TRADER - FIX.SUITE

Messaging Guidelines

Version: 1.0

Last modified: 06/29/2020

SUMÁRIO

Change Log

Date	Version	Description	Author
June 29, 2020	1.0	- Initial version	RC, AYSF

1 DESCRIPTION

This document is intended to assist those who wish to develop applications that connect to FIX.SUITE services through the FIX protocol.

1.1 Benefits

1.2 System functions and characteristics

FIX.SUITE is based on the 4.4 version of the Financial Information Exchange ("FIX") Protocol. FIX is a technical specification for electronic communication of trade-related messages. It is an open standard managed by members of FIX Protocol Limited (https://www.fixtrading.org/).

This document outlines the B3 FIX implementation and is provided for third-parties which need trading connectivity through FIX.SUITE. It is assumed that the reader of this document has basic knowledge of the FIX protocol.

1.3 Contract information

For FIX.SUITE contract information, please contact the B3 Business Service Development team through the email address contratacao@b3.com.br or by phone +55 11 2565-5080.

For technical questions, please contact our Trading Support team through the email address tradingsupport@b3.com.br or by phone +55 11 2565-5000, option 2.

2 MARKET SEGMENT

2.1 Trading Platform Schedule

The following table describes the trading schedules for the platform in each market segment:

Segment	Schedule
FIX.SUITE Voice	Brought down daily between 22:00 and 3:00 (local time). On weekends between Fri 22:00 and Sun 12:00

> ⚠ In general, for TRADER FIX.SUITE, customers may connect every day or keep connected through the week. B3 highly recommends that customers remain disconnected during the weekends, unless when participating in scheduled mock tests.

3   NETWORK CONNECTIVITY

The following sections describe all connectivity options for FIX.SUITE.

3.1 Physical/Link Layer Options

Market participants can choose from the following connectivity offers.

3.1.1   RTM

Through the agreement between B3 and RTM, the interconnection between the technological infrastructures maintained and managed, respectively, by B3 and RTM was made possible, in order to allow access to the services made available in their technological infrastructures, by RTM participants and B3 participants. .

3.1.2   Internet

Through a connection with direct access to the Internet, previously authorized participants can obtain access to technological infrastructures and their respective services made available and exposed on the Internet by B3.

3.2 Authentication

FIX sessions may require the user to provide authentication data on the Logon message. The following tables depicts the fields used to convey such information:

Trade Login

Tag	Tag Name	Req´d	Datatype	Comment
553	Username	Y	String	Trader username
95	RawDataLength	Y	Integer	Password length, this field must come before Tag 96
96	RawData	Y	String	Password

Logon

Tag	Tag Name	Req´d	Datatype	Comment
98	EncryptMethod	Y	Int (1)	Must be "0"
108	HeartBtInt	Y	Int	Recommended: "30"
95	RawDataLength	N	Length	Required when this message contains authentication data. For more details on authentication data in Logon messages, please contact B3.
96	RawData	N	Data	Required when this message contains authentication data. For more details on authentication data in Logon messages, please contact B3.
58	Text	Y	String (250)	Customers should use this field to provide the name and certified version of the client solution used to connect to the Exchange. For example: Solution name 1.0
141	ResetSeqNumFlag	N	Boolean (1)	Indicates that the both sides of the FIX session should reset sequence numbers.
464	TestMessageIndicator	N	Boolean (1)	Sent only by B3
553	Username	N	String	Userid or username.
10	CheckSum	N	String	Always unencrypted, always last field in message
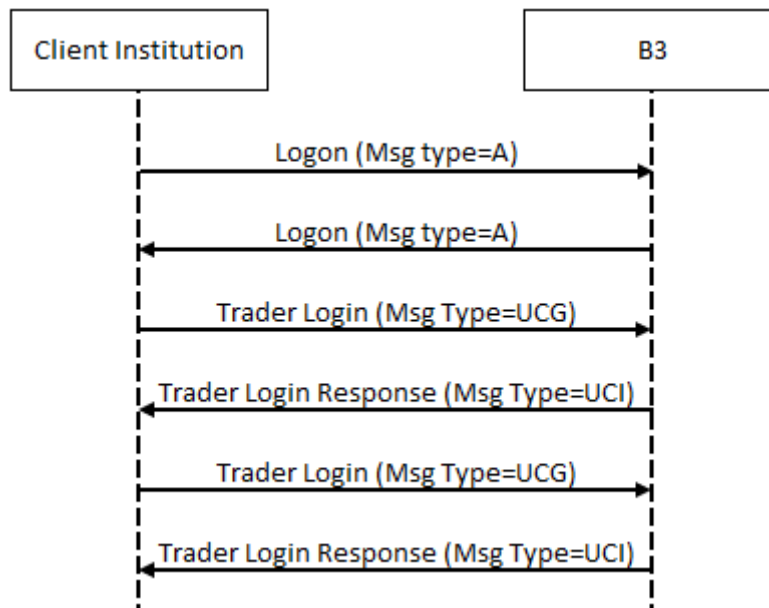
3.2.1 Password Renewal

Passwords are initially provided by B3 Trading Support Department (SSN) and then handed to clients to include in their applications. Users may change the password whenever it's necessary by sent e-mail to controledenegociacao@b3.com.br

3.2.2 Password Policy

In order to enforce security, some policies are in place and must be considered when changing passwords. The Password Policy comprehends the following aspects:

3.2.3 Password Age

By default, passwords are configured to not expire.

3.2.4 Session Lockout

In case a wrong password is provided, the authentication will fail and the connection will be shut down. A Logout message will be sent to indicate the failure in authentication. During the next 3 minutes the FIX session will be locked and no connection will be accepted within this time. The system allows up to 5 wrong

attempts to establish a connection, after what the FIX session is locked and users will need to contact B3 Trading Support Department (SSN) in order to restore the session.

3.2.5 Minimum Length

All passwords need to be at least 8 characters long. Requests for new passwords that don't conform to this requirement will be rejected.

3.2.6 Password History

The system records the last 10 passwords assigned to the FIX session. The new password must have not been used before.

3.2.7 Password Strength

In order to guarantee that passwords meet some strength requirements, the formation rule determines that all passwords must be composed of characters listed in three out of four categories:

- At least one lowercase character (from a through z)
- At least one uppercase character (from A through Z)
- At least one digit (from 0 through 9)
- At least one special character (non-alphanumeric)

Requests for new passwords that don't conform to this requirement will be rejected.

3.3 Throttle

The throttling mechanism controls the flow of messages at the FIX session level and was implemented to regulate the number of messages sent to B3 in order to optimize performance.

The throttling parameter is specified in messages per second and different actions may be taken should the throttle parameter be exceeded (queue or reject). So, two parameters may be set:

- The maximum amount of messages – which defines the maximum number of messages that will be processed per second;
- The reject / non-reject exceeded messages – defines if the exceeded messages must be rejected or queued.

If a message exceeds the maximum rate set, it can be rejected or queued. In case of rejection, a "Business Message Reject" error message will be sent with Business Reject Reason = "Throttle limit exceeded". Client systems can cross-reference the business message reject message with the originating message that was throttled by verifying the content of tag 45 (RefSeqNum). This tag will contain the FIX session level sequence number (tag 34) of the message that was rejected.

If non-reject is set, the throttle mechanism will withhold the messages exceeded until the end of the second, in this case, a higher latency would be observed in the response.

Assuming a scenario in which the limit is set to 50 messages per second. The first period of time begins when the gateway receives the first message and if more than 50 messages are sent before the next second, they are throttled.

3.4 Start of Day Procedures

The FIX session sequence number is reset to one at the beginning of each calendar day. Note that if client systems try to log on with a sequence number different than one at the start of day, the logon request will be rejected. However, during the day, client systems must not reset the sequence number, or all messages from the start of day will be retransmitted.

4   CERTIFICATION

B3 has a certification environment used by the participants and by Independent Software Vendors (ISVs) for testing and certification purposes of their software before accessing the productive environment of the Exchange.

The validation and the tests on acquired or under development solutions can be carried out during work days from 08:30 to 18:30 (local time), with no follow up needed from the certification team.

The certification environment can be access through a connection with direct access to the Internet, or using connection between the technological infrastructures maintained and managed, respectively, by B3 and RTM.

5   APPLICATION MESSAGE SCENARIOS

The following sections provide examples of the most common application message scenarios. In all scenarios, if a message is malformed or fails specific business level conditions, it will be rejected with either a Session Reject (invalid tag for message, invalid body length, etc) or Business Message Reject message (e.g., conditionally required field missing).

5.1 Order Management

5.1.1 Simple Voice

In this example, a simple voice is sent by the client institution. This voice is accepted by the counterparty.
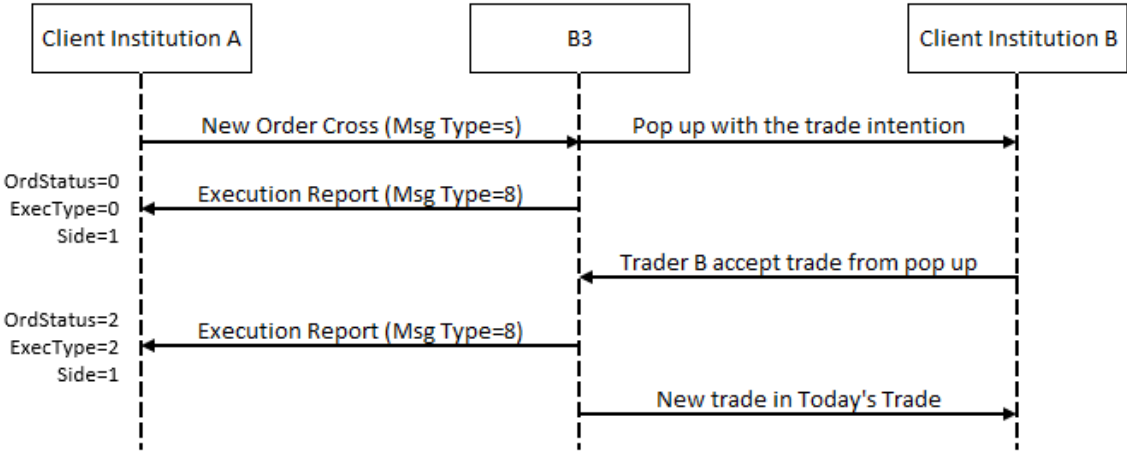

Figure 1 – Simple Voice

5.1.2 Funds Transfer

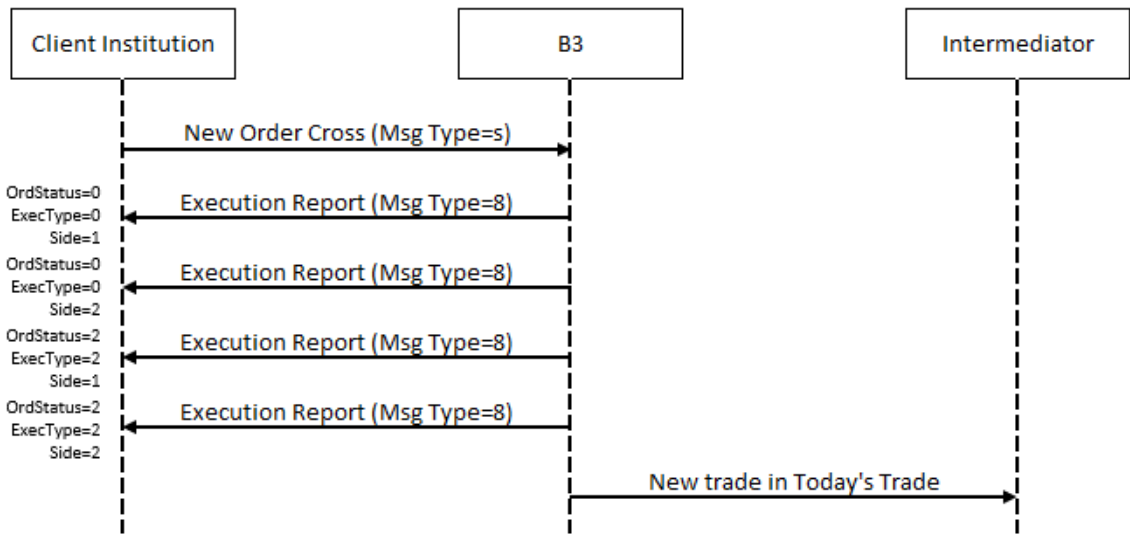In this example, a funds transfer is sent by the client institution. This voice is automatically accepted by the intermediator.

Figure 2 – Funds Transfer