

SERVICE AND TECHNICAL DESCRIPTION

Exchange Hosting Service

SEPTEMBER 2021 – VERSION 1.1



BORSA ITALIANA

TABLE OF CONTENTS

- 1. Introduction 4**
 - 1.1. Document history 4**
 - 1.2. Purpose 4**
 - 1.3. Readership 4**
 - 1.4. Amendment of this Documentation 4**
- 2. Overview of the Service 6**
 - 2.1. Key Features of the Service 6**
 - 2.2. Performance Improvements 7**
 - 2.3. Service Offering 7**
 - 2.4. Customer Benefits 8**
 - 2.5. High Level Network Diagram 8**
 - 2.6. Pre-requisites for the Service 9**
 - 2.7. Ordering the Hosting Service 9**
- 3. Network and Connectivity Design 10**
 - 3.1. Connectivity to Exchange Services 10**
 - 3.2. Customer Connectivity 12**
 - 3.3. Network Frequently Asked Questions (FAQs) 12**
- 4. Site Procedures 14**
 - 4.1. Health and Safety 14**
 - 4.2. Access to site and Delivery to Site 14**
 - 4.3 Disposal of Waste Material 15**
 - 4.4 Site Frequently Asked Questions (FAQs) 16**
- 5. Additional Added Value Services 17**
 - 5.1. Time Synchronisation Service 17**
 - 5.1.1. Precision Time Protocol (PTP) Time Feed 17
 - 5.1.2. GPS Time Feed 19
 - 5.2. Remote Hands Service 20**
- 6. Equipment Installation 22**
 - 6.1. Equipment Installation 22**
 - 6.1.1. Installation Guidelines 22
 - 6.1.2. Power Configuration 24

6.2. Demarcations points	25
6.2.1. Power Demarcation point	25
6.2.2. Network Connections Demarcation Point	25
6.3. Customer Enablement Process	25
6.4. Testing Policy and Procedures.....	26
6.4.1. Management Connectivity Testing	26
6.5. Installation Frequently Asked Questions (FAQs)	26
7. Service Operation	27
7.1. System Monitoring of the Exchange Hosting Service	27
7.2. Reporting a Fault with the Exchange Hosting Service	27
7.3. Change Management Process	27
7.4. Exchange Routine and Unscheduled Maintenance	28
7.5. Customer Usage of the Hosting Service.....	28
7.5.1. Service Prohibitive Purposes	28
8. Escalation Procedures	29
9. Data Centre Technical Specification	30
9.1. General Datacentre Characteristics	30
9.1.1. The building	31
9.1.2. Human Flow management and anti-terrorism measures.....	32
9.1.3. Electrical system	32
9.1.4. Fire prevention	33
9.1.5. Air conditioning systems	34
9.1.6. Passive security	34
9.1.7. Security	35
9.1.8. Power	35
10. Contacts	36

1. INTRODUCTION

1.1. Document history

Version	Date	Description
1.0	April 2021	Version 1.
1.1	September 2021	Clarify policy in paragraph 3.2

1.2. Purpose

The purpose of this document is to provide customers with a detailed definition of the Borsa Italiana Exchange 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 at the following link:

<http://www.borsaitaliana.it/borsaitaliana/gestione-mercati/connettivita/connettivita.htm>

1.3. Readership

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 Documentation

This document may be amended at any time and, areas impacting service provision will be effective following 30 days’ 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

The Exchange Hosting Service provides 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 trading hardware within the Exchange's Data Centre 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, and Accredited Borsa Italiana Service Providers.

For further information, please contact the Milan Hosting team via our email address: hostingops-milan@borsaitaliana.it.

2.1. Key Features of the Service

- **Hosting within the Exchange's data centre** where the IDEM/IDEX market, the MTA, TAH, MOT, EuroTLX, SEDEX and ETFplus markets are located as well as the GTP 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 following Exchange Group Markets** - potential to connect to any of the following markets:
 - Borsa Italiana IDEM and IDEX markets;
 - Borsa Italiana MTA, TAH, MOT, EuroTLX, SEDEX and ETFplus markets
 - MTS
- **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,
- **Additional added value services:**
 - Dedicated team of skilled engineers available for remote hands activities
 - MiFID II compliant time synchronisation service.

