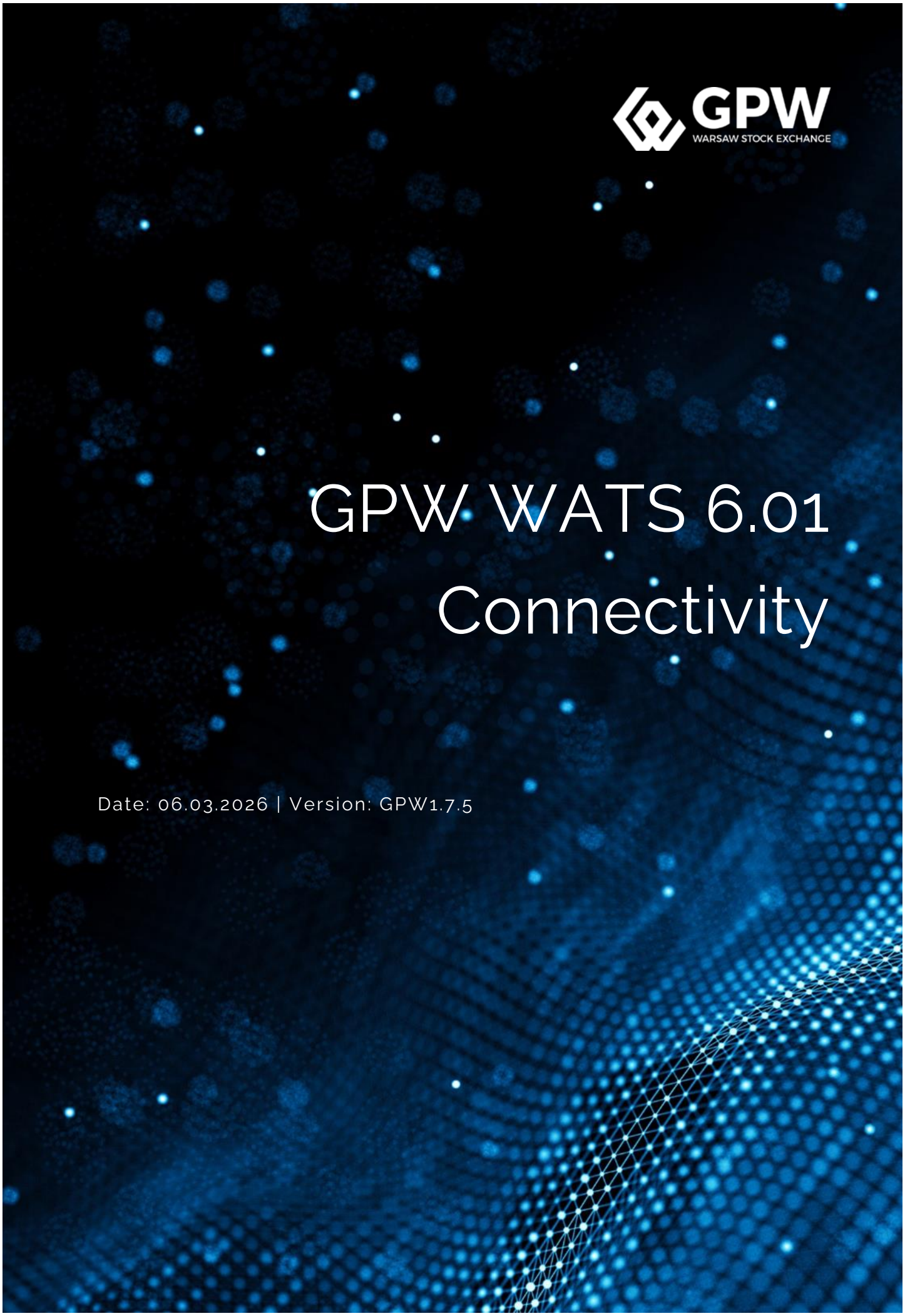


GPW WATS 6.01 Connectivity

Date: 06.03.2026 | Version: GPW1.7.5

CONTENTS

1. DISCLAIMER

This document is for information purposes only and does not form any part of contractual documentation.

Reasonable care has been taken to ensure details contained within are accurate and not misleading at the time of publication. Warsaw Stock Exchange is not responsible for any errors or omissions contained in this document.

Warsaw Stock Exchange reserves the right to treat information contained in this document subject to later change without prior notice.

This document contains confidential information to Warsaw Stock Exchange and may not be reproduced, disclosed, or used in whole or part, in any manner, without prior written consent from the owner of this document. Information included in this document shall be maintained and exercised with adequate security measures necessary to protect confidential information from unauthorized access or disclosure.

In case of sections of documentation at a High level work progress according to the current version of *GPW WATS Advancement of Documentation*, Warsaw Stock Exchange will endeavor to limit changes to these sections of documents to those related to:

1. correcting errors in the documentation or in the software;
2. clarification of the documentation content or removing ambiguity;
3. implementation of approved change requests or;
4. regulatory changes.

2. PREFACE

Warsaw Stock Exchange has prepared this document to help in the implementation process of GPW WATS trading platform.

This section describes the basic information about Connectivity. You can learn about the target audience, the document purpose and all the necessary documents you should read in relation to this specification.

2.1. TARGET AUDIENCE

This document has been prepared for development staff, Independent Software Vendors who produce software integrated with GPW WATS, analysts, market participants and all clients who want to deepen their knowledge about GPW WATS.

2.2. DOCUMENT PURPOSE

This document presents information on available options, requirements, and procedures for network connectivity with GPW WATS via all types of connections available and supported by Warsaw Stock Exchange (GPW).

2.3. ASSOCIATED DOCUMENTS

GPW WATS 6.01 Connectivity is a part of GPW WATS documentation set.

Please check the following documents to learn about the construction of Trading System.

- GPW WATS 1.01 Trading System.

Please check the documentation of the trading protocols supported by GPW WATS.

- GPW WATS 2.01 Native Order Gateway Specification,
- GPW WATS 2.02 FIX Order Gateway Specification.

Please check the description of the communication with Data Distribution Service.

- GPW WATS 3.01 Market Data Protocol.

Please check the description of the communication with Internet Data Distribution System.

- GPW WATS 3.02 Internet Data Distribution System,
- GPW WATS 3.03 Streaming Messages for IDDS,
- GPW WATS 3.04 Rest API Messages for IDDS.

Please check the additional documentation, which explains other services provided within GPW WATS.

- GPW WATS 4.01 Drop Copy Gateway,
- GPW WATS 4.02 Post Trade Gateway,
- GPW WATS 5.01 Risk Management Gateway.

Please check the additional documentation describing the following:

- GPW WATS 2.03 Rejection Codes,
- GPW WATS 2.04 BenDec Message Definition Format,
- GPW WATS 4.03 Contract Notes,
- **GPW WATS 6.01 Connectivity** (this document),
- GPW WATS 6.02 (ENG) Short Code Record Keeping,
- GPW WATS 6.02 (PL) Mapowanie Short Code,
- GPW WATS 6.03 Short-Long Mapper User Guide.

It is recommended to read ***GPW WATS 1.01 Trading System*** document first.

3. Document History

Version	Date	Description
0.51	29.06.2023	The initial publication of the documentation.
0.52	26.07.2023	Publication of v0.52.
0.53	16.08.2023	Publication of v0.53.
0.54	20.09.2023	Publication of v0.54.
0.55	5.10.2023	Two chapters added: • 6.2.1.2 IPVPN L3 • 6.2.1.5 HFT Access.
0.56	08.11.2023	Publication of v0.56.
0.57	01.12.2023	Appendix A has been updated.
0.58	15.12.2023	Publication of v0.58.
0.59	09.01.2024	Publication of v0.59.
0.59.1	14.02.2024	Appendix B has been updated.
0.62	29.03.2024	IP addresses for the Equinix WA3 have changed.
1.0	30.04.2024	Publication of v1.0. No changes in the document.
1.1	28.06.2024	Connectivity details and IP Addresses WA2 and WA3 modification.
1.1.2	9.08.2024	Publication of v1.1.2. No changes in the document.
1.2	18.09.2024	Publication of v1.2. No changes in the document.
1.3	15.10.2024	The final version of the environmental IP address
1.3.1	31.10.2024	Addresses for iDDS and WATSON and encryption for DDS
1.3.2	8.11.2024	GPW WATS unicast source (eUAT) for WA3 has been changed from: 91.234.144.240/28 to 91.234.144.224/28. Port addresses for DDS::BBO::Replay NonGPW have been changed form 11157 to 12157 for both WA3 and WA2.
1.4	6.12.2024	Unpublished version. No changes in the document.
1.5	3.02.2025	5.1.1 - OEG PTG FIX service deleted IDDS service section added (8.3.2.2, 8.4.2.2, 8.5.2.2) Appendix B - TNSI operator added
1.5.4	30.04.2025	**5.1.1 Euat and pre-prod service organization section** - table has been assessed (a full list of changes is available in a comparison (change log) document). **6.3.1.5. Bandwidth** specification amended (a full list of changes is available in a comparison (change log) document) **8.5.2.1. Multicast Groups** - Table added
1.6	26.05.2025	8.3.2.1 Multicast Group - IDs numbers changed. StreamID column added. (**prePROD**) 8.4.2.1 Multicast Group - ID numbers changed. StreamID column added. (**PROD-Bis**) 8.3.2.1 Multicast Group - ID numbers changed. StreamID column added. (**eUAT**)
1.6.5	18.06.2025	**8.5.2 Market Data** Full Market Data DDS::OMD::Snapshot GPW Only - IP address changed. DDS::OMD::Replay GPW Only - IP address changed.
1.6.6	10.07.2025	Publication of v1.6.6. No changes in the document.
1.6.7	30.07.2025	Addresses for iDDS and mTLS connection have been updated6.2.1.3 Technical Details of the Solution – dscp marking scheme has been deleted. 6.3.1.5 Bandwidth – dscp marking information has been deleted Information about Stream1 and Stream2 has been deleted. Site A has been changed to WA3 name. Site B has been changed to WA2 name.
1.6.8	19.08.2025	Market Data addressing changed for PRE-PROD and PROD-BIS

Version	Date	Description
		FQDN for WATSON changed DDS Services names verification. PROD-BIS env. IP addresses verification
1.6.15	29.09.2025	IDDS , GUI RMA, deployment status updated
1.6.16	24.10.2025	Publication of v1.6.16. No changes in the document.

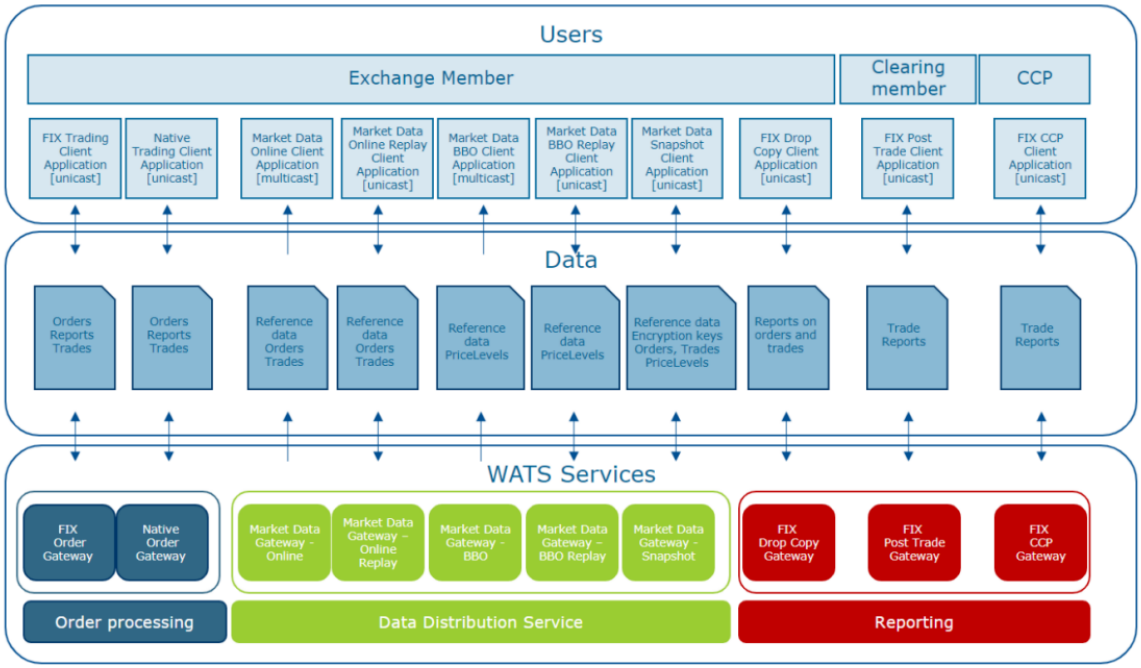
1.7.1	18.11.2025	Appendix A
		• 8.2 IP Addresses Detail WA 3 and WA2 – the section has been updated
		• 8.3 PROD (pre-PROD)
		  ○ 8.3.2 Market Data – the sections has been updated
		• 8.4 PROD-Bis
		  ○ 8.4.2.3 Watson System – the section has been updated
		  ○ 8.4.2.4 GUI RAM – the section has been updated
		• 8.5 eUAT
		  ○ 8.5.2.4 GUI RAM – the section has been updated

