Customer Managed Connectivity - Milan

Service and Technical Description

October 2017

Version 3

London Stock Exchange Group

Table of Contents

1.0 Document Scope

The purpose of this document is to provide customers with a detailed definition of the Borsa Italiana Customer Managed Connectivity (CMC) service. This document is published by Borsa Italiana (the "Exchange"). Other relevant documentation relating to the Exchange is also available from our website.

1.1 **Structure of this document**

This document contains the following sections:

1. **Document Scope** – identifies the purpose and scope of this document
2. **Introduction** – details the key features of Customer Managed Connectivity
3. **Accredited Connectivity Partners** – provides a description of accredited physical access suppliers
4. **Customer Access Ports** – details the Exchange's Customer Access Ports
5. **Technical** – provides the technical details around the Customer Managed Connectivity service including physical connectivity, IP addressing, security and testing
6. **Millennium Exchange Services –** details key information around Millennium Exchange information delivery
7. **Testing Policy and Procedures** – provides detail around the Exchange's Customer Development Service
8. **Confidentiality and Security**
9. **Contacts** – provides the Exchange's contacts for support and services
10. **Frequently Asked Questions (FAQ)**

Unless otherwise defined in this Customer Managed Connectivity Service and Technical Description, words which are capitalised shall have the meaning given to them in the Customer Managed Connectivity Services Terms and Conditions.

1.2 **Version History**

The Customer Managed Connectivity Service and Technical Description document has had the following iterations:

Issue	Date	Description
1.0	December 2015	First issue of the Customer Managed Connectivity Service and Technical Description
2.0	June 2017	Second issue of the Customer Managed Connectivity Service and Technical
3.0	October 2017	Third issue of the Customer Managed Connectivity Service and Technical

Readers of this document are reminded to check the Borsa Italiana website for updates www.borsaitaliana.it

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 here from.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 the stated notice period in accordance with the Terms and Conditions of the relevant service or product.

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

2.0 Introduction

Customer Managed Connectivity (CMC) provides an optimised network infrastructure, offering resiliency and scalability, to allow Customers to access to Borsa Italiana markets and services as well as trading venues and services based in LSEG's London Data Centers with additional choice, flexibility and exceptional control. Our Accredited Connectivity Partner programme offers customers a choice of circuit suppliers from partners committed to supporting mission critical market data and trading access.

The Exchange provides customers with either:

- a choice of scalable physical access ports to terminate their chosen Accredited Connectivity Partner circuits on, underpinned by a resilient and scalable network infrastructure.

- Internet Access through VPN LAN to LAN between Client's site and Exchange's site

