



London
Stock Exchange Group

Service Description

January 2011 - Version 1.3

Exchange Hosting

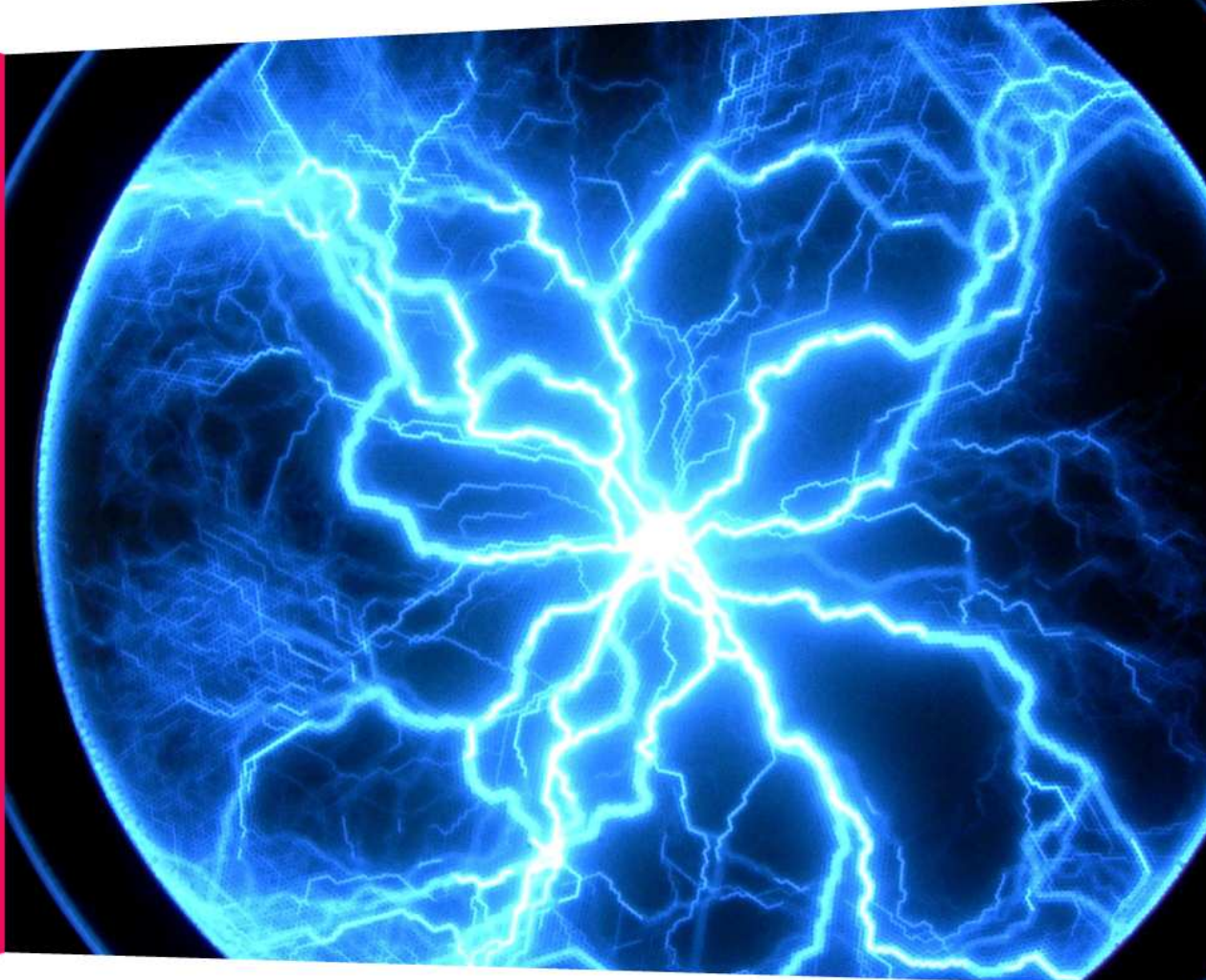




Table of Contents

1 Document Scope	5
1.1 Structure of this Document	5
1.2 Version History	5
1.3 Use of This Documentation	6
1.4 Amendment of this document	6
2 Overview of the Service	7
2.1 Key features of the Service	7
2.2 Performance Improvements	7
2.3 Data Centre – High Level Specification	8
2.4 Customer Benefits of the Service	9
2.5 High Level Network Diagram	9
2.6 Pre-requisites for the Service	10
2.7 Ordering the Hosting Service	10
3 Network and Connectivity Design	12
3.1 Connectivity to Exchange Services	12
3.2 Customer Connectivity	13
3.2.1 Customer Proprietary Connections	13
3.2.2 Blt Network	14
3.3 Network Frequently Asked Questions (FAQs)	16
4 Site Procedures	17
4.1 Health and Safety	17
4.1.1 Site Instructions for Customers	17
4.2 Access to site and Delivery to Site	18
4.3 Disposal of Waste Material	18
4.4 Site Frequently Asked Questions (FAQs)	18
5 Equipment Installation	19
5.1 Equipment Installation	19
5.1.1 Installation Guidelines	19
5.1.2 Power Configuration	21
5.2 Demarcations points	22
5.2.1 Power Demarcation point	22
5.2.2 Network Connections Demarcation Point	22
5.3 Customer Enablement Process	22
5.4 Testing Policy and Procedures	23
5.4.1 Management Connectivity Testing	23
5.5 Installation Frequently Asked Questions (FAQs)	23
6 Service Operation	24
6.1 System Monitoring of the Exchange Hosting Service	24
6.2 Reporting a Fault with the Exchange Hosting Service	24
6.3 Change Management Process	24
6.4 Exchange Routine and Unscheduled Maintenance	24
6.5 Customer Usage of the Hosting Service	25



6.5.1	Service Prohibitive Purposes	25
7	Escalation Procedures	26
8	Data Centre Technical Specification	27
8.1	General Datacentre Characteristics	27
8.1.1	Introduction	27
8.1.2	The building	28
8.1.3	Human Flow management and anti-terrorism measures	29
8.1.4	Electrical system	29
8.1.5	Fire prevention	30
8.1.6	Air conditioning systems	31
8.1.7	Passive security	31
8.1.8	Security	32
8.1.9	Power	32
9	Service Contacts	33
10	Appendix A - Time Synch Service	34
10.1	Service Overview	34
10.2	Ordering the Service	34



Index of Figures

FIG 1 – HOSTING MARKET AND MANAGEMENT CONNECTION – HIGH LEVEL	9
FIG 2 – CUSTOMER’S SITE CONNECTION – HIGH LEVEL	10

Index of Tables

TABLE 1 - VERSION HISTORY	5
TABLE 2 - DATA CENTRE – HIGH LEVEL SPECIFICATION	8
TABLE 3 - SERVICE CONTACTS	33



1 Document Scope

The purpose of this document is to provide customers with a detailed definition of the Borsa Italiana Hosting Service, including all relevant technical configurations and hosting facility specifications.