1.7.1.1	12.12.2025	**6.2.1.2.2 Customer connectivity architecture** – new section has been added **8.3 Authentication using Microsoft Entra External ID** – a new chapter has been added The following sections have been updated: • 8.4.2.4 GUI RMA • 8.5.2.3 Watson System • 8.5.2.4 GUI RMA • 8.6.2.3 Watson System • 8.6.2.4 GUI RMA
1.7.2	20.02.2026	Mcast group IP addressing correlation with specific TCP services (replay and snapshot) Bandwith recommendations section updated with the test results.
1.7.5	06.03.2026	Market Data decryption for tch Multicast Channel

4. GPW WATS Services (Interfaces)

4.1. GPW WATS Services (Interfaces) – General Overview

Figure 1. GPW WATS Services



4.2. GPW WATS Services (Interfaces) – Description

Services	Description
OEG::BIN (TCP)	Order Entry Gateway::BIN
OEG::FIX (TCP)	Order Entry Gateway::FIX
OEG::DCP FIX (TCP)	Order Entry Gateway::Drop copy service (FIX only)
DDS::OMD::Stream (UDP)	Distribution Data Service - On-line Market Data
DDS::OMD::Replay (TCP)	Distribution Data Service - On-line Market Data::Replay
DDS::OMD::Snapshot (TCP)	Distribution Data Service - On-line Market Data::Snapshot
DDS::OMD::BBO::Stream (UDP)	Distribution Data Service - Best Bid Offer
DDS::OMD::BBO::Replay (TCP)	Distribution Data Service - Best Bid Offer::Replay
DDS::OMD::BBO::Snapshot (TCP)	Distribution Data Service - Best Bid Offer::Snapshot

Detailed service specification and functionalities (see: Associated Documents).

4.3. Order Entry Gateway (OEG) - Architectural Context

Order Entry Gateway (OEG) - both types (BIN and FIX) and OEG Drop Copy will be up and running and accessible in both GPW sites (WA3 and WA2).

Confidential data will be transmitted over a unicast connection (TCP).

Order Entry Gateways located in WA3 in normal operation mode guarantee minimal internal GPW WATS latency between OEG and GPW WATS Core Matching Engine, but total client latency is determined by network (WAN) delays and the routing path "client-to-client".

4.3.1. ORDER ENTRY GATEWAY (OEG::DCP FIX)

Drop Copy Gateway is a standard functionality which allows receiving private messages for the client.

4.4. DATA DISTRIBUTION SYSTEM (DDS) - ARCHITECTURAL CONTEXT

DDS::OMD::Stream and its sub-services (Replay and Snapshot) are dedicated to market data transmission.

Market data will be transmitted over a multicast (UDP) simultaneously inside two parallel feeds, both with the same data content (in redundant mode, in different multicast groups: Stream A from WA3 only and Stream B from WA2 only).

When there is a technical incident or GPW decision, client applications and connectivity configuration should be ready to receive and operate based on single market data feed (Stream A or Stream B) only.

5. GPW WATS INSTANCES

5.1. TRADING SYSTEM INSTANCES: EUAT, PROD AND PROD-BIS

Instance	Description
EUAT	External User Acceptance Test instance Fully functional GPW WATS instance located in two GPW Sites (WA3 and WA2).
PRE-PROD -> PROD	(planned) PRE-PROD is PROD instance of GPW WATS system before "go-live" located in two GPW Sites (WA3 and WA2).
PROD-BIS	(planned) Additional GPW WATS instance installed on minimum set of hardware. Single site instance functionally representative of PRE-PROD (PROD) for client software functional tests and diagnostics

5.1.1. EUAT AND PRE-PROD SERVICE ORGANISATION

GPW WATS EUAT instances consist of:

- 2 OEG::BIN per Site,
- 2 OEG::FIX per Site,
- 1 OEG::DCP per Site,
- 1 DDS service with four physical Data Feed per Site (see table below):

Services	SITE	Description	Market/Source
OEG::BIN1 (TCP)	WA3	Order Entry Gateway:: BIN (nb 1)	All
OEG::BIN2 (TCP)	WA3	Order Entry Gateway:: BIN (nb 2)	All
OEG::FIX1 (TCP)	WA3	Order Entry Gateway:: FIX (nb 1)	All
OEG::FIX2 (TCP)	WA3	Order Entry Gateway:: FIX (nb 2)	All
OEG::DCP::FIX (TCP)	WA3	Order Entry Gateway:: Drop copy service (FIX only)	All
DDS::OMD::StreamA - All (UDP)	WA3	Distribution Data - On-line Market Data	All
DDS::OMD::ReplayA - All(TCP)	WA3	Distribution Data - On-line Market Data:: Replay	All
DDS::OMD::SnapshotA - All (TCP)	WA3	Distribution Data - On-line Market Data:: Snapshot	All
DDS::OMD::BBO::StreamA - All (UDP)	WA3	Distribution Data - Best Bid Offer	All
DDS::OMD::BBO::ReplayA - All (TCP)	WA3	Distribution Data - Best Bid Offer:: Replay	All
DDS::OMD::BBO::SnapshotA - All (TCP)	WA3	Distribution Data - Best Bid Offer:: Snapshot	All
DDS::OMD::StreamA - GPW (UDP)	WA3	Distribution Data - On-line Market Data	GPW Only
DDS::OMD::ReplayA - GPW (TCP)	WA3	Distribution Data - On-line Market Data:: Replay	GPW Only
DDS::OMD::SnapshotA - GPW (TCP)	WA3	Distribution Data - On-line Market Data:: Snapshot	GPW Only
DDS::OMD::StreamA - All(en.) (UDP)	WA3	Distribution Data - Best Bid Offer	All/encr.
DDS::OMD::ReplayA - All(en.) (TCP)	WA3	Distribution Data - Best Bid Offer Market Data:: Replay	All/encr.
DDS::OMD::SnapshotA - All(en.) (TCP)	WA3	Distribution Data - Best Bid Offer Market Data:: Snapshot	All/encr.

Services	SITE	Description	Market/Source
OEG::BIN1 (TCP)	WA2	Order Entry Gateway:: BIN (nb 1)	All
OEG::BIN2 (TCP)	WA2	Order Entry Gateway:: BIN (nb 2)	All
OEG::FIX1 (TCP)	WA2	Order Entry Gateway:: FIX (nb 1)	All
OEG::FIX2 (TCP)	WA2	Order Entry Gateway:: FIX (nb 2)	All
OEG::DCP::FIX (TCP)	WA2	Order Entry Gateway:: Drop copy service (FIX only)	All

Services	SITE	Description	Market/Source
DDS::OMD::StreamB - All (UDP)	WA2	Distribution Data - On-line Market Data	All
DDS::OMD::ReplayB - All(TCP)	WA2	Distribution Data - On-line Market Data:: Replay	All
DDS::OMD::SnapshotB - All (TCP)	WA2	Distribution Data - On-line Market Data:: Snapshot	All
DDS::OMD::BBO::StreamB - All (UDP)	WA2	Distribution Data - Best Bid Offer	All
DDS::OMD::BBO::ReplayB - All (TCP)	WA2	Distribution Data - Best Bid Offer:: Replay	All
DDS::OMD::BBO::SnapshotB - All (TCP)	WA2	Distribution Data - Best Bid Offer:: Snapshot	All
DDS::OMD::StreamB - GPW (UDP)	WA2	Distribution Data - On-line Market Data	GPW Only
DDS::OMD::ReplayB - GPW (TCP)	WA2	Distribution Data - On-line Market Data:: Replay	GPW Only
DDS::OMD::SnapshotB - GPW (TCP)	WA2	Distribution Data - On-line Market Data:: Snapshot	GPW Only
DDS::OMD::StreamB - All(en.) (UDP)	WA2	Distribution Data - Best Bid Offer	All/encr.
DDS::OMD::ReplayB - All(en.) (TCP)	WA2	Distribution Data - Best Bid Offer Market Data:: Replay	All/encr.
DDS::OMD::SnapshotB - All(en.) (TCP)	WA2	Distribution Data - Best Bid Offer Market Data:: Snapshot	All/encr.

MARKET DATA ENCRYPTION

Market Data Feed is encrypted.

Certain message fields sent from DDS::OMD::StreamA - All(en.) and DDS::OMD::StreamB - All(en.) and corelated DDS::OMD::ReplayB - All(en.) (TCP) streams are encrypted. Data decryption requires capturing the encryption key, transmitted in EncryptionKey messages streamed during the initial DDS::OMD::Snapshot session. More details on the decryption process can be found in GPW WATS 3.01 Market Data Gateway Protocol Specification document.

5.1.1.1. Prod-Bis Service Organization

This will be provided in the next version of the documentation,

5.1.2. GPW WATS STANDARD OPERATION MODE

GPW WATS EUAT and PRE-PROD (PROD) system modules (services) operate in parallel in two GPW Data Centers: WA3 and WA2.

Based on GPW WATS architecture designs, all hardware units in WA3 and WA2 can host GPW WATS OEG services.

Under normal operating conditions, the network infrastructure of each GPW actively participates in providing redundant connections between GPW and client. Resources (servers) and active Trading System modules during standard operation mode in WA3 and WA2 are up and running.

GPW WATS market data multicast feeds are distributed in parallel: (Stream A) from WA3 and (Stream B) from WA2.

By design, DDS Market Data feeds (Stream A and Stream B) are identical. When the network or DDS module malfunctions, the client is obliged to use only one (Stream A or Stream B) Market Data feed accessible from one of the GPW Sites.

5.1.3. GPW WATS TECHNICAL EMERGENCY OPERATION MODE

5.1.3.1. Scenario 1 – Client Network Issue

Connection between the client and GPW WATS excludes SPoF (single point of failure). Routing and network topology should guarantee access to GPW services in the event of a single network connection failure.

Traffic from the client's system should be redirected to an active network connection to GPW WATS platform.

DDS service access and Market Data feed in this situation is limited to Single stream (Stream A or Stream B) depending on the physical network connectivity termination point.

5.1.3.2. Scenario 2 – GPW WATS Single Service Failure

A Single service can be restarted (rebuilt) on free resources and available for clients without technical connectivity reconfiguration.

5.1.3.3. Scenario 3 – GPW WATS Site Failure

Services are only available for clients at one specific GPW WATS site.

This scenario does not provide the facility to connect to GPW WATS services configured in an inaccessible site.

IMPORTANT:

These scenarios mentioned are not applicable to clients who use the Collocation type of access.

6. GPW WATS CONNECTIVITY

6.1. GENERAL RULES

6.1.1. RESPONSIBILITY AND RECOMMENDATION

GPW does not manage any parts of network or application infrastructure at client's location used to access GPW WATS, thus all client's network infrastructure, in particular edge network devices used to access GPW WATS is managed by a client.

GPW's responsibility for the demarcation point is the network device port managed by telecommunication service providers, which communicate directly with devices managed by GPW. Each Participant is required to order and maintain the lines necessary to communicate with GPW at its own expense. Any operational issues with these lines will be resolved by the Participant and network provider as defined in the SLA.

6.1.2. CLIENT NETWORK DESIGN

The client is responsible for designing the technical infrastructure necessary to implement access to GPW WATS on the client side (including installation and configuration of edge network devices with all aspects of redundancy). However, GPW will provide the general requirements which must be met by each client solution connected to GPW WATS.

6.1.3. CONNECTION SECURITY

Data transfer security between GPW WATS and external client applications is based on the following assumptions:

- WAN connection to GPW WATS is provided over a classified data network.
- It is managed and controlled by individual telecommunication service providers.
- Implementation of connections must comply with GPW requirements. Connections can only be implemented between authorized GPW sites and external client locations.

Data security – Telecommunication service providers provide lines over non-public networks and must ensure adequate separation of communication between clients and only allow communication between clients and GPW. Telecommunication service providers are also responsible for preventing data sniffing and unauthorized access.

6.1.4. GENERAL REMARKS TO CONNECTIVITY AND GPW REQUIREMENTS

The technical documentation published by GPW obliges clients to be compliant with all requirements and recommendations included in it.

Access to GPW services can be realized by clients connected to GPW directly, authorized by GPW network connections. Only telecommunication service providers authorized by GPW can provide connectivity with an appropriate level of redundancy.

GPW is not responsible for any damage caused by improper protection of the application and network resources on the client site (this also applies to telecommunication connections as they are the responsibility and the property of the client).