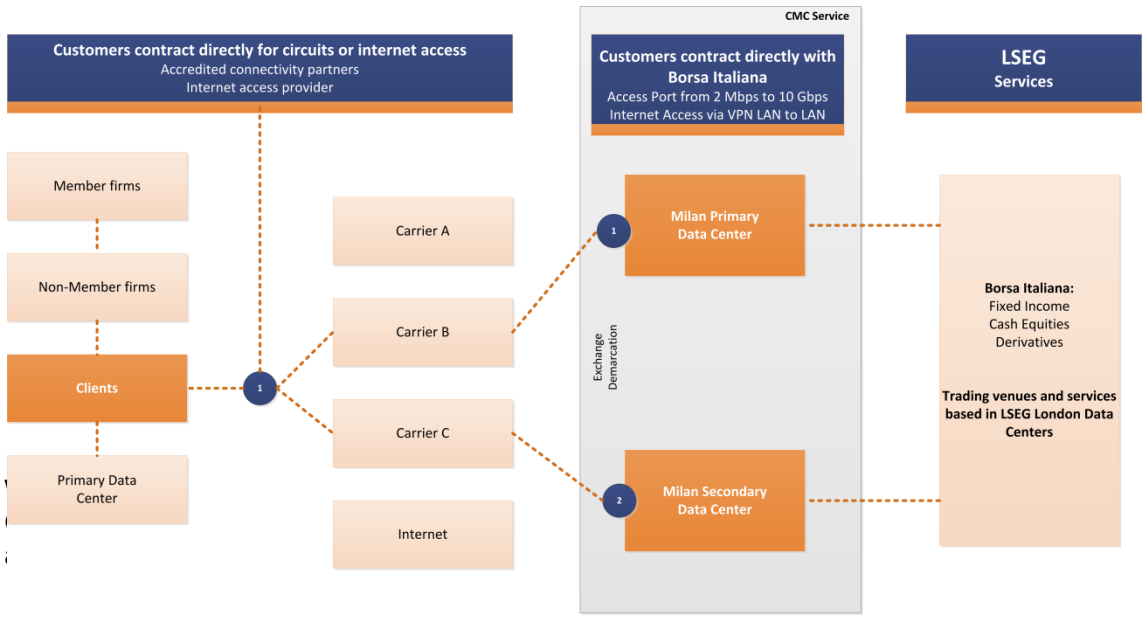

Figure 1 - High Level Overview Customer Managed Connectivity

3.0 Accredited Connectivity Partners

The Exchange's Accredited Connectivity Partner programme has been established to provide customers greater choice and flexibility when connecting directly to Borsa Italiana.

A number of industry leading telecommunication providers have committed to working with the Exchange to provide direct and dedicated connectivity to Group services.

For an up to date list of our Accredited Connectivity Partners please contact Borsa Italiana website as per the details in section 8.0 of this document.

3.1 **Ordering Physical Access Circuits**

Customers contract directly with an Accredited Connectivity Partner for physical access circuits between the customer premises and the Exchange sites.

The Exchange treats the security of its data, customers and market access, with the utmost importance.

Prior to entering into any contractual arrangements for circuit provision from the Accredited Connectivity Partners, customers should contact their Business Development Technology to make sure requirements are fully understood and can be met.

Customers should ensure any circuits provided by our Accredited Connectivity Partners can support the transportation of standard Ethernet frames.

Benefits for Customers:

- A selection of physical circuit providers providing additional choice for direct and dedicated connectivity
- Working with organisations which are committed to supporting financial markets
- Ability to leverage existing relationships or build new ones
- Potential for cost savings through direct negotiations

4.0 Customer Access Ports

The Exchange's Customer Access Ports provide the physical gateway to markets and services available across Borsa Italiana's suite of products and trading venues and services based in LSEG London Data Centers.

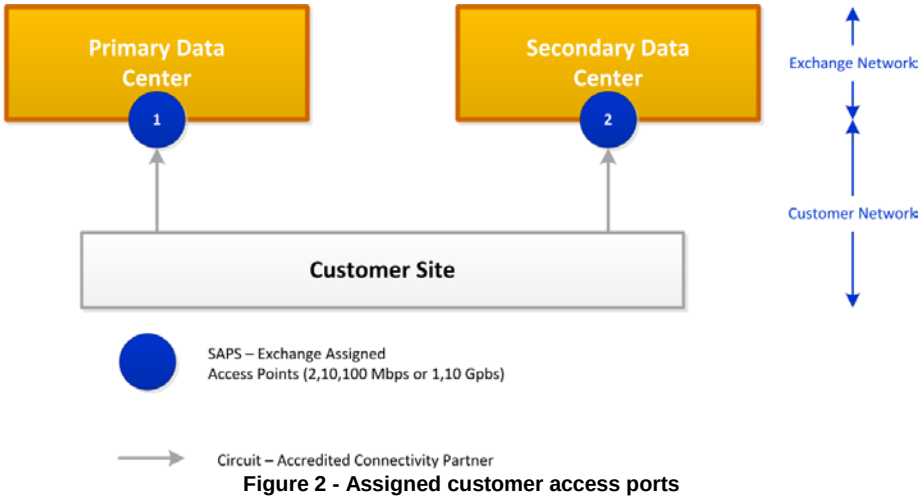

Figure 2 - Assigned customer access ports

Benefits to customers:

- Choice of access speeds from 2Mb to 10Gb
- Resilient or singular set up, providing access to Production and DR facilities
- Direct Connectivity platform to the Exchange
- Support for all existing and future Borsa Italiana (and LSEG) services
- Provides a secure environment supporting mission critical and sensitive transactions

5.0 VPN LAN to LAN

Trough the VPN LAN to LAN access mode, the Client's site is connected to Primary Exchange's site to access to markets and services available across Borsa Italiana's suite of products and trading venues and services based in LSEG London Data Centers.

