a USB port.

Basic Technical Specification of "VPN Standalone Client":

The installation of the VPN SW requires a PC with a Pentium processor or higher, at least one USB port, running Windows XP Professional SP2 and higher (at least 512 MB RAM), for which the user must have administrator rights. It is also possible to install the SW under Windows Server 2003 SP1. The use of cryptographic devices other than the USB Token iKey specified below and other active IPSec connections is not recommended. In addition, the Programme Module is installed on this PC.

The PC must have an Internet connection and a fixed Internet IP address (public IP address). Such an IP address shall be communicated to the Exchange prior to the installation, together with any subsequent

changes. If a PC connected to the Internet is located behind a firewall, outgoing communication to the Internet must be permitted at the firewall, on the UDP protocol ports udp/4500 and udp/500 for the target IP address of the Exchange access VPN gate. It is possible to carry out translations within the firewall (NAT or PAT) to a registered IP address in the Internet, reported to the Exchange. The dial-up/DSL Internet connection of a participant's PC is possible; however, the connection provider must ensure the assigning of a fixed IP address (see above). In such a case, it is necessary to ensure a high degree of PC system protection (updates, antivirus program, etc.).

The member's/participant's PC will obtain another IP address after it is authenticated (private IP address). Such an IP address will be assigned from ranges according to RFC1918.

The Exchange will provide the following for the installation and use of the VPN Standalone Client:

- Preconfigured Cisco VPN Client software, together with an installation manual
- Control software for the HW dongle
- Hardware dongle (USB Token Rainbow iKey 2032) with a generated pair of RSA keys
- Certification of the root certification authority issuing the certificate
- HW dongle access PIN
- Access UID and password for the client's further authentication

3. Site to Site VPN

The communication channel is implemented via a data connection between private networks of the Exchange and the Participant. This is ensured by the Exchange's central communication device (central VPN gateway) and the Participant communication device (member VPN gateway). The central communication device is connected to the central Exchange network featuring ATS Exchange servers. Participant communication devices are connected to the Participant's data network, in which PCs featuring the Programme Module are also connected. The central communication system is interconnected with the Participant communication device via the Internet (Communication Environment according to Annex 1, Art. 2) and the internal communication among private networks is secured via the IPSec protocol.

Basic Technical Specification of "Site to Site VPN":

IPSec parameters:

Phase 1: certificate or preshared-key, AES256, SHA1, Group 2
Phase 2: AES256, SHA HMAC (esp-aes-256 esp-shahmac), no PFS

The private IP addresses of the Participants' part of the network (IP subnet) and the central part of the network are assigned and defined by the Exchange from the range of private IP addresses routed on the Internet according to RFC 1918. The translation of IP addresses (NAT/PAT) to another address space (if any) shall be arranged by the Participant.

The Public Internet IP addresses of the central communication system (central VPN gateway) and the Participant communication device (member VPN gateway) will be communicated between the Exchange and the Participant. In addition, the parties will communicate the pre-shared key in a secure manner, or the

Participant will be issued a certificate for the Participant communication device (on the basis of a cryptographic application generated in this system)

The technical specification of the “Site to Site VPN” may be specified on the basis of an agreement between the Exchange and the Participant.

CENTRAL SECURITIES DEPOSITORY PRAGUE

Annex 3

Application for Registration in Communication System

Company name		
Identification number		
Type of membership		☐ Trading member ☐ CSD participant and participant in settlement system ☐ CSD participant ☐ Clearing bank☐ Data vendor ☐ IT service provider (for test environment only)
Connection		☐ Operating environment ☐ Testing environment
Address - front office		
Person responsible for communication		
	E-mail	
	Phone	
Address - back office		
Person responsible for communication		
	E-mail	
	Phone	
Type of application connection (see Article 5 (1) of the Regulation)		☐ Communication server + ODBC ☐ Webservices interface ☐ CDCP Enter

Comments:

This application serves as a basic document for establishing a subject in the Communication System.

The website interface includes two application connections, Communication Server interface + ODBC includes only one application connection.

Participants requiring more application connections must complete the form provided in Annex 5

I hereby request the registration of the aforesaid data regarding our company in the Communication System.
Date and signature of authorized person:

CENTRAL SECURITIES DEPOSITORY PRAGUE

Annex 4

Application for the Installation of Participant Communication System

Company name		
Participant code (to be completed by CSD)		
Address and location of the Participant Communication System		
Contact person		
	E-mail	
	Phone	
The technical parameters of the Communication Environment will be specified by the provider		
Type of the Communication Environment		❑ Ethernet IP - Site to Site LL/ETH ❑ Internet VPN - Standalone Client ❑ Internet VPN (Site to Site VPN)
Type of application connection		❑ Communication server + ODBC ❑ Webservices interface ❑ CDCP Enter
Ethernet IP	Connection speed in kbps	
Parameters Internet VPN	IP address of the client / GW in the Internet	

I hereby request the installation of a Participant Communication System according to the data above.
Date and signature of authorized person:

CENTRAL SECURITIES DEPOSITORY PRAGUE

Annex 5

Application for Additional Connection

Company name		
Participant code		
Address and location of the member communication system		
Contact person		
	E-mail	
	Phone	

Type of additional connection	
I. Service according to Art. 7 (1) (b) of the Regulation i.e. possibility of making use of another application connection (Communication Server or Programme Module) within the Production Environment	❑ Communication server + ODBC ❑ Webservices interface ❑ CDCP Enter
II. Service according to Art. 7 (1) (c) of the Regulation i.e. possibility of making use of another communication and application connection (another line connection)	❑ Communication server + ODBC ❑ Webservices interface ❑ CDCP Enter
III. Service according to Art. 7 (1) (d) of the Regulation i.e. another connection to ATS - new participant's code	❑ Communication server + ODBC ❑ Webservices interface ❑ CDCP Enter

Please complete in the event of another line connection (service according to Art. 7 (1) (c) of the Regulation):

Type of the Communication Environment		❑ Ethernet IP - Site to Site LL/ETH ❑ Internet VPN - Standalone Client ❑ Internet VPN (Site to Site VPN)
Ethernet IP	Connection speed in kbps	
Parameters of Internet VPN	IP address of the client / GW in the Internet	

Date and signature of authorized person:

CENTRAL SECURITIES DEPOSITORY PRAGUE

Annex 6

Technical Conditions Regarding the Installation of Participant Communication System

Prior to the installation of a Participant Communication System, the Participant in question is obliged:

a) to allow for the installation of the Participant Communication System elements on dates and times agreed with the Exchange or a contractor authorized by the Exchange to carry out such installation;

b) to ensure that contact persons and persons responsible for the respective IT equipment are present during the installation and offer their cooperation (network administrators, etc.);

c) to create conditions for the installation and operation of the Participant Communication System elements, as well as space adequate for the installation and operation of such systems;

d) to secure the area where the Participant Communication System elements are operated against unauthorized access;

e) to allow for the installation and location of the Participant Communication System elements - at a place located at a maximum distance of 2 metres from the data interfaces - on the selected Communication Environment, and not more than 2 metres from the access to the Participant's LAN;

f) To provide one electrical outlet (220 V) within 2 metres of the place where the Participant Communication System elements will be located, for the purpose of supplying power for the Participant Communication System elements;

g) To provide the necessary connection cables for the connection of the Participant Communication System to the Participant's LAN;

h) To allow for a test to be performed on the functionality of the Communication System.