The client's network system and application connections used for communication with GPW must permit a full diagnosis of its operations. Results of this diagnosis must be made available to all parties involved.

6.1.5. ACTIVE / ACTIVE MODE

In normal operating mode, both sites (WA3 and WA2) are active and accept Client connections.

Both telecommunication lines between the client and WA3 and WA2 should always be active.

GPW recommends setting the configuration with active OEG and DDS sessions (and connections) in parallel with both GPW sites (WA3 and WA2).

6.2. CONNECTIVITY – TECHNICAL ASPECTS

6.2.1. SUPPORTED ACCESS

6.2.1.1. Equinix Fabric

GPW WATS will be visible as a dedicated service for Equinix Fabric network users.

Connection standards for Equinix Fabric are defined in the documentation provided by Equinix. The standard connection is based on 100Mbps per client and 10Gbps port. GPW recommends redundancy connection provided by Equinix. Technical standard: fiber optic, single mode (two single fibers).

6.2.1.2. IPVPN L3

6.2.1.2.1. General Information

Redundant DCs

The GPW WATS system is deployed in two main Equinix sites, WA2 and WA3, which provide service to System as active/active deployments. Both sites are equipped with the complete technical infrastructure necessary to support trading on the GPW market. Under normal operating conditions, each site's network infrastructure actively provides access to System.

Redundant Connections

Physical connectivity with both GPW sites (WA3 and WA2) is required to provide full redundant access to GPW WATS. GPW recommendation is to use two different MPLS operators to provide such connectivity to each location.

Both connections must always be active and consider production under normal operation conditions. If any link that the client prefers for unicast or multicast traffic fails, the traffic will automatically switch to the other link using redundancies provided by routing protocols. The above mechanism will ensure an uninterrupted flow of network traffic and reliable access to GPW WATS.

The client application communicating with GPW WATS transaction system should have redundancy and high availability mechanisms supported by System. In particular, the client application receiving market data should receive this data from two redundant multicast channels GPW WATS provides over separate paths.

Redundant market data access

Market data will be available through two redundant multicast channels, A and B streams, sent from Equinix's WA3 and WA2 locations, respectively. These multicast channels will be transmitted via different routes and a completely independent technical infrastructure that is fully redundant.

Addresses of GPW WATS

The detailed specification of access to GPW WATS, in the addresses of external interfaces of the Trading System, are provided in **APPENDIX A,** also have been published on the portal dedicated to GPW clients and are available upon request sent to GPW helpdesk: ts@gpw.pl. The addresses of external interfaces of the Trading System will be all the required addresses, including those used in failover and disaster recovery procedures. The addresses' usage will be determined in agreement with GPW's telecommunication operator partners.

Division of responsibilities

The demarcation point of the responsibility of the GPW is the port of the network device administered by the telecommunication operator, which communicates directly with devices administered by the GPW. The GPW will not manage any network and application infrastructure elements on client side. The GPW is unable to monitor the operating status of MPLS operator lines on client side. The client orders and maintains lines necessary to communicate with the GPW at client's own expense. Any operating issues with the lines will be resolved by the client with the MPLS operator as defined in the SLA with the operator. The GPW offers edge application infrastructure (appropriate edge application servers) at its sites to provide access of clients to GPW Trading System elements over WAN.

Security

Security of data exchange between the GPW Trading System and external client applications is based on the following:

- the wide area network supporting the connection of the GPW Trading System with external client applications is not a public network.
- It is managed and controlled by individual telecommunication operators (certified by the GPW).
- The implementation of connections complies with the GPW's requirements; in particular, connections can only be implemented between authorized GPW sites and external client locations.

6.2.1.2.2. Customer connectivity architectures

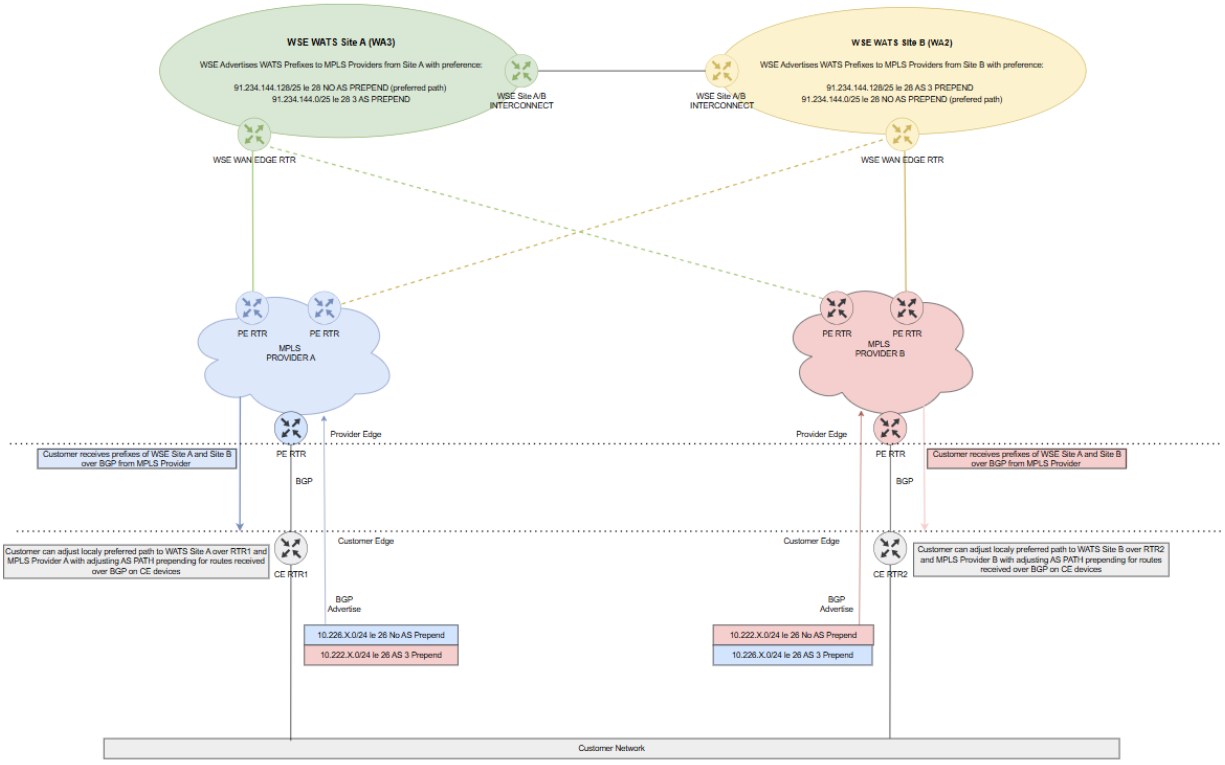
Customer prefixes for WATS access from range 10.222.X.0/24 and 10.226.X.0/24 are assigned by WSE. Below scenarios illustrate the general network path between WSE - Network Providers - End Customers over available connection methods and can be used for reference to build Customer connectivity to WATS. Please take into consideration that below scenarios don't address specific Customer network requirements such as firewall placement, address translation (NAT) in Customer network that can influence network path from Customer to WSE WATS infrastructure.

6.2.1.2.2.1. SCENARIO 1

Customer single homed with two MPLS Providers using two edge routers

- Customer is using two edge devices (CE RTR) with BGP peering to MPLS Provider (PE RTR).
- Customer advertises prefixes to WSE from two CE devices with both CE devices advertising 10.226.X.0/24 le 26 and 10.222.X.0/24 le 26.

- Customer is receiving all WSE WATS Site A and Site B prefixes on each MPLS provider BGP peering.
- Customer routing preference can be adjusted on Customer edge devices (CE RTR) :
    - Preference towards WSE Site A / B prefixes - adding AS PATH prepending to WSE Site A / B routes received from MPLS Providers on BGP peering
    - Preference from WSE to Customer prefixes - adding AS PATH prepending to Customer prefixes advertised to MPLS Providers on BGP peering
- To avoid asymmetric routing configuration, the Customer can advertise one assigned prefix as prefered over MPLS Provider A and other as preferred over MPLS Provider B using AS PATH prepending on CE Devices.



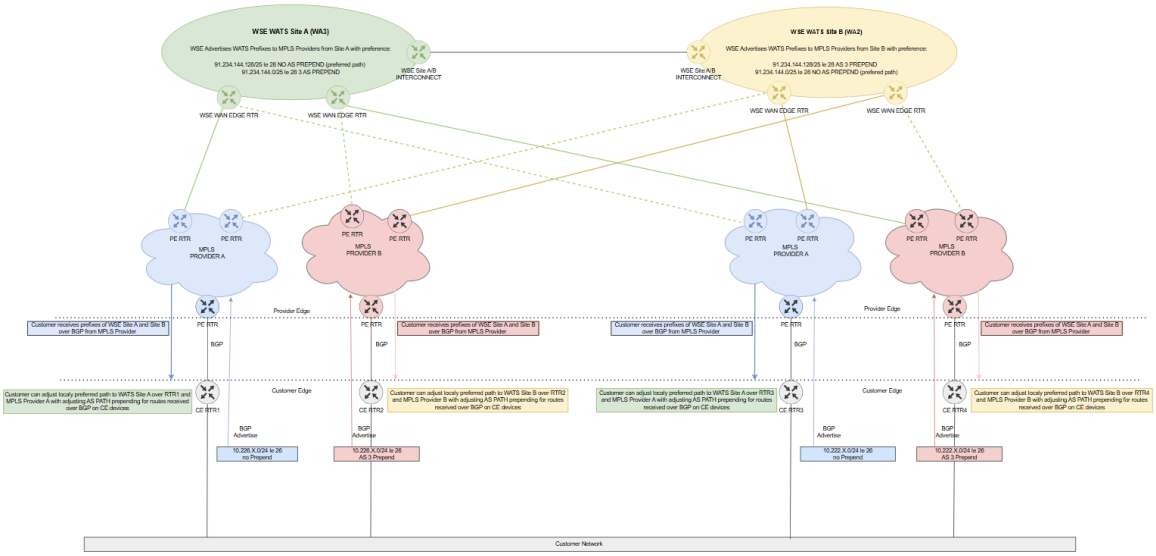
6.2.1.2.2. SCENARIO 2

Customer dual homed with two MPLS Providers using four edge routers

- Customer is using four edge devices (CE RTR) with BGP peering to MPLS Provider (PE RTR).
- Customer advertises prefixes to WSE from four edge devices with two advertising 10.226.X.0/24 le 26 and two devices advertising 10.222.X.0/24 le 26.
- Customer is receiving all WSE WATS Site A and Site B prefixes on each MPLS provider BGP peering.
- Customer routing preference can be adjusted on Customer edge devices (CE RTR) :
    - Preference towards WSE Site A / B prefixes - adding AS PATH prepending to WSE Site A / B routes received from MPLS Providers on BGP peering

- Preference from WSE Site A/B to Customer prefixes - adding AS PATH prepending to Customer Prefixes advertised to MPLS Providers on BGP peering

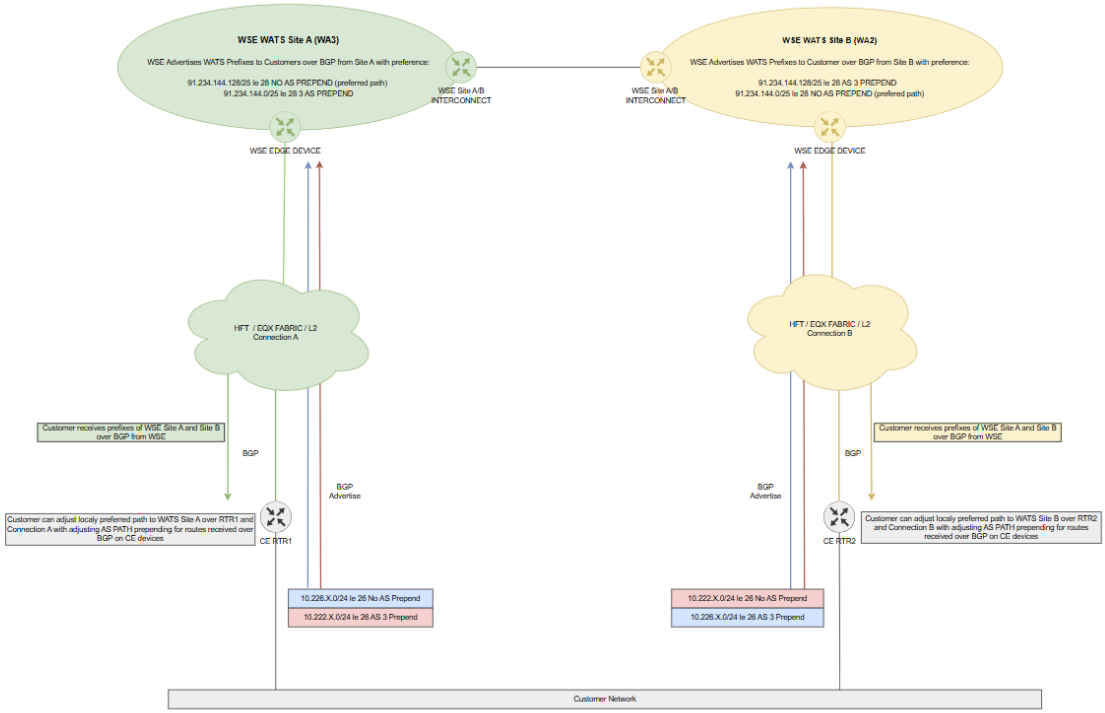
- To avoid asymmetric routing configuration the Customer can advertise one assigned prefix as prefered for WSE Site A access and other as preferred for WSE Site B access using AS PATH prepending on CE Devices