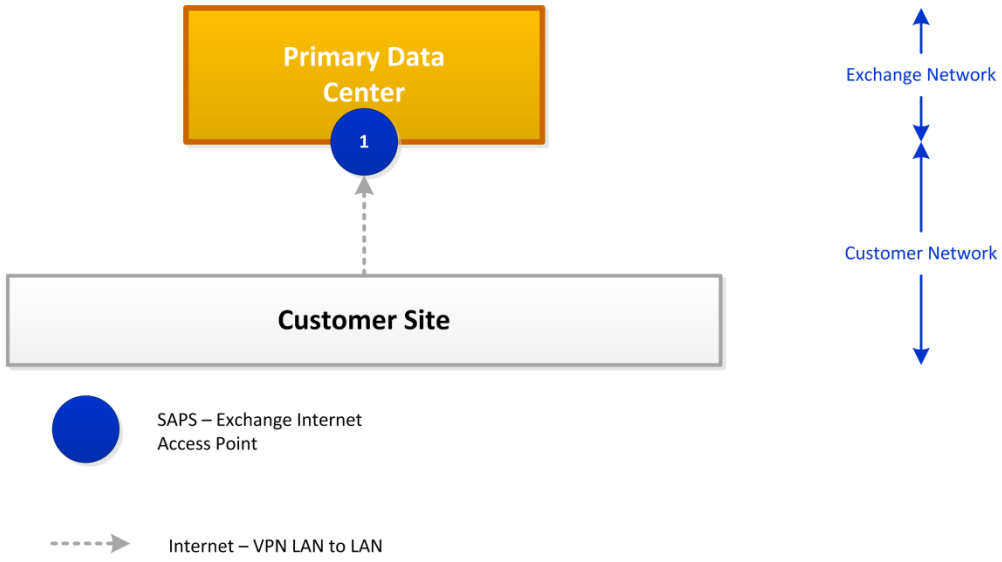

Figure 3 - Internet Access Point

Customer Managed Connectivity VPN (CMC VPN) utilises a customer's existing connection to the internet to provide connectivity to London Stock Exchange Group (LSEG) through a secure Virtual Private Network (VPN).

6.0 Technical

This document describes the interface provided by the Exchange to customers who wish to access the Group's markets and services, using the Customer Managed Connectivity service:CMC – Access Ports

- Network physical interface
- Security aspects of the network
- Network connectivity such as addressing and routing details

- Network failover
- IP addresses

CMC – Internet Access (VPN LAN to LAN)

- Configuration Parameters

Customers should make sure they understand and complete any additional obligations required of particular Exchange Services before ordering connectivity.

6.1 CMC – Access Ports

a) Physical Connection

In order to access the Exchange Services, a physical connection must be made between the customer and the Exchange Equipment. Note, this connection must be delivered to the Exchange Data Centres from an ACP Point of Presence which is geographically located outside the PDC or SDC respectively.

Customer access to the network is made via a Service Access Point (SAP). Customers are responsible for providing their own switching/routing equipment at their site. For physical access circuits between the customer site and the Exchange sites, customers are responsible for direct contract negotiations with the Exchange's list of Accredited Connectivity Partners. Where advised on the Customer Managed Connectivity Service Order Form, the Exchange will provide the cross connects between the customer circuits at the Exchange Sites to the Customer Access Ports provided on the Exchange Equipment.

The SAP provides both the physical and logical interface to the IP Network.