This document is published by Borsa Italiana (the “Exchange”). Other relevant documentation relating other Borsa Italiana services is also available from our website <http://www.borsaitaliana.it/borsaitaliana/intermediari/gestione-mercati/gestione-mercati.en.htm>.

1.1 Structure of this Document

This document contains the following section:

1. **Document Scope** – identifies the purpose and scope of this document
2. **Overview of the Service** – details the key features of the Hosting Service
3. **Network and Connectivity Design** – details the generic Exchange and Management connectivity design for the Hosting Service
4. **Site Procedures** – details the processes for becoming authorised for site access, requesting access to attend the site, lists key data centre policies and identifies the health and safety procedures
5. **Equipment Installation** – details the key information and processes required for installation of customer equipment in the Data Centre
6. **Service Operation** – details the Remote Hands Service assistance, market supervision support and ongoing operations
7. **Escalation Procedures** – identifies the high level issue reporting and escalation process should there be an interruption to the Hosting Service
8. **Data Centre Specification** – identifies the key data centre specifications
9. **Service Contacts** – provides the Exchange’s contacts for customer communications and requests for services
10. **Appendix A – Time Synchronisation Service** – identified the high-level service details for the Time Sync Facility.

1.2 Version History

The Hosting Service and Technical Description document has had the following iterations:

Issue	Date	Description
1.0	May 2010	First issue of the Exchange Hosting Service and Technical Description.

Table 1 - Version History



Any amendments to this document will be communicated and circulated to Customers.

1.3 Use of This Documentation

This confidential document is the property of the Exchange, and neither the document nor its contents may be disclosed to a third party, nor may it be copied, without the Exchange's prior written consent.

The Exchange endeavours to ensure that the data and other material in this publication are correct and complete but does not accept liability for any error herein or omissions herefrom.

The development of Exchange products and services is continuous and published information may not be up to date. It is important to check the current position with the Exchange.

1.4 Amendment of this document

This document may be amended at any time and, areas impacting service provision will be effective following 30 day's notice (in accordance with the Hosting Service Agreement).

The Exchange will distribute revised documentation to all identified individuals electronically once updated.



2 Overview of the Service

As the speed of our systems improve the relative impact of network latency becomes greater. In order to enhance further these improvements, we have developed a Hosting Service to provide customers with the fastest possible access to our markets.

Exchange Hosting - the ultimate option in terms of low-latency connectivity - allows customers to host their servers within the Exchange's Data Centre (I.Net - BT Italia) putting them as close as possible to trading and market data systems.

The service is available to Trading Participants who are either trading on an Agency or Proprietary basis. The Hosting Service is also available to Information Vendors that receives the market data feed through the DDM Plus Service.

For further information, please contact the Client Technology Services Italy team via our email address – clients-services@borsaitaliana.it.

2.1 Key features of the Service

- **Hosting within the Exchange's data centre** where the IDEM/IDEX market and the DDM Plus service central systems are located - as close as possible to the Exchange's core trading and information systems;
- **Elimination of network latency** attributable to network connections between the customer site and the Exchange;
- **Purpose-built Data Centre** providing high standards of security, access, power and cooling, and entirely managed by the Exchange;
- **Access to the Exchange Group Markets** - potential to connect to any of the following markets:
 - Borsa Italiana IDEM and IDEX markets;
- Wide choice of client connectivity options – customers have the choice between:
 - Proprietary lines connected to data centre's Telco cabinets; wide range of different carrier connectivity options,
 - Exchange proprietary network, called Bit Network.
- **Additional added value services:**
 - Local high precision Time Sync providing access to high precision time sync source via NTP signals

2.2 Performance Improvements

Customers utilising the Exchange Hosting Service will be provided with the following key performance benefits produced by reducing the latency between the Exchange's IDEM and DDM Plus platforms and the Customer's own trading applications:



- propagation delay: reduced components for packets to pass through
- transmission delay: physically close to the matching engines and market data infrastructure
- processing delay: significantly less components for packets to be processed

For further information on the specific latency savings please contact the Client technology Italy department.

2.3 Data Centre – High Level Specification

Service Offering	Phase 2:
Access to the following markets (Production and Test)	
Borsa Italiana IDEM and IDEX markets	✓
DDM Plus service	✓
Power usage (kilowatt per cabinet)	3kW or 5kW
Trading/Information cross-connections (per customer)	Up to 4 physical connections
Connections to the production environment	2
Connections to the test environment	2
Connectivity cross-connections (per customer)	Up to 2 physical connections
Connections for customer connectivity purposes (Bit Network and/or customer proprietary lines)	2
Management connectivity	
Wide range of different carrier connectivity options	✓
Low Latency connectivity	✓
Resilient carrier provision available	✓
Internet VPN connection available for Back-Up	✓
Exchange proprietary network (Bit Network) available	✓
Time Synchronisation	
NTP connectivity required	✓

Table 2 - Data Centre - High Level Specification

The Hosting Service includes access to the market from a single site and so does not include any physical disaster recovery facilities. In the event of an incident at the hosting site, clients would be required to revert to trading via their own hosted trading facility using existing connectivity (such as Bit Network or Service Provider solution).



2.4 Customer Benefits of the Service

With the increased speed of delivery of Market Data to customers and the ability to execute orders with reduced network latency, the following benefits are available to customers:

- improved performance of algorithmic trading capability
- increased probability of accessing available liquidity
- ability to react more quickly to market changes
- removes network capacity constraints

2.5 High Level Network Diagram

The following high level diagram identifies the market connectivity between the customer equipment and the Exchange's trading and datafeed services, and the connectivity from the customer's servers to the customers own location.