6.2.1.2.2.3. SCENARIO 3

Customer connected over two dedicated HFT / L2 / EQX Fabric

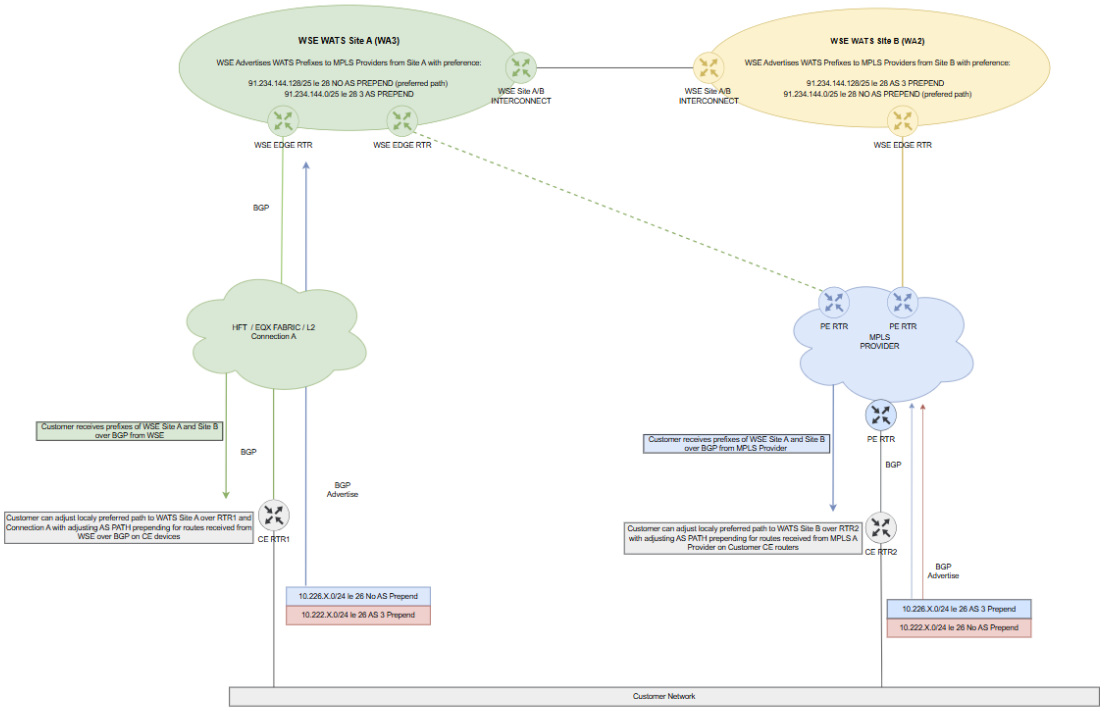
- Customer is using 2 edge devices (CE RTR) with BGP peering to WSE Edge Devices (PE RTR).
- Customer advertises own prefixes to WSE from 2 CE devices - preferring 10.226.X.0/24 over CE RTR1 and 10.222.X.0/24 le 26 over CE RTR2
- Customer is receiving all WSE WATS Site A and Site B prefixes on each WSE BGP peering.
- Customer routing preference can be adjusted on own edge devices (CE RTR) :
    - Preference towards WSE Site A / B prefixes - adding AS PATH prepending to WSE Site A / B routes received from WSE Edge Devices
    - Preference from WSE to Customer Prefixes - adding AS PATH prepending to Customer Prefixes advertised to WSE Edge Devices
- To avoid asymmetric routing configuration the Customer should advertise one assigned prefix as preferred over Connection A and other as preferred over Connection B using AS PATH prepending on CE Devices.



6.2.1.2.2.4. SCENARIO 4

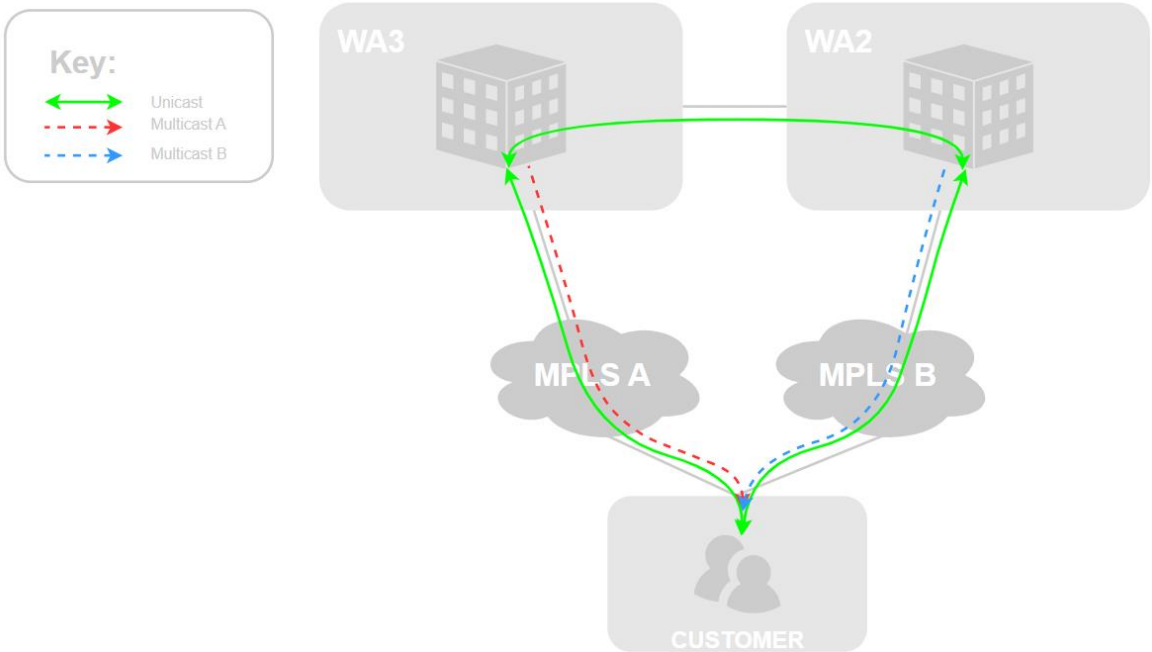
Customer connected over MPLS and HFT / L2 / EQX Fabric

- Customer is using two edge devices (CE RTR) with one BGP peering to WSE Edge Device over HFT / L2 / EQX Fabric connection and other over MPLS BGP peering.
- Customer advertises prefixes to WSE from two CE devices - preferring 10.226.X.0/24 over CE RTR1 and 10.222.X.0/24 le 26 over CE RTR2
- Customer is receiving all WSE WATS Site A and Site B prefixes on each WSE BGP peering.
- Customer routing preference can be adjusted on Customer edge devices (CE RTR) :
    - Preference towards WSE Site A / B prefixes - adding AS PATH prepending to WSE Site A / B routes received from WSE / MPLS Provider Edge Devices
    - Preference from WSE to Customer Prefixes - adding AS PATH prepending to Customer Prefixes advertised to WSE / MPLS Provider Edge Devices
- To avoid asymmetric routing configuration the Customer should advertise one assigned prefix as preferred over Connection A and other as preferred over MPLS using AS PATH prepending on CE Devices.

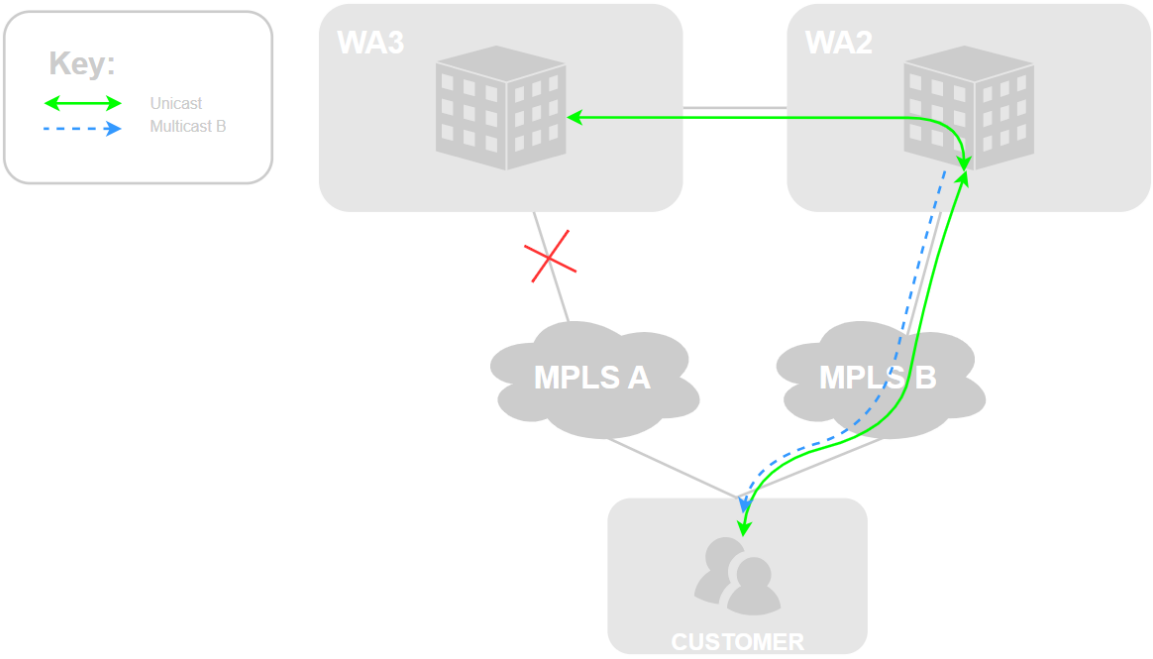


6.2.1.2.3. Typical Failover Scenarios

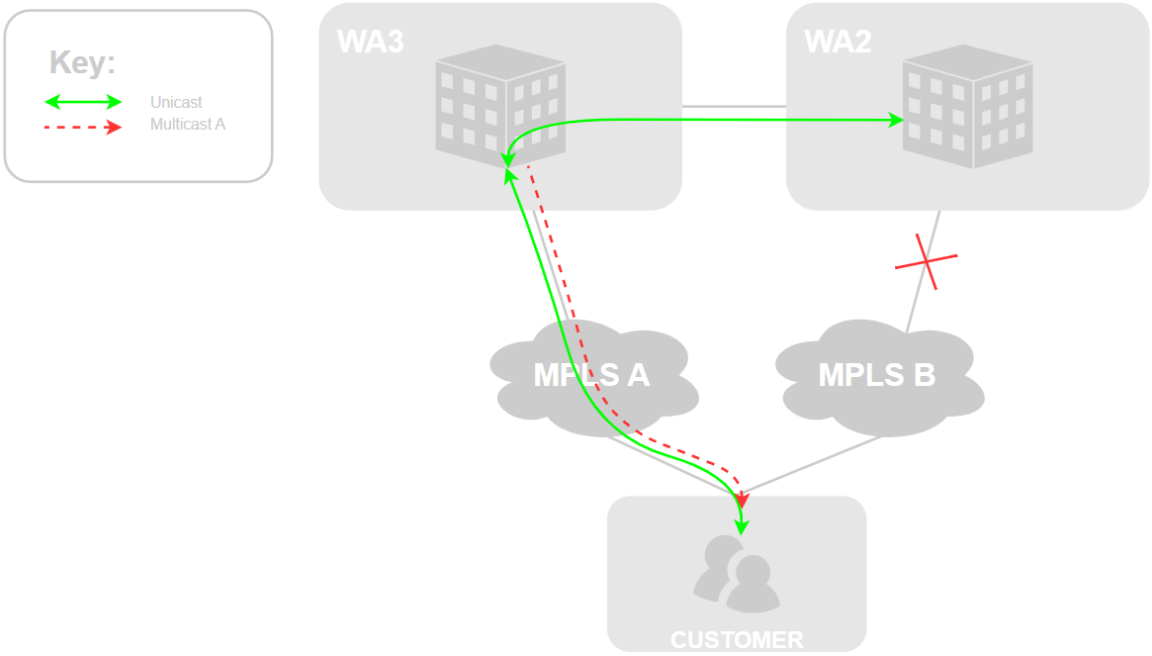
This scenario represents regular operation where both locations are accessible via two independent MPLS providers. Unicast flow is available from both sites. Two multicast separate streams are available from both locations.



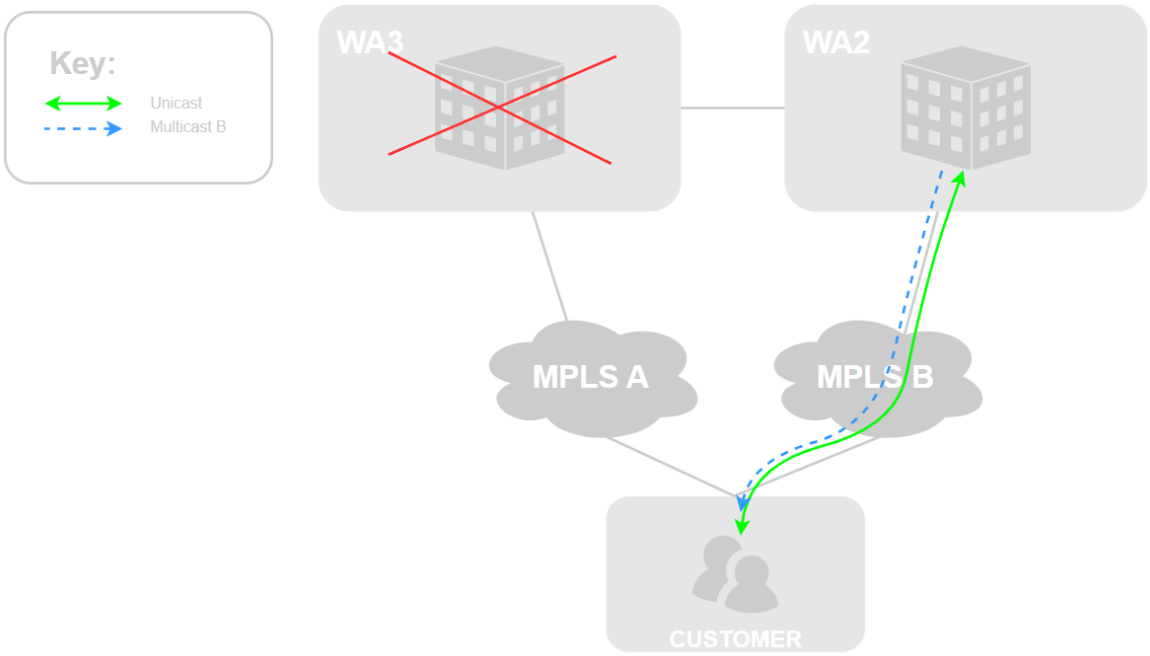
This scenario represents a failure of the MPLS link provider in WA3. Unicast traffic is available from both location WA2 and WA3 and multicast flow is available only from the WA2 site. Based on the application performance or respond time customer should decide which unicast flow is a better choice.



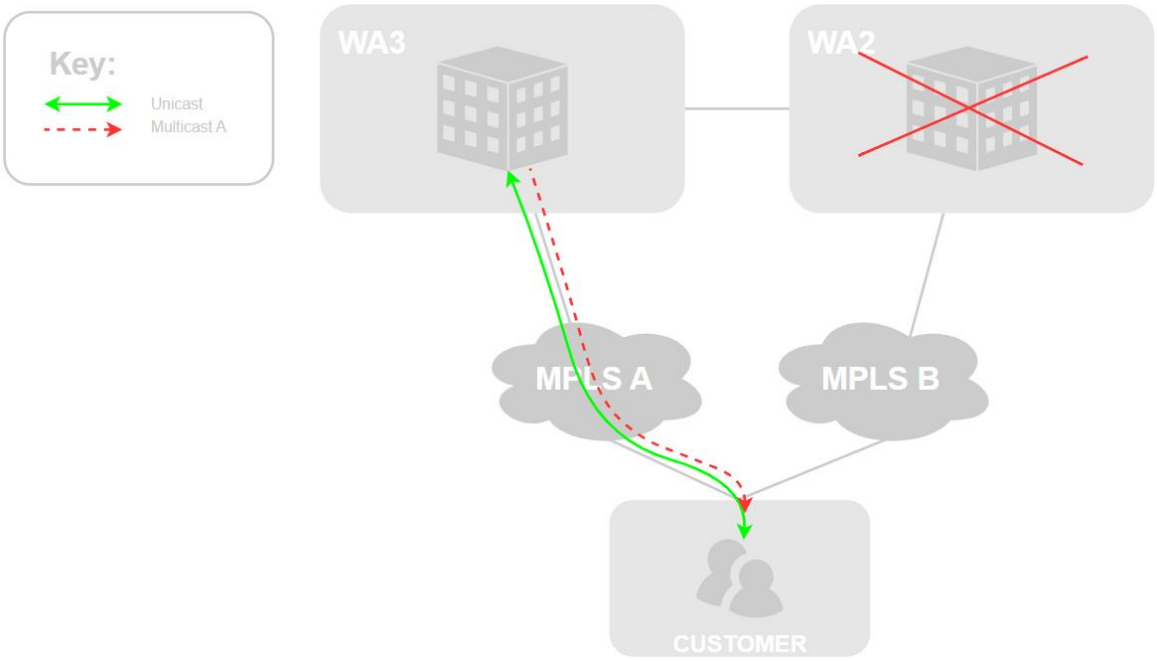
This scenario represents a failure of the MPLS link provider in WA2. Unicast traffic is available from both location WA2 and WA3 and multicast flow is available only from the WA3 site. Based on the application performance or respond time, customers should decide which unicast flow is a better choice.



This scenario represents a failure of the WA3 site. Unicast and multicast flows are available only from the WA2 site.



This scenario represents a failure of the WA2 site. Unicast and multicast flows are available only from the WA3 site.



6.2.1.3.-Technical Details of the Solution

Public (Market) Data

Public data will be transmitted over a multicast (UDP) and sent simultaneously in two streams, A (FROM WA3) and B (FROM WA2), both with the same data content (in redundant mode, in different multicast groups in stream A and B) in order to enable control of data completeness and cohesion by Exchange Member, Data Vendor or External Administrator's application and to make retransmit or refresh decisions. Public data under normal conditions as well as under refresh requests of an Exchange Member, Data Vendor or External Administrator will be sent from

the GPW over a multicast – communication necessary to send requests (from the Exchange Member, Data Vendor or External Administrator application) to retransmit missing public messages and refresh requests will be sent over a unicast (TCP). Requests to retransmit missing messages from Exchange Member, Data Vendor or External Administrator to the GPW and retransmission of missing messages from the GPW to Exchange Member, Data Vendor or External Administrator will be sent over a unicast (TCP). The direct sources of public messages (streams A and B) will be the GPW servers:

- DDS– supporting public data transmission under normal conditions.

Additional services (Replay and Snapshot) are unicast.

Confidential Data (Processing Orders)

Confidential data will be transmitted over a unicast (TCP): two protocols may be used at application level: Binary and FIX. Communication with the GPW in this regard will be sent to/from OEG (...) edge servers at the GPW.

Dynamic Routing

The dynamic routing must be available on the border between the Exchange Member, Data Vendor or External Administrators and MPLS operators (unicast border). Implementing dynamic routing between Exchange Members, Data Vendors, External Administrators, and MPLS operators aims to detect network failures and provide dynamic fail-over to other available paths to the GPW WATS application hosted in two GPW Equinix location.

It is important to mention that the GPW offers dynamic BGP routing between its edge devices and every MPLS operator. It is worth noting that there is no direct BGP peering connection between Exchange Member, Data Vendor, or Third-Party Administrator and the Exchange, regardless of the circumstances.

Marking Packets

The QoS feature is used to provide the most desirable flow of traffic through a network. QoS allows classifying the network traffic, police, and prioritize the traffic flow, and help avoid traffic congestion in a network. The control of traffic is based on the fields in the packets that flow through SystemGPW will not mark unicast traffic in QoS from WA3 and WA2. All traffic is treated as best-effort, and to ensure that such traffic provide the lowest possible latency and probability of packet loss in the network, customers must discuss their Quality of Service (QoS) configuration with their MPLS service provider, as the provider is responsible for determining how packets are routed and treated on the MPLS network. The provider is also responsible for ensuring the end-to-end quality of the QoS service, which falls outside the scope of GPW.

The production servers' IP addresses are sent individually with TCP ports and other application parameters to each Exchange Member, Data Vendor or External Administrator and agreed at the implementation phase.

Data Security

Ensuring data security is of utmost importance for the GPW. However, it is important to note that the traffic between the GPW and its Exchange Members, Data Vendors or External Administrators is not encrypted.

Telecommunication operators provide lines over non-public networks and must ensure adequate separation of communication between Exchange Members, Data Vendors or External Administrators and allow communication only between them and the GPW. Additionally, telecommunication operators are responsible for preventing data sniffing and unauthorized access to ensure the security of the data.

Physical Connectivity

Following the recommendation provided by GPW, it is highly advisable to employ SFP+ modules for all physical connections between the GPW edge devices and MPLS providers. It is predominantly because SFP+ transceivers facilitate upgrading speeds to higher than 1G in the future without incurring the need for module replacement.

In addition, single-mode modules should be utilized. Nevertheless, all technical specifications should be taken into consideration during the implementation of the solution.

The physical connection between GPW edge devices and the MPLS provider in each Equinix colocation can be shared by multiple customers using the same MPLS provider and GPW recommends MPLS providers to establish two redundant physical connected, each one can connected to cluster of GPW edge devices.

The GPW recommends a 150M bandwidth for multicast and unicast traffic per client. Nevertheless, the MPLS service provider must ensure logical separation between clients when multiple clients from the same provider share a physical connection and ensure proper propagation of GPW prefixes to the client's MPLS network.

Another option is to connect the operator's MPLS edge device via two physical links bundled into a logical port-channel to two separate GPW WATS switches utilizing MLAG technology to provide better resilience on the GPW WATS side. It is recommended that this option be discussed with an operator during the initial conversation regarding service provisioning in WA3 or WA2 locations.

GPW recommends full redundancy on each level of client infrastructure for GPW WATS services and separation from currently used network devices.

6.2.1.4.Leased Lines

Leased lines are point-to-point Ethernet lines between the client location and GPW Sites. GPW allows installation of physical access lines used for communication with GPW only over professional fiber optic cables, which ensure the necessary quality, scalability, and security of data transmission. It is expected that the client orders connections with the necessary capacity from two different telecommunication service providers, one to GPW WA3 and one to GPW WA2, which will ensure redundancy in communication with GPW WATS. The network capacity (bandwidth) is identical for both sites.

Leased line connection to GPW WATS can be set up in cooperation with any telecommunication service provider that will be able to provide a professional fiber optic circuit from a client location to GPW Sites over their own infrastructure or using third party shared infrastructure (not limited to the IPVPN L3 Telecom Provider list).

6.2.1.5.VPN Connection

In the PRODUCTION environment VPN connections guarantee access to OEG services only.

DDS: OMD and DDS::BBO services will not be accessible via VPN connection.

For EUAT environment VPN connections guarantee access to OEG and DDS (multicast) services only for testing and ISVs purposes.

6.2.1.6. HFT Access

6.2.1.6.1. General Information

Redundant DCs

The GPW WATS system is deployed in two main Equinix sites, WA3 and WA2, which provide service to System as active/active deployments. Both sites are equipped with the complete technical infrastructure necessary to

support trading on the GPW market. Under normal operating conditions, each site's network infrastructure actively provides access to System.

Redundant Connections

Physical connectivity to both GPW locations (WA3 and WA2) is required to ensure fully redundant access to the GPW WATS system. GPW recommends using two different physical cables that will be connected to two switches in each location to provide maximum redundancy.

Both connections must always be active and consider production under normal operation conditions. If any location that the client prefers for unicast or multicast traffic fails, the traffic will automatically switch to the other location using redundancies provided by routing protocols. The above mechanism will ensure an uninterrupted flow of network traffic and reliable access to the GPW WATS system.

The client application communicating with the GPW WATS transaction system should have redundancy and high availability mechanisms supported by System. In particular, the client application receiving market data should receive this data from two redundant multicast channels the GPW WATS provides over separate paths.

Redundant Market Data Access

Market data will be available through two redundant multicast channels, A and B streams, sent from Equinix's WA3 and WA2 locations, respectively. These multicast channels will be transmitted via different routes and a completely independent technical infrastructure that is fully redundant.

Addresses of the GPW WATS System

The detailed specification of access to the GPW WATS, the addresses of external interfaces of the Trading System, are provided in **APPENDIX A -** also have been published on the portal dedicated to GPW clients and are available upon request sent to GPW helpdesk: ts@gpw.pl. The addresses of external interfaces of the Trading System will be all the required addresses, including those used in failover and disaster recovery procedures. The addresses' usage will be determined in agreement with GPW's telecommunication operator partners.

Division of Responsibilities

The demarcation point of the responsibility of the GPW is the port of the network device manage by the customer, which is directly connected with devices administered by the GPW. The GPW will not manage any network and application infrastructure elements on client side. The GPW can monitor the status of direct links between GPW edge and customer, however usually inter-connections lines are provided by Equinix and any operating issues with the lines will be resolved by the client with the Equinix operator as defined in the SLA with the operator. The GPW offers edge application infrastructure (appropriate edge application servers) at its sites to provide access of clients to GPW Trading System elements over direct link connected to GPW infrastructure.

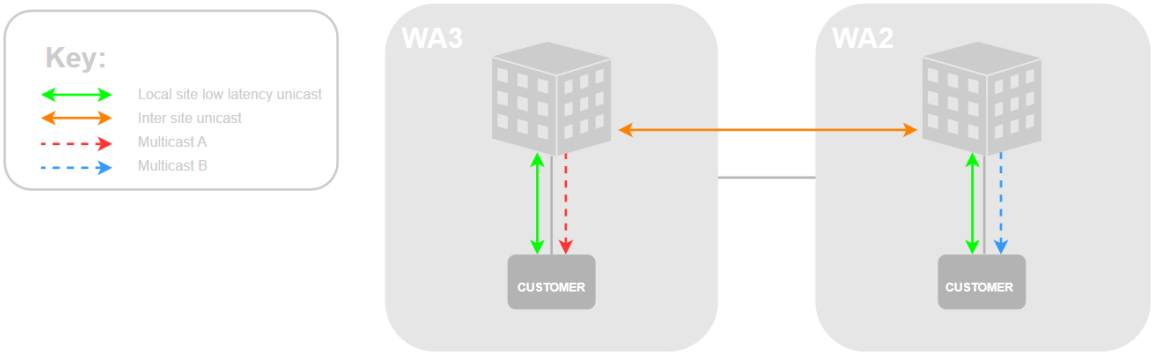
Security

Security of data exchange between the GPW Trading System and external client applications is based on the following:

- Direct connection of the GPW Trading System with external client applications is based on a private dedicated physical link.
- It is managed and controlled by WSA and external customer only.
- The implementation of connections complies with the GPW's requirements; in particular, connections is a direct physical cable between two entities only.

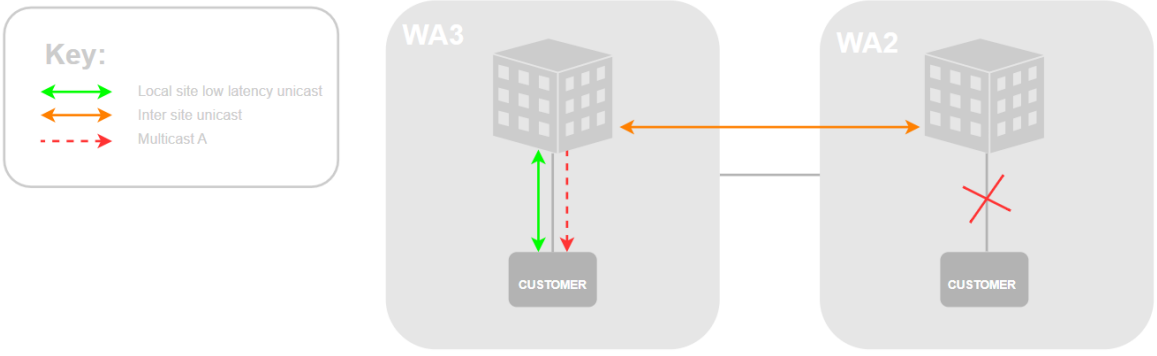
6.2.1.6.2. Typical Failover Scenarios

This scenario represents regular operation where both locations are accessible via two independent private connections in each Equinix colocation. The low latency unicast flow is available from each site. Two multicast separate streams are available from both locations.



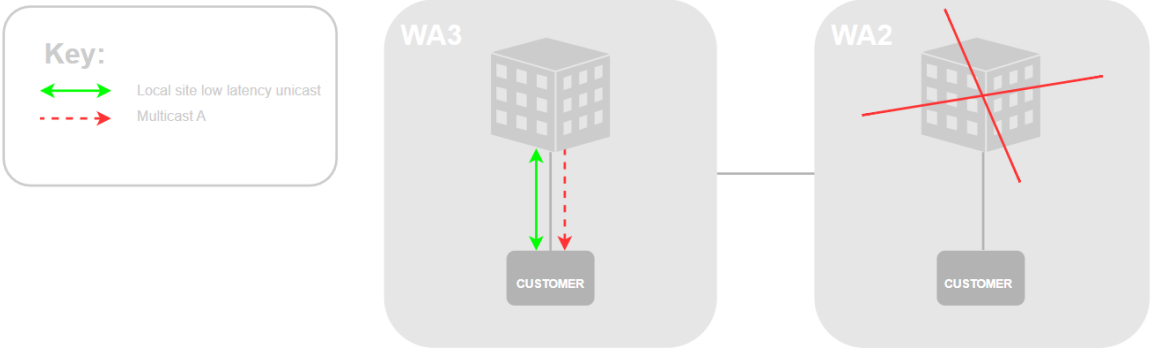
This scenario represents a failure of the direct connection in WA3. The low latency unicast traffic is available from a location WA2, and not low latency unicast traffic is available from WA3 over DCI link. Multicast flow is available only from the WA2 site.

This scenario represents a failure of the direct connection in WA2. The low latency unicast traffic is available from a location WA3, and not low latency unicast traffic is available from WA2 over DCI link. Multicast flow is available only from the WA3 site.



This scenario represents a failure of the WA3 site. Unicast and multicast flows are available only from the WA2 site.

This scenario represents a failure of the WA2 site. Unicast and multicast flows are available only from the WA3 site.



6.2.1.6.3. Technical Details of The Solution

Public (Market) Data

Public data will be transmitted over a multicast (UDP) and sent simultaneously in two streams, A (FROM WA3) and B (FROM WA2), both with the same data content (in redundant mode, in different multicast groups in stream A and B) in order to enable control of data completeness and cohesion by the Exchange Member, Data Vendor or External Administrator's application and to make retransmit or refresh decisions. Public data under normal conditions as well as under refresh requests of an Exchange Member, Data Vendor or External Administrator will be sent from the GPW over a multicast – communication necessary to send requests (from the Exchange Member, Data Vendor or External Administrator application) to retransmit missing public messages and refresh requests will be sent over a unicast (TCP). Requests to retransmit missing messages from an Exchange Member, Data Vendor or External Administrator to the GPW and retransmission of missing messages from the GPW to the Exchange Member, Data Vendor or External Administrator will be sent over a unicast (TCP). The direct sources of public messages (streams A and B) will be the GPW servers:

- DDS – supporting public data transmission under normal conditions.

Additional services (Reply and SnapShot) are unicast.

Confidential Data (Processing Orders)

Confidential data will be transmitted over a unicast (TCP); two protocols may be used at application level: Binary and FIX. Communication with the GPW in this regard will be sent to/from OEG (...) edge servers at the GPW.

Dynamic Routing

The recommended dynamic routing protocol between GPW WATS FTD edge and customer edge is a BGP for unicast and PIM-SM for multicast. Implementing dynamic routing between both entities aims to detect network failures and provide dynamic fail-over to other available paths to the GPW WATS application hosted in two GPW Equinix locationWarsaw Stock Exchange strongly recommended using the BFD feature to provide sub-seconds failover for any control plane issues, which can speed up failure detection much faster than relying on setting BGP or PIM timers.

Data Security

Ensuring data security is of utmost importance for the GPW. However, it is important to note that the traffic between the GPW and its customers is not encrypted.

Physical Connectivity

Following the recommendation provided by GPW, it is highly advisable to employ SFP+ modules for all physical connections between the GPW edge devices and customer edge. It is predominantly because SFP+ transceivers facilitate upgrading speeds to higher than 1G in the future without incurring the need for module replacement.

In addition, single-mode modules should be utilized. Nevertheless, all technical specifications should be taken into consideration during the implementation of the solution.

GPW WATS recommends connecting the customer edge device via two physical links bundled into a logical port-channel to two separate GPW WATS switches utilizing MLAG technology to provide better resilience on the GPW WATS side. It is recommended that this option be discussed with a customer during the initial conversation regarding service provisioning in WA3 or WA2 locations.

6.2.2. TELECOMMUNICATION SERVICES PROVIDERS

For IPVPN L3 connectivity, GPW currently supports and authorizes telecommunication service providers listed in Appendix B.

GPW certified telecommunication service providers are obliged to require GPW Clients to obtain the formal GPW approval of each connection to be set up from the client's location to GPW Sites. The requirement includes parameters of inter-connections between GPW Participant's networks and telecommunication service providers.

Currently, in cooperation with telecommunication service providers, GPW is planning and preparing the network infrastructure needed to distribute GPW WATS services. More detailed information and a detailed access procedure will be provided in later versions of this document.

6.2.3. ADDITIONAL INFORMATION

Leased lines connectivity to GPW WATS can be set up by any telecommunication service providers depending on the client's business needs.

6.2.4. COLOCATION SERVICE

Colocation is a dedicated service at WA3. All colocation clients have guaranteed access to GPW WATS services (DDS and OEG) with identical latency.

All technical aspects of client equipment installation should be confirmed with Equinix directly.

Connectivity parameters for collation: see Appendix A.

6.3. Connectivity Details

6.3.1. GPW Locations (DATA CENTERS)

GPW WATS is in two locations: WA3 and WA2. Both locations are equipped with the complete technical infrastructure necessary to support trading on GPW. In normal mode, network infrastructure of both locations actively participates in redundant access to the processing center, where the active Core Matching Engine Module is started.

Core Matching Engine Module location and co-location service determine WA3 as a privileged location.

GPW recommended connectivity technical standards.

6.3.1.1. Network Traffic Routing

IP communication between GPW edge network devices and clients will be based on BGP routing. As for IPVPN L3 technology, GPW will have BGP peering with all certified telecommunication providers at each site providing GPW WATS services to clients. For leased lines GPW will have direct BGP peering with the client edge devices.

6.3.1.2. Client Addressing

As for IPVPN L3 connections, the IP addresses of clients and network parameters are agreed upon between GPW and telecommunication service providers per the request of GPW Client. For leased line connections, client connectivity details are discussed directly with GPW. All connectivity details (peering and source addressing, AS number) are discussed with GPW and telecommunication service providers or clients before establishing connectivity to GPW. GPW will provide GPW WATS services from both GPW Sites using public IPv4 addressing and an AS number.

6.3.1.3. Unicast Communication

Unicast communication between GPW and client is based on BGP routing. GPW WATS Unicast services provided from GPW locations will be presented as IPv4 BGP prefixes from both GPW Sites.

When there is a network failure, connection between the client and GPW WATS unicast services, considered the main unicast traffic, should be switched to an alternative network path based on BGP routing.

6.3.1.4. Multicast Communication

Multicast communication is based on BGP routing and the PIM protocol. Based on GPW WATS Data Distribution System architecture, connectivity to the market data feed should be as follows: Multicast A from WA3 should be configured as a separate connection to the market data feed, Multicast B from WA2. In normal operating mode, Multicast A and Multicast B will be distributed from two different GPW sites. Due to bandwidth restrictions, during network failure, only one market data feed should be received and routing both market data feeds using one network link is not allowed.

6.3.1.5. Bandwidth

Bandwidth specification – target GPW recommendation for GO-LIVE date (see table below).

NOTICE: Recommendation based on:

- Contractual WATS performance (40.000 orders/sec)

Service (one Site)	Bandwidth EUAT (One Site)	Bandwidth PrePROD (One Site)	Bandwidth PROD-BIS (WA3 only)
OEG::BIN (for all FIX and BIN session till 40.000 order / sec)	10 Mbps	10 Mbps	10 Mbps
OEG::FIX (see above)	10 Mbps	10 Mbps	10 Mbps
DDS::OMD::Stream1	40 Mbps	40 Mbps	40 Mbps
DDS::OMD::Stream2	40 Mbps	40 Mbps	n/a
DDS::BBO::Stream1	40 Mbps	40 Mbps	40 Mbps
DDS::BBO::Stream2	40 Mbps	40 Mbps	n/a
OEG::BIN (or FIX) + DDS::OMD::Stream1	50 Mbps	50 Mbps	50 Mbps
OEG::BIN (or FIX) + DDS::OMD::Stream2	50 Mbps	50 Mbps	n/a
OEG::BIN (or FIX) + DDS::BBO::Stream1	50 Mbps	50 Mbps	50 Mbps
OEG::BIN (or FIX) + DDS::BBO::Stream2	50 Mbps	50 Mbps	n/a
OEG::BIN (or FIX) + DDS::OMD::Stream1 + DDS::BBO::Stream1	100 Mbps	100 Mbps	n/a
OEG::BIN (or FIX) + DDS::OMD::Stream1 + DDS::BBO::Stream1 + DDS::OMD::Stream2 + DDS::BBO::Stream2	200 Mbps	200 Mbps	n/a

Stream1 – full market data with information from all segments, sources, and market operators.
Stream2 – market data without the GPW market data feed.
Clients should consider the possibility of reserving additional bandwidth above the value required for EUAT/PRE-PROD (PROD). Exact bandwidth requirements may be different and depend on client needs, including private and public data, total traffic, and instances of GPW WATS running on the same link.

IMPORTANT:

Due to the planned performance tests, GPW on the EUAT environment until opening the PRE-PROD GPW WATS instance, GPW recommends:

- When Client decides to connect to DDS and OEG services – GPW recommends allocating **100 Mbps.**
- When Client decides not to connect to DDS service and connect only to OEG service – GPW recommends allocating **at least 10 Mbps**.

BANDWIDTH TESTING

GPW perfomed some internal testing for below mcast groups as per the recommendation for 200Mbs MPLS bandwith. We are joining mcast groups from PRE-PROD and EUAT environment, in below schema, what should fullfill most of the scenarios for market operators.

Test 1	StreamID 11 WA2	StreamID 11 WA3	StreamID 211 WA2	StreamID 211 WA3	OK
Test 2	StreamID 11 WA2	StreamID 11 WA3	StreamID 12 WA2	StreamID 12 WA3	OK
Test3	StreamID 11 WA2	StreamID 12 WA2	StreamID 211 WA2	StreamID 212 WA2	OK
Test4	StreamID 11 WA3	StreamID 12 WA3	StreamID 211 WA3	StreamID 212 WA3	OK

For above 4 tests with the use of 200Mbs testing circuit purchase from one of the MPLS operator there are no single packet missing during the performance/capacity tests. So please take it as a reference for bandwith allocation, but exact requirements for bandwith may be different and depends on client needs. Testing environment architecture was MPLS circuit with draft rosen Multcast VPN implementation over provider network. As a CPE there has been used Cisco ISR 4431 with IOS isr4400-universalk9.17.12.05a.SPA.bin

7. GPW WATS CONNECTIVITY PROCEDURES

7.1. GPW WATS EUAT CONNECTIVITY GUIDE

Clients who would like to connect to GPW WATS EUAT are kindly asked for their cooperation in taking the necessary preparation steps described below.

7.1.1. STEPS TO CONNECT

Connecting to EUAT GPW WATS requires taking a series of actions:

- Readying software implementing protocols supported by System.
- Obtaining appropriate IP addresses of GPW WATS services.
- Obtaining credentials, required to authorize protocol login procedure to System (i.e., connection ID and token for the OEG::BIN (TCP) and the DDS::OMD::Snapshot (TCP), SenderCompID, SenderSubID, TargetCompID, TargetSubID for the OEG::FIX (TCP)).

Clients may consider these publicly available source code examples, which allow to connect to both the OEG and DDS:

Location	Description
access-client-rust	Rust source code example which implements connection to native binary Trading Port and Market Data (snapshot, stream, and replay).
access-client-cpp	C++ source code example which implements connection to native binary Trading Port and Market Data (snapshot, stream, and replay).
access-client-java	Java source code example which implements connection to native binary Trading Port and Market Data (snapshot, stream, and replay).

To run any of the three above sources you need to be familiar with the following information:

7.2. GPW WATS PROD/PROD-BIS CONNECTIVITY GUIDE

Clients who would like to connect to GPW WATS PROD/PROD-BIS are kindly asked for their cooperation in taking the necessary preparation steps described below.

7.2.1. STEPS TO CONNECT

Connecting to PROD/PROD-BIS GPW WATS requires taking a series of actions:

- Readying software implementing protocols supported by System.
- Obtaining appropriate IP addresses of GPW WATS services.
- Obtaining credentials, required to authorize protocol login procedure to System (i.e., connection ID and token for the OEG::BIN (TCP) and the DDS::OMD::Snapshot (TCP), SenderCompID, SenderSubID, TargetCompID, TargetSubID for the OEG::FIX (TCP)).

8. Appendix A

8.1. IP Addresses Details WA3 and WA2 (information for the connectivity providers and customers)

As mentioned above the BGP is the preferred routing protocol for the logical connection between the GPW and MPLS provider. As part of the project, GPW has reserved the public address **91.234.144.0/24** and the BGP AS number **24732** for peer-to-peer communication with all MPLS providers who will provide the GPW WATS service to their customers. Location WA3 will use the range **91.234.144.128/25** and location WA2 will use the range **91.234.144.0/25**

For BGP sessions, it is recommended to use BFD for sub second failover in case of a physical link or hardware issue. BFD provides much faster failure detection than standard BGP hold time, even though BGP timers can be adjusted to low values. Additionally, it is highly advised to use MD5 authentication to secure BGP TCP sessions between peers.

The following table shows the address breakdown for the Equinix WA3.

WA3	
Subnet	**Comments**
91.234.144.129/32	GPW WATS multicast PIM RP (Prod)
91.234.144.144/28	GPW WATS multicast source (Prod)
91.234.144.160/28	GPW WATS unicast source (Prod)
91.234.144.130/32	GPW WATS multicast PIM RP (Prod-Bis)
91.234.144.176/28	GPW WATS multicast source (Prod-Bis)
91.234.144.192/28	GPW WATS unicast source (Prod-Bis)
91.234.144.131/32	GPW WATS multicast PIM RP (eUAT)
91.234.144.208/28	GPW WATS multicast source (eUAT)
91.234.144.224/28	GPW WATS unicast source (eUAT)

A single IP address is allocated for each specific environment (Prod, Prod-BIS, eUAT) at the WA3 DC to serve as the PIM Rendezvous Point. Redundancy is ensured using the Anycast-RP mechanism.

Each MPLS P2P connection will be allocated a dedicated /30 subnet. Further details regarding the allocation will be determined during the implementation stage.

In certain cases, if the MPLS operator wants to establish a greater level of redundancy and connect their device to GPW edge devices in WA3 via port-channel technology, a dedicated /29 subnet will be allocated.

Table below shows allocated range for WA3 MPLS P2P connections.

WA3	
Subnet	**Comments**
10.56.4.0/24	MPLS P2P connections
10.56.5.0/24	MPLS P2P connections

The following table shows the address breakdown for the Equinix WA2.

WA2	
Subnet	**Comments**
91.234.144.1/32	GPW WATS multicast PIM RP (Prod)
91.234.144.16/28	GPW WATS multicast source (Prod)
91.234.144.32/28	GPW WATS unicast source (Prod)
91.234.144.2/32	GPW WATS multicast PIM RP (Prod-Bis)
91.234.144.48/28	GPW WATS multicast source (Prod-Bis)
91.234.144.64/28	GPW WATS unicast source (Prod-Bis)
91.234.144.3/32	GPW WATS multicast PIM RP (eUAT)
91.234.144.80/28	GPW WATS multicast source (eUAT)
91.234.144.96/28	GPW WATS unicast source (eUAT)

A single IP address is allocated for each specific environment (Prod, Prod-BIS, eUAT) at the WA2 DC to serve as the PIM Rendezvous Point. Redundancy is ensured using the Anycast-RP mechanism.

Each MPLS P2P connection will be allocated a dedicated /30 subnet. Further details regarding the allocation will be determined during the implementation stage.

In certain cases, if the MPLS operator wants to establish a greater level of redundancy and connect their device to GPW edge devices in WA2 via port-channel technology, a dedicated /29 subnet will be allocated.

Table below shows allocated range for WA2 MPLS P2P connections.

WA2	
Subnet	**Comments**
10.52.4.0/24	MPLS P2P connections
10.52.5.0/24	MPLS P2P connections

8.2. IP Addresses Details WA3 and WA2 (information for Connectivity Providers and customers)

In addition to the above IP addresses for the WA3 and WA2 Equinix locations, GPW has allocated a dedicated private address space **10.226.0.0/16 and 10.222.0.0/16** respectively, from which customers will be allocated /24 subnets for dedicated GPW WATS environment built on the customer side. That subnet will be advertised by customer BGP session to the MPLS provider and propagated to GPW WATS environment on the GPW side. Customer or MPLS provider are suppose to ensure the prefixes advertised to GPW are within the lenth of the subnet mask between /24 and /26. The GPW's imposition of addressing for GPW WATS environments on the client side will help avoid situations with overlapping IP addresses and the use of NAT, which will simplify deployment.

Two tables below show the private range allocation for customers GPW WATS environment.

WA3	
Subnet	Comments
10.226.0.0/16	Private range allocated for customers GPW WATS environment

WA2	
Subnet	Comments
10.222.0.0/16	Private range allocated for customers GPW WATS environment

Exact subnet allocation will be decided during the implementation phase and validated case by case with customers, The subnets will be assigned to customer in accordance with the plan below, taking into account the separation of access to environment, where "x" will be unique to the customer. If the customer requires more than 120 hosts on the environment, will be given another two subnets /24.

Access to the WATS environment	WA2 WA3	
	10.222.x.0/24	**10.226.x.0/24**
PROD (PREPROD)	10.222.x.0/26	10.226.x.0/26
PROD-Bis	10.222.x.64/26	10.226.x.64/26
EUAT	10.222.x.128/26	10.226.x.128/26
for future use	10.222.x.192/26	10.226.x.192/26

8.3. AUTHENTICATION USING MICROSOFT ENTRA EXTERNAL ID

Watson and RMA use Microsoft Entra External ID as its primary authentication provider. Entra External ID is the Customer Identity and Access Management (CIAM) solution adopted within our organization and its used to securely manage external users. partners and customers accessing this application.

Authentication is implemented using the OpenID Connect (OIDC) protocol, which provides standardized secure and interoperable user sign-in and token-based access flows.

To enhance security, the solution also supports Multi-Factor Authentication. MFA is enforced using email-based One-Time Password codes.

8.4. PROD (PREPROD)

8.4.1. TRADING PORTS

Port	Parameter	Description	WA3		WA2	
OEG::BIN	IP address	TCP/IP address of the service.	91.234.144.164	91.234.144.165	91.234.144.36	91.234.144.37
	Port	TCP/IP port of the service.	10132	10132	10132	10132

Port	Parameter	Description	WA3		WA2	
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member			
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member			
OEG::FIX	IP address	TCP/IP address of the service.	91.234.144.164	91.234.144.165	91.234.144.36	91.234.144.37
	Port	TCP/IP port of the service.	10133	10133	10133	10133
	SenderCompID	Numerical value used to identify company sending the message.	Individually set with WSE Exchange Member			
	TargetCompID	Numerical value used to identify company receiving the message.	fix_port_A_1	fix_port_A_2	fix_port_A_1	fix_port_A_2
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member			
OEG::DCP FIX	IP address	TCP/IP address of the service.	91.234.144.164		91.234.144.36	
	Port	TCP/IP port of the service.	10134		10134	
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member			
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member			
	TargetCompID	Numerical value used to identify company receiving the message.	dc_port_A_1			

8.4.2. MARKET DATA

Full Market Data

Port	Parameter	Description	WA3	WA2
DDS::OMD::Snapshot All Data	IP address	TCP port of the service.	91.234.144.166	91.234.144.38
	Port	TCP/IP port of the service.	10150	10150
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	

Port	Parameter	Description	WA3	WA2
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay All Data	IP address	TCP/IP address of the service.	91.234.144.166	91.234.144.38
	Port	TCP/IP port of the service.	10152	10152
Mcast IP address	**IP address**	**Mcast group address**	**233.1.3.1**	**233.1.2.1**

Port	Parameter	Description	WA3	WA2
DDS::OMD::Snapshot GPW Only	IP address	TCP port of the service.	91.234.144.166	91.234.144.38
	Port	TCP/IP port of the service.	10154	10154
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay GPW Only	IP address	TCP/IP address of the service.	91.234.144.166	91.234.144.38
	Port	TCP/IP port of the service.	10156	10156
Mcast IP address	**IP address**	**Mcast group address**	**233.1.3.3**	**233.1.2.3**

Best Bid Offer

Port	Parameter	Description	WA3	WA2
DDS::BBO::Snapshot All Data	IP address	TCP port of the service.	91.234.144.166	91.234.144.38
	Port	TCP/IP port of the service.	10151	10151
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::BBO::Replay All Data	IP address	TCP/IP address of the service.	91.234.144.166	91.234.144.38
	Port	TCP/IP port of the service.	10153	10153
Mcast IP address	**IP address**	**Mcast group address**	**233.1.3.2**	**233.1.2.2**

Full Market Data (Crypted)

Port	Parameter	Description	WA3	WA2
DDS::OMD:: Snapshot All Data	IP address	TCP port of the service.	91.234.144.167	91.234.144.39
	Port	TCP/IP port of the service.	10155	10155
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay ALL Data	IP address	TCP/IP address of the service.	91.234.144.167	91.234.144.39
	Port	TCP/IP port of the service.	10157	10157
Mcast IP address	**IP address**	**Mcast group address**	**233.1.3.4**	**233.1.2.4**

8.4.2.1.Multicast Groups

Site	Multicast Groups	StreamID	IP address	Port	Encrypted
WA3	#M011 All Data Full Depth	11	233.1.3.1	31001	No
WA3	#M012 All Data BBO	12	233.1.3.2	31002	No
WA3	#M013 GPW Only Full Depth	13	233.1.3.3	31003	No
WA3	#M014 All Data Full Depth	14	233.1.3.4	31004	**Yes**

Site	Multicast Groups	StreamID	IP address	Port	Encrypted
Site	**Multicast Groups**	**StreamID**	**IP address**	**Port**	**Encrypted**
WA2	#M011 All Data Full Depth AllGPW	11	233.1.2.1	21001	No
WA2	#M012 All Data BBO AllGPW	12	233.1.2.2	21002	No
WA2	#M013 GPW Only Full Depth	13	233.1.2.3	21003	No
WA2	#M014 All Data Full Depth	14	233.1.2.4	21004	**Yes**

8.4.2.2. IDDS service

PRE-PROD (PROD) iDDS service

Access to the IDDS data is available via public Internet. In order to obtain the access to the application, it is necessary to provide source Public IP addressing not longer than /32 per data center.

fqdn	Port
idds.prod.gpw.pl	443 (REST API)
mb.prod.gpw.pl	443 (KAFKA)

Access to the IDDS data requires mTLS authentication.

8.4.2.3. Watson system

Access to the WATSON is provided via MPLS service, HFT connection and S2S VPN access only.

Fqdn is resolved via Public DNS.

fqdn	Port
watson.prod.gpw.pl	443

8.4.2.4. GUI RMA

Access to the GUI RMA is provided via MPLS service, HFT connection and S2S VPN access only.

Fqdn is resolved via Public DNS.

The application uses Microsoft Entra External ID for authentication.

fqdn	Port
rma.prod.gpw.pl	443

8.5. PROD-BIS – NOT PRESENT YET

8.5.1. TRADING PORTS

Port	Parameter	Description	WA3		WA2	
OEG::BIN	IP address	TCP/IP address of the service.	91.234.144.197	91.234.144.198	91.234.144.68	91.234.144.69

Port	Parameter	Description	WA3		WA2	
	Port	TCP/IP port of the service.	11132	11132	11132	11132
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member			
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member			
OEG::FIX	IP address	TCP/IP address of the service.	91.234.144.197	91.234.144.198	91.234.144.68	91.234.144.69
	Port	TCP/IP port of the service.	11133	11133	11133	11133
	SenderCompID	Numerical value used to identify company sending the message.	Individually set with WSE Exchange Member			
	TargetCompID	Numerical value used to identify company receiving the message.	Individually set with WSE Exchange Member			
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member			
OEG::DCP FIX	IP address	TCP/IP address of the service.	91.234.144.197		91.234.144.68	
	Port	TCP/IP port of the service.	11134		11134	

8.5.2. MARKET DATA

Full Market Data

Port	Parameter	Description	WA3	WA2
DDS::OMD::Snapshot All Data	IP address	TCP port of the service.	91.234.144.199	91.234.144.70
	Port	TCP/IP port of the service.	11150	11150
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay All Data	IP address	TCP/IP address of the service.	91.234.144.199	91.234.144.70
	Port	TCP/IP port of the service.	11152	11152
Port	**Parameter**	**Description**	**WA3**	**WA2**
DDS::OMD::Snapshot GPW Only	IP address	TCP port of the service.	91.234.144.199	91.234.144.70
	Port	TCP/IP port of the service.	11154	11154
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay GPW Only	IP address	TCP/IP address of the service.	91.234.144199	91.234.144.70
	Port	TCP/IP port of the service.	11156	11156

Best Bid Offer

Port	Parameter	Description	WA3	WA2
DDS::BBO::Snapshot All Data	IP address	TCP port of the service.	91.234.144.199	91.234.144.70
	Port	TCP/IP port of the service.	11151	11151
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::BBO::Replay All Data	IP address	TCP/IP address of the service.	91.234.144.199	91.234.144.70
	Port	TCP/IP port of the service.	11153	11153

Full Market Data (Crypted)

Port	Parameter	Description	WA3	WA2
DDS::OMD:: Snapshot All Data	IP address	TCP port of the service.	91.234.144.200	91.234.144.71
	Port	TCP/IP port of the service.	11155	11155
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay ALL Data	IP address	TCP/IP address of the service.	91.234.144.200	91.234.144.71
	Port	TCP/IP port of the service.	11157	11157

8.5.2.1. Multicast Groups

Site	Multicast Groups	StreamID	IP address	Port	Encrypted
WA3	#M111 All Data Full Depth	111	233.2.3.1	31101	No
WA3	#M112 All Data BBO	112	233.2.3.2	31102	No
WA3	#M113 GPW Only Full Depth	113	233.2.3.3	31103	No
WA3	#M114 All Data Full Depth	114	233.2.3.4	31104	Yes
Site	**Multicast Groups**	**StreamID**	**IP address**	**Port**	**Encrypted**
WA2	#M111 All Data Full Depth AllGPW	111	233.2.2.1	21101	No
WA2	#M112 All Data BBO AllGPW	112	233.2.2.2	21102	No
WA2	#M113 GPW Only Full Depth	113	233.2.2.3	21103	No
WA2	#M114 All Data Full Depth	114	233.2.2.4	21104	Yes

.

8.5.2.2. IDDS service

PROD-Bis iDDS service – not present yet.

Access to the IDDS data is available using via public internet. In order to obtain the access to the System, it is necessary to provide source Public IP addressing not longer than /32 per data center.

fqdn	Port
idds.prodbis.gpw.pl	443 (https)
mb.prodbis.gpw.pl	443 (kafka)

8.5.2.3. Watson System

PROD-Bis WATSON service – not present yet.

Access to the WATSON system is provided via MPLS service, HFT connection and S2S VPN access.

Fqdn is resolved via Public DNS.

The application uses Microsoft Entra External ID for authentication.

fqdn	Port
watson.prodbis.gpw.pl	443

8.5.2.4. GUI RMA

PROD-Bis GUI RMA service – not present yet.

Access to the GUI RMA is provided via MPLS service, HFT connection and S2S VPN access.

Fqdn is resolved via Public DNS.

The application uses Microsoft Entra External ID for authentication.

fqdn	Port
rma.prodbis.gpw.pl	443

8.6. EUAT

8.6.1. TRADING PORTS

Port	Parameter	Description	WA3		WA2	
OEG::BIN	IP address	TCP/IP address of the service.	91.234.144.228	91.234.144.229	91.234.144.100	91.234.144.101
	Port	TCP/IP port of the service.	12132	12132	12132	12132
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member			
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member			
OEG::FIX	IP address	TCP/IP address of the service.	91.234.144.228	91.234.144.229	91.234.144.100	91.234.144.101
	Port	TCP/IP port of the service.	12133	12133	12133	12133
	SenderCompID	Numerical value used to identify company sending the message.	Individually set with WSE Exchange Member			
	TargetCompID	Numerical value used to identify company	fix_port_A_1	fix_port_A_2	fix_port_A_1	fix_port_A_2

Port	Parameter	Description	WA3	WA2
		receiving the message.		
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
OEG::DCP FIX	IP address	TCP/IP address of the service.	91.234.144.228	91.234.144.100
	Port	TCP/IP port of the service.	12134	12134
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
	TargetCompID	Numerical value used to identify company receiving the message.	dc_port_A_1	

8.6.2. MARKET DATA

Full Market Data

Port	Parameter	Description	WA3	WA2
DDS::OMD::Snapshot All Data	IP address	TCP port of the service.	91.234.144.230	91.234.144.102
	Port	TCP/IP port of the service.	12150	12150
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay All Data	IP address	TCP/IP address of the service.	91.234.144.230	91.234.144.102
	Port	TCP/IP port of the service.	12152	12152
Mcast IP address	**IP address**	**Mcast group address**	**233.3.3.1**	**233.3.2.1**
Port	Parameter	Description	WA3	WA2
DDS::OMD::Snapshot GPW Only	IP address	TCP port of the service.	91.234.144.230	91.234.144102
	Port	TCP/IP port of the service.	12154	12154
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay GPW Only	IP address	TCP/IP address of the service.	91.234.144.230	91.234.144.102
	Port	TCP/IP port of the service.	12156	12156
Mcast IP address	**IP address**	**Mcast group address**	**233.3.3.3**	**233.3.2.3**

Best Bid Offer

Port	Parameter	Description	WA3	WA2
DDS::BBO::Snapshot All Data	IP address	TCP port of the service.	91.234.144.230	91.234.144.102
	Port	TCP/IP port of the service.	12151	12151

Port	Parameter	Description	WA3	WA2
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::BBO::Replay All Data	IP address	TCP/IP address of the service.	91.234.144.230	91.234.144.102
	Port	TCP/IP port of the service.	12153	12153
Mcast IP address	**IP address**	**Mcast group address**	**233.3.3.2**	**233.3.2.2**

Full Market Data (Crypted)

Port	Parameter	Description	WA3	WA2
DDS::OMD:: Snapshot All Data	IP address	TCP port of the service.	91.234.144.231	91.234.144.103
	Port	TCP/IP port of the service.	12155	12155
	Connection ID	Numerical identifier of the connection.	Individually set with WSE Exchange Member	
	Token	Textual secret allowing authorization of the connection.	Individually set with WSE Exchange Member	
DDS::OMD::Replay ALL Data	IP address	TCP/IP address of the service.	91.234.144.231	91.234.144.103
	Port	TCP/IP port of the service.	12157	12157
Mcast IP address	**IP address**	**Mcast group address**	**233.3.3.4**	**233.3.2.4**

8.6.2.1. Multicast Groups

Site	Multicast Groups	StreamID	IP address	Port	Encrypted*
WA3	#M211 All Data Full Depth	211	233.3.3.1	31201	No
WA3	#M212 All Data BBO	212	233.3.3.2	31202	No
WA3	#M213 GPW Only Full Depth	213	233.3.3.3	31203	No
WA3	#M214 All Data Full Depth	214	233.3.3.4	31204	Yes
Site	**Multicast Groups**		**IP address**	**Port**	**Encrypted***
WA2	#M211 All Data Full Depth	211	233.3.2.1	21201	No
WA2	#M212 All Data BBO	212	233.3.2.2	21202	No
WA2	#M213 GPW Only Full Depth	213	233.3.2.3	21203	No
WA2	#M214 All Data Full Depth	214	233.3.2.4	21204	Yes

* The date of enabling encryption will be agreed with market participants.

8.6.2.2. IDDS service

Access to the IDDS data is available using via public internet. In order to obtain the access to the System, it is necessary to provide source Public IP addressing not longer than /32 per data center.

Fqdn	Port
idds.euat.gpw.pl	443 (https)
mb.euat.gpw.pl	443 (kafka)

Access to the IDDS data requires mTLS authentication.

8.6.2.3. Watson system

Access to the WATSON system is provided via MPLS service, HFT connection and S2S VPN access only.

Fqdn is resolved via Public DNS.

The application uses Microsoft Entra External ID for authentication.

Fqdn	Port
watson.euat.gpw.pl	443

8.6.2.4. GUI RMA

Access to the GUI RMA is provided via MPLS service, HFT connection and S2S VPN access only.

Fqdn is resolved via Public DNS.

The application uses Microsoft Entra External ID for authentication.

Fqdn	Port
rma.euat.gpw.pl	443

9. APPENDIX B

Table below represents supported MPLS operators, however this is not a defining list and GPW can support other providers too.

Operator	Unicast support	Multicast support	Supported technology	
Orange Polska S.A	YES	YES	MPLS/L2	https://www.orange.pl/
Exatel S.A.	YES	YES	MPLS/L2	https://exatel.pl/
ATMAN Sp. z o.o.	YES	YES	MPLS/L2	https://www.atman.pl/
Colt IQ, Colt Technology Services	YES	YES	MPLS	https://www.colt.net/
ICE Data, Intercontinental Exchange	YES	YES	MPLS	https://www.theice.com/
Hawe Telekom	YES	YES	L2	https://hawetelekom.com/
T-Mobile	YES	YES	L2	https://www.t-mobile.pl/
Netia	YES	YES	L2	https://www.netia.pl/
TNSI	YES	YES	MPLS	https://www.tnsi.com

10. APPENDIX C

Market Data services, Multicast Channels.