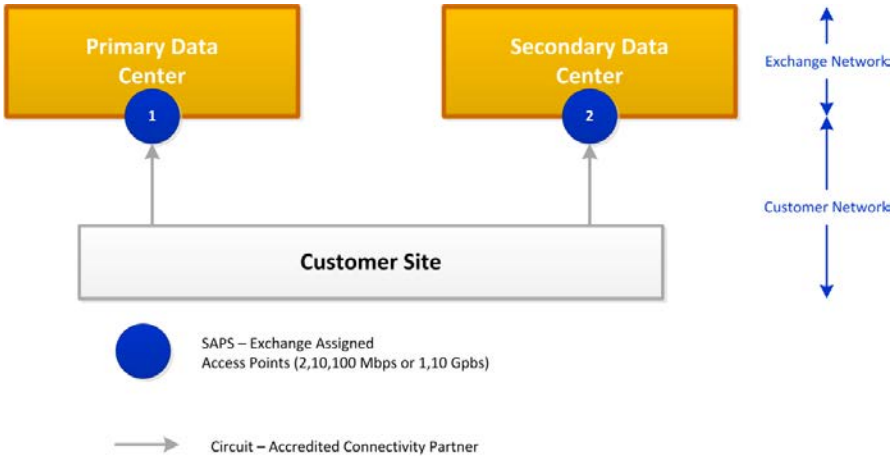

Figure 4 - Service access point

b) SAP Requirements

At the Customer Site

Customers should ensure adequate facilities exist for the installation of the equipment supporting their SAP and the associated communications equipment e.g. the Accredited Connectivity Partner circuits. It is suggested Customers should be vigilant and make sure power supplies of the correct rating, adequate ventilation and appropriate environmental conditions are in a place for their connectivity.

At the Exchange Site

Customers must communicate to the Exchange as soon as practical, the circuit termination details provided by the Accredited Connectivity Partner.

Exchange Site locations may vary from time to time, and the Exchange will confirm on the relevant Service Order Form, the responsibilities for the cross connect between the customer circuit and the Exchange assigned Customer Access Port.

On the Service Order form – the Exchange will stipulate the required physical handoff at the relevant Exchange Site.

Security Controls

It is the responsibility of the customer to implement security controls between the equipment at the Customer site and the Exchange Equipment.

The Exchange will implement the following security controls to minimise the risk of unauthorised access to the network:

- Incoming and outgoing filters ensure a customer SAP can exchange only pre-defined and agreed upon routing information.
- Each Customer Access Port will maintain an access list of allowable IP addresses and only packets from addresses in that list will be permitted through the Customer Access Port.
- Customers can use the 'ping' command to test the connectivity between their own systems and the Exchange Network (the Exchange switch interface only).

Firewalls

It is expected that customers will use firewalls to implement security controls between the Exchange Network and their own networks. Any firewall installed between the customer and the Exchange Network must be able to allow IP multicast packets to pass through.

c) Network Connectivity

The Exchange uses TCP/IP (Transmission Control Protocol/Internet Protocol) for network connectivity. The Exchange currently only supports IPv4.

A full explanation of IP is beyond the scope of this document. Customers are advised to refer to the Internet Engineering Task Force website for more detailed technical information about the Internet Protocol: http://www.ietf.org

Logical Interfaces

The Exchange will provide a L3 router port over each Customer Access Port. The Exchange uses L3 point-to-point logical connections.

Customers should configure the relevant local L3 interfaces on theirs devices for valid connectivity.

d) Network Addressing

Exchange IP Addressing

The Exchange will assign IP addressing for the network link between customer equipment and exchange equipment.

Dynamic (*recommended*)

For the network link between the customer equipment and assigned Customer Access Port, the exchange will provide a /30 RFC1918 address range. The highest usable IP address within the range will always be reserved for the Exchange Customer Access Port of the point to point network link.

Static

VRRP

For the network link between the customer equipment and assigned Exchange Customer Access Port(s), the exchange will provide a /29 RFC1918 address range. The 3 highest usable IP addresses within the range will always be reserved for exchange equipment, with the remainder available to customers. The addresses will be assigned roles as follows:

Example 192.168.1.0/29

Available IP Address	Role
192.168.1.1	*Customer switch 1*
192.168.1.2	*Customer switch 2*
192.168.1.3	*Customer HSRP/VRRP*
192.168.1.4	Exchange switch 1
192.168.1.5	Exchange switch 2
192.168.1.6	**Exchange VRRP**

In this case the Customer has to configure L2 access ports on theirs devices, providing L2 connectivity between them in order to guarantee VRRP protocol connectivity.

Static ONLY (No Resilience connectivity)

For the network link between the customer equipment and assigned Customer Access Port, the exchange will provide a /30 RFC1918 address range. The highest usable IP address within the range will always be reserved for the Customer Access Port of the point to point L3 network link.