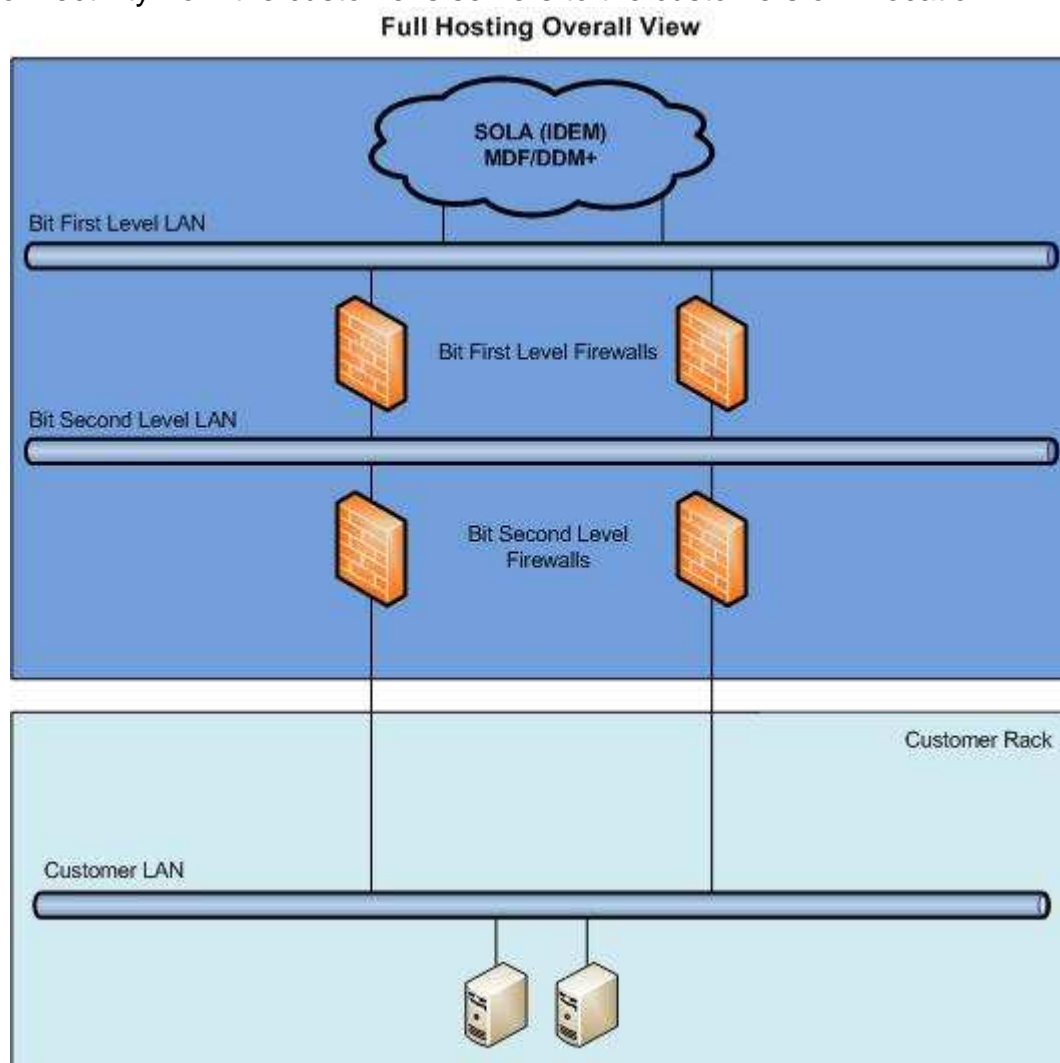


Fig 1 - Hosting Market and Management Connection - High Level



The following high diagram identifies the options for the connection of the Customer's site to the Customer's Exchange hosted equipment.

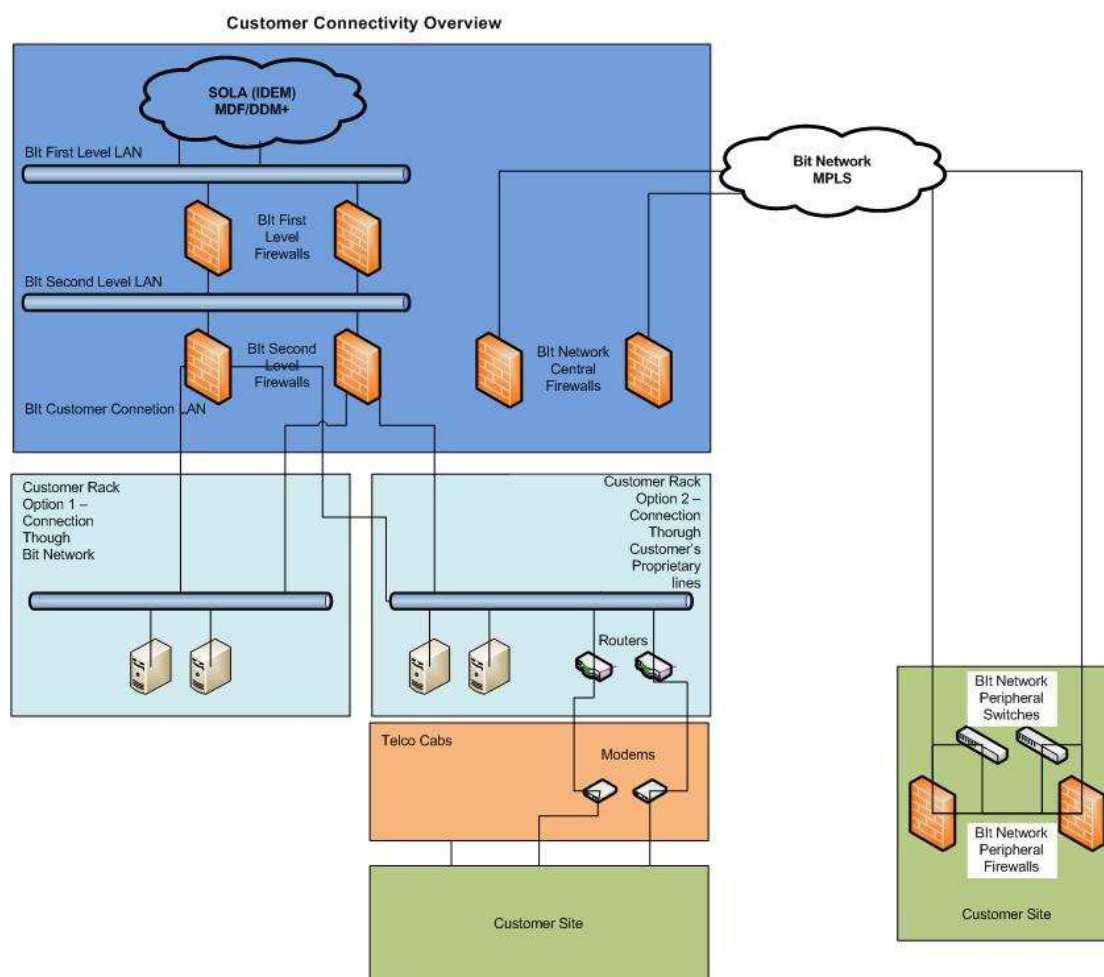


Fig 2 - Customer's site connection - High Level

Please refer to the 'Network and Connectivity Design' section for more detail

2.6 Pre-requisites for the Service

Customers that wish to use the Exchange Hosting Service must have comply with, inter alia, the following criterion:

- Trading arrangements in place (direct with the Exchange) at the time of customer testing; or
- Trading membership process in progress with the Exchange

2.7 Ordering the Hosting Service

Customers who are interested in taking the Exchange Hosting Service should contact the Client Technology Services Italy team via email clients-services@borsaitaliana.it or contact +39 02 72 42 6 348/647/606.



For any contractual issue please refer to the Hosting Service Agreement document.



3 Network and Connectivity Design

This section sets out the market connectivity between the Customer Equipment and the relevant Exchange Services. In addition, this section identifies the connectivity for dedicated management traffic from the Customer Equipment to the Customer's own location via either the Customer's own chosen carriers (utilising the Management Connectivity Service) or via the Exchange-provided Bit Network connection.

It is important to note that all configuration changes to the Exchange Hosting environment and infrastructure are completed during the identified change window – 18:00 to 22:00 each weekday (excludes Italy public holidays and weekends).

3.1 Connectivity to Exchange Services

The network design that has been implemented provides the lowest latency solution while ensuring sufficient security and operational standards are maintained.

For access to the markets, customers have to connect its own primary and secondary switches connecting to Exchange primary and secondary Hosting access firewalls.

Care should be taken when deciding the model of the switches to be used to ensure compatibility with available power and rack chassis mounting.

Each of the connections provided to customers to the trading systems are 100 Mbps copper connection terminated in a local patch panel within the customers cabinet.

The Exchange, SOLA and MDF/DDM+, operates with Unicast protocol connections only.

As standard, clients are offered **4** 100 Mbps physical connections in the following configuration:

- 2 x customer switches to Exchange firewalls for production environment connection (for all provided services)
- 2 x customer switches to Exchange firewalls for test environment connection (for all provided services)

Please be aware the Hosting architecture only permits a single pair of Customer switches to directly interface with the Exchange.

Customers should consider the available connections in their network design. The number of connection described above is to be considered per rack. If the



Customer requests N racks, it will have $4 * N$ available connections in the following configuration:

- $N * 2$ x customer switches to Exchange firewalls for production environment connection (for all provided services)
- $N * 2$ x customer switches to Exchange firewalls for test environment connection (for all provided services)

The client subnet that will directly interface with Exchange services will be provided by the Exchange. The customer's servers may belong to the provided subnet or to another one but in this case they will have to use the provided subnet as interconnection VLAN.

Once customers have their switches connected to the Exchange firewalls a simple "telnet" test to the IP(s) of the service(s) it will access (SOLA SAIL or HSVF IP/port, DDM+ TAX Servers IP/port, etc.) can be completed.

The Exchange monitors each port on the Access firewalls however, as the Exchange cannot determine if the device interfacing its systems has been purposely disconnected, the Exchange will only investigate an issue when it has identified that *all* ports on a specific firewall or if the firewall itself has failed. Customers should therefore escalate any specific single port issues that arise to the Exchange as a matter of urgency.

The Exchange recommends customers to use a teamed network configuration on their servers when connecting to the Exchange firewalls to maximise the resilient infrastructure, however this is not mandatory.

3.2 Customer Connectivity

This section identifies in more detail the connectivity options for Customers from their hosted equipment to their own locations. This allows the hosted systems to be managed and monitored by the Customer remotely as well as to allow remote systems (at the Customer's IT site(s)) to access the Exchange services.

As standard, clients are offered **2 100 Mbps** physical connections for the customer connectivity that can be used either in case of use of Blt Network or in case of use of Customer Proprietary Connections. The number of connection described above is to be considered per rack. If the Customer requests N racks, it will have $N * 2$ 100 Mbps physical connections for the customer connectivity.

3.2.1 Customer Proprietary Connections

The Exchange Hosting Service has an open connectivity policy allowing customers to evaluate and select their carrier lines from a list of suppliers that have existing presence at the Data Centre. The Exchange provides the final delivery of the circuit from the carriers' Point of Presence (POP) in our facility to the Customer's cabinet.



The main Italian and European carriers are already present in the Exchange Data Centre. The Hosting Service room and the datacentre's Telco Cabs are already cross-connected with a set of 100 Mb Ethernet connections. Customer's proprietary lines may require dedicated cross-connections between the datacentre's Telco Cabs and the Exchange Hosting room (e.g. dedicated fibre Gb connections); the cross-connection may imply the application of additional fees that have to be evaluated for each specific case.

3.2.2 Blt Network

The Exchange may provide the Client with the network infrastructure – lines and relevant apparatus – which connects the Client's site to the Hosting Service dedicated room in the Exchange datacentre.

The Blt Network service includes the monitoring of the network infrastructure. The Blt Network is also used for trading and datafeed connections to the Exchange services.

Borsa Italiana provides a Service Desk service to the Clients through which Clients are informed of possible problems affecting the network infrastructure. Such Service Desk is available by calling the toll free number 0080026772000 or to the email address service-desk@borsaitaliana.it, from 7:30 am CE to 8:30 pm CE.

There are four different connection modes between the Client's site and the central technological infrastructure of the Blt Network, at the choice of the Client:

- GOLD mode;
- SILVER mode;
- BRONZE mode.

The following is a detailed description of the connection modes.

3.2.2.1 GOLD mode

Through the GOLD access mode, the Client's site is connected to the Hosting Service room through:

- 2 communication lines (one is the primary line, the other one for back-up purposes), provided by different carriers;
- the following communication peripheral apparatus, installed at the Client's head office:
 - 2 routers
 - 2 firewalls
 - 2 switches



The available bandwidth sizes for the GOLD connections are:

- 2 Mbps
- 10 Mbps

Please see the documentation available on the Borsa Italiana' website, <http://www.borsaitaliana.it> for detailed technical information on the infrastructure (models, dimensions, occupied space, etc.) installed at the Customer's head office.

Should a problem occur on one of the two lines available or one of the communication apparatus – one of the two switches, firewalls or routers – the back-up line or apparatus is automatically activated. The recovery procedure is automatically activated by the infrastructure installed at the Client's head office.

3.2.2.2 SILVER mode

Through the SILVER (Standard and Plus) access mode, the Client's site is connected to the Hosting Service room through:

- 1 communication line;
- the following communication peripheral apparatus, installed at the Client's head office:
 - 1 router
 - 1 firewall

The available bandwidth sizes for the SILVER connections are:

- 2 Mbps
- 10 Mbps

Please see the documentation available on the Borsa Italiana' website, <http://www.borsaitaliana.it> for detailed technical information on the infrastructure (models, dimensions, occupied space, etc.) installed at the Customer's head office.

Upon the Client's request, Borsa Italiana configures an Internet client VNP connection which is used in the event of problems with the primary connection line. This way, should problems with the primary connection line occur, the Client can continue to have access to the central technological infrastructure of the Blt Network through its own VNP Internet connection.

3.2.2.3 BRONZE mode

Through the BRONZE access mode, the Client's site is connected to the Hosting Service room through an Internet connection.



The Exchange shall configure 1 Internet client connection VPN LAN to LAN, provided by the Client.

The Client shall provide the Exchange with:

- 1 Internet client connection VPN LAN to LAN;
- Network device which is able to support the connection VPN LAN to LAN.

3.3 Network Frequently Asked Questions (FAQs)

This section identifies the most common questions the Exchange is asked during the installation period.

Q) Can I use fibre to connect to your firewalls?

A) No, currently we are providing copper only up to 100 Mbps Full Duplex.

Q) Do I have to dual home my servers?

A) We would recommend that you dual home your connections to our firewalls, however, ultimately, that is your choice as you will have reduced resiliency.

Q) Once I have my switches connected to your firewalls what simple test can I do to confirm basic connectivity?

A) You should be able to telnet one of the IPs and ports of the services you need to access to

Q) Can we run routing protocol with your firewalls?

A) No, this is currently not supported. You have to use static routing.

Q) Can I have 1 Gbps or 10 Gbps fibre connection to your firewall?

A) We are currently evaluating the opportunity however this is not an available option at this time.

Q) Can I use a single (resilient) connection for all services provided?

A) Yes, this is the recommended configuration

Q) Do I have to install 2 switches?

A) Yes, we strongly advise the use of 2 switches as this provides you with the resilient set-up which we have designed in our network. Please also remember the switches should be layer 3 capable.

Q) How many servers can I have?

A) This is more limited by power/cabinet.



4 Site Procedures

This section identifies the processes and procedures required to provide access to the site. It also details the health and safety controls and requirements.

The access to datacentre must be requested to the Service-Desk (Service-Desk@borsaitaliana.it, toll free: 0080026772000, from mobile: +39 02 45411399) with one business day notice.

Urgent access (e.g. for urgent hardware failure fix) may be requested with lower notice, but the Exchange does not guarantee that the access is given before the next business day.

The access to the datacentre is allowed from 8 am to 8 pm Italian Time. Access to the Hosting Service room is allowed after the market closure (5.40 pm Italian Time).

4.1 Health and Safety

The Exchange takes the health and safety of its employees and visitors very seriously and has established processes and procedures to maintain a high standard in the Data Centre.

Should a customer be aware of a potential hazard, unsafe situation or unsafe working practice, they should communicate the hazard to the Data Centre Manager immediately.

All accidents must be reported to the Data Centre Manager who will ensure that the accident is recorded and an appropriate report made. "Near misses" must also be reported and recorded. The Hosting Data Centre Manager will ensure appropriate action is taken.

All customers are required to keep the work area in a tidy condition and must ensure that walkways are maintained free from obstruction.

4.1.1 Site Instructions for Customers

The Exchange will provide each authorised individual with a Site Instructions pack which will contain information such as:

- Hazards that may be encountered while working in our Data Centre (Exchange Risk Assessment)
- A list of general policies and procedures
- Actions to take on discovery of a fire or other emergency
- Evacuation procedures



Each authorised individual will be required to confirm they have read, understand and agree to adhere to the policies and processes before being allowed to complete work on site.

4.2 Access to site and Delivery to Site

The location of our Data Centre is:

Via Darwin 85
Settimo Milanese (MI)
20019
Italy

The main contact for arranging the delivery of the equipment as well as the set-up is the Client Technology Services Italy office:

Email: Clients-Services@borsaitaliana.it
Telephone: +39 02 72 42 6 348-606-647

4.3 Disposal of Waste Material

It is the responsibility of the customers to arrange the removal of all waste material from the Data Centre.

If customers have difficulty in removing their waste packaging material they should contact us via our Help Desk at least 24 hours in advance so the Exchange can make arrangements on the customer's behalf. Please be aware the Exchange is unable to dispose of any waste electrical equipment.

4.4 Site Frequently Asked Questions (FAQs)

Q) What is the physical Address of exchange with Postal/Country code?

A) The address of the datacentre is:

I.Net
Settimo Milanese (MI)
20019
Italy

Q) What is the physical Address for Shipping with Postal/Country code?

A) Same as above

Q) Are there any special requirements for shipping hardware to this location internationally?

A) The shipping, as well as the installation, should be noticed with 2 business days of advance to ourselves in order to arrange the datacentre access rights

Q) Does the Customer have 24x7 support & Access into our Cage/Rack(s)?

A) Support is provided from 7.30 am to 8.30 pm Italian time. Access is granted with the next business day (best effort)



5 Equipment Installation

5.1 Equipment Installation

Customer installations must meet the standards identified in this section and will be subject to Exchange approval either ahead of Service “go-live” or following any subsequent changes. The Exchange requests Customers to submit, in advance of any installation, the cabinet installation elevation and network designs in a professional and clear format. In particular the Exchange is keen to understand that the devices being installed will utilise the cold and hot aisle layout and that all devices are suitable for the cabinets.

The Exchange can provide any cabling to the detailed specification of the customers (e.g. the cabling required for customer’s proprietary lines connection to the Exchange Hosting room). The additional cabling may imply with additional fees (to be analysed for each specific case. Customers should approach their Exchange Hosting contact to request a quote for this activity.

Customers can choose to install their own equipment into their allocated cabinets on condition that a suitable health and safety risk assessment and method statement has been submitted to the Exchange in advance.

Where Customers require more than one cabinet and the cabinets are required to be interconnected, adjacent racks will be selected when available (depending upon requirements) and various solutions will be offered to accommodate inter-rack cabling.

The Exchange will complete all under floor cabling on behalf of Customers. Customers are NOT permitted to access any under floor areas within the data centre. If there is a requirement to lift floor tiles this will be completed by an Exchange resource.

Where Exchange support is required during any installation, Customers are asked to provide a minimum of 7 working days notice.

The Exchange reserves the right to remove equipment not installed to this standard and if corrective actions are not performed by the Customer. All corrective work will be completed at cost to the customer.

5.1.1 Installation Guidelines

It is important that all equipment installation conforms to the following standards:

- Once all equipment has been installed the remaining free cabinet space must be completely blanked off using the approved blanking panels.
- If monitors are required, these must be of the collapsible KVM type, which occupy 1U of cabinet space, to facilitate the effective use of blanking plates.



- All cabling must be neatly installed and tie-wrapped to ensure there is no loose cabling, and that the cabinet door is able to close unhindered

5.1.1.1 Rack mounting equipment guidelines

The cabinets allow customers to stack computer components vertically; however customers must take precautions to provide for rack stability and safety.

- Before working on the rack or extending a component on rails, customers should be sure that the levelling feet have been extended to the floor, the full weight of the rack rests on the feet, and the rack is level and stable.
- Extend only one component at a time. The rack may become unstable if more than one component is extended.
- All equipment must be installed by competent engineers who are adhering to approved industry installation standards and the hardware manufacturers install guidelines.

5.1.1.2 Equipment positioning guidelines

The following assembly guidelines must be adhered to for an implementation to comply with the installation standard:

- Hardware must be installed in accordance with the Exchange approved technical rack design
- For safety and rack stability, customers should load the heavier components first (these should be at the bottom of the rack.)
- The copper networks drop bar is installed rear facing at rack location U42 (top of rack) and, when required, the optical networks drop bar will be installed rear facing at U41.
- Cabling should not obstruct airflow within the rack.

All equipment installed into Hosting cabinets which draws air for cooling purposes from the front or rear of the chassis, must be installed to draw cool air from the “cold” aisle and blow air into the “hot” aisle. Confirmation as to where the hot and cold aisle can be confirmed in advance, once the rack design of the installation is provided to the Exchange.

5.1.1.3 Server cable management guidelines

As identified previously, the Exchange will complete all under floor cabling on behalf of customers. Customers are NOT permitted to access any under floor areas within the data centre. If there is a requirement to lift floor tiles this will be completed by an Exchange resource via a request to the Exchange.

The following standard practices must be adhered to by the customer within their cabinets



- Customers are not permitted to alter the Exchange interfacing copper or fibre patch panels within their cabinets without prior Exchange consent
- All cables must be neatly concealed in the correct cable management rack conduit
- The cabling in the cabinets must be tidy and not so excessive that it prevents the cabinet door from closing
- Cables should not cross from one side of the cabinet to the other side. Cables coming from the left/right hand side of the cabinet should connect to the left/right half side of the patch panel
- Patching on cabinets that host the equipment should be performed so that all cables are drawn away from the fan to allow for easy replacement of parts should this be required. This method will also assist in heat dissipation.
- It is required that cable installations are secured and bundled with Velcro or Millipede cable ties as they do not exert any undue stress to the cables
- Kinks or collapses should be avoided where possible by supporting the cable bundles correctly. These occur when cable ties have secured the bundled cables as they pass from the vertical cable management in the cabinet to the patch panel where they are terminated.
- Cables should be individually tied to the support bar, and not tied in groups
- All cables should reasonably fit the installation. Excessive length in cables is not permitted

5.1.2 Power Configuration

Two power strips are provided in each cabinet as standard. Each of these power strips are fed via a separate UPS supply. Customers are therefore recommended to use equipment which has dual power supplies to avoid potential single points of failure.

All Exchange Hosting cabinets have the ability to provide up to 5kW. The Exchange provides customers up to 3kW or up to 5kW based on the agreed contract.

Please note that customers exceeding their agreed allocated power levels will be served a request to reduce their power draw within an identified timeframe (which may be immediately). The Exchange reserves the right to disconnect the power to the cabinet if the issue is not resolved within the timeframe and may result in the Exchange terminating the agreement with the customer.

5.1.2.1 Power Distribution Units

The customer is required to provide its own Power Distribution Unit (PDU) for each requested rack. Single phase 32 Amps PDUs are to be used. IEC AC Power recepticals are used.



5.2 Demarcations points

5.2.1 Power Demarcation point

The Customer is responsible for the power connection from either the Exchange-provided cabinet power bars (the “power demarcation point”) to the Customer’s Equipment or to the Customer’s own power bars if supplied by the Customer.

5.2.2 Network Connections Demarcation Point

5.2.2.1 Demarcation Point - Trading and Information services

All network connectivity to the trading and information services will be presented in the network patch panels in each cabinet. Connections from these patch panels to the Customer Equipment is the responsibility of the Customer. Connectivity of the patch panel to the Exchange’s trading and information services and the patch panel itself is the responsibility of the Exchange.

The Exchange is not responsible for the provision of cables or physical connecting Customer Equipment to the cabinet patch panels within their cabinet.

5.2.2.2 Demarcation Point – Customer Connectivity

The Exchange has responsibility for provisioning and operating the connections from the Customer’s Carrier and the Customer’s cabinet. The demarcation for the service for both fibre and copper media types are from the Datacentre provisioned patch panel in the Telco cabinet (and including the patch panel) (the “**Carrier Demarcation**”) to, and including the Exchange provisioned patch panel installed in the Customer’s cabinet (“**Customer Cabinet Demarcation**”).

A reminder that the Exchange is not responsible for the Carriers’ services or cabling beyond the areas outside of the areas identified above.

Unless specifically requested by the Customer, the Exchange is not responsible for the provision of cables or physical connecting of customer equipment to the cabinet patch panels within their cabinet.

5.3 Customer Enablement Process

Customers can access the following markets from the Hosting Services facility:

- Borsa Italiana IDEM market
- Borsa Italiana MDF and DDM plus market real-time data feed
- Borsa Italiana BCS Clearing service



5.4 Testing Policy and Procedures

5.4.1 Management Connectivity Testing

It is essential that Customers are able to prove connectivity to their equipment via their management connection before any other testing is considered. The Exchange's network teams are available to liaise with Customers while they troubleshoot their connections.

The on-boarding team will liaise with the Exchange networks teams to ensure customers have adequate assistance during this initial network testing and troubleshooting phase.

5.5 Installation Frequently Asked Questions (FAQs)

Q) Should the Customer provide patch cables or can the Exchange?

A) The cable should be provided by the Customer

Q) What is the size of a single rack/cabinet (in U) and the dimensions?

A) Each rack has 42 rack units with the standard Rack Unit dimension

Q) What type of PDUs are used (amps/volts)?

A) PDU have to be provided by the customer and should be single phase 32 amps ones

Q) What is the kW per rack/cabinet?

A) The power may be up to 3 KW or 5 KW with different pricing

Q) What type of AC Power connection do you use?

A) IEC

Q) Who is the Customer main contact for the setup?

A) The main contact for the set-up is the Client Technology Services Italy office:

Email: Clients-Services@borsaitaliana.it

Telephone: +39 02 72 42 6 348-606-647

Q) Who is the Customer main contact for Exchange connectivity?

A) For the set-up phase the contact is the same as above, once in production the main contact is the Service Desk (the same for all production issues):

Email: Service-Desk@borsaitaliana.it

Toll free: 0080026772000

From mobile: +39 02 45411399

Q) Who is the Customer main contact for production issues?

A) Same as above (Service-Desk)



6 Service Operation

6.1 System Monitoring of the Exchange Hosting Service

As detailed previously, the Exchange monitors each port on the access firewalls however, as the Exchange cannot determine if the device interfacing the Exchange has been purposely disconnected, the Exchange will only investigate an issue when we have identified that all ports on a specific firewall or if the firewall itself has failed. Customers should therefore escalate any specific single port issues that arise to the Exchange as a matter of urgency (see section 7).

The Exchange does not actively monitor clients' side connections.

Where a site incident has occurred the Exchange will communicate with the customers impacted as appropriate (see section 7).

6.2 Reporting a Fault with the Exchange Hosting Service

Customers who have an issue with Exchange Hosting Service should raise an event via the Service Desk (service-desk@borsaitaliana.it, toll free: 0080026772000, from mobile: +39 02 45411399). This number is available for 7.30 am to 8.30 pm our operators will escalate any issue to the correct support team.

Customers are requested to provide their name and contact details, company name, the nature of the issue and any remedial activities that have been attempted prior to the call. The Exchange engineers will liaise directly with the customer once some preliminary checks have taken place.

6.3 Change Management Process

Where Customers require changes to their installation that require a change in the way they interface with the Exchange, the Customer must provide notice of the change and obtain Exchange approval ahead of any change.

Customers should contact either the Client Technology Services Italy team via email clients-services@borsaitaliana.it or telephone +39 02 72 42 6 348/647/606

6.4 Exchange Routine and Unscheduled Maintenance

The Exchange may need to perform routine or unscheduled maintenance to the data centre from time to time which may lead to restricted access for customers. Where notice can be provided in advance the Exchange will communicate by email notification to the Primary Authorised Individuals. Customers should be aware that there may be occasions where we are unable to communicate in advance.



6.5 Customer Usage of the Hosting Service

The use of the Hosting Service must comply with the terms of the Agreement agreed for the Hosting Service. For a copy of the Master Terms and relevant Schedules, please contact the Client Technology Services Italy team via email clients-services@borsaitaliana.it or contact +39 02 72 42 6 348/647/606. Any breach of these terms could result in the Hosting Service being suspended immediately until the issue has been resolved.

6.5.1 Service Prohibitive Purposes

The following sections provide guidance to customers on specific Exchange policy with regards to some of the prohibitive purposes of using the Exchange Hosting and added value services.

6.5.1.1 Reselling of Cabinet Space

Cabinet space may **not** be resold, sub-licensed or leased to third parties by Customers. For the avoidance of doubt however, where a Customer is providing Agency trading services and, whereby, the cabinet owners' trading codes are used for all trades on any of the relevant Exchange Group Markets, this will not be considered reselling, leasing, or licensing.

6.5.1.2 Customer Cabinet Cross-Connects

Customers are permitted to request the use of, and installation by the Exchange of, certain communications lines between separate Customer cabinets for the purposes of Trading Flow only (these lines are known as "cross connects"). Customers are not permitted to utilise these cross connects for any other purpose (including, without limitation, the transportation of any market data, time sync messages, etc), unless permitted under the Hosting Services Master Terms and Schedules (as relevant) or as otherwise agreed in writing by the Exchange.



7 Escalation Procedures

In the unlikely event of a data centre incident or failure which either leads to restricted access or to a suspension of the Exchange Hosting Service we will communicate to the Customer and advise of specific issue and the impact to the Hosting service. The Exchange will continue to communicate updates to those contacts throughout the incident and will provide estimated recovery time if available.

If access is required following an incident, we will attempt to provide this to customers as soon as possible, however it is our priority to ensure the environment is safe before permitting access to the Hosting area. In addition, to ensure the Hosting environment remains safe we will arrange access for customers in a timely manner.

As identified in the previous section, where customers believe they have an issue with their cabinet, configuration or other Exchange Hosting service they should raise an event via the Service Desk (service-desk@borsaitaliana.it, toll free: 0080026772000, from mobile: +39 02 45411399).



8 Data Centre Technical Specification

8.1 General Datacentre Characteristics

8.1.1 Introduction

Datacentres are rapidly evolving to respond to higher growth, consolidation and security demands. Increasingly demanding uptime and service availability requests combined with new technologies and equipment make design efforts more challenging. A Data Centre must be able to support rapid growth without discontinuity, the addition of new services without the need for extensive restructuring and must not have any single point of failure while still providing precise indications on guaranteed uptime.

On the subject of infrastructural and physical security, the most recent inputs from the technological and contextual evolution have emphasized the value of an infrastructure whose design goal is the Customer's Business Continuity.

In fact, when a Company assesses the features of an external data centre for their mission critical architecture, it privileges the capacity to truly minimize Business discontinuity risks and to maximize problem response time and quality rather than pure cost rationalization.

Among the scenario changes that have the biggest impacts on **data centre design** are:

- the change in passive security policies after September 11, 2001
- the demonstration that power supply can be unreliable in continuity and unpredictable in quality, following the events in America on August 14 and in Italy on September 28, 2003, with impacts on fire risks
- the introduction of new servers that occupy less space, consume more electricity and disperse more heat (blade machines) and the need to restrict power consumption as much as possible
- band availability that permits large volume data exchange from one site to the next.

When defining design specification, these elements require special attention concerning:

- anti-terrorism measures and human flow management
- space and power dimensioning, electrical and mechanical distribution flexibility
- fire prevention
- air conditioning system power and flexibility.



8.1.2 The building

The geographical location of the site is excellent from the seismic and flood risk standpoints and concerning risks due to the vicinity of hazardous industrial plants. The Settimo Milanese area where the building is located is not subject to any critical risks due to the presence, within a range of 4 km, of hazardous material industries or warehouses; no airports are located in the area. The location is not adjacent to waterways that risk overflowing and the waterbed is sufficiently deep.

The building, designed and built according to anti-seismic criteria, is made up of two main structures with five floors aboveground and an underground floor where the fire prevention and air conditioning water tanks are located.

The ground floor is devoted to entrance, power centres and warehouses while the fourth floor is intended for office space.

Floors 1, 2 and 3 are exclusively reserved for data rooms and are completely surrounded by an external hallway, protected by a reinforced concrete wall, which houses all equipments that data centre needs (air conditioning and water supply for air conditioning and fire systems). The presence of the concrete shield grants the building a superior physical security on one hand, and on the other hand allows O&M procedures on the equipments to be completed without entering data rooms.

Each such floor extends for about 1000 square meters per structure and is a single REI 120/180 compartment that contains additional REI 120 compartments within.

The two main structures are connected by a central structure that guarantees physical separation while permitting access from one wing to the other; the central structure also houses the vertical conduits for electrical and utility systems.

The structure includes a main entrance at the front of the building and two, separate rear entrances for material deliveries and emergency exits.

The roof has a rain water drain system and waterproof system without PVC membrane.

Overall dimensions are about 14,740 gross square meters of which 5,940 net square meters are dedicated to the Data Centre and 1,800 gross square meters to office space; the remaining space houses technological systems (for power and cooling) warehouses and common spaces.



Data rooms main modules (330sqm each) can be flexibly divided into smaller modules (customer specific data rooms), down to a minimum of 13 square meters, in order both to support substantial initial installations and to accompany the customer gradual adoption of outsourcing and/or Business Continuity solutions.

I.NET Business Continuity and Disaster Recovery proposition includes also a workplace recovery offering, with specifically designed office spaces.

All technological systems were designed to be *single point of failure* free with N+N redundancy to guarantee service continuity even during extraordinary maintenance.

The centre is attended by specialized technical personnel, 24/7, 365 days a year to operate and monitor technological systems.

8.1.3 Human Flow management and anti-terrorism measures

Multiple data room access control allows the best human flow management, with individual entrance systems (like the ones used in banks), badge controls and TV/CC.

Emergency exits are equipped with audible alarms and are controlled and monitored by closed circuit cameras activated by motion sensors. Alarms and control devices are able to work in any condition.

All the security measures provided allow an all year round, 24x7, Customer access to the Business Factory.

To counter the threats that terrorism puts on business continuity, the physical infrastructure is subject to very strict requirements.

I.NET's Business Factory has reinforced concrete walls surrounding the entire structure with an external, collapsible wall.

Except for the top floor which is intended as office space, the external reinforced concrete wall has no windows, only 18 cm high slots.

Anti-climb barriers, external lighting, dual technology sensor detection system and closed circuit cameras monitored around the clock by a surveillance squad with all alarms concentrated in the Control Room have all been implemented to prevent intrusions.

8.1.4 Electrical system

The need for a company to operate without interruption (uptime virtually 100%) requires an electrical system that can:



- guarantee continuity and redundancy even during potential catastrophic events such as fire or critical breakdowns and therefore must be able to provide solutions with 2N + 2N redundancy
- guarantee the completion of all routine and extraordinary maintenance without losing continuity and redundancy
- have autonomous power generation capacity that not to be considered only as a simple redundancy of normal supply but also as an autonomous system and therefore, as such, self-redundant.

Two distinct rooms dedicated to electrical systems (Battery, Converter, UPS, distribution rooms) are located in each of the two main structures.

I.NET's Business Factory stands out for its unique ability to meet requirements of power consumption and heat dispersion superior to current standards in order to host without concern new generation equipment installations and/or support an uneven distribution of power needs within the room.

8.1.5 Fire prevention

Fire prevention must be as thorough as possible: each room in the building has an automatic fire prevention system with built-in protection, except for the power rooms where only detection is in place.

8.1.5.1 Smoke detection

All rooms, including technical utility rooms, are equipped with fire point detectors; data rooms have redundant VESDA smoke detection systems (both at the ceiling and under the floor), able to generate alarms to warn surveillance personnel, to automatically activate associated extinguisher systems and manage any faults, activating the backup system.

8.1.5.2 Fire extinguishers

REI120 compartments are contained within the two production buildings to separate all critical rooms from each other and from the rest of the building (battery, converter, UPS, warehouse).

All vertical conduits are external and separated from the building and also the electrical and mechanical interconnections between the two buildings are external.

In building areas reserved for data rooms, the automatic room saturation extinguisher system guarantees power continuity during and after a fire event as well as the personal safety of anyone within the rooms; a double discharge of gaseous chemical extinguisher is used. The system is able to control several hotbeds simultaneously, preventing smoke invasions, sudden temperature peaks and the dispersion of residue harmful to man and equipment.



Arrangements have also been made to house, upon specific customer request, a second sprinkler (spray) fire extinguisher to put out fire in case it gets out of control. This second system will interrupt power.

Non-technological areas in general (i.e. halls, systems hallways, offices) are protected by sprinkler systems. In the event of fire, power is cut off only in the affected areas.

Battery, Converter, UPS rooms have only a detection system in place which can locally interrupt power in order to avoid fire propagation; thanks to system redundancy, there are no interruptions in power distribution in the rest of the areas.

Water pipes are not located inside areas reserved for data rooms. Liquid detection probes are located in areas deemed critical outside the Data Centre; any water leaks are suitably conveyed or pumped to external drains.

8.1.6 Air conditioning systems

Air conditioning systems must be able to guarantee target air pressure, temperature and humidity values in every system point, even in “extreme” conditions and must guarantee the possibility of maintenance without causing difficulties.

Waterbed (more than 40 meters deep) water is the main means of cooling in summertime, while in winter a free cooling system is in place.

All air conditioners are located outside the data rooms to avoid vibrations or risk leakage inside the rooms. In case of fault in the waterbed water or free cooling system all air conditioning units are automatically activated and can work autonomously.

As well as the power systems, air conditioning and In and Out air flow management systems have been designed to meet heat dispersion requirements superior to current market standards.

8.1.7 Passive security

- External protection
- Two separate building
- No external openings
- External armed concrete shield
- Aseismic structure
- External steel barriers
- Duplicated technical rooms



8.1.8 Security

- 2 security systems (VESDA):
 - continuous air analysis
 - burned molecules survey
 - Alarm
- 2 different extinction systems for each floor
 - Primary GAS INERGEN
 - Secondary WATER SPRINKLER 4l/MIN. for each mq.
 - 2 x 300 m³ bathtubs
- 4 access compasses with Optical acknowledgment
- 98 external & internal cameras
- 118 contacts for detect intrusions
- 658 badge readers
- 2 control rooms
- 84 lines for electrical and environmental acquisition points
- 2450 acquisition points
- 500 presence sensors
- 14 PLC
- 2 Supervisor servers
- 2 anti fire control rooms
- 1 anti intrusion control room
- 2 video recorder systems

8.1.9 Power

- 8MW dedicated to client systems
- 15kW avg./m²
- 2MW dedicated to cooling, light and services
- 10MW max. Power
- Diesel generator
- 4 days fuel storage capacity
- 1 electrical cabinet for each side of the building (2)
- 5 TRAFO (2.500 kW each) for each side of the building
- 6 UPS –1.200 kW for each side of the building



9 Service Contacts

Request Access to Site	Client Technology Services Italy clients-services@borsaitaliana.it +39 02 72 42 6 348/647/606
Service Fault or Incident	Service Desk service-desk@borsaitaliana.it Toll free: 0080026772000 From mobile: +39 02 45411399
Notification of Site Delivery	Client Technology Services Italy clients-services@borsaitaliana.it +39 02 72 42 6 348/647/606
Exchange Hosting Sales and Technical Account Management	Client Technology Services Italy clients-services@borsaitaliana.it +39 02 72 42 6 348/647/606
Service Desk	Service Desk service-desk@borsaitaliana.it Toll free: 0080026772000 From mobile: +39 02 45411399

Table 3 - Service Contacts



10 Appendix A - Time Synch Service

The Exchange can provide a highly precise time synchronisation service for Customers located in the Data Centre.

Customers are not permitted to install their own antenna in the Exchange Hosting Data Centre.

10.1 Service Overview

The Time Sync Service is provided via standard NTP service. The service is provided through the two production connections provided for the market connection.

Customers will be provided with the destination IP Addresses of the source module during the implementation activities.

10.2 Ordering the Service

A Service Order form for the Time Sync Service can be requested from the Client Technology Services Italy (clients-services@borsaitaliana.it, +39 02 72 42 6 348/647/606).



London
Stock Exchange Group

