INFORMATION DELIVERY PORTAL (IDP) – NLMD UAT PHASE

User Connectivity Overview

Created by:	**Johannesburg Stock Exchange**
Version	**1.0**
Date:	**2 March 2018**

TABLE OF CONTENTS

1. VERSION CONTROL

Version	Author	Date	Reason for changes
1.0	Nasheen Sharma	20/02/2018	Created.
1.1	Neil Vendeiro	02/03/2018	Revision based on internal review

2. INTRODUCTION

This document outlines the various connectivity requirements, which includes the delivery protocols, for the access and retrieval of data files from the JSE's delivery server, Information Delivery Portal (IDP).

This document is only relevant to the Non-Live Market Data User Acceptance Test (UAT) exercise, with the production version of the document, that is available on the JSE, being applicable for the production mode.

Note: Any IDP User ID created for new users of IDP during the UAT will become the relevant for production data file access once the ITaC changes go live.

Subscribers will be able to access the data files either via the Internet or via a leased line to the JSE delivery server, IDP, in Johannesburg. The JSE provides different protocols for accessing / for connectivity to the IDP service and these are covered in section 5.

Any problems in respect of the data in any file or in respect of connectivity must be communicated to the JSE Customer Support team for assistance. The JSE Customer Support team will conduct initial investigations and where necessary, the problem will be referred to the technical support staff of the JSE.

JSE Customer Support Contact details: CustomerSupport@jse.co.za		
Service Times	**All times are in South African Standard Time (SAST)**	**Contact Number**
JSE Business Hours:	06h30 – 19h00	+27 (0)11 520 7777
After Hours:	19h00 – 06h30	+27 (0)11 520 7900 (this number is automatically routed to the standby person) Or +27 (0)83 611 9315

3. AUTHENTICATION CREDENTIALS

The JSE deems the below access control measures critical to ensure that clients only access the information that they are licensed for and therefore entitled to. This structure also better protects the JSE from malicious activities.

On this basis, clients involved in the download service will be required to provide some personal information such as their email address, identification number and mobile number. This information will be kept strictly confidential and only used for the formal registration of user ID's and password resets.

To be able to access the service, you will need to have one or more valid user ID's and passwords as per the below guidelines.

- Clients that make use of an **automated routine to download the data files** will be required to register for a company level service account which must only be used for the purpose of automated scripting based downloads. This password will be changed on an annual basis. The JSE strongly recommends that this user name and password be maintained in a configuration file, rather than then being embedded into the scripting code, to better accommodate password changes. **Please note that this service account information must only be known by the required people that have to support the environment.**
- **Clients that make use of manual methods to download the data files,** as primary or acting as backup to the automated scripts, will be required to register an individual user account for each individual person that will be involved in doing download. These user level credentials will be personal and should therefore be treated as such i.e. no username and password sharing should be allowed. Users will be forced to change their password on a monthly basis.

4. PROVISION OF USER ID AND PASSWORD

1. A representative from the JSE Client Data team will provide clients with their Sign-on credentials with 72 hours of the initial request.
2. A representative from the JSE Customer Support team will contact clients to confirm receipt of the file(s), User ID and Password.
3. The onus is on clients to test as soon as they have received the above mentioned information to ensure that their access to the system is correctly configured. Any issues experienced should be immediately reported to the JSE Customer Support team.

5. CONNECTIVITY PROTOCOLS

When connecting to the IDP portal, clients will be allowed access through the use of different protocols. Clients connecting over direct leased lines will be able to make use of File Transfer Protocol (FTP), File Transfer Protocol Secure (FTPS) and a Web service over Hyper Test Transfer Protocol Secure (HTTPS). Clients connecting over the internet will be able to make use of File Transfer Protocol Secure (FTPS) and a Web service over Hyper Test Transfer Protocol Secure (HTTPS).

5.1. FTP (Only available for dedicated leased lines)

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files from a server to a client using the Client–server model on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.

5.1.1. FTP access via the client access network (dedicated leased lines):

Domain Name System (DNS) and IP Address	***For IDP (Not Secured)*** accessftp.jse.co.za **(We recommend using this to protect against future IP address changes)** or 196.216.152.18
Ports	**21** Target Port for **FTP** **20** Return Data Port for **FTP**
Credentials	As supplied by JSE Client Data
File Location for IDP	/IDP

5.2. FTPS

FTPS is a File Transfer Protocol with enhanced security features and provides Transport Layer Security (TLS) connections for inbound and outbound traffic. This is similar to standard FTP but performs operations over an encrypted link (TLS) and is secure. To keep in line with industry best practice, the JSE enforces connections to only take place over TLS versions 1.0 and above, as previous versions of SSL (versions 2 & 3) are deemed vulnerable to sniffing, decryption and malicious attack.

Therefore, **FTPS connections will require implicit TLS 1.0 and above, capable software clients connecting to TCP port 990 using passive mode.**

5.2.1. FTPS Protocol Support

The JSE supports the use of the following secure protocols for FTPS communication:

- TLS 1.0
- TLS 1.1
- TLS 1.2

The JSE does not support the use of the following ciphers for FTPS communication:

- Triple DES (3DES)
- RC4

5.2.1.1. FTPS access via the client access network (dedicated leased lines):

Domain Name System (DNS) and IP Address	***For IDP Securely*** accessidp.jse.co.za **(We recommend using this to protect against future IP address changes)** or 196.216.152.16
Ports	**990** for **FTPS** **65235 to 65535** Return Port range for **FTPS** The revised port range for FTPS allows an increase in the number of concurrent connections to the platform.
Credentials	As supplied by JSE Client Data
File Location for IDP	/IDP

5.2.1.2. FTPS access via the Internet:

Domain Name System (DNS)	***For IDP Securely*** idp.jse.co.za
Ports	**990** Target Port for **FTPS** **65235 to 65535** Return Port range for **FTPS** The revised port range for FTPS allows an increase in the number of concurrent connections to the platform.
Credentials	As supplied by JSE Client Data
File Location for IDP	/IDP

5.3. HTTPS (Only available for the Internet)

HTTPS uses HTTP but additionally activates Web server security, in the form of Transport Security Layer (TLS). This means that the communications between the client and the (host) Web server are encrypted and, additionally, that the host Web server may be validated by the client using a Digital Certificate on the server. To keep in line with industry best practice, the JSE enforces connections to only take place over TLS versions 1.0 and above, as previous versions of SSL (versions 2 & 3) are deemed vulnerable to sniffing, decryption and malicious attack.

5.3.1. HTTPS Protocol Support

The JSE supports the use of the following secure protocols for HTTPS communication:

- TLS 1.0
- TLS 1.1
- TLS 1.2

The JSE does not support the use of the following ciphers for HTTPS communication:

- Triple DES (3DES)
- RC4

5.3.1.1. HTTPS access via the Internet:

Domain Name System (DNS)	https://idp.jse.co.za/IDPService.svc
Credentials	As supplied by JSE Client Data
Usage	Clients will have to request a wsdl file from the idp web service using the specified URL below or load the file using xml below. Clients can then use the wsdl to generate a proxy client that will communicate with the service.
WSDL	https://idp.jse.co.za/IDPService.svc?wsdl

```
<?xml version="1.0" encoding="utf-8" ?>
<wsdl:definitions name="IDPService" targetNamespace="https://idp.jse.co.za/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:wsa10="http://www.w3.org/2005/08/addressing"
xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
xmlns:msc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" xmlns:tns="https://idp.jse.co.za/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:i0="http://tempuri.org/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
 <wsdl:import namespace="http://tempuri.org/" location="https://idp.jse.co.za/IDPService.svc?wsdl=wsdl0" />
<wsdl:types>
<xsd:schema targetNamespace="https://idp.jse.co.za/Imports">
 <xsd:import schemaLocation="https://idp.jse.co.za/IDPService.svc?xsd=xsd0" namespace="https://idp.jse.co.za/" />
 <xsd:import schemaLocation="https://idp.jse.co.za/IDPService.svc?xsd=xsd1"
namespace="http://schemas.microsoft.com/2003/10/Serialization/" />
 </xsd:schema>
 </wsdl:types>
<wsdl:message name="IIDP_InitializeDownload_InputMessage">
 <wsdl:part name="parameters" element="tns:InitializeDownload" />
 </wsdl:message>
<wsdl:message name="IIDP_InitializeDownload_OutputMessage">
 <wsdl:part name="parameters" element="tns:InitializeDownloadResponse" />
 </wsdl:message>
<wsdl:message name="IIDP_GetFileList_InputMessage">
 <wsdl:part name="parameters" element="tns:GetFileList" />
 </wsdl:message>
<wsdl:message name="IIDP_GetFileList_OutputMessage">
 <wsdl:part name="parameters" element="tns:GetFileListResponse" />
 </wsdl:message>
<wsdl:portType name="IIDP">
<wsdl:operation name="InitializeDownload">
 <wsdl:input wsaw:Action="https://idp.jse.co.za/IIDP/InitializeDownload"
message="tns:IIDP_InitializeDownload_InputMessage" />
```

```
 <wsdl:output wsaw:Action="https://idp.jse.co.za/IIDP/InitializeDownloadResponse"
message="tns:IIDP_InitializeDownload_OutputMessage" />
 </wsdl:operation>
<wsdl:operation name="GetFileList">
 <wsdl:input wsaw:Action="https://idp.jse.co.za/IIDP/GetFileList" message="tns:IIDP_GetFileList_InputMessage" />
 <wsdl:output wsaw:Action="https://idp.jse.co.za/IIDP/GetFileListResponse"
message="tns:IIDP_GetFileList_OutputMessage" />
 </wsdl:operation>
 </wsdl:portType>
<wsdl:service name="IDPService">
<wsdl:port name="secure" binding="i0:secure">
 <soap12:address location="https://idp.jse.co.za/IDPService.svc" />
<wsa10:EndpointReference>
 <wsa10:Address>https://idp.jse.co.za/IDPService.svc</wsa10:Address>
 </wsa10:EndpointReference>
 </wsdl:port>
 </wsdl:service>
 </wsdl:definitions>
```

6. FOLDER AND FILE NAMES

Once a connectivity protocol has been chosen, the below file directories may be used as a quick reference guide for specific file downloads for a client. Please remember to have both the target and return ports open for the chosen connectivity protocol.

For **client specific files for the purposes of this testing phase**, a reference table is included below:

Market	File Name	File Location
Equity Derivatives Market (FXM)	1.ED_Test.zip	\Members Test\Member ABC\IDP
	2.ED10_Test.zip	
	3.ED11_Test.zip	
	4.ED12_Test.zip	
	5.ED15_Test.zip	
	6.ED17_Test.zip	
Currency Derivatives Market (FXM)	1.CD_Test.zip	
	2.CD10_Test.zip	
	3.CD11_Test.zip	
	4.CD15_Test.zip	
	5.CD16_Test.zip	
	6.CD17_Test.zip	

Historical information is available for up to 30 days for all files. These have an extension of the following format: D<YYMMDD> where

- YY is the year
- MM is the month (from 01 – 12)
- DD is the day of the month

e.g DDAP.SPRD.(alpha).ED_Test.zip.D170301