All IP addressing relating to Exchange markets and services will be made available to customers as part of the onboarding process.

Customer IP Addressing

Customer source IP addressing, can be represented by a customer's own registered addressing, or alternatively make use of private addressing (RFC1918) assigned by the Exchange. The Exchange will serve as the central administrator of all private address ranges.

If a customer is using their own registered IP addressing, the following rules apply:

- The customer provided IP address subnets have to be a public range and registered to their company e.g. on RIPE or associated internet registry database.
- The registered subnet for production has to be a minimum of a /27
- The registered subnet for Customer Testing has to be a minimum of a /28

Please note that the production registered IP addressing can only be configured for production services, and likewise the testing registered IP addressing can only be configured for testing services.

The subnets should support growth within the customer network to avoid running out of host addresses.

The subnet is dedicated to a single customer SAP and cannot be used elsewhere on the Borsa Italiana network or via another customer SAP.

Routing

Customer routing on the Customer Network is the responsibility of the customer - the following section describes how customer routing should be implemented.

Dynamic

BGPv4 is the routing protocol to be used between the Exchange and Customer equipment, for the dynamic propagation of routing information, and is available on all Customer Access Ports (2, 10, 100Mbps or 1, 10 Gbps).

Customers may elect to use a registered AS number in conjunction with their own registered address ranges. Alternatively, as previously described, where a customer is assigned private addressing, the Exchange will also assign a private AS number.

The /30 address range assigned to the L3 point-to-point connection determine the BGP peers on the subnet.

The highest usable IP address in the subnet will always be the Exchange BGP peer, whilst customers should assign the next usable IP address to its BGP peer.

VRRP (Virtual Router Redundancy Protocol)
A /29 subnet will be assigned by the Exchange, with the highest three IP addresses representing Exchange equipment and lowest three IP addresses representing the customer equipment.

VRRP relies on the successful communication of VRRP messages over a common layer 2 network between the Exchange Customer Access Ports. Customers are responsible for providing this network, and must not filter VRRP messages.

Customers are required to point their static routes at the Exchange VRRP address.

Network Failover

For rapid failover detection, the Exchange supports BFD* (Bi-directional Forwarding Detection) between the Customer Access Port within the Exchange site, and the customer equipment.

The Exchange Network has been designed to be resilient through the use of its optimised network infrastructure.

The Exchange is able to provide Customer Access Ports at both the Exchange primary site and its backup datacentre locations.

If the primary Customer Access Port fails then network connectivity with the Exchange will automatically be maintained via the secondary Customer Access Port. Any physical investigation work related to a Customer Access Port will be performed outside of market hours.

Should customers use static routing options, the Exchange does not guarantee successful failover in all conditions.

*is not supported on VRRP deployments.

Confirming Connectivity

To enable customers to confirm connectivity between their own systems and the Exchange Network, the Exchange supports ICMP ‘ping’ messages to the Exchange Interface IP address.

Network Address Translation

Where customers use a different private addressing scheme or there is conflict between the IP addresses allocated by the Exchange and the customer’s network, then Network Address Translation (NAT) must be performed. Any NAT device should employ static address translation. Responsibility for NAT is with the customer.

IP Multicast
The Exchange supports the use of IP Multicast for the dissemination of market information. Data flow from the Exchange to customers will be unidirectional and statically forwarded - customers will not be able to send data to the Exchange using multicast. No dynamic multicast routing is supported.

6.2 **CMC – Internet Access (VPN LAN to LAN)**

a) Configuration Parameters

Lan-to-Lan connection allows a private and secure connection to be established between two end-points (generally firewalls or concentrators) through the public network. One end-point is situated in Primary Exchange data centre and the other at the customer site.

The VPN LAN to LAN configuration is performed with authentication and encryption protocols between the Exchange network and the customer's. Compatible protocols are defined by Exchange.