2.2. Performance Improvements

Customers utilising the Exchange Hosting Service will be provided with the following key performance benefits produced by reduced latency between the Exchange's IDEM, MTA, TAH, MOT, EuroTLX, SEDEX and ETFPlus markets and GTP platforms and the Customer's own trading applications:

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

For further information on the specific latency savings please contact the Hosting Team.

2.3. Service Offering

Access to the following markets (Production and Test)	
Borsa Italiana IDEM and IDEX markets	Yes
MTA, TAH, MOT, EuroTLX, SEDEX and ETFplus markets	Yes
MTS	Yes
Market Data Services	Yes
Power usage (kilowatt per cabinet)	3kW or 5kW
Cabinet Connectivity	
Trading/Information cross-connections to the production environment	2+
Trading/Information cross-connections to the CDS environment (if required)	2+
Management cross-connections for Customer connectivity purpose ¹	2+
Cabinet to Cabinet cross-connections – Trading Participant (Non-Member) cabinet to Trading Participant (Member) cabinet	1+
Time Synchronisation	
GPS Time Synchronisation	
PTP Time Synchronisation	
Value Added Services	
Highly skilled remote hands service	

¹Wide range of different carrier connectivity options; Resilient carrier provision available

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 BitNet, CMC or Service Provider solution).

2.4. Customer Benefits

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 customer equipment and the Exchange’s trading and datafeed services:

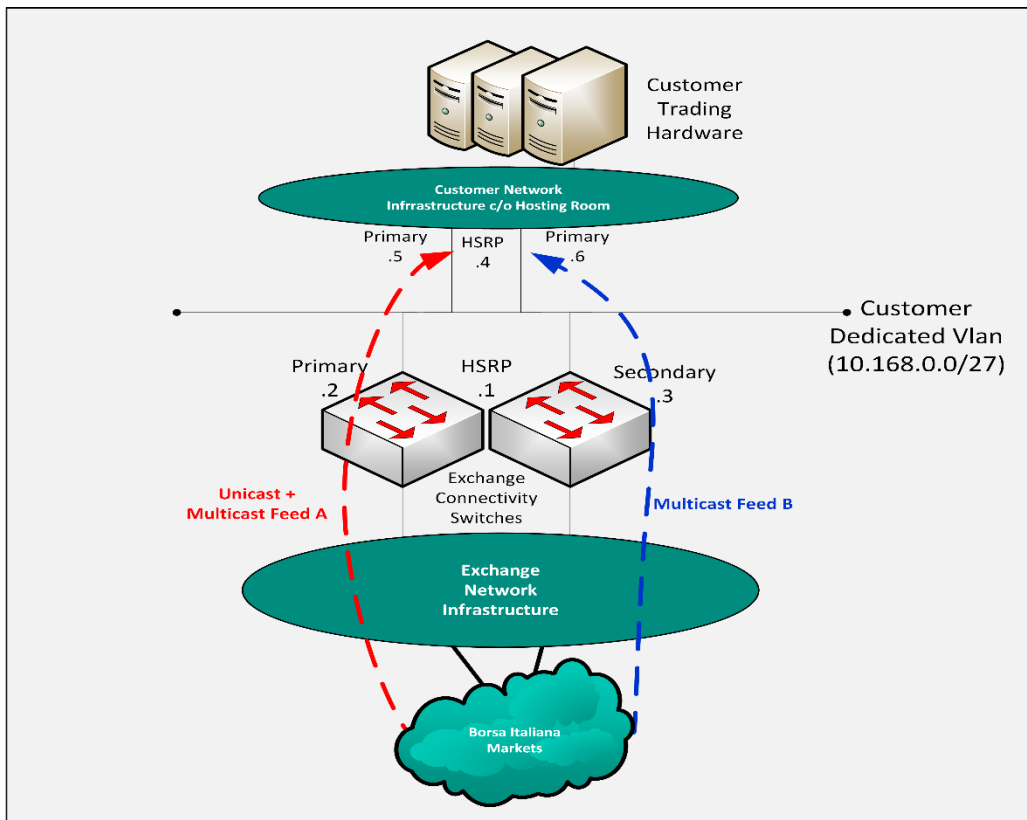


Figure 1 - Hosting Market Connection – High Level

The following high-level diagram identifies the options for the connection of the Customer’s site to the Customer’s Exchange hosted equipment:

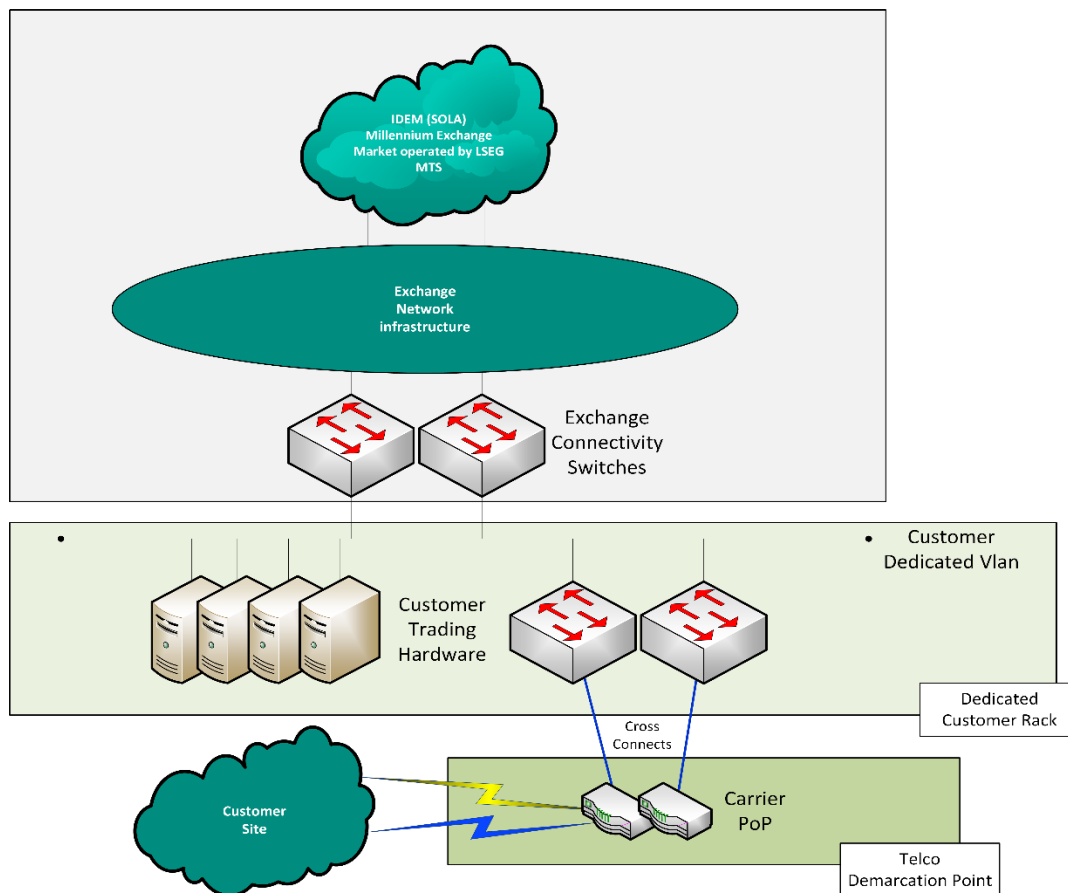


Figure 2 - Overview Customer Connectivity – High Level

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 comply with, inter alia, the Exchange, Trading Membership process and regulations.

2.7. Ordering the Hosting Service

The Customers who are interested in taking the Exchange Hosting Service should contact the Exchange Hosting team via email hostingops-milan@borsaitaliana.it or contact Milan Hosting Team.

For any questions of a contractual nature please refer to the Hosting Service Agreement.

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 the customer's own chosen carriers.

It is important to note that all configuration changes to the Exchange Hosting environment and infrastructure are completed during the identified change window – 6:00 pm to 01:00 am each weekday (excludes Italian 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 their primary and secondary switches to the Exchange primary and secondary switches.

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

Each trading system connection provided to the customer cabinet is 10 Gbps LC multimode fibre terminating within the customers cabinet.

The Exchange services may operate either in Unicast or Multicast:

- SOLA operates with:
 - Unicast protocol connections for the trading interface
 - Multicast and/or Unicast protocol connections for the market datafeed (HSVF) interface
- Millennium Exchange operates with:
 - Unicast protocol connections for the trading interface
 - Multicast protocol connections for the market datafeed (GTP) interface

As standard, clients are offered the following physical connections:

- 2 x customer switches to Exchange switches for production environment connection (all services included)
 - These connections are 10 Gbps, in both cases the connections are provided in multimode fibre with LC connector
- 2 x customer switches to Exchange switches for CDS environment connection (all services included) – installation upon request.
 - These connections are 1 Gbps copper

Additional market handoffs can be ordered by the Customers (subject to availability and applicable terms).

The client subnets that will directly interface with Exchange services will be provided by the Exchange. The customer's servers must present themselves to the production and CDS (if applicable) environment with addresses that belongs to the given subnets.

As standard, the following subnets are offered to the customer for each market handoff:

- 1x subnet /27, included in the range 10.168.0.0/16, for the connection between Customer and Production Exchange switches and for access Production environment
- 1x subnet /28, included in the range 10.168.0.0/16, for the connection between Customer and CDS Exchange switches and for access CDS environment

Once customers have their switches connected to the Exchange switches a simple "ping" test to the IP(s) of Exchange Switches can be completed.

The Exchange monitors each port on the access switches 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 switch are down or if the switch itself has failed. Customers should therefore escalate single port issues 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 switches to maximise the resilient infrastructure, however this is not mandatory.

3.2. Customer Connectivity

Customer Proprietary Connections can be used by Customer to reach their hosted equipment (for management and administration purposes) from their own locations. These also allow customer remote systems (located at the customer's IT site(s)) to access the Exchange services.

The Exchange Hosting Service has an open connectivity policy allowing customer to evaluate and select their carrier lines from a list of suppliers that have existing presence at the data centre. The main Italian and European carriers are already present in the Exchange data centre. The Exchange connects to **two carrier areas** within the Primary Data Centre via structured cabling whereby Carriers, who supply services to clients of the Exchange Hosting Service, can be connected to collocated cabinets.

Customers are kindly invited to ask the Exchange's Hosting Team for a pre-check as to which Telco room should be used by selected Carrier for ending their WAN connections.

The Exchange provides the final delivery of the circuit from the carriers' Point of Presence (PoP) to the Service Providers co-location cabinet. These connections are delivered in single mode fibre with LC connector.

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 copper to connect to your production switches?

A) No, we provide 10 Gbps LC multimode fibre full duplex production connections.

Q) Can I use fibre to connect to your test switches?

A) No, currently we provide 1 Gbps copper full duplex for test connections.

Q) Do I have to dual home my servers?

A) We would recommend you dual home your connections to our switches, however, ultimately, this is your choice as it affects your resiliency.

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

A) You should be able to ping the IPs of the Exchange Hosting Switches

Q) Can we run routing protocol with your switches?

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

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) 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 limited only by cabinet space and power allowance.

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.

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

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 onsite data centre engineer immediately.

All accidents must be reported to both the onsite data center engineer and Milan Hosting Team who will ensure that the accident is recorded, and an appropriate report made. "Near misses" must also be reported and recorded. The Milan Hosting Team 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.

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 C. Darwin 85,
Settimo Milanese (MI)
20019, Italy

The main contact for arranging the delivery of the equipment as well as the access to the hosting room is the Hosting Team:

Email : **hostingops-milan@borsaitaliana.it**
Telephone: +39 02 72 426 418 / +39 02 72 426 348

Access can be requested for 6:00 pm - 01:00 am the following morning Monday to Friday as well as weekends on special request sending an email to hosting ops team at least 24 hours in advance.

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

In order to ensure the protection of our customers, employees, and reducing the spread of the coronavirus (COVID-19), the following temporary site access restrictions are in place (until further notice) to access Milan Hosting Room; the health and well-being of our colleagues, customers and guests is of paramount importance to Euronext N.V., and we would like to thank you for your assistance in adhering to these policies:

- All visitors must adhere to social distancing requirements (following current local Government rules and guidelines, with a minimum of 2 meter or 6 feet of separation at all times) and wear masks before entering site and keep them on for the duration of their visit. This is MANDATORY, if any visitor is seen via CCTV not wearing a mask, they will be asked to leave site immediately
- Upon arrival the visitors must present Government issued photo ID
- A maximum of 3 customer or third-party engineers are permitted on site at same time for any break fix or scheduled activities during standard access hours.
- Visiting engineers are only allowed entry to the site to start their work and exit upon completion (no leaving and returning for food/cigarette breaks will be allowed)
- It is mandatory that visitors do not take food, drink or smoke in the DC hall, if they are seen via CCTV to have food or drink in the hall they will be asked to leave site immediately
- Visiting engineers are only to be working in VERY CLOSE proximity to the approved cabinet location
- Security will prepare Visitors Passes in advance, and will only be handed over once ID has been confirmed

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:

BT Italia
Via C.Darwin 85,
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) All planned works must be undertaken during the Exchange's standard change window.

5. ADDITIONAL ADDED VALUE SERVICES

The Exchange Hosting Service is also able to provide Customers with added value services such as Time Synchronisation and Remote Hands.

5.1. Time Synchronisation Service

The Exchange can provide a range of resilient, highly precise time synchronisation services for Customers located in the Data Centre.

The Time Synchronisation Service consists of two delivery formats:

- Precision Time Protocol (PTP)
- GPS

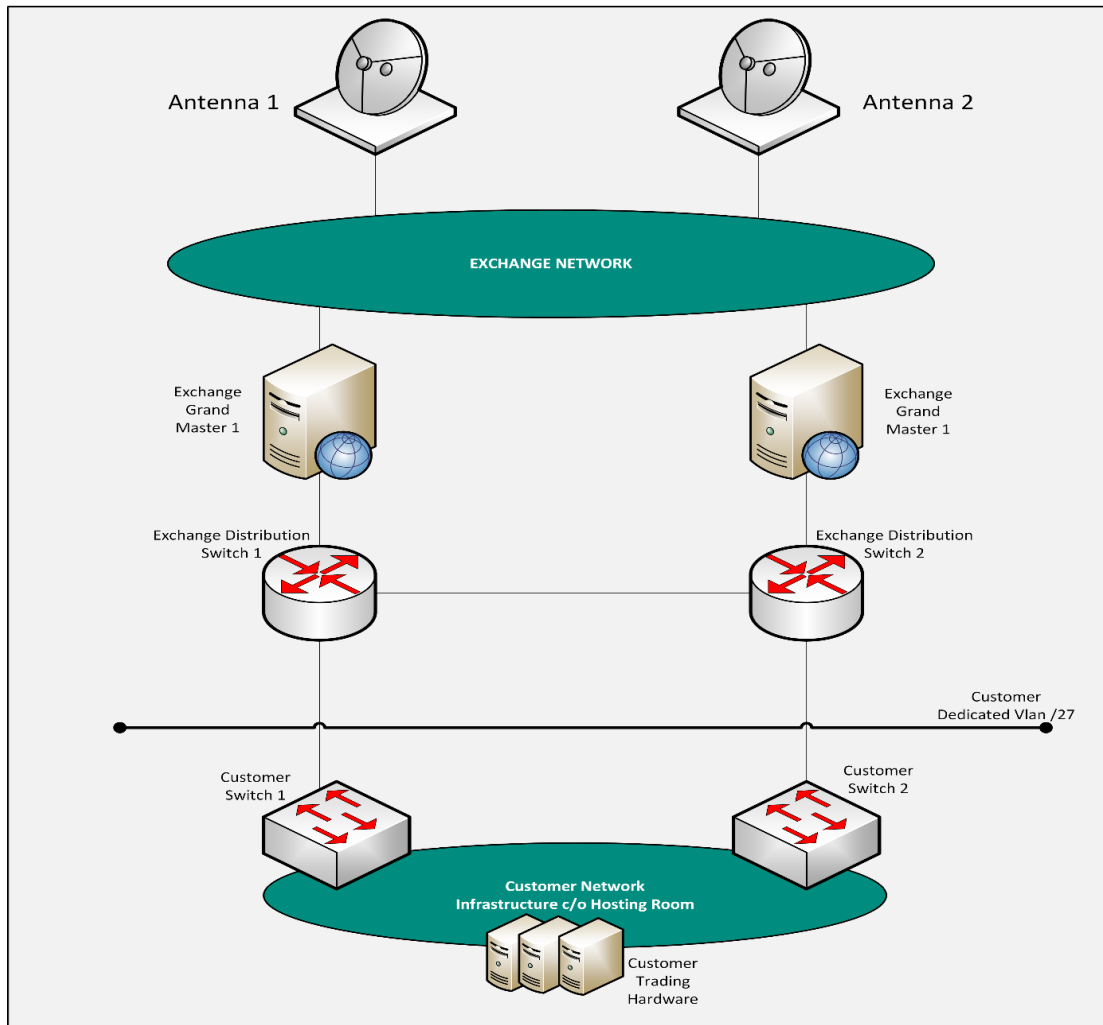
The service is duplicated for resilient delivery of the time signal. Customers are not permitted to install their own GPS antenna in the Exchange Hosting Data Centre

5.1.1. Precision Time Protocol (PTP) Time Feed

The Precision Time Protocol (PTP) time feed provides resilient and diverse feeds that achieve MiFID II compliant accuracy.

To maintain accuracy and resiliency, the PTP Feed is serviced by two separate GPS antennae located in diverse positions on the Exchange Data Centre roof. Furthermore there is resiliency built in across the solution to ensure an alternative source is available in case of issues with the primary.

The following schematic diagram identifies equipment setup for PTP time source and PTP feed distribution:



Grandmaster Clock Time Server

Figure 3 - Schematic of equipment setup for PTP time source and PTP Feed Distribution

- The PTP Time Feed is provided using two resilient Spectracom VelaSync Grandmaster Time servers, with Rubidium oscillator.
- Two VelaSync Grandmaster time servers are utilised within the PTP architecture and are cross-connected to provide resiliency.
- The VelaSync devices are fed by dual power (on different PDUs) for resiliency.

Handoff / Presentation

Customers will be presented with two multimode fibre (LC termination) connections, each of which interfaces with its own Grandmaster for resiliency. The infrastructure will be 10G. The IP address range will be x/27 and communicated to Customers by the Exchange.

Key Benefits of the PTP Service

- Resilient and accurate time provision based on diverse GPS feeds.
- High-spec infrastructure to maintain time signal accuracy.
- The PTP time feed is derived from the same GPS signal and antenna as used by the Exchange for the Market Platform timestamping.
- No hardware infrastructure required from the Exchange, reducing need for cabinet space or power provision.

5.1.2. GPS Time Feed

For the GPS Time Service, Customers are provided with two resilient and diverse connections for the provision of L1 GPS signal.

To maintain accuracy and resiliency, the GPS Feed is serviced by two separate GPS antennae located in diverse positions on the Exchange Data Centre roof. Furthermore, there is resiliency built in across the solution to ensure an alternative source is available in case of issues with the primary. Each GPS antenna is connected to separate GPS splitter boxes in the Exchange hosting room. Customers are presented with two coaxial connections, each of which interfaces with Exchange GPS splitter box.

The following schematic diagram identifies equipment setup for distribution of the GPS signal:

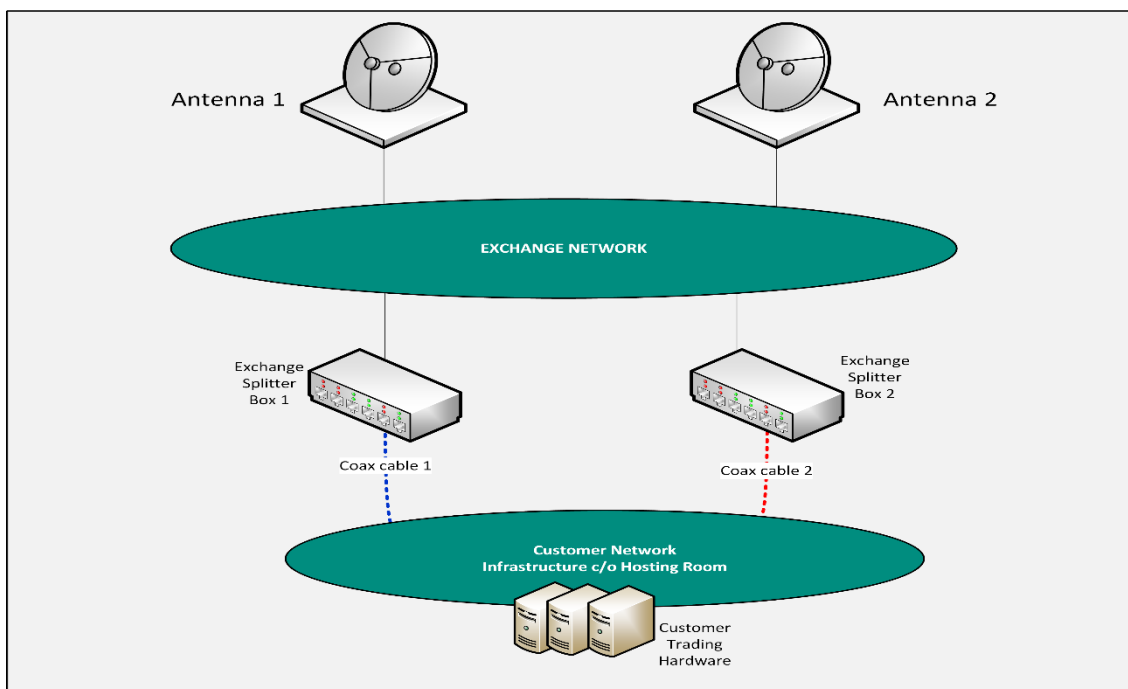


Figure 4 - Schematic of equipment setup for GPS time source and GPS Feed Distribution

5.2. Remote Hands Service

The Exchange can provide support on-site for a range of installation, planned and reactive activities as requested.

The remote hands service is available during the standard change windows, which are as follows:

- Monday – Friday 6:00 pm to 01:00 am the following morning

Outside of the standard change window an on-call emergency service is also available for the following limited support activities on request:

- Re-booting of Customer Equipment
- Visual “lights-on” inspection

Remote hands are able to perform most changes required, including:

- Racking of servers, switches and any other devices
- Patching within and between cabinets
- Installing power supplies
- Installing structured cabling
- Replacing PCI cards, RAM, server HDDs, hot swappable power supplies
- Basic configuration of iLO, DRAC or similar Out of Band management interfaces to allow remote access
- Installation and management of x-connect between Customer cabinet and Data Centre Telco Meet Me areas (Management connectivity services - south side).

Remote hands are NOT able to perform any configuration tasks beyond initial setup of OOB management or that require access to a device’s OS directly.

Requesting Remote Hands

A customer can request Remote Hands assistance sending an email at **hostingops-milan@borsaitaliana.it** . The request must originate from an authorized contact of customer organisation and must include the following information:

- Detailed schedule of works, including label names, “U” position and all relevant steps including diagrams and patching schedules as appropriate
- Any time constraints such as “do not start before”
- Customer contact for work commencement and completion
- The preferred date and time the action is to be undertaken

The Exchange will communicate with the requester to confirm when the task has been scheduled, completed and to ensure no further action is required. If a cabinet is found not to be adequately labelled or the instructions are not sufficiently clear then the engineer will not complete the task.

The Exchange will use its best endeavours to fulfil the Customer's instructions in relation to such Services, but the Exchange will not be responsible for the successful outcome of any remote hands activities or for any relevant unexpected consequence affecting in any way the customer, including the customer equipment and the customer's business.

Remote Hands Fees

Relevant charges payable to the Exchange for the provision of such Remote Hands Services are priced upon customer's request, and mutual agreed by the Parties in writing prior to the commencement of the provision of such Services by the Exchange.

6. EQUIPMENT INSTALLATION

6.1. 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. The Exchange insists on devices being installed correctly not to disrupt the hot and cold aisle layout.

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 and overhead 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.

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.

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

6.1.1.1. 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.

6.1.1.2. 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.)
- 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.

6.1.1.3. Server cable management guidelines

As identified previously, the Exchange will complete all under floor and over head cabling on behalf of customers. Customers are NOT permitted to access any under floor/cable tray 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

6.1.2. Power Configuration

All Exchange Hosting cabinets should be equipped with two power strips for a resilient supply. Each power strip is 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.

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.

6.1.2.1. Power Distribution Units

As standard, the customer provides its own Power Distribution Unit (PDU) for each requested rack. Single phase 32 Amps PDUs are to be used. IEC AC Power receptacles are used.

6.2. Demarcations points

6.2.1. Power Demarcation point

The Exchange is responsible for the connection between the IEC AC Power receptacle (the “power demarcation point”) and the Customer’s power bars.

6.2.2. Network Connections Demarcation Point

6.2.2.1. Demarcation Point - Trading and Information services

All network connectivity to the Exchange’s trading and information services is the responsibility of the Exchange.

6.2.2.2. 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 (fibre Singlemode with LC connector) is from the data centre provisioned patch panel in the Telco cabinet (and including the patch panel) (the “**Carrier Demarcation**”) to, 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.

6.3. Customer Enablement Process

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

- Borsa Italiana IDEM market Borsa Italiana MTA, TAH, MOT, EuroTLX, SEDEX and ETFplus markets
- Borsa Italiana MDF, DDM Plus and GTP market real-time data feed
- Borsa Italiana BCS Clearing service
- MTS

6.4. Testing Policy and Procedures

6.4.1. 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.

6.5. Installation Frequently Asked Questions (FAQs)

Q) Should the Customer provide patch cables or can this be done by 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, 600mm width.

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

A) As per standard PDUs should be provided by the customer and should be single phase 32 amps ones. It is strongly advised that PDUs are horizontal and rack mounted.

Q) What is the power limit per rack/cabinet?

A) The power may be up to 3 kW or 5 kW with respective pricing

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

A) IEC

Q) Who is the Customer's main contact for installation?

A) The main contact for the set-up is the Hosting Team:

Email: **hostingops-milan@borsaitaliana.it**

Telephone: +39 02 72 426 418 / +39 02 72 426 348

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

A) Same as above

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

A) Same as above

7. SERVICE OPERATION

7.1. System Monitoring of the Exchange Hosting Service

As detailed previously, the Exchange monitors each port on the access switches; however, as the Exchange cannot determine if the device interfacing with the Exchange has been purposely disconnected, the Exchange will only investigate an issue when we have identified that all ports on a specific switch is down or if the switch itself has failed. Customers should therefore escalate single port issues that may arise to the Exchange as a matter of urgency (see section 8).

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.

7.2. Reporting a Fault with the Exchange Hosting Service

Customers who have an issue with Exchange Hosting Service should contact the Hosting team on **hostingops-milan@borsaitaliana.it** or +39 02 72 426 418 / +39 02 72 426 348.

7.3. Change Management Process

Where customers will proceed with changes to their installation that require an alternation to the way they interface with the Exchange, the customer must provide notice and obtain Exchange approval ahead of the activity.

Customers should contact the Hosting team via **hostingops-milan@borsaitaliana.it** or +39 02 72 426 418 / +39 02 72 426 348.

7.4. 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.

7.5. 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. Please see the Service Agreement document for further details.

7.5.1. 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.

7.5.1.1. 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 sub-licensing.

7.5.1.2. 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 synchronised messages, etc), unless permitted under the Hosting Services Master Terms and Schedules (as relevant) or as otherwise agreed in writing by the Exchange.

8. 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 contact the Hosting team on **hostingops-milan@borsaitaliana.it** or +39 02 72 426 418 / +39 02 72 426 348.

9. DATA CENTRE TECHNICAL SPECIFICATION

9.1. General Datacentre Characteristics

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.

9.1.1. 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 houses the 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.

BT 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.

9.1.2. 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.

BT'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.

9.1.3. 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 is 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.

BT'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.

9.1.4. 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.

9.1.4.1. 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.

9.1.4.2. 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.

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.

9.1.5. 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.

9.1.6. Passive security

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

9.1.7. 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

9.1.8. 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

10. CONTACTS

To order Exchange Hosting services or to discuss your connectivity relationship in greater detail please contact:

Milan Hosting Team

T: +39 02 72 426 418

T: +39 02 72 426 348

E: hostingops-milan@borsaitaliana.it

If you require technical support due to an incident or failure please contact:

Client Support

T (toll free): 0080026772000

T (from mobile): +39 02 45411399

E: Client-Support@borsaitaliana.it

To enable Borsa Italiana Test and Production Services via Exchange Hosting SAP please contact:

Customer Relationship Management

T: +39 02 72426 512

E: clients-services@borsaitaliana.it

CONTACT

Milan Hosting Team

hostingops-milan@borsaitaliana.it

+39 02 72 426 418

+39 02 72 426 348

<http://www.borsaitaliana.it/borsaitaliana/gestione-mercati/connettivita/connettivita.en.htm>

Disclaimer

This publication is for information purposes only and is not a recommendation to engage in investment activities. This publication is provided "as is" without representation or warranty of any kind. Whilst all reasonable care has been taken to ensure the accuracy of the content, Euronext does not guarantee its accuracy or completeness. Euronext will not be held liable for any loss or damages of any nature ensuing from using, trusting or acting on information provided. No information set out or referred to in this publication shall form the basis of any contract. The creation of rights and obligations in respect of financial products that are traded on the exchanges operated by Euronext's subsidiaries shall depend solely on the applicable rules of the market operator. All proprietary rights and interest in or connected with this publication shall vest in Euronext. No part of it may be redistributed or reproduced in any form without the prior written permission of Euronext. Euronext disclaims any duty to update this information. Euronext refers to Euronext N.V. and its affiliates. Information regarding trademarks and intellectual property rights of Euronext is located at www.euronext.com/terms-use.

© 2020, Euronext N.V. - All rights reserved



borsaitaliana.it