ON-BOARDING TOOL
USER GUIDE

HKEX Orion Market Data Platform
Securities Market & Index Datafeed Products
Mainland Market Data Hub (MMDH)

Version 1.2
8 March 2016

DOCUMENT HISTORY

Distribution Version

Version	Date of Issue	Comments
V1.0	23 Nov 2012	First Distribution Issue
V1.1	27 May 2013	Revised library setup
V1.2	8 Mar 2016	Include VCM & CAS canned data set

CONTENTS

1 Introduction

MMDH On-Boarding Tool is a simulation tool that provides testing facilities with simulated market data for the MMDH Information Vendors and End-users (Clients). MMDH On-Boarding Tool facilitates the development, enhancement and testing of the Clients' application systems which receive and process data from MMDH. As HKEX implements changes to MMDH from time to time to support its business initiatives, MMDH On-Boarding Tool will help Clients ensure their readiness for the implementation before joining the Client Test or Market Rehearsal (MR) as required by HKEX.

MMDH On-Boarding Tool also facilitates Clients' workload test (e.g. capacity and performance tests) with the built-in throttle control mechanism. Clients can also make use of the On-Boarding Tool for the testing of their own system development / enhancement. By distributing different test datasets (test data files) to the Clients, HKEX can support clients in testing their systems' readiness for various implementations of MMDH initiatives.

Table 1 Acronyms used in this document

AES	Advanced Encryption Standard
CFB	Cipher FeedBack
DH	Diffie-Hellman
HKEX	Hong Kong Exchanges and Clearing Limited
IV	Information Vendor
MMDH	Mainland Market Data Hub
OMD	Orion Market Data Platform
SHA	Secure Hash Algorithm

1.1 OMD On-Boarding Tool Components

Component	Description
MMDH On-Boarding Tool	MMDH On-Boarding Tool reads canned data and sends messages to Client's application system
MMDH testing client	MMDH testing client application is used to verify the MMDH On-Boarding Tool setup and if it runs properly
Canned Data	Fictitious trading data to facilitate testing - Separate files may exist for different testing purpose (e.g. workload test or functional test) - MMDH On-Boarding Tool will read the canned data and send respective messages to Client's application system.

2 System Requirement, Installation, and Configuration

2.1 Hardware Requirements

- 64-bit AMD or Intel processor
- 4 GB RAM
- 20 GB available disk space

2.2 Software Requirements

HKEX will not provide the follow software / libraries. Clients should go to official website and download software / libraries

- Red Hat Enterprise Linux (RHEL) 6.2 64-bit Edition, or CentOS 6.2 64-bit
- Boost C++ Libraries (Recommended Version: 1.53.0)
- Xerces-C++ (Recommended Version: 3.1.1)
- Crypto++ (Recommended Version: 5.6.1)
- Pantheios (Recommended Version 1.0.1-beta213)
- STLSoft C and C++ Libraries (Recommended Version 1.9.114)

2.3 Network Requirements

- Mode of transmission – IP-based Network
- Communication Line Speed – LAN is preferred with bandwidth greater than the configured Workload rate. e.g. 10Mbps or above is recommended.
- Communication Protocol – TCP

2.4 Installation Procedures

Step	Description

1.	Install Boost C++ Libraries
	
	`tar xvfz boost_1_53_0.tar.gz`
	`cd boost_1_53_0`
	`./bootstrap.sh`
	`./b2`
	
	Modify ~/.bashrc to include the following
	
	`export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/user/Development/include/boost_1_53_0/stage/lib`
	
	`source ~/.bashrc`

2.	Install Xerces-C++
	
	`tar xvf xerces-c-3.1.1-x86_64-linux-gcc-3.4.tar.gz`
	
	Modify ~/.bashrc to include the following
	
	`export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/user/Development/include/xerces-c-3.1.1-x86_64-linux-gcc-3.4/lib`
	
	`source ~/.bashrc`

3.	Install Crypto++
	
	`unzip cryptopp561.zip -d cryptopp561`
	
	`cd cryptopp561`
	
	Modify GNUmakefile
	Uncomment the following
	`# CXXFLAGS += -fPIC`
	
	`make`
	`make libcryptopp.so`
	`make install PREFIX=/home/user/Development/include/cryptopp`
	
	Modify ~/.bashrc to include the following
	
	export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/user/Development/include/cryptopp/lib
	
	`source ~/.bashrc`

4.	Install pantheios and Install stlsoft
	
	unzip pantheios-1.0.1-beta213.zip
	
	unzip stlsoft-1.9.114
	
	Modify ~/.bashrc to include the following
	
	`export PANTHEIOS_ROOT=~/Development/include/pantheios-1.0.1-beta213`
	`export STLSOFT=~/Development/include/stlsoft-1.9.114`
	
	`source ~/.bashrc`
	
	`cd ~/Development/include/pantheios-1.0.1-beta213/build/gcc44.unix.file64bit`
	`make build`

5.	If you are installing from a disc (e.g. CD or DVD), you need to create a mount point and mount the file system. For example,
	
	`mkdir /media/OMD`
	`mount -t udf /dev/sr0 /media/OMD`

6.	Copy the 'mmdh_onboardingTools_1.0.tar.gz' directory from the provided media to the desired host. For example, `cp -r /media/OMD/mmdh_onboardingTools_1.1.tar.gz /home/userid`
7.	Extract the TAR/GZIP file to the correct directory `tar xvzf mmdh_onboardingTools_1.1.tar.gz -C /opt` *Note* - the tool will not work if they are not in the correct directory structure.
8.	Add the correct directory permissions `chown -R {userid:usergroup} /opt/HKEX` Where userid & usergroup are system account that using to run the onboarding tool.

9.	To verify the installation was successful, the following command will show the contents of the install directory
	
	`ls /opt/HKEX/omd/mmdh/`
	
	If successful, the directory will contain
	
	`bin config data lib log`

10.	If you are installing from a disc, unmount the file system and remove the mount point. For example,
	
	`umount /dev/sr0`
	`rmdir /media/OMD`

2.5 Configuration

Configuration is at "/opt/HKEX/omd/mmdh/config/MMDH.xml".

2.5.1 Sample Configuration

The following shows the content of a sample configuration file.

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<MMDH>
  <Address>127.0.0.1</Address>
  <Port>17000</Port>
  <UserName>omd-client1</UserName>
  <PasswordPolicy>


    <!-- MinLength in number of characters -->
    <MinLength>8</MinLength>

    <!-- 0 = Password may contain uppercase character A to Z -->
    <!-- 1 = Password must contain uppercase character A to Z -->
    <ContainUpper>1</ContainUpper>

    <!-- 0 = Password may contain uppercase character a to z -->
    <!-- 1 = Password must contain lowercase character a to z-->
    <ContainLower>1</ContainLower>

    <!-- 0 = Password may contain digit -->
    <!-- 1 = Password must contain digit 0 to 9 -->
    <ContainDigit>1</ContainDigit>

    <!-- Password must be different from last N passwords -->
    <DiffFromLast>5</DiffFromLast>
  </PasswordPolicy>

  <!-- Most recent password is at top of Passwords list -->
  <Passwords>
    <Password>Aa000000</Password>
    <Password>Aa111111</Password>
    <Password>Aa222222</Password>
    <Password>Aa333333</Password>
    <Password>Aa444444</Password>
  </Passwords>

  <!-- ThrottleRate in messages per second -->
```

```
  <ThrottleRate>1000</ThrottleRate>

  <!-- ThrottleInterval in ms -->
  <ThrottleInterval>10</ThrottleInterval>

  <CannedDataPath>/opt/onboardingtool/data/p1-
canned.dat</CannedDataPath>
  <Log>
    <!--
       SEV_EMERGENCY       =   0   /* system is unusable */
       SEV_ALERT           =   1   /* action must be taken
immediately */
       SEV_CRITICAL        =   2   /* critical conditions */
       SEV_ERROR           =   3   /* error conditions */
       SEV_WARNING         =   4   /* warning conditions */
       SEV_NOTICE          =   5   /* normal but significant
condition */
       SEV_INFORMATIONAL   =   6   /* informational */
       SEV_DEBUG           =   7   /* debug-level messages */
      -->
    <SeverityCeiling>
      <File>7</File>
      <Console>3</Console>
      <Syslog>3</Syslog>
    </SeverityCeiling>
    <Path>../log</Path>

    <!-- 0 = Disable outgoing message, 1 = Enable outgoing message --
>
    <EnableOutgoingMsg>1</EnableOutgoingMsg>
  </Log>

  <ReportPath>/opt/onboardingtool/report</ReportPath>
</MMDH>
```

2.5.2 Configuration Description (MMDH.xml)

Configuration	Description
<Address>	The MMDH On-Boarding ToolIP address for the Client's application system to connect to
<Port>	The MMDH On-Boarding Toolport number for the Client's application system to connect to
<UserName>	Used in the Logon (1101) message Username field
<PasswordPolicy>	Password policy related configuration
<MinLength>	Minimum number of character required for a valid password
<ContainUpper>	Whether password is required to contain uppercase character A to Z
<ContainLower>	Whether password is required to contain lowercase character a to z
<ContainDigit>	Whether password is required to contain digit 0 to 9
<DiffFromLast>	Password is different from the last N password, where N is specified using this parameter.
<Passwords>	List of current and previously used passwords
<Password>	The first entry is the current password.
<ThrottleRate>	The number of messages to send out in a second
<ThrottleInterval>	The number of milliseconds between start sending out two batches of messages

<CannedDataPath>	The full path and file name for canned data
<Log>	Logging related configuration
<SeverityCeiling>	The largest severity level that will be logged
<File>	The largest severity level that will be logged to file
<Console>	The largest severity level that will be logged to console
<Syslog>	The largest severity level that will be logged to syslog
<Path>	Log file path
<EnableOutgoingMsg>	Enable outgoing message logging. When this option is enabled, outgoing messages will be logged to YYYYMMDD-HHMMSS-MmdhServer.log
<ReportPath>	Path to save report to

3 System Functions

3.1 Scope

MMDH On-Boarding Tool provides securities market data simulation and workload testing facilities to Clients. The system functions and the relationship diagram between MMDH On-Boarding Tool and Clients' application systems are listed below.

3.1.1 Unsupported functions

Only the following password policies are checked.

- Password shall contain at least 8 characters
- Password shall contain a combination of letters (both upper & lower case) and numbers(0-9)
- New password shall not be the same as any of the last 5 passwords

The following messages are not supported in the On-Boarding Tool.

Message	Message Type
Logout	1103
Refresh Request	1201
Refresh Response	1202
Refresh Complete	203

For Logon Response (1102), only the following SessionStatus values are handled.

SessionStatus	Description
0	Session active
1	Session password changed
3	New session password does not comply with policy
5	Invalid username or password
104	Already Connected

3.1.2 System Functions

- Logon Request
- Change Password Request
- Functional Test Simulation
- Workload Test Simulation
- Reporting and Logging

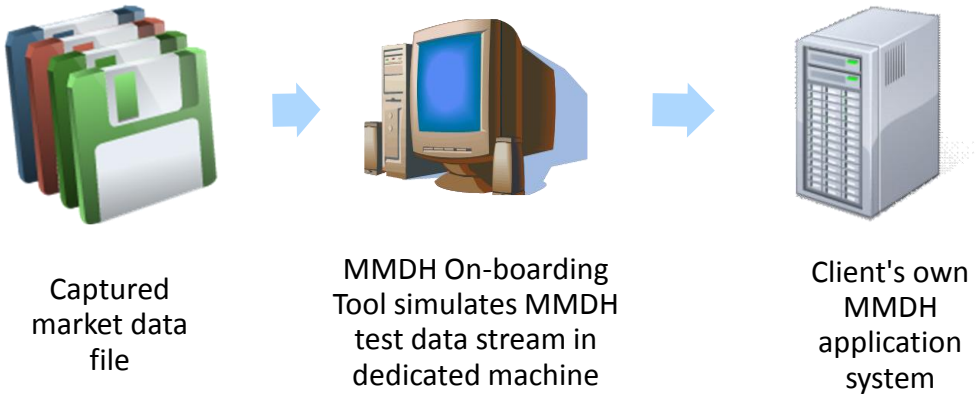
Details will be provided in subsequent sections 3.2 to 3.6.

Function	Description
Logon Request	Handles logon request from Client's application system following the same mechanism as production MMDH except that it does not support intra-day recovery. (i.e. InternalSeqNum in Logon Request will be ignored). It will authenticate the username / password sent by MMDH Client's application system .
Change Password Request	Handles change password request from Client's application system following the same mechanism as production MMDH. It will check against the password history and reject a new password if it is the same as any of the last N passwords, where N is a configurable parameter.

Functional Test Simulation	Plays back simulated market data to assist Clients in conducting their functional test, either to prepare for implementation of the HKEX initiatives, or for their own application system enhancement.
Workload test Simulation	Plays back simulated market data to assist Clients in conducting their workload test, either to prepare for message volume upgrade initiated by HKEX, or for their performance and capacity test for their application system.
Reporting and Logging	Offers "MMDH On-Boarding Tool Workload Report" to Clients to verify their workload test result Offers "Log file" to Clients for their verification of the functional test result or for troubleshooting.

3.1.3 System Relationship Diagram

Clients use captured data for their internal testing



3.2 Logon request

The following is a list of steps to logon to MMDH On-Boarding Tool.

1. MMDH Client's application system initiates connection request.
2. MMDH On-Boarding Tool accepts connection request.
3. MMDH On-Boarding Tool sends Send Key message to MMDH Client's application system .
4. MMDH Client's application system sends logon message to On-Boarding Tool.
5. If authentication is successful, the On-Boarding Tool sends logon response with SessionStatus equal to 0 (Session Active) followed by market data messages. Otherwise, it sends logon response with SessionStatus equal to 5 (Invalid username or password).

Please refer to MMDH interface specification section 3.4.1. The password will be encrypted using the following.

1. OMD public key field and Client's application system's private key, both generated using the same set of Diffie-Hellman (DH) parameters (prime, generator, subgroup order)
2. Initialization Vector in the Send Key message provided by MMDH On-Boarding Tool

The AES CFB mode is used for encryption and decryption

Please refer to Appendix B for MMDH Logon Encryption Sample.

3.3 Change Password Request

- Client's application can change the password by specifying EncryptedNewPasswordLen and EncryptedNewPassword
  fields within the Logon (1101) message. MMDH On-Boarding Tool simulates MMDH to handle change password request and sends back corresponding response message to Client's application systems. (Please refer to MMDH interface specification sections 3.4.2 and 3.4.3 for details.)

3.4 Functional Test Simulation

After successful logon, MMDH On-Boarding Tool will use the configuration in MMDH.xml to playback the desired simulated market dataset according to the workload rate.

HKEX will provide different simulated market datasets for different testing purposes. Clients can load the appropriate dataset to MMDH On-Boarding Tool and start playing back for their functional test on their own MMDH application systems.

MMDH On-Boarding Tool can store and use multiple test data files. Clients are recommended to store all test files in `/opt/HKEX/omd/mmdh/data` and input the correct test file before the test session starts.

3.5 Workload Test Simulation

Simulated market data playback is intended to assist Clients in conducting their workload test. Workload test prepares Clients for HKEX initiated message volume upgrade, and for their application system's performance and capacity test. The <ThrottleRate> and <ThrottleInterval> parameters in the MMDH On-Boarding Tool configuration file (MMDH.xml) control market data feed workload.

3.6 Reporting and Logging

MMDH On-Boarding Tool provides "MMDH On-Boarding Tool Workload Report" to Clients to verify their workload test result. Each test session generates the report and puts the report in a folder defined by <ReportPath> parameter in the MMDH On-Boarding Tool configuration file (MMDH.xml). Please refer to section 2.5 for details.

MMDH On-Boarding Tool provides "Log file" to Clients for checking against their application system receiving log. It helps Clients to verify their application's functionalities and correctness. The "Log file" also facilitates their verification of the functional test result and for their troubleshooting.

3.6.1 MMDH On-Boarding Tool Workload Report

The test report name is in the format of YYYYMMDD-HHMMSS-Report.log. It shows the workload rate and delay information throughout the whole test session. It is a text file and the sample report layout is shown as below.

Report Field	Description
Time	The per minute statistics sampling interval in HH:MM format
Workload Rate	The market data message dissemination rate in messages per second for the statistics sampling interval

Max Delay	Delay is defined as the time difference between the time when MMDH On-Boarding Tool is ready in sending the market data message and the time when MMDH On-Boarding Tool sends the same market data message to the Client. Max Delay for a statistics sampling interval is the largest delay for all messages sent out within the statistics sampling interval.
Mean Delay	Mean Delay for a statistics sampling interval is the average delay for all messages sent out within the statistics sampling interval.

```
Date: 2012-10-22
Configured Workload Rate: 10000 messages per second (msg/s)

Time     Workload Rate (msg/s) Max Delay (s) Mean Delay (s)
   11:13           9994.806485      0.007856       0.002018

Average of [Workload Rate (msg/s)] = 9994.806485
Maximum of [Max Delay (s)]         = 0.007856
Average of [Mean Delay (s)]        = 0.002018
```

3.6.2 Log File

The log file name is in the format of YYYYMMDD-HHMMSS-MmdhServer.log. It contains messages received by MMDH On-Boarding Tool (incoming) and messages sent out by MMDH On-Boarding Tool (outgoing). It is a text file and the sample report layout is shown as below.

Field	Description
Process ID	Is always MmdhServer
Thread ID	Different threads have different thread IDs
Date time	The local date and time at which the message was logged
Severity	The severity level of the log message
Entry	Incoming messages have "[Incoming]" prefix Outgoing messages have "[Outgoing]" prefix

Sample Log

[MmdhServer.140030807193376, Oct 22 14:14:23.165; Notice]: Logon Configuration:
In the above sample, we have

Field	Value
Process ID	MmdhServer
Thread ID	140030807193376
Date time	Oct 22 14:14:23.165
Severity	Notice
Entry	Logon Configuration:

4 Operational Procedures

4.1 Starting OMD On-Boarding Tool

Step	Description

1.	Run the MMDH On-Boarding Tool
	
	`cd /opt/HKEX/omd/mmdh/bin`
	`./MmdhServer -c ../config/MMDH.xml`

2.	You will see the following message. `Please enter throttle rate (ENTER = 10000 messages per second)`
3.	Do one of the following 1. Press the Enter key to accept default throttle rate 2. Input another throttle rate and press the Enter key to use the new rate
4.	The selected throttle rate similar to the following will be shown. `Throttle rate is 10000 messages per second.`
5.	You will see the following message. Please enter canned data path (ENTER = `/opt/HKEX/omd/mmdh/data`/mmdh_canned_data_02102012.cap)
6.	Do one of the following 1. Press the Enter key to accept default canned data path 2. Input another canned data path and press the Enter key to use the new path
7.	The selected canned data path similar to the following will be shown. `Canned data path is` `/opt/HKEX/omd/mmdh/data`/mmdh_canned_data_02102012.cap
8.	You will see the following header showing the current date. Date: 2012-10-18 Configured Workload Rate: 10000 messages per second (msg/s) Time Workload Rate (msg/s) Max Delay (s) Mean Delay (s)
9.	Client's Application system connect to MMDH On-Boarding Tool

10.	You will see something similar to the following at the MMDH On-Boarding Tool terminal. The output will be updated every 5 seconds before completion.
	
	`16:09:50 9796.695877 0.004535 0.001633`
	`16:09:55 10012.334631 0.008353 0.001383`
	`16:10:00 9992.793737 0.007968 0.001363`
	`16:10:05 9964.659816 0.004953 0.001237`
	
	`Average of [Workload Rate (msg/s)] = 9996.656777`
	`Maximum of [Max Delay (s)] = 0.008353`
	`Average of [Mean Delay (s)] = 0.001359`

11.	You will see something similar to the following in the report. The report will be updated every minute before completion.
	
	`Date: 2012-10-18`
	`Configured Workload Rate: 10000 messages per second (msg/s)`
	
	`Time Workload Rate (msg/s) Max Delay (s) Mean Delay (s)`
	`16:09 10008.867897 0.008353 0.001387`
	`16:10 9986.874052 0.007968 0.001337`
	
	`Average of [Workload Rate (msg/s)] = 9996.656777`
	`Maximum of [Max Delay (s)] = 0.008353`
	`Average of [Mean Delay (s)] = 0.001359`

Verify MMDH On-Boarding Tool setup and run properly using MMDH testing client

Step	Description

1.	Run the MMDH testing client in another terminal
	
	`cd /opt/HKEX/omd/mmdh/bin`
	`./MmdhClient -c ../config/MMDH.xml`

2.	You will see the following message. `Please enter a password (maximum 20 characters)`
3.	Input the password and press the Enter key
4.	You will see the following message. `Please enter a new password (maximum 20 characters, ENTER = none)`
5.	Do one of the following 1. Press the Enter key if you are not changing password 2. Input the new password to change to and press the Enter key
6.	You will see the following message at the testing client terminal. `LogonResponse: 0 (Session active)`

4.2 Log Files

There are three types of log files in the MMDH On-boarding Tool and they are described as follows.

Log file	Description
YYYYMMDD-HHMMSS-MmdhClient.log	Contains MmdhClient log messages
YYYYMMDD-HHMMSS-MmdhServer.log	Contains MmdhServer log messages
YYYYMMDD-HHMMSS-Report.log	Contains a report that shows per minute and overall workload rate, max delay, and mean delay

Log files can be found at the log file path.

4.3 Test Result Verification

4.3.1 Functional Test Simulation

Clients can check if the following criteria are met to verify if their systems are functional ready for subsequent HKEX on-boarding activities.

- No error generated during the test session
- All outgoing messages logged in the MmdhServer log file, e.g. YYYYMMDD-HHMMSS-MmdhServer.log have been received by Client's application system. The messages can be verified by matching the Sequence Number (SeqNum) in this sent log file.

4.3.2 Workload Test Simulation

Clients can check if the following criterion is met to verify if their systems can handle MMDH planned capacity for participating in subsequent HKEX on-boarding activities.

- No error generated during the test session

4.3.3 Result Checking for System Readiness

HKEX may request clients to submit functional and/or workload test simulation test results with the corresponding log/report. This confirms that their systems are ready for HKEX major business initiative implemented in MMDH, for joining HKEX arranged Readiness Test, Client Tests and Market Rehearsals.

Appendix A Troubleshooting

A.1 MMDH On-Boarding Tool cannot be installed

Please make sure the target installation machine meet the system requirement stated in section 2 and root privilege is required during installation.

A.2 MMDH On-Boarding Tool cannot be started

Please make sure the target installation machine meet the system requirement stated in section 2 and:

- Required LAN connection is enabled
- Required port number (stated in <Port> parameter in MMDH.xml) is not used by other software or blocked by any security software such as firewall.

A.3 Cannot open config file

Make sure that MMDH.xml exists and in the correct location

A.4 Cannot open canned data

Make sure that canned data file exists and in the correct location

A.5 Server 127.0.0.1:17000 Error: Connection refused

Make sure that MmdhServer is started before MmdhClient

A.6 Server 127.0.0.1:17000 Error: Connection reset by peer

Check if MmdhServer is still running

A.7 LogonResponse: 5 (Invalid username or password)

Check MMDH.xml to make sure that you have entered the correct password

A.8 LogonResponse: 3 (New session password does not comply with policy)

Check MMDH.xml to make sure that the new password complies with password policy

Appendix B MMDH Logon Encryption Sample

An example shows how to logon to MMDH.

```
switch (msgType) {
   case SEND_KEY_TYPE:
   {
    // Make use of Prime, Generator, PrimeOrderSubgroup, and OMDPublicKey fields
    // in Send Key message
    processSendKeyMsg();

     // Generate Diffie-Hellman public and private keys
     generateKeyPair();

     // Create shared key using generated private key and received OMDPublicKey field
     computeSharedKey();

     // Calculate SHA-256 message digest
     calcDigest();

     // Use AES to encrypt password
     aesEncrypt(password, passwordLen, encryptedPassword);

     // If change password, use AES to encrypt new password
     aesEncrypt(newPassword, newPasswordLen, encryptedNewPassword);

     break;
  }

  case LOGON_RESPONSE_TYPE:
  {
     processLogonResponseMsg();
     break;
  }

  default:
     break;
}
```

Clients can follow above pseudo code to compose Logon message. The following shows Send Key message sample field values. Clients can derive the encrypted password as per illustration.

Field	Value
MsgSize	532
MsgType	1105
Prime	b1 0b 8f 96 a0 80 e0 1d de 92 de 5e ae 5d 54 ec 52 c9 9f bc fb 06 a3 c6 9a 6a 9d ca 52 d2 3b 61 60 73 e2 86 75 a2 3d 18 98 38 ef 1e 2e e6 52 c0 13 ec b4 ae a9 06 11 23 24 97 5c 3c d4 9b 83 bf ac cb dd 7d 90 c4 bd 70 98 48 8e 9c 21 9a 73 72 4e ff d6 fa e5 64 47 38 fa a3 1a 4f f5 5b cc c0 a1 51 af 5f 0d c8 b4 bd 45 bf 37 df 36 5c 1a 65 e6 8c fd a7 6d 4d a7 08 df 1f b2 bc 2e 4a 43 71
Generator	a4 d1 cb d5 c3 fd 34 12 67 65 a4 42 ef b9 99 05 f8 10 4d d2 58 ac 50 7f d6 40 6c ff 14 26 6d 31 26 6f ea 1e 5c 41 56 4b 77 7e 69 0f 55 04 f2 13 16 02 17 b4 b0 1b 88 6a 5e 91 54 7f 9e 27 49 f4 d7 fb d7 d3 b9 a9 2e e1 90 9d 0d 22 63 f8 0a 76 a6 a2 4c 08 7a 09 1f 53 1d bf 0a 01 69 b6 a2 8a d6 62 a4 d1 8e 73 af a3 2d 77 9d 59 18 d0 8b c8 85 8f 4d ce f9 7c 2a 24 85 5e 6e eb 22 b3 b2 e5
PrimeOrderSubgroup	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f5 18 aa 87 81 a8 df 27 8a ba 4e 7d 64 b7 cb 9d 49 46 23 53
OMDPublicKey	10 f3 54 8b ba 42 5d 99 80 0d 1a cd 89 07 ae 75 8b 17 06 5f 47 8a 8e 47 7b 6b 5c 00 3c 60 ac ea 9d 6c 78 30 53 78 d9 f4 90 20 2a e4 a5 9b 52 47 cc c7 2b 26 ba 60 16 eb fe cc da ae cc c0 c1 9a a7 e1 d4 21 bc f5 be 8e f3 7f 60 1b 5b ec 03 2f 5f 08 a4 97 58 76 09 b2 ae de d0 87 9b 2d 4e 42 ac a2 82 b9 0a a0 75 bf 7e 26 45 84 7e 7b eb 3d 46 fc 72 ba 75 19 c2 08 86 9b 56 fe ba e2 32 c5 e7 da 0c 79 bc 11 8d 95 54 1d b1 5d c8 55 68 c5

The following shows Logon message field values using Client Public Key derived from the information provided in above SendKey message and the Client Private Key.

Field	Value
MsgSize	190
MsgType	1101
Username	omd-client1
InternalSeqNum	0
ClientPublicKey	40 3e 53 0b 3b ff 20 30 98 23 66 45 13 dd 60 0b 00 9e d5 99 3d 3d c8 ae a2 d2 ea c1 8b 89 1d c9 90 de c4 5f 06 98 77 33 83 db a1 29 6f b8 e9 e5 d5 fc 9c aa b3 0d f4 97 9a 6a f9 50 72 cc 59 1e eb 6d 23 06 d6 85 57 54 30 8e 37 db 23 56 af 71 a5 de ed 44 52 37 3e 38 28 45 55 f9 56 c2 d7 c1 cb 52 2b 7a 2c d2 f6 fb 04 9a 7c f4 07 6f 50 15 92 76 27 2d f9 b2 46 90 6d d6 2e 1e 73 a8 87 0e

ClientPrivateKey	7d 83 02 bc 77 c5 b6 5c 01 61 f5 f6 d2 7f 5f 49 c4 18 d5 fb
EncryptedPasswordLen	8
EncryptedPassword	29 b8 34 2d 61 5d 46 14
EncryptedNewPasswordLen	0
EncryptedNewPassword	