The network component that has to be installed at the customer site is not provided by Exchange, but is the client's responsibility to provide. It must be able to:

- support IPSec tunnel LAN to LAN in pre-shared secret modality (no certificates are used)
- Perform NAT of customer networks on the addresses (for Production and or CDS environments) provided by Exchange. These addresses will be used on the IPsec tunnel
- Support the following protocols:

VPN Peer and NAT Source	VPN Peer IP	91.235.120.50
	NAT Source for all VPN connections to Production environment	Assigned by Exchange
	NAT Source for all VPN connections to CDS environment	
IKE Phase 1	Authentication	Pre-shared Key
IKE Phase 1 Proposal	Group	2
	ESP-e	3DES
	ESP-a	SHA-1
IKE Phase 2	Group	2
	Protocol	ESP

Proposal	Enc_alg	3DES
	Auth_alg	SHA-1
NAT Traversal		Disabled
IKE Negotation mode		Main

7.0 Testing Policy and Procedures

7.1 **Customer Development Service (CDS) Enablement's**

The Customer Development Service (CDS) can be accessed via the Customer Managed Connectivity service.

The CDS provides a fully functioning live simulation of the Live Service against which our customers can develop, test, and run their Trading and Information applications. The CDS also provides model based testing scenarios to help customers with their development efforts.

To access the CDS via the Customer Managed Connectivity service, customer will be required to amend their CDS Configuration Form (CF) with the new SAP and IP information. Amendments can be requested through BItClub or directly with your dedicated Business Development Technology relationship manager .

7.2 **Production Enablements**

To access production trading and information applications via the Customer Managed Connectivity service, customers will be required to amend their Production Configuration Form (CF), advising the new SAP and IP range required for the specific enablements. Amendments to the CF should be requested through BItClub or directly with your dedicated Business Development Technology relationship manager .

7.3 **Live Connectivity (LCON) Test**

Customers are required to successfully complete a Live Connectivity Test (LCON) for at least one enablement per Software Instance per new SAP, prior to accessing the live environment.

It is the responsibility of the customer to confirm that all enablements that they have elected not to LCON are successfully connected. Further information can be requested from your dedicated TAM.

8.0 Confidentiality and Security

The Exchange treats the location of our Data Centre as highly confidential and so must not be included in any public documentation or disseminated.

The Exchange itself uses third parties to comprehensively vet all employees. In particular, checks for criminal records, background, qualifications and range of other criteria are undertaken.

The Exchange has an appointed Information Security Manager who is responsible for controlling and co-ordinating information and security measures and controls at the Exchange. The Exchange maintains a comprehensive information security library incorporating a range of policies, standards and procedures used for the control and management of IT Security.

The Exchange has an annual penetration test plan for evaluating a range of infrastructure components. This supplements comprehensive compliance and security monitoring tools and procedures.

The Exchange has robust security arrangements in place, which are audited by an external agency on a regular basis with agreed recommendations implemented.

9.0 Contacts

To order CMC services or to discuss your connectivity relationship in greater detail please contact Business Development Technology on the following:

Telephone: +39 0272 426 909 / +39 0 272 426 418
Email: connectivity@borsaitaliana.it

If you require technical support due to an incident or failure please contact the Service Desk at:

Telephone: +390245411399

Email: service-desk@borsaitaliana.it

10.0 Frequently Asked Questions (FAQ)

How do I order Customer Managed Connectivity (CMC)?

Customers can request order forms by emailing Business Development Technology *connectivity@borsaitaliana.it* or calling +39 0272426909 / +39 0272426418

Can I upgrade my BItNet connectivity to CMC?

BItNet is on a completely separate network infrastructure to CMC, and as such there is no upgrade path to CMC. If a customer wishes to replace their current BItNet connectivity with CMC, they should contact Business Development Technology.

Where can I find a list of Accredited Connectivity Partners?

For an up to date list of Accredited Connectivity Partners please check the Group website.

Additionally, if you have a specific carrier preference and they are not listed please speak with Business Development Technology.

Which are the available bandwidth sizes?

The available bandwidth sizes are 2, 10, 100 Mbps or 1, 10 Gbps.

Are there additional cross connect charges between customer circuits and Customer Access Ports at the Borsa Italiana primary and backup datacentres?

There are no charges for cross connects between the Accredited Connectivity Partner circuits and the Customer Access Ports.

Does CMC support all current services I am taking on BItNet?

Yes, CMC supports all current services for BItNet, and is built for supporting the long term evolution of